Versión 2.7.0.0

Technical Support Appliance
Guía de configuración

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información de "Avisos" en la página 145.

Vigésimo tercera edición (agosto de 2020)

Esta edición se aplica a la versión 2, release 7 modificación 0 de IBM® Technical Support Appliance y a todos los releases y modificaciones posteriores hasta que se indique de lo contrario en nuevas ediciones.

Contenido

Figuras ..... **vii**

Capítulo 1. Introducción **1**
Cuentas de usuario y grupos de usuarios 1
Alcances de descubrimiento y Conjuntos de alcances 2
Credenciales de descubrimiento 2
Planificación de descubrimiento 3
Planificación de transmisión 3

Capítulo 2. Requisitos previos **5**
Descarga de una imagen de TSA 5
Requisitos para TSA 5
Navegadores web necesarios 5
Requisitos de configuración para las conexiones al servicio de soporte de IBM 6
Requisitos de credenciales y de software para el entorno de descubrimiento 6

Capítulo 3. Instalación de Technical Support Appliance **9**
Instalación mediante la interfaz web de VMware ESXi 9
Instalación de TSA en Microsoft Hyper-V 12
Cambio de contraseña de *tsausr* (necesario) 19
Configuración de los datos de red 19

Capítulo 4. Configurar el Technical Support Appliance **21**
Inicio de sesión en Technical Support Appliance 21
Aceptación del acuerdo de licencia 23
Utilización del Asistente de instalación para la configuración inicial 25
Configurar la conectividad con IBM 26
Registrar el Technical Support Appliance 27
Configurar el reloj 29
Configuración de la planificación de transmisión 31
Actualización de Technical Support Appliance 32
Configurar los valores de red 33
Configurar los valores de red básicos 33
Configurar los valores de red avanzados 35
Configuración de certificados 41
Ver el estado del certificado de servidor SSL 42
Generar y descargar CSR 42
Instalar un certificado personalizado (utilizando firmantes) 43
Instalar un certificado personalizado (método alternativo) 44
Restaurar el certificado predeterminado 45
Planificar la limpieza de datos de inventario 46

Capítulo 5. Configurar el descubrimiento y la transmisión a IBM **49**
Alcances de descubrimiento 49
Alcances dinámicos de HMC 49
Alcances dinámicos de VMware 57
Alcances de descubrimiento general 66
Importar un conjunto de alcances 71
Configuración de descubrimiento 72

Configurar los valores de conexión....72
Credenciales de descubrimiento....73
Ver las credenciales....73
Ver información detallada de credenciales....74
Añadir credenciales....74
Modificar credenciales....77
Suprimir credenciales....78
Planificación de descubrimiento....78
Ver la planificación de descubrimiento....79
Añadir planificación de descubrimiento....80
Modificar la planificación de descubrimiento....82
Suprimir la planificación de descubrimiento....83
Ejecutar el descubrimiento....83
Ejecutar el descubrimiento en alcances....86
Historial de descubrimiento....89
Planificación de transmisión....89
Ver la planificación de transmisión....90
Modificar la planificación de transmisión....90
Deshabilitar la planificación de transmisión....92
Ejecutar la transmisión....92
Instantánea de datos....93
Ver el resumen de inventario....95
Depuración de problemas de descubrimiento....96
Estado de autenticación....96
Dispositivos desconocidos....97

Capítulo 6. Configurar las tareas administrativas....99
Información de estado....99
Ver el registro de actividad....99
Ver el archivo de limpieza de inventario....100
Contraseñas....101
Cambiar la contraseña....101
Seguridad....101
Modificar los valores de tiempo de espera de sesión....101
Modificar la duración de la contraseña....102
Copia de seguridad y restauración....102
Actualizar....104
Habilitar el mantenimiento planificado....106
Registro y rastreo....107
Apagado....108
Herramientas....110
Herramientas de red....110
Herramientas de base de datos....111
Documentación....112

Capítulo 7. Contactar con el servicio de soporte de IBM en relación a Technical Support Appliance (TSA)....115
Abrir un caso en IBM Support Portal....115
Crear una solicitud de servicio a través de IBM Call Center....115

Apéndice A. Instalación de TSA utilizando el Cliente de VMware vSphere....117

Apéndice B. Configuración de Technical Support Appliance....123
Registrar el Technical Support Appliance....123
Configurar la conectividad con IBM....125
Configurar el reloj....127
Configuración de la planificación de transmisión....129

Actualizar 130

Apéndice C. Configuración de los datos de red DHCP 133

Apéndice D. Cuentas de usuario y grupos de usuarios 135
Visualizar cuentas de usuario y grupos de usuarios 135
Añadir cuentas de usuario y grupos de usuarios 135
Añadir un grupo de usuarios 136
Añadir una cuenta de usuario 138
Modificar cuentas de usuario y grupos de usuarios 140
Modificar cuentas de usuario 140
Modificar grupos de usuarios 141
Suprimir cuentas de usuario y grupos de usuarios 142
Suprimir cuentas de usuario 142
Suprimir grupos de usuarios 142

Accesibilidad 143

Avisos 145
Marcas registradas 146

Figuras

1. Crear/Registrar máquina virtual....9

2. Seleccionar el tipo de creación....10

3. Seleccionar archivos OVF y VMDK....10

4. Seleccionar almacenamiento....11

5. Opciones de despliegue....11

6. Revisar los valores seleccionados....12

7. Hyper-V Manager....13

8. Nombre de máquina virtual....13

9. Especificar generación....14

10. Memoria de inicio....15

11. Configurar red....16

12. Conectar disco duro virtual....17

13. Resumen....18

14. Hyper-V Manager....18

15. Cambiar contraseña....19

16. Nueva contraseña....19

17. Realizar configuración de red....19

18. Configuración de red....20

19. Inicio de sesión....22

20. Cambiar contraseña....22

21. Acuerdo de licencia....24

22. Asistente de instalación....25

23. Conectividad de IBM....26

24. Registro..... 28

25. Reloj..... 30

26. Semanalmente los días (dom - sáb)..... 31

27. Disponibilidad de actualizaciones..... 32

28. No hay ninguna actualización disponible..... 32

29. Asistente de instalación completado..... 33

30. Red..... 34

31. Acceda a la página Red (opciones avanzadas)..... 36

32. Red (opciones avanzadas) - Global..... 37

33. Red (opciones avanzadas) - Interfaces de red..... 38

34. Red (opciones avanzadas) - Configuración de DNS..... 39

35. Red (opciones avanzadas) - Rutas de red..... 40

36. Nueva ruta de red..... 41

37. Estado de certificado de servidor SSL..... 42

38. Solicitud de firma de certificado..... 43

39. Instalar certificado personalizado..... 44

40. Instalación de certificado personalizado..... 45

41. Establecer el certificado del dispositivo al predeterminado..... 46

42. Planificación de limpieza de inventario..... 47

43. Alcances dinámicos de HMC..... 50

44. Ver un Conjunto de alcances dinámicos de HMC..... 51

45. Añadir conjunto de alcances dinámicos de HMC..... 52

46. Ejemplo: Especificar información de acceso de las LPAR de Linux..... 53

47. Alcances dinámicos de VMware..... 58

48. Ver conjunto de alcances dinámicos de VMware..... 59

49. Añadir conjunto de alcances dinámicos de VMware..... 60

50. Especificar información de acceso de la máquina virtual de Linux..... 61

51. Especificar información de acceso de la máquina virtual de Windows..... 62

52. Conjunto de alcances de descubrimiento..... 67

53. Alcances de descubrimiento general..... 68

54. Importar conjunto de alcances..... 72

55. Nuevas credenciales de descubrimiento..... 73

56. Detalles de credencial de descubrimiento..... 74

57. Nuevas credenciales de descubrimiento..... 75

58. Planificación de descubrimiento..... 80

59. Añadir planificación de descubrimiento..... 81

60. Semanalmente los días (dom - sáb)..... 82

61. Ejecutar descubrimiento en alcances específicos..... 84

62. Alcances dinámicos de HMC..... 85

63. Ejecutar el descubrimiento en Alcances dinámicos de VMware..... 85

64. Alcances de descubrimiento..... 86

65. Ejecutar descubrimiento en alcances específicos..... 87

66. Alcances dinámicos de HMC..... 87

67. Ejecutar descubrimiento en alcances específicos..... 88

68. Alcances dinámicos de VMWare..... 88

69. Ejecutar el descubrimiento en alcances dinámicos de VMware..... 89

70. Historial de descubrimiento..... 89

71. Editar planificación de transmisión..... 91

72. Semanalmente los días (dom - sáb)..... 91

73. Ejecutar transmisión ahora..... 93

74. Instantánea de datos..... 94
75. Fecha de instantánea de datos..... 94
76. Resumen de inventario..... 95
77. Detalle del resumen de inventario..... 96
78. Estado de autenticación..... 97
79. Registro de actividad..... 99
80. Archivo de limpieza de inventario..... 100
81. Copia de seguridad y restauración..... 103
82. Actualizar..... 105
83. Disponibilidad de actualizaciones..... 105
84. Realizar actualización ahora..... 106
85. Registro y rastreo..... 108
86. Apagado..... 109
87. Herramientas de red..... 110
88. Documentación..... 113
89. Desplegar plantilla de OVF..... 117
90. Origen de plantilla de OVF..... 118
91. Nombre y ubicación..... 119
92. Almacenamiento..... 120
93. Formato de disco..... 121
94. Listo para finalizar..... 122
95. Registro..... 124
96. Conectividad de IBM..... 126
97. Reloj..... 128
98. Editar planificación de transmisión..... 129

99. Semanalmente los días (dom - sáb).....130

100. Actualizar..... 131

101. Disponibilidad de actualizaciones.....131

102. Realizar actualización ahora.....132

103. Realizar configuración de red.....133

104. Configuración de red.....133

105. Dirección IP DHCP..... 134

106. Grupos.....136

107. Añadir grupo de usuarios..... 137

108. Cuentas de usuario y grupos de usuarios..... 138

109. Añadir cuenta de usuario.....139

110. Modificar cuenta de usuario administrador..... 141

Capítulo 1. Introducción

Technical Support Appliance (TSA) es una herramienta de fácil uso que le permite obtener más valor de sus contratos de soporte de IBM. TSA descubre elementos clave de las tecnologías de la información y sus relaciones dentro de su infraestructura de TI y, a continuación, 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 las aplicaciones, el middleware, los servidores y los componentes de red de su centro de datos.

TSA incluye una interfaz de usuario (IU) basada en web para configurar y personalizar el acceso a su sistema y a sus datos. La IU también le permite modificar las planificaciones de descubrimiento y transmisión de datos.

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

Los 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.

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.

Cuentas de usuario y grupos de usuarios

Para ejecutar cualquier función de TSA se requiere un cierto nivel de autorización. Si un usuario autenticado intenta llevar a cabo una función sin tener el nivel de autorización adecuado, se muestra un error y no se ejecuta la función.

Dentro de una organización, se pueden crear roles para diversas funciones de trabajo. Se asignan permisos para llevar a cabo ciertas operaciones a roles específicos. A los usuarios de TSA se les asignan unos roles en particular, y mediante esas asignaciones de rol tienen los permisos para llevar a cabo funciones de sistema concretas. De esta forma, cualquier usuario que tenga asignado un rol tendrá el nivel de autorización asociado a ese rol, y es fácil añadir un Usuario a un rol, cambiar usuarios de un rol a otro o eliminar usuarios de un rol.

En TSA, los roles se gestionan con grupos de usuarios que tienen asociados niveles de autorización. Los usuarios se gestionan con cuentas de usuario. A las cuentas de usuario se les puede asignar la pertenencia a uno o más grupos de usuarios, y al ser miembros de esos grupos, los usuarios tienen el nivel de autorización para llevar a cabo ciertas funciones.

Además, los grupos de usuarios se pueden restringir a conjuntos de alcances seleccionados. Un conjunto de alcances es una colección de direcciones IP, rangos de direcciones o subredes que identifican los elementos de TI que TSA puede descubrir. Especificar restricciones de conjunto de alcances para un grupo de usuarios es una forma de limitar más el acceso de los miembros de ese grupo de usuarios. Por ejemplo, es posible crear grupos de usuarios específicos de una plataforma, como por ejemplo usuarios responsables de man tener sistemas Linux®, mediante una combinación de restricciones de nivel de autorización y conjunto de alcances asociadas a un grupo de usuarios concreto.

Alcances de descubrimiento y Conjuntos de alcances

Los alcances de descubrimiento identifican los recursos que desea que TSA descubra. Los alcances de descubrimiento se agrupan en conjuntos de alcances de descubrimiento.

Puede especificar alcances de descubrimiento utilizando una dirección IP, un rango de direcciones IP o una red o subred para definir los recursos a los que se accede durante el descubrimiento. Un alcance de descubrimiento puede ser tan pequeño como una sola dirección IP, o tan grande como un rango de direcciones IP o una red.

Para simplificar la creación de un conjunto de alcances, se puede utilizar un archivo para importar una lista de direcciones IP. Para obtener más información, consulte la sección "Importar un conjunto de alcances" en la página 71.

Como más direcciones IP haya en el alcance de descubrimiento, más dura el descubrimiento. Puede modificar el tamaño del descubrimiento deshabilitando o habilitando conjuntos de alcances de descubrimiento o excluyendo las direcciones IP, los rangos de direcciones IP, o las redes o subredes de un alcance dentro de un conjunto de alcances.

Nota: Para conseguir un mejor rendimiento, limite el número acumulativo de direcciones IP (dirección IP, rangos, subredes y exclusiones) en un conjunto de alcances a 400 o menos.

Tareas relacionadas

Añadir cuentas de usuario y grupos de usuarios
Puede añadir cuentas de usuario y grupos de usuarios para controlar el acceso a las funciones de TSA.

Credenciales de descubrimiento

Las Credenciales de descubrimiento son una colección de nombres de usuario, contraseñas o claves SSH, y cadenas de comunidad SNMP (Simple Network Management Protocol) que TSA utiliza para acceder a los recursos durante el descubrimiento.

Debe configurar y realizar el mantenimiento de las credenciales de descubrimiento de los recursos que desea descubrir. La información de acceso que tiene que proporcionar varía según el tipo de credencial, pero generalmente incluya al menos un nombre de usuario y una contraseña o clave SSH.

Una credencial de descubrimiento se puede aplicar a todos los conjuntos de alcances o restringirse a un solo conjunto de alcances. Definir credenciales que se aplican a un solo conjunto de alcances mejora el rendimiento e impide los intentos de inicio de sesión no válidos, que pueden dar como resultado que se bloquee la cuenta.

Al acceder a un recurso, TSA utiliza de forma secuencial cada una de las credenciales asociadas a un alcance en particular en el orden en que aparece en la página **Credenciales de descubrimiento** hasta que el recurso da permiso a TSA para acceder a él. Por ejemplo, al acceder a un sistema informático, TSA utiliza el primer nombre de usuario y contraseña especificados en la lista de credenciales para sistemas informáticos y asociados al conjunto de alcances que lo contiene. Si el nombre de usuario y la contraseña son incorrectos para un sistema informático en particular, TSA automáticamente utiliza el siguiente nombre de usuario y contraseña especificados en la lista de credenciales para sistemas informáticos.

Consejo: Antes de guardar las credenciales, puede probar si ha especificado credenciales válidas para los distintos tipos de sistemas, como por ejemplo **Sistema informático**, **Sistema informático (Windows)**, **SNMP** o **SNMPV3**. Con estas pruebas puede asegurarse de que las credenciales se han definido de forma válida.

Consejo:

- Utilice una cuenta de servicio con una contraseña común para todos los dispositivos de un tipo concreto, como por ejemplo AIX o Windows. Se puede definir una sola credencial para descubrir todas las instancias de este tipo de dispositivo.
- Utilice cuentas donde no caduquen las contraseñas.

- Utilice claves SSH siempre que sea necesario.

Planificación de descubrimiento

Los descubrimientos se ejecutan en días y horas planificados para asegurarse de que los datos descubiertos son siempre actuales y precisos. TSA tiene una planificación de "Descubrimiento completo" que lleva a cabo un descubrimiento de todos los conjuntos de alcances definidos. Esta planificación predeterminada puede modificarse según sus necesidades. También puede crear planificaciones que permitan el descubrimiento de los conjuntos de alcances que se van a distribuir en distintas horas y fechas. También puede ver los detalles, el historial y el estado del último descubrimiento que se ha ejecutado.

Al modificar una planificación de descubrimiento, se debe especificar el nombre, los conjuntos de alcances, la hora de inicio y la frecuencia de los descubrimientos. Si la planificación de descubrimiento es la planificación de descubrimiento predeterminada solo puede modificar la hora de inicio y la frecuencia de los descubrimientos. También puede ejecutar descubrimientos a demanda.

La duración del descubrimiento depende de varios factores que también incluyen el número y la complejidad de los recursos y puede tardar hasta 72 horas en completarse.

Planificación de transmisión

Los datos descubiertos se empaquetan y se transmiten de forma segura al servicio de soporte de IBM en fechas y horas planificadas para asegurarse de que IBM tiene la información más actualizada y más exacta. TSA tiene una planificación de transmisión predeterminada que puede modificar según sus necesidades. También puede ejecutar transmisiones a demanda. También puede ver el estado de la última transmisión que ha ejecutado.

El tiempo transcurrido para una transmisión depende de la cantidad de datos descubiertos.

Capítulo 2. Requisitos previos

Para configurar y utilizar TSA, es necesario cumplir ciertos requisitos previos, como por ejemplo las credenciales necesarias para el entorno de descubrimiento y los requisitos de configuración para conectarse a IBM Support.

Nota: Todos los requisitos previos de las secciones siguientes son obligatorios para TSA con la excepción de los requisitos especificados en la sección "Requisitos para TSA" en la página 5.

Descarga de una imagen de TSA

Hay disponibles imágenes de TSA para los servidores de Microsoft Hyper-V [*TSA-HYPERV-<versión>*] y VMware [*TSA-VMWARE-<versión>*] .

Puede obtener las instrucciones de descarga en: https://ibm.biz/TSAdemo

Requisitos para TSA

Para poder configurar y utilizar TSA, se deben cumplir los requisitos previos siguientes.

Hardware x86 de 64 bits
TSA se debe cargar en sistemas x86 de 64 bits.

Hipervisor
TSA necesita VMware ESXi o Microsoft Hyper-V

Nota: Se recomienda utilizar cualquier versión admitida de ESXi o Hyper-V.

Procesador
TSA necesita un procesador de cuatro núcleos y 2,26 GHz, como mínimo.

CPU
TSA necesita cuatro CPU de 64 bits.

Memoria
TSA necesita 16 GB de memoria.

Dispositivo de almacenamiento de acceso directo (DASD)
TSA necesita 150 GB de DASD.

Red
TSA necesita un adaptador Ethernet de 1 Gigabit.

Navegadores web necesarios

Para configurar y supervisar el descubrimiento y la transmisión, se utiliza una interfaz de usuario basada en web.

TSA admite los navegadores de Internet siguientes:

- Mozilla Firefox V68.9.0 Extended Support Release (ESR)
- Microsoft Edge V83.0.478.54 para Windows 10
- Google Chrome V83.0.4103.116 (64 bits)

Puede descargar estos navegadores de los sitios siguientes:

- Mozilla Firefox (http://www.mozilla.org/products/firefox/)
- Microsoft Edge (https://www.microsoft.com/en-us/edge)

- Google Chrome (https://support.google.com/chrome/answer/95346?hl=en)

Requisitos de configuración para las conexiones al servicio de soporte de IBM

TSA se puede conectar al servicio de soporte de IBM a través de una conexión directa o mediante un proxy proporcionado por el usuario que debe configurar para permitir la comunicación con IBM. Si utiliza un proxy, no se admite la inspección TLS/SSL. Las solicitudes que vayan por un proxy deben poder fluir directamente a IBM sin terminación TLS/SSL.

Asegúrese de que su cortafuegos permite conexiones a las direcciones IP y el nombre de host de servidor de IBM, tal como se explica en la tabla Conexiones de red. Si la red no permite el acceso a los servidores de IBM, las transacciones de TSA al servicio de soporte de IBM no se podrán realizar.

Tabla 1. Conexiones de red

Nombre de DNS	Dirección IP	Puerto	Protocolo
esupport.ibm.com	129.42.54.189	443	HTTPS (a IBM)
	129.42.56.189		
	129.42.60.189		

El entorno de servidor de IBM es totalmente compatible con NIST SP800-131A, y admite el protocolo TLS 1.2, funciones hash SHA-256 o más fuertes y claves RSA con una potencia de al menos 2048 bits.

Nota: No se admite la inspección SSL, si la utiliza en el proxy, deshabilítela para estos flujos.

En proxies Blue Coat, deshabilite la "detección de protocolo" para servidores IBM. Añada estas reglas de configuración:

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

Requisitos de credenciales y de software para el entorno de descubrimiento

Para descubrir puntos finales o recursos en su entorno, TSA debe tener acceso a esos recursos. Se recomienda crear una cuenta de servicio en cada recurso que sea específicamente para utilizar con TSA para acceder a ese recurso.

Tras crear una cuenta de servicio en un recurso, debe definir y mantener credenciales en TSA que coincidan con las credenciales definidas en el recurso para esa cuenta de servicio. TSA utiliza esas credenciales para acceder al recurso. Los requisitos para las credenciales varían según el entorno y el tipo de recurso que desea descubrir, pero generalmente incluyen un nombre de usuario y una contraseña o una clave SSH. Algunos recursos, además tienen requisitos de software específicos.

Tipo de credencial	Información de acceso
Sistema informático	**Nombre de usuario:** Nombre de usuario para acceder al dispositivo. **Contraseña / Frase de contraseña** Contraseña / frase de contraseña para acceder al dispositivo. **Tipo de autenticación:** El tipo de autenticación para el dispositivo. • **Contraseña** - Utilizar la contraseña proporcionada. • **PKI** - Utilizar la clave SSH asociada al conjunto de alcances específico.
Sistema informático (Windows)	**Nombre de usuario:** Nombre de usuario para acceder al sistema Windows. **Contraseña:** Contraseña para acceder al sistema Windows.
Elemento de red (SNMP)	**Cadena de comunidad:** La cadena de comunidad del dispositivo.
Elemento de red (SNMPV3)	**Nombre de usuario:** El nombre de usuario para acceder al dispositivo. **Contraseña:** La contraseña para acceder al dispositivo. **Contraseña privada:** La contraseña que se utiliza si se ha establecido el cifrado de datos para SNMP. **Protocolo de autenticación:** El tipo de protocolo de autenticación que utiliza SNMP. • Ninguno • MD5 • SHA
Otros (dispositivo Cisco)	**Nombre de usuario:** El nombre de usuario para acceder al dispositivo Cisco. **Contraseña:** La contraseña del dispositivo Cisco. **Contraseña de habilitación:** La contraseña de habilitación del dispositivo Cisco.
Otros (CiscoWorks)	**Nombre de usuario:** El nombre de usuario para acceder al servidor de CiscoWorks. **Contraseña:** La contraseña para acceder al servidor de CiscoWorks.

Nota: Para obtener más información sobre requisitos de software y de credenciales, consulte la Guía del asistente de configuración.

Capítulo 3. Instalación de Technical Support Appliance

TSA incluye software preinstalado. Se empaqueta y distribuye en forma de imagen para instalaciones de VMware o en forma de imagen VHDX para instalaciones de Microsoft Hyper-V. Para VMware, TSA se puede instalar utilizando el Cliente de VMware vSphere o la interfaz web de VMware (para ESXi). Para Hyper-V, TSA se puede instalar utilizando Hyper-V Manager. En esta sección, se indican los pasos necesarios para instalar TSA utilizando cualquiera de estos métodos.

Instalación mediante la interfaz web de VMware ESXi

Antes de empezar
TSA necesita que se cargue VMware ESXi 6.5 o superiores para controlar el hardware.

Acerca de esta tarea
Siga estos pasos para instalar la imagen de TSA.

Procedimiento

1. Inicie una sesión en el sistema ESXi mediante la interfaz web de VMware ESXi.
2. Pulse **Crear/Registrar máquina virtual**. Se muestra el asistente **Nueva máquina virtual**.

Figura 1. Crear/Registrar máquina virtual

3. En la pantalla **Seleccionar el tipo de creación**, seleccione la opción **Desplegar una máquina virtual a partir de un archivo OVF u OVA** y pulse **Siguiente**.

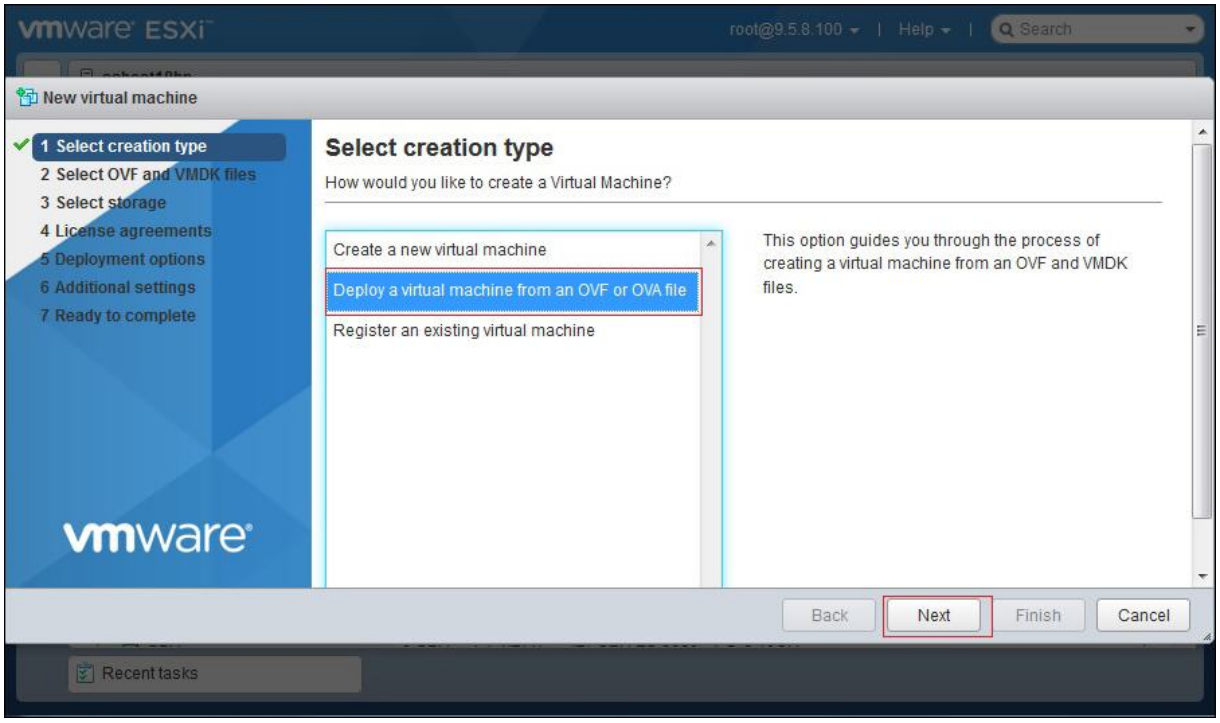

Figura 2. Seleccionar el tipo de creación

4. En la pantalla **Seleccionar archivos OVF y VMDK**, escriba un nombre para la máquina virtual, o bien utilice el valor predeterminado.

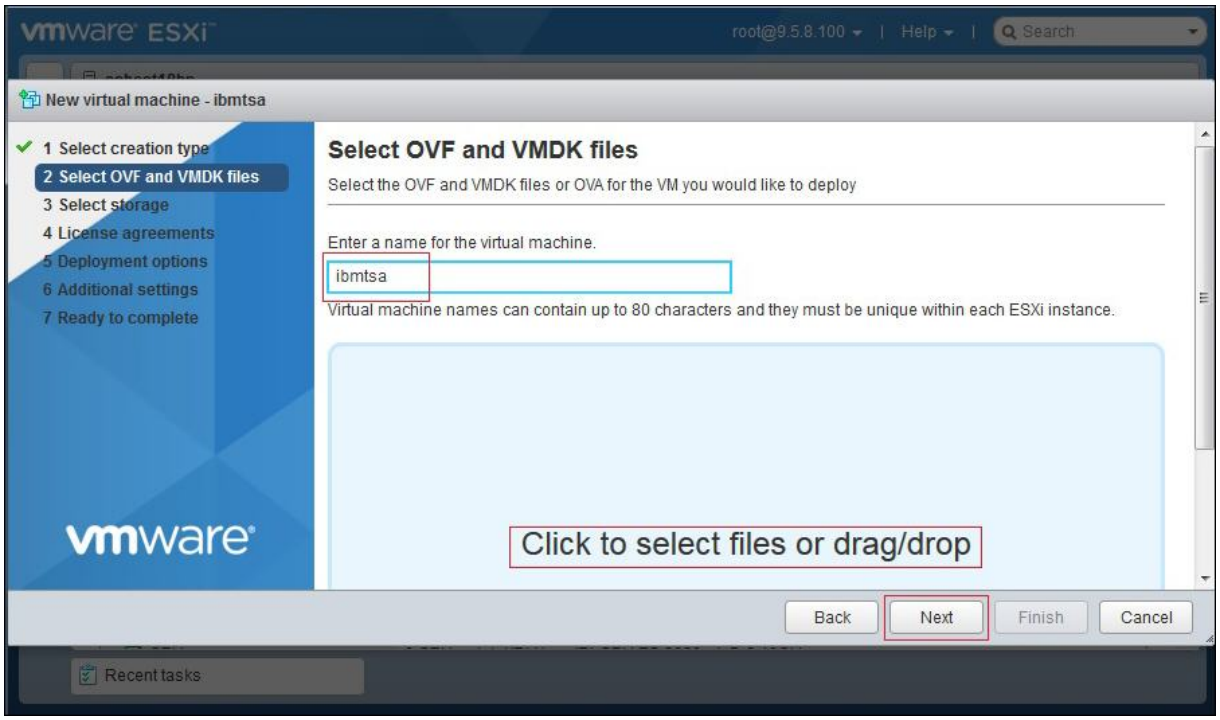

Figura 3. Seleccionar archivos OVF y VMDK

5. Pulse el recuadro **Pulse para seleccionar archivos o arrástrelos y suéltelos** y seleccione el archivo de imagen que ha descargado de Fix Central; a continuación, pulse **Siguiente**.
6. En la pantalla **Seleccionar almacenamiento**, en la lista que aparece, seleccione el almacén de datos en el que desea guardar la configuración y los archivos de disco. A continuación, pulse **Siguiente**.

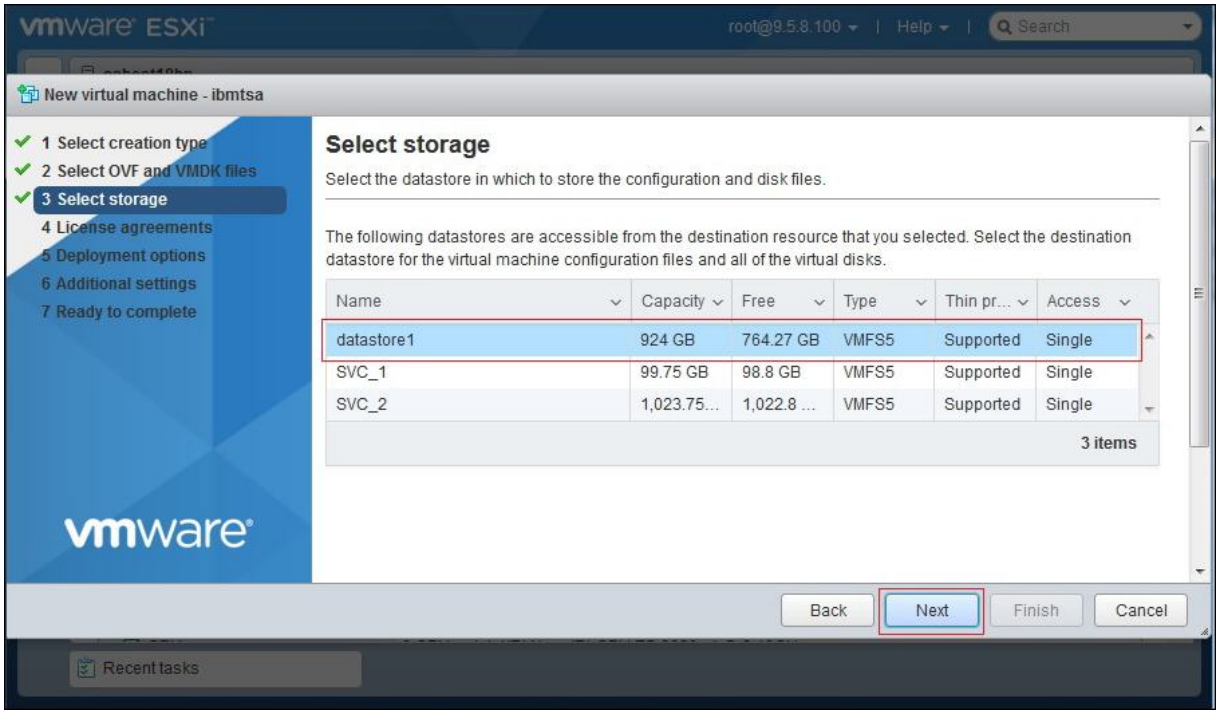

Figura 4. Seleccionar almacenamiento

7. En la pantalla **Opciones de despliegue**, seleccione las correlaciones de red de la lista desplegable **Red de VM**.

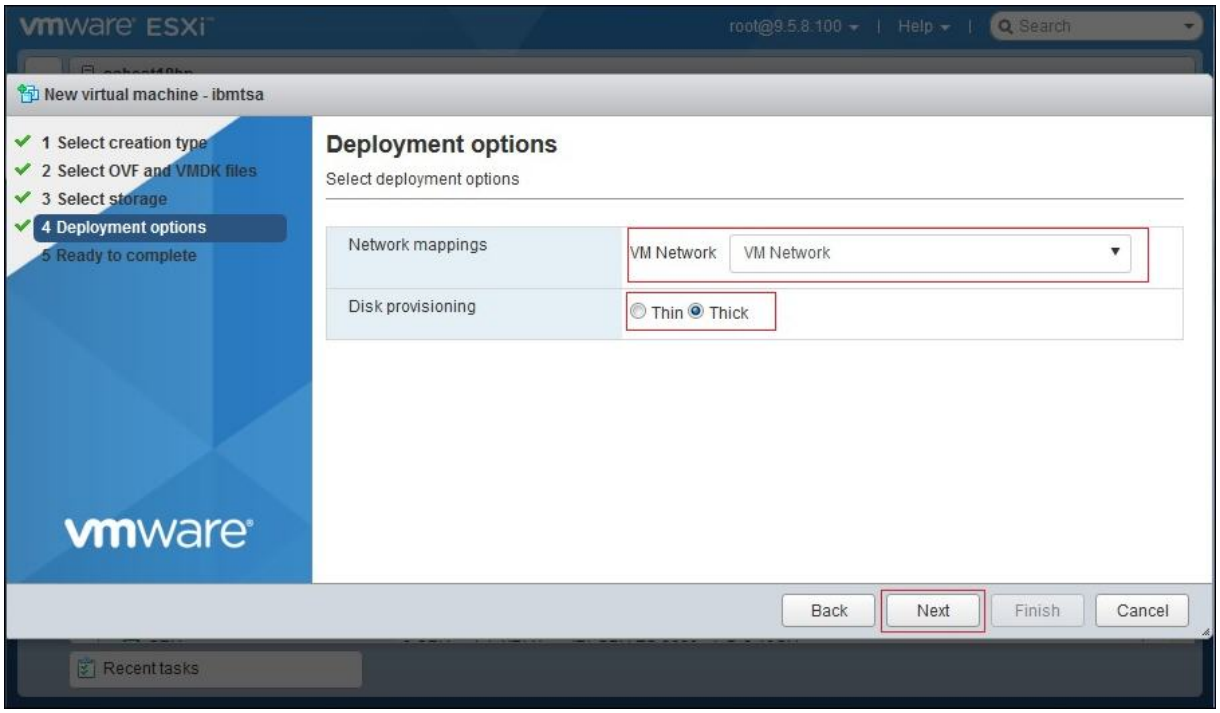

Figura 5. Opciones de despliegue

8. Seleccione la opción **Grueso** para el aprovisionamiento de disco y, a continuación, pulse **Siguiente**.
9. En la pantalla **Listo para finalizar**, revise todos los valores que ha especificado. Si desea realizar algún cambio, pulse **Atrás** y cambie las opciones pertinentes. Si está satisfecho, pulse **Finalizar**.

Importante: No renueve el navegador mientras se esté desplegando la máquina virtual.

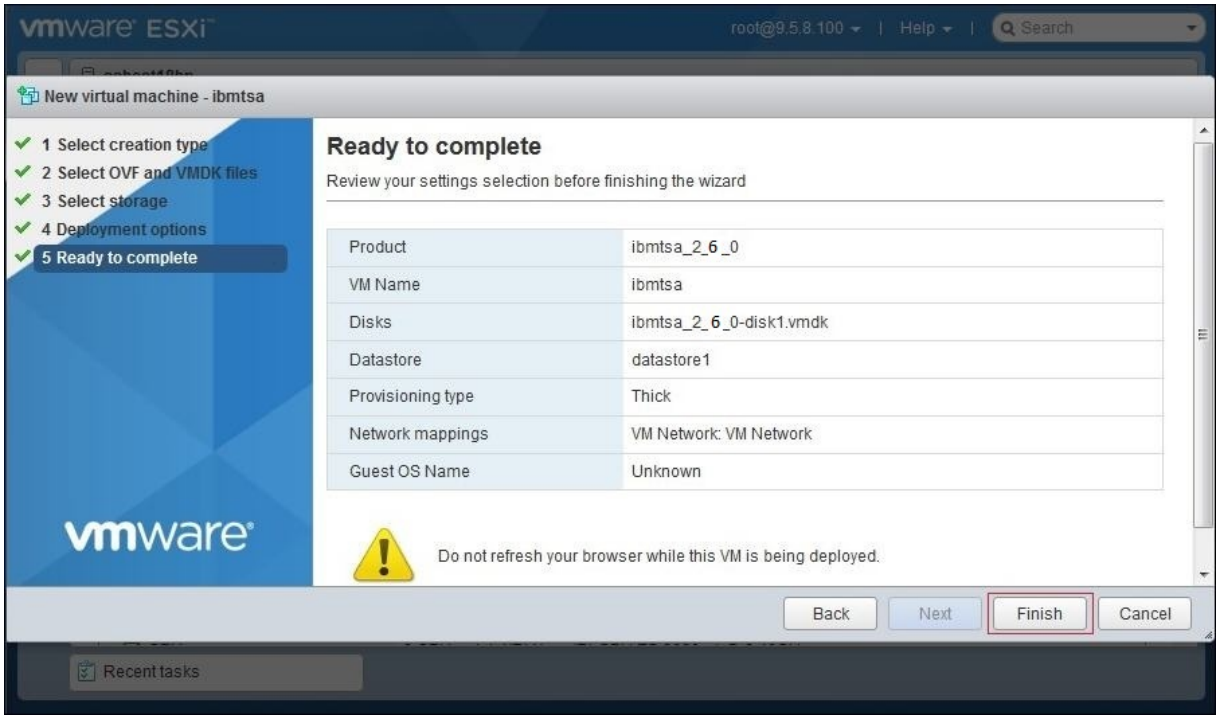

Figura 6. Revisar los valores seleccionados

La máquina virtual de TSA estará instalada en el sistema.

10. En la consola de TSA, en **ibmtsa login**, indique **`tsausr`**, y en **Password**, indique **`configTsa`**.
11. Necesario: Para cambiar la contraseña de inicio de sesión, continúe con la lista de pasos de la sección "Cambio de contraseña de tsausr (necesario)" en la página 19.
12. Para finalizar la instalación, continúe con la lista de pasos de la sección "Configuración de los datos de red" en la página 19.

Instalación de TSA en Microsoft Hyper-V

Antes de empezar

Para poder configurar y utilizar TSA en Hyper-V, se deben cumplir los requisitos previos siguientes:

- Hyper-V Server 2012, 2016 o 2019
- Hyper-V Manager
- Conmutador de red virtual creado mediante Hyper-V Manager

Acerca de esta tarea

Siga estos pasos para instalar TSA en Hyper-V.

Procedimiento

Para instalar TSA en Hyper-V, siga estos pasos:

1. Después de descargar la imagen de TSA, extraiga el archivo *ibmtsa_2700.vhdx* de *ibmtsa_2700.zip* y muévalo a un directorio en el servidor de Hyper-V.
2. Inicie Hyper-V Manager y conéctese al servidor de Hyper-V desde el sistema cliente.
3. Pulse **Examinar** y seleccione la imagen que está guardada en el sistema.

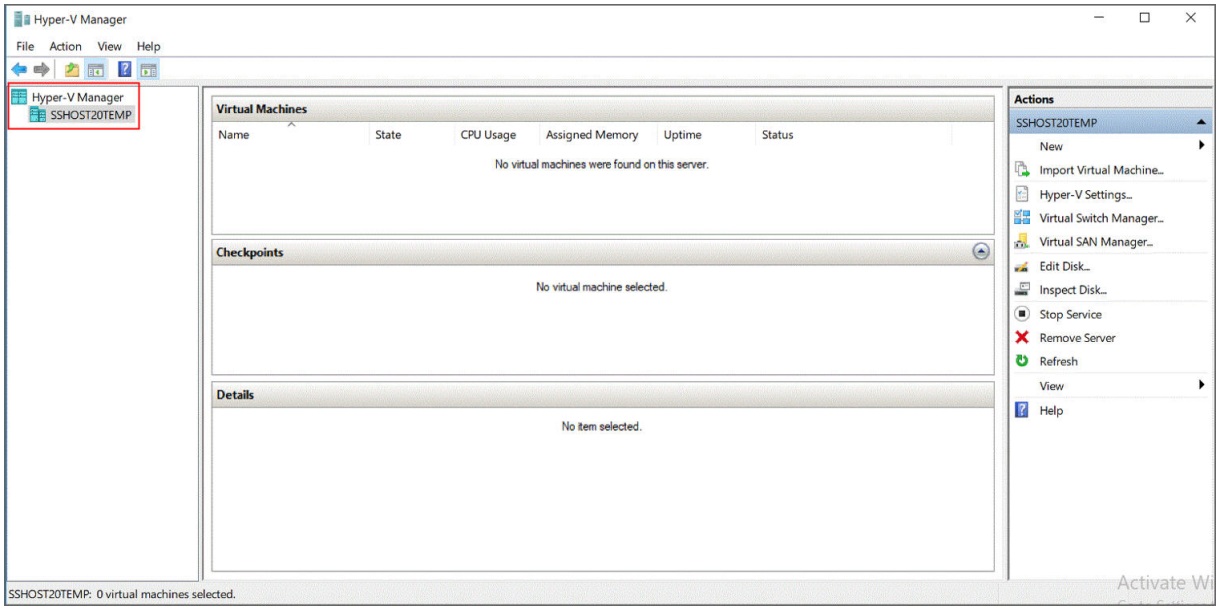

Figura 7. Hyper-V Manager

4. En el menú **Acción**, seleccione **Nueva** → **Máquina virtual**. Se muestra el **Asistente de nueva máquina virtual**.
5. Escriba el **Nombre** de la nueva máquina virtual y pulse **Siguiente**.

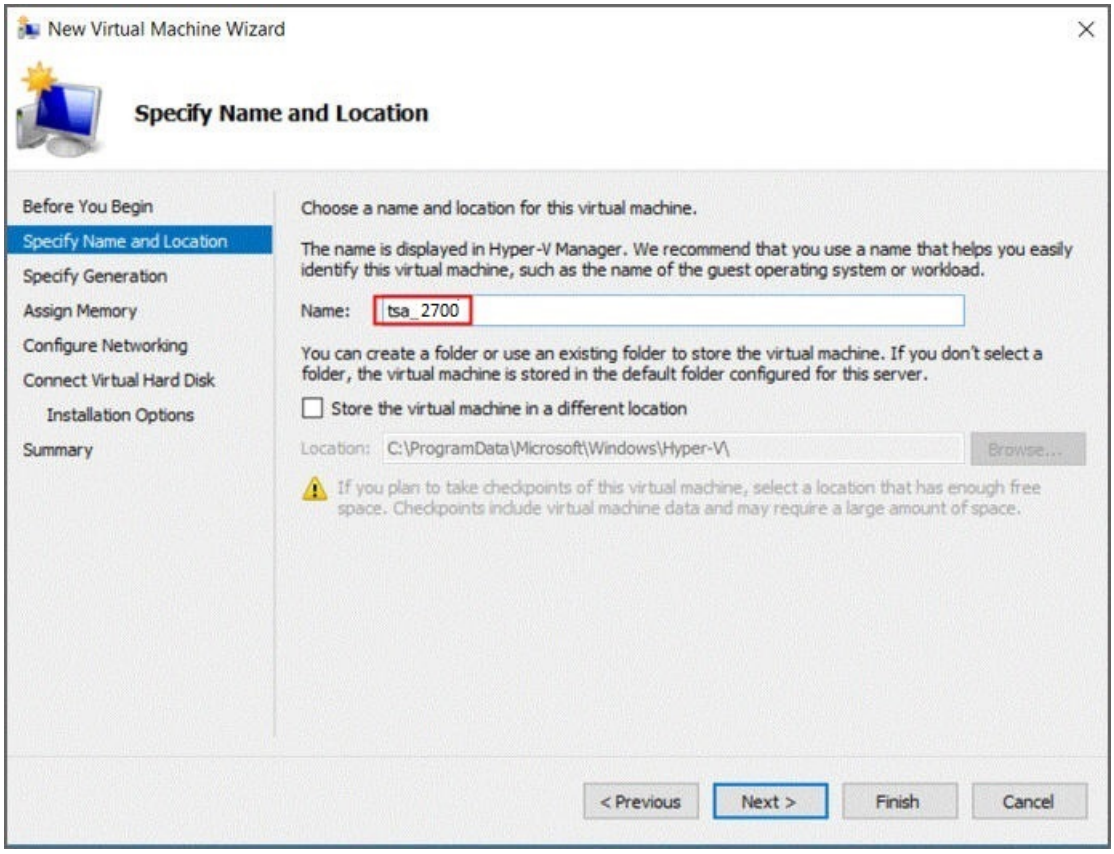

Figura 8. Nombre de máquina virtual

6. Seleccione **Generación 1** como generación de la máquina virtual y pulse **Siguiente**.

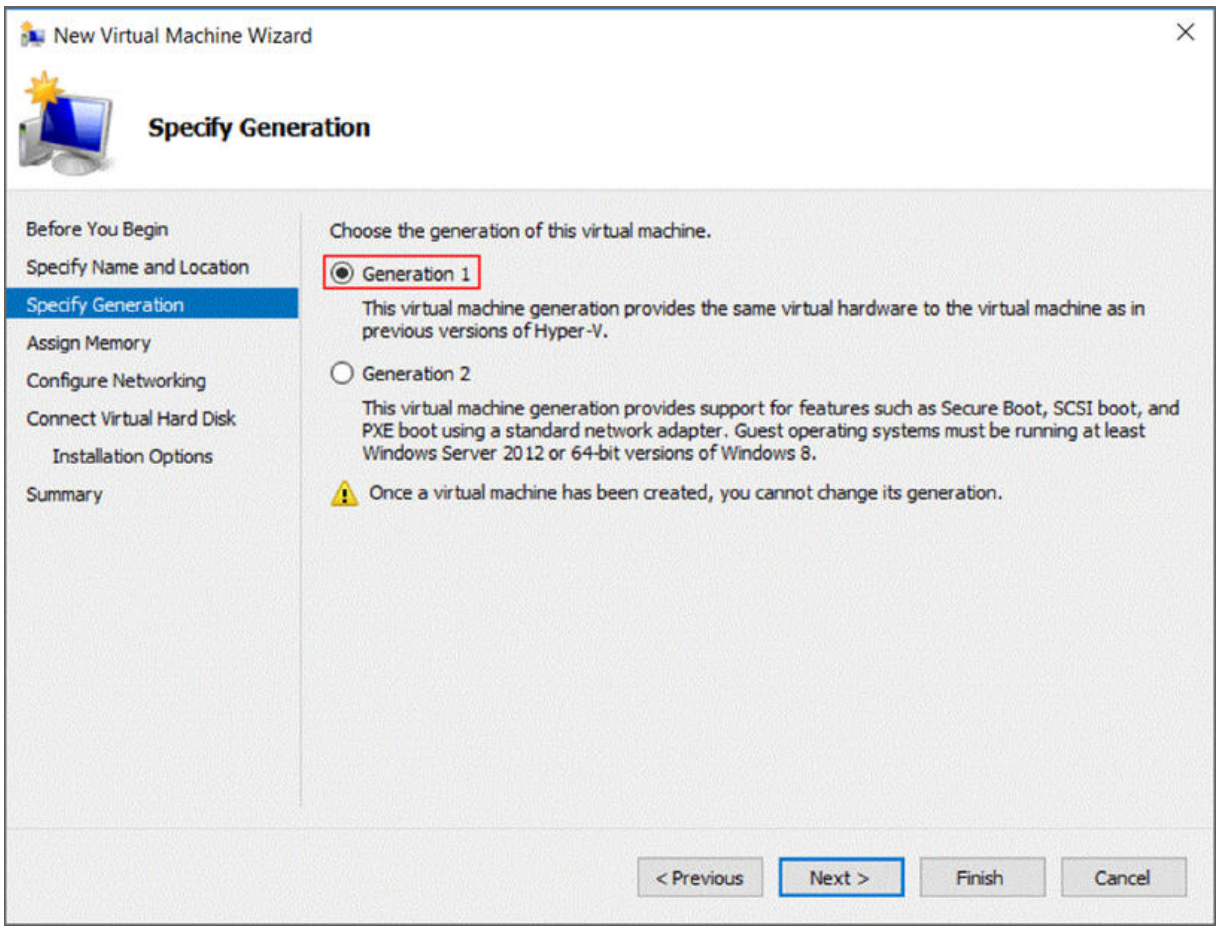

Figura 9. Especificar generación

7. En **Memoria de inicio**, escriba *16384* MB y pulse **Siguiente**.

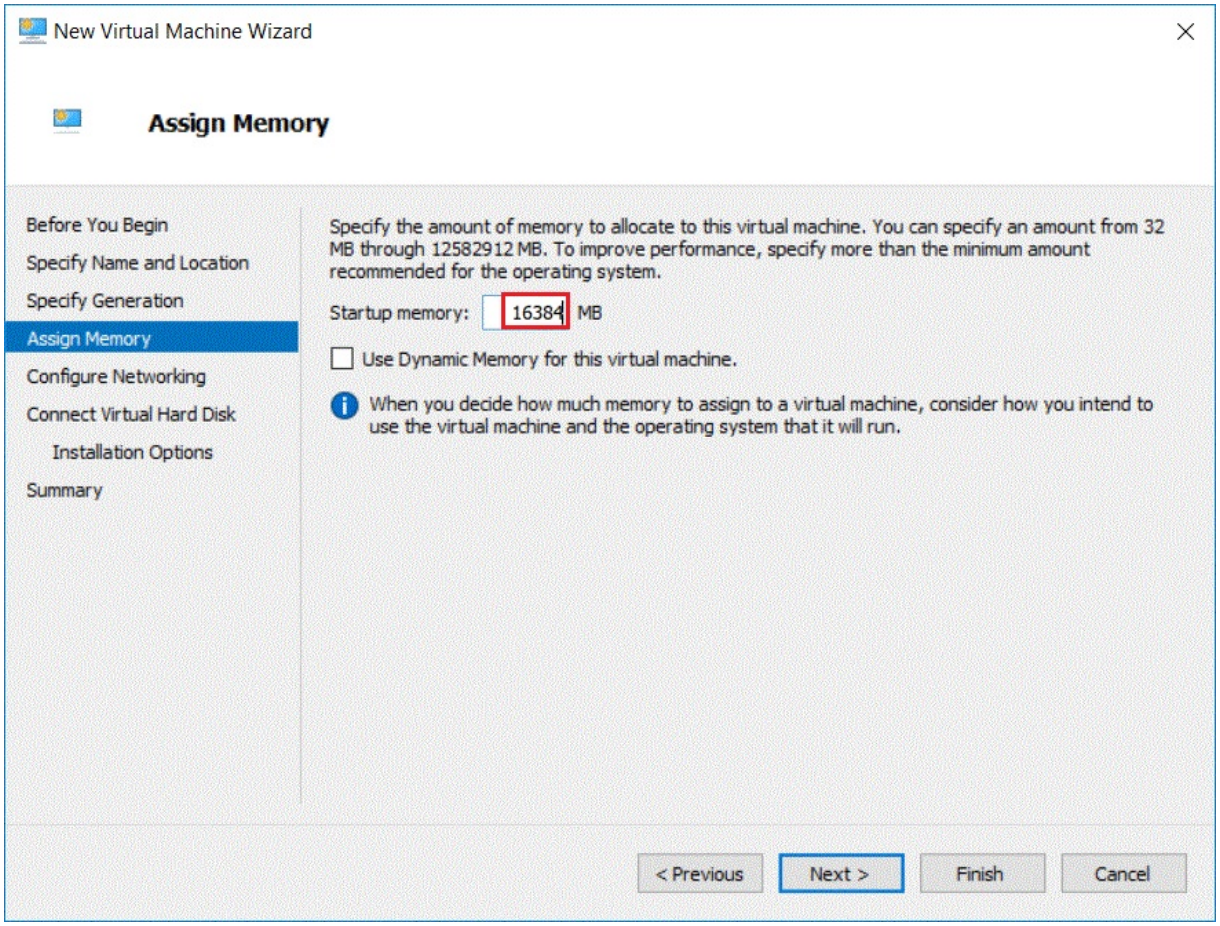

Figura 10. Memoria de inicio

8. Seleccione un conmutador virtual preconfigurado y pulse **Siguiente**.

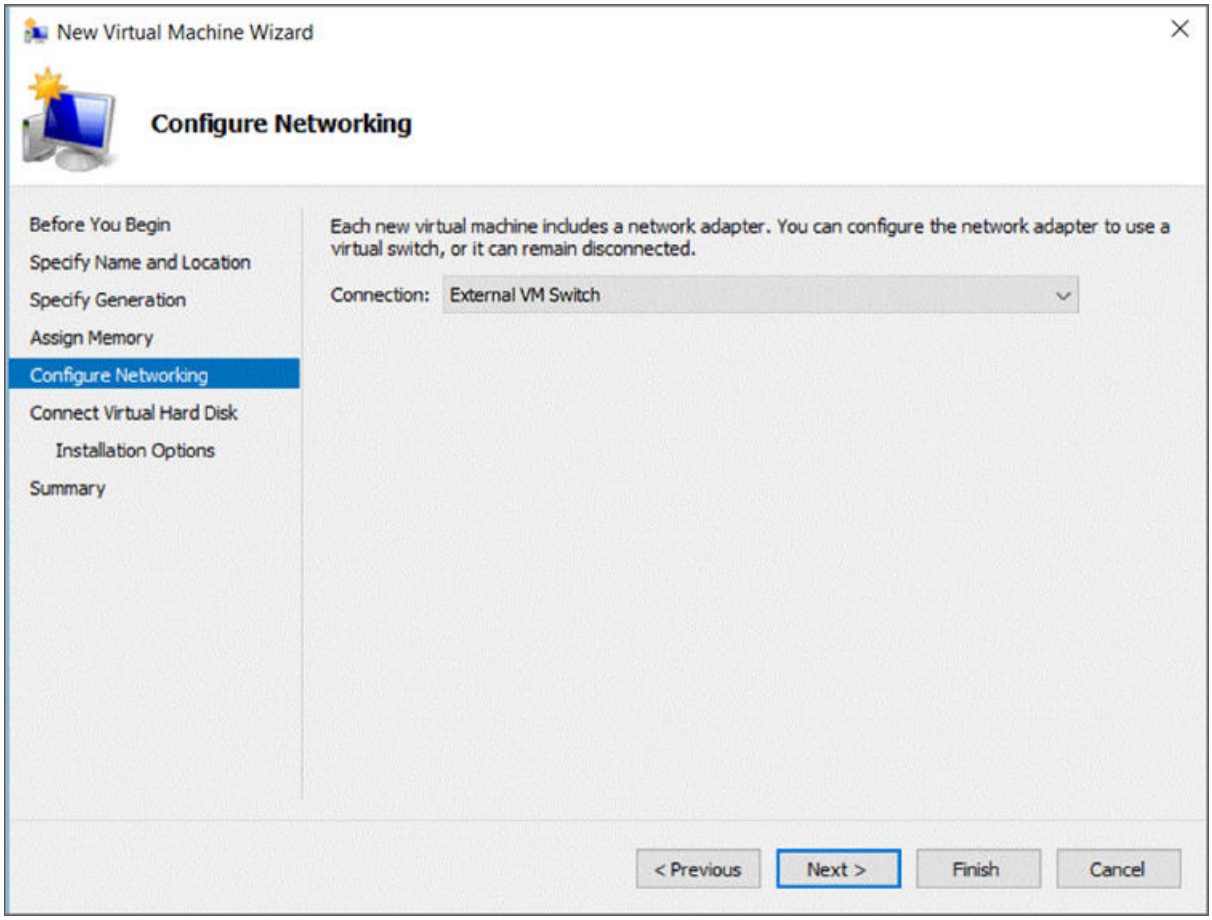

Figura 11. Configurar red

9. Seleccione la opción **Utilizar un disco duro virtual existente**, busque el archivo *ibmtsa_2700.vhdx* que ha copiado en el servidor de Hyper-V en el Paso 2 y pulse **Siguiente**.

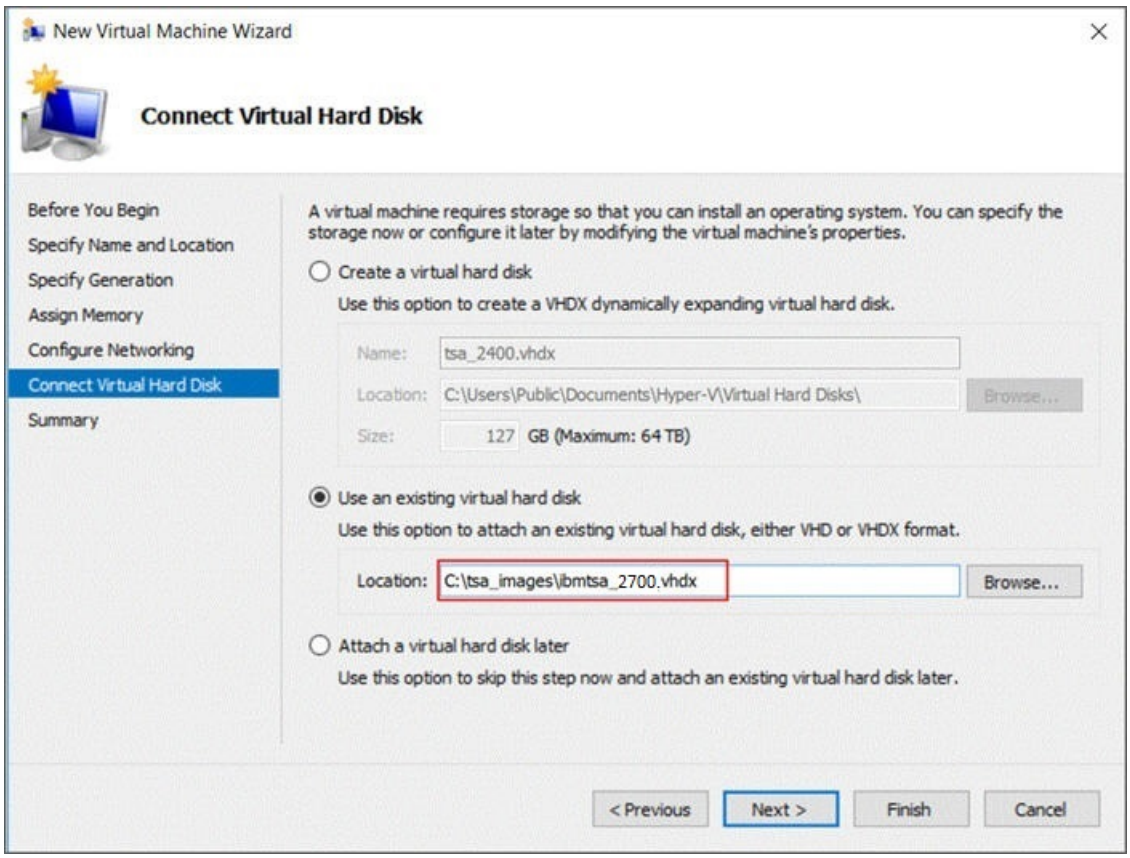

Figura 12. Conectar disco duro virtual

10. En la página **Resumen**, revise los valores y pulse **Finalizar**.

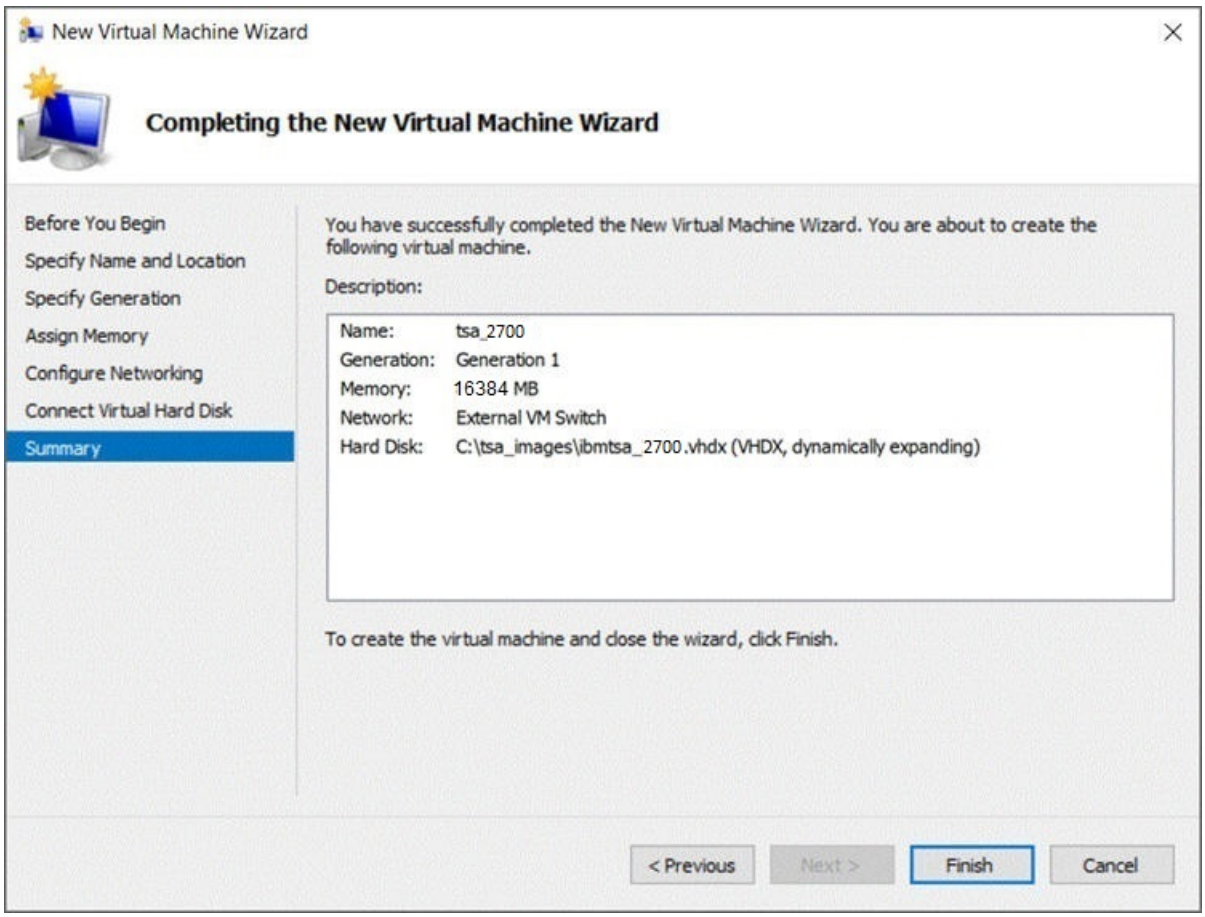

Figura 13. Resumen

11. La nueva máquina virtual se añade en Hyper-V Manager. Seleccione la máquina virtual, vaya al menú **Acción** y pulse **Iniciar**.

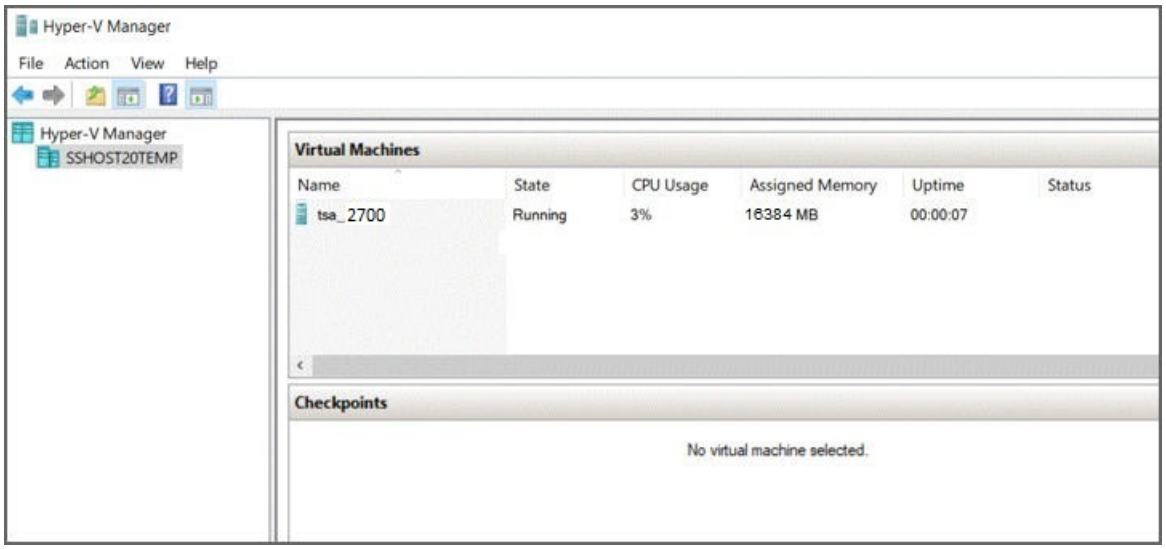

Figura 14. Hyper-V Manager

12. En el menú **Acción**, seleccione **Conectar** para iniciar una sesión de consola. En la consola de TSA, en **ibmtsa login**, indique **`tsausr`**, y en **Password**, indique **`configTsa`**.
13. Necesario: Para cambiar la contraseña de inicio de sesión, continúe con la lista de pasos de la sección "Cambio de contraseña de tsausr (necesario)" en la página 19.
14. Para finalizar la instalación, continúe con la lista de pasos de la sección "Configuración de los datos de red" en la página 19.

Cambio de contraseña de *tsausr* (necesario)

Por motivos de seguridad, se recomienda cambiar la contraseña inicial de *tsausr*. Siga estos pasos para cambiar la contraseña de *tsausr*.

Procedimiento

1. Seleccione la opción **2) Change tsausr password** en **TSA Config Menu**.

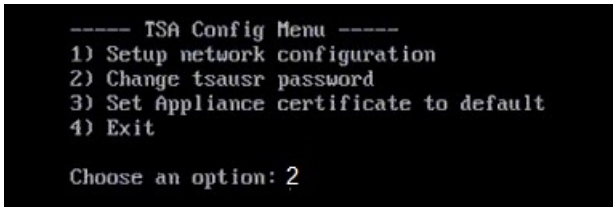

Figura 15. Cambiar contraseña

2. Escriba la nueva contraseña en el indicador de solicitud de contraseña **New password**. Escriba la misma contraseña en el indicador de solicitud de contraseña **Retype new password**. La nueva contraseña debe tener una longitud de al menos 7 caracteres.

Figura 16. Nueva contraseña

Configuración de los datos de red

Procedimiento

1. Seleccione la opción **1) Setup network configuration** en **TSA Config Menu**.

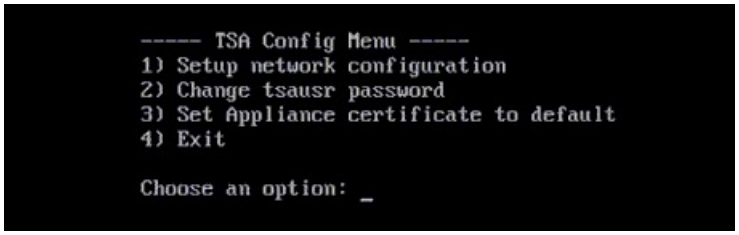

Figura 17. Realizar configuración de red

2. Indique los siguientes datos de configuración de red.

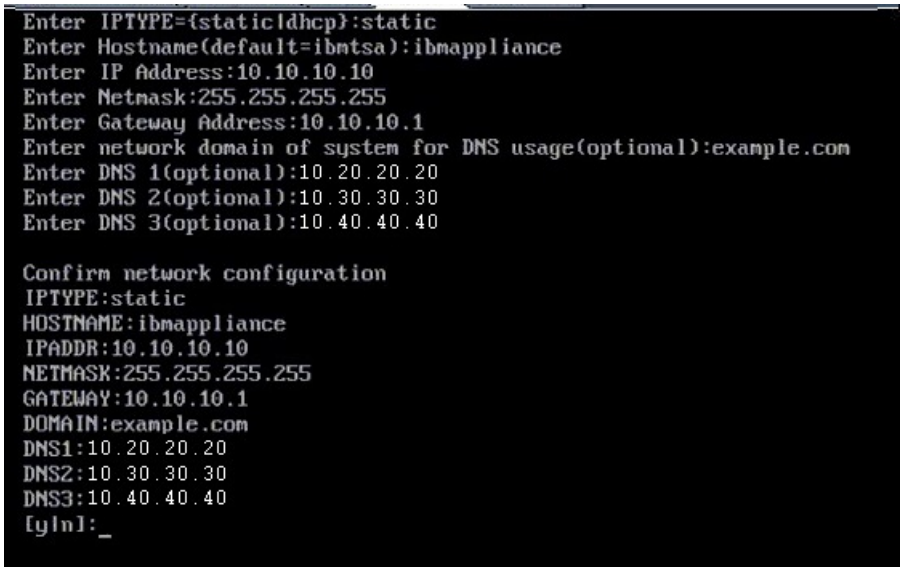

Figura 18. Configuración de red

a) **Enter IPTYPE = {static|dhcp}**. Indique `static` o dhcp. Si es `static`, siga estos pasos o efectúe los pasos de configuración de dhcp de la sección Apéndice C, “Configuración de los datos de red DHCP”, en la página 133.

IPTYPE: static

Enter Hostname(default=ibmtsa). Puede cambiar el nombre de host predeterminado. El nombre de host que utilice debe ser exclusivo.

Enter IP Address.

Enter Netmask y **Enter Gateway**.

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

Enter DNS 1(optional), **Enter DNS 2(optional)** y **Enter DNS 3(optional)**.

Los datos de configuración de red especificados se muestran para confirmarlos.

b) Indique **[y|n]** para confirmar o descartar la configuración de red. Al indicar **y**, se guarda la configuración de red y se reinicia el sistema automáticamente.

Nota: Si hay alguna configuración incorrecta, puede modificar los datos. Indique **n** para ignorar los valores actuales y reiniciar la configuración del paso “2.a” en la página 20.

c) El sistema se reinicia a los 15 segundos para que se aplique la nueva configuración de red.

d) Acceda a TSA desde el navegador utilizando HTTP seguro con el nombre de host o la dirección IP que se haya indicado anteriormente.
Por ejemplo, `https://<nombre de host | dirección IP>.`

Nota: La primera vez que se conecte, puede que el navegador muestre una excepción de seguridad. Debe aceptar el certificado de seguridad y continuar con el inicio de sesión de TSA.

Nota: Para modificar los valores de red básicos para TSA a través de la interfaz de usuario, siga los pasos de “Configurar los valores de red básicos” en la página 33. Para configurar los valores de red avanzados, siga los pasos que se indican en “Configurar los valores de red avanzados” en la página 35.

3. Configure el Technical Support Appliance utilizando los pasos que se describen en Capítulo 4, “Configurar el Technical Support Appliance”, en la página 21.

Resultados

Tras configurar satisfactoriamente TSA, consulte Capítulo 5, “Configurar el descubrimiento y la transmisión a IBM”, en la página 49.

Capítulo 4. Configurar el Technical Support Appliance

Acerca de esta tarea
Siga estos pasos para iniciarse rápidamente en TSA. Si aún no lo ha hecho, revise Capítulo 2, “Requisitos previos”, en la página 5.

Procedimiento

1. “Inicio de sesión en Technical Support Appliance” en la página 21
2. “Aceptación del acuerdo de licencia” en la página 23
3. “Utilización del Asistente de instalación para la configuración inicial” en la página 25
   a) “Configurar la conectividad con IBM” en la página 26
   b) “Registrar el Technical Support Appliance” en la página 27
   c) “Configurar el reloj” en la página 29
   d) “Configuración de la planificación de transmisión” en la página 31
   e) “Actualización de Technical Support Appliance” en la página 32
4. “Configurar los valores de red” en la página 33
5. “Configuración de certificados” en la página 41.
6. Opcional: Apéndice D, “Cuentas de usuario y grupos de usuarios”, en la página 135

Qué hacer a continuación
Al terminar de configurar TSA, consulte Capítulo 5, “Configurar el descubrimiento y la transmisión a IBM”, en la página 49 para obtener información sobre cómo llevar a cabo otras tareas.

Inicio de sesión en Technical Support Appliance

Procedimiento

1. Abra un navegador de Internet desde un sistema con acceso de red a TSA.
   Para obtener más información, consulte “Navegadores web necesarios” en la página 5.
2. Introduzca el siguiente URL en la barra de direcciones del navegador:

   ```
   https://<nombre de host o dirección IP>
   ```

   Nota: Si el `<nombre de host>` no funciona, pruebe con la dirección IP asignada de TSA.
3. Cuando se le solicite, indique la información siguiente:

   ID de usuario:
   Indique `admin`

   Contraseña:
   Escriba la contraseña del administrador de TSA.

   La contraseña inicial es `passw0rd`. Debe cambiar esta contraseña inicial al iniciar sesión en TSA.

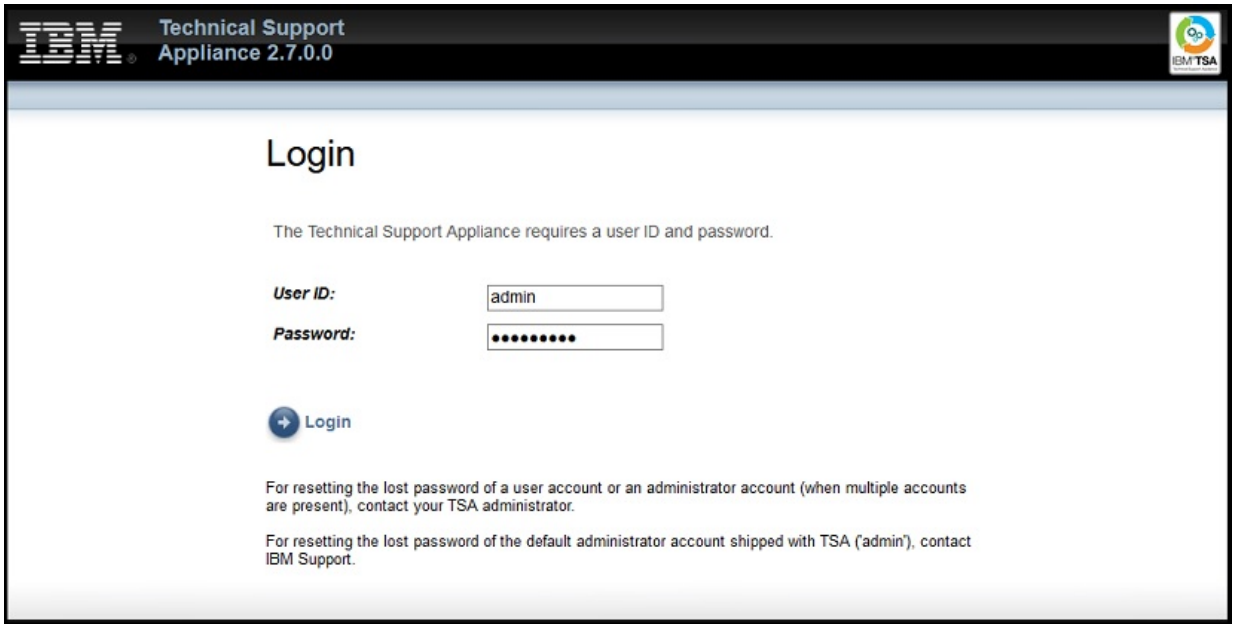

Figura 19. Inicio de sesión

Con el primer iniciar sesión, se visualiza la página **Cambiar contraseña**.

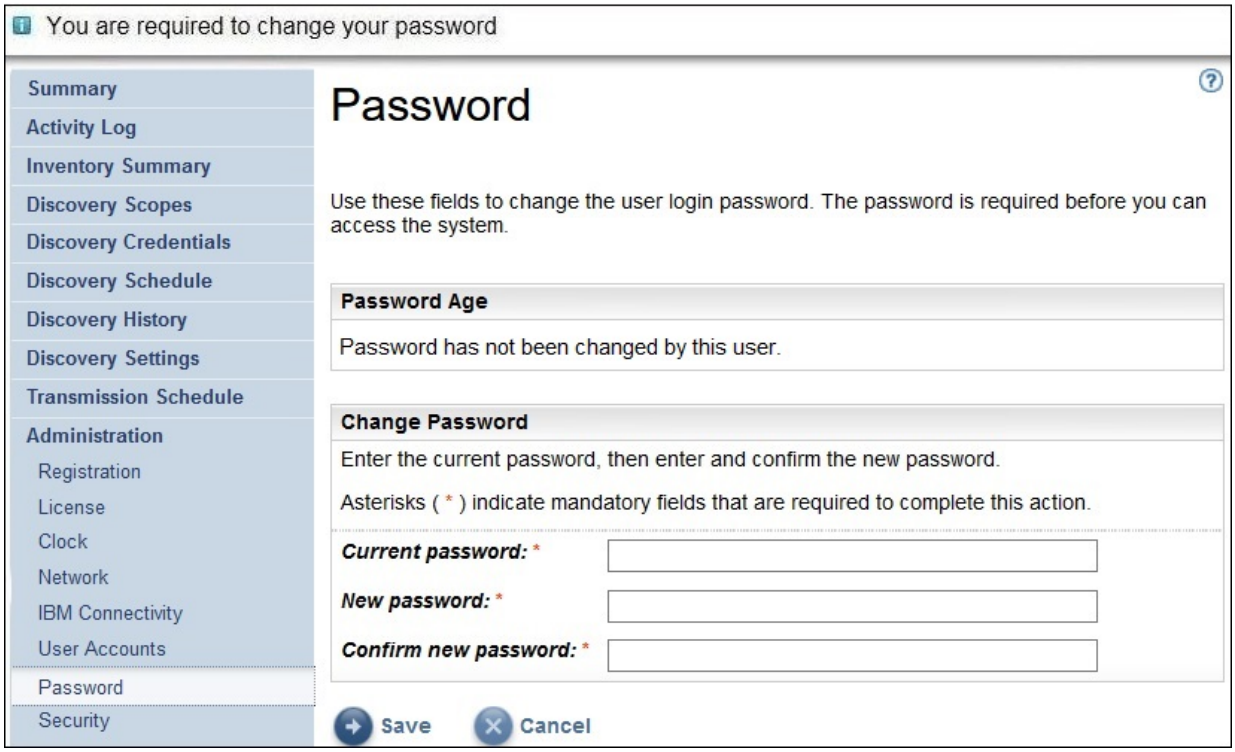

Figura 20. Cambiar contraseña

Para cambiar la contraseña inicial, siga estos pasos:

a) Introduzca una contraseña nueva.

La contraseña debe ajustarse a las reglas siguientes:

- Debe tener como mínimo 8 caracteres de largo
- Debe contener al menos un carácter alfabético y uno no alfabético
- No puede contener el nombre de usuario

- No puede ser igual que ninguna de las ocho contraseñas anteriores
- Se debe cambiar al menos cada 90 días, pero no se puede cambiar más de una vez al día.

b) Vuelva a escribir la nueva contraseña en el campo **Confirmar nueva contraseña**.

Las dos contraseñas que introduzca se comparan para confirmar que coinciden antes de guardar la contraseña.

c) Anote la nueva contraseña para su referencia futura.

Importante: No se puede recuperar una contraseña, de forma que si se pierde o se olvida una contraseña, no se puede iniciar sesión en TSA para cambiar las credenciales. Si pierde u olvida la contraseña de una cuenta de usuario o cuenta de administrador (si tiene varias cuentas), póngase en contacto con el administrador de TSA. Si pierde u olvida la contraseña de la cuenta de administrador predeterminada (que se proporciona con TSA), póngase en contacto con el servicio de soporte de IBM.

d) Pulse **Guardar**. En el primer inicio de sesión, se visualiza la página **Acuerdo de licencia**.

Aceptación del acuerdo de licencia

Lea y acepte el Acuerdo de licencia para continuar.

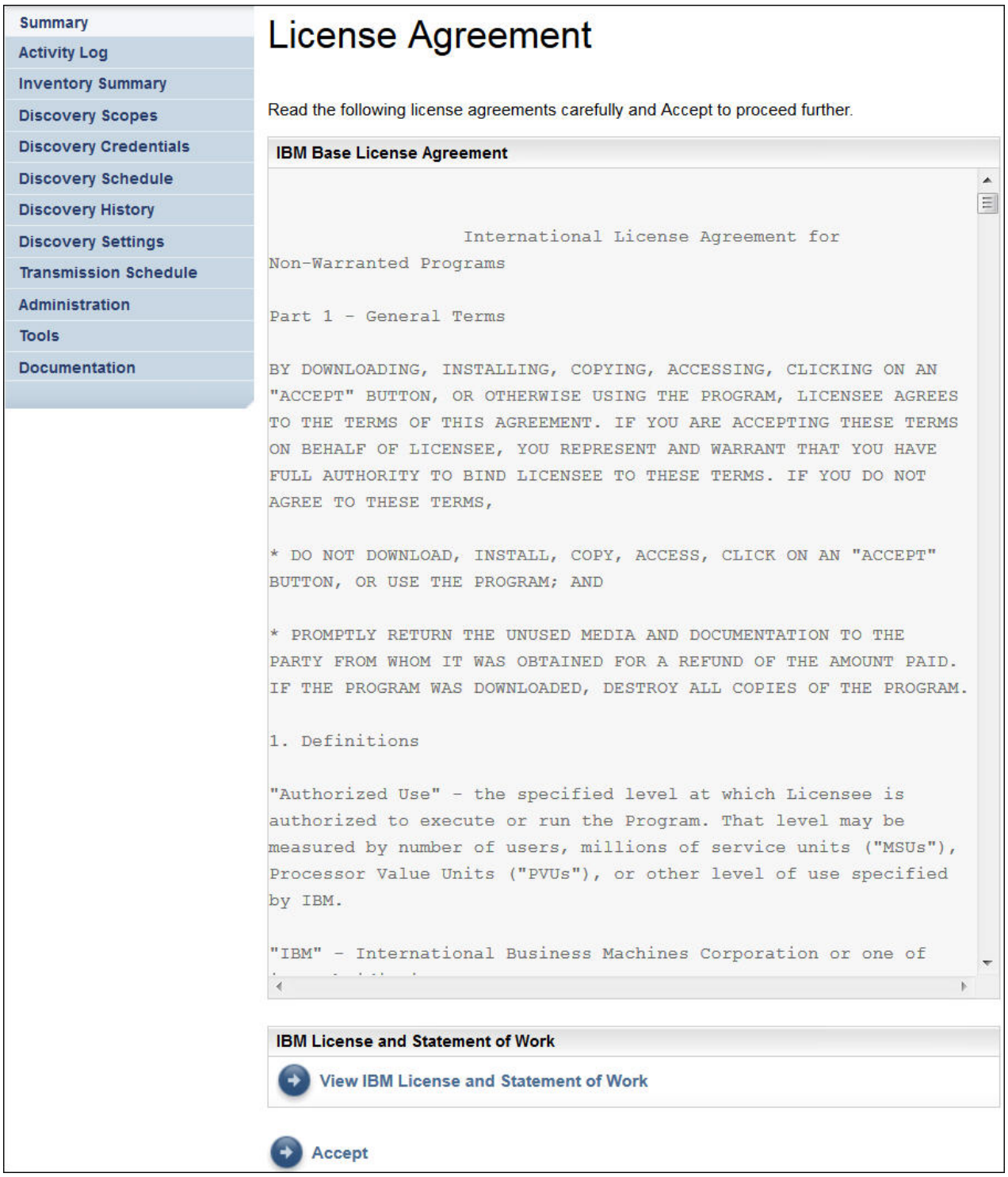

Figura 21. Acuerdo de licencia

El Acuerdo de licencia incluye los siguientes elementos:

- **Acuerdo de licencia básico de IBM**: muestra el acuerdo de licencia básico de IBM.
- **Licencia de IBM y Descripción del servicio**: pulse **Ver Licencia de IBM y Descripción del servicio** para ver la licencia de IBM y la descripción del servicio.

  Nota: TSA es compatible con el RGPD [EU/2016/679]. Ahora puede ver la información de conformidad con el RGPD en la sección **Licencia de IBM y Descripción del servicio**.

- **Avisos e información de IBM**: pulse **Ver avisos e información de IBM** para ver los avisos y la información de IBM.
- **Términos y condiciones de código con licencia por separado**: pulse **Ver términos y condiciones de código con licencia por separado** para ver los términos y condiciones de código con licencia por separado.

Pulse **Aceptar** para aceptar el acuerdo. Una vez que haya aceptado la licencia, aparece el **Asistente de instalación** para ayudarle a configurar TSA. Puede configurar TSA utilizando el **Asistente de instalación** o puede salir del asistente y configurar los valores de TSA según sus requisitos.

Nota: En el panel de navegación, pulse **Administración** > **Licencia** para ver el Acuerdo de licencia más reciente que ha aceptado.

Conceptos relacionados

"Utilización del Asistente de instalación para la configuración inicial" en la página 25
Utilice el **Asistente de instalación** para configurar TSA para la configuración inicial.

"Configuración de Technical Support Appliance" en la página 123
Si sale u omite la configuración de alguno de los valores en el **Asistente de instalación**, puede configurarlos manualmente en el menú de navegación de la izquierda de TSA.

Utilización del Asistente de instalación para la configuración inicial

Utilice el **Asistente de instalación** para configurar TSA para la configuración inicial.

Después de aceptar el acuerdo de licencia, el **Asistente de instalación** se visualiza automáticamente.

Nota: Para iniciar el **Asistente de instalación** manualmente, en el panel de navegación, pulse **Herramientas** > **Asistente de instalación** > **Iniciar asistente de instalación**.

Figura 22. Asistente de instalación

El **Asistente de instalación** le guiará en los pasos siguientes:

- "Configurar la conectividad con IBM" en la página 26
- "Registrar el Technical Support Appliance" en la página 27
- "Configurar el reloj" en la página 29
- "Configuración de la planificación de transmisión" en la página 31
- "Actualización de Technical Support Appliance" en la página 32

Nota: Si sale u omite la configuración de alguno de los valores en el **Asistente de instalación**, puede configurarlos manualmente en el panel de navegación de TSA. Para obtener más información sobre la

configuración de estos valores, consulte Apéndice B, “Configuración de Technical Support Appliance”, en la página 123.

Configurar la conectividad con IBM

Procedimiento

Puede ver, cambiar y probar la configuración que TSA utiliza para conectarse a IBM.

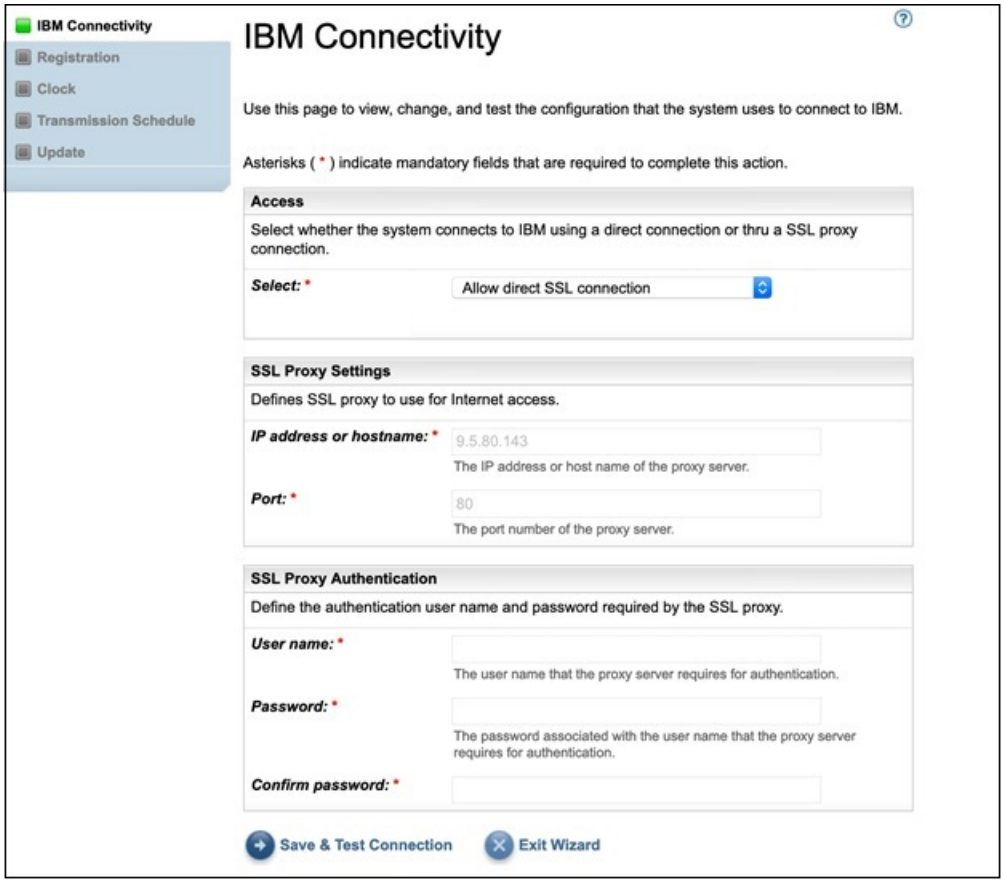

Figura 23. Conectividad de IBM

1. En el panel **Acceso**, seleccione uno de los siguientes tipos de acceso a Internet:

   Permitir conexión SSL directa
   TSA se conecta a IBM utilizando una conexión directa.

   Utilizar conexión proxy SSL
   TSA se conecta a IBM utilizando una conexión proxy SSL.

   Utilizar conexión proxy SSL de autenticación
   TSA se conecta a IBM utilizando una conexión proxy SSL de autenticación.

2. Si selecciona **Utilizar conexión proxy SSL** o **Utilizar conexión proxy SSL de autenticación**, especifique la siguiente información del servidor proxy:

   Dirección IP o nombre de host
   La dirección IP o el nombre de host del servidor proxy.

   Nota: El nombre de host que especifique no puede contener ningún guión bajo ("_").

   Puerto
   El número de puerto del servidor proxy.

3. Si selecciona **Utilizar conexión proxy SSL de autenticación**, especifique la siguiente información del servidor proxy:

Nombre de usuario
El nombre de usuario que requiere el servidor proxy para la autenticación.

Contraseña
La contraseña asociada al nombre de usuario que requiere el servidor proxy para la autenticación.

Confirmar contraseña
Vuelva a escribir la contraseña. Las dos contraseñas que introduzca se comparan para confirmar que coinciden antes de guardar la contraseña.

Qué hacer a continuación

- Pulse **Guardar y probar conexión** para guardar y probar la conexión especificada. Si la conexión es satisfactoria, se visualiza el botón **Continuar**.
- Pulse **Continuar** para ir a la página **Registro**.

  -o bien-
- Pulse **Salir del asistente** para salir del **Asistente de instalación** e ir a la página **Resumen**.

Registrar el Technical Support Appliance

Puede ver y cambiar el contacto de servicio del sistema y la ubicación física.

Procedimiento

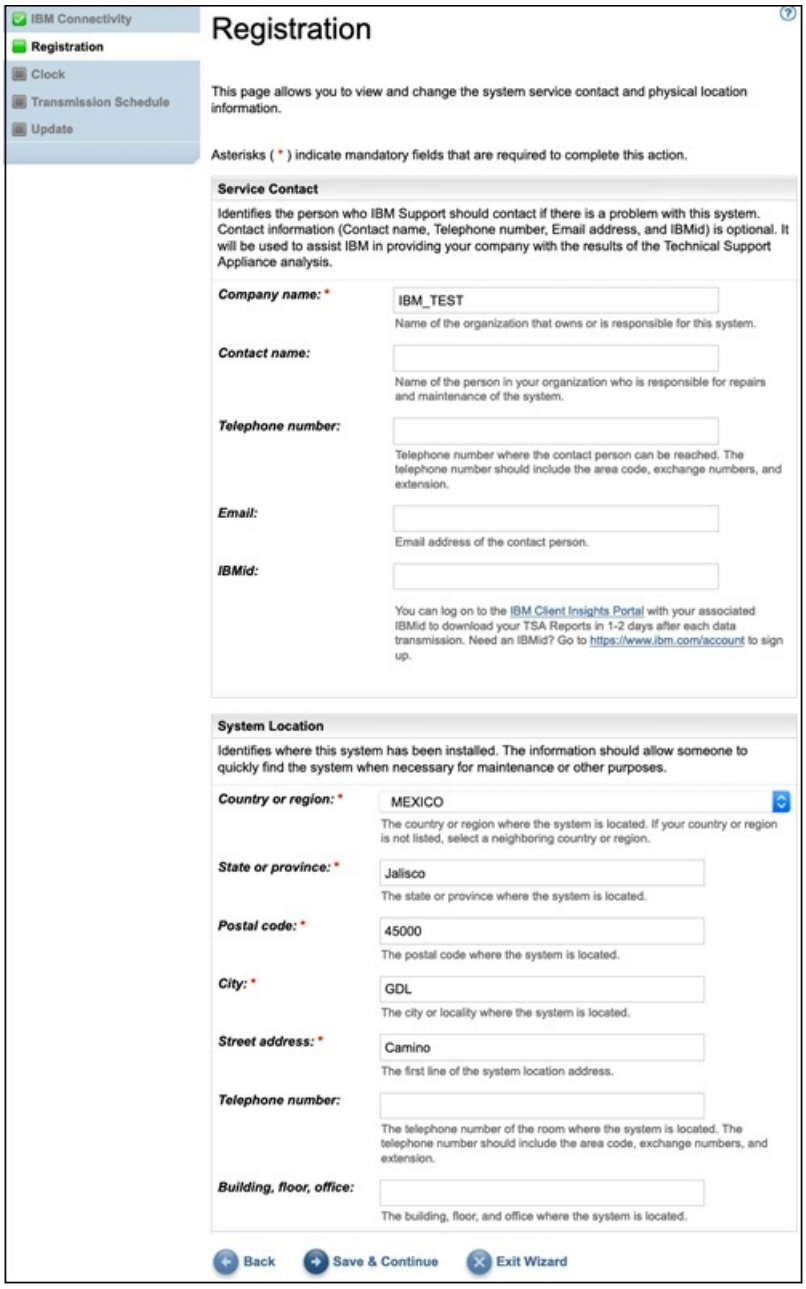

Figura 24. Registro

1. Especifique la información de contacto del servicio en los siguientes campos:

   Nombre de la empresa
   El nombre de la organización que utiliza TSA.

   Nombre del contacto
   (Opcional) El nombre de la persona de la organización responsable de TSA.

   Número de teléfono
   (Opcional) El número de teléfono donde se puede localizar a la persona de contacto. El número de teléfono debe incluir el código de área, los números de intercambio y la extensión. No utilice paréntesis en el número de teléfono.

   Correo electrónico
   (Opcional) La dirección de correo electrónico de la persona de contacto.

IBMid
(Opcional) El IBMid de la persona a la que desea dar autorización para ver los informes de IBM Client Insights Portal.

Nota: Puede iniciar sesión en https://clientinsightsportal.ibm.com/ con su IBMid asociado para descargar los informes de TSA pasados 1-2 días de cada transmisión de datos. Para registrarse para obtener un IBMid, vaya a https://www.ibm.com/account.

Nota: El contacto de servicio identifica a la persona con la que el servicio de soporte de IBM se debe poner en contacto si hay algún problema con el sistema. La información de contacto se utiliza para ayudar a IBM a proporcionar a la empresa los resultados del análisis del Technical Support Appliance.

2. Especifique la información de la ubicación del TSA en los siguientes campos:

País o región
El país o región donde se encuentra TSA.

Estado o provincia
El estado o la provincia donde se encuentra TSA. Si no está seguro del estado, escriba *Desconocido*.

Código postal
El código postal donde se encuentra el TSA.

Ciudad
La ciudad o la localidad donde se encuentra TSA.

Dirección postal
La dirección de la ubicación de TSA.

Número de teléfono
(Opcional) El número de teléfono de la sala donde se encuentra TSA. El número de teléfono debe incluir el código de área, los números de intercambio y la extensión. No utilice paréntesis en el número de teléfono.

Edificio, planta, oficina
(Opcional) El edificio, la planta y la oficina donde se encuentra TSA.

Qué hacer a continuación

- Pulse **Guardar y continuar** para guardar la información de registro y continuar en la página **Reloj**.
- Pulse **Volver** para volver a la página **Conectividad de IBM**.

-o bien-

- Pulse **Salir del asistente** para salir del **Asistente de instalación** e ir a la página **Resumen**.

Configurar el reloj

Puede definir la hora del sistema de TSA, la fecha y el huso horario local durante la configuración.

Procedimiento

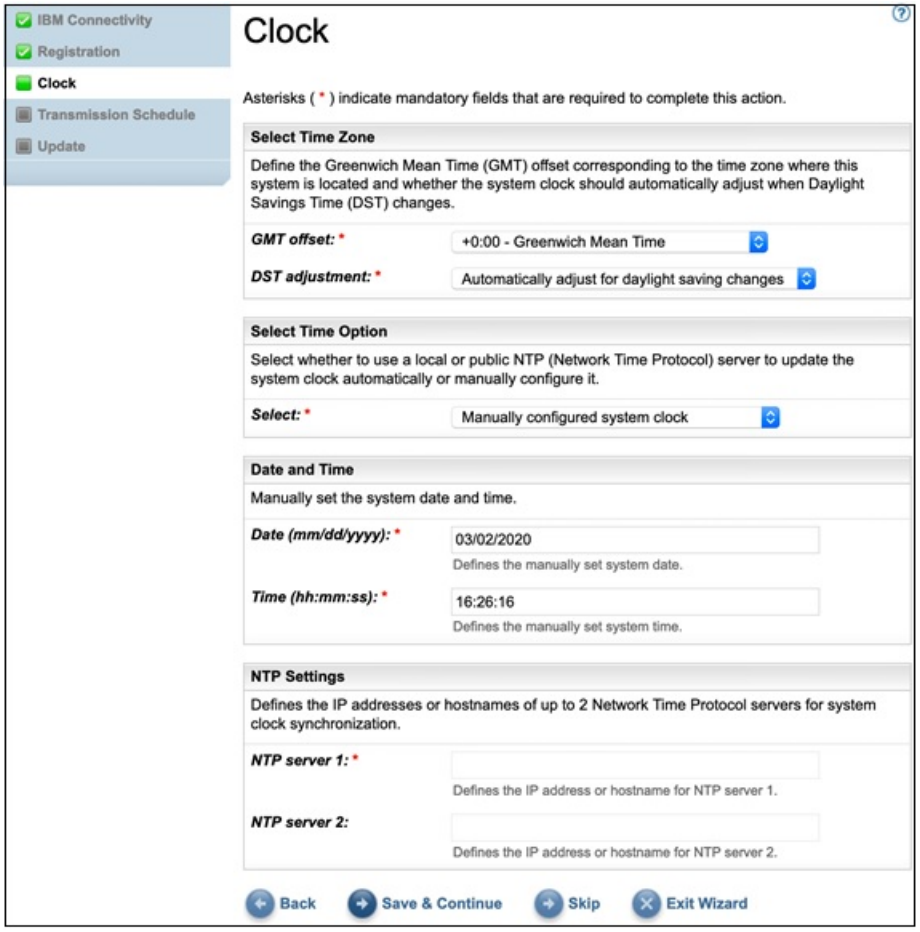

Figura 25. Reloj

1. Seleccione el huso horario local en la lista desplegable **Diferencia GMT**.
2. Seleccione el ajuste de horario de verano (DST - Daylight Saving Time) en la lista desplegable **Ajuste de DST**.

   Nota: No todos los husos horario tienen horario de verano. Si se selecciona esta opción para un huso horario que no admite DST, se muestra un mensaje de error.
3. Seleccione un método para actualizar el reloj del sistema en la lista desplegable **Seleccionar opción de hora**.

   Entre las opciones se incluye sincronizar el reloj del sistema con un servidor NTP (Network Time Protocol) para actualizar el reloj del sistema automáticamente, o configurar manualmente el reloj del sistema.

   a) Si selecciona configurar manualmente el reloj del sistema, debe definir la fecha y la hora del sistema. Indique la información de fecha y hora en los campos **Fecha** y **Hora**.

   b) Si selecciona sincronizar el reloj del sistema con un servidor NTP (Network Time Protocol) para actualizar el reloj del sistema automáticamente, debe especificar las direcciones IP y los nombres de host de los servidores NTP. Escriba la información de dirección IP o nombre de host de hasta dos servidores en los campos **servidor NTP**.

      Nota: Asegúrese de que el Servidor NTP es accesible a través de la red para TSA.

Qué hacer a continuación

- Pulse **Guardar y continuar** para guardar la información de reloj y continuar en la página **Planificación de transmisión**.

-o bien-

- Pulse **Omitir** para saltar a la página **Planificación de transmisión**.

Para modificar los valores en el paso anterior del asistente:

- Pulse **Volver** para volver a la página **Registro**.

Para salir del asistente:

- Pulse **Salir del asistente** para salir del **Asistente de instalación** e ir a la página **Resumen**.

Configuración de la planificación de transmisión

TSA proporciona una planificación predeterminada para ejecutar el proceso de transmisión a las horas especificadas. Puede modificar esta planificación según sus necesidades.

Procedimiento

1. Utilice las listas desplegables **A la hora** y **En el minuto** para seleccionar una nueva hora.
2. Seleccione el **Modo de selección del día**.

Semanalmente los días (dom - sáb)
Para planificar la transmisión en un día o días concretos de la semana, seleccione la opción **Semanalmente los días (dom - sáb)**.

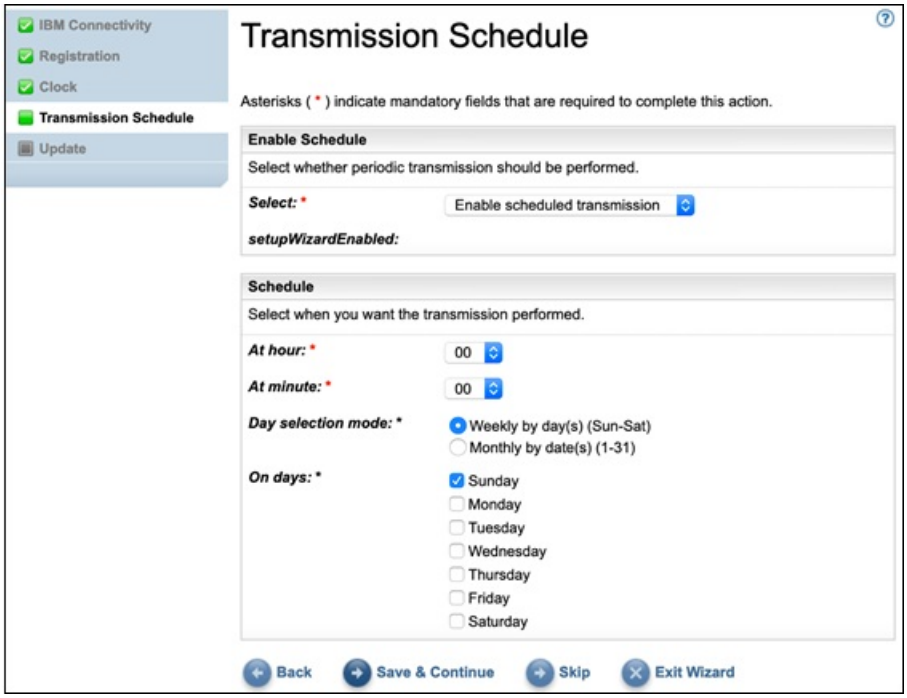

Figura 26. Semanalmente los días (dom - sáb)

En el campo **Los días**, seleccione los recuadros adecuados para seleccionar uno o más días de la semana.

Mensualmente los días (1-31)
Para planificar la transmisión en unos días concretos del mes, seleccione la opción **Mensualmente los días (1-31)**.

En el campo **Los días**, seleccione los recuadros adecuados para seleccionar uno o más días del mes.

Nota: Si selecciona los días más allá de un mes específico, el trabajo se activa el último día de ese mes en concreto.

Nota: Asegúrese de que la hora de inicio del descubrimiento sea anterior a la hora de transmisión para evitar largos retardos en la transmisión de los datos que se acaban de recopilar.

Qué hacer a continuación

- Pulse **Guardar y continuar** para guardar la planificación de transmisión y continuar en la página **Actualizar**.

  -o bien-

- Pulse **Omitir** para saltar a la página **Actualizar**.

Para modificar los valores en el paso anterior del asistente:

- Pulse **Volver** para volver a la página **Reloj**.

Para salir del asistente:

- Pulse **Salir del asistente** para salir del **Asistente de instalación** e ir a la página **Resumen**.

Actualización de Technical Support Appliance

Puede actualizar TSA a la versión más reciente disponible.

Si hay una actualización disponible, aparece la siguiente página **Actualizar**.

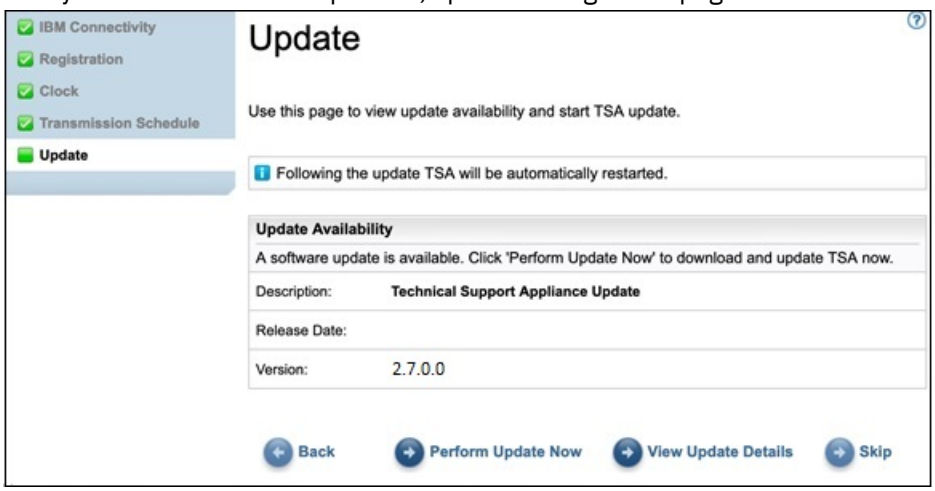

Figura 27. Disponibilidad de actualizaciones

- Pulse **Realizar actualización ahora** para instalar la actualización y completar el **Asistente de instalación**.

  -o bien-

- Pulse **Ver detalles de actualización** para ver información sobre el contenido de la actualización.

Para modificar los valores en el paso anterior del asistente:

- Pulse **Volver** para volver a la página **Planificación de transmisión**.

Para completar el asistente:

- Pulse **Omitir** para completar el **Asistente de instalación** sin aplicar la actualización.

Si no hay una actualización disponible, aparece la siguiente página **Actualizar**.

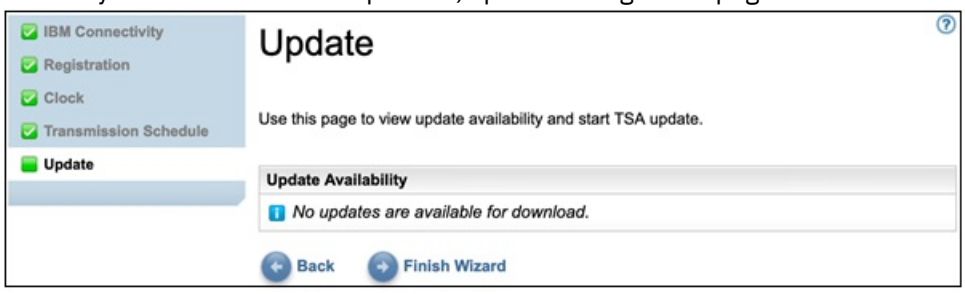

Figura 28. No hay ninguna actualización disponible

- Pulse **Finalizar asistente** para completar el **Asistente de instalación**. Se mostrará la página **Asistente de instalación completado**.

  -o bien-

- Pulse **Volver** para volver a la página **Planificación de transmisión**.

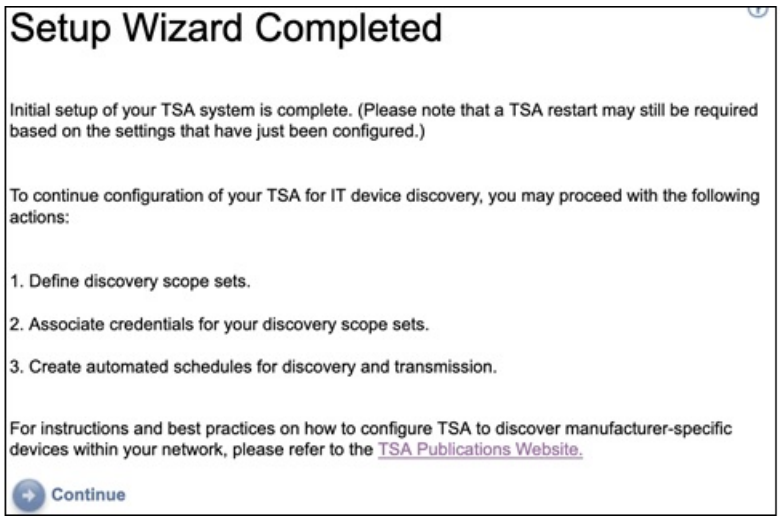

Figura 29. Asistente de instalación completado

- Pulse **Continuar** para ir a la página **Resumen**.

  Nota: Algunas modificaciones en la página **Reloj** requieren reiniciar el sistema. Por ejemplo, si define la fecha o la hora, o cambia de configuración manual a configuración de servidor NTP, se le solicitará que reinicie el sistema.

  – Pulse **Aceptar** para finalizar el **Asistente de instalación** y volver a la página **Resumen**. Se muestra la página **Resumen** y el sistema se reinicia.

Nota: Si sale u omite la configuración de alguno de los valores en el **Asistente de instalación**, puede configurarlos manualmente en el panel de navegación de TSA. Para obtener más información sobre la configuración de estos valores, consulte Apéndice B, “Configuración de Technical Support Appliance”, en la página 123.

Configurar los valores de red

La instalación de TSA requiere la configuración de valores de red básicos. Si estos valores son adecuados para su red de TI, puede omitir esta sección.

Antes de empezar

Utilice la página **Red** para realizar cualquiera de estas acciones:

- Cambiar los valores de red básicos iniciales
- Configurar TSA para acceder a varias redes

Para configurar los valores de red básicos con la consola, siga los pasos que se indican en la sección “Configuración de los datos de red” en la página 19.

Configurar los valores de red básicos

Utilice la página **Red** para alterar los valores de red iniciales.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Red**.

Se muestra la página **Red**.

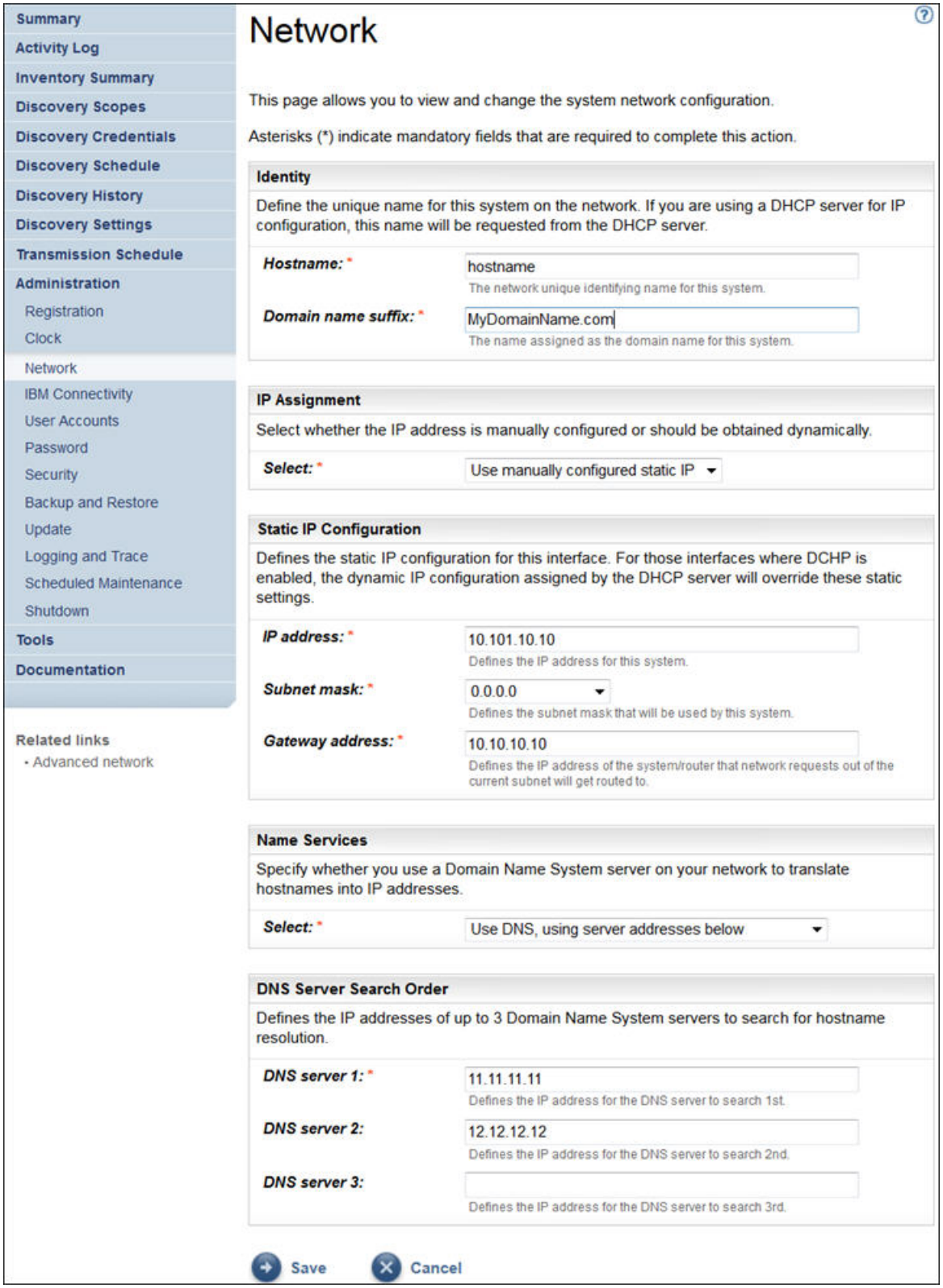

Figura 30. Red

2. En el campo **Nombre de host**, especifique el nombre exclusivo de este sistema en la red local.
3. En el campo **Sufijo de nombre de dominio**, especifique el nombre que se utiliza como nombre de dominio para este sistema en la red local.

4. Seleccione **Utilizar IP estática configurada manualmente** para la *Asignación de IP*. Para la asignación de dirección DHCP, consulte la sección Apéndice C, “Configuración de los datos de red DHCP”, en la página 133.
5. Configure la dirección IP estática:
   a) En el campo **Dirección IP**, indique la dirección IP de este sistema.
   b) En la lista desplegable **Máscara de subred**, seleccione la máscara de subred que debe utilizar este sistema.
   c) En el campo **Dirección de puerta de enlace**, indique la dirección IP del sistema o del direccionador que maneja as solicitudes fuera de la subred actual.
6. Especifique los **Servicios de nombres** según la asignación de IP.
   a) Para la IP estática configurada manualmente, seleccione la opción **Utilizar DNS utilizando las direcciones de servidor siguientes**.
   b) Para la asignación de dirección IP de DHCP, seleccione la opción **Utilizar DNS, pero obtener direcciones de servidor mediante DHCP**.
7. Especifique hasta tres direcciones IP de servidores DNS (Domain Name System) para utilizar al resolver nombres de host.

   TSA realiza búsquedas en los servidores en el orden en que se visualizan.
8. Pulse **Guardar** para guardar la configuración de red.

   Se le solicitará que reinicie el sistema.

   PRECAUCIÓN: Vaya con cuidado al cambiar los valores de red. Si se hace algún error con la configuración de red, puede que no se pueda acceder a la IU de TSA. En ese caso, se debe utilizar la consola de TSA para reparar la configuración de red.

   - Para VMware, utilice la interfaz web de VMware ESXi o el cliente de VMware vSphere
   - Para Microsoft Hyper-V, utilice Hyper-V Manager
9. Pulse **Cancelar** para salir de la página **Red** sin guardar los valores.

Configurar los valores de red avanzados

Si desea configurar TSA para acceder a varias redes, utilice la página **Red (opciones avanzadas)** para especificar estos valores de red.

Para configurar los valores de red avanzados, siga estos pasos:

1. En el panel de navegación, pulse **Administración** > **Red**.
2. En el panel de navegación inferior, en **Enlaces relacionados**, pulse **Red avanzada**.

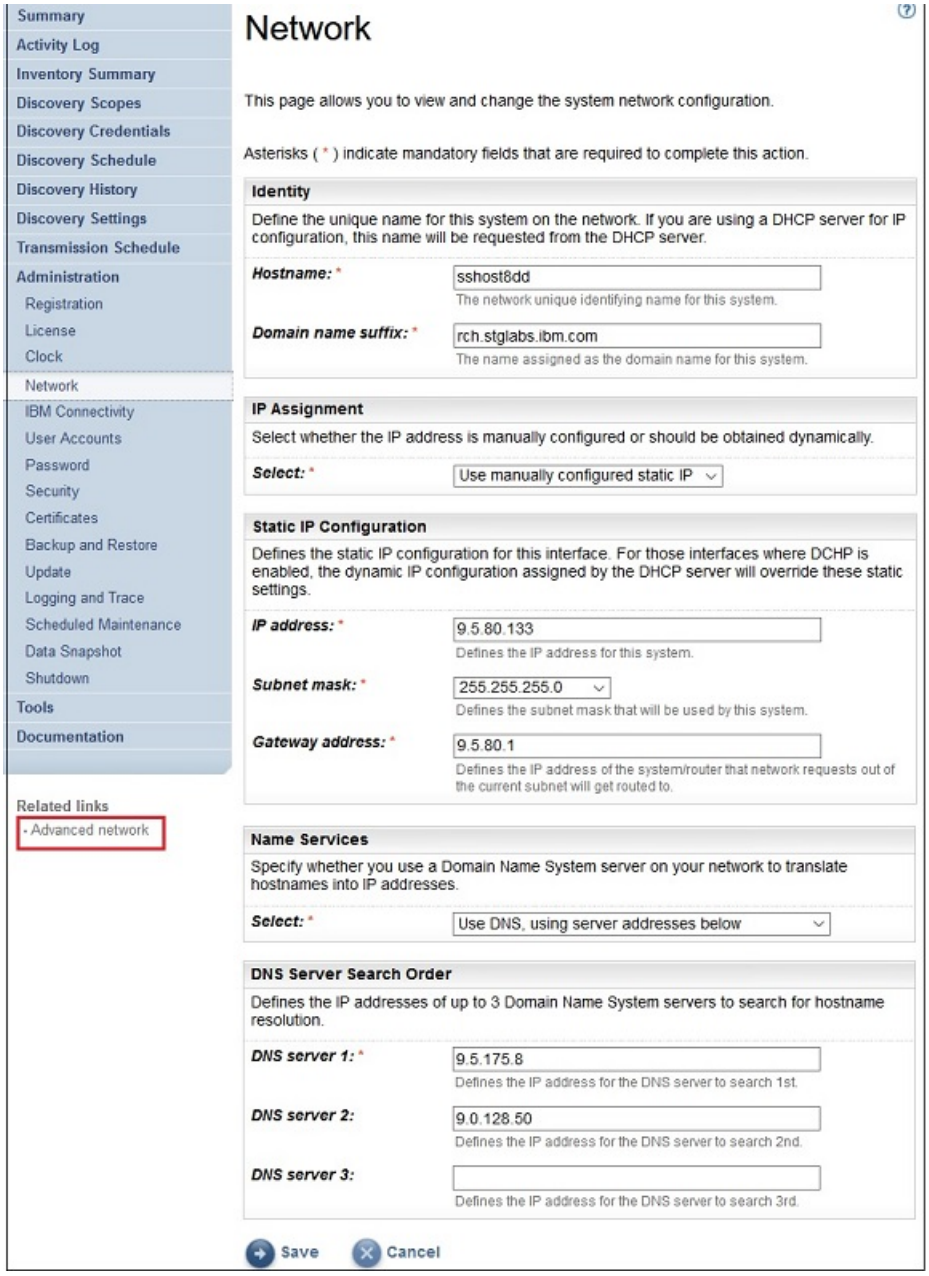

Figura 31. Acceda a la página Red (opciones avanzadas)

Se visualizará la página **Red (opciones avanzadas)**.

La página **Red (opciones avanzadas)**se divide en las siguientes páginas:

- Global
- Interfaces de red
- Configuración de DNS
- Rutas de red

Para acceder a cada una de estas páginas, pulse en la pestaña correspondiente a la página que desea visualizar.

Importante: Debe pulsar **Guardar** antes de salir de una página para guardar los cambios que haya hecho en los campos de esa página. Se le solicitará que reinicie el sistema para que los cambios entren en vigor.

Global

Utilice esta página para ver y modificar la configuración global de red:

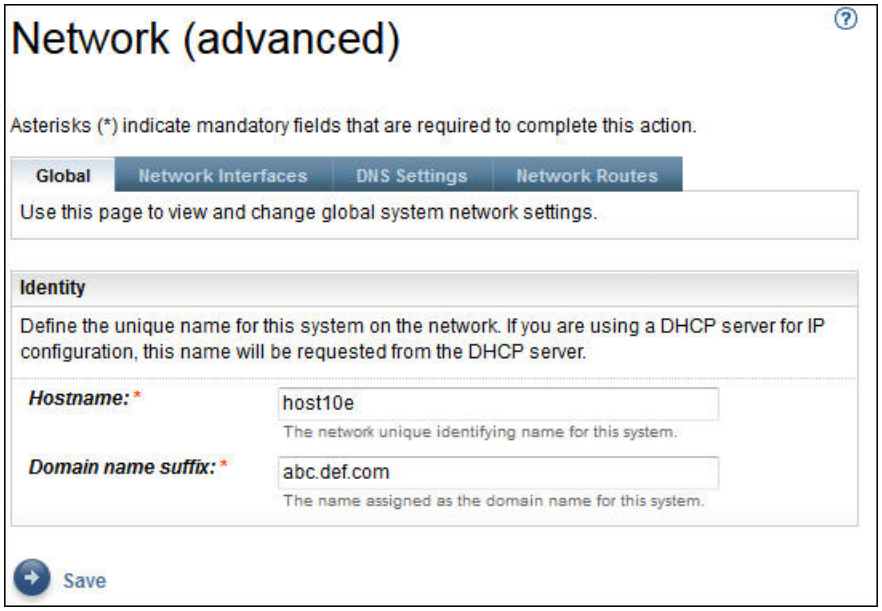

Figura 32. Red (opciones avanzadas) - Global

Identidad

Defina la identidad de este sistema en la red.

1. En el campo **Nombre de host**, especifique un nombre exclusivo para este sistema.
2. En el campo **Sufijo de nombre de dominio**, especifique el nombre utilizado como nombre de dominio para este sistema.

Interfaces de red

TSA está configurado para tener dos controladores de interfaz de red (NIC) - eth0 y eth1. Utilice esta página para ver y cambiar la configuración actual de la interfaz de red seleccionada.

1. Pulse **eth0** para seleccionar la interfaz de red eth0.
2. Pulse **eth1** para seleccionar la interfaz de red eth1.

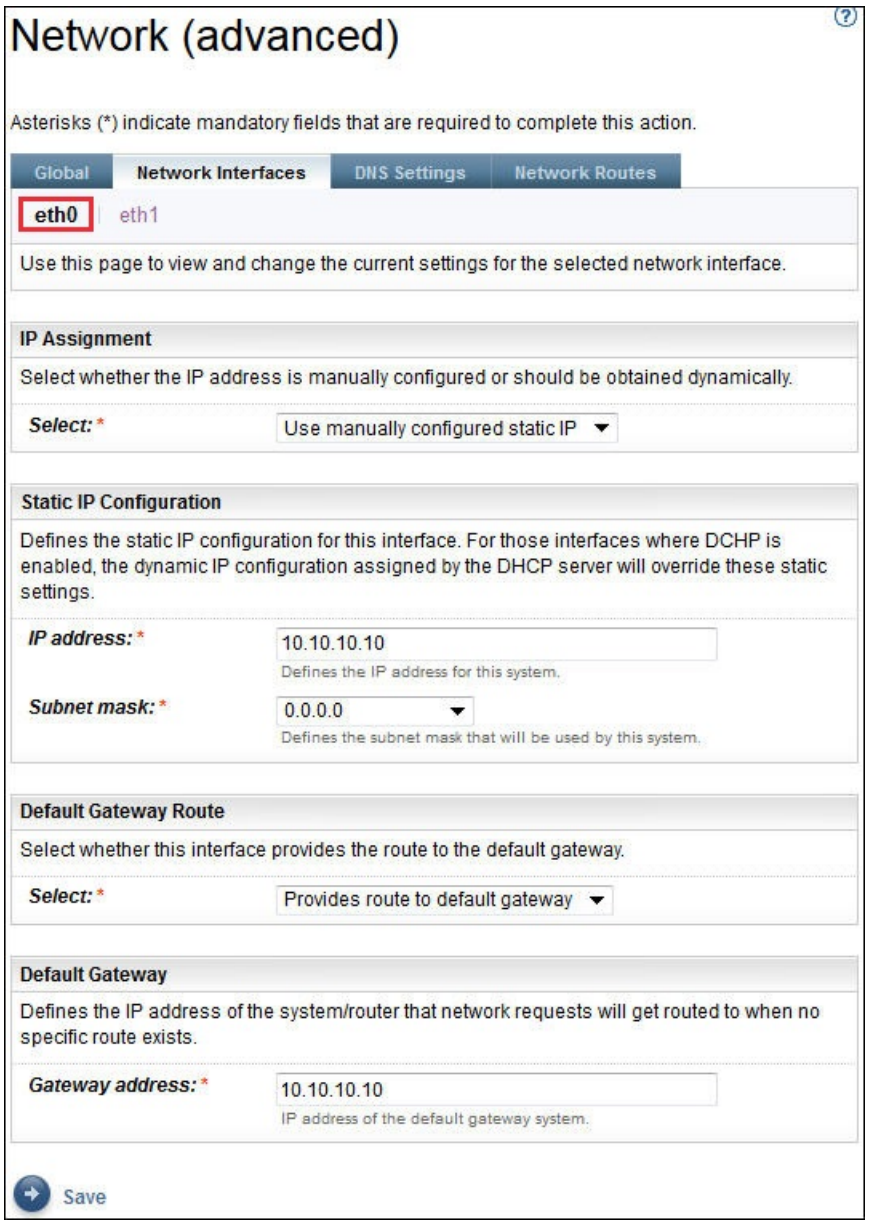

Figura 33. Red (opciones avanzadas) - Interfaces de red

Asignación de IP

Seleccione un método para asignar la dirección IP de este sistema. Puede ser obtener de forma dinámica la dirección IP de un servidor DHCP o utilizar una dirección IP estática configurada manualmente. Si elige utilizar una dirección IP estática configurada manualmente, debe configurar la dirección IP del sistema en esta página.

Configuración de IP estática

Si ha seleccionado configurar manualmente una dirección IP estática, especifique la información de IP para esta interfaz de red como se indica a continuación:

1. En el campo **Dirección IP**, especifique la dirección IP para este sistema.
2. En la lista desplegable **Máscara de subred**, seleccione la máscara de subred que debe utilizar este sistema.

Ruta de puerta de enlace predeterminada

Especifique siesta interfaz de red proporciona una ruta a la puerta de enlace predeterminada.

Puerta de enlace predeterminada

En el campo **Dirección de puerta de enlace**, especifique la dirección IP de la puerta de enlace predeterminada de este sistema.

Configuración de DNS

Utilice esta página para ver y cambiar la configuración de DNS.

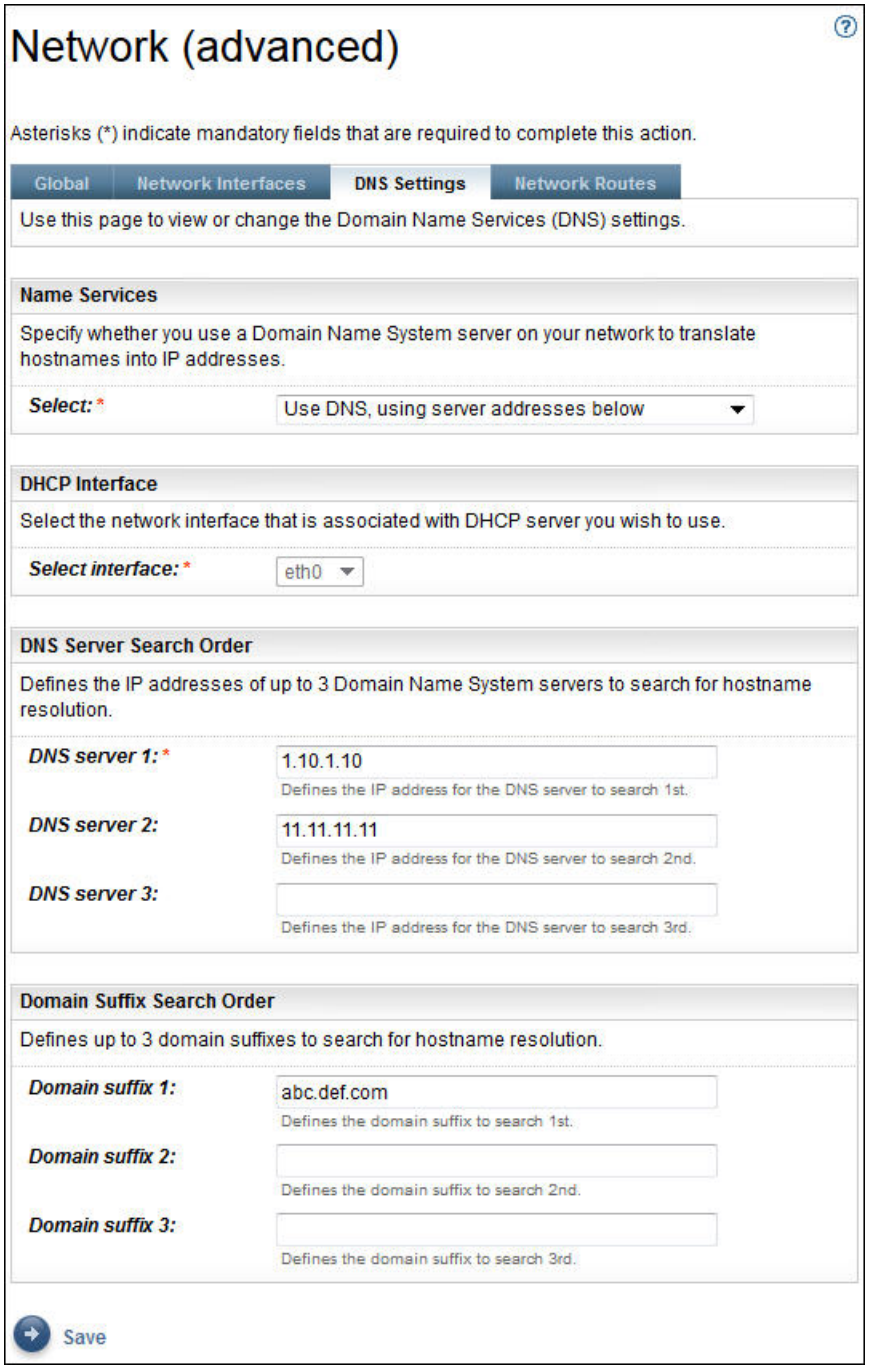

Figura 34. Red (opciones avanzadas) - Configuración de DNS

Servicios de nombres

Especifique un DNS (Domain Name System) en la red para convertir los nombres de host en direcciones IP. Puede elegir entre las opciones siguientes:

- Utilizar DNS, pero obtener las direcciones de servidor de un servidor DHCP.

Si elige esta opción, debe seleccionar la interfaz de red asociada al servidor DHCP que desea utilizar.

- Utilizar DNS con las direcciones de servidor que especifique.

  Si elige esta opción, debe especificar al menos un servidor DNS en esta página.

Interfaz DHCP
Seleccione la interfaz de red asociada al servidor DHCP que desea utilizar.

Orden de búsqueda de servidores DNS
Si elige utilizar DNS con las direcciones de servidor que usted especifique, introduzca hasta tres direcciones IP de servidores DNS (Domain Name System) para utilizar al resolver nombres de host. TSA realiza búsquedas en los servidores en el orden en que se visualizan.

Orden de búsqueda de sufijos de dominio
Si elige utilizar DNS con las direcciones de servidor que usted especifique, introduzca hasta tres sufijos de nombre de dominio para utilizar al resolver nombres de host. TSA busca en estos sufijos de nombre de dominio en el orden en que se visualizan.

Rutas de red

Utilice esta página para ver, añadir, cambiar o suprimir entradas de direccionamiento estático.

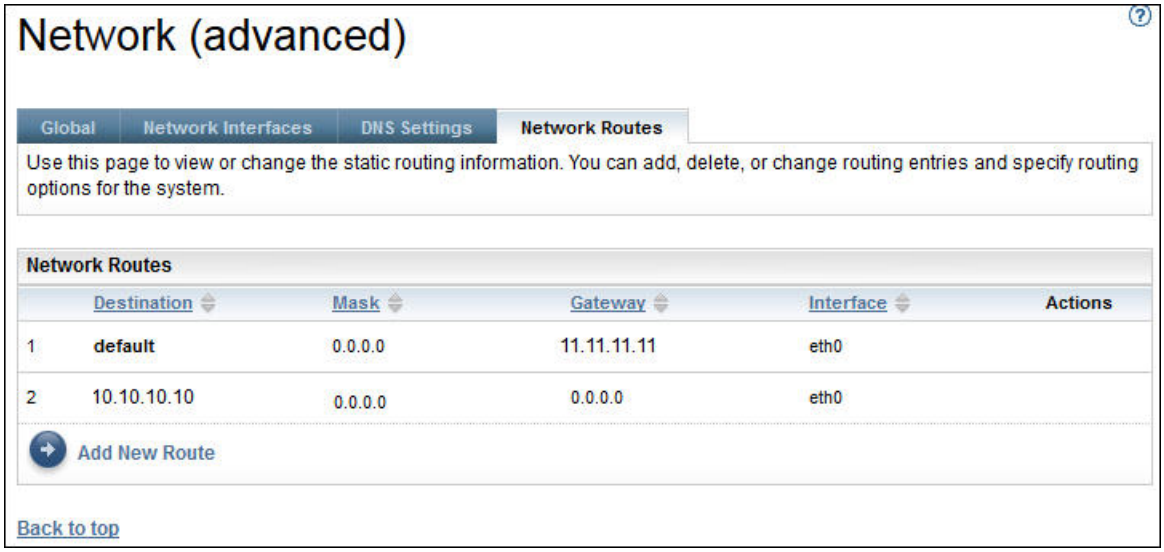

Figura 35. Red (opciones avanzadas) - Rutas de red

Se muestra la siguiente información para cada ruta de red:

Destino

Especifica el host o la dirección de subred de la red TCP/IP de destino.

Máscara
Especifica la máscara de subred a utilizar como máscara de red al añadir una ruta. Esta es la dirección de subred de la parte de host de la dirección IP. Las interfaces de red pueden utilizar máscaras de subred distintas, lo que proporciona la capacidad de añadir rutas seleccionando una máscara de subred (rutas de subred variables). Debe seleccionar una máscara de subred al añadir una ruta, en notación decimal con puntos de 32 bits.

Puerta de enlace
Especifica la dirección de puerta de enlace TCP/IP para direccionar los paquetes de IP.

Interfaz
Seleccione el adaptador en el menú. Es el nombre del adaptador de red asociado a la entrada de tabla.

Acciones
Pulse en el icono **Suprimir** para suprimir la ruta.

Nota: Las dos rutas que se muestran en la imagen no se pueden modificar ni suprimir.

Pulse **Añadir nueva ruta** para definir una nueva ruta de red estática. Se visualizará la página **Ruta de red**.

Añadir rutas de red

Puede añadir rutas de red estáticas.

Procedimiento

Para añadir una ruta de red, siga estos pasos:

1. En la página **Red (opciones avanzadas) - Rutas de red**, pulse **Añadir nueva ruta**. Se visualizará la página **Ruta de red**.

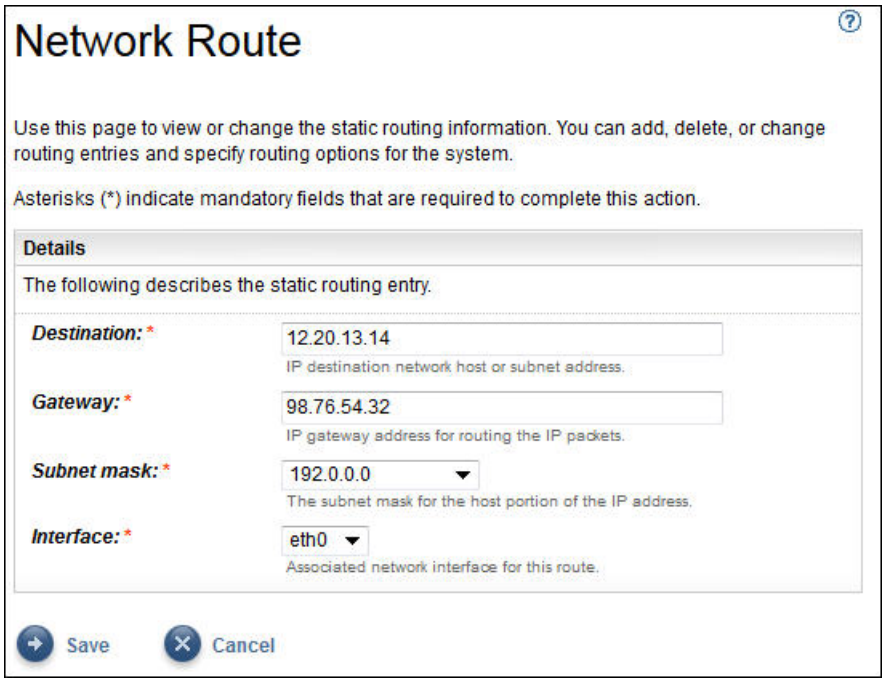

Figura 36. Nueva ruta de red

2. En el campo **Destino**, especifique la dirección IP del host de red o de la subred de destino de TCP/IP.
3. En el campo **Puerta de enlace**, especifique la dirección de la puerta de enlace TCP/IP para direccionar la información. La dirección debe estar en notación decimal con puntos de 32 bits. Por ejemplo: `xxx.xxx.xxx.xxx`.
4. En la lista desplegable **Máscara de subred**, seleccione la máscara de red a utilizar como máscara de red para esta ruta.
5. En la lista desplegable **Interfaz**, seleccione el adaptador de red a asociar a esta ruta.
6. Pulse **Guardar** para guardar esta ruta de red.

Configuración de certificados

La página **Certificados** permite ver la información de firma de certificados, generar e instalar certificados, o importar certificados. Se trata de los certificados de servidor que TSA presenta a un servidor web cuando se accede a la interfaz de usuario.

La configuración predeterminada de TSA implementa un certificado de servidor SSL autofirmado para facilitar la configuración. Para una mayor seguridad, se recomienda sustituir el certificado predeterminado una vez que se hayan completado el despliegue inicial y los pasos de configuración. Puede utilizar TSA para generar e instalar un certificado de servidor SSL autofirmado que sea exclusivo de este TSA, para generar e instalar un certificado personalizado firmado por la entidad emisora de certificados que elija, o para cargar su propio archivo de almacén de claves Java que contenga un certificado de servidor SSL personalizado.

Puede instalar un certificado personalizado utilizando uno de los siguientes métodos:

- “Instalar un certificado personalizado (utilizando firmantes)” en la página 43
- “Instalar un certificado personalizado (método alternativo) ” en la página 44

Ver el estado del certificado de servidor SSL

Al configurar TSA se instala el certificado de TSA predeterminado que se entrega con el Technical Support Appliance.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Certificados**.
   Se muestra la página **Certificados**.

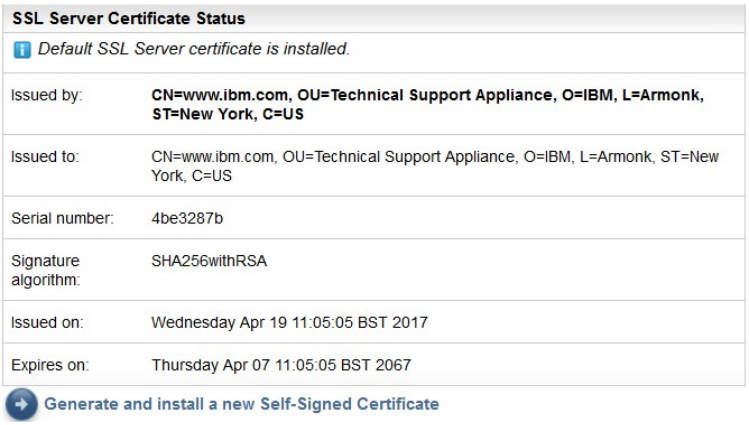

Figura 37. Estado de certificado de servidor SSL

   En la sección **Estado de certificado de servidor SSL** se muestra información sobre el certificado de servidor SSL que hay instalado en TSA. La información de certificados incluye *Emitido por*, *Emitido para*, *Emitido el*, *Caduca el*, *Número de serie* y *Algoritmo de firma*.
2. Pulse **Generar e instalar un nuevo certificado autofirmado** para instalar un certificado autofirmado que sea exclusivo de este TSA. Se muestra un mensaje de aviso indicando que el dispositivo se reiniciará automáticamente después de generar e instalar un certificado autofirmado.

   Nota: El botón **Generar e instalar un nuevo certificado autofirmado** solo está visible si el certificado instalado en TSA es el certificado predeterminado.

Generar y descargar CSR

Para solicitar un certificado SSL que esté certificado por una entidad emisora de certificados, tiene que proporcionar la siguiente información para generar y descargar el archivo de solicitud de firma de certificado (CSR - Certificate Signing Request).

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Certificados**.
   Se muestra la página **Certificados**.

Figura 38. Solicitud de firma de certificado

2. Introduzca el nombre completo de host (FQDN) del TSA en el campo **Nombre común**. El límite mínimo de caracteres es 1 y el límite máximo de caracteres es 64.
3. Especifique el nombre de organización, que permite diferenciar entre divisiones dentro de una organización, en el campo **Unidad organizativa**.
4. Especifique el nombre de la corporación, la sociedad limitada, la universidad o el organismo gubernamental en el campo **Organización**.
5. Especifique el nombre de la ciudad o localidad donde se opera TSA en el campo **Ciudad**.
6. Especifique el nombre de estado o provincia donde se opera TSA en el campo **Estado**. Si no está seguro del estado o si el estado no se aplica en su país, escriba *Desconocido*.
7. Seleccione el nombre del país donde se opera TSA en el menú desplegable **País**.
8. Especifique el número de días para los que es válido el certificado, empezando desde el momento en que se ha creado el certificado, en el campo **Número de días hasta el vencimiento**.
9. Pulse **Generar y descargar archivo de solicitud de firma de certificado** para crear y descargar el archivo de solicitud de firma de certificado (CSR -Certificate Signing Request) con la información especificada.

   Nota: Para restaurar el certificado predeterminado que se empaqueta con TSA, consulte la sección "Restaurar el certificado predeterminado" en la página 45.

Instalar un certificado personalizado (utilizando firmantes)

Utilice esta característica para instalar in certificado personalizado. Necesita el certificado de servidor generado por una entidad emisora de certificados, el certificado raíz de la entidad emisora de certificados y los certificados intermedios de la entidad emisora de certificados, si los hay.

Antes de empezar

Asegúrese de que los archivos de certificado (certificado raíz, intermedio y de servidor) están en cualquiera de los formatos siguientes -

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

Procedimiento

Siga los pasos siguientes para cargar e instalar los certificados en el TSA:

1. En el panel de navegación, pulse **Administración** > **Certificados**.

Se muestra la página **Certificados**.

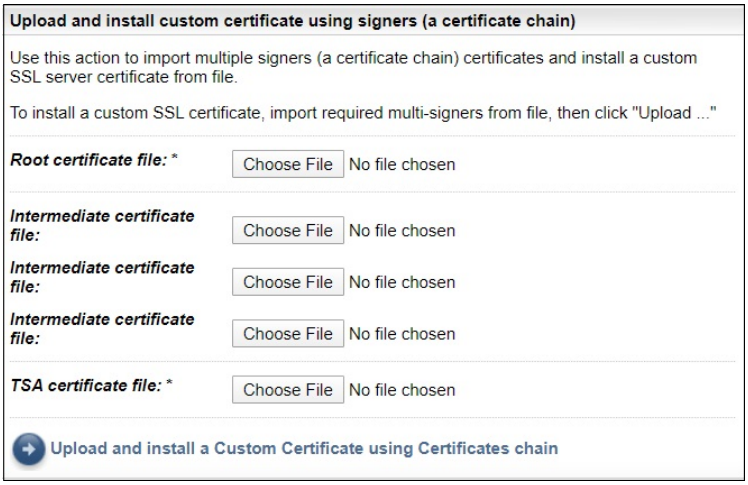

Figura 39. Instalar certificado personalizado

2. En el campo **Archivo de certificado raíz**, especifique la ubicación del archivo de certificado raíz que desea instalar en TSA.
3. En el campo **Archivo de certificado intermedio**, especifique la ubicación del archivo de certificado intermedio que desea instalar en TSA.

   Nota: Puede haber varios archivos de certificado intermedio (máximo 3) según los diversos firmantes que se hayan importado.
4. En el campo **Archivo de certificado de TSA**, especifique la ubicación del archivo de certificado de servidor de TSA que desea instalar en TSA.
5. Pulse **Cargar e instalar un certificado personalizado utilizando una cadena de certificados** para cargar todos los archivos (*Archivo de certificado raíz*, *Archivos de certificado intermedio*, *Archivo de certificado de TSA*) que ha especificado e instalar un certificado personalizado utilizando una cadena de certificados.

   Nota: Para restaurar el certificado predeterminado que se empaqueta con TSA, consulte la sección “Restaurar el certificado predeterminado” en la página 45.

Instalar un certificado personalizado (método alternativo)

Utilice esta característica para instalar in certificado personalizado. Puede utilizar esta función para desplegar un archivo de almacén de claves Java completo ya creado.

Antes de empezar

Se recomienda utilizar las funciones **Solicitud de firma de entidad emisora de certificados** y **Cargar e instalar el certificado personalizado utilizando firmantes (una cadena de certificados)** de la página **Certificados** para desplegar un certificado personalizado. No obstante, si ya ha creado un almacén de claves Java completo de forma independiente (que contenga las claves, el certificado personalizado y los certificado de autoridad emisora de certificados relevantes) puede utilizar esta función para desplegar el archivo de almacén de claves. Debe proporcionar la ubicación del archivo de almacén de claves y la contraseña para el archivo.

Nota: Cuando cree el archivo de almacén de claves, asegúrese de que la contraseña de entrada de clave y la contraseña del almacén de claves sean idénticas.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Certificados**.

   Se muestra la página **Certificados**.

Figura 40. Instalación de certificado personalizado

2. Para instalar un certificado de servidor personalizado, siga estos pasos.
   a) Indique la contraseña del certificado en el campo **Contraseña de certificado**.
   b) Escriba de nuevo la contraseña en el campo **Confirmar contraseña**.

      Las dos contraseñas que introduzca se comparan para confirmar que coinciden antes de guardar la contraseña.
   c) Especifique la ubicación del archivo de almacén de claves Java que contiene el certificado personalizado en el campo **Archivo de certificado personalizado**.
   d) Pulse **Cargar e instalar un archivo JKS completo** para cargar el archivo de almacén de claves Java que ha especificado e instale un certificado personalizado. El archivo de almacén de claves Java debe incluir el certificado personalizado y cualesquiera certificados raíz e intermedios relevantes de la entidad emisora de certificados. El dispositivo se reiniciará para activar el uso del nuevo certificado.

Nota: Para restaurar el certificado predeterminado que se empaqueta con TSA, consulte la sección "Restaurar el certificado predeterminado" en la página 45.

Resultados

Una vez instalado el nuevo certificado, el TSA se reinicia automáticamente. Tras completarse el reinicio, es posible que en su navegador aparezca una solicitud de seguridad sobre si el nuevo certificado es de confianza.

Restaurar el certificado predeterminado

Para restaurar el certificado predeterminado que se empaqueta con TSA, utilice la consola de TSA y seleccione la opción **Establecer el certificado del dispositivo al predeterminado**.

Procedimiento

1. Inicie la consola de TSA.
2. Seleccione la opción **3) Establecer el certificado del dispositivo al predeterminado** en el **Menú de configuración de TSA**.

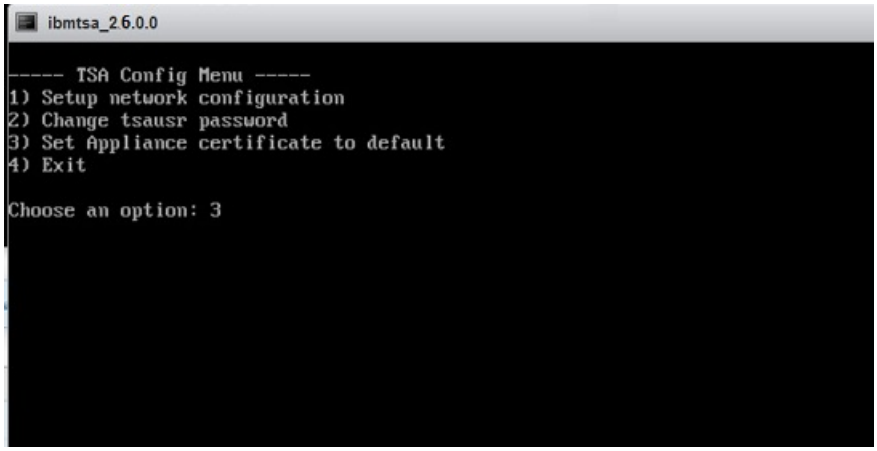

Figura 41. Establecer el certificado del dispositivo al predeterminado

3. **Confirmar que se establece el certificado del dispositivo al certificado predeterminado [s|n]:** Indique **s** para confirmar que desea establecer el certificado del TSA al certificado predeterminado.

Resultados

Una vez instalado el certificado predeterminado, el TSA se reinicia automáticamente en 5 segundos. Tras completarse el reinicio, es posible que en su navegador aparezca una solicitud de seguridad sobre si el certificado predeterminado es de confianza.

Planificar la limpieza de datos de inventario

Puede planificar o ejecutar manualmente una tarea de limpieza de todos los datos de inventario recopilados en los recursos, desde el momento en que se descubren.

Acerca de esta tarea

Atención: Se recomienda ejecutar la tarea de limpieza una vez a la semana para la mayoría de instalaciones.

Para ver la planificación actual de la tarea de limpieza de inventario, seleccione **Resumen de inventario** > **Planificación de limpieza de inventario**.

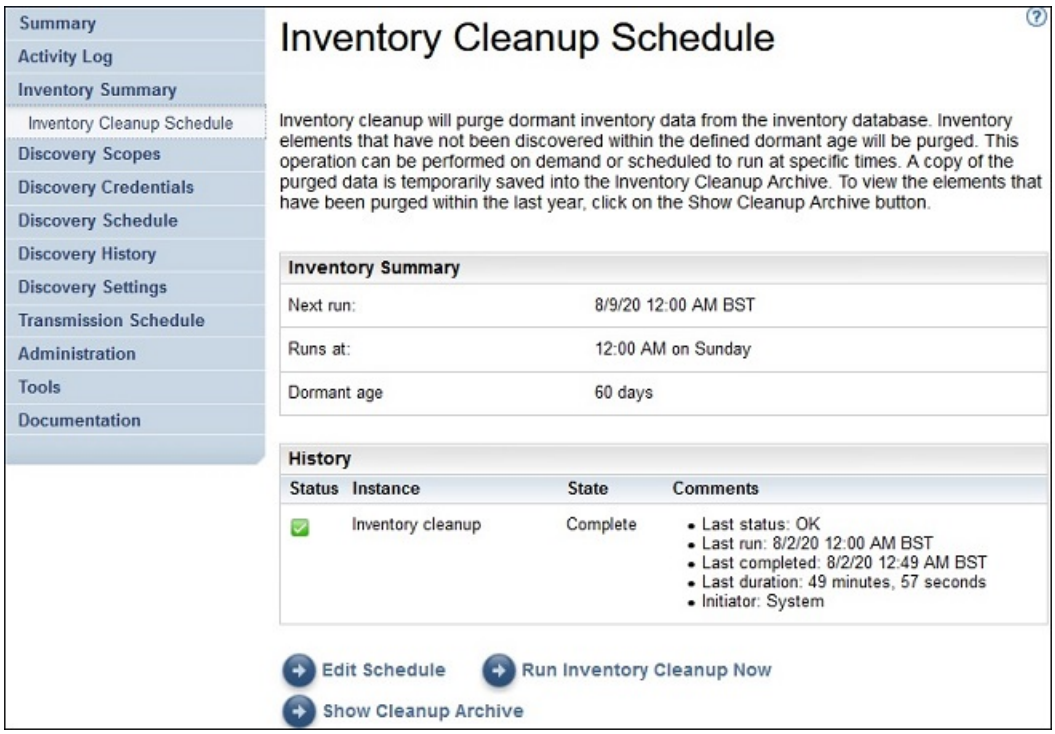

Figura 42. Planificación de limpieza de inventario

Para ejecutar la limpieza de inventario manualmente, pulse **Ejecutar limpieza de inventario ahora**.

Para editar, habilitar o deshabilitar la planificación de limpieza de inventario actual, siga estos pasos:

Procedimiento

1. En la página **Planificación de limpieza de inventario**, pulse **Editar planificación**.
2. En la página **Configuración de inventario**, seleccione **Habilitar limpieza de inventario planificada** para habilitar la tarea de limpieza de inventario o **Deshabilitar limpieza de inventario planificada** para deshabilitar la tarea de limpieza de inventario.
3. Si elige habilitar la tarea de limpieza de inventario, complete los pasos siguientes:
   a) Seleccione las listas desplegables **A la hora** y **En el minuto** para seleccionar una nueva hora.
   b) Seleccione el **Modo de selección del día**. Para planificar la limpieza de inventario en un día o días concretos de la semana, seleccione la opción **Semanalmente los días (dom - sáb)** o, para planificarla limpieza de inventario en unos días concretos del mes, seleccione la opción **Mensualmente los días (1-31)**.
   c) En el campo **Los días**, seleccione los recuadros adecuados para seleccionar días distintos o adicionales de la semana o del mes.

      Nota: Si selecciona los días más allá de un mes específico, el trabajo se activa el último día de ese mes en concreto.
4. Seleccione el periodo durante el cual desea conservar los datos de inventario en la lista **Tiempo de inactividad**.
5. Pulse **Guardar**.

Capítulo 5. Configurar el descubrimiento y la transmisión a IBM

Una vez completada la configuración de TSA, puede utilizar diversas características de administración para gestionar el descubrimiento, la transmisión y los trabajos.

Alcances de descubrimiento

Un alcance de descubrimiento especifica la dirección IP, el rango de direcciones IP o la red que se va a utilizar para descubrir elementos de TI. Los alcances de descubrimiento se agrupan en conjuntos de alcances de descubrimiento.

TSA proporciona varios tipos de alcances de descubrimiento:

- Conjuntos de alcances dinámicos de HMC: pueden utilizarse para descubrir HMC junto con todas las particiones que gestiona.
- Conjuntos de alcances dinámicos de VMware: pueden utilizarse para descubrir los hosts VMware vCenter o ESXi junto con todas las máquinas virtuales en los hosts ESXi.
- Alcances de descubrimiento general: se utilizan para descubrir los demás recursos que no se descubren utilizando un conjunto de alcances dinámicos. Las direcciones IP, el rango de direcciones IP o las redes pueden especificarse manualmente, o puede importarse una lista de direcciones IP desde un archivo a TSA.

Alcances dinámicos de HMC

Puede definir alcances dinámicos de HMC para recopilar un inventario detallado de las HMC, los IBM Power Systems que gestionan, y las LPAR de VIOS, AIX y Linux en dichos sistemas.

Acerca de esta tarea

Además de recuperar información de inventario de las HMC definidas, TSA también consulta las LPAR que gestionan estas HMC dinámicamente, sin que sea necesario crear y mantener muchas definiciones de alcances. Debe definir un alcance para las HMC y seleccionar los tipos de LPAR (AIX, VIOS y Linux) que desea explorar automáticamente cuando se descubran estas HMC. La ventaja es que aunque cambien las LPAR, no es necesario volver a configurar TSA.

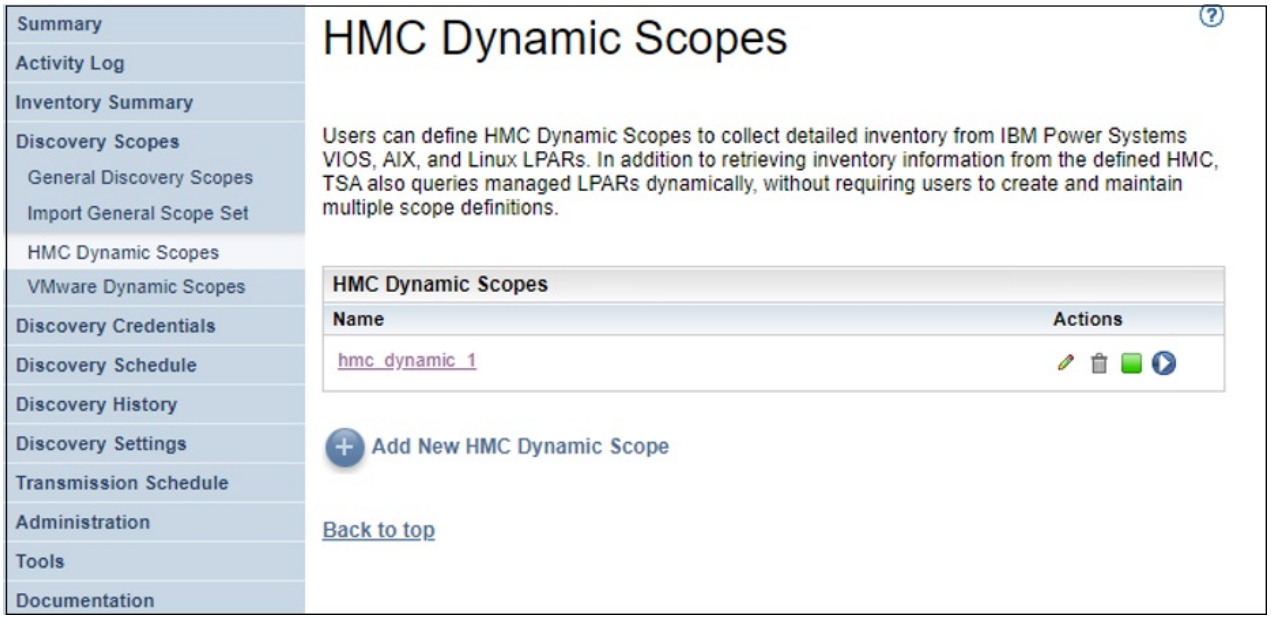

Figura 43. Alcances dinámicos de HMC

Visualización de alcances dinámicos de HMC
Puede visualizar los alcances dinámicos de HMC existentes.

Acerca de esta tarea

Para visualizar los alcances dinámicos de HMC existentes, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC** en el panel de navegación. Se mostrará la página **Alcances dinámicos de HMC**. El panel **Alcances dinámicos de HMC** contiene una lista de los Alcances dinámicos de HMC.

Para visualizar los alcances y credenciales asociados con un conjunto de alcances dinámicos específico, pulse el nombre del conjunto de alcances en la columna **Nombre**. Se mostrará la página **Conjunto de alcances dinámicos de HMC**.

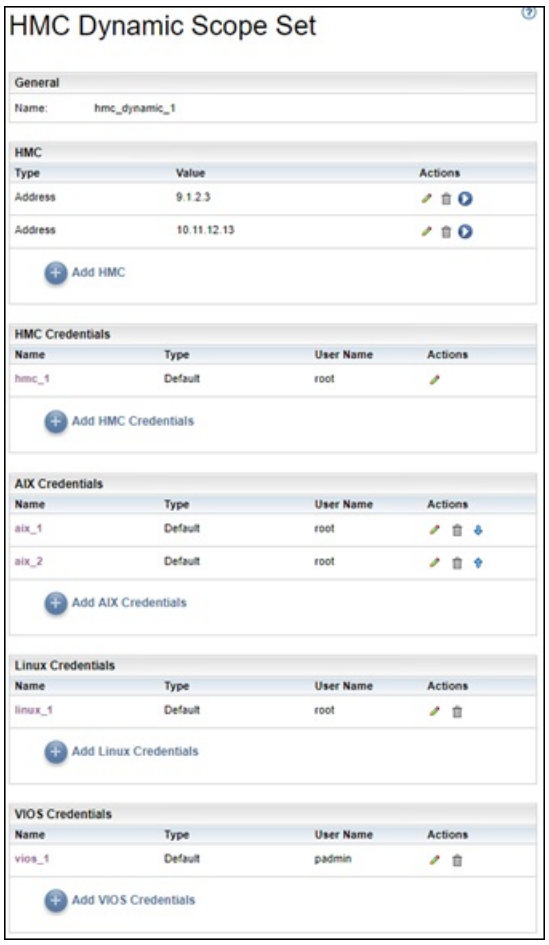

Figura 44. Ver un Conjunto de alcances dinámicos de HMC

El panel **HMC** muestra la lista de direcciones IP de las HMC que descubre el conjunto de alcances dinámicos. Los distintos paneles de credenciales como, por ejemplo, **Credenciales de AIX**, muestran las credenciales que se han configurado en el conjunto de alcances.

Añadir alcances dinámicos de HMC

Para añadir un Conjunto de alcances dinámicos de HMC, especifique la dirección IP de una HMC individual junto con la credencial para acceder a la HMC. De manera opcional, puede especificar las credenciales de AIX, Linux y VIOS para permitir el descubrimiento de las LPAR de IBM Power Systems que gestiona la HMC. Una vez creado el Conjunto de alcances dinámicos de HMC, puede editarse para definir direcciones IP de HMC adicionales. Los Conjuntos de alcances dinámicos de HMC también pueden editarse para dar soporte a varias credenciales para acceder a las HMC, así como a varias credenciales para acceder a las LPAR.

Acerca de esta tarea

Para añadir un conjunto de alcances, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**.
   Se mostrará la página **Alcances dinámicos de HMC**.
2. Para definir un nuevo conjunto de alcances dinámicos de HMC, pulse **Añadir nuevo alcance dinámico de HMC**.
   Se mostrará la página **Conjunto de alcances dinámicos de HMC**.

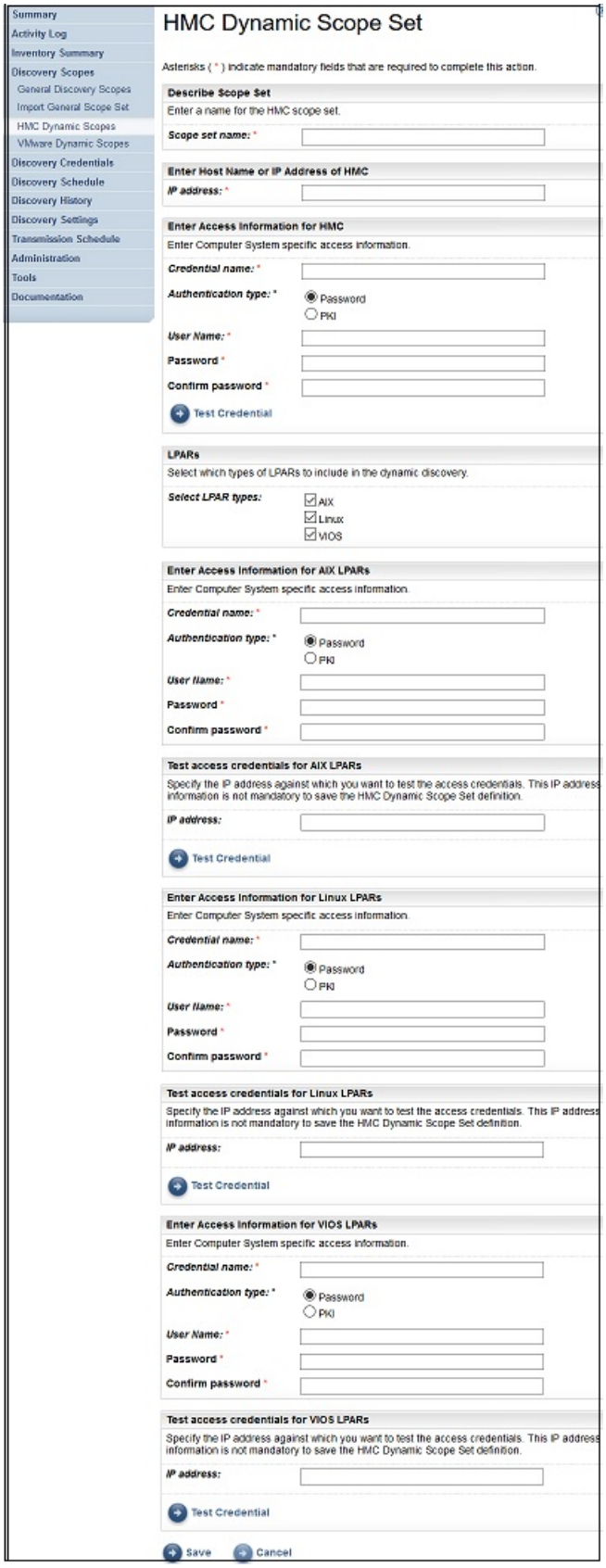

Figura 45. Añadir conjunto de alcances dinámicos de HMC

3. En el panel **Describir el conjunto de alcances**, especifique un nombre exclusivo en el campo **Nombre de conjunto de alcances**.

4. En el panel **Especificar nombre de host o dirección IP de la HMC**, especifique el nombre de host o la dirección IP de la HMC.
5. En el panel **Especificar información de acceso para la HMC**, especifique los detalles siguientes:
   a) Especifique el **Nombre de credencial**.
   b) Seleccione el **Tipo de autenticación**.
      - **Contraseña** - Utiliza la contraseña proporcionada.
      - **PKI** - Utiliza la clave SSH asociada al conjunto de alcances específico.
   c) Especifique el **Nombre de usuario** que se utiliza para autenticarse con la HMC.
   d) Cuando el **Tipo de autenticación** sea **Contraseña**, especifique la **Contraseña** y repítala en **Confirmar contraseña**.
   e) Cuando el **Tipo de autenticación** sea **PKI**, especifique la **Frase de contraseña** y **Confirmar frase de contraseña** si la clave SSH está cifrada. Si la clave SSH no está cifrada, deje estos dos campos en blanco.
   f) Si **Tipo de autenticación** es **PKI**, pulse **Elegir archivo** y cargue la clave privada en TSA. Debe desplegar externamente la clave pública en la HMC.
   g) Opcional: Pulse **Probar credencial** para probar las credenciales de la HMC de destino.
6. En el panel **LPAR**, seleccione los tipos de LPAR (AIX, LINUX, VIOS) que se van a incluir en el descubrimiento dinámico.
7. Si selecciona cualquiera de los tipos de LPAR (AIX, Linux, VIOS), especifique la información de acceso correspondiente.

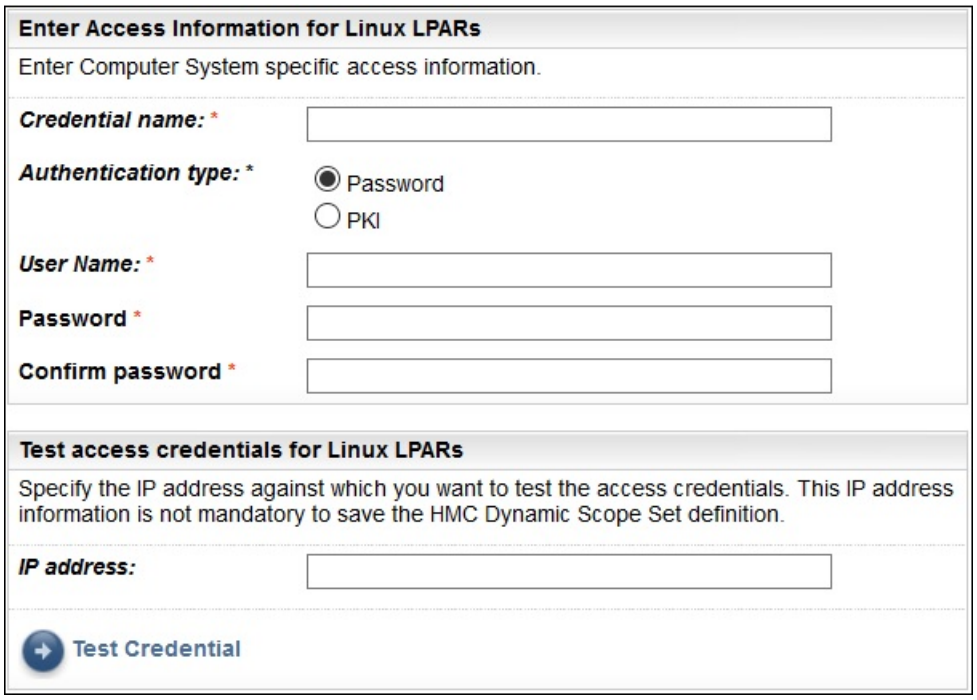

Figura 46. Ejemplo: Especificar información de acceso de las LPAR de Linux

   a) Especifique el **Nombre de credencial**.
   b) Seleccione el **Tipo de autenticación**.
      - **Contraseña** - Utiliza la contraseña proporcionada.
      - **PKI** - Utiliza la clave SSH asociada al conjunto de alcances específico.
   c) Especifique el **Nombre de usuario** que se utiliza para autenticarse con la LPAR respectiva.
   d) Cuando el **Tipo de autenticación** sea **Contraseña**, especifique la **Contraseña** y repítala en **Confirmar contraseña**.

e) Cuando el **Tipo de autenticación** sea **PKI**, especifique la **Frase de contraseña** y **Confirmar frase de contraseña** si la clave SSH está cifrada. Si la clave SSH no está cifrada, deje estos dos campos en blanco.

f) Si **Tipo de autenticación** es **PKI**, pulse **Elegir archivo** y cargue la clave privada en TSA. Debe desplegar externamente la clave pública en cada LPAR.

g) Opcional: Especifique la **dirección IP** de una LPAR gestionada por esta HMC y pulse **Probar credencial** para probar las credenciales de la LPAR de objetivo.

8. Pulse **Guardar** para guardar el conjunto de alcances dinámicos de HMC.

Modificar alcances dinámicos de HMC - Direcciones IP de HMC
Puede modificar la lista de direcciones IP de HMC asociadas con un conjunto de alcances dinámicos de HMC existente.

Acerca de esta tarea
Para modificar la lista de direcciones IP de HMC, siga estos pasos.

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**.
   Se mostrará la página **Alcances dinámicos de HMC**.
2. Para editar el conjunto de alcances, pulse el icono .
   Se mostrará la página **Conjunto de alcances dinámicos de HMC**.
   - Para añadir una dirección IP de HMC al conjunto de alcances, siga estos pasos:
     a. En el panel **HMC**, pulse **Añadir HMC**. Se mostrará la página **Alcances dinámicos de HMC**.
     b. Especifique la **Dirección IP** de la HMC en el panel **Describir dirección o host**.
     c. Pulse **Guardar** para añadir la HMC.
   - Para editar una dirección IP de HMC en el conjunto de alcances, siga estos pasos:
     a. En el panel **HMC**, pulse el icono . Se mostrará la página **Alcances dinámicos de HMC**.
     b. Modifique la **Dirección IP** de la HMC en el panel **Describir dirección o host**.
     c. Pulse **Guardar** para modificar la HMC.
   - Para suprimir una dirección IP de HMC en el conjunto de alcances, siga estos pasos:
     a. En el panel **HMC**, pulse el icono .
     b. En el recuadro de diálogo, pulse **Aceptar** para confirmar la supresión.

        Nota: Un Conjunto de alcances dinámicos de HMC siempre debe tener al menos una dirección IP de HMC definida. TSA no permite suprimir todas las direcciones IP de HMC.

Modificar alcances dinámicos de HMC - Credenciales
Puede modificar la lista de credenciales asociadas con un conjunto de alcances dinámicos de HMC existente.

Acerca de esta tarea
Un Conjunto de alcances dinámicos de HMC siempre debe tener al menos una credencial de HMC definida. TSA no permite suprimir todas las credenciales de HMC. Si no hay credenciales para AIX, Linux o VIOS, TSA no recopila información detallada para ese tipo de LPAR.

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**.
   Se mostrará la página **Alcances dinámicos de HMC**.

2. Para editar el conjunto de alcances, pulse el icono .

   Se mostrará la página **Conjunto de alcances dinámicos de HMC**.

   - Para añadir una credencial de HMC para AIX, Linux o VIOS, siga estos pasos:

     a. En el panel **Credenciales** correspondiente, pulse **Añadir credenciales**. Por ejemplo, para añadir una credencial de HMC, pulse **Añadir credenciales de HMC** en el panel **Credenciales de HMC**. Se mostrará la página **Nuevas credenciales de descubrimiento de HMC**.

     b. Especifique el **Nombre de credencial**.

     c. Seleccione el **Tipo de autenticación**.

        – **Contraseña** - Utiliza la contraseña proporcionada.

        – **PKI** - Utiliza la clave SSH asociada al conjunto de alcances específico.

     d. Especifique el **Nombre de usuario** que se utiliza para autenticarse en HMC o la LPAR correspondiente.

     e. Cuando el **Tipo de autenticación** sea **Contraseña**, especifique la **Contraseña** y repítala en **Confirmar contraseña**.

     f. Cuando el **Tipo de autenticación** sea **PKI**, especifique la **Frase de contraseña** y **Confirmar frase de contraseña** si la clave SSH está cifrada. Si la clave SSH no está cifrada, deje estos dos campos en blanco.

     g. Si **Tipo de autenticación** es **PKI**, pulse **Elegir archivo** y cargue la clave privada en TSA. Debe desplegar externamente la clave pública en las HMC o LPAR.

     h. **Opcional:** especifique la **dirección IP** de la HMC o LPAR y pulse **Probar credencial** para probar las credenciales de la LPAR de objetivo.

     i. Pulse **Guardar** para guardar la credencial del conjunto de alcances dinámicos de HMC.

   - Para editar una credencial de HMC para AIX, Linux o VIOS, siga estos pasos:

     a. En el panel **Credenciales** correspondiente, pulse el icono para la credencial que desee modificar. Por ejemplo, para editar una credencial de HMC, pulse en el panel **Credenciales de HMC** para la credencial que desee modificar. Se mostrará la página **Editar credenciales de descubrimiento de HMC**.

     b. En el panel **Especificar información de acceso**, puede modificar los detalles siguientes:

        1) Especifique el **Nombre de usuario** que se utiliza para autenticarse en HMC o la LPAR correspondiente.

        2) Seleccione el **Tipo de autenticación**.

           – **Contraseña** - Utiliza la contraseña proporcionada.

           – **PKI** - Utiliza la clave SSH asociada al conjunto de alcances específico.

        3) Cuando el **Tipo de autenticación** sea **Contraseña**, especifique la **Contraseña** y repítala en **Confirmar contraseña**.

        4) Cuando el **Tipo de autenticación** sea **PKI**, especifique la **Frase de contraseña** y **Confirmar frase de contraseña** si la clave SSH está cifrada. Si la clave SSH no está cifrada, deje estos dos campos en blanco.

        5) Si **Tipo de autenticación** es **PKI**, pulse **Elegir archivo** y cargue la clave privada en TSA. Debe desplegar externamente la clave pública en cada HMC o LPAR.

     c. **Opcional:** especifique la **dirección IP** de la HMC o LPAR y pulse **Probar credencial** para probar las credenciales de la LPAR de objetivo.

     d. Pulse **Guardar** para actualizar las modificaciones de la credencial correspondiente.

   - Para suprimir una credencial de HMC para AIX, Linux o VIOS, siga estos pasos:

     a. En el panel **Credenciales** correspondiente, pulse el icono **Suprimir** para la credencial correspondiente. Por ejemplo, para suprimir una credencial de HMC, pulse el icono en el

panel **Credenciales de HMC** para la credencial que desee suprimir. Se muestra un mensaje de confirmación.

b. Pulse **Aceptar** para suprimir la credencial correspondiente.

- Para modificar una credencial de HMC para AIX, Linux o VIOS, siga estos pasos:

a. Si hay más de una credencial de HMC para AIX, Linux o VIOS, puede modificarse el orden de las credenciales para las HMC o las LPAR. Cuando hay una única credencial, las flechas arriba y abajo no aparecen en la columna **Acciones** para el panel de credenciales.

b. En el panel **Credenciales** correspondiente, pulse los iconos o para reordenar la credencial correspondiente.

Habilitación o deshabilitación de conjuntos de alcances dinámicos
Puede habilitar o deshabilitar un Conjunto de alcances dinámicos de HMC.

Acerca de esta tarea

Un conjunto de alcances deshabilitado se omite durante un descubrimiento planificado.

Nota: Siempre puede realizarse un descubrimiento manual independientemente del estado del conjunto de alcances.

Deshabilitación de conjuntos de alcances dinámicos

Procedimiento

Para deshabilitar un conjunto de alcances dinámicos de HMC, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**.
   Se mostrará la página **Alcances dinámicos de HMC**.
2. Pulse el icono **Habilitar** junto al conjunto de alcances que desee deshabilitar.

Habilitación de conjuntos de alcances dinámicos

Procedimiento

Para habilitar un conjunto de alcances dinámicos de HMC, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**.
   Se mostrará la página **Alcances dinámicos de HMC**.
2. Pulse el icono **Deshabilitar** junto al conjunto de alcances que desee habilitar.

Descubrimiento de una HMC
Puede iniciar manualmente un descubrimiento de una HMC individual en un Conjunto de alcances dinámicos de HMC. El descubrimiento recopila información sobre la HMC junto con las LPAR asociadas.

Procedimiento

Para iniciar manualmente un descubrimiento de una HMC, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**.
   Se mostrará la página **Alcances dinámicos de HMC**.
2. Pulse el icono para el Conjunto de alcances dinámicos de HMC necesario. Se mostrará la página **Conjunto de alcances dinámicos de HMC**.
3. Pulse el icono al lado de la dirección IP de HMC que desee descubrir.

Descubrimiento de conjuntos de alcances dinámicos
Puede iniciar manualmente un descubrimiento de un Conjunto de alcances dinámicos de HMC. El descubrimiento recopila información sobre las HMC definidas en el conjunto de alcances junto con las LPAR asociadas.

Procedimiento

Para iniciar manualmente un descubrimiento de un Conjunto de alcances dinámicos de HMC, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**.
   Se mostrará la página **Alcances dinámicos de HMC**.
2. Pulse el icono **Ejecutar** junto al conjunto de alcances que desee descubrir.

Suprimir alcances dinámicos de HMC
Puede suprimir un conjunto de alcances dinámicos de HMC.

Procedimiento

Para suprimir un conjunto de alcances dinámicos de HMC, siga estos pasos:

1. En el panel de navegación, pulse **Alcances dinámicos de HMC**.
   Se mostrará la página **Alcances dinámicos de HMC**.
2. Pulse en el icono **Suprimir** junto al conjunto de alcances que desee suprimir.
3. Pulse **Aceptar** para confirmar que desea suprimir el conjunto de alcances dinámicos de HMC.

   Nota: Cuando confirma la supresión del conjunto de alcances dinámicos de HMC, también se suprime la información de acceso correspondiente para las LPAR de AIX, Linux o VIOS.

Alcances dinámicos de VMware

Puede definir alcances dinámicos de VMware para recopilar inventario detallado de instancias de VMware vCenter Server y ESXi. Los alcances dinámicos de VMware también recopilan información sobre los servidores x86 gestionados por la instancia de VMware vCenter Server o ESXi, y las máquinas virtuales de Linux y Windows en esos sistemas.

TSA recupera información de inventario de las instancias de VMware vCenter Server y ESXi definidas. TSA también consulta las máquinas virtuales gestionadas dinámicamente por las instancias de VMware, sin necesidad de crear y mantener varias definiciones de alcance. Debe definir un alcance para las instancias de VMware y seleccionar los tipos de máquinas virtuales (Linux y Windows) que desea explorar automáticamente cuando se descubran estas instancias de VMware. La ventaja es que aunque cambien las máquinas virtuales, no es necesario volver a configurar TSA.

El descubrimiento de VMware vCenter Server encuentra todas las instancias de VMware ESXi que gestiona, lo que elimina la necesidad de descubrir las instancias de VMware ESXi directamente. Para las instancias de VMware ESXi que no están gestionadas por VMware vCenter Server, TSA puede descubrirlas directamente definiendo VMware ESXi en el alcance dinámico de VMware.

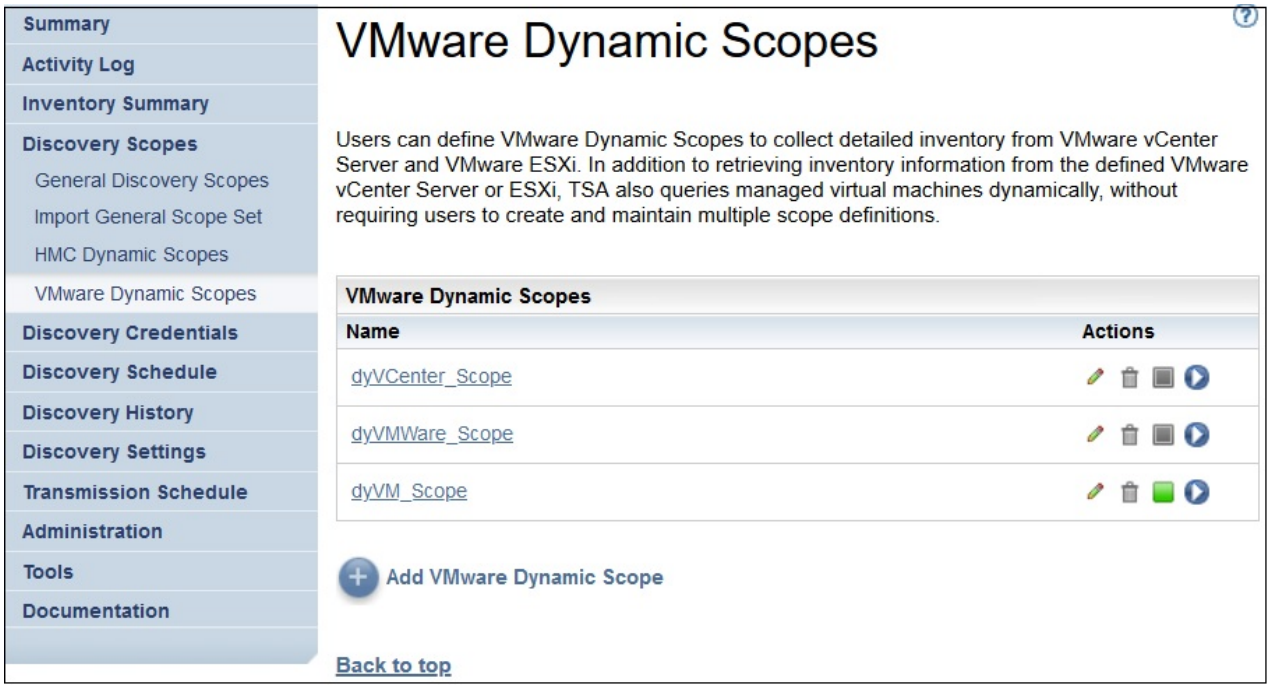

Figura 47. Alcances dinámicos de VMware

Visualización de alcances dinámicos de VMware, conjuntos de alcances y credenciales.
Puede visualizar los alcances dinámicos de VMware y los conjuntos de alcances existentes.

Acerca de esta tarea

Para visualizar los conjuntos de alcances dinámicos de VMware existentes, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMware** en el panel de navegación. Se mostrará la página **Alcances dinámicos de VMware**. El panel **Alcances dinámicos de VMware** contiene una lista de los alcances dinámicos de VMware.

Para visualizar los alcances y credenciales asociados con un conjunto de alcances dinámicos específico, pulse el nombre del conjunto de alcances en la columna **Nombre**. Se mostrará la página **Conjunto de alcances dinámicos de VMware**.

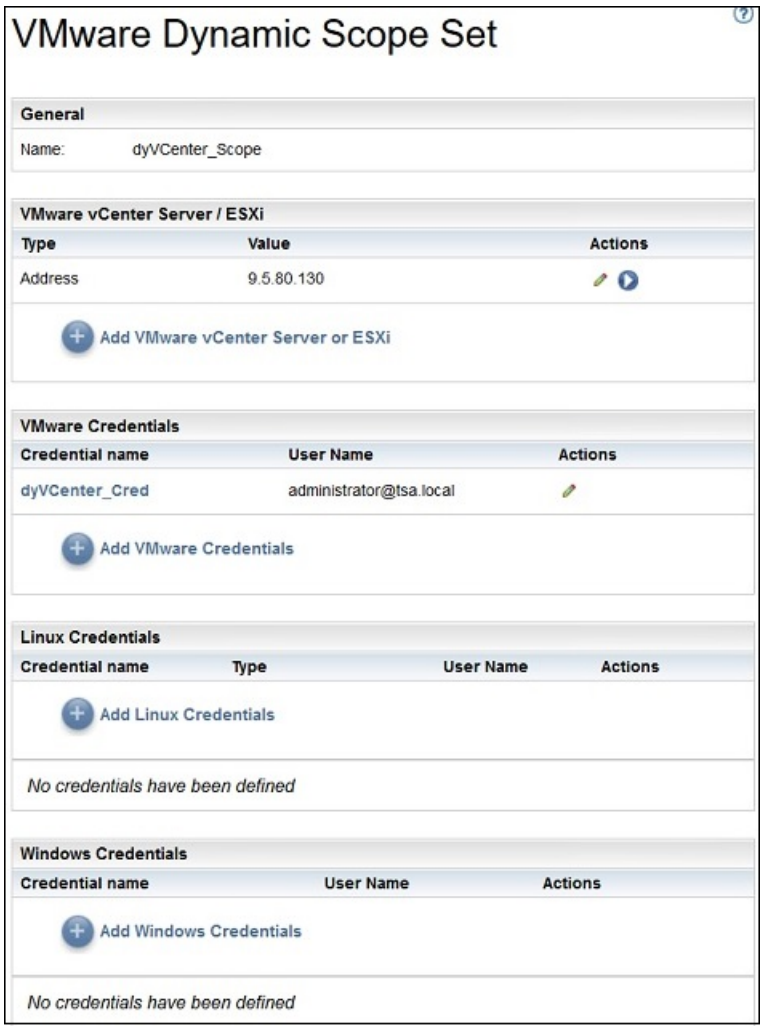

Figura 48. Ver conjunto de alcances dinámicos de VMware

El panel **VMware vCenter Server / ESXi** muestra la lista de direcciones IP de las instancias de VMware vCenter Server y ESXi que descubre el conjunto de alcances dinámicos. Los distintos paneles de credenciales como, por ejemplo, **Credenciales de Linux**, muestran las credenciales que se han configurado en el conjunto de alcances.

Adición de alcances dinámicos de VMware

Para añadir un Conjunto de alcances dinámicos de VMware, especifique la dirección IP de una instancia de ESXi o VMware vCenter Server individual junto con la credencial para acceder a la instancia de VMware. De manera opcional, puede especificar las credenciales de Linux y Windows para permitir el descubrimiento de las máquinas virtuales de los servidores x86 que gestiona la instancia de VMware. Una vez creado el Conjunto de alcances dinámicos de VMware, puede editarse para definir direcciones IP de VMware vCenter Server o ESXi adicionales. Los Conjuntos de alcances dinámicos de VMware también pueden editarse para dar soporte a varias credenciales para acceder a la instancia de VMware y varias credenciales para acceder a las máquinas virtuales.

Acerca de esta tarea

Para añadir un conjunto de alcances dinámicos de VMware, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMware**. Se mostrará la página **Alcances dinámicos de VMware**.

2. Para definir un nuevo conjunto de alcances dinámicos de VMware, pulse **Añadir alcance dinámico de VMware**.

   Se mostrará la página **Conjunto de alcances dinámicos de VMware**.

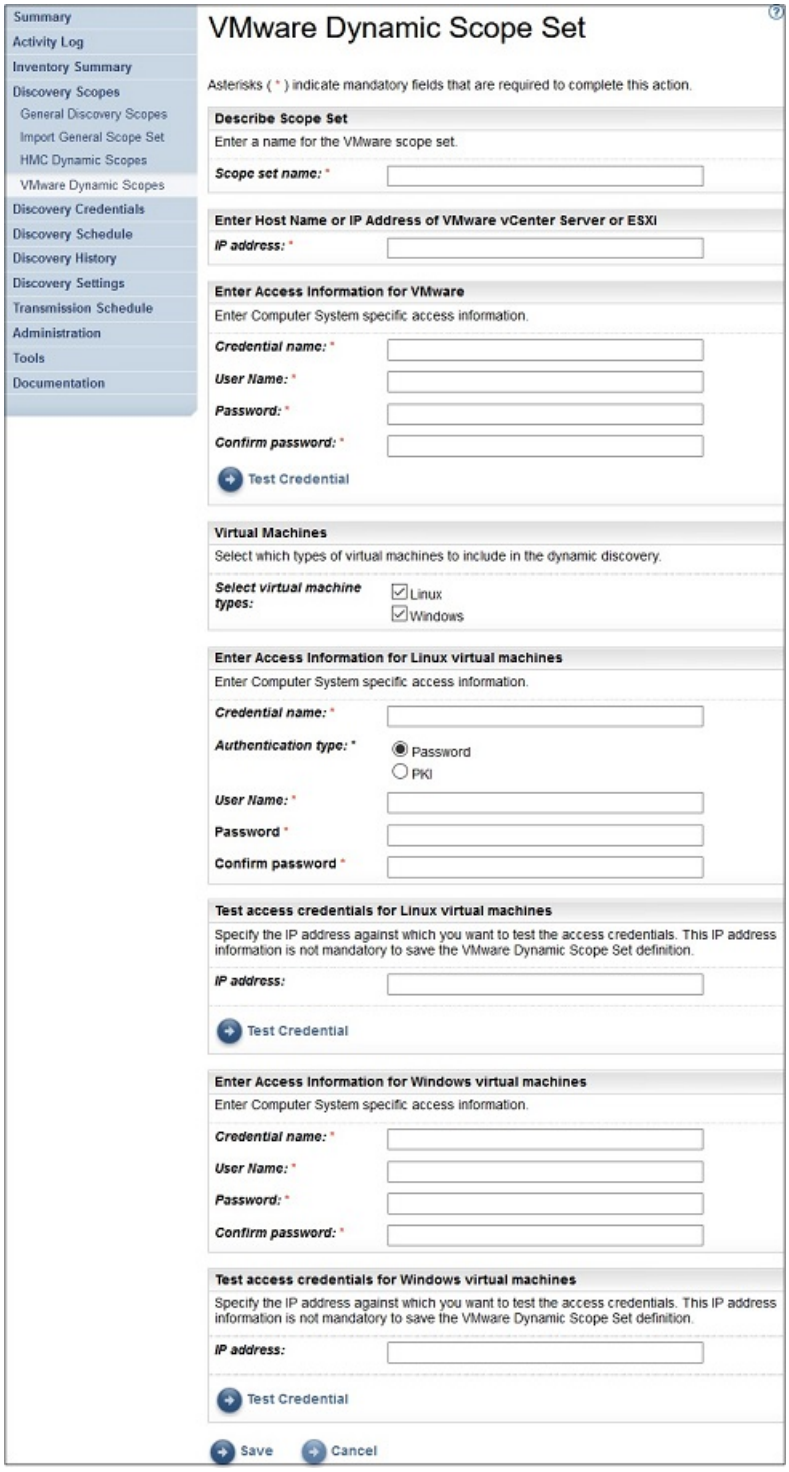

Figura 49. Añadir conjunto de alcances dinámicos de VMware

3. En el panel **Describir el conjunto de alcances**, especifique un nombre exclusivo en el campo **Nombre de conjunto de alcances**.
4. En el panel **Especificar nombre de host o dirección IP de VMware vCenter Server o ESXi**, especifique el nombre de host o la dirección IP de VMware vCenter Server o ESXi.
5. En el panel **Especificar información de acceso de VMware**, especifique los detalles siguientes:
   a) Especifique el **Nombre de credencial**.

b) Especifique el **Nombre de usuario** que se utiliza para autenticarse en la instancia de VMware vCenter Server o ESXi.

c) Introduzca la **Contraseña** y repítala en **Confirmar contraseña**

d) Opcional: Pulse **Probar credencial** para probar las credenciales de la instancia de VMware vCenter Server o ESXi de destino.

6. En el panel **Máquinas virtuales**, seleccione las máquinas virtuales (Linux, Windows) que se van a incluir en el descubrimiento dinámico.
7. Si selecciona la máquina virtual de Linux, especifique la información de acceso correspondiente.

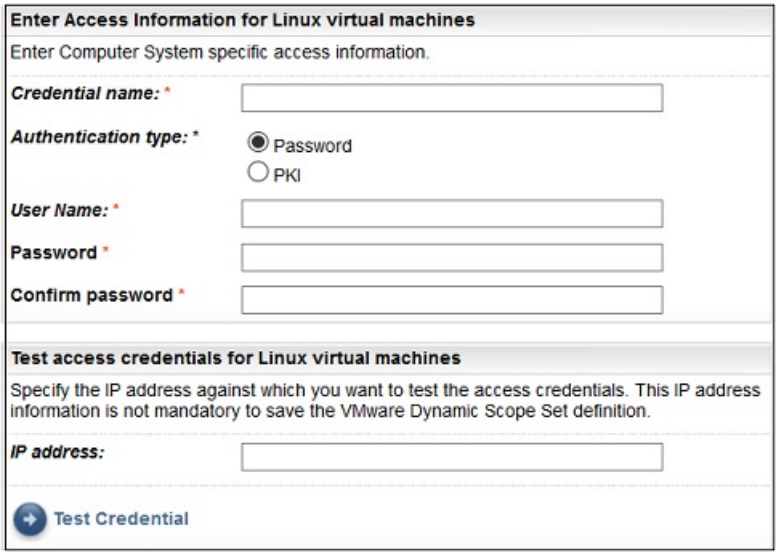

Figura 50. Especificar información de acceso de la máquina virtual de Linux

a) Especifique el **Nombre de credencial**.

b) Seleccione el **Tipo de autenticación**.

- **Contraseña** - Utiliza la contraseña proporcionada.
- **PKI** - Utiliza la clave SSH asociada al conjunto de alcances específico.

c) Especifique el **Nombre de usuario** que se utiliza para autenticarse con la máquina virtual respectiva.

d) Cuando el **Tipo de autenticación** sea **Contraseña**, especifique la **Contraseña** y repítala en **Confirmar contraseña**.

e) Cuando el **Tipo de autenticación** sea **PKI**, especifique la **Frase de contraseña** y **Confirmar frase de contraseña** si la clave SSH está cifrada. Si la clave SSH no está cifrada, deje estos dos campos en blanco.

f) Si **Tipo de autenticación** es **PKI**, pulse **Elegir archivo** y cargue la clave privada en TSA. Debe desplegar externamente la clave pública en cada máquina virtual.

g) Opcional: Especifique la **dirección IP** de la máquina virtual y pulse **Probar credencial** para probar las credenciales de la máquina virtual de destino.

8. Si selecciona la máquina virtual de Windows, especifique la información de acceso correspondiente.

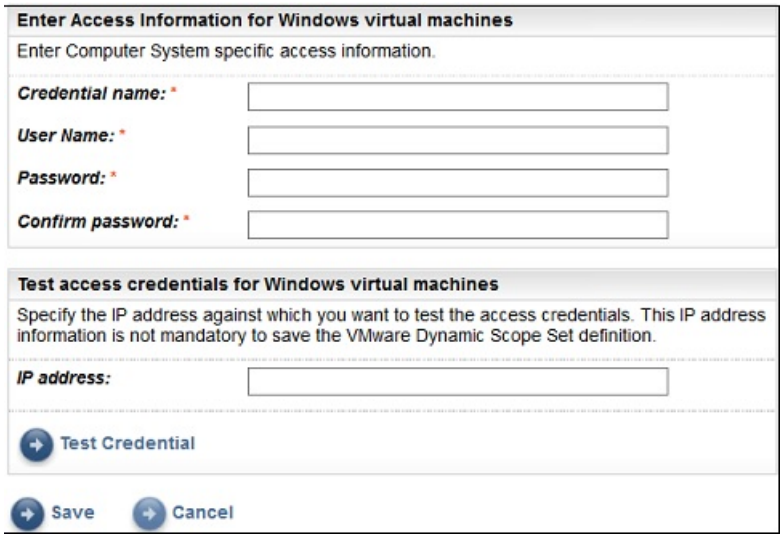

Figura 51. Especificar información de acceso de la máquina virtual de Windows

a) Especifique el **Nombre de credencial**.

b) Especifique el **Nombre de usuario** que se utiliza para autenticarse con la máquina virtual respectiva.

c) Introduzca la **Contraseña** y repítala en **Confirmar contraseña**.

d) Opcional: Especifique la **dirección IP** de la máquina virtual y pulse **Probar credencial** para probar las credenciales de la máquina virtual de destino.

9. Pulse **Guardar** para guardar el conjunto de alcances dinámicos de VMware.

Modificar alcances dinámicos de VMware - Direcciones IP de VMware vCenter Server o ESXi
Puede modificar la lista de direcciones IP de VMware vCenter Server o ESXi asociadas con un conjunto de alcances dinámicos de VMware existente.

Acerca de esta tarea
Para modificar la lista de direcciones IP de VMware vCenter Server o ESXi, siga estos pasos.

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMware**.
   Se mostrará la página **Alcances dinámicos de VMware**.
2. Para editar el conjunto de alcances, pulse el icono .
   Se mostrará la página **Conjunto de alcances dinámicos de VMware**.
   - Para añadir una dirección IP de VMware vCenter Server o ESXi al conjunto de alcances, siga estos pasos:
     a. En el panel **VMware vCenter Server / ESXi**, pulse **Añadir VMware vCenter Server o ESXi**. Se mostrará la página **Alcances dinámicos de VMware**.
     b. Especifique la **Dirección IP** de VMware vCenter Server o ESXi en el panel **Describir dirección o host**.
     c. Pulse **Guardar** para añadir la instancia de VMware vCenter Server o ESXi.
   - Para editar una dirección IP de VMware vCenter Server o ESXi existente en el conjunto de alcances, siga estos pasos:
     a. En el panel **VMware vCenter Server/ESXi**, pulse el icono . Se mostrará la página **Alcances dinámicos de VMware**.

b. Modifique la **Dirección IP** de la instancia de VMware vCenter Server o ESXi en el panel **Describir dirección o host**.

c. Pulse **Guardar**.

- Para suprimir una dirección IP de VMware vCenter Server o ESXi existente en el conjunto de alcances, siga estos pasos:

  a. En el panel **VMware vCenter Server/ESXi**, pulse el icono  .

  b. En el recuadro de diálogo, pulse **Aceptar** para confirmar la supresión.

  Nota: Un conjunto de alcances dinámicos de VMware siempre debe tener al menos una dirección IP de VMware vCenter Server o ESXi definida. TSA no permite suprimir todas las direcciones IP de VMware.

Modificar alcances dinámicos de VMware - Credenciales

Puede modificar la lista de credenciales asociadas con un conjunto de alcances dinámicos de VMware existente.

Acerca de esta tarea

Un conjunto de alcances dinámicos de VMware siempre debe tener al menos una credencial de VMware definida. TSA no permite suprimir todas las credenciales de VMware. Si no hay credenciales para Linux o Windows, TSA no recopila información detallada relacionada con ese tipo de máquina virtual.

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMware**.
   Se mostrará la página **Alcances dinámicos de VMware**.
2. Para editar el conjunto de alcances, pulse el icono  .
   Se mostrará la página **Conjunto de alcances dinámicos de VMware**.

   - Para añadir una credencial para VMware o Windows, siga estos pasos:

     a. En el panel **Credenciales** correspondiente, pulse **Añadir credenciales**. Por ejemplo, para añadir una credencial de VMware, pulse **Añadir credenciales de VMWare** en el panel **Credenciales de VMWare**. Se mostrará la página **Nuevas credenciales de descubrimiento de VMware**.

     b. Especifique el **Nombre de credencial**.

     c. Especifique el **Nombre de usuario** que se utiliza para autenticarse en las instancias de VMware vCenter Server o ESXi, o en las máquinas virtuales de Windows.

     d. Introduzca la **Contraseña** y repítala en **Confirmar contraseña**.

     e. **Opcional:** especifique la **dirección IP** de la instancia de VMware vCenter Server o ESXi, o la máquina virtual de Windows, y pulse **Probar credencial** para probar las credenciales del destino.

     f. Pulse **Guardar** para guardar la credencial correspondiente.

   - Para añadir una credencial para Linux, siga estos pasos:

     a. En el panel **Credenciales de Linux**, pulse **Añadir credenciales de Linux**. Se mostrará la página **Nuevas credenciales de descubrimiento de VMware**.

     b. Especifique el **Nombre de credencial**.

     c. Seleccione el **Tipo de autenticación**.

     – **Contraseña** - Utiliza la contraseña proporcionada.

     – **PKI** - Utiliza la clave SSH asociada al conjunto de alcances específico.

     d. Especifique el **Nombre de usuario** que se utiliza para autenticarse en las máquinas virtuales de Linux.

     e. Cuando el **Tipo de autenticación** sea **Contraseña**, especifique la **Contraseña** y repítala en **Confirmar contraseña**.

f. Cuando el **Tipo de autenticación** sea **PKI**, especifique la **Frase de contraseña** y **Confirmar frase de contraseña** si la clave SSH está cifrada. Si la clave SSH no está cifrada, deje estos dos campos en blanco.

g. Si **Tipo de autenticación** es **PKI**, pulse **Elegir archivo** y cargue la clave privada en TSA. Debe desplegar externamente la clave pública en las máquinas virtuales de Linux.

h. **Opcional:** especifique la **dirección IP** de la máquina virtual de Linux y pulse **Probar credencial** para probar las credenciales de la máquina virtual de Linux de destino.

i. Pulse **Guardar** para guardar la credencial de Linux.

- Para editar una credencial para VMware o Windows, siga estos pasos:

  a. En el panel **Credenciales** correspondiente, pulse el icono para la credencial que desee modificar. Por ejemplo, para editar una credencial de VMware, pulse en el panel **Credenciales de VMware** para la credencial que desee modificar. Se mostrará la página **Editar credenciales de descubrimiento de VMware**.

  b. En el panel **Especificar información de acceso**, puede modificar los detalles siguientes:

     1) Especifique el **Nombre de usuario** que se utiliza para autenticarse al conectarse a las instancias de VMware vCenter Server o ESXi, o las máquinas virtuales de Windows.

     2) Introduzca la **Contraseña** y repítala en **Confirmar contraseña**.

  c. **Opcional:** especifique la **dirección IP** de la instancia de VMware vCenter Server o ESXi, o la máquina virtual de Windows, y pulse **Probar credencial** para probar las credenciales del destino.

  d. Pulse **Guardar** para actualizar las modificaciones de la credencial correspondiente.

- Para editar una credencial para Linux, siga estos pasos:

  a. En el panel **Credenciales de Linux**, pulse el icono para la credencial que desee modificar. Se mostrará la página **Editar credenciales de descubrimiento de VMware**.

  b. En el panel **Especificar información de acceso**, puede modificar los detalles siguientes:

     1) Seleccione el **Tipo de autenticación**.

        – **Contraseña** - Utiliza la contraseña proporcionada.

        – **PKI** - Utiliza la clave SSH asociada al conjunto de alcances específico.

     2) Especifique el **Nombre de usuario** que se utiliza para autenticarse en la máquina virtual de Linux.

     3) Cuando el **Tipo de autenticación** sea **Contraseña**, especifique la **Contraseña** y repítala en **Confirmar contraseña**.

     4) Cuando el **Tipo de autenticación** sea **PKI**, especifique la **Frase de contraseña** y **Confirmar frase de contraseña** si la clave SSH está cifrada. Si la clave SSH no está cifrada, deje estos dos campos en blanco.

     5) Si **Tipo de autenticación** es **PKI**, pulse **Elegir archivo** y cargue la clave privada en TSA. Debe desplegar externamente la clave pública en las máquinas virtuales de Linux.

     6) **Opcional:** especifique la **dirección IP** de la máquina virtual y pulse **Probar credencial** para probar las credenciales de la máquina virtual de Linux de destino.

  c. Pulse **Guardar** para actualizar las modificaciones de la credencial correspondiente.

- Para suprimir una credencial para VMware, Linux o Windows, siga estos pasos:

  a. En el panel **Credenciales** correspondiente, pulse el icono **Suprimir** para la credencial correspondiente. Por ejemplo, para suprimir una credencial de VMware, pulse el icono en el panel **Credenciales de VMware** para la credencial que desee suprimir. Se muestra un mensaje de confirmación.

  b. Pulse **Aceptar** para suprimir la credencial correspondiente.

- Para modificar una credencial para VMware, Linux o Windows, siga estos pasos:
  a. Si hay más de una credencial para VMware Linux o Windows, puede modificarse el orden de las credenciales para las máquinas virtuales o VMware. Cuando hay una única credencial, las flechas arriba y abajo no aparecen en la columna **Acciones** para el panel de credenciales.
  b. En el panel **Credenciales** correspondiente, pulse los iconos o para reordenar la credencial correspondiente.

Habilitación o deshabilitación de conjuntos de alcances dinámicos
Puede habilitar o deshabilitar un Conjunto de alcances dinámicos de VMware.

Acerca de esta tarea

Un conjunto de alcances deshabilitado se omite durante un descubrimiento planificado.

Nota: Siempre puede realizarse un descubrimiento manual independientemente del estado del conjunto de alcances.

Deshabilitación de conjuntos de alcances dinámicos

Procedimiento

Para deshabilitar un conjunto de alcances dinámicos de VMware, siga estos pasos:
1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMware**. Se mostrará la página **Alcances dinámicos de VMware**.
2. Pulse el icono **Habilitar** junto al conjunto de alcances que desee deshabilitar.

Habilitación de conjuntos de alcances dinámicos

Procedimiento

Para habilitar un conjunto de alcances dinámicos de VMware, siga estos pasos:
1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMware**. Se mostrará la página **Alcances dinámicos de VMware**.
2. Pulse el icono **Deshabilitar** junto al conjunto de alcances que desee habilitar.

Descubrimiento de un VMware vCenter o ESXi
Puede iniciar manualmente un descubrimiento de un VMware vCenter Server o ESXi individual en un conjunto de alcances dinámicos de VMware. El descubrimiento recopila información sobre la instancia de VMware junto con las máquinas virtuales asociadas.

Procedimiento

Para iniciar manualmente un descubrimiento de un VMware vCenter Server o ESXi, siga estos pasos:
1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMware**. Se mostrará la página **Alcances dinámicos de VMware**.
2. Pulse el icono para el Conjunto de alcances dinámicos de VMware necesario. Se mostrará la página **Conjunto de alcances dinámicos de VMware**.
3. Pulse el icono al lado de la dirección IP de VMware vCenter Server o ESXi que desee descubrir.

Descubrimiento de conjuntos de alcances dinámicos
Puede iniciar manualmente un descubrimiento de un Conjunto de alcances dinámicos de VMware. El descubrimiento recopila información sobre las instancias de VMware vCenter Server o ESXi definidas en el conjunto de alcances junto con las máquinas virtuales asociadas.

Procedimiento

Para iniciar manualmente un descubrimiento de un Conjunto de alcances dinámicos de VMware, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMware**.
   Se mostrará la página **Alcances dinámicos de VMware**.
2. Pulse el icono **Ejecutar** junto al conjunto de alcances que desee descubrir.

Supresión de alcances dinámicos de VMware

Puede suprimir un conjunto de alcances dinámicos de VMware.

Procedimiento

Para suprimir un conjunto de alcances dinámicos de VMware, siga estos pasos:

1. En el panel de navegación, pulse **Alcances dinámicos de VMware**.
   Se mostrará la página **Alcances dinámicos de VMware**.
2. Pulse en el icono **Suprimir** junto al conjunto de alcances que desee suprimir.
3. Pulse **Aceptar** para confirmar que desea suprimir el conjunto de alcances dinámicos de VMware.

   Nota: Cuando confirma la supresión del conjunto de alcances dinámicos de VMware, también se suprime la información de acceso correspondiente para las máquinas virtuales de Linux o Windows.

Alcances de descubrimiento general

El proceso de descubrimiento busca elementos de TI dentro de la infraestructura. Un alcance de descubrimiento define una única dirección IP o un rango de IP que se descubren durante el proceso de descubrimiento. Los alcances de descubrimiento se agrupan en conjuntos de alcances denominados por el usuario.

Visualizar alcances de descubrimiento y conjuntos de alcances

Puede visualizar los alcances de descubrimiento y los conjuntos de alcances existentes.

Acerca de esta tarea

Para visualizar los conjuntos de alcances de descubrimiento, pulse **Alcances de descubrimiento** > **Alcances de descubrimiento general** en el panel de navegación. Se mostrará la página **Alcances de descubrimiento general**. El panel **Alcances de descubrimiento general** contiene una lista de conjuntos de alcances.

Para visualizar los alcances que contiene un conjunto de alcances, pulse en el conjunto de alcances. Se mostrará la página **Conjunto de alcances de descubrimiento**.

- El panel **General** muestra el nombre del conjunto de alcances.
- El panel **Recuento de direcciones IP** muestra el número total de direcciones IP en el conjunto de alcances específico.
- En el panel **Alcances** se muestra información detallada sobre los alcances del conjunto de alcances.

Añadir alcances de descubrimiento

Puede añadir un conjunto de alcances y un nuevo alcance a este conjunto, añadir un alcance a un conjunto de alcances o mover alcances a otros conjuntos de alcances. Para añadir un alcance, especifique una dirección IP válida, un rango de direcciones IP, una red o una sub red.

Acerca de esta tarea

Sugerencias: A continuación se indican algunas consideraciones prácticas para configurar los alcances de descubrimiento y los conjuntos de alcances.

- Como más direcciones IP haya en el alcance de descubrimiento, más dura el descubrimiento. Puede modificar el tamaño del descubrimiento deshabilitando o habilitando conjuntos de alcances o excluyendo direcciones IP, rangos de direcciones IP, redes o subredes de un alcance dentro de un conjunto de alcances.

  Para minimizar el tiempo que dura un descubrimiento, configure alcances de descubrimiento de forma que apunten solo a los elementos que desea descubrir y deshabilite conjuntos de alcances o excluya las direcciones IP, los rangos de direcciones IP, las redes o las subredes,que no desea o no necesita descubrir.

  Nota: Para optimizar el rendimiento, limite el número acumulativo de direcciones IP de un conjunto de alcances a 400 o menos. Para obtener información sobre cómo importar un conjunto de alcances, consulte la sección “Importar un conjunto de alcances” en la página 71
- No todos los elementos son iguales. Por ejemplo, un direccionador con docenas de interfaces puede tardar más en hacer un descubrimiento completo que un solo host.
- Si utiliza la autenticación PKI para el descubrimiento de dispositivos, solo se puede asociar una clave SSH a cada conjunto de alcances.

Para obtener más información sobre las mejores prácticas para configurar los alcances de descubrimiento, consulte la Guía del asistente de configuración de TSA.

Para añadir un conjunto de alcances y un alcance, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances de descubrimiento general**.

   Se mostrará la página **Alcances de descubrimiento general**.
2. Para definir un nuevo conjunto de alcances de descubrimiento, pulse **Añadir nuevo conjunto de alcances**.

   Se mostrará la página **Conjunto de alcances de descubrimiento**.

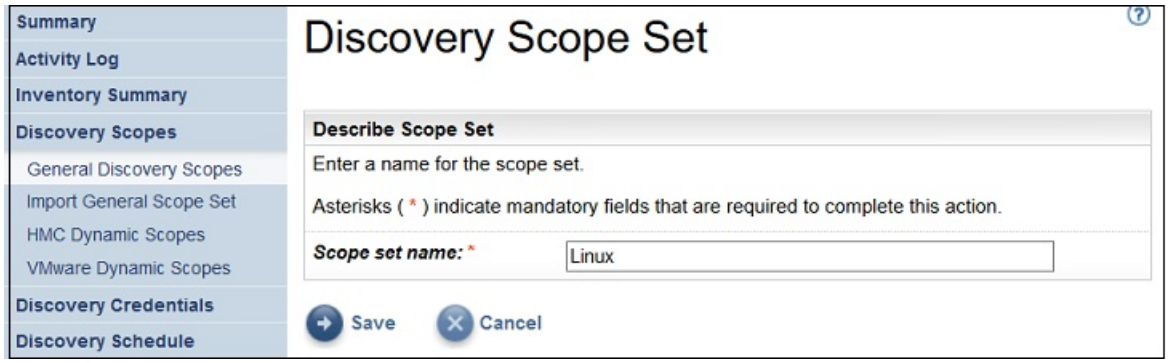

Figura 52. Conjunto de alcances de descubrimiento

   a) Especifique un nombre de conjunto de alcances exclusivo en el campo de nombre de **Conjunto de alcances**.

   b) Pulse **Guardar**.

      Se crea el nuevo conjunto de alcances y se visualiza la página **Alcances de descubrimiento general**.

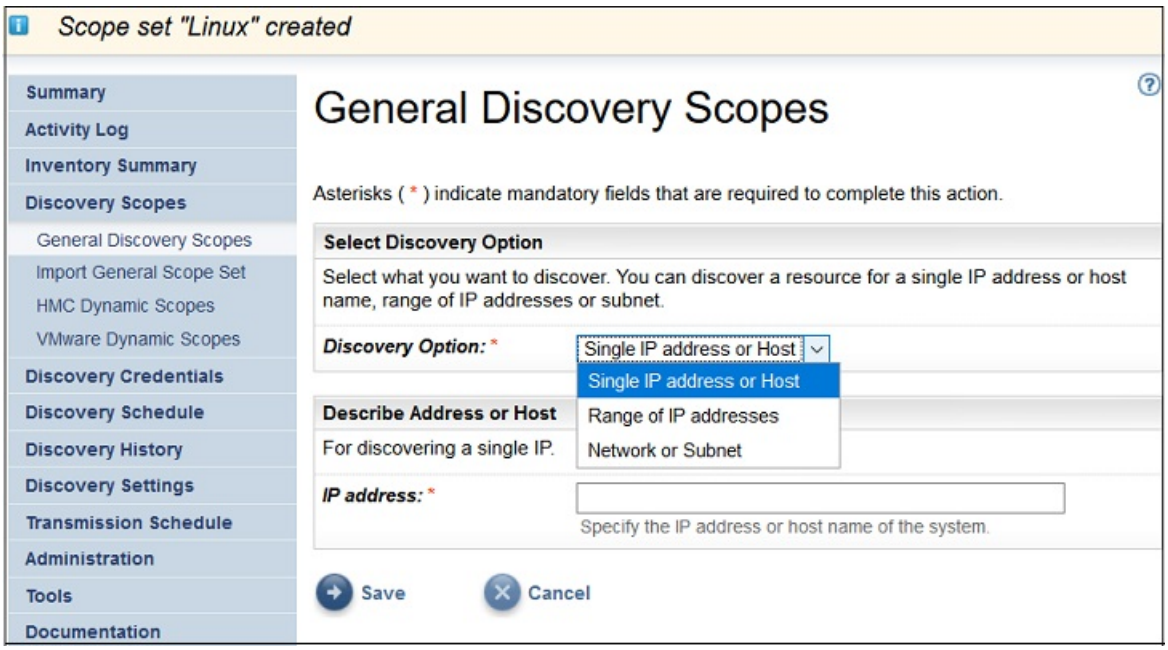

Figura 53. Alcances de descubrimiento general

3. Especifique una de las siguientes opciones en el panel **Seleccionar opción de descubrimiento**:
   - `Una sola dirección IP o host`

     En **Describir dirección o host**, especifique la dirección IP o el nombre de host.
   - `Rango de direcciones IP`

     En **Describir rango de direcciones**, especifique la dirección IP inicial, la dirección IP final y, opcionalmente, una descripción en los campos proporcionados.
   - `Red o subred`

     En **Describir red o subred**, especifique la dirección IP, la máscara y, opcionalmente, una descripción en los campos proporcionados.
4. Si desea excluir hosts, direcciones IP, un rango de direcciones IP o subredes del descubrimiento, pulse **Añadir exclusión** y siga estos pasos:
   a) Seleccione **Host**, **Rango** o **Subred**.
   b) Especifique la dirección IP, el rango de direcciones IP o la subred que desee excluir del descubrimiento.
   c) Opcional: Especifique una descripción de la dirección IP, el rango de direcciones IP o la subred que va a excluir del descubrimiento.

      Nota: Las exclusiones solo son aplicables para un alcance definido con un rango de direcciones IP o una subred.

      Nota: No se puede reutilizar una dirección IP, un rango de direcciones IP, una subred ni una descripción en ningún alcance ni en ninguna exclusión dentro de un conjunto de alcances.
   d) Para añadir más exclusiones, pulse **Añadir exclusión** y siga los pasos anteriores para definir más exclusiones.
5. Pulse **Guardar** para guardar el alcance y las exclusiones. Se muestra la página **Conjunto de alcances de descubrimiento** con el nuevo alcance en la lista.
6. Para añadir más alcances a este conjunto de alcances, pulse **Añadir nuevo alcance** y siga los pasos anteriores para definir más alcances.

   Nota: Para optimizar el rendimiento, limite el número acumulativo de direcciones IP de un conjunto de alcances a 400 o menos.

Añadir un alcance de descubrimiento a un conjunto de alcances existente
Puede añadir un alcance a un conjunto de alcances existente.

Procedimiento

Para añadir un alcance a un conjunto de alcances existente, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances de descubrimiento general**.

   Se mostrará la página **Alcances de descubrimiento general**.
2. En el panel **Alcances de descubrimiento general**, pulse el conjunto de alcances al que desea añadir un alcance.

   Se mostrará la página **Conjunto de alcances de descubrimiento**.
3. Pulse **Añadir nuevo alcance**.

   Se mostrará la página **Alcances de descubrimiento general**.
4. En el panel **Seleccionar opción de descubrimiento**, especifique una de las siguientes opciones.
   - `Una sola dirección IP o host`

     En **Describir dirección o host**, especifique la dirección IP o el nombre de host.
   - `Rango de direcciones IP`

     En **Describir rango de direcciones**, especifique la dirección IP inicial, la dirección IP final y, opcionalmente, una descripción en los campos proporcionados.
   - `Red o subred`

     En **Describir red o subred**, especifique la dirección IP, la máscara y, opcionalmente, una descripción en los campos proporcionados.
5. Si desea excluir hosts, direcciones IP, un rango de direcciones IP o subredes del descubrimiento, pulse **Añadir exclusión** y siga estos pasos:
   a) Seleccione **Host**, **Rango** o **Subred**.
   b) Especifique la dirección IP, el rango de direcciones IP o la subred que desee excluir del descubrimiento.
   c) Opcional: Especifique una descripción de la dirección IP, el rango de direcciones IP o la subred que va a excluir del descubrimiento.

      Nota: Las exclusiones solo son aplicables para un alcance definido con un rango de direcciones IP o una subred.

      Nota: No se puede reutilizar una dirección IP, un rango de direcciones IP, una subred ni una descripción en ningún alcance ni en ninguna exclusión dentro de un conjunto de alcances.
   d) Para añadir más exclusiones, pulse **Añadir exclusión** y siga los pasos anteriores para definir más exclusiones.
6. Pulse **Guardar** para guardar el alcance y las exclusiones.

   Se muestra la página **Conjunto de alcances de descubrimiento** con el nuevo alcance en la lista.

Modificar un conjunto de alcances de descubrimiento
Puede modificar un conjunto de alcances de descubrimiento cambiando los valores del conjunto de alcances.

Acerca de esta tarea
Para modificar un conjunto de alcances de descubrimiento existente, siga estos pasos.

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances de descubrimiento general**.

Se mostrará la página **Alcances de descubrimiento general**.

2. Para editar el conjunto de alcances, pulse en el icono **Editar** junto al conjunto de alcances.

   Se mostrará la página **Conjunto de alcances de descubrimiento**. Puede editar el conjunto de alcances editando un alcance, añadiendo un alcance, moviendo un alcance a otro conjunto de alcances o suprimiendo un alcance.

   - Para añadir un alcance, siga estos pasos:
     a. Pulse **Añadir nuevo alcance**.
     b. En el panel **Seleccionar opción de descubrimiento**, especifique una de las siguientes opciones:
        – `Una sola dirección IP / host`

          En **Describir dirección o host**, escriba la dirección IP o el nombre de host.
        – `Rango de direcciones IP`

          En **Describir rango de direcciones**, especifique la dirección IP inicial, la dirección IP final y, opcionalmente, una descripción en los campos proporcionados.
        – `Red o subred`

          En **Describir red o subred**, especifique la dirección IP, la máscara y, opcionalmente, una descripción en los campos proporcionados.

        Nota: Proporcione un nombre exclusivo en **Descripción**. Si especifica una descripción que ya existe para algún otro alcance dentro de este conjunto de alcances, TSA no le permitirá crear el nuevo alcance. Si el campo **Descripción** está en blanco, TSA crea automáticamente la descripción utilizando el rango de direcciones IP / la máscara de subred.
     c. Si desea excluir hosts, direcciones IP o subredes del descubrimiento, pulse **Añadir exclusión** y siga estos pasos:
        1) Seleccione **Host**, **Rango** o **Subred**.
        2) Especifique la dirección IP, el rango de direcciones IP o la subred que desee excluir del descubrimiento.
        3) Para añadir más exclusiones, pulse **Añadir exclusión** y siga los pasos anteriores para definir más exclusiones.
     d. Pulse **Guardar** para guardar el alcance y las exclusiones. Se muestra la página **Conjunto de alcances de descubrimiento** con el nuevo alcance en la lista.
   - Para mover un alcance a otro conjunto de alcances, siga estos pasos:
     a. Pulse **Mover alcances**.
     b. En la página **Mover alcances de un conjunto a otro**, seleccione los alcances que desea mover en la lista **Alcances**.
     c. En la lista **Conjunto de alcances de destino** seleccione el conjunto de alcances al que desea mover los alcances.
     d. Pulse **Mover**.
   - Para editar un alcance, siga estos pasos:
     a. Pulse el icono **Editar** de un alcance.
     b. Puede modificar la **Opción de descubrimiento**, las **Direcciones IP**, las **Exclusiones**, etc.
     c. Pulse **Guardar** para guardar el alcance y las exclusiones. Se muestra la página **Conjunto de alcances de descubrimiento** con el nuevo alcance en la lista.
   - Para suprimir un alcance, siga estos pasos:
     a. Pulse en el icono **Suprimir** junto al alcance que desee suprimir.
     b. Pulse **Aceptar** para confirmar que desea suprimir el alcance de descubrimiento.

Suprimir alcances de descubrimiento
Puede suprimir alcances de descubrimiento existentes dentro de un conjunto de alcances, o suprimir conjuntos de alcances enteros.

Acerca de esta tarea

Procedimiento

Para suprimir un alcance de descubrimiento, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances de descubrimiento general**.
   Se mostrará la página **Alcances de descubrimiento general**.
2. Edite el conjunto de alcances que contiene el alcance de descubrimiento que desea suprimir pulsando en el icono **Editar** junto al conjunto de alcances.
   Se mostrará la página **Conjunto de alcances de descubrimiento**.
3. Pulse en el icono **Suprimir** junto al alcance que desee suprimir.
4. Pulse **Aceptar** para confirmar que desea suprimir el alcance de descubrimiento.

Suprimir conjuntos de alcances de descubrimiento
Puede suprimir conjuntos de alcances de descubrimiento existentes.

Procedimiento

Nota: Para poder suprimir un conjunto de alcances, debe suprimir todas las credenciales asociadas al conjunto de alcances.

Para suprimir un conjunto de alcances de descubrimiento, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances de descubrimiento general**.
   Se mostrará la página **Alcances de descubrimiento general**.
2. Pulse en el icono **Suprimir** junto al conjunto de alcances que desee suprimir.
3. Pulse **Aceptar** para confirmar que desea suprimir el conjunto de alcances de descubrimiento.

Importar un conjunto de alcances

Puede importar una lista de direcciones IP para definir un nuevo conjunto de alcances.

Acerca de esta tarea
Se crea un nuevo conjunto de alcances basado en el nombre especificado y la lista de direcciones IP del archivo de entrada. TSA lleva a cabo las siguientes validaciones cuando se importa un conjunto de alcances:

- Comprueba si el nombre del conjunto de alcances ya existe.
- Valida cada línea del archivo para comprobar si es una dirección IP válida.
- Ignora los espacios en blanco iniciales y finales al validar cada dirección IP.
- Ignora las direcciones IP duplicadas.

Procedimiento

Para importar las direcciones IP, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Importar conjunto de alcances general**.
   Se mostrará la página **Importar conjunto de alcances general**.
2. Especifique el **Nombre del nuevo conjunto de alcances**.

Nota: Especifique un nombre exclusivo que no esté utilizado por ninguno de los conjuntos de alcances existentes. Si se especifica un nombre de conjunto de alcances que ya existe, se muestra un mensaje de error: `El nombre del conjunto de alcances ya existe`.

3. Pulse **Elegir archivo** para seleccionar el archivo de texto.

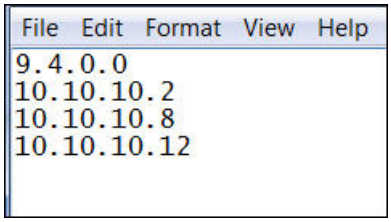

Figura 54. Importar conjunto de alcances

Nota: El archivo de texto debe formatearse como una sola columna, donde cada fila contenga una sola dirección IP y ningún otro dato.

4. Pulse **Importar archivo de conjunto de alcances** para importar el conjunto de alcances. Cuando la importación se completa satisfactoriamente, se muestra un mensaje de estado: **`El conjunto de alcances se ha importado satisfactoriamente`**.

   Nota: Si el archivo de conjunto de alcances tiene más de 400 direcciones IP, se muestra un mensaje de aviso: **`El conjunto de alcances se ha importado satisfactoriamente. Pero el número de elementos de alcance supera las directrices recomendadas, limítelo a 400 para obtener un mejor rendimiento.`**

5. Tras importar el conjunto de alcances, podrá editar el conjunto de alcances en la sección **Alcances de descubrimiento general** de la interfaz de usuario y asociar las credenciales en la sección **Credenciales de descubrimiento**.

Configuración de descubrimiento

Utilice la página **Configuración de descubrimiento** para ajustar los Valores de descubrimiento avanzados.

Configurar los valores de conexión

Utilice la página **Configuración de conexión** para configurar el Descubrimiento SLP y descubrir dispositivos de almacenamiento EMC a través de proveedores SMI-S de EMC.

Acerca de esta tarea

De forma predeterminada, un trabajo de descubrimiento intenta encontrar proveedores SMI-S de EMC ejecutando una consulta SLP para determinar su dirección IP y su puerto. Si SLP no está disponible en su red, (por ejemplo, si existen algunas políticas de seguridad que bloquean los mensajes SLP) todavía se puede llevar a cabo el descubrimiento de dispositivos de almacenamiento EMC deshabilitando el descubrimiento SLP y configurando los puertos en los que el proveedor SMI-S de EMC está a la escucha de solicitudes de consulta.

Procedimiento

1. Seleccione **Habilitar** o **Deshabilitar** para habilitar o deshabilitar el Descubrimiento SLP.

   Nota: De forma predeterminada, el descubrimiento SLP está habilitado.

2. Si deshabilita el descubrimiento SLP, debe definir uno o más puertos de conexión para el proveedor SMI-S de EMC

   a) **Puerto(s) HTTPS de SMI-S de EMC:** 5989 es el puerto HTTPS predeterminado en el que el proveedor SMI-S de EMC está a la escucha de solicitudes de consulta. Si especifica varios puertos,

sepárelos por comas. El SMI-S de EMC está a la escucha, en estos puertos, de solicitudes de conexión (como por ejemplo de TSA). TSA necesita saber ese puerto para iniciar la conexión.

b) **Puerto(s) HTTP de SMI-S de EMC:** 5988 es el puerto HTTP predeterminado en el que el proveedor SMI-S de EMC está a la escucha de solicitudes de consulta. TSA primero intenta una conexión HTTPS (si está configurada) y, si falla, intenta conectarse a través de los puertos HTTP que hay definidos. Si desea evitar las conexiones HTTP, no defina puertos HTTP. Si especifica varios puertos HTTP, sepárelos por comas. El SMI-S de EMC está a la escucha, en estos puertos, de solicitudes de conexión (como por ejemplo de TSA). TSA necesita saber ese puerto para iniciar la conexión.

3. Pulse **Guardar** para guardar la configuración de conexión. Obtendrá el mensaje - *La configuración de conexión de descubrimiento se ha guardado satisfactoriamente.*

Credenciales de descubrimiento

Las Credenciales de descubrimiento son los nombres de usuario, contraseñas o claves SSH, y las cadenas de comunidad SNMP (Simple Network Management Protocol) que TSA utiliza para acceder a los recursos que se configuran en **Alcances de descubrimiento general** durante el descubrimiento.

Ver las credenciales

El proceso de descubrimiento requiere credenciales, como por ejemplo ID de usuario y contraseñas, para acceder a los recursos.

Acerca de esta tarea

Importante: La información de acceso que especifique debe coincidir con la información de acceso del recurso de descubrimiento de destino. Si cambia la información de acceso, como por ejemplo una contraseña, en el recurso de destino, asegúrese de cambiar también la información de acceso del Technical Support Appliance asociado.

Puede visualizar las credenciales existentes pulsando **Credenciales de descubrimiento** en el panel de navegación. Aparece la página **Credenciales de descubrimiento**.

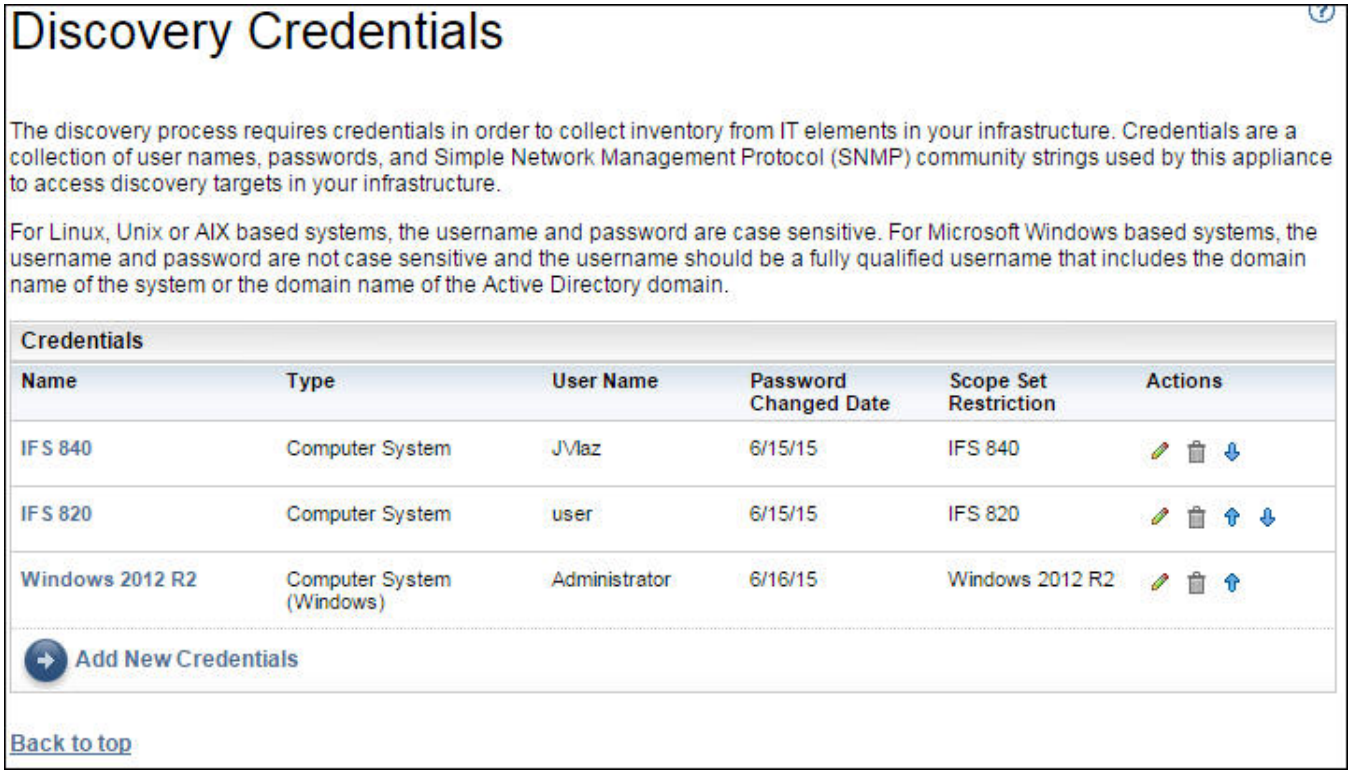

Figura 55. Nuevas credenciales de descubrimiento

Ver información detallada de credenciales

Puede ver información detallada sobre una credencial de descubrimiento específica.

Acerca de esta tarea

Para ver la información detallada de una credencial, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Credenciales de descubrimiento**.
   Se abre la página**Credenciales de descubrimiento** con una lista de todas las credenciales existentes.
2. Para ver la información detallada de una credencial específica, pulse en el nombre de la credencial.
   Se abre la página**Credenciales de descubrimiento** con información de la credencial seleccionada.

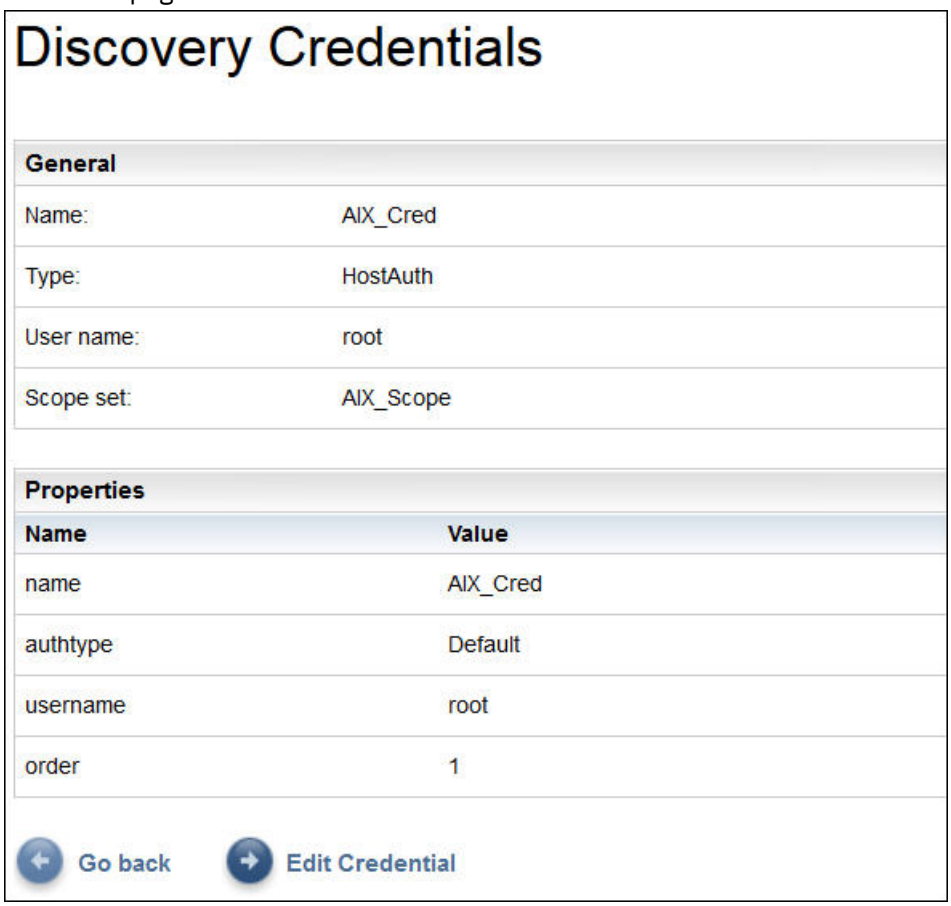

Figura 56. Detalles de credencial de descubrimiento

Tareas relacionadas

Modificar credenciales
Puede modificar las credenciales existentes para proporcionar control de acceso en el proceso de descubrimiento.

Añadir credenciales

Puede añadir credenciales para proporcionar control de acceso en el proceso de descubrimiento.

Acerca de esta tarea

Para añadir credenciales, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Credenciales de descubrimiento**.

Aparece la página **Credenciales de descubrimiento**.

2. Para crear una credencial, pulse **Añadir nuevas credenciales**.

   Se mostrará la página **Nuevas credenciales de descubrimiento**.

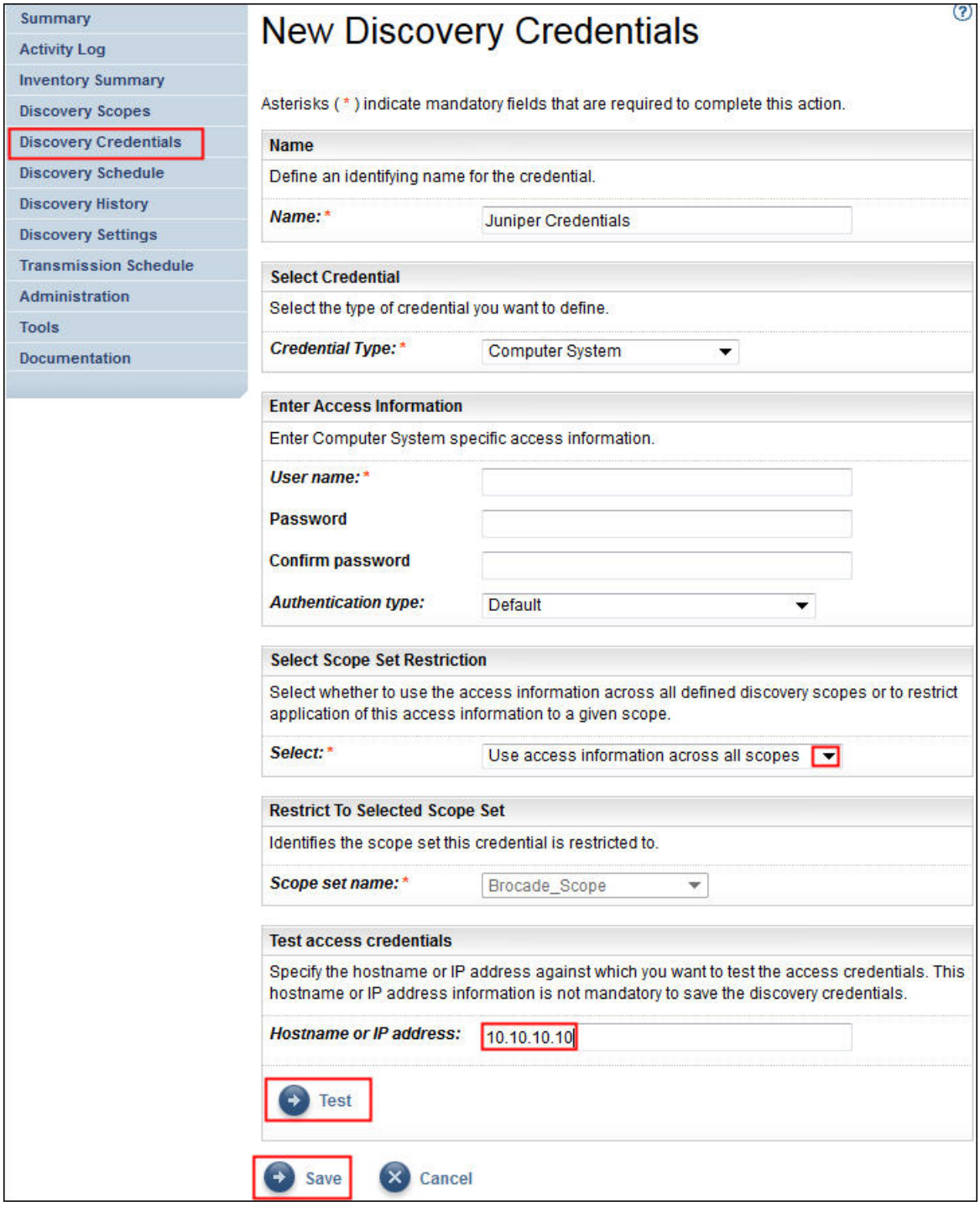

Figura 57. Nuevas credenciales de descubrimiento

a) En el campo **Nombre**, escriba un nombre identificativo para la credencial.

b) En la lista desplegable **Tipo de credencial** , seleccione el tipo de credencial que desea crear.

c) En el panel **Especificar información de acceso**, especifique la información necesaria según el tipo de credencial que ha seleccionado.

La información necesaria depende del tipo de credencial. Para obtener información sobre la información de acceso que se necesita para cada tipo de credencial, consulte “Requisitos de credenciales y de software para el entorno de descubrimiento ” en la página 6.

Importante: La información de acceso que especifique debe coincidir con la información de acceso del recurso de descubrimiento de destino. Si cambia la información de acceso del recurso de destino, asegúrese de cambiar también la información de acceso del TSA asociado. Para obtener más información, consulte la Guía del asistente de configuración de IBM Technical Support Appliance.

Consejo: En la página **Credenciales de descubrimiento** se muestra la última vez que se ha cambiado la contraseña. Si cambia regularmente la contraseña en el recurso de destino, puede utilizar esta información para asegurarse de que también cambia la contraseña en TSA para que coincida con la nueva contraseña del recurso de destino. Para obtener información sobre cómo visualizar las credenciales de descubrimiento, consulte “Ver las credenciales” en la página 73.

d) El panel **Seleccionar Restricción de conjunto de alcances** se utiliza para especificar si una credencial está limitada a un único conjunto de alcances o si se aplica a todos los conjuntos de alcances. Si **Tipo de credencial** es **Sistema informático** y el **Tipo de autenticación** es **PKI**, este panel no se visualiza. Las credenciales de PKI deben tener siempre como alcance un único conjunto de alcances.

Consejo: Crear credenciales de descubrimiento restringidas a un conjunto de alcances específico puede mejorar el rendimiento al reducir el número de credenciales que se prueban para los recursos que se están descubriendo.

e) El panel **Restringir al conjunto de alcances seleccionado** se utiliza para limitar una credencial a un único conjunto de alcances. Este panel está visible en una de estas dos condiciones.

- El panel **Seleccionar Restricción de conjunto de alcances** tiene seleccionado **Limitar la información de acceso al alcance especificado**, o bien
- **Tipo de credencial** es **Sistema informático** y el **Tipo de autenticación** es **PKI**.

La credencial solo se utiliza para descubrir el conjunto de alcances seleccionado. Al ejecutar un descubrimiento con un conjunto de alcances distinto, la credencial no se utiliza. Este método impide los intentos de inicio de sesión no válidos que pueden provocar que se bloquee el acceso del usuario a la cuenta.

f) Si el tipo de credencial es **Sistema informático**, **Sistema informático (Windows)**, **SNMP** o **SNMPV3**, puede verificar si las credenciales son correctas. La función **Probar** del tipo de credencial **Sistema** admite los siguientes dispositivos:

- Dispositivos que utilizan autenticación basada en SSH o en Telnet
- XIV
- DS6000 y DS8000
- VMware ESXi
- VMware vCenter Server
- EMC CLARiiON / VNX / VMAX vía EMC SMI-S
- IBM TS3100 / TS3200
- IBM TS3310
- IBM TS3500
- IBM TS4500
- IBM TS7700
- IBM DS3000, DS4000 y DS5000 si están protegidos mediante contraseña
- Windows
- Palo Alto Networks (PAN-OS)

Para probar las credenciales, especifique una dirección IP o un nombre de host del dispositivo de destino con el que desea probar las credenciales y pulse **Probar**.

Nota:

- El nombre de host que especifique no puede contener ningún guión bajo ("_").
- Para ejecutar un descubrimiento o probar credenciales en sistemas con los sistemas operativos Linux, AIX, IBM i, o HP-UX, habilite SSH.

g) Pulse **Guardar**.

En la página **Credenciales de descubrimiento** se muestra la nueva credencial.

Nota: Se recomienda hacer una copia de seguridad de la configuración de TSA al crear o modificar credenciales de descubrimiento.

3. Para cambiar el orden en que TSA utiliza una credencial para acceder a un recurso, pulse en el icono **Flecha arriba** o en el icono **Flecha abajo** junto a la credencial para desplazarla hacia arriba o hacia abajo en la lista.

Para obtener información sobre cómo se utiliza el orden, consulte "Credenciales de descubrimiento" en la página 2.

Se volverá a mostrar la página con la lista de **Credenciales de descubrimiento** con el nuevo orden.

Modificar credenciales

Puede modificar las credenciales existentes para proporcionar control de acceso en el proceso de descubrimiento.

Acerca de esta tarea

Para modificar credenciales, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Credenciales de descubrimiento**.

Se abre la página**Credenciales de descubrimiento** con una lista de todas las credenciales existentes.

2. Para editar una credencial, pulse en el icono **Editar** junto a la credencial.

Se mostrará la página **Editar credenciales de descubrimiento**.

a) En el panel **Modificar la información de acceso**, puede cambiar la información de acceso de esta credencial.

Importante: La información de acceso que especifique debe coincidir con la información de acceso del recurso de descubrimiento de destino. Si cambia la información de acceso del recurso de destino, asegúrese de cambiar también la información de acceso del TSA asociado. Para obtener más información, consulte la Guía del asistente de configuración de IBM Technical Support Appliance.

Consejo: En la página **Credenciales de descubrimiento** se muestra la última vez que se ha cambiado la contraseña. Si cambia regularmente la contraseña en el recurso de destino, puede utilizar esta información para asegurarse de que también cambia la contraseña en TSA para que coincida con la nueva contraseña del recurso de destino. Para obtener información sobre cómo visualizar las credenciales de descubrimiento, consulte "Ver las credenciales" en la página 73.

b) El panel **Seleccionar Restricción de conjunto de alcances** se utiliza para especificar si una credencial está limitada a un único conjunto de alcances o si se aplica a todos los conjuntos de alcances. Si el **Tipo de credencial** es **Sistema informático** y el **Tipo de autenticación** es **PKI**, este panel no se visualiza. Las credenciales de PKI deben tener siempre como alcance un único conjunto de alcances.

Consejo: Crear credenciales de descubrimiento restringidas a un conjunto de alcances específico puede mejorar el rendimiento al reducir el número de credenciales que se probarán para los recursos que se descubran.

c) El panel **Restringir al conjunto de alcances seleccionado** se utiliza para limitar una credencial a un único conjunto de alcances. Este panel está visible en una de estas dos condiciones:

- El panel **Seleccionar Restricción de conjunto de alcances** tiene seleccionado **Limitar la información de acceso al alcance especificado**, o bien
- **Tipo de credencial** es **Sistema informático** y el **Tipo de autenticación** es **PKI**.

La credencial solo se utilizará cuando se descubra el conjunto de alcances seleccionado. Esta credencial no se utilizará con ningún otro conjunto de alcances. Este método impide los intentos de inicio de sesión no válidos que pueden provocar que se bloquee el acceso del usuario a la cuenta.

d) Si el tipo de credencial es **Sistema informático**, **Sistema informático (Windows)**, **SNMP** o **SNMPV3**, puede verificar si las credenciales son correctas. Para probar las credenciales, especifique una dirección IP o un nombre de host del destino con el que desea probar las credenciales y pulse **Probar**.

Nota: El nombre de host que especifique no puede contener ningún guión bajo ("_").

e) Pulse **Guardar**.

En la página **Credenciales de descubrimiento** se muestra la credencial modificada.

3. Para cambiar el orden de prioridades en que TSA utiliza una credencial para acceder a un recurso, pulse en el icono **Flecha arriba** o en el icono **Flecha abajo** junto a la credencial para desplazarla hacia arriba o hacia abajo en la lista.

   Para obtener información sobre cómo se utiliza el orden, consulte "Credenciales de descubrimiento" en la página 2.

   Se volverá a mostrar la página con la lista de **Credenciales de descubrimiento** con el nuevo orden.

Conceptos relacionados

Credenciales de descubrimiento
Las Credenciales de descubrimiento son una colección de nombres de usuario, contraseñas o claves SSH, y cadenas de comunidad SNMP (Simple Network Management Protocol) que TSA utiliza para acceder a los recursos durante el descubrimiento.

Requisitos de credenciales y de software para el entorno de descubrimiento
Para descubrir puntos finales o recursos en su entorno, TSA debe tener acceso a esos recursos. Se recomienda crear una cuenta de servicio en cada recurso que sea específicamente para utilizar con TSA para acceder a ese recurso.

Suprimir credenciales

Puede suprimir las credenciales que TSA utiliza al acceder a los recursos.

Acerca de esta tarea

Para suprimir una credencial, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Credenciales de descubrimiento**.
   Aparece la página **Credenciales de descubrimiento**.
2. Pulse en el icono **Suprimir** junto a la credencial que desea suprimir.
3. Pulse **Aceptar** para confirmar que desea suprimir la credencial.

Planificación de descubrimiento

Se planifican descubrimientos para garantizar que los datos descubiertos son siempre actuales y precisos. Puede ver la planificación de descubrimiento y detalles de los últimos descubrimientos, modificar las planificaciones de descubrimiento y deshabilitar descubrimientos planificados. También puede ejecutar un descubrimiento en el momento que elija.

Antes de empezar

De forma predeterminada, TSA utiliza la planificación Descubrimiento completo para descubrir todos los elementos de TI definidos en los alcances dinámicos de VMware y HMC, así como los alcances de descubrimiento general. TSA distribuye automáticamente la detección de elementos de TI durante el proceso de descubrimiento para minimizar el impacto.

Una alternativa es crear varias planificaciones definidas por el usuario. Esto permite el descubrimiento de alcances de descubrimiento específicos para distribuirlos en distintas fechas y horas, cuando el impacto en la red y los elementos de TI sea mínimo (o ideal). En este caso, la planificación de descubrimiento completo debe inhabilitarse a favor de las planificaciones definidas por el usuario.

Al principio de los descubrimientos planificados, el dispositivo ejecuta el trabajo de mantenimiento previo al descubrimiento, durante el cual algunas funciones, como el Resumen de inventario; los Alcances de descubrimiento, las Planificaciones de descubrimiento y las Credenciales. Durante el trabajo de mantenimiento previo al descubrimiento, el estado del **Discovery Manager** en la pantalla **Resumen** es el símbolo de aviso (). Además, se muestra un mensaje de aviso en las pantallas de TSA que indica que algunas funciones no están disponibles temporalmente: `Como parte del mantenimiento previo al descubrimiento, el Discovery Manager está temporalmente fuera de línea. Es posible que algunas funciones de la interfaz de usuario relacionadas con el descubrimiento o el inventario no muestren ninguna información o solo información parcial durante este tiempo (normalmente de hasta 10 minutos).`

Una vez que el mantenimiento previo al descubrimiento ha finalizado satisfactoriamente, el estado del **Discovery Manager** vuelve a estado *Correcto*() en la página **Resumen** y reanuda la actividad de descubrimiento completa (al cabo de 10 minutos).

Ver la planificación de descubrimiento

Puede ver la información de resumen sobre una planificación de descubrimiento.

Acerca de esta tarea

Para ver la planificación de descubrimiento, siga estos pasos:

Procedimiento

En el panel de navegación, pulse **Planificación de descubrimiento**.

Se mostrará la página **Planificación de descubrimiento**.

En el panel **Planificación** se muestra el nombre de la planificación, la siguiente ejecución planificada, la planificación de ejecuciones y las acciones (Editar ( ), Suprimir ( ), Habilitar / Deshabilitar(/), Ejecutar) para cada planificación.

Pulse en el icono para ver todos los conjuntos de alcances que están asignados a la planificación. Para la planificación de descubrimiento completo, el icono lista todos los conjuntos de alcances que están definidos en TSA y que están asignados de forma predeterminada a la planificación.

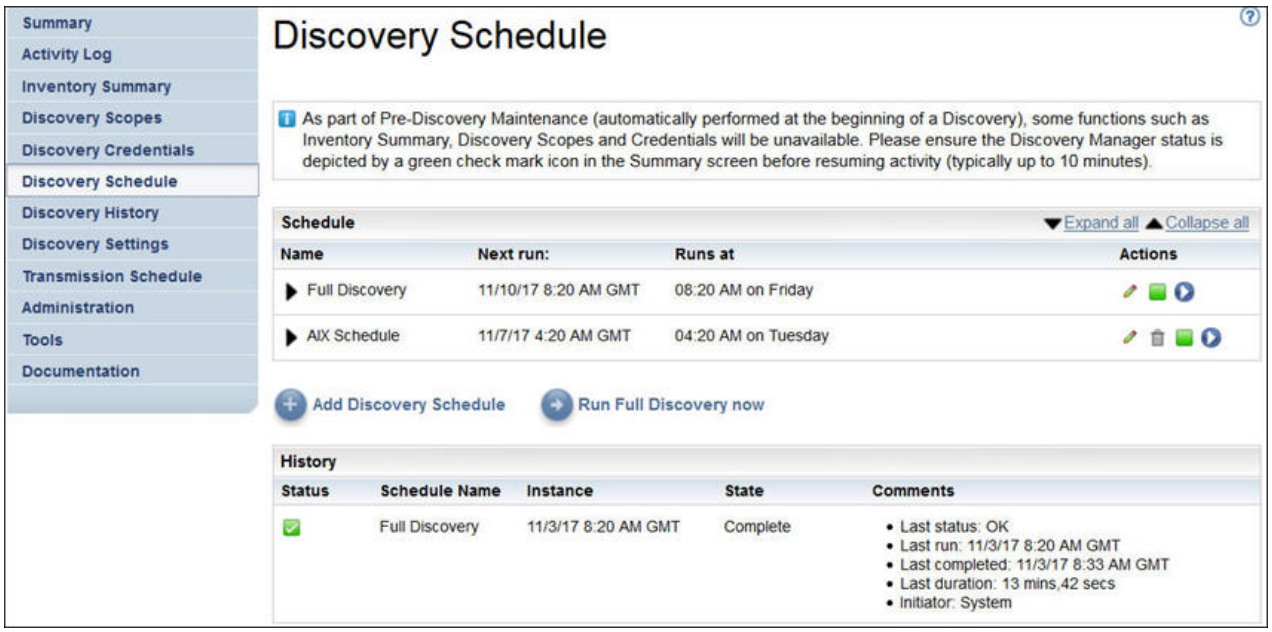

Figura 58. Planificación de descubrimiento

Nota: Si tiene un TSA que es una instalación nueva, migrada o actualizada a la última versión, el nuevo TSA tiene una planificación de descubrimiento denominada **Descubrimiento completo** creada con la fecha predeterminada (a las 02:15 los martes). La planificación Descubrimiento completo se puede editar o deshabilitar, pero no se puede suprimir. Si tiene planificaciones de descubrimiento predefinidas (habilitadas / deshabilitadas), se restauran los mismos valores tras la migración.

En el panel **Historial** se muestra el estado, el nombre de planificación y otros detalles de los trabajos actualmente en ejecución y los descubiertos anteriormente.

Añadir planificación de descubrimiento

Puede añadir nuevas planificaciones para que el proceso de descubrimiento se ejecute a una hora especificada. Las nuevas planificaciones permiten al TSA descubrir un subconjunto de los elementos de TI en la fecha y hora planificadas.

Procedimiento

1. En el panel de navegación, pulse **Planificación de descubrimiento**.
   Se mostrará la página **Planificación de descubrimiento**.
2. Pulse **Añadir planificación de descubrimiento**. Se mostrará la página **Añadir planificación de descubrimiento**.

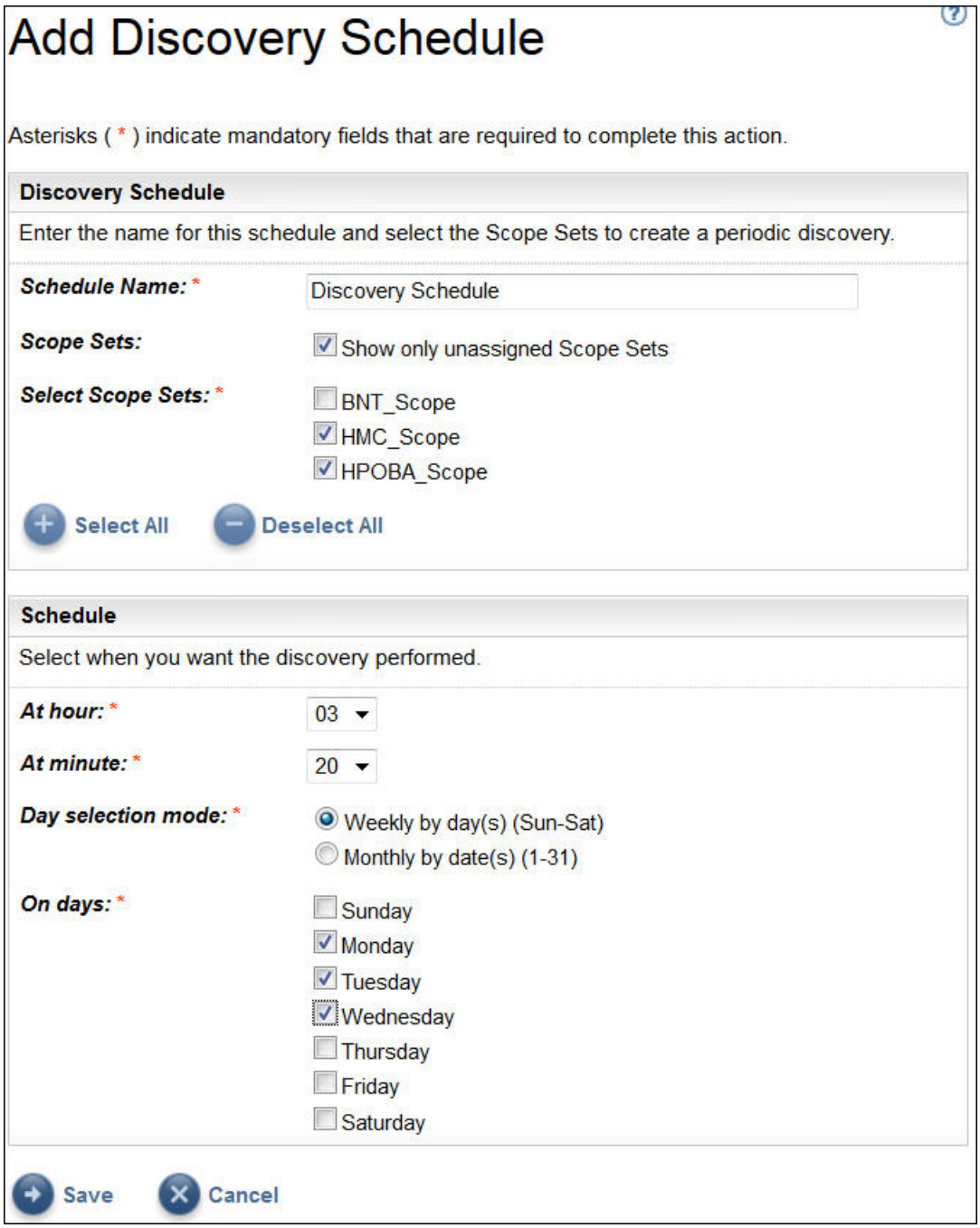

Figura 59. Añadir planificación de descubrimiento

3. En el campo **Nombre de planificación**, escriba un nombre identificativo para la planificación.
4. Seleccione la opción **Mostrar solo los conjuntos de alcances sin asignar** para ver solo los conjuntos de alcances que no están asignados a ninguna otra planificación de descubrimiento definida por el usuario.
5. Seleccione los conjuntos de alcances deseados de la lista **Seleccionar conjuntos de alcances**.

   Puede utilizar **Seleccionar todo** / **Deseleccionar todo** para seleccionar todos los conjuntos de alcances o ninguno.
6. Utilice las listas **A la hora** y **En el minuto** para seleccionar una nueva hora.
7. Seleccione el **Modo de selección del día**.

   Semanalmente los días (dom - sáb)
   Para planificar el descubrimiento en un día o días concretos de la semana, seleccione la opción **Semanalmente los días (dom - sáb)**.

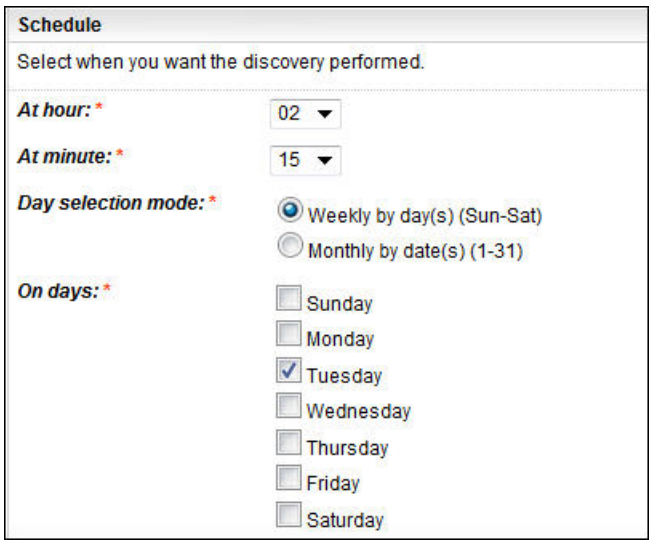

Figura 60. Semanalmente los días (dom - sáb)

En el campo **Los días**, seleccione los recuadros adecuados para seleccionar uno o más días de la semana.

Mensualmente los días (1-31)
Para planificar el descubrimiento en unos días concretos del mes, seleccione la opción **Mensualmente los días (1-31)**.

En el campo **Los días**, seleccione los recuadros adecuados para seleccionar uno o más días del mes.

Nota: Si selecciona los días más allá de un mes específico, el trabajo se activa el último día de ese mes en concreto.

8. Pulse **Guardar**.
   Se volverá a mostrar la página **Planificación de descubrimiento** con la nueva planificación.

Modificar la planificación de descubrimiento

TSA proporciona una planificación predeterminada para ejecutar el proceso de descubrimiento a las horas especificadas. Puede modificar la planificación predeterminada o utilizar las planificaciones personalizadas según sus necesidades.

Acerca de esta tarea

Procedimiento

1. En el panel de navegación, pulse **Planificación de descubrimiento**.
   Se mostrará la página **Planificación de descubrimiento**.
2. Pulse en el icono **Editar planificación** ( ).
   Se mostrará la página **Editar planificación de descubrimiento**.
   a) Edite el **Nombre de planificación**, los **Conjuntos de alcances** y **Seleccionar conjuntos de alcances** según necesite en el panel **Planificación de descubrimiento**.

      Nota: Estos campos no se pueden editar para el Descubrimiento completo predeterminado.
   b) Edite los campos **A la hora**, **En el minuto**, **Modo de selección del día** y **Los días** según necesite en el panel **Planificación**.
3. Pulse **Guardar**.
   Se volverá a mostrar la página **Planificación de descubrimiento** con la planificación modificada.

Suprimir la planificación de descubrimiento

Puede suprimir descubrimientos planificados.

Procedimiento

Para suprimir descubrimientos planificados, siga estos pasos:

1. En el panel de navegación, pulse **Planificación de descubrimiento**.
   Se mostrará la página **Planificación de descubrimiento**.
2. Pulse en el icono de la planificación que desea suprimir.
   Nota: No se puede suprimir la planificación de descubrimiento completo predeterminada, pero se puede deshabilitar, si se quiere.
   Se muestra un mensaje de confirmación para suprimir la planificación de descubrimiento seleccionada.
3. Pulse **Aceptar** para suprimir la planificación.

Ejecutar el descubrimiento

Puede ejecutar un descubrimiento a demanda en lugar de esperar al siguiente descubrimiento planificado. Puede ejecutar un descubrimiento en todos los alcances de descubrimiento definidos, una planificación de descubrimiento específica, o en conjuntos de alcances de descubrimiento o en alcances específicos.

Procedimiento

Para ejecutar un descubrimiento en todos los alcances definidos, siga estos pasos:

1. En el panel de navegación, pulse **Planificación de descubrimiento**. Se mostrará la página **Planificación de descubrimiento**.
2. Pulse **Ejecutar descubrimiento completo ahora**. La sección Historial se actualiza indicando que el descubrimiento se está ejecutando.
   Nota: TSA intenta minimizar los impactos en el entorno de red. Como resultado, el proceso de descubrimiento utiliza un método iterativo y mesurado que puede hacer que un descubrimiento completo tarde hasta 72 horas. Puede supervisar el proceso de descubrimiento en la sección **Resumen de trabajos** de la página **Resumen**.
3. Para ejecutar un descubrimiento en un alcance específico, pulse el icono **Ejecutar** de dicho alcance.
4. Consulte la página **Resumen** (pulse **Resumen** en el panel de navegación). El descubrimiento se muestra en el panel **Resumen de trabajos**. La página **Resumen** se renueva periódicamente para mostrar el estado actual de TSA. Una vez que el trabajo deja de aparecer en el panel **Resumen de trabajos**, compruebe **Registro de actividad** (pulse **Registro de actividad** en el panel de navegación). El descubrimiento se debe realizar sin errores.

Ejecutar el descubrimiento en Conjuntos de alcances generales

Procedimiento

Para ejecutar un descubrimiento en un conjunto de alcances específico, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances de descubrimiento general**.
   Se mostrará la página **Alcances de descubrimiento general**. En esta página se muestra una lista de todos los conjuntos de alcances definidos para este TSA.

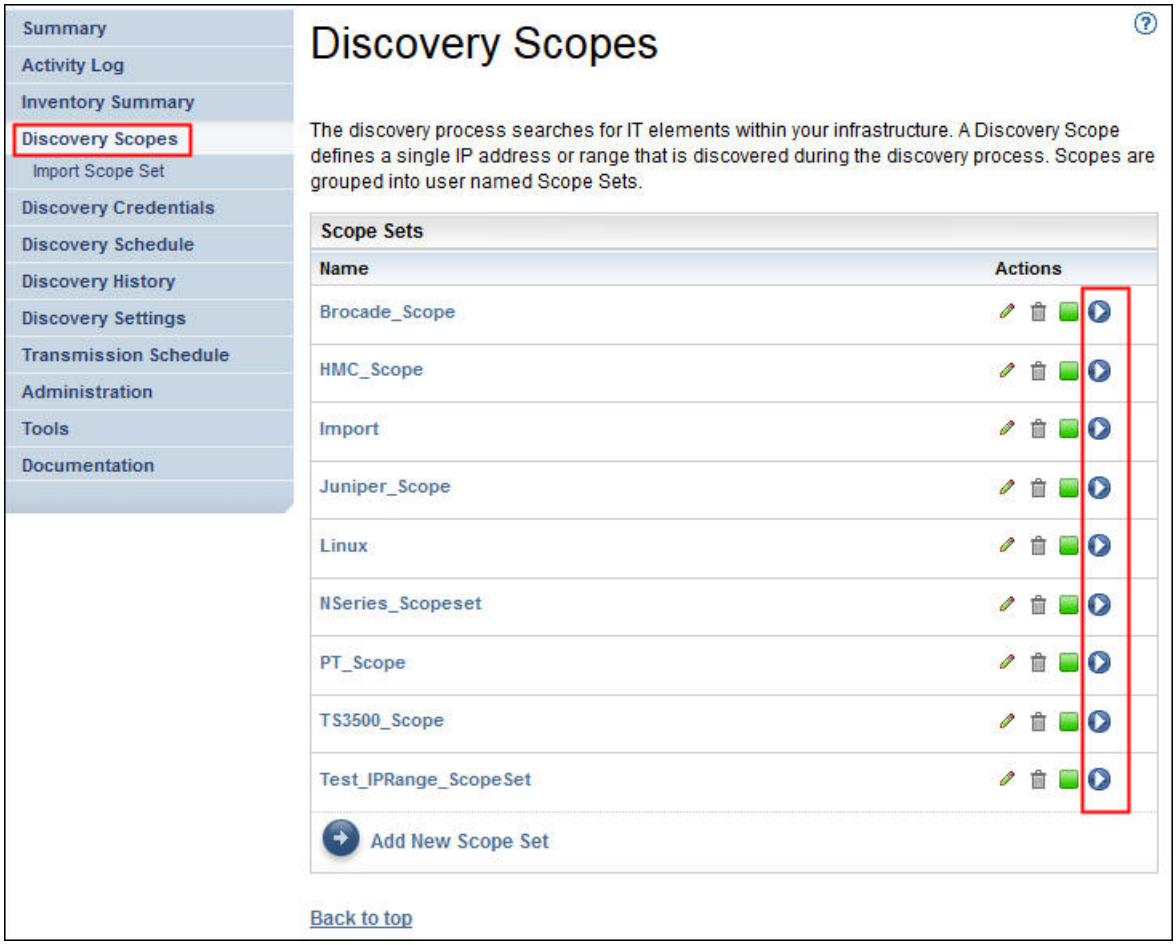

Figura 61. Ejecutar descubrimiento en alcances específicos

2. Para ejecutar un descubrimiento en un conjunto de alcances específico, pulse el icono **Ejecutar** de dicho conjunto de alcances.
3. Consulte la página **Resumen** (pulse **Resumen** en el panel de navegación). El descubrimiento se muestra en el panel **Resumen de trabajos**. La página **Resumen** se renueva periódicamente para mostrar el estado actual de TSA. Una vez que el trabajo deja de aparecer en el panel **Resumen de trabajos**, compruebe **Registro de actividad** (pulse **Registro de actividad** en el panel de navegación). El descubrimiento se debe realizar sin errores.

Ejecutar el descubrimiento en Conjuntos de alcances dinámicos de HMC

Procedimiento

Para ejecutar un descubrimiento en un conjunto de alcances específico, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**.

   Se mostrará la página **Alcances dinámicos de HMC**. En esta página se muestra una lista de todos los conjuntos de alcances definidos para este TSA.

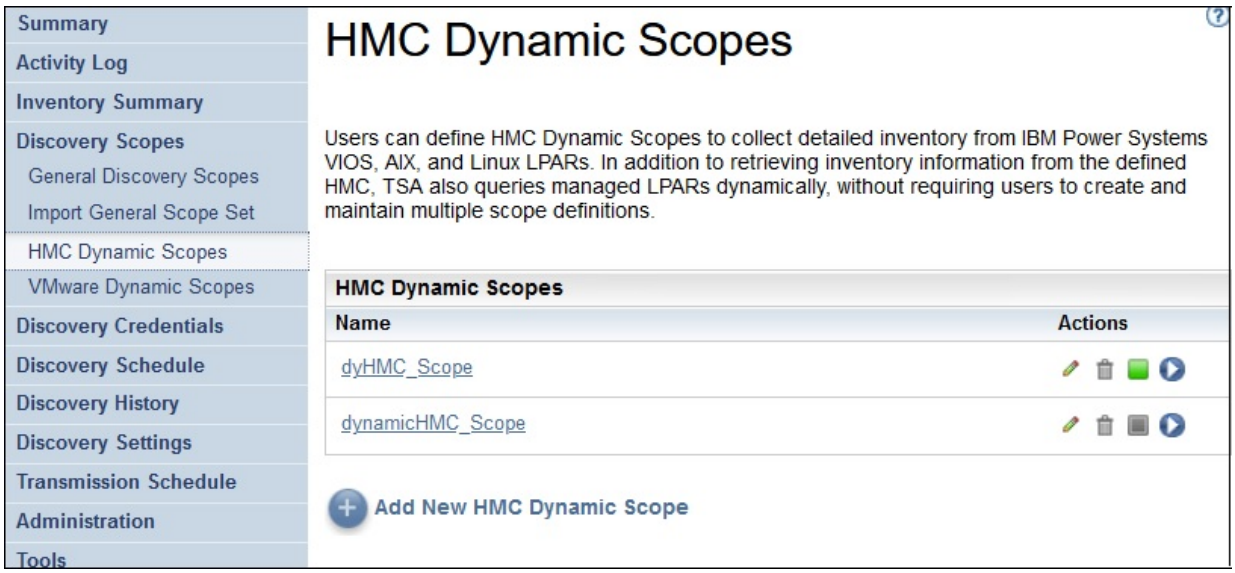

Figura 62. Alcances dinámicos de HMC

2. Para ejecutar un descubrimiento en un conjunto de alcances específico, pulse el icono **Ejecutar** de dicho conjunto de alcances.
3. Consulte la página **Resumen** (pulse **Resumen** en el panel de navegación). El descubrimiento se muestra en el panel **Resumen de trabajos**. La página **Resumen** se renueva periódicamente para mostrar el estado actual de TSA. Una vez que el trabajo deja de aparecer en el panel **Resumen de trabajos**, compruebe **Registro de actividad** (pulse **Registro de actividad** en el panel de navegación). El descubrimiento se debe realizar sin errores.

Ejecutar el descubrimiento en Conjuntos de alcances de VMware

Procedimiento

Para ejecutar un descubrimiento en un conjunto de alcances específico, siga estos pasos:

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Conjunto de alcances dinámicos de VMware**.

   Se mostrará la página **Alcances dinámicos de VMWare**. En esta página se muestra una lista de todos los conjuntos de alcances definidos para este TSA.

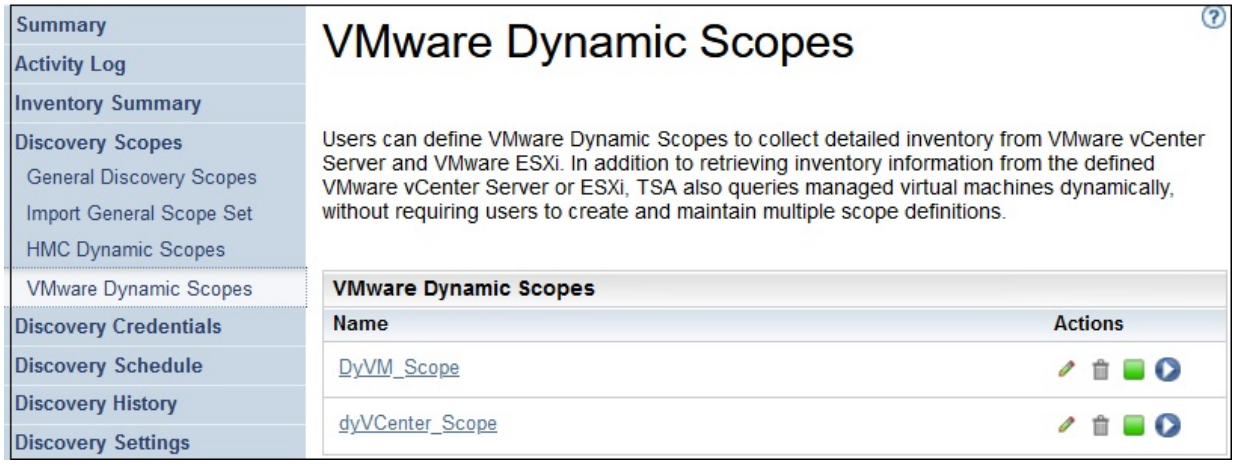

Figura 63. Ejecutar el descubrimiento en Alcances dinámicos de VMware

2. Para ejecutar un descubrimiento en un conjunto de alcances específico, pulse el icono **Ejecutar** de dicho conjunto de alcances.

3. Consulte la página **Resumen** (pulse **Resumen** en el panel de navegación). El descubrimiento se muestra en el panel **Resumen de trabajos**. La página **Resumen** se renueva periódicamente para mostrar el estado actual de TSA. Una vez que el trabajo deja de aparecer en el panel **Resumen de trabajos**, compruebe **Registro de actividad** (pulse **Registro de actividad** en el panel de navegación). El descubrimiento se debe realizar sin errores.

Ejecutar el descubrimiento en alcances

Puede ejecutar un descubrimiento a demanda en lugar de esperar al siguiente descubrimiento planificado. Puede ejecutar un descubrimiento en todos los alcances de descubrimiento definidos, una planificación de descubrimiento específica, o en conjuntos de alcances de descubrimiento o en alcances específicos.

Ejecutar el descubrimiento en Alcances generales

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances de descubrimiento general**. Se mostrará la página **Alcances de descubrimiento general**.

Figura 64. Alcances de descubrimiento

2. Pulse el conjunto de alcances que contiene el alcance que desea descubrir.

   Se mostrará la página **Conjunto de alcances de descubrimiento**. Esta página muestra todos los alcances definidos en dicho conjunto de alcances.

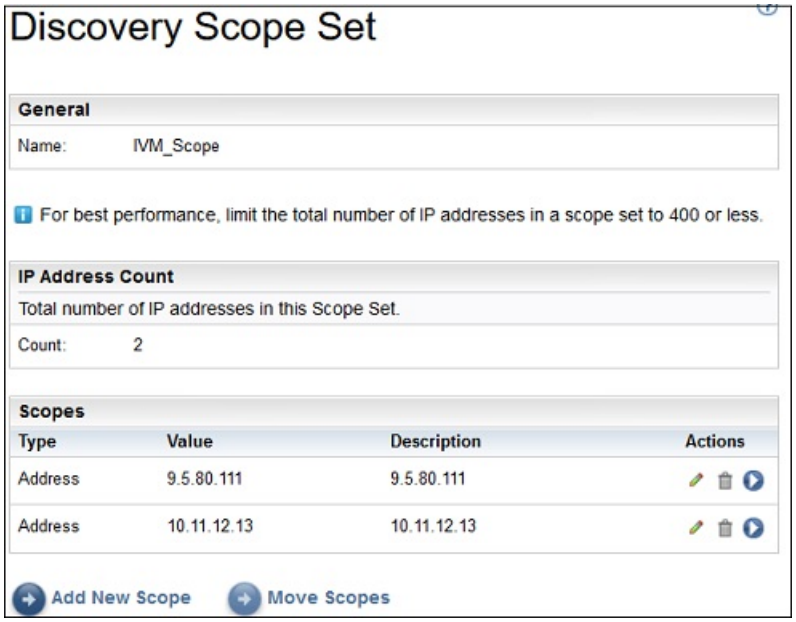

Figura 65. Ejecutar descubrimiento en alcances específicos

3. Para ejecutar un descubrimiento en un alcance específico, pulse el icono **Ejecutar** de dicho alcance.
4. Consulte la página **Resumen** (pulse **Resumen** en el panel de navegación). El descubrimiento se muestra en el panel **Resumen de trabajos**. La página **Resumen** se renueva periódicamente para mostrar el estado actual de TSA. Una vez que el trabajo deja de aparecer en el panel **Resumen de trabajos**, compruebe **Registro de actividad** (pulse **Registro de actividad** en el panel de navegación). El descubrimiento se debe realizar sin errores.

Ejecutar el descubrimiento en Alcances dinámicos de HMC

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de HMC**. Se mostrará la página **Alcances dinámicos de HMC**.

Figura 66. Alcances dinámicos de HMC

2. Pulse el conjunto de alcances que contiene el alcance que desea descubrir.

Se mostrará la página **Conjunto de alcances dinámicos de HMC**. Esta página muestra todos los alcances definidos en dicho conjunto de alcances.

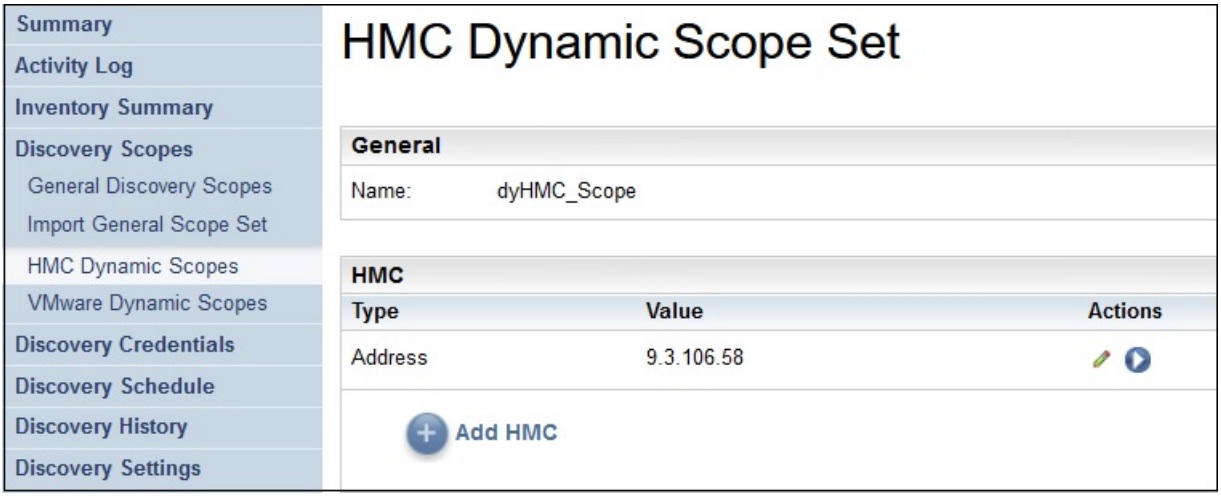

Figura 67. Ejecutar descubrimiento en alcances específicos

3. Para ejecutar un descubrimiento en un alcance específico, pulse el icono **Ejecutar** de dicho alcance.
4. Consulte la página **Resumen** (pulse **Resumen** en el panel de navegación). El descubrimiento se muestra en el panel **Resumen de trabajos**. La página **Resumen** se renueva periódicamente para mostrar el estado actual de TSA. Una vez que el trabajo deja de aparecer en el panel **Resumen de trabajos**, compruebe **Registro de actividad** (pulse **Registro de actividad** en el panel de navegación). El descubrimiento se debe realizar sin errores.

Ejecutar el descubrimiento en Alcances dinámicos de VMWare

Procedimiento

1. En el panel de navegación, pulse **Alcances de descubrimiento** > **Alcances dinámicos de VMWare**. Se mostrará la página **Alcances dinámicos de VMWare**.

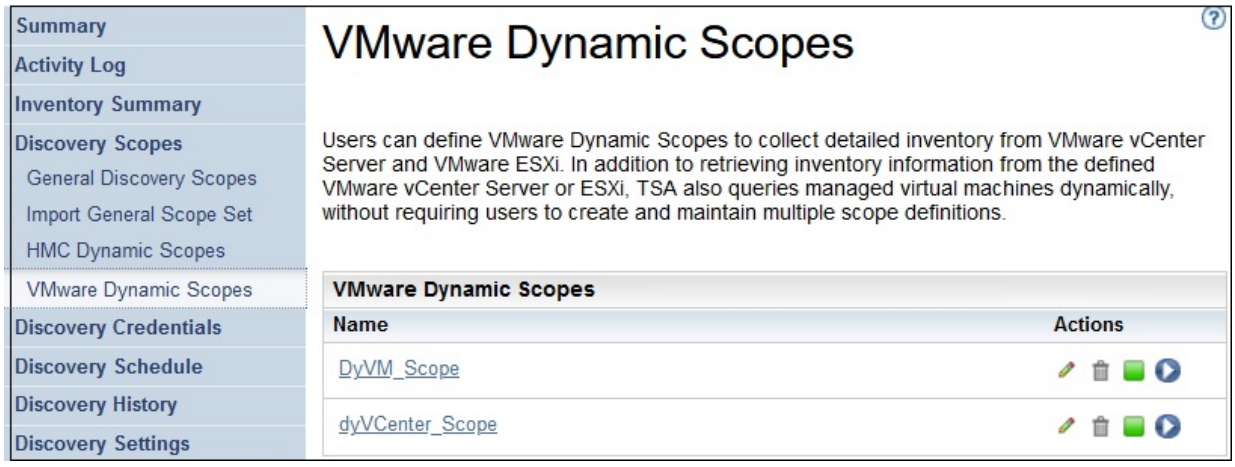

Figura 68. Alcances dinámicos de VMWare

2. Pulse el conjunto de alcances que contiene el alcance que desea descubrir.

   Se mostrará la página **Conjunto de alcances dinámicos de VMWare**. Esta página muestra todos los alcances definidos en dicho conjunto de alcances.

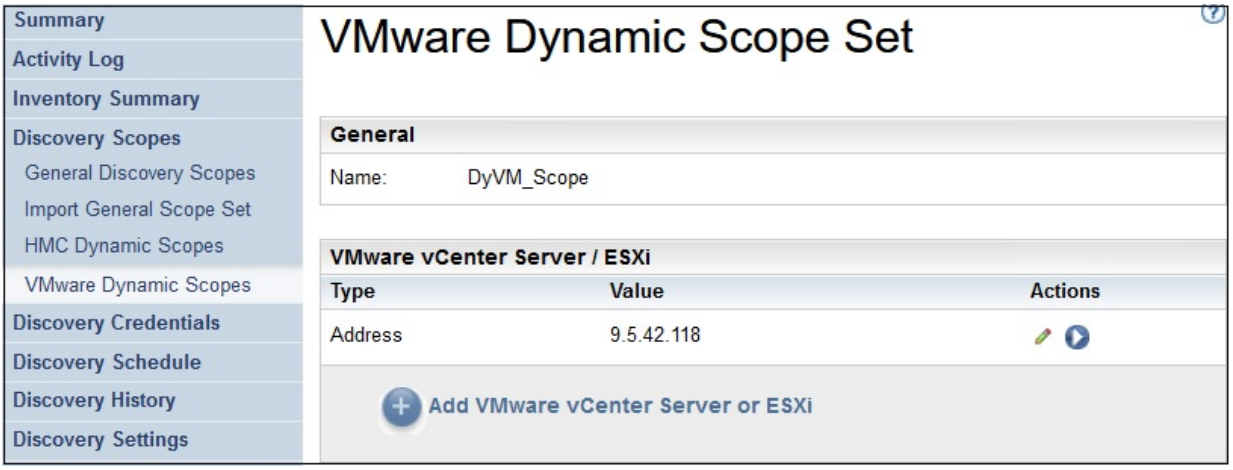

Figura 69. Ejecutar el descubrimiento en alcances dinámicos de VMware

3. Para ejecutar un descubrimiento en un alcance específico, pulse el icono **Ejecutar** de dicho alcance.
4. Consulte la página **Resumen** (pulse **Resumen** en el panel de navegación). El descubrimiento se muestra en el panel **Resumen de trabajos**. La página **Resumen** se renueva periódicamente para mostrar el estado actual de TSA. Una vez que el trabajo deja de aparecer en el panel **Resumen de trabajos**, compruebe **Registro de actividad** (pulse **Registro de actividad** en el panel de navegación). El descubrimiento se debe realizar sin errores.

Historial de descubrimiento

Puede ver los detalles de un descubrimiento una vez se ha completado y descargar un archivo de registro de diagnóstico del descubrimiento.

Procedimiento

Para ver el historial de descubrimiento o descargar un archivo de registro de diagnóstico, siga estos pasos:

1. En el panel de navegación, pulse **Historial de descubrimiento**.

   Se mostrará la página **Historial de descubrimiento**. Se muestra una lista de entradas de descubrimiento. Cada entrada indica el estado, el nombre y las horas de inicio y de finalización de un descubrimiento.

   

   Figura 70. Historial de descubrimiento
2. Para mostrar más información sobre una entrada de la lista **Entradas de historial**, pulse en el nombre de la misma.

   El panel **Información de entrada** muestra información sobre el descubrimiento seleccionado.
3. Para descargar un archivo de registro de diagnóstico correspondiente a un descubrimiento, pulse en el icono **Descargar** del descubrimiento.
4. Para suprimir un archivo de registro de diagnóstico de un descubrimiento, pulse en el icono **Suprimir** del descubrimiento.

Planificación de transmisión

La transmisión de datos se planifica para asegurarse de que los datos descubiertos se envían de forma regular a IBM Support. Puede ver la planificación de transmisión y los detalles de las últimas

transmisiones, modificar la planificación de transmisión y deshabilitar las transmisiones planificadas. También puede enviar los datos a IBM en cualquier otro momento.

Ver la planificación de transmisión

Puede ver la información de resumen sobre una planificación de transmisión.

Acerca de esta tarea

Para ver la planificación de transmisión, siga estos pasos:

Procedimiento

En el panel de navegación, pulse **Planificación de transmisión**.

Se mostrará la página **Planificación de transmisión**.

En el panel **Planificación** se muestra la siguiente ejecución planificada y las horas de ejecución planificadas. En el panel **Historial** se muestra el estado y otros detalles del trabajo que hay actualmente en ejecución y de los trabajos de transmisión anteriores.

Modificar la planificación de transmisión

TSA proporciona una planificación predeterminada para ejecutar el proceso de transmisión a las horas especificadas. Puede modificar esta planificación según sus necesidades.

Procedimiento

1. En el panel de navegación, pulse **Planificación de transmisión**.

   Se mostrará la página **Planificación de transmisión**.

   En el panel **Planificación** se muestra la siguiente ejecución planificada y las horas de ejecución planificadas. En el panel **Historial** se muestra el estado y otros detalles del trabajo que hay actualmente en ejecución y de los trabajos de transmisión anteriores.
2. Pulse **Editar planificación**.

   Se mostrará la página **Planificación de transmisión**.

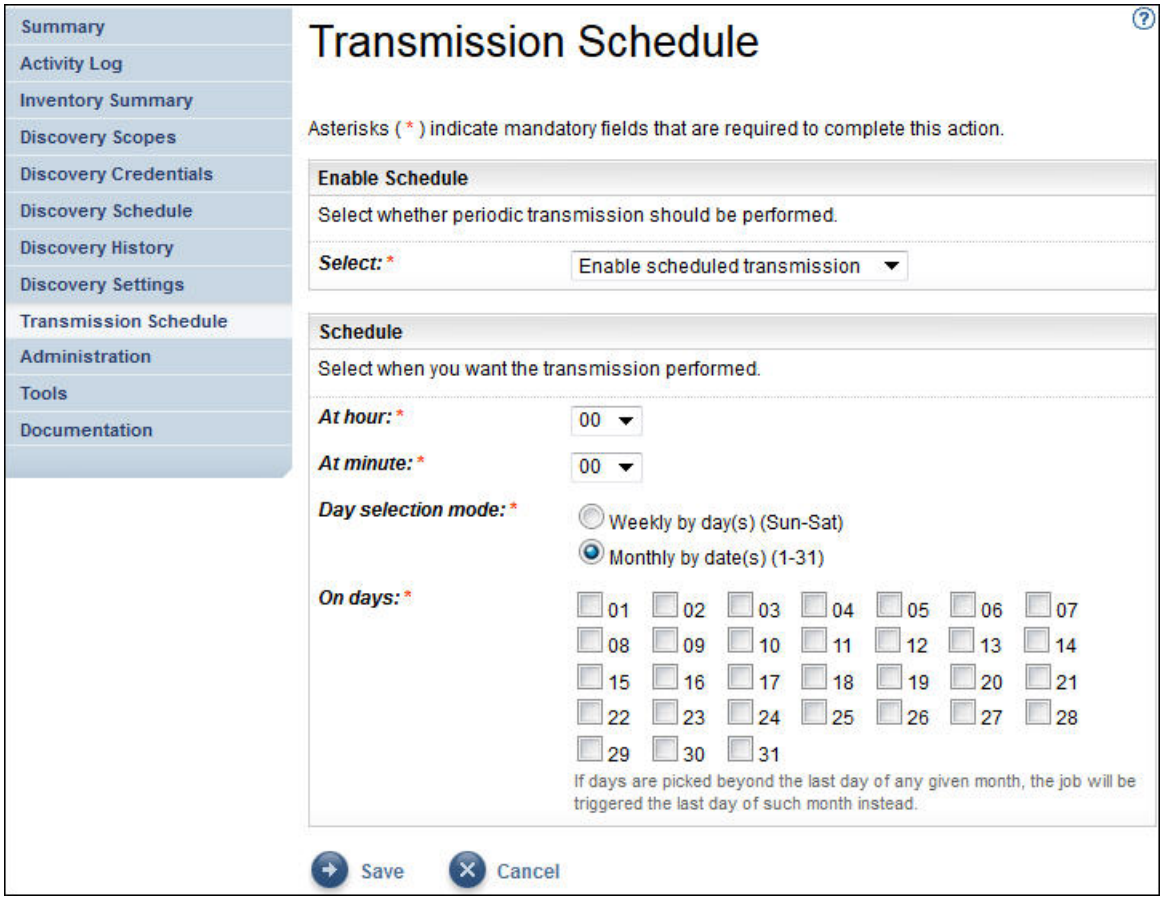

Figura 71. Editar planificación de transmisión

a) Utilice las listas desplegables **A la hora** y **En el minuto** para seleccionar una nueva hora.

b) Seleccione el **Modo de selección del día**.

Semanalmente los días (dom - sáb)

Para planificar la transmisión en un día o días concretos de la semana, seleccione la opción **Semanalmente los días (dom - sáb)**.

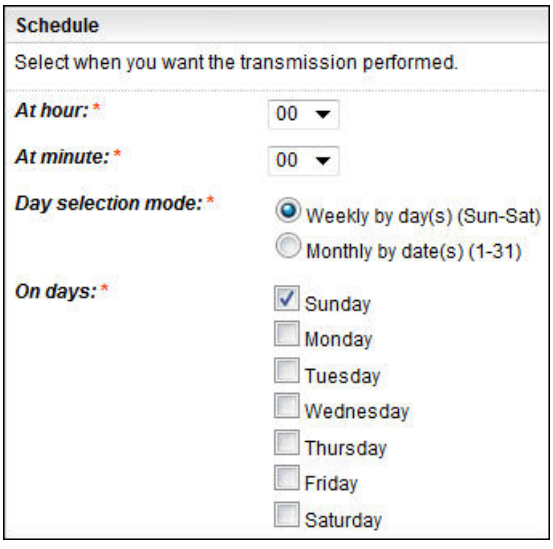

Figura 72. Semanalmente los días (dom - sáb)

En el campo **Los días**, seleccione los recuadros adecuados para seleccionar uno o más días de la semana.

Mensualmente los días (1-31)

Para planificar la transmisión en unos días concretos del mes, seleccione la opción **Mensualmente los días (1-31)**.

En el campo **Los días**, seleccione los recuadros adecuados para seleccionar uno o más días del mes.

Nota: Si selecciona los días más allá de un mes específico, el trabajo se activa el último día de ese mes en concreto.

3. Pulse **Guardar**.

   Se volverá a mostrar la página **Planificación de transmisión** con la nueva planificación.

Deshabilitar la planificación de transmisión

Puede deshabilitar transmisiones de datos planificadas.

Procedimiento

Para deshabilitar transmisiones planificadas, siga estos pasos:

1. En el panel de navegación, pulse **Planificación de transmisión**.

   Se mostrará la página **Planificación de transmisión**.

2. Pulse **Editar planificación**.

   Se mostrará la página **Planificación de transmisión**.

3. En el panel **Habilitar planificación**, seleccione **Deshabilitar transmisión planificada**.
4. Pulse **Guardar**.

   Se mostrará la página **Planificación de descubrimiento** y en el panel **Planificación** se indica que el descubrimiento planificado está deshabilitado. Puede habilitar las transmisiones planificadas pulsando **Habilitar transmisión planificada**.

Ejecutar la transmisión

Puede ejecutar una transmisión a demanda, en lugar de esperar a la siguiente transmisión planificada.

Procedimiento

1. En el panel de navegación, pulse **Planificación de transmisión**.

   Se mostrará la página **Planificación de transmisión**.

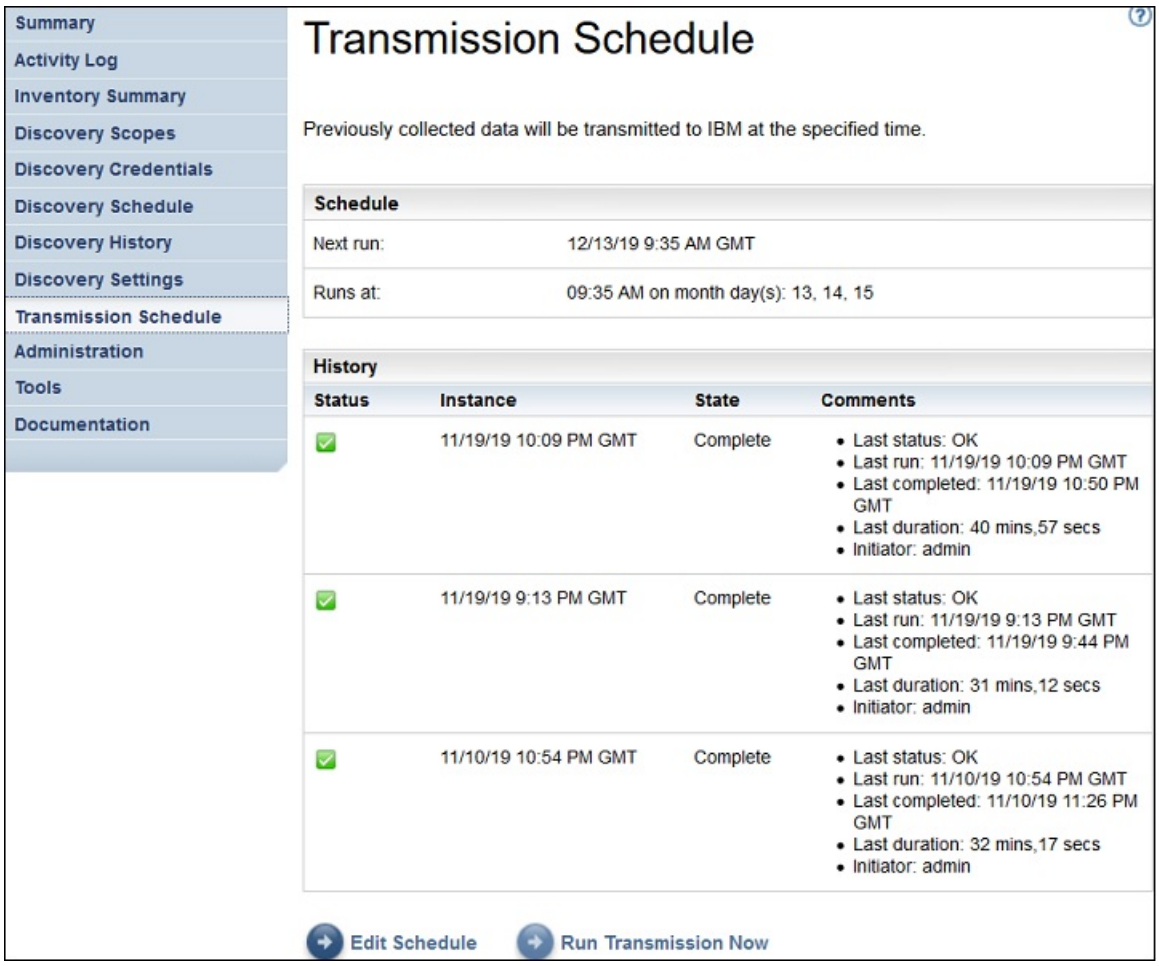

Figura 73. Ejecutar transmisión ahora

2. Pulse **Ejecutar transmisión ahora**.

   El panel **Historial** se actualiza indicando que la transmisión se está ejecutando.

3. Consulte la página **Resumen** (pulse **Resumen** en el panel de navegación). La transmisión se muestra en el panel **Resumen de trabajos**. La página **Resumen** se renueva periódicamente para mostrar el estado actual de TSA. Una vez que el trabajo deja de aparecer en el panel **Resumen de trabajos**, compruebe **Registro de actividad** (pulse **Registro de actividad** en el panel de navegación). La transmisión se debe realizar sin errores.

Instantánea de datos

Puede generar y guardar una copia local de los datos sin formato y sin procesar que TSA recopila sin tener que transmitir los datos a IBM. También puede ver los últimos datos que se han transmitido a IBM.

1. En el panel de navegación, pulse **Administración** > **Instantánea de datos**. Se visualizará la página **Instantánea de datos**.

Figura 74. Instantánea de datos

Nota: El botón **Descargar última instantánea de datos** solo está habilitado si existe una instantánea de datos o una transmisión completada.

2. Pulse **Generar instantánea de datos ahora** para recopilar los últimos datos que ha descubierto TSA y generar una nueva instantánea de datos. Aparece el mensaje siguiente: `Trabajo de instantánea de datos en curso. Puede tardar hasta 2 horas. Consulte el estado en las páginas Registro de actividad o Resumen`. Pulse **Resumen** en el menú de navegación para ver la página **Resumen**. El panel **Resumen de trabajos** muestra el estado de la recopilación de instantánea de datos hasta que finaliza. Pulse **Registro de actividad** en el menú de navegación para ver el estado de finalización de la solicitud de instantánea de datos.
3. Si ha finalizado la transmisión o el servicio de instantánea de datos, aparece la **Fecha de instantánea de datos**.

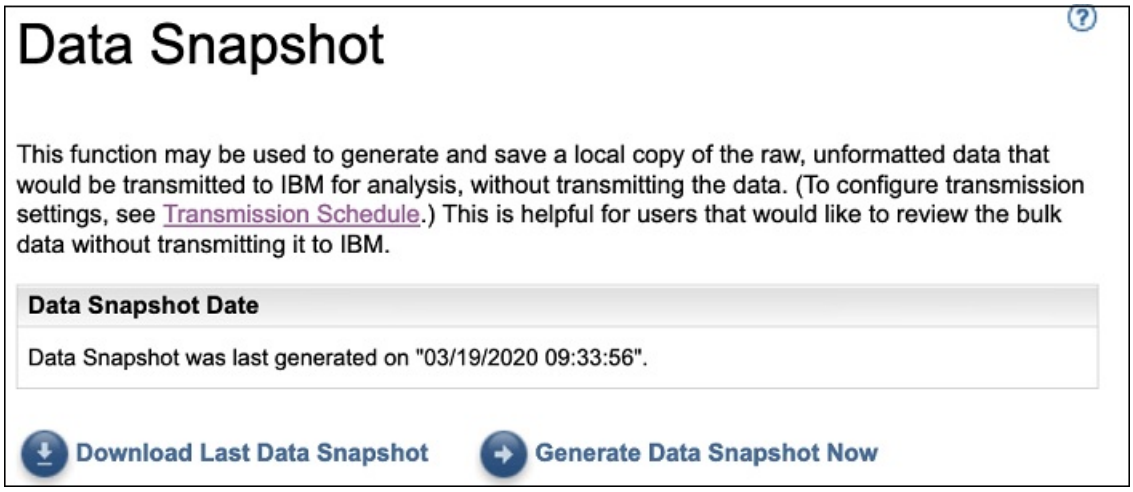

Figura 75. Fecha de instantánea de datos

4. Pulse **Descargar última instantánea de datos** para descargar la última instantánea de datos. Especifique una ubicación para el archivo resultante (*collection.tar.xz*). En función de la cantidad de datos, la operación de descarga puede tardar más tiempo en completarse. Para extraer el contenido del archivo *.tar.xz*, utilice el programa de utilidad *tar* (para Linux) o el programa de utilidad *7-Zip* (disponible para Linux y Windows).

   Nota:

   - Si hay algún trabajo de recopilación o transmisión en curso, aparece el mensaje siguiente: `Hay un trabajo de recopilación en ejecución actualmente. La instantánea de datos más reciente se generó el <<timestamp>>. ¿Está seguro de que desea descargar la recopilación?`.
     - Pulse **Aceptar** para continuar con la descarga.
     - Pulse **Cancelar** para cancelar la descarga y esperar a que finalice el trabajo de recopilación que se está ejecutando actualmente.

- Si no hay ningún trabajo de recopilación o transmisión en curso, aparece el mensaje siguiente: La `instantánea de datos más reciente se generó el <<timestamp>>. ¿Está seguro de que desea descargar la recopilación?`. Pulse **Aceptar** para continuar con la descarga.

Ver el resumen de inventario

Utilice la página **Resumen de inventario** para ver el resumen de elementos de TI, como por ejemplo sistemas, sistemas operativos y subsistemas de almacenamiento que se han descubierto.

Pulse en **Resumen de inventario** en el panel de navegación para ver la página **Resumen de inventario**.

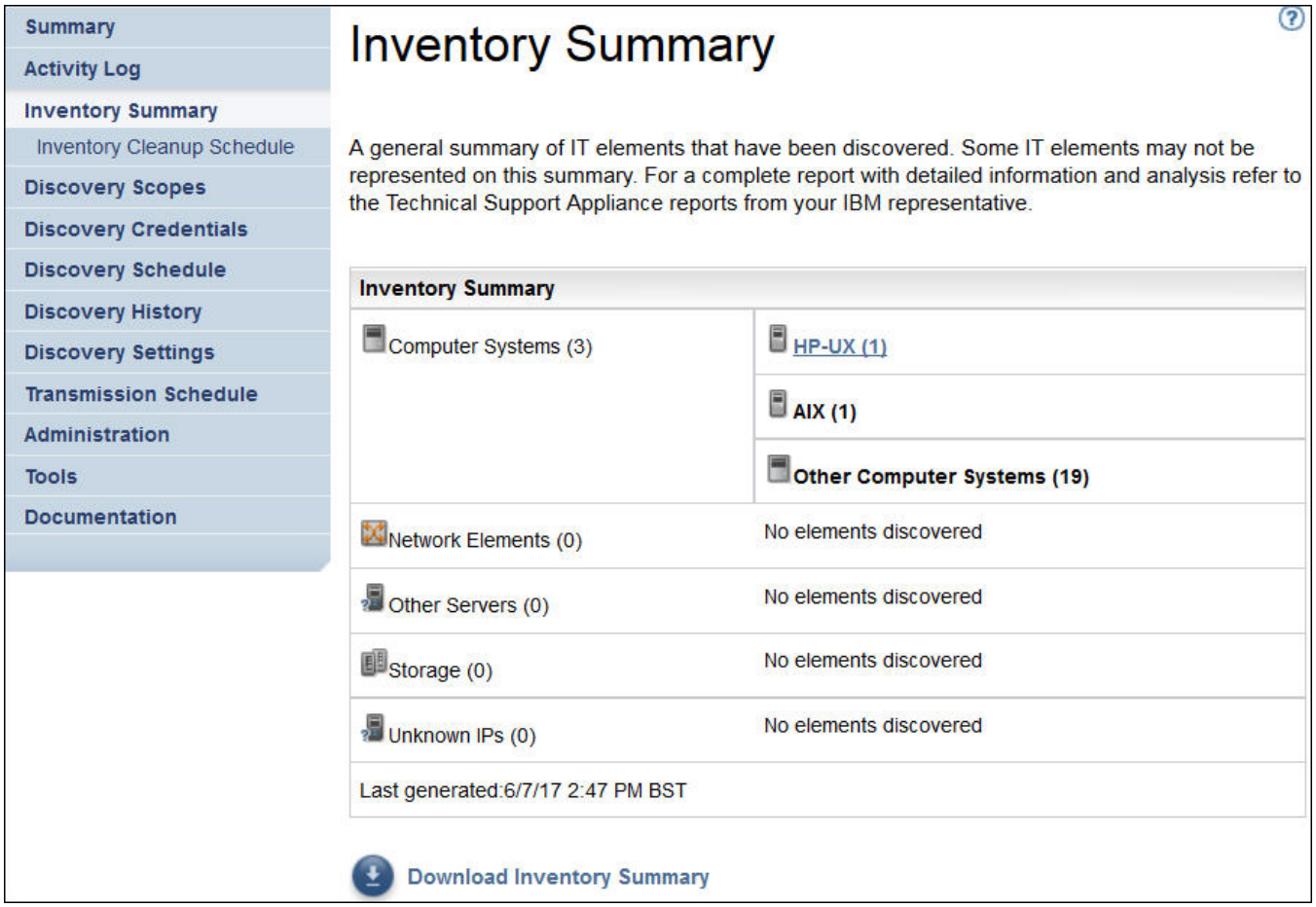

Figura 76. Resumen de inventario

En la página Resumen de inventario se muestran seis grupos distintos de elementos de TI.

- **Hipervisores**: Incluye hipervisores como por ejemplo HMC, IBM Flex System Manager, VMware, VIOS, etc.
- **Sistemas**: Incluye sistemas físicos.
- **Sistemas operativos**: Incluye sistemas operativos como por ejemplo AIX, Linux, etc. ejecutándose en bare metal o en un entorno virtualizado.
- **Elementos de red**: Incluye conmutadores y direccionadores.
- **Almacenamiento**: Incluye subsistemas de almacenamiento, como por ejemplo IBM XIV, IBM FlashSystem, EMC y dispositivos de almacenamiento de HP. Además también incluye los dispositivos de cinta.
- **IP desconocidas**: Dispositivos que puedan no haberse clasificado por motivos como los siguientes:
  - Un cortafuegos bloquea el acceso al dispositivo.

  - No se han definido credenciales para el dispositivo. Consulte la página **Estado de autenticación** (**Herramientas** → **Estado de autenticación**) para obtener información sobre direcciones IP y credenciales asociadas.
  - No existe ningún sensor para este tipo de dispositivo.
- La fila **Generado por última vez** indica la última vez en que se ha completado el trabajo de resumen de inventario.

Nota: Los datos de este panel se visualizan brevemente después de iniciar TSA. Si ve la página en este intervalo de tiempo, aparece un mensaje informativo: **`Generación de resumen de inventario en curso`**. Una vez cumplimentada la información de resumen, se renueva aproximadamente cada 30 minutos. Para renovarla manualmente, pulse el icono **Renovar** en el navegador.

Cada grupo muestra la lista de tipos de dispositivo y el recuento para cada tipo de dispositivo.

1. Pulse en cualquiera de los hiperenlaces de tipo de dispositivo para ver la página **Detalle del resumen de inventario**.

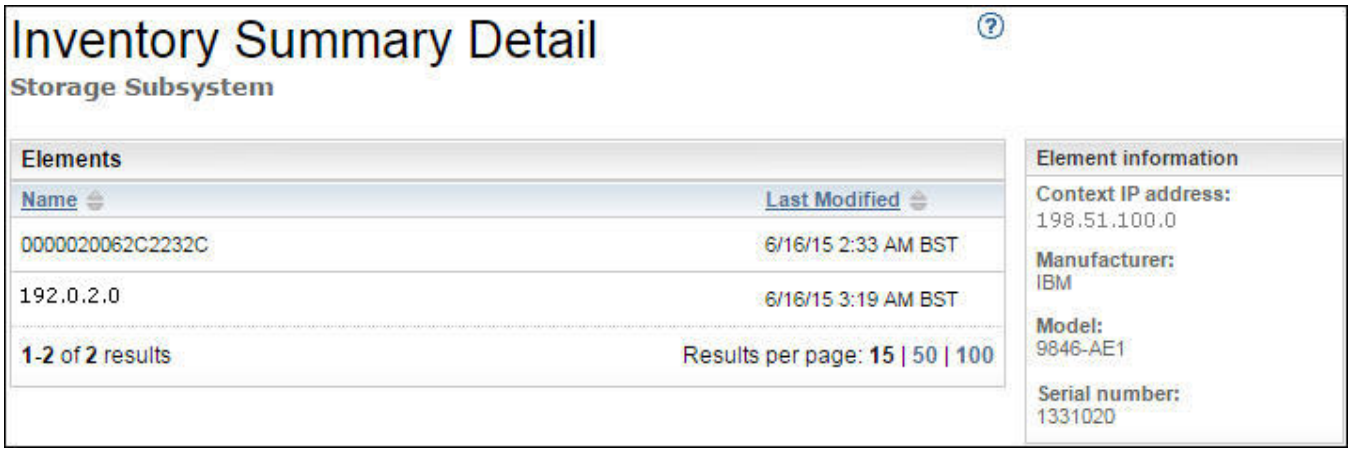

Figura 77. Detalle del resumen de inventario

2. Seleccione cualquiera de los dispositivos de la lista para ver la **Información de elemento**, como por ejemplo *Dirección IP de contexto*, *Fabricante*, *Modelo* y *Número de serie*.

   Nota: Para los dispositivos detectados por TSA para los que no se han definido credenciales válidas, la **Información de elemento** no se rellena. El TSA requiere un inicio de sesión satisfactorio en el dispositivo para poder proporcionar estos detalles.

Pulse **Descargar resumen de inventario** para descargar un archivo con un resumen de los dispositivos que se han descubierto.

Depuración de problemas de descubrimiento

Estado de autenticación

Utilice la página **Estado de autenticación** para ver un resumen de los elementos de TI que hay definidos en los conjuntos de alcances y que tienen problemas de credenciales.

Para ver el estado de autenticación, pulse **Herramientas** > **Estado de autenticación** en el panel de navegación. Se muestra la página **Estado de autenticación**.

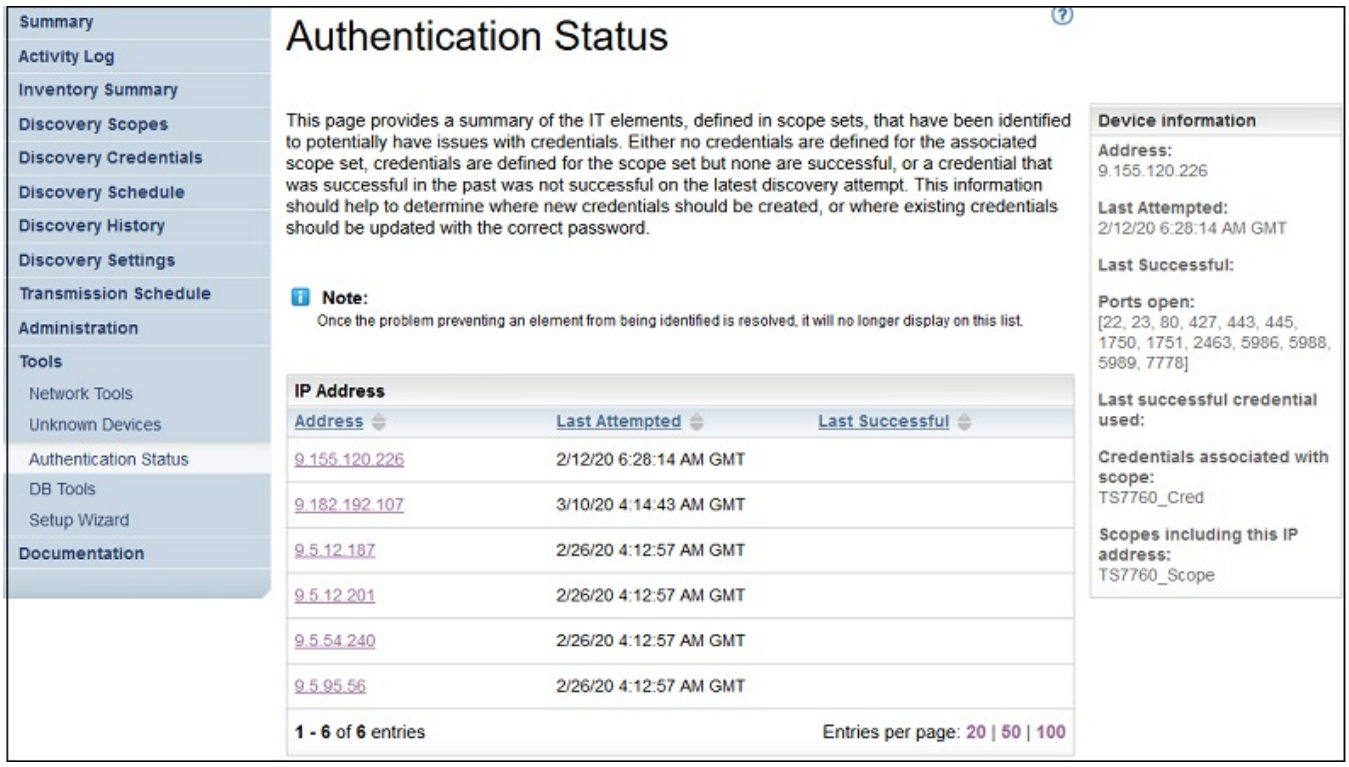

Figura 78. Estado de autenticación

El estado muestra todas las IP de dispositivo que han notificado errores de credenciales. Los problemas pueden ser debido a cualquiera de los siguientes motivos:

- No hay credenciales definidas para el conjunto de alcances asociado.
- Se han definido credenciales para el conjunto de alcances pero no son satisfactorias.
- Las credenciales que eran satisfactorios en el pasado no lo son en el intento de descubrimiento más reciente.

Pulse el enlace de dirección IP correspondiente para verla información de dispositivo como por ejemplo *Intentado por última vez*, *Satisfactorio por última vez*, *Puertos abiertos*, *Última credencial satisfactoria utilizada*, *Fecha en que se ha cambiado la credencial*, *Credencial asociada al alcance* y *Alcances que incluyen esta dirección IP*. Esta información es útil para determinar dónde se deben crear nuevas credenciales, o dónde hay que actualizar las credenciales existentes con la contraseña correcta.

Nota: Cuando se resuelve el problema de credenciales de un dispositivo, dicho dispositivo deja de aparecer en la lista.

Dispositivos desconocidos

Puede visualizar información sobre dispositivos que TSA ha descubierto pero no es capaz de identificar completamente.

Para visualizar estos dispositivos desconocidos, pulse en **Herramientas** > **Dispositivos desconocidos** en el panel de navegación. Se muestra la página **Dispositivos desconocidos**.

Puede pulsar en cualquier entrada de la lista de IP desconocidas para visualizar información adicional sobre ese dispositivo.

Capítulo 6. Configurar las tareas administrativas

Información de estado

TSA proporciona información de resumen, registros e informes que permiten encontrar rápidamente información sobre trabajos, inventario descubierto e información de producto.

Puede visualizar la información de resumen general sobre trabajos, inventario e información de producto pulsando **Resumen** en el panel de navegación. La página **Resumen** se renueva frecuentemente para mostrar la información de resumen más actualizada. La página **Resumen** incluye la información siguiente:

- **Estado del sistema**

  El panel **Estado del sistema** muestra el estado de los servicios actuales y de las tareas que se están llevando a cabo. Puede visualizar las páginas de los servicios pulsando en el nombre del puede en el panel **Estado del sistema**.
- **Resumen de trabajos**

  En el panel **Resumen de trabajos** se muestra un resumen de los trabajos actuales.
- **Resumen de inventario**

  En el panel **Resumen de inventario** se muestra una lista del inventario descubierto.
- **Información sobre el producto**

  En el panel **Información del producto** se muestra el nombre de host y el ID de TSA.

Ver el registro de actividad

El registro de actividad muestra mensajes de registro de los procesos de descubrimiento y transmisión. Puede pulsar en las entradas del registro de actividad para ver más información.

Puede visualizar el registro de actividad pulsando **Registro de actividad** en el panel de navegación. Se muestra una lista de entradas de registro. Cada entrada muestra el mensaje, la gravedad y la hora en que se ha producido la actividad.

Figura 79. Registro de actividad

Nota: Dado que los descubrimientos se ejecutan en conjuntos de alcances individuales, puede que haya varias entradas de registro para un descubrimiento completo.

Para visualizar detalles ampliados sobre una entrada de registro de actividad, pulse en el mensaje de esa entrada.

Para guardar los archivos de registro en el sistema, pulse **Descargar todos los registros**.

Para borrar el registro, pulse **Borrar registro**.

Ver el archivo de limpieza de inventario

Puede ver el inventario que se ha limpiado de acuerdo con el tiempo de inactividad que ha especificado en la **Planificación de limpieza de inventario**

Acerca de esta tarea

Para ver el inventario suprimido, siga estos pasos:

Procedimiento

1. En la página **Planificación de limpieza de inventario**, pulse **Mostrar archivo de limpieza**. Se muestra la página **Archivo de limpieza de inventario**.

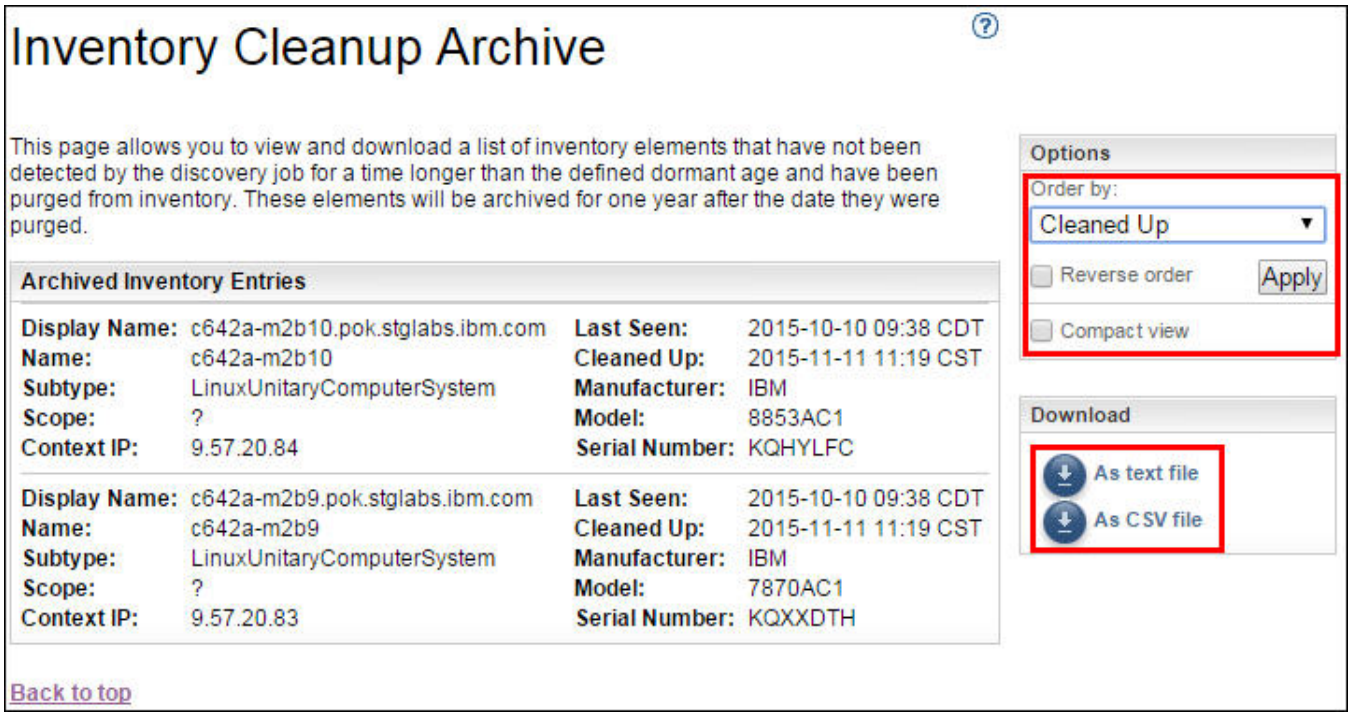

Figura 80. Archivo de limpieza de inventario

2. En la página **Archivo de limpieza de inventario**, puede ver los elementos que se han depurado del inventario como parte del proceso de limpieza.

   Nota:

   - En este archivo, puede ver la información de inventario solo de un año. Pasado un año, la información del archivo se depura.
   - El archivo estará vacío (es decir, que no se limpiará ningún objeto), si todos los destinos definidos se están descubriendo activamente dentro del último año.

3. Utilice el panel **Opciones** para reordenar los detalles de inventario.
   a) Seleccione la propiedad **Ordenar por** en el panel **Opciones** y pulse **Aplicar** para ordenar la vista de detalles de inventario.
   b) Seleccione la opción **Orden inverso** para ver los detalles en orden inverso para la propiedad seleccionada.
   c) Seleccione la opción **Vista compacta** para ver un resumen del inventario.

4. Pulse en **Como archivo de texto** o en **Como archivo CSV** para descargar los detalles de inventario. Guarde los detalles de inventario para manejar los datos localmente y también para conservar los datos en el sistema durante un periodo más largo (más de un año). Los datos que se conservan en este archivo se guardan solo durante un año y después se depuran.

Contraseñas

Puede utilizar contraseñas para proteger las cuentas de usuario de TSA.

Cambiar la contraseña

Puede cambiar la contraseña de usuario de TSA.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Contraseña**.
   Se muestra la página **Contraseña**.
2. Especifique su contraseña actual en el campo **Contraseña actual**.
3. Escriba la nueva contraseña en el campo **Nueva contraseña**.
   La contraseña debe ajustarse a las reglas siguientes:
   - Debe tener como mínimo 8 caracteres de largo
   - Debe contener al menos un carácter alfabético y uno no alfabético
   - No puede contener el nombre de usuario
   - No puede ser igual que ninguna de las ocho contraseñas anteriores
   - Se debe cambiar al menos cada 90 días, pero no se puede cambiar más de una vez al día.
4. Vuelva a escribir la nueva contraseña en el campo **Confirmar contraseña**.
   Las dos contraseñas que introduzca se comparan para confirmar que coinciden antes de guardar la contraseña.
5. Pulse **Guardar**.

Qué hacer a continuación

Importante: No se puede recuperar una contraseña, de forma que si se pierde o se olvida una contraseña, no se puede iniciar sesión en TSA para cambiar las credenciales. Si pierde u olvida la contraseña de una cuenta de usuario o cuenta de administrador (si tiene varias cuentas), póngase en contacto con el administrador de TSA. Si pierde u olvida la contraseña de la cuenta de administrador predeterminada (que se proporciona con el dispositivo), póngase en contacto con el servicio de soporte de IBM. Para obtener más información, consulte la sección "Inicio de sesión en Technical Support Appliance" en la página 21.

Seguridad

Puede acceder y modificar los programas de utilidad y las funciones de seguridad de TSA.

En la página **Seguridad** se listan todos los programas de utilidad de seguridad disponibles. En esta página, puede modificar los valores del tiempo de espera de sesión o modificar la duración máxima de la contraseña de todas las cuentas de usuario.

Modificar los valores de tiempo de espera de sesión

Por seguridad, se cierra la sesión del usuario en TSA tras un período de inactividad. Puede impedir que TSA cierre automáticamente la sesión del usuario o cambiar el tiempo que tarda en cerrar la sesión del usuario.

Deshabilitar el tiempo de espera de sesión
Puede impedir que TSA cierre automáticamente la sesión del usuario tras un período de inactividad deshabilitando el tiempo de espera de sesión.

Procedimiento

1. Marque el recuadro de selección **Deshabilitar tiempo de espera de sesión**.
2. Pulse **Cambiar la configuración de tiempo de espera de sesión**.

Modificar el valor de tiempo de espera de sesión
De forma predeterminada, se cierra la sesión del usuario pasados 20 minutos de inactividad. Puede aumentar el tiempo hasta que se cierra la sesión del usuario modificando el valor de tiempo de espera de sesión.

Procedimiento

1. Desmarque el recuadro de selección **Deshabilitar tiempo de espera de sesión**.
2. En el campo **Tiempo de espera de sesión**, especifique el tiempo en segundos que tardará TSA en cerrar la sesión del usuario.

   Nota: Este valor de tiempo de espera de sesión no puede ser inferior a 20 minutos.
3. Pulse **Cambiar la configuración de tiempo de espera de sesión**.

Modificar la duración de la contraseña

Como medida de seguridad, se obliga a todos los usuarios a cambiar su contraseña de inicio de sesión de TSA tras un número específico de días. De forma predeterminada, la duración máxima de una contraseña es de 90 días, pero se puede modificar a 30 o 60 días.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Seguridad**. Se muestra la página **Seguridad**.
2. En la página **Seguridad**, desplácese hacia abajo para ver el panel **Duración máxima de la contraseña**.
3. En el panel **Duración máxima de la contraseña**, seleccione la duración deseada (30 días, 60 días o 90 días) en la lista desplegable **Duración máxima**.
4. Pulse **Cambiar Duración máxima de la contraseña** para actualizar el valor. Se mostrará el mensaje de confirmación - *Duración máxima de la contraseña actualizada* .

Copia de seguridad y restauración

Puede hacer una copia de seguridad y restaurar la configuración de TSA.

Importante: Se recomienda especialmente realizar una copia de seguridad de manera periódica. Asimismo, debe realizarse una copia de seguridad después de hacer cambios en las credenciales o los conjuntos de alcances.

Fecha de copia de seguridad

Muestra la fecha y hora en las que se ha realizado la copia de seguridad más reciente.

Resumen de configuración

Utilice esta opción para ver un resumen de la configuración actual de TSA antes de guardarla.

Para visualizar el resumen de configuración de TSA, siga estos pasos:

1. En el panel de navegación, pulse **Administración** > **Copia de seguridad y restauración**. Se muestra la página **Copia de seguridad y restauración**.

2. Pulse **Ver resumen** para ver el resumen de la configuración actual de TSA. La información visualizada muestra las configuraciones que TSA guarda si se hace una copia de seguridad.

   Nota: Esta información se muestra mediante una ventana emergente. Si su navegador web bloquea las ventanas emergentes, puede que tenga que autorizar al navegador para abrir ventanas emergentes procedentes de TSA.

   En la página **Resumen**, en la sección **Copia de seguridad** se muestra la información relacionada con el estado de la copia de seguridad con los mensajes siguientes:

   - Un icono de *Correcto* (), si la última copia realizada en los últimos 60 días.
   - Un icono de *Aviso* (), si no se ha hecho copia de seguridad durante más de 60 días pero menos de 90 días.
   - Un icono de *Error* (), si no se ha hecho copia de seguridad durante más de 90 días.

Copia de seguridad

Utilice esta opción para guardar una copia de la configuración de TSA.

Para hacer una copia de seguridad de la configuración de TSA, siga estos pasos:

1. En el panel de navegación, pulse **Administración** > **Copia de seguridad y restauración**. Se muestra la página **Copia de seguridad y restauración**.

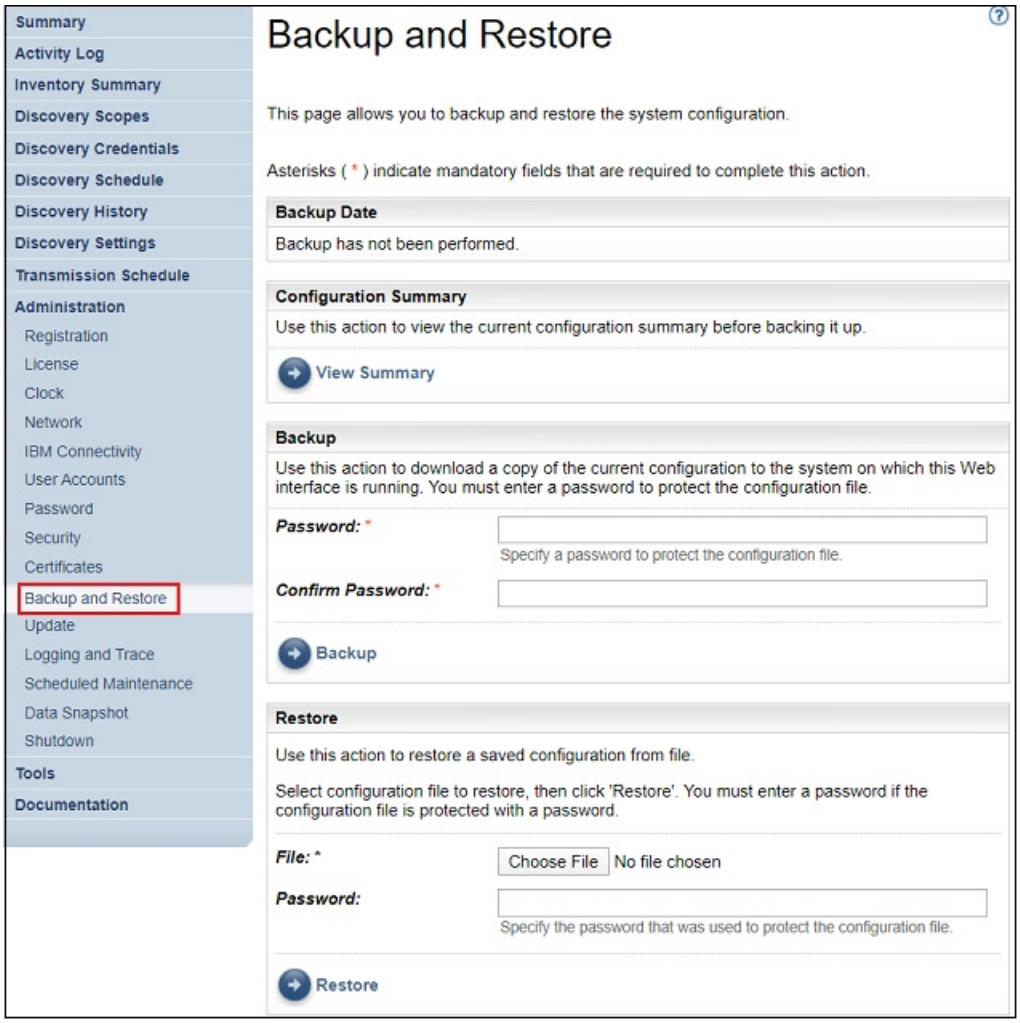

Figura 81. Copia de seguridad y restauración

2. Especifique una contraseña en el panel **Copia de seguridad** para proteger el archivo de configuración.

3. Escriba de nuevo la contraseña en el campo **Confirmar contraseña**. Las dos contraseñas que introduzca se comparan para confirmar que coinciden antes de guardar la contraseña.

   Nota: Tiene que guardar la contraseña de forma segura ya que se necesita durante la restauración.
4. Pulse **Copia de seguridad** y guarde el archivo comprimido de configuración de copia de seguridad en el sistema.

   Nota: El archivo de configuración de copia de seguridad que se genera solo lo puede abrir TSA.

   Nota: Si ha cambiado la contraseña de administrador recientemente, haga una copia de seguridad después de cambiar la contraseña y utilice el último archivo de copia de seguridad para hacer la restauración.

Restaurar

Utilice esta opción para restaurar una copia guardada anteriormente de la configuración.

Para restaurar una configuración de TSA, siga estos pasos:

1. En el panel de navegación, pulse **Administración** > **Copia de seguridad y restauración**. Se muestra la página **Copia de seguridad y restauración**.
2. Pulse **Elegir archivo** para localizar y seleccionar el archivo de configuración que desea restaurar.
3. Introduzca la contraseña que se utiliza para hacer copia de seguridad del archivo de configuración.
4. Pulse **Restaurar**.

   El trabajo de restauración se muestra en el panel de Resumen de trabajos de la página d e **Resumen**. Cuando se haya completado la restauración, se le solicitará que se reinicie del sistema.

   Nota: Si se restaura desde una copia de seguridad, se suprimen las configuraciones existentes. Todas las configuraciones, incluyendo las definiciones de alcance y las credenciales se sustituyen por las del archivo de copia de seguridad.

Nota: Asegúrese de que el estado del Discovery Manager es Correcto (✅) en la página **Resumen** cuando realice operaciones de copia de seguridad o restauración. Si el Discovery Manager no está en ejecución, obtendrá el mensaje: `"El Discovery Manager no está en ejecución. Asegúrese de que el estado del Discovery Manager se representa con un icono de marca de selección de color verde en la pantalla Resumen antes de reanudar la actividad (generalmente unos 10 minutos)."` Pasados 10 minutos, si el Discovery Manager no está en ejecución, póngase en contacto con el servicio de soporte de IBM.

Actualizar

Puede buscar y descargar actualizaciones para TSA.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Actualización**.
   Se muestra la página **Actualización**.

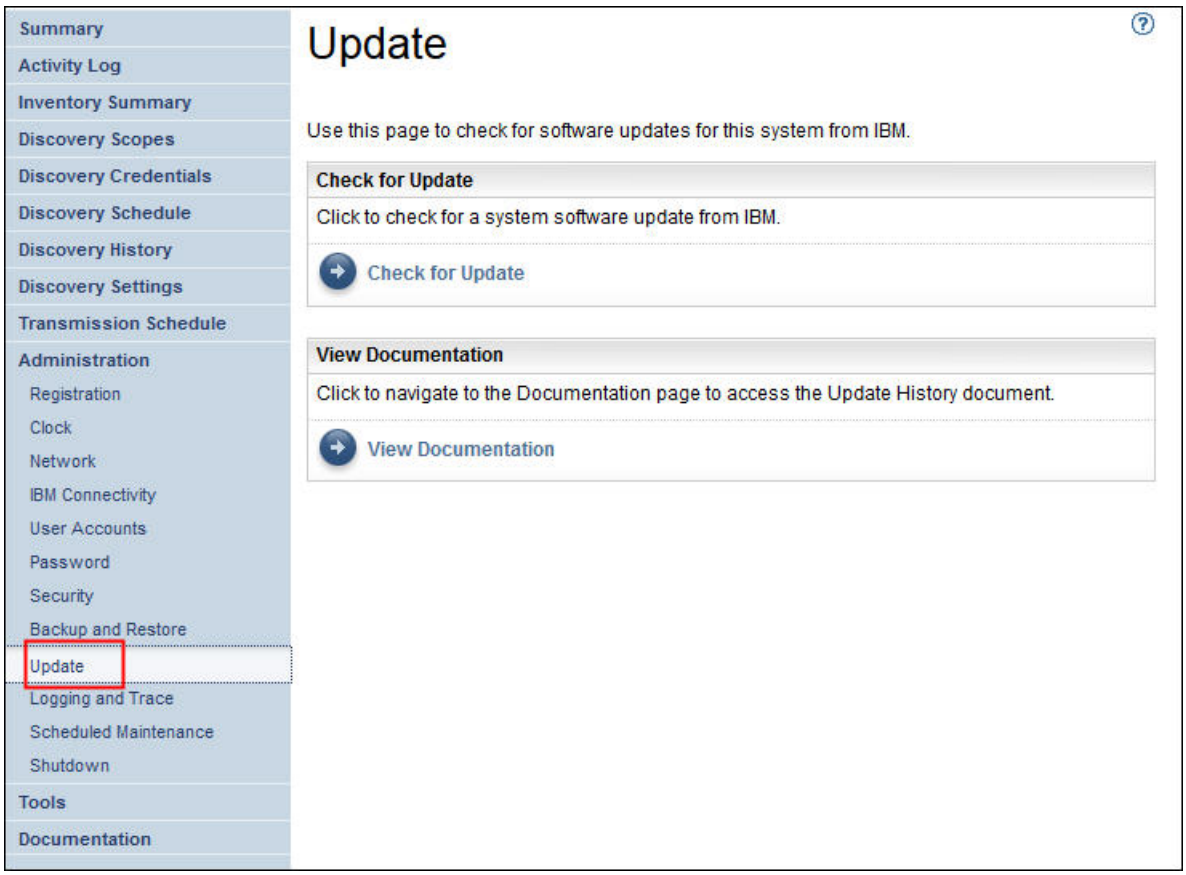

Figura 82. Actualizar

2. Pulse **Buscar actualizaciones**.

   Aparecen las actualizaciones disponibles en la página **Disponibilidad de actualizaciones**.

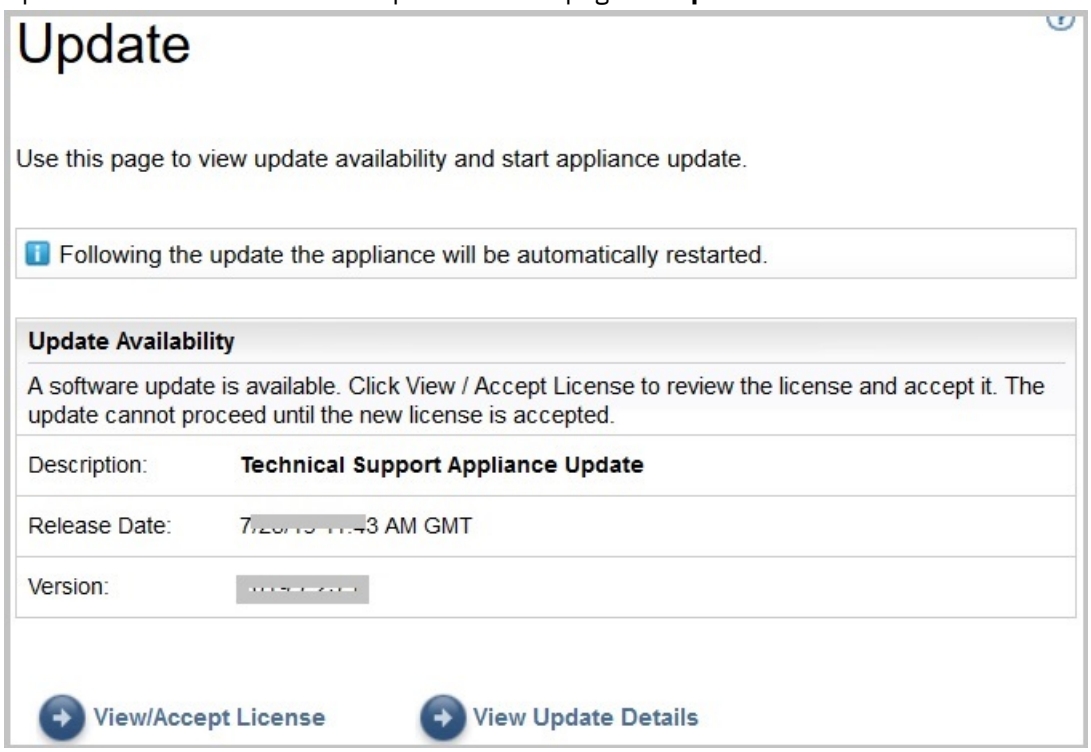

Figura 83. Disponibilidad de actualizaciones

a) En algunos releases de TSA, debe aceptar un nuevo acuerdo de licencia antes de proceder con la actualización. Si hay una nueva licencia, pulse **Ver/Aceptar licencia** y aparecerá la página **Acuerdo de licencia**.

b) Pulse el botón **Aceptar** en la página **Acuerdo de licencia** para aceptar el nuevo Acuerdo de licencia. Se muestra de nuevo la página **Actualizar** con el botón **Realizar actualización ahora**. Si no se requiere aceptar un nuevo acuerdo de licencia, no se muestra el botón **Ver/Aceptar licencia**; pulse **Realizar actualización ahora** para continuar.

Nota:

- Una vez que acepta la licencia, deja de visualizarse el botón **Ver/Aceptar licencia**.
- En el panel de navegación, pulse **Administración** > **Licencia** para ver el Acuerdo de licencia más reciente que ha aceptado.

c) Para instalar las actualizaciones, pulse **Realizar actualización ahora**.

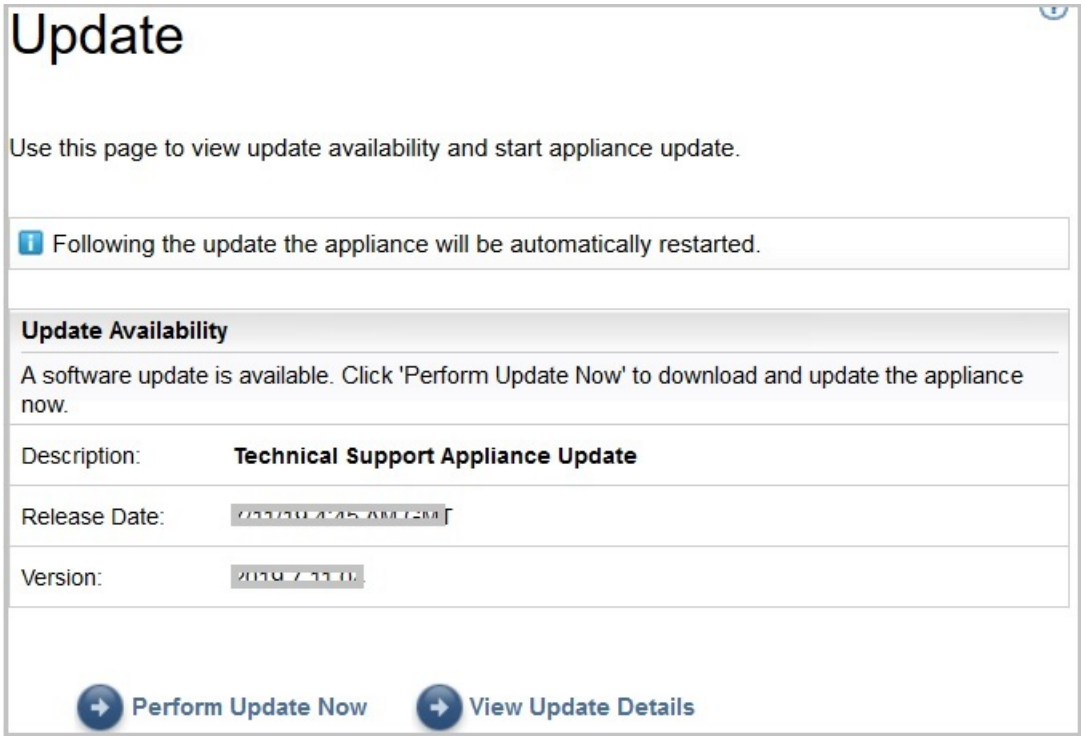

Figura 84. Realizar actualización ahora

Una vez completada la actualización, TSA se reinicia automáticamente.

d) Para ver información sobre el contenido de la actualización, pulse **Ver detalles de actualización**.

Habilitar el mantenimiento planificado

Para mantener TSA ejecutándose con un rendimiento óptimo, se recomienda habilitar la característica de Mantenimiento planificado.

Acerca de esta tarea

El trabajo de mantenimiento planificado garantiza un rendimiento óptimo de TSA. Siempre puede habilitar o deshabilitar esta característica. Si habilita el mantenimiento planificado, puede establecer el día y la hora en que se debe ejecutar automáticamente el mantenimiento. El estado del mantenimiento planificado se muestra en la sección **Estado del sistema** de la página **Resumen**.

Si planifica el trabajo de mantenimiento, el sistema se reinicia automáticamente después del mantenimiento y se le notifica el reinicio del sistema una hora antes de que se produzca. Por ejemplo,

```
Debido al mantenimiento planificado, se pondrá en cola un trabajo de reinicio
del sistema dentro de 59 minuto(s).
```

Importante: No planifique el mantenimiento del dispositivo a menos de 30 minutos de otros trabajos planificados como por ejemplo Transmisión de descubrimiento o Limpieza de inventario. Si planifica el mantenimiento a menos de 30 minutos de otros trabajos planificados, TSA no puede ejecutarlos.

Procedimiento

Para editar la planificación de mantenimiento, efectúe los pasos siguientes:

1. En el panel de navegación, pulse **Mantenimiento planificado**.

   En la página **Mantenimiento planificado** se muestra la **Planificación** de la siguiente ejecución planificada y la hora de ejecución planificada. En la sección **Historial** se muestra el estado y otros detalles del trabajo que hay actualmente en ejecución y de los trabajos de mantenimiento anteriores.
2. En la página **Mantenimiento planificado**, pulse en **Editar planificación**.
   a) En el panel **Habilitar planificación**, seleccione si desea habilitar o deshabilitar el mantenimiento planificado.
   b) Si elige habilitar la tarea de Mantenimiento planificado, seleccione las listas desplegables **A la hora** y **En el minuto** para seleccionar una nueva hora.
   c) Seleccione el **Modo de selección del día**. Para planificar el mantenimiento en un día concreto de la semana, seleccione la opción **Semanalmente los días (dom - sáb)** o, para planificar el mantenimiento en unos días concretos del mes, seleccione la opción **Mensualmente los días (1-31)**.
   d) Seleccione el recuadro adecuado del campo **Los días**, para seleccionar días distintos o adicionales de la semana o del mes.

      Nota: Si selecciona los días más allá de un mes específico, el trabajo se activa el último día de ese mes en concreto.
3. Pulse **Guardar**.

   Se vuelve a mostrar la página **Mantenimiento planificado** con la nueva planificación.

Registro y rastreo

Puede ver y modificar los valores de rastreo de diagnóstico de TSA. También puede modificar los valores de los niveles de rastreo de Discovery Manager. Modificar estos valores puede afectar al rendimiento, por lo que se recomienda no hacerlo a menos que se lo indique el servicio de soporte de IBM.

1. En el panel de navegación, pulse **Administración** > **Registro y rastreo**. Se muestra la página **Registro y rastreo**. En el panel **Nivel de rastreo de TSA**, se muestra el valor actual de rastreo (Error, Aviso, Información, Depuración o Rastreo).

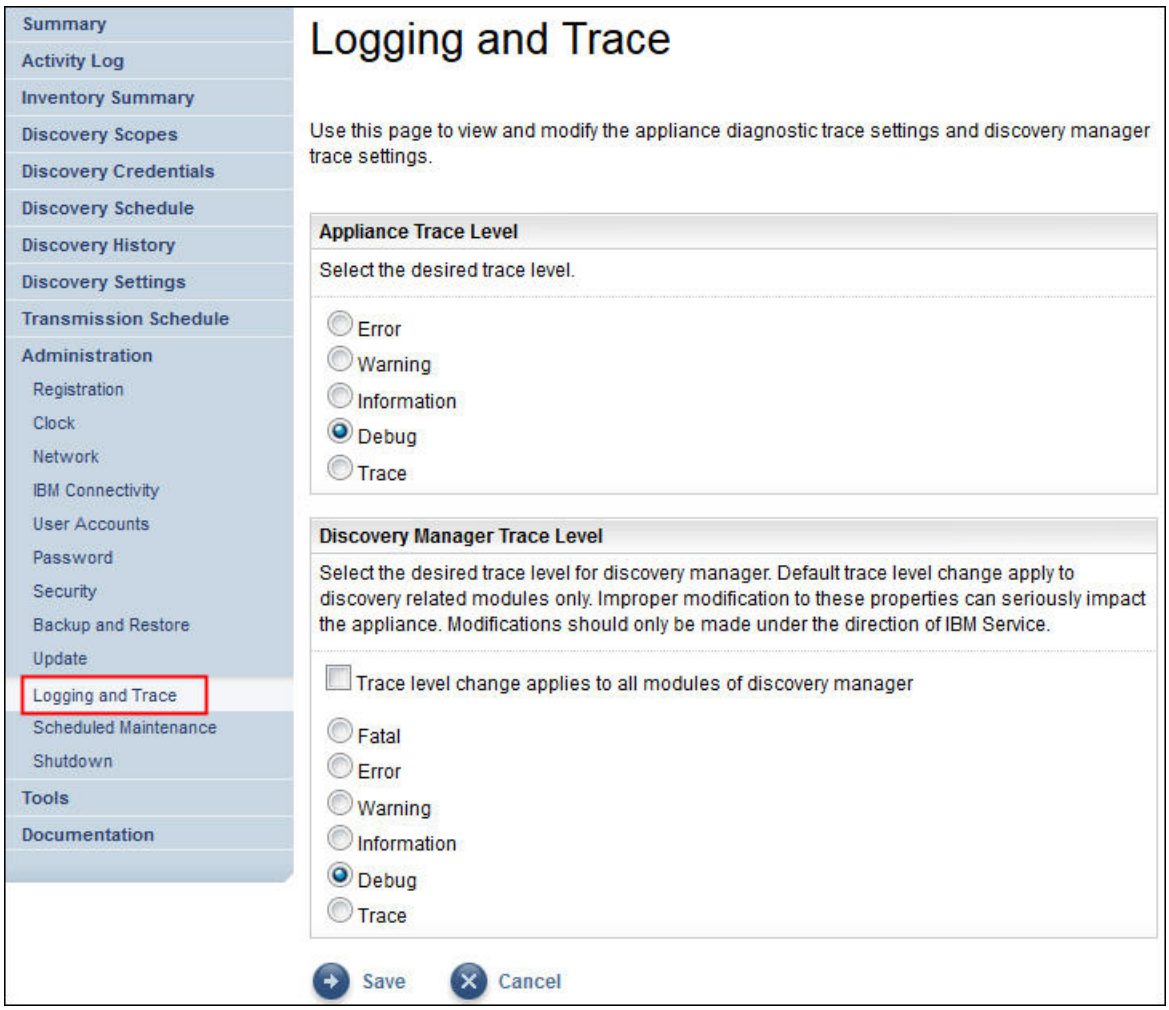

Figura 85. Registro y rastreo

2. Si es necesario, puede cambiar los valores de rastreo en el panel **Nivel de rastreo de TSA** pulsando el botón de selección junto al valor de rastreo deseado.
3. Pulse **Guardar**.

Nota: De forma predeterminada, el nivel de rastreo de *Nivel de rastreo de TSA* y sus paneles *Nivel de rastreo de Discovery Manager* está definido en el nivel **Depuración**.

Para ver y modificar los valores **Nivel de rastreo de Discovery Manager**, siga estos pasos.

Importante: Haga modificaciones a esta sección solo si se lo indica el servicio de IBM.

1. En el panel de navegación, pulse **Administración** > **Registro y rastreo**. Se muestra la página **Registro y rastreo**, que indica el valor actual de rastreo.
2. Marque **El cambio de nivel de rastreo se aplica a todos los módulos del gestor de descubrimiento** si desea que el nivel de rastreo se aplique a todos los módulos del Discovery Manager.
3. Marque el botón de selección junto al valor de rastreo deseado.
4. Pulse **Guardar**.

Apagado

Puede suspender o reanudar operaciones de TSA o cerrar y después reiniciar o apagar el TSA.

El Apagado tarda unos minutos en completarse.

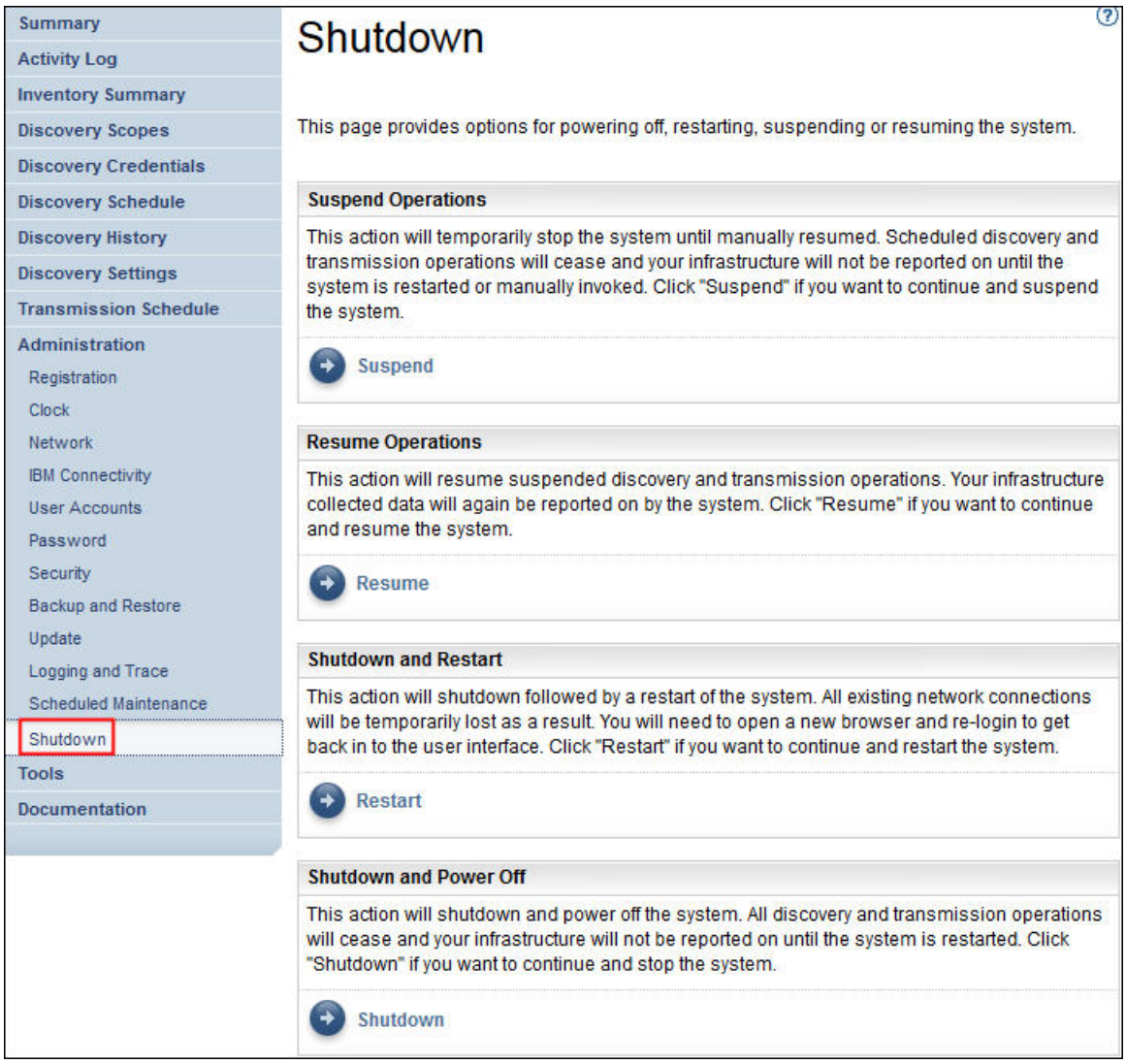

Figura 86. Apagado

Suspender operaciones

Esta acción detiene temporalmente TSA. Todas las operaciones de descubrimiento y transmisión se detienen y no se notifica ninguna información a IBM hasta que se reanudan las operaciones.

Para suspender las operaciones de TSA, siga estos pasos:

1. En el panel de navegación, pulse **Administración** > **Apagar**. Se muestra la página **Apagar**.
2. Pulse **Suspender**.

Reanudar operaciones

Esta acción reanuda el TSA que se ha detenido temporalmente. Todas las operaciones de descubrimiento y transmisión se reanudan y se notifica información IBM según lo planificado.

Para reanudar las operaciones de TSA, siga estos pasos:

1. En el panel de navegación, pulse **Administración** > **Apagar**. Se muestra la página **Apagar**.
2. Pulse **Reanudar**.

Apagar y reiniciar

Esta acción cierra y después reinicia TSA. Se pierden temporalmente todas las conexiones de red existentes. Debe abrir un nuevo navegador y volver a iniciar sesión.

Para cerrar y reiniciar TSA, siga estos pasos:

1. En el panel de navegación, pulse **Administración** > **Apagar**. Se muestra la página **Apagar**.
2. Pulse **Reiniciar**.

Apagar y desconectar

Esta acción cierra y después apaga TSA. Todas las operaciones de descubrimiento y transmisión cesan y no se notifica su infraestructura hasta que se reinicia TSA.

Para cerrar y apagar TSA, siga estos pasos:

1. En el panel de navegación, pulse **Administración** > **Apagar**. Se muestra la página **Apagar**.
2. Pulse **Apagar**.

Nota: Tras apagar el dispositivo, debe encender TSA utilizando la interfaz web de VMware ESXi o Hyper-V Manager.

Herramientas

TSA proporciona herramientas para ayudarle a configurar el entorno de TSA.

Puede acceder a estas herramientas pulsando en **Herramientas** en el panel de navegación.

Herramientas de red

Utilice la página **Herramientas de red** para obtener herramientas de diagnóstico e información de los protocolos de red que utiliza TSA.

Para acceder a estas herramientas de diagnóstico, pulse **Herramientas** > **Herramientas de red** en el panel de navegación. Se visualizará la página **Herramientas de red**.

La página Herramientas de red está dividida en pestañas. Pulse en cualquier pestaña para visualizar la página que corresponde a esa pestaña.

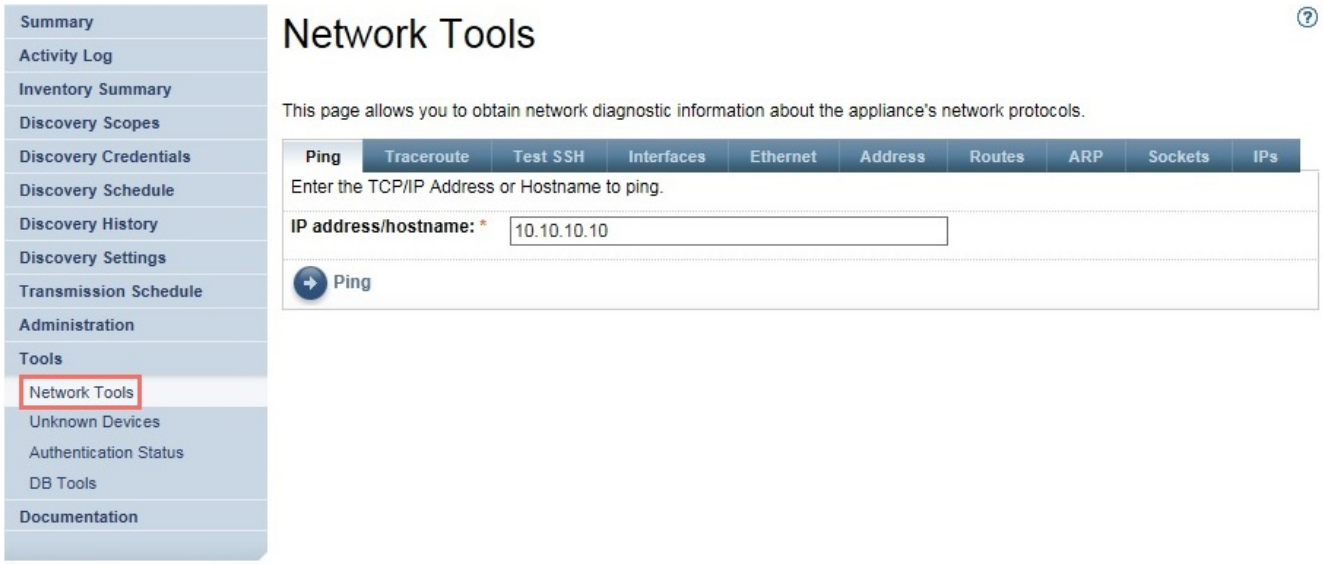

Figura 87. Herramientas de red

Ping
Utilice esta página para enviar una solicitud de eco a un host remoto para comprobar si el host está accesible y para recibir información sobre el nombre de host o la dirección IP.

Ruta de rastreo
Utilice esta página para visualizar la ruta que toman los paquetes hasta un host remoto.

Probar SSH
Utilice esta página para probar si un host remoto es accesible con SSH utilizando las credenciales de descubrimiento definidas para ese host.

Interfaces
Utilice esta página para visualizar las estadísticas de las interfaces de red que hay configuradas actualmente.

Ethernet
Utilice esta página para visualizar la configuración de las tarjetas Ethernet que hay configuradas actualmente.

Dirección
Utilice esta página para visualizar las direcciones IP de las interfaces de red que hay configuradas actualmente.

Rutas
Utilice esta página para visualizar las tablas de direccionamiento de IP de Kernel y las interfaces de red correspondientes.

ARP
Utilice esta página para visualizar el contenido de las conexiones ARP (Address Resolution Protocol - protocolo de resolución de direcciones).

Sockets
Utilice esta página para visualizar información sobre los sockets TCP/IP.

IP
Utilice esta página para visualizar información sobre las reglas de filtrado de paquetes de IP.

Nota: El nombre de host que especifique no puede contener ningún guión bajo ("_").

Herramientas de base de datos

Utilice la página **Herramientas de base de datos** para ejecutar operaciones de mantenimiento de datos. Se recomienda utilizar estas funciones únicamente cuando se lo indique el servicio de soporte de IBM.

Puede ejecutar las siguientes operaciones en la base de datos:

Volver a crear la base de datos de inventario

Cuando se vuelve a crear la base de datos de inventario, se pierden todos los datos de inventario. Además, se pierden las credenciales si se desmarca el recuadro **Conservar credenciales** o si el Discovery Manager no está disponible.

Para volver a crear la base de datos, efectúe los pasos siguientes:

1. En el panel de navegación, pulse **Herramientas** > **Herramientas de BD**.
2. Seleccione el recuadro **Conservar credenciales** en la sección **Volver a crear la base de datos de inventario** para conservar todas las credenciales de descubrimiento. Si no lo selecciona, se perderán las credenciales y tendrá que volver a configurar todas las credenciales. Para obtener más información sobre las credenciales de descubrimiento, consulte “Credenciales de descubrimiento” en la página 73.

   Nota: Las credenciales solo se pueden conservar si el Discovery Manager está en ejecución (estado verde).
3. Pulse **Volver a crear la base de datos de inventario**. Se muestra el siguiente mensaje de aviso - `Esta acción apagará temporalmente el Discovery Manager. ¿Seguro que desea volver a crear la base de datos de inventario?`

4. Pulse **Aceptar** para volver a crear la base de datos de inventario. Aparece el mensaje siguiente: Se ha iniciado la recreación de la base de datos. La recreación de la base de datos puede tardar aproximadamente 6 horas; mientras tanto, aparece el siguiente mensaje dbinit starting en la página Resumen. Transcurridas las 6 horas, pude comprobar el **Registro de actividad** para ver el estado Recreación de la base de datos de inventario satisfactoria.

   Nota: Al volver a crear la base de datos de inventario, el Discovery Manager se apaga temporalmente y se borra el *archivo de limpieza de inventario*.

Realizar RUNSTATS

Para ejecutar el mandato **RUNSTATS**, complete los pasos siguientes:

1. En el panel de navegación, pulse **Herramientas** > **Herramientas de BD**.
2. Pulse **Realizar RUNSTATS**. Se mostrará el siguiente mensaje de aviso: ¿Seguro que desea realizar RUNSTATS en las tablas de la base de datos de inventario?
3. Pulse **Aceptar**. Aparece el mensaje siguiente: RUNSTATS se ha iniciado. Pasados unos 30 minutos, puede comprobar el registro de actividad. Una vez que el trabajo se ha completado, se añade el siguiente mensaje al registro de actividad: RUNSTATS para base de datos de inventario satisfactorio.

Realizar REORG

Para ejecutar el mandato **REORG**, complete los pasos siguientes:

1. En el panel de navegación, pulse **Herramientas** > **Herramientas de BD**.
2. Pulse **Realizar REORG**. Se mostrará el siguiente mensaje de confirmación: ¿Seguro que desea realizar REORG en las tablas de la base de datos de inventario?
3. Pulse **Aceptar**. Se añade el siguiente mensaje al registro de actividad: REORG se ha iniciado. Pasados unos 30 minutos, puede comprobar el registro de actividad. Una vez que el trabajo se ha completado, se añade el siguiente mensaje al registro de actividad: REORG de la base de datos de inventario satisfactorio.

Documentación

Utilice la página **Documentación** 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 TSA desde el sitio web de TSA en: https://ibm.biz/TSAdemo.

Procedimiento

Para ver la documentación y obtener más información sobre Technical Support Appliance, siga estos pasos:

1. Pulse **pulse** en el menú de navegación de la izquierda.

Figura 88. Documentación

2. Para obtener más información sobre Technical Support Appliance, pulse el enlace: https://ibm.biz/TSAdemo
3. En la página **Instalar TSA**, encontrará enlaces disponibles a la imagen de TSA, la guía de instalación, la guía de configuración y las guías de aprendizaje correspondientes.

Capítulo 7. Contactar con el servicio de soporte de IBM en relación a Technical Support Appliance (TSA)

El servicio de soporte de IBM está disponible de lunes a viernes en el horario laboral de su zona horaria.

Acerca de esta tarea

Puede ponerse en contacto con el servicio de soporte de IBM con cualquiera de estas dos opciones:

1. Abrir un caso en IBM Support Portal
2. Crear una solicitud de servicio a través de IBM Call Center

Abrir un caso en IBM Support Portal

Procedimiento

1. Inicie una sesión en https://www.ibm.com/mysupport/s/

   Nota: Primero debe crear una cuenta para acceder a IBM Support Portal.
2. Pulse **Abrir un caso** en la esquina superior derecha del portal. Se mostrará la página **Abrir un caso**.
3. Seleccione el **Tipo de soporte**.
4. Especifique el **Título**, el **Fabricante del producto** y el **Producto**.

   Nota: Para direccionar la solicitud directamente al equipo de Technical Support Appliance, especifique `Technical Support Appliance` en el campo **Producto**.
5. Seleccione la **Gravedad**
6. Especifique una **Descripción** y seleccione su idioma preferido.
7. Si no hay disponible un agente que hable su idioma y está interesado en comunicarse en inglés, seleccione **Sí**.
8. Pulse **Enviar caso**.

Crear una solicitud de servicio a través de IBM Call Center

Procedimiento

1. Marque el número de teléfono correcto según el país de origen: https://www.ibm.com/planetwide
2. Seleccione el idioma.
3. Seleccione 1 (productos de IBM)
4. Seleccione 2 (Soporte de software).
5. Utilice el ID de producto *5621IZX01* o el nombre de producto *Technical Support Appliance*.
6. Se le solicitará lo siguiente:
   - Número/área geográfica de la empresa
   - Nombre de cliente/empresa
   - Dirección/Ciudad/Estado/Código postal
   - Edificio/Planta
   - Número de teléfono donde se encuentra TSA.
   - Nombre/correo electrónico/número de teléfono de la persona de contacto
   - Descripción del problema

- Nivel de gravedad

Apéndice A. Instalación de TSA utilizando el Cliente de VMware vSphere

Antes de empezar
TSA necesita que se cargue VMware ESXi 6.5 o superiores para controlar el hardware.

Acerca de esta tarea
Siga estos pasos para instalar la imagen de TSA. Para obtener información sobre los requisitos, consulte “Requisitos para TSA” en la página 5.

Nota: El procedimiento (pasos de 1 a 12) es un ejemplo/referencia de cómo desplegar la imagen de TSA. Algunos de estos pasos pueden variar en función de los procedimientos locales de despliegue de máquinas virtuales.

Procedimiento

Para instalar TSA, siga estos pasos:

1. Inicie el Cliente de VMware vSphere.
2. Inicie sesión para conectarse al sistema ESXi.
3. En vSphere Client, pulse **Archivo** > **Desplegar plantilla de OVF**. Se muestra el asistente **Desplegar plantilla de OVF**.

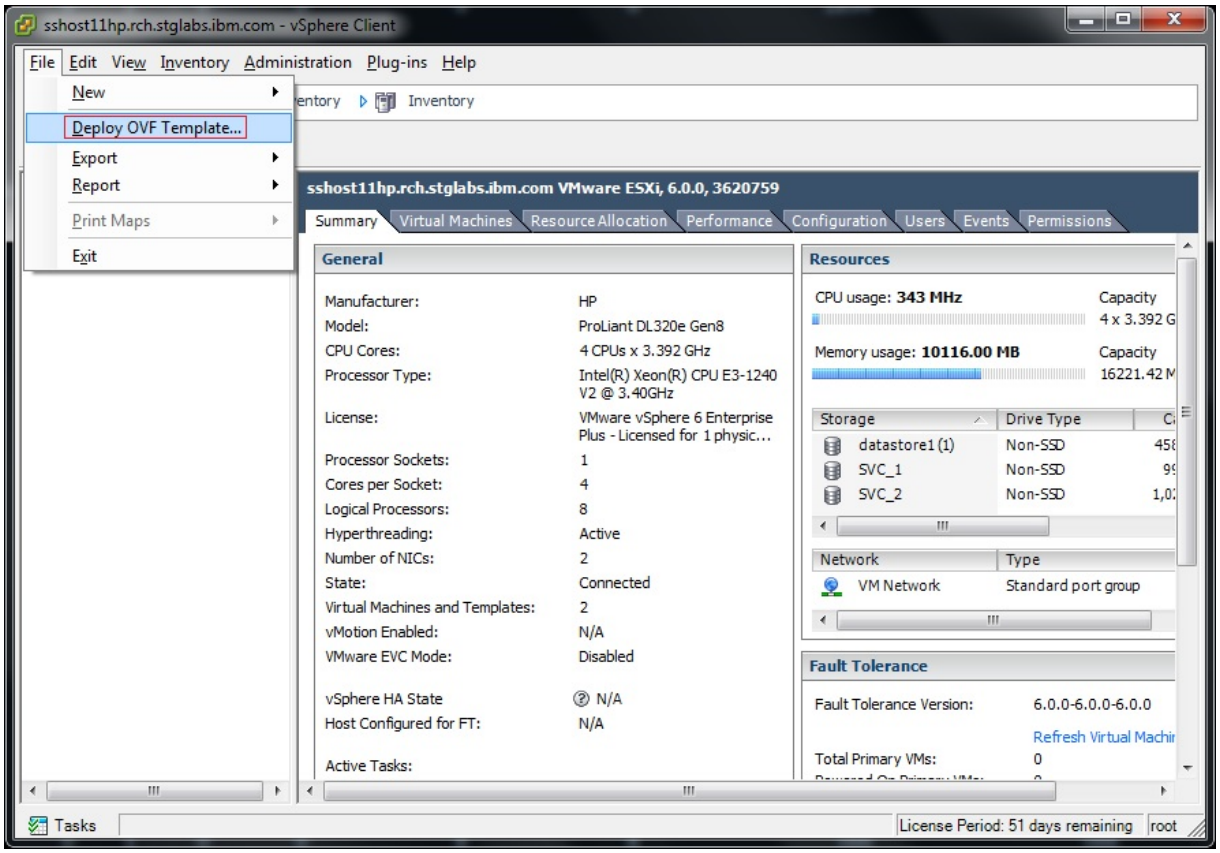

Figura 89. Desplegar plantilla de OVF

4. Pulse **Examinar** y seleccione la imagen que está guardada en el sistema.

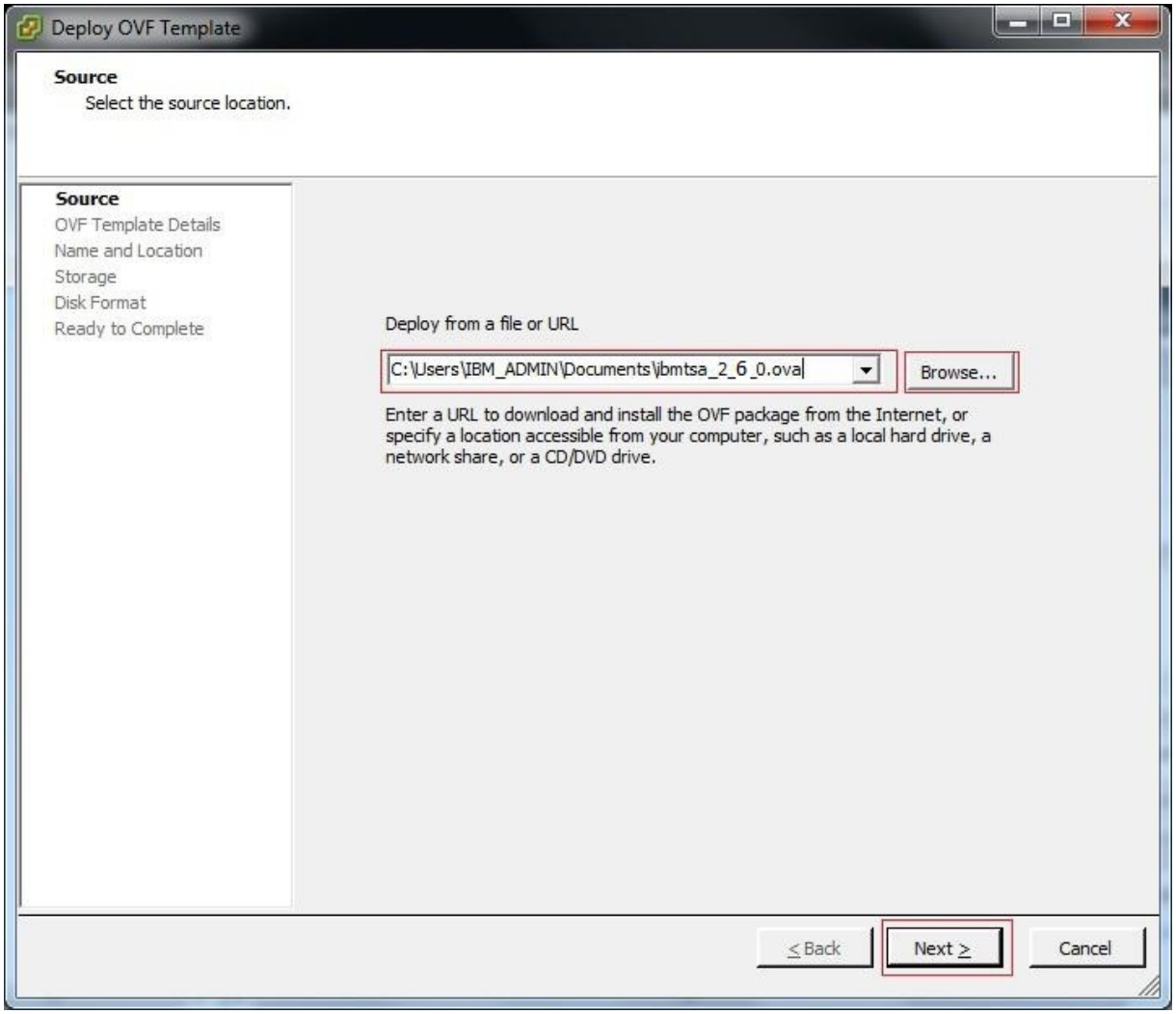

Figura 90. Origen de plantilla de OVF

5. Pulse **Siguiente**. Aparecen los **Detalles de plantilla de OVF**.
6. Pulse **Siguiente**. Aparece el panel **Nombre y ubicación**.

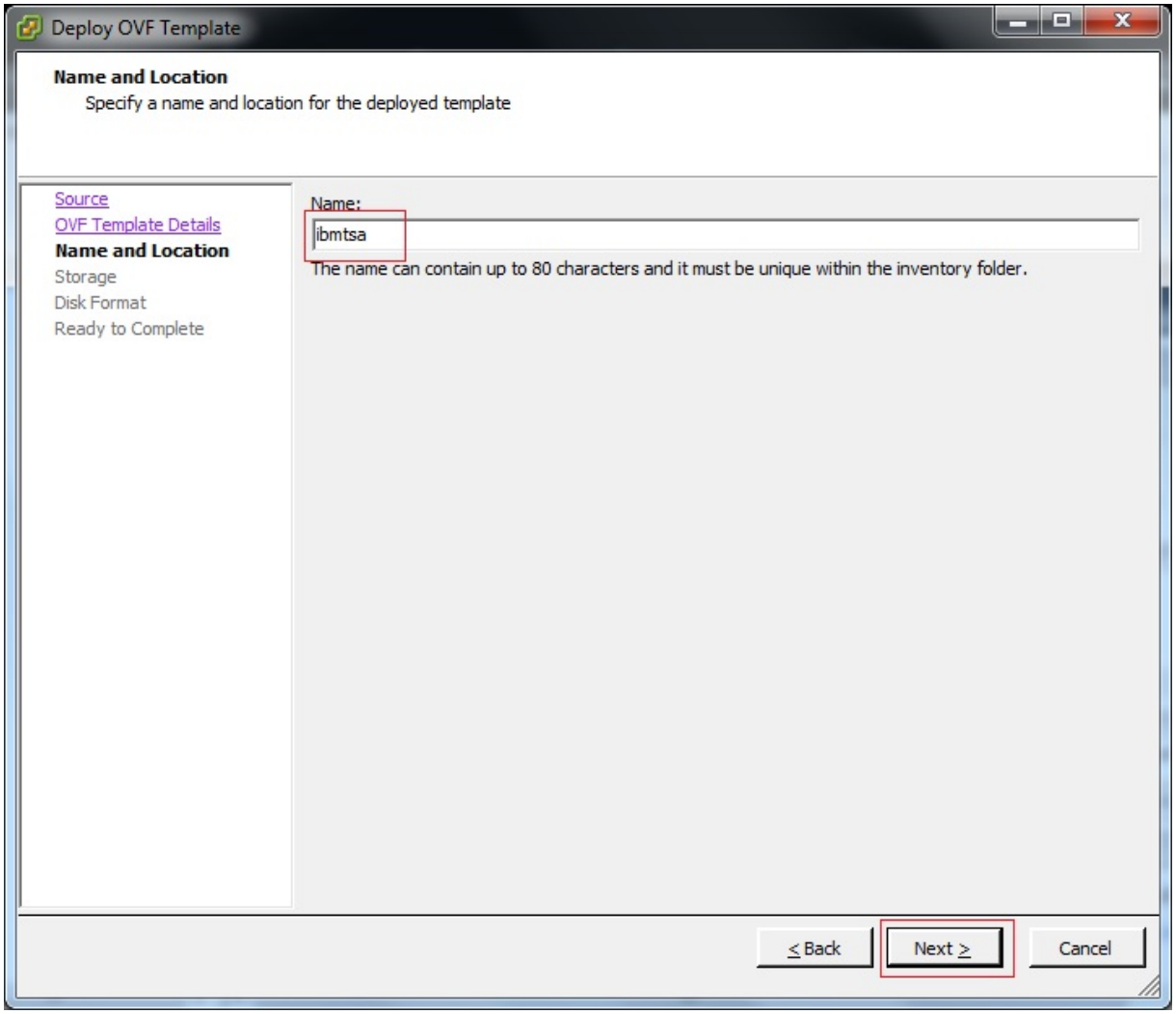

Figura 91. Nombre y ubicación

7. En el panel **Nombre y ubicación**, indique el **Nombre** de la máquina virtual, o bien utilice el valor predeterminado, y pulse **Siguiente**.
8. En el panel **Almacenamiento**, seleccione el almacén de datos (almacenamiento para los archivos de máquina virtual) y pulse **Siguiente**.

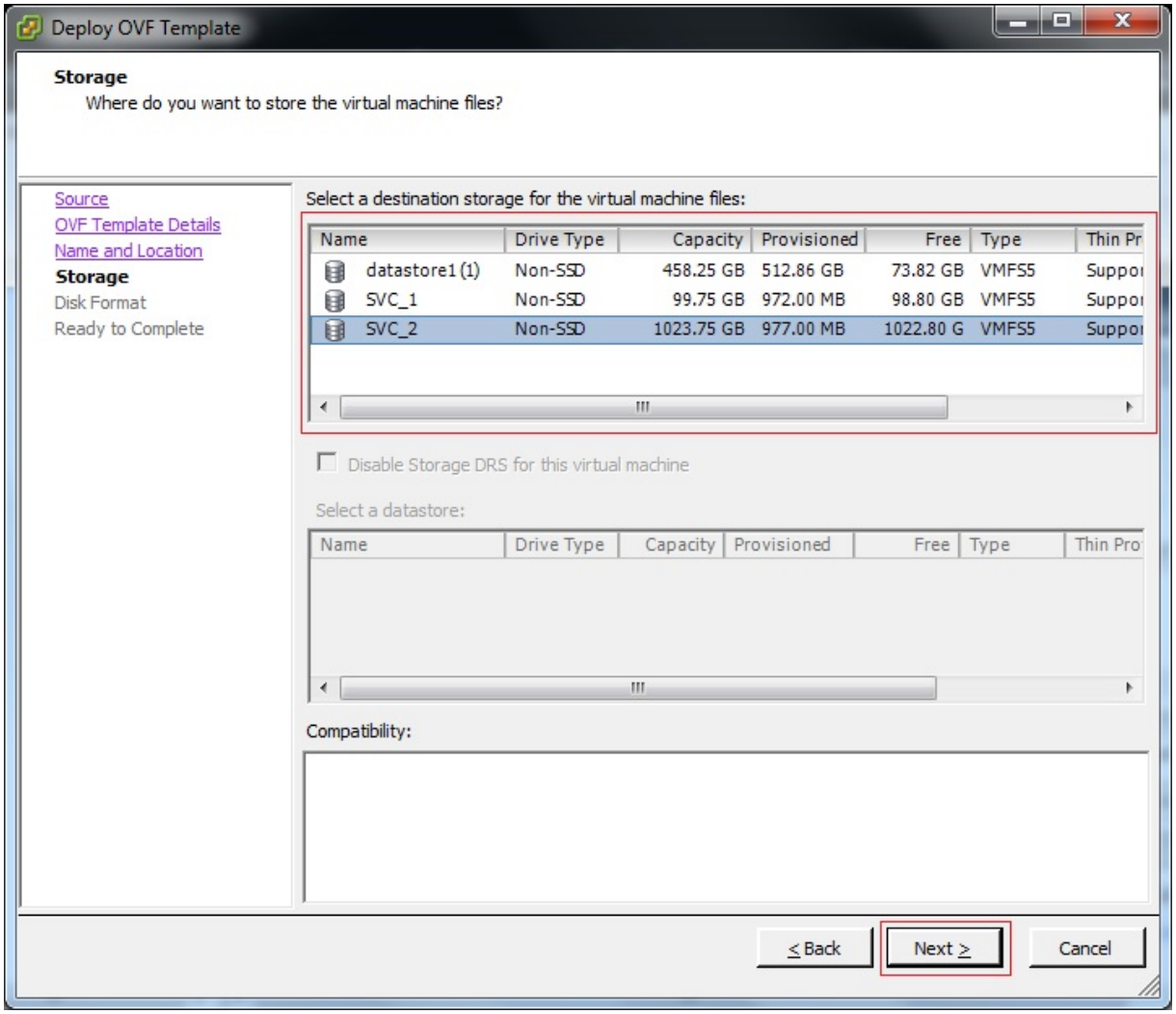

Figura 92. Almacenamiento

9. En el panel **Formato de disco**, seleccione la opción **Puesta a cero rápida con aprovisionamiento grueso** y pulse **Siguiente**.

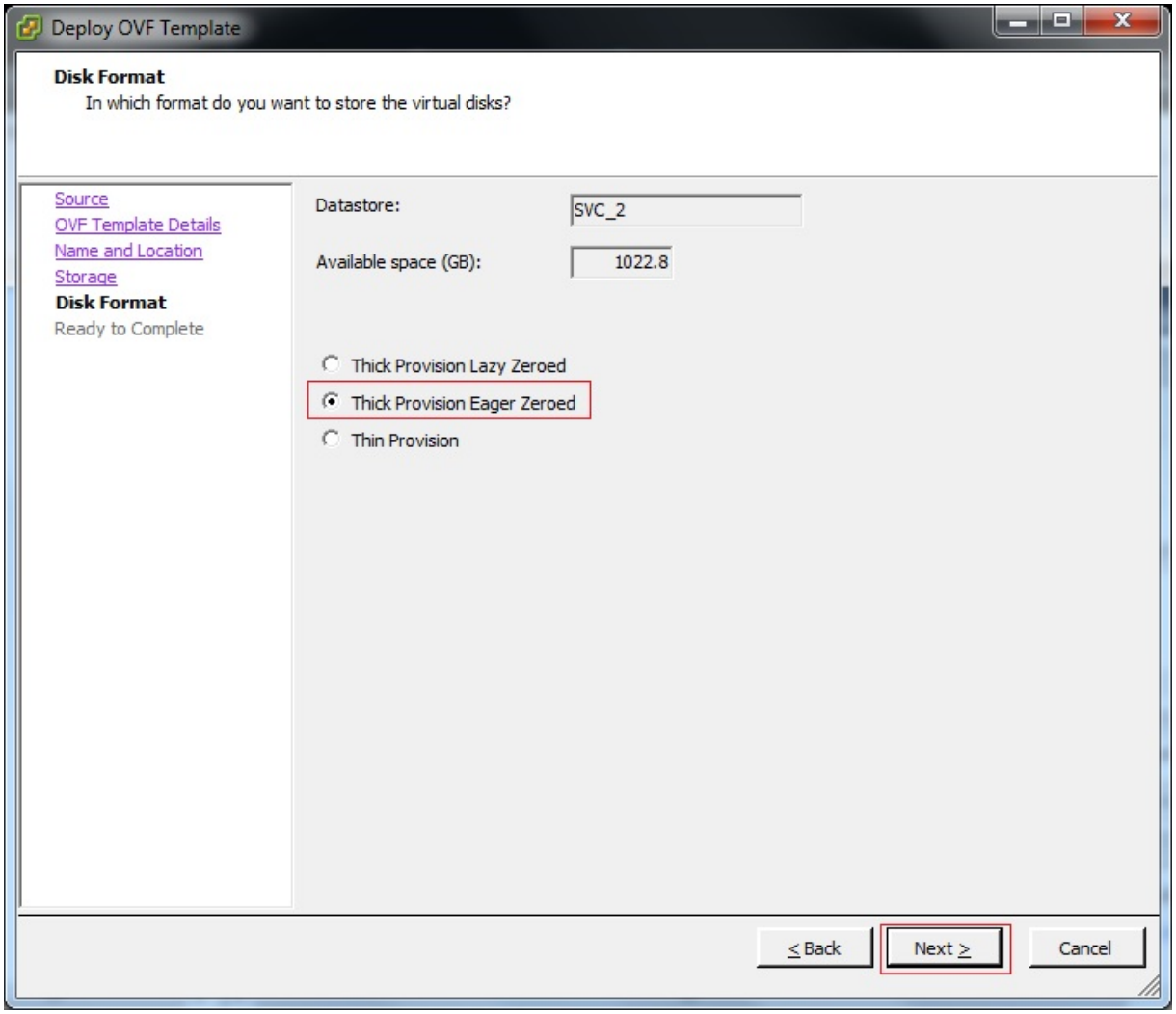

Figura 93. Formato de disco

10. Si ESXi tiene una única conexión de red, continúe en el paso siguiente. De otro modo, seleccione la red que corresponda en el panel **Correlación de red** y pulse **Siguiente**.
11. Opcional: Seleccione la opción **Encender tras el despliegue** para encender la máquina virtual automáticamente tras el despliegue. También puede encender manualmente la máquina virtual al finalizar el despliegue.

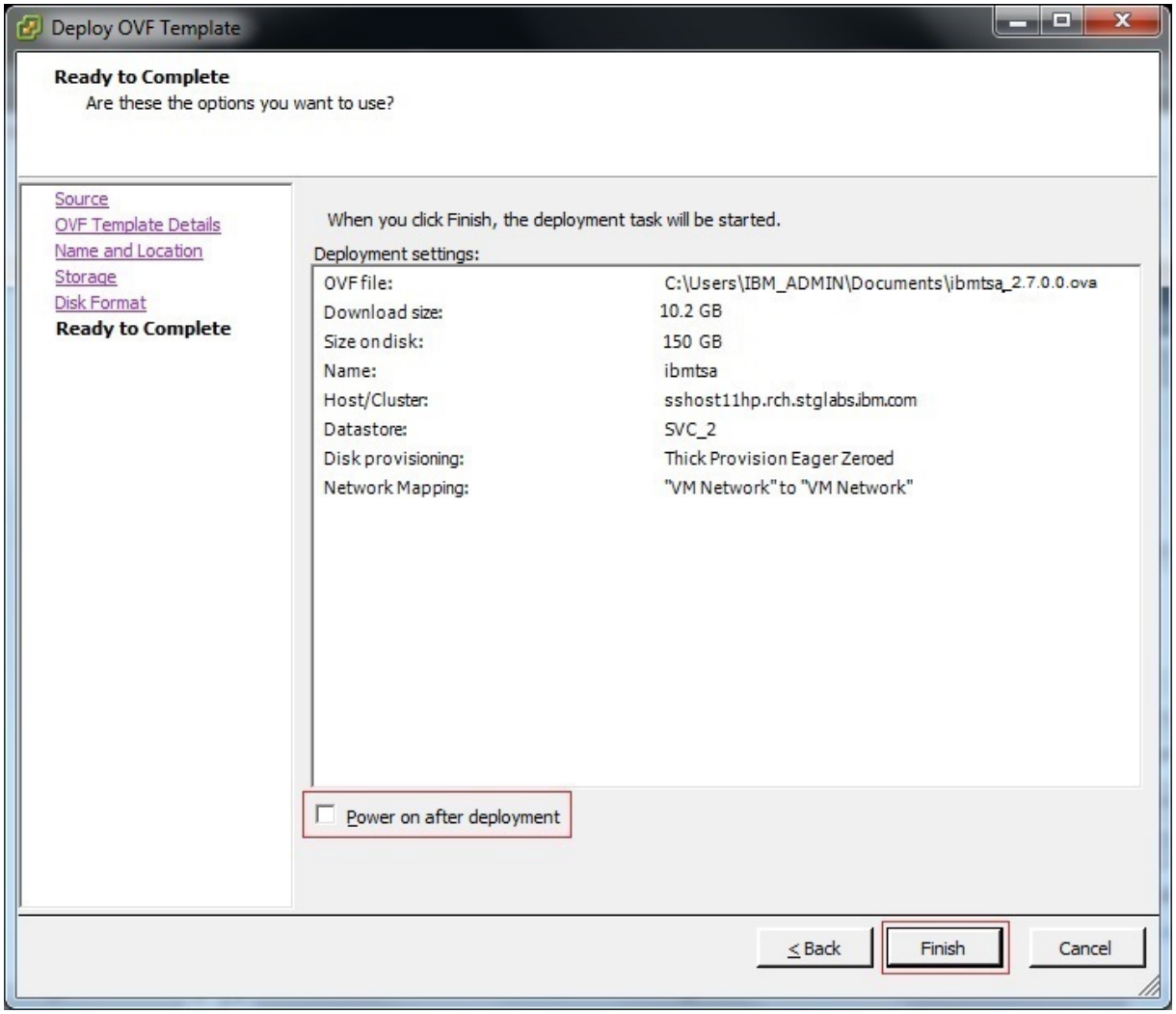

Figura 94. Listo para finalizar

12. Pulse **Finalizar**. El despliegue de TSA puede tardar unos 30 minutos en realizarse, pero varía en función de la velocidad de la conexión de red entre el sistema del usuario y el sistema VMware ESXi.
13. Una vez realizado correctamente el despliegue de TSA, seleccione la nueva máquina virtual desplegada y pulse la pestaña **Consola** de vSphere Client.
14. Inicie sesión en la consola de TSA y realice la configuración de red. En **ibmtsa login**, indique **`tsausr`**, y en **Password**, indique **`configTsa`**.
15. Necesario: Para cambiar la contraseña de inicio de sesión, continúe con la lista de pasos de la sección “Cambio de contraseña de tsausr (necesario)” en la página 19.
16. Para finalizar la instalación, continúe con la lista de pasos de la sección “Configuración de los datos de red” en la página 19.

Apéndice B. Configuración de Technical Support Appliance

Si sale u omite la configuración de alguno de los valores en el **Asistente de instalación**, puede configurarlos manualmente en el menú de navegación de la izquierda de TSA.

Registrar el Technical Support Appliance

El registro recopila información necesaria para identificar el TSA cuando éste pasa información a IBM para su análisis.

Acerca de esta tarea
Para registrar, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Registro**.
   Se muestra la página **Registro**.

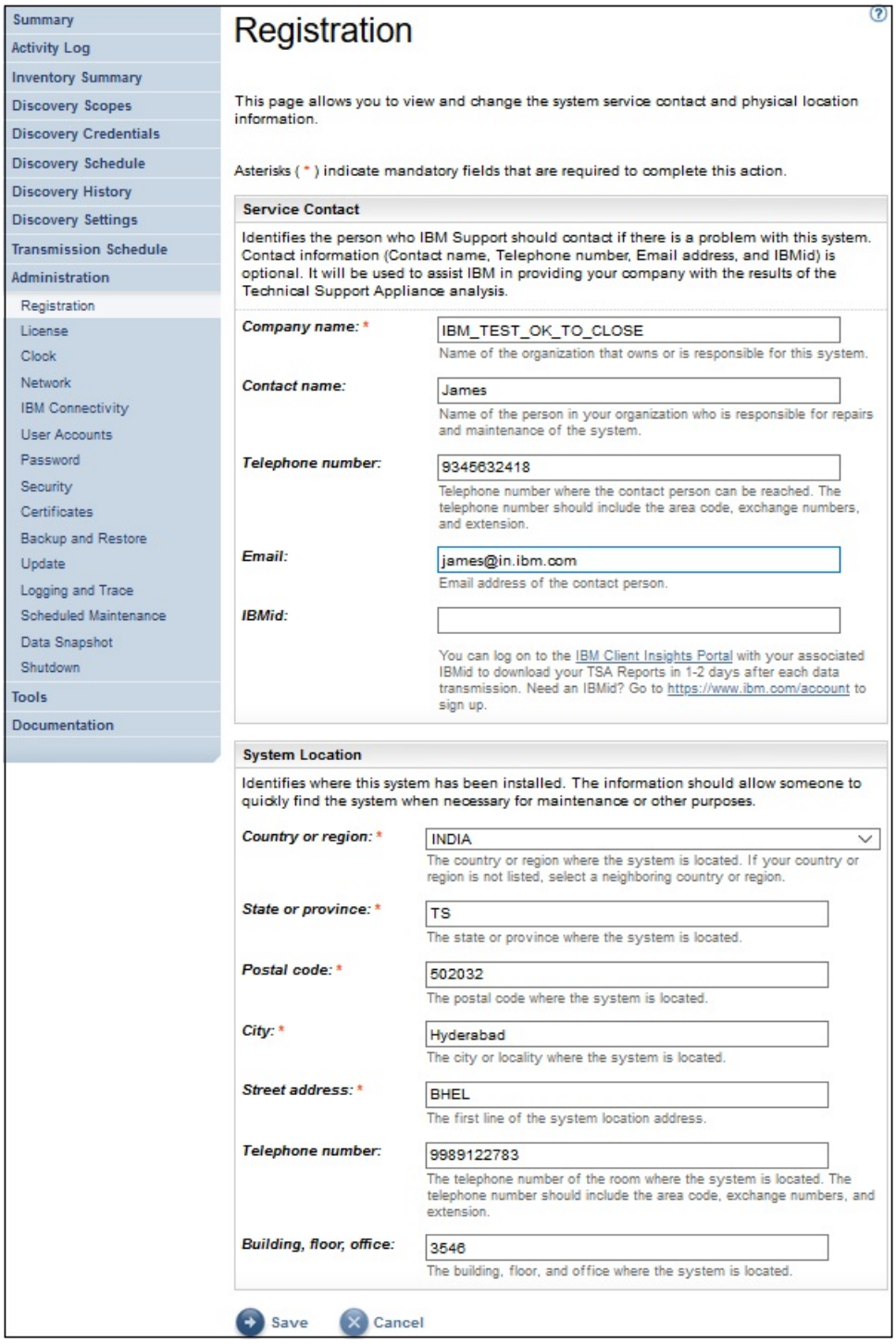

Figura 95. Registro

2. Especifique la información de contacto del servicio en los siguientes campos:

Nombre de la empresa
El nombre de la organización que utiliza TSA.

Nombre del contacto
(Opcional) El nombre de la persona de la organización responsable de TSA.

Número de teléfono
(Opcional) El número de teléfono donde se puede localizar a la persona de contacto. El número de teléfono debe incluir el código de área, los números de intercambio y la extensión. No utilice paréntesis en el número de teléfono.

Correo electrónico
(Opcional) La dirección de correo electrónico de la persona de contacto.

IBMid
(Opcional) El IBMid de la persona a la que desea dar autorización para ver los informes de IBM Client Insights Portal.

Nota: Puede iniciar sesión en https://clientinsightsportal.ibm.com/ con su IBMid asociado para descargar los informes de TSA pasados 1-2 días de cada transmisión de datos. Para registrarse para obtener un IBMid, vaya a https://www.ibm.com/account.

Nota: El contacto de servicio identifica a la persona con la que el servicio de soporte de IBM se debe poner en contacto si hay algún problema con el sistema. La información de contacto se utiliza para ayudar a IBM a proporcionar a la empresa los resultados del análisis del Technical Support Appliance.

3. Especifique la información de la ubicación del TSA en los siguientes campos:

País o región
El país o región donde se encuentra TSA.

Estado o provincia
El estado o la provincia donde se encuentra TSA. Si no está seguro del estado, escriba *Desconocido*.

Código postal
El código postal donde se encuentra el TSA.

Ciudad
La ciudad o la localidad donde se encuentra TSA.

Dirección postal
La dirección de la ubicación de TSA.

Número de teléfono
(Opcional) El número de teléfono de la sala donde se encuentra TSA. El número de teléfono debe incluir el código de área, los números de intercambio y la extensión. No utilice paréntesis en el número de teléfono.

Edificio, planta, oficina
(Opcional) El edificio, la planta y la oficina donde se encuentra TSA.

4. Pulse **Guardar** para guardar la información de registro.

Configurar la conectividad con IBM

Especifique la información de conexión a Internet a utilizar al conectar con IBM.

Antes de empezar
Asegúrese de que su cortafuegos permite conexiones a las direcciones IP y el nombre de host de servidor de IBM, tal como se explica en Tabla 1 en la página 6. Si la red no permite el acceso a los servidores de IBM, las transacciones de TSA al servicio de soporte de IBM no se podrán realizar.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Conectividad de IBM**.

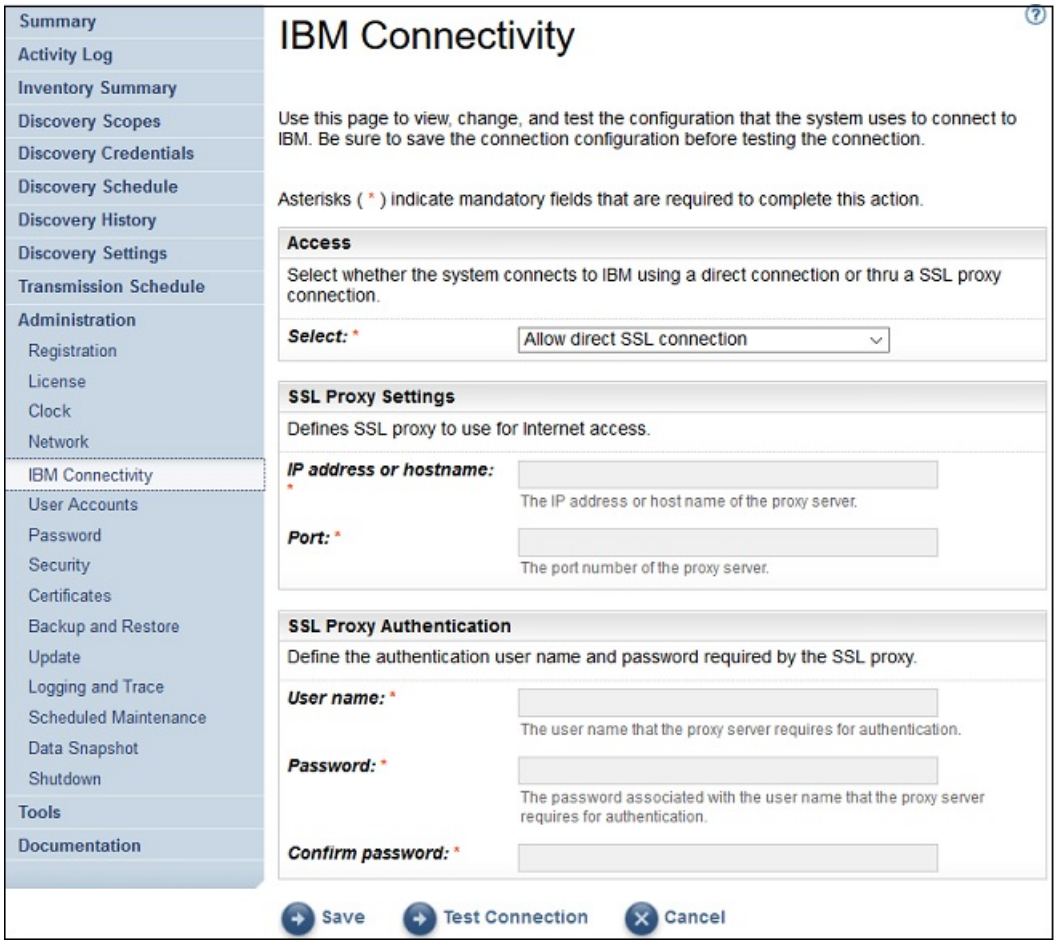

Figura 96. Conectividad de IBM

2. En el panel **Acceso**, seleccione uno de los siguientes tipos de acceso a Internet:

   Permitir conexión SSL directa
   TSA se conecta a IBM utilizando una conexión directa.

   Utilizar conexión proxy SSL
   TSA se conecta a IBM utilizando una conexión proxy SSL.

   Utilizar conexión proxy SSL de autenticación
   TSA se conecta a IBM utilizando una conexión proxy SSL de autenticación.

3. Si selecciona **Utilizar conexión proxy SSL** o **Utilizar conexión proxy SSL de autenticación**, especifique la siguiente información del servidor proxy:

   Dirección IP o nombre de host
   La dirección IP o el nombre de host del servidor proxy.

   Nota: El nombre de host que especifique no puede contener ningún guión bajo ("_").

   Puerto
   El número de puerto del servidor proxy.

4. Si selecciona **Utilizar conexión proxy SSL de autenticación**, especifique la siguiente información del servidor proxy:

   Nombre de usuario
   El nombre de usuario que requiere el servidor proxy para la autenticación.

   Contraseña
   La contraseña asociada al nombre de usuario que requiere el servidor proxy para la autenticación.

Confirmar contraseña
Vuelva a escribir la contraseña. Las dos contraseñas que introduzca se comparan para confirmar que coinciden antes de guardar la contraseña.

5. Pulse **Guardar** para guardar la información de conexión a IBM.
6. Pulse **Probar conexión** para probar la conexión especificada.

Importante:

- Guarde la configuración de conexión antes de probar la conexión.
- Debe tener una conexión con IBM operativa, si no, las funciones de TSA no funcionarán.

Conceptos relacionados

Requisitos de configuración para las conexiones al servicio de soporte de IBM
TSA se puede conectar al servicio de soporte de IBM a través de una conexión directa o mediante un proxy proporcionado por el usuario que debe configurar para permitir la comunicación con IBM. Si utiliza un proxy, no se admite la inspección TLS/SSL. Las solicitudes que vayan por un proxy deben poder fluir directamente a IBM sin terminación TLS/SSL.

Configurar el reloj

Debe definir la hora del sistema de TSA, la fecha y el huso horario local durante la configuración.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Reloj**.
   Se muestra la página **Reloj**.

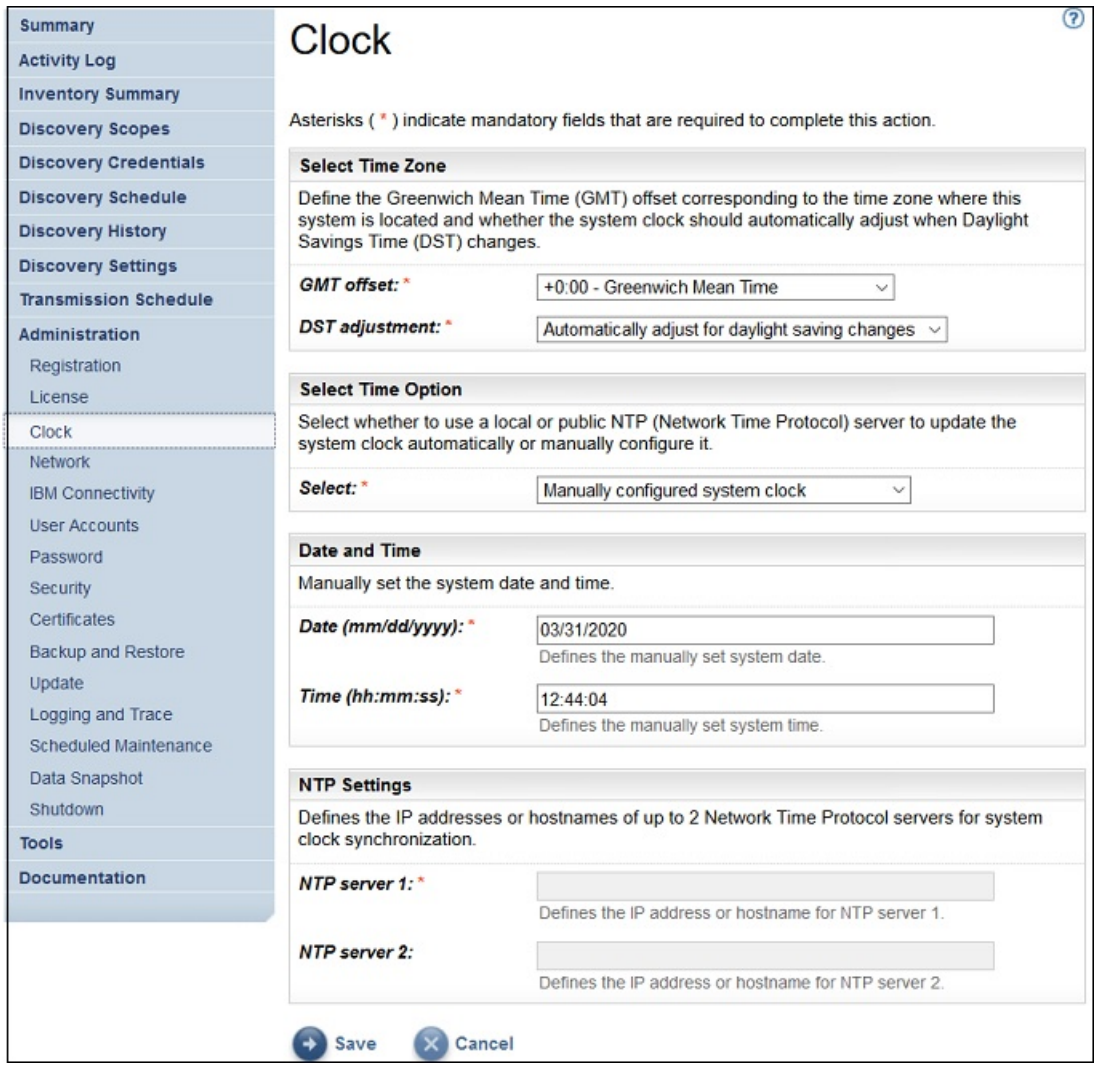

Figura 97. Reloj

2. Seleccione el huso horario local en la lista desplegable **Diferencia GMT**.
3. Seleccione el ajuste de horario de verano (DST - Daylight Saving Time) en la lista desplegable **Ajuste de DST**.

   Nota: No todos los husos horario tienen horario de verano. Si se selecciona esta opción para un huso horario que no admite DST, se muestra un mensaje de error.
4. Seleccione un método para actualizar el reloj del sistema en la lista desplegable **Seleccionar opción de hora**.

   Entre las opciones se incluye sincronizar el reloj del sistema con un servidor NTP (Network Time Protocol) para actualizar el reloj del sistema automáticamente, o configurar manualmente el reloj del sistema.

   a) Si selecciona configurar manualmente el reloj del sistema, debe definir la fecha y la hora del sistema. Indique la información de fecha y hora en los campos **Fecha** y **Hora**.

   b) Si selecciona sincronizar el reloj del sistema con un servidor NTP (Network Time Protocol) para actualizar el reloj del sistema automáticamente, debe especificar las direcciones IP y los nombres de host de los servidores NTP. Escriba la información de dirección IP o nombre de host de hasta dos servidores en los campos **servidor NTP**.

      Nota: Asegúrese de que el Servidor NTP es accesible a través de la red para TSA.
5. Pulse **Guardar** para guardar la información del reloj.

Resultados

Nota: Algunas modificaciones requieren reiniciar el sistema. Por ejemplo, si define la fecha o la hora, o cambia de configuración manual a configuración de servidor NTP, se le solicitará que reinicie el sistema.

Configuración de la planificación de transmisión

TSA proporciona una planificación predeterminada para ejecutar el proceso de transmisión a las horas especificadas. Puede modificar esta planificación según sus necesidades.

Procedimiento

1. En el panel de navegación, pulse **Planificación de transmisión**.
   Se mostrará la página **Planificación de transmisión**.

   En el panel **Planificación** se muestra la siguiente ejecución planificada y las horas de ejecución planificadas. En el panel **Historial** se muestra el estado y otros detalles del trabajo que hay actualmente en ejecución y de los trabajos de transmisión anteriores.
2. Pulse **Editar planificación**.
   Se mostrará la página **Planificación de transmisión**.

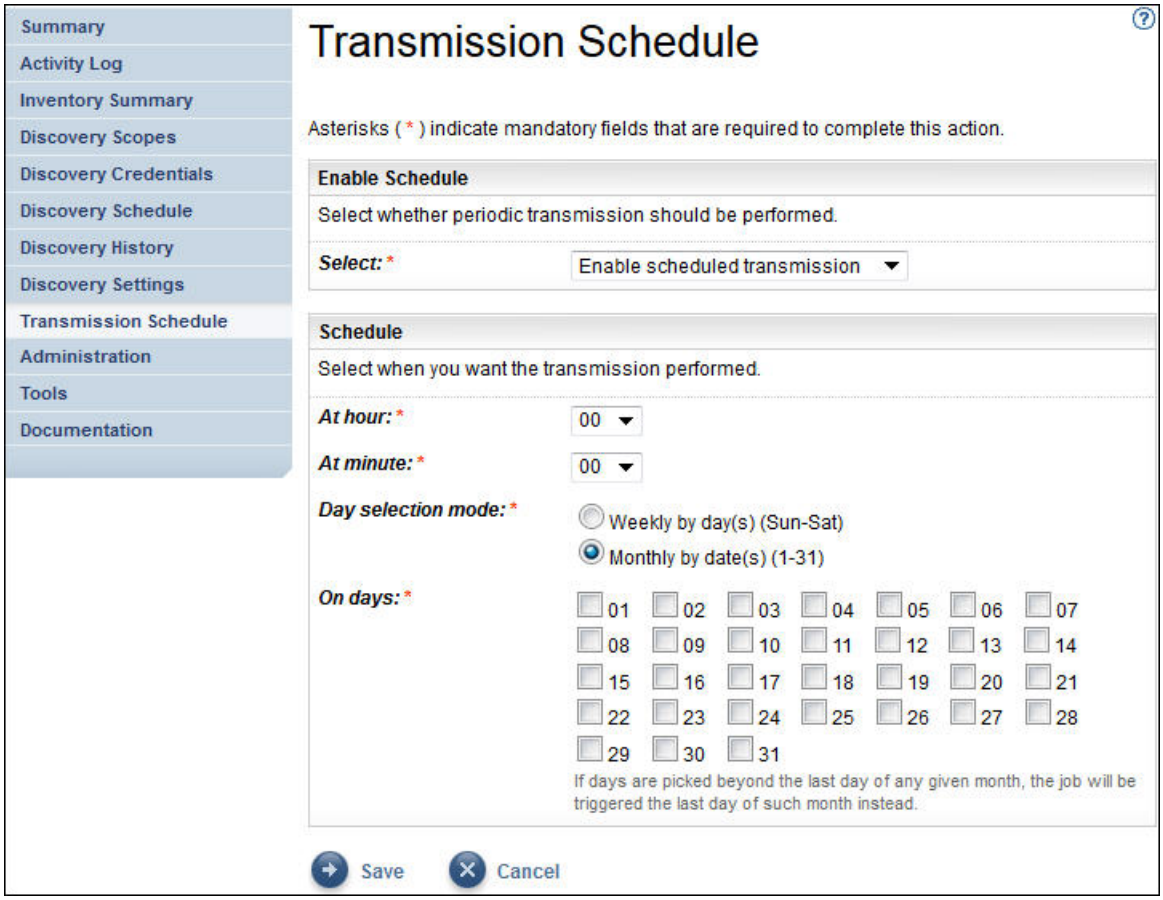

Figura 98. Editar planificación de transmisión

   a) Utilice las listas desplegables **A la hora** y **En el minuto** para seleccionar una nueva hora.

   b) Seleccione el **Modo de selección del día**.

   Semanalmente los días (dom - sáb)
   Para planificar la transmisión en un día o días concretos de la semana, seleccione la opción **Semanalmente los días (dom - sáb)**.

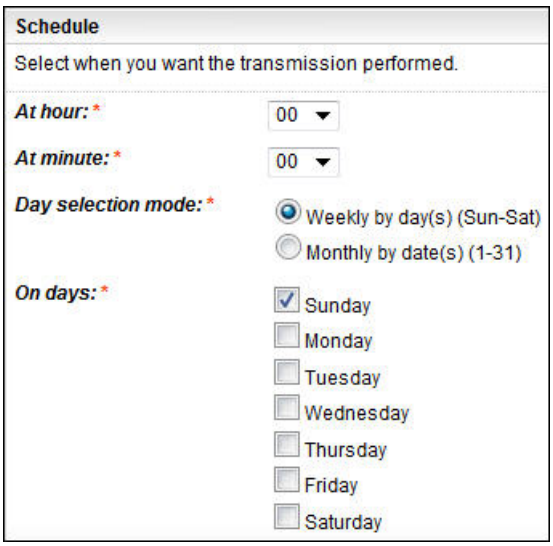

Figura 99. Semanalmente los días (dom - sáb)

En el campo **Los días**, seleccione los recuadros adecuados para seleccionar uno o más días de la semana.

Mensualmente los días (1-31)

Para planificar la transmisión en unos días concretos del mes, seleccione la opción **Mensualmente los días (1-31)**.

En el campo **Los días**, seleccione los recuadros adecuados para seleccionar uno o más días del mes.

Nota: Si selecciona los días más allá de un mes específico, el trabajo se activa el último día de ese mes en concreto.

3. Pulse **Guardar**.

   Se volverá a mostrar la página **Planificación de transmisión** con la nueva planificación.

Actualizar

Puede buscar y descargar actualizaciones para TSA.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Actualización**.

   Se muestra la página **Actualización**.

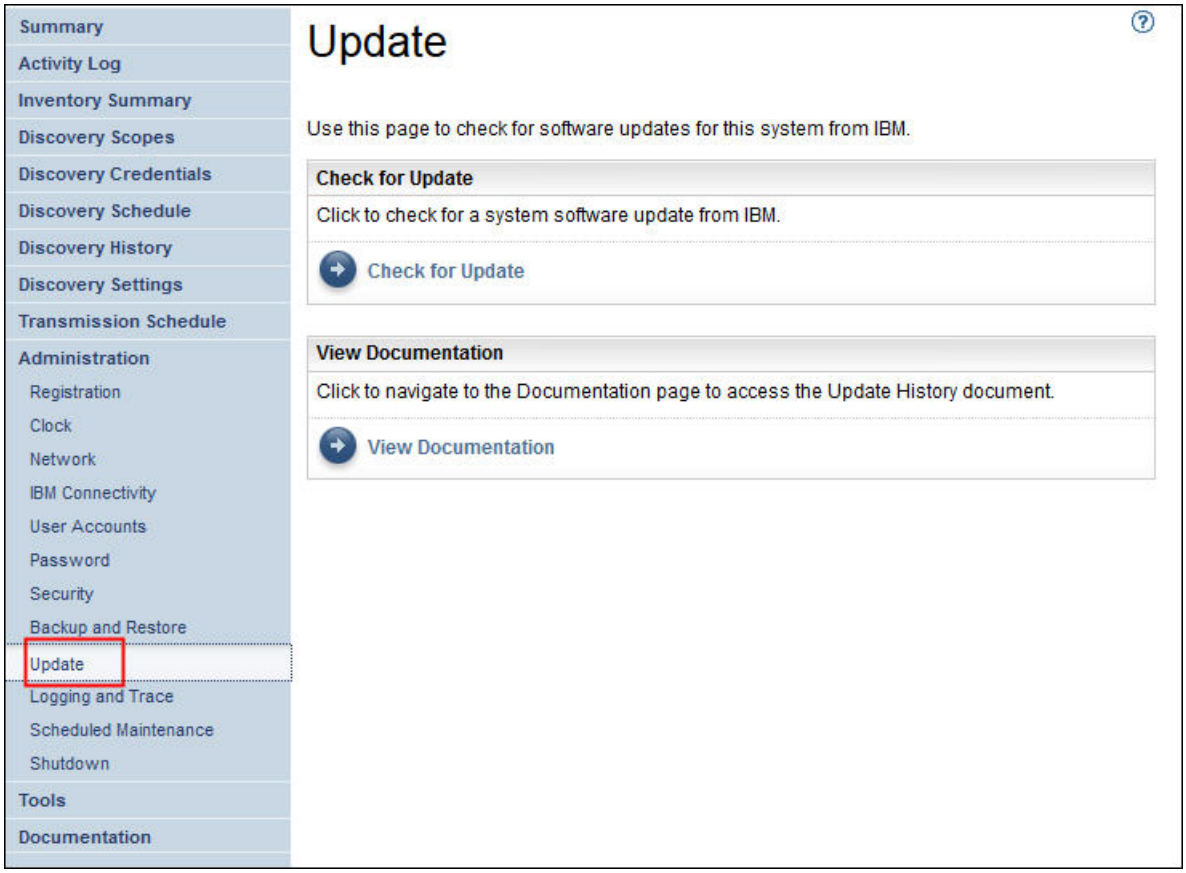

Figura 100. Actualizar

2. Pulse **Buscar actualizaciones**.

   Aparecen las actualizaciones disponibles en la página **Disponibilidad de actualizaciones**.

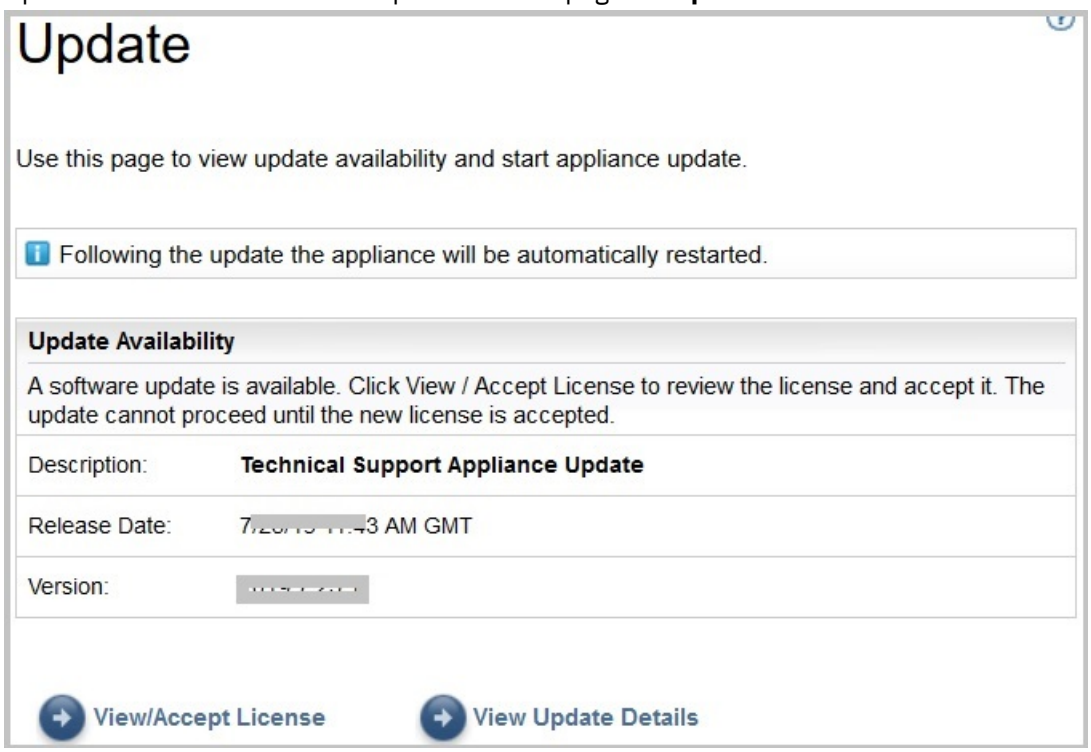

Figura 101. Disponibilidad de actualizaciones

a) En algunos releases de TSA, debe aceptar un nuevo acuerdo de licencia antes de proceder con la actualización. Si hay una nueva licencia, pulse **Ver/Aceptar licencia** y aparecerá la página **Acuerdo de licencia**.

b) Pulse el botón **Aceptar** en la página **Acuerdo de licencia** para aceptar el nuevo Acuerdo de licencia. Se muestra de nuevo la página **Actualizar** con el botón **Realizar actualización ahora**. Si no se requiere aceptar un nuevo acuerdo de licencia, no se muestra el botón **Ver/Aceptar licencia**; pulse **Realizar actualización ahora** para continuar.

Nota:

- Una vez que acepta la licencia, deja de visualizarse el botón **Ver/Aceptar licencia**.
- En el panel de navegación, pulse **Administración** > **Licencia** para ver el Acuerdo de licencia más reciente que ha aceptado.

c) Para instalar las actualizaciones, pulse **Realizar actualización ahora**.

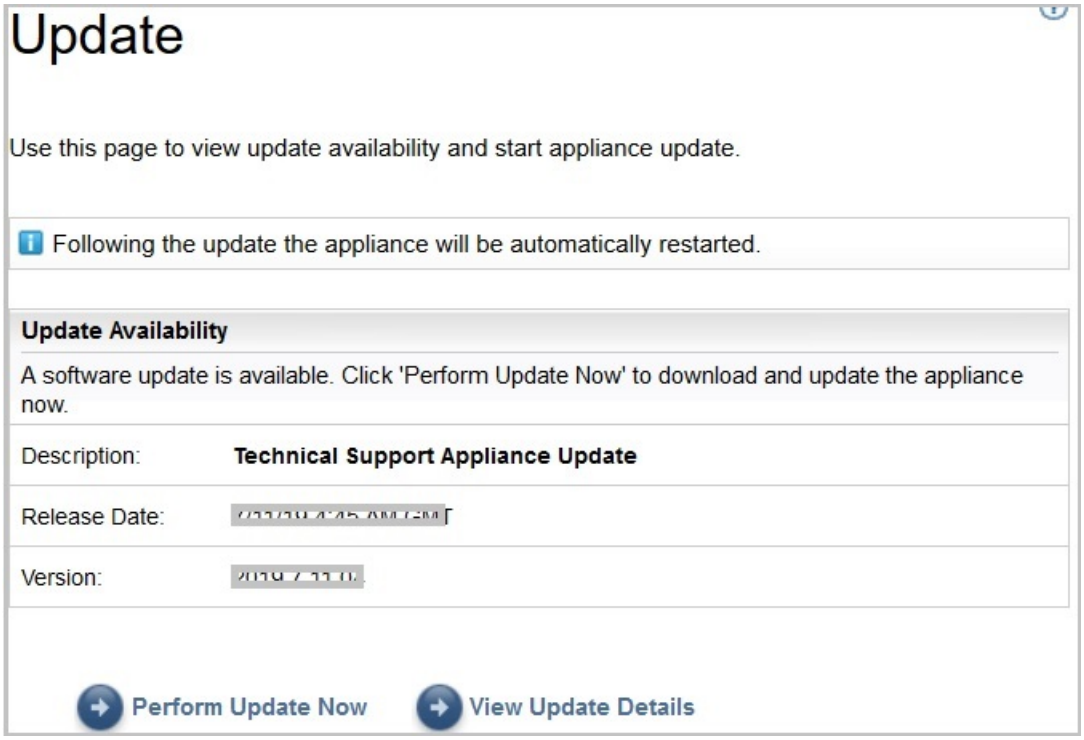

Figura 102. Realizar actualización ahora

Una vez completada la actualización, TSA se reinicia automáticamente.

d) Para ver información sobre el contenido de la actualización, pulse **Ver detalles de actualización**.

Apéndice C. Configuración de los datos de red DHCP

Siga estos pasos para configurar los detalles de la red DHCP:

Procedimiento

1. Seleccione la opción **1) Setup network configuration** en **TSA Config Menu**.

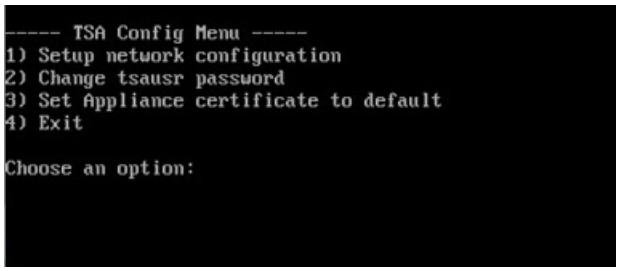

Figura 103. Realizar configuración de red

2. Indique los siguientes datos de configuración de red.

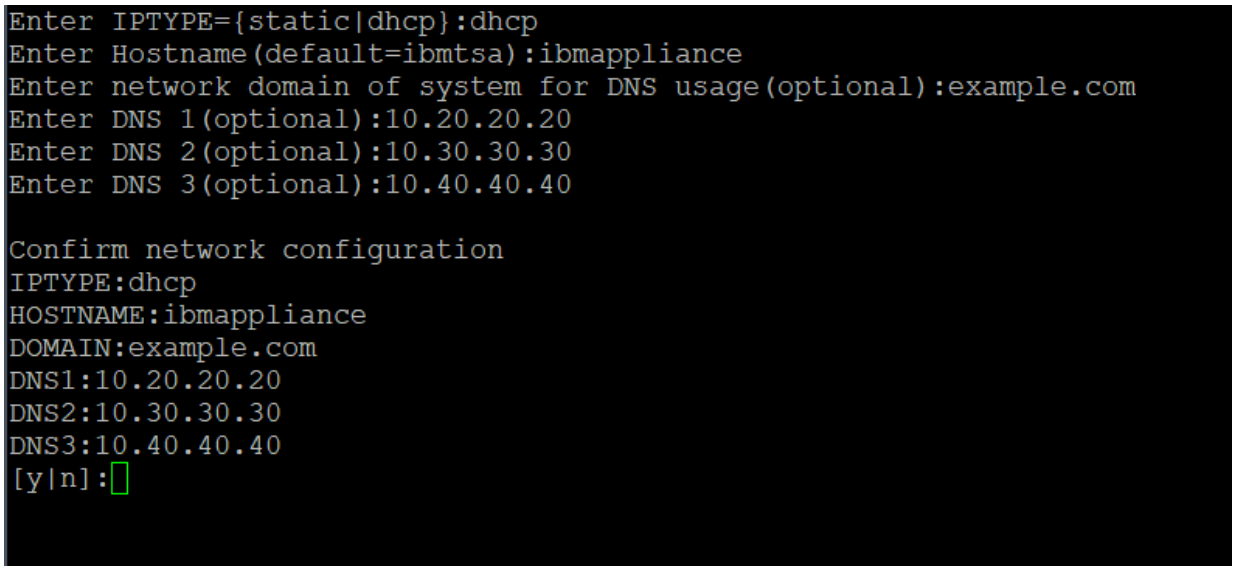

Figura 104. Configuración de red

a) **Enter IPTYPE = {static|dhcp}**. Indique dhcp.

IPTYPE: dhcp

Enter Hostname(default=ibmtsa). Puede cambiar el nombre de host predeterminado. El nombre de host que utilice debe ser exclusivo.

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

Enter DNS 1(optional), **Enter DNS 2(optional)** y **Enter DNS 3(optional)**.

Los datos de configuración de red especificados se muestran para confirmarlos.

b) Indique **[y|n]** para confirmar o descartar la configuración de red. Al indicar **y**, se guarda la configuración de red y se reinicia el sistema automáticamente.

Nota: Si hay alguna configuración incorrecta, puede modificar los datos. Indique **n** para ignorar los valores actuales y reiniciar la configuración del paso "2.a" en la página 133.

c) El sistema rearranca a los 15 segundos para que se aplique la nueva configuración de red.

d) Tras el rearranque del sistema, inicie una sesión en el gestor de virtualización y anote la **dirección IP** de la pestaña **Resumen**.

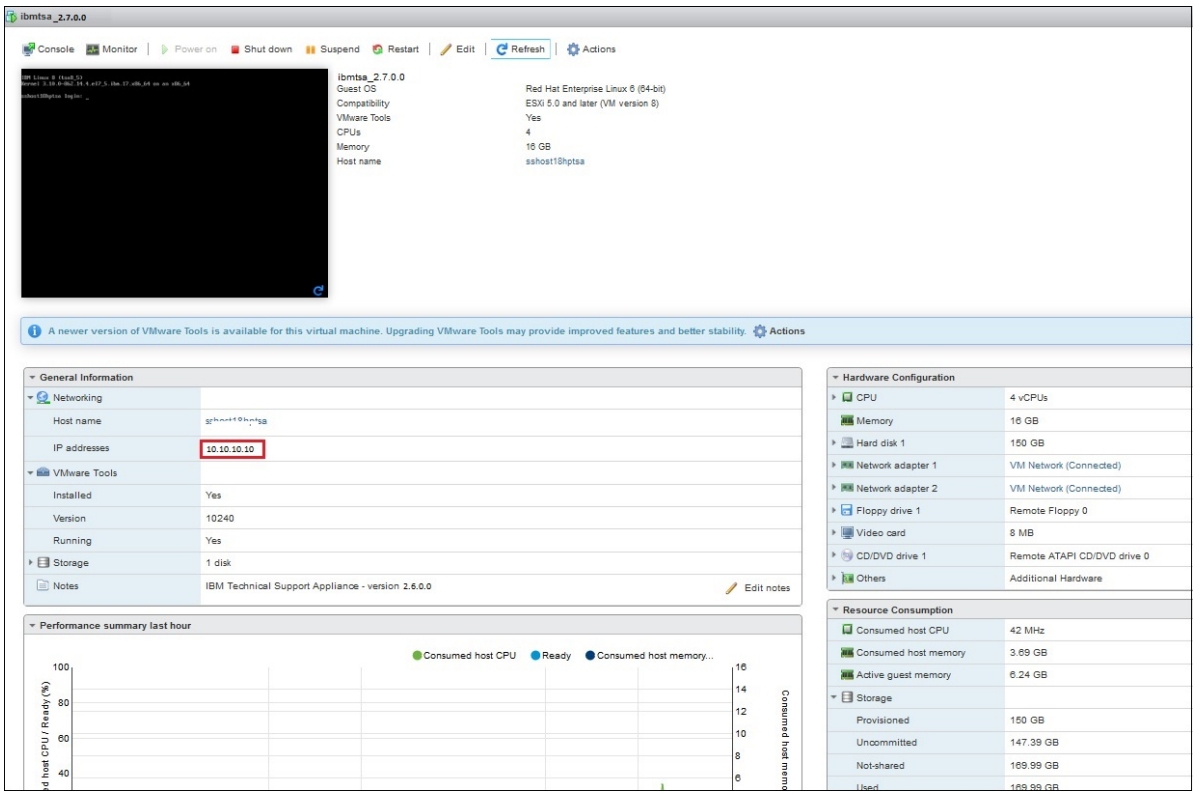

Figura 105. Dirección IP DHCP

e) Acceda a TSA desde el navegador con el URL que ha obtenido en el paso anterior.
Por ejemplo, `https://newhost1.new.abclabs.example.com`

Nota: La primera vez que se conecte, puede que el navegador muestre una excepción de seguridad. Debe aceptar el certificado de seguridad y continuar con el inicio de sesión de TSA.

Apéndice D. Cuentas de usuario y grupos de usuarios

Puede utilizar las cuentas de usuario y los grupos de usuarios para otorgar acceso a las funciones de TSA.

Antes de empezar

TSA se instala con una cuenta de usuario denominada **admin**. Esta cuenta tiene autoridad para ejecutar cualquier función de TSA. Puede añadir cuentas de usuario por los siguientes motivos:

- Permitir que un usuario actúe como copia de seguridad del usuario **admin**.
- Permitir que algunos usuarios accedan a una cantidad limitada de funciones en TSA.

Acerca de esta tarea

Para ejecutar cualquier función de TSA se requiere un cierto nivel de autorización. Si un usuario autenticado intenta llevar a cabo una función sin tener el nivel de autorización adecuado, se muestra un error y no se ejecuta la función.

En TSA, los niveles de autorización están asociados a grupos de usuarios. A los usuarios se les asigna la pertenencia a uno o más grupos de usuarios, y al ser miembros de esos grupos, los usuarios tienen el nivel de autorización para llevar a cabo ciertas funciones.

TSA tiene predefinido un grupo de usuarios **Administrador** y una cuenta de usuario **admin**. El grupo de usuarios **Administrador** tiene acceso no restringido a todas las funciones del sistema. La cuenta de usuario **admin** está asignada al grupo de usuarios **Administrador**.

Visualizar cuentas de usuario y grupos de usuarios

Puede visualizar las cuentas de usuario y los grupos de usuarios existentes.

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Cuentas de usuario**.
   Se muestra la página **Cuentas de usuario y grupos de usuarios**.
2. Para visualizar las cuentas de usuario existentes, pulse en la pestaña **Cuentas**.
   En la tabla Cuentas de usuario se muestran las cuentas de usuario.

   Consejo: Para ver la información detallada de una cuenta de usuario específica, pulse en el nombre de la cuenta de usuario. En el panel **General**, se muestra el nombre de usuario, el nombre completo y la descripción asociados a la cuenta de usuario seleccionada. Pulse el panel **Miembro de** en la derecha para ver los grupos de usuarios a los que pertenece esta cuenta de usuario.
3. Para visualizar los grupos de usuarios existentes, pulse en la pestaña **Grupos**.
   En la tabla Grupos de usuarios se muestran la¡os grupos de usuarios.

   Consejo: Para ver la información detallada de un grupo de usuarios específico, pulse en el nombre del grupo de usuarios. En el panel **General**, se muestra el nombre y el nivel de autorización asociados al grupo de usuarios. Pulse el panel **Restricciones de alcances** en la derecha para ver los conjuntos de alcances que el grupo de usuarios seleccionado puede descubrir. Pulse el panel **Miembros** para ver las cuentas de usuario asociadas a este grupo de usuarios.

Añadir cuentas de usuario y grupos de usuarios

Puede añadir cuentas de usuario y grupos de usuarios para controlar el acceso a las funciones de TSA.
Conceptos relacionados
Alcances de descubrimiento y Conjuntos de alcances

Los alcances de descubrimiento identifican los recursos que desea que TSA descubra. Los alcances de descubrimiento se agrupan en conjuntos de alcances de descubrimiento.

Añadir un grupo de usuarios

Puede añadir grupos de usuarios para controlar el acceso a las funciones de TSA.

Acerca de esta tarea

Para añadir un grupo de usuarios, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Cuentas de usuario**.
   Se muestra la página **Cuentas de usuario y grupos de usuarios**.
2. Pulse en la pestaña **Grupos**.

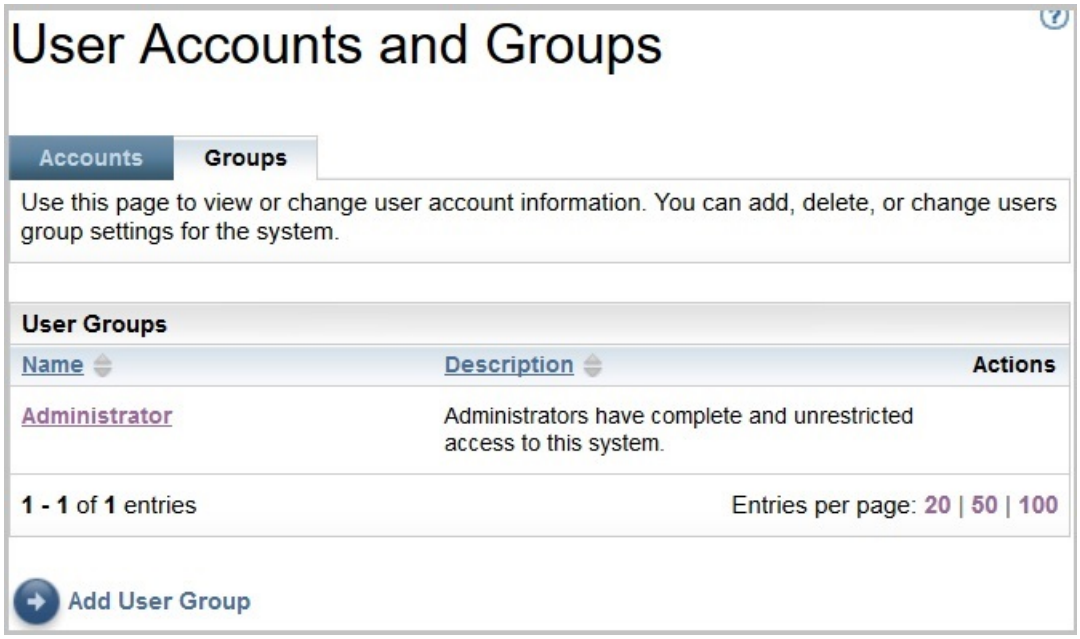

Figura 106. Grupos

3. Pulse **Añadir grupo de usuarios**.
   Se muestra la página **Grupo de usuarios**.

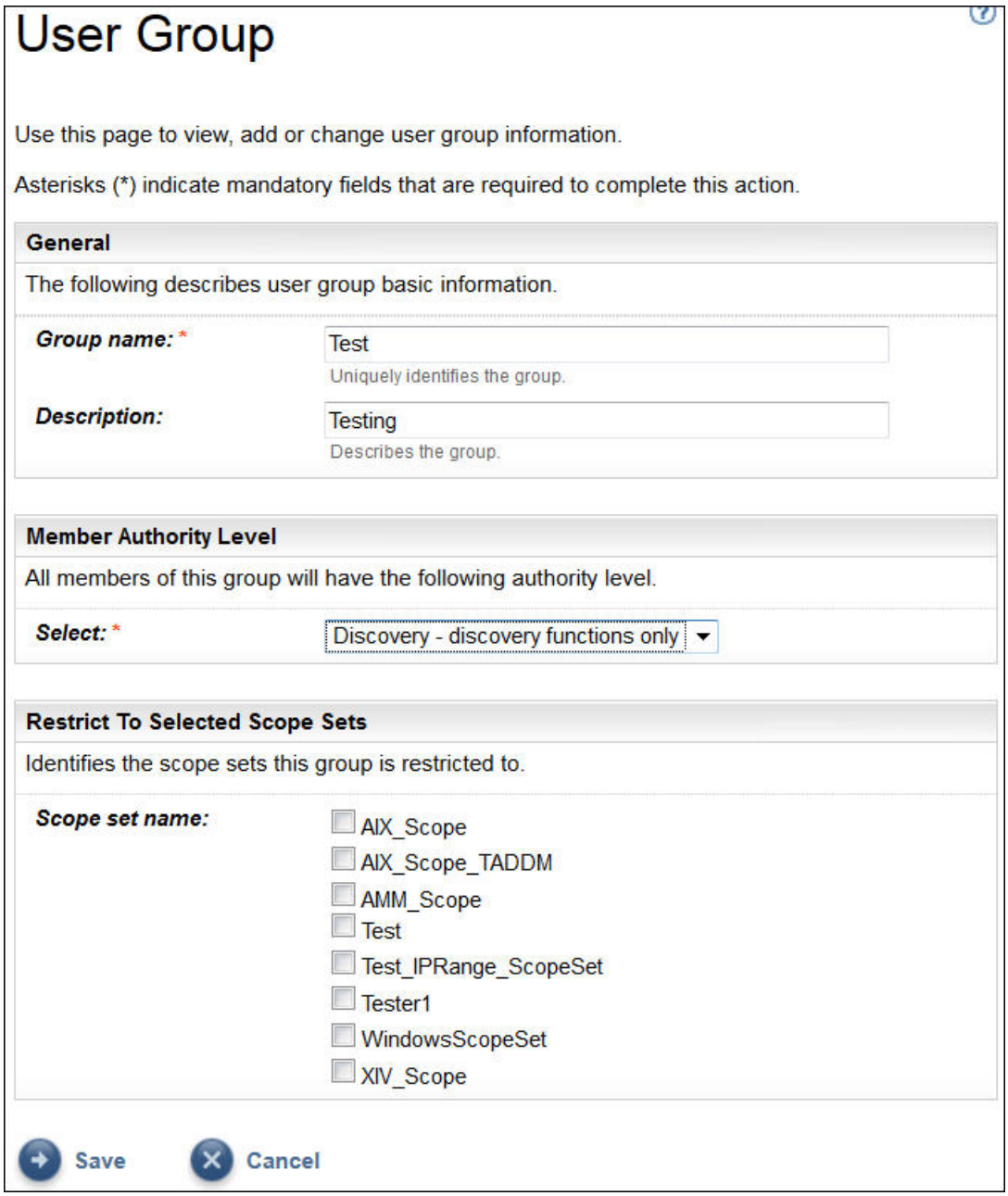

Figura 107. Añadir grupo de usuarios

4. En el campo **Nombre del grupo**, especifique un nombre exclusivo para este grupo de usuarios.
5. Opcional: En el campo **Descripción**, especifique una descripción para este grupo de usuarios.
6. Seleccione el nivel de autorización que desea que tengan los miembros de este grupo de usuarios.

   TSA define los siguientes niveles de autorización de grupo:

   - **Administrador** – sin restricciones
   - **Descubrimiento** – solo funciones de descubrimiento
   - **Visitante** – acceso solo de lectura
7. Si especifica el nivel de autorización *Descubrimiento* para este grupo de usuarios, debe seleccionar al menos un conjunto de alcances que esté restringido a este grupo de usuarios.

   Para obtener más información sobre conjuntos de alcances, consulte "Alcances de descubrimiento y Conjuntos de alcances" en la página 2.
8. Pulse **Guardar** para guardar el grupo de usuarios.

Se muestra la página **Cuentas de usuario y grupos de usuarios** con el nuevo grupo de usuarios en la lista.

Añadir una cuenta de usuario

Puede añadir cuentas de usuario para controlar el acceso a las funciones de TSA.

Acerca de esta tarea

Para añadir una cuenta de usuario, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Cuentas de usuario**.
   Se muestra la página **Cuentas de usuario y grupos de usuarios**.

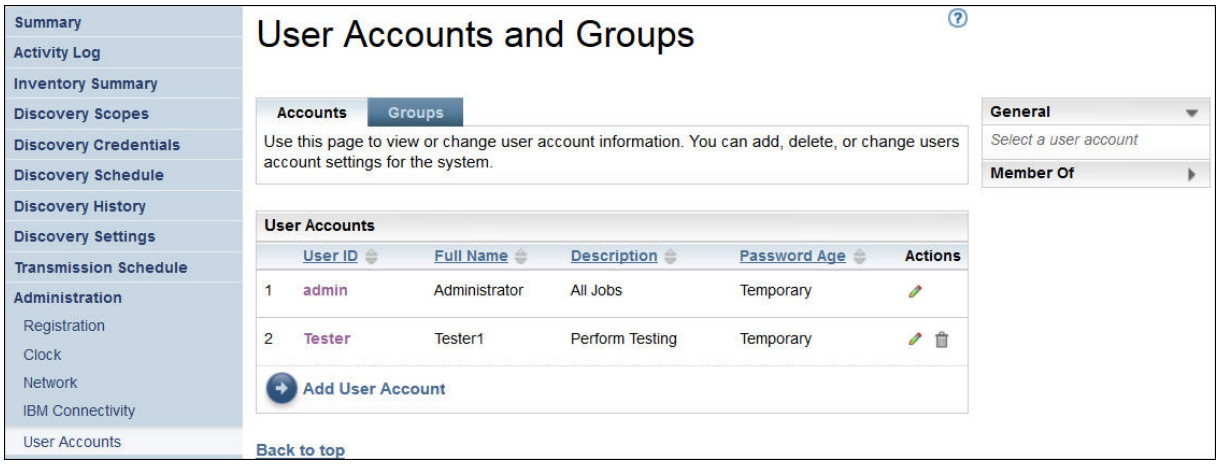

Figura 108. Cuentas de usuario y grupos de usuarios

2. Para definir una cuenta de usuario nueva, pulse **Añadir cuenta de usuario**.
   Se muestra la página **Cuenta de usuario**.

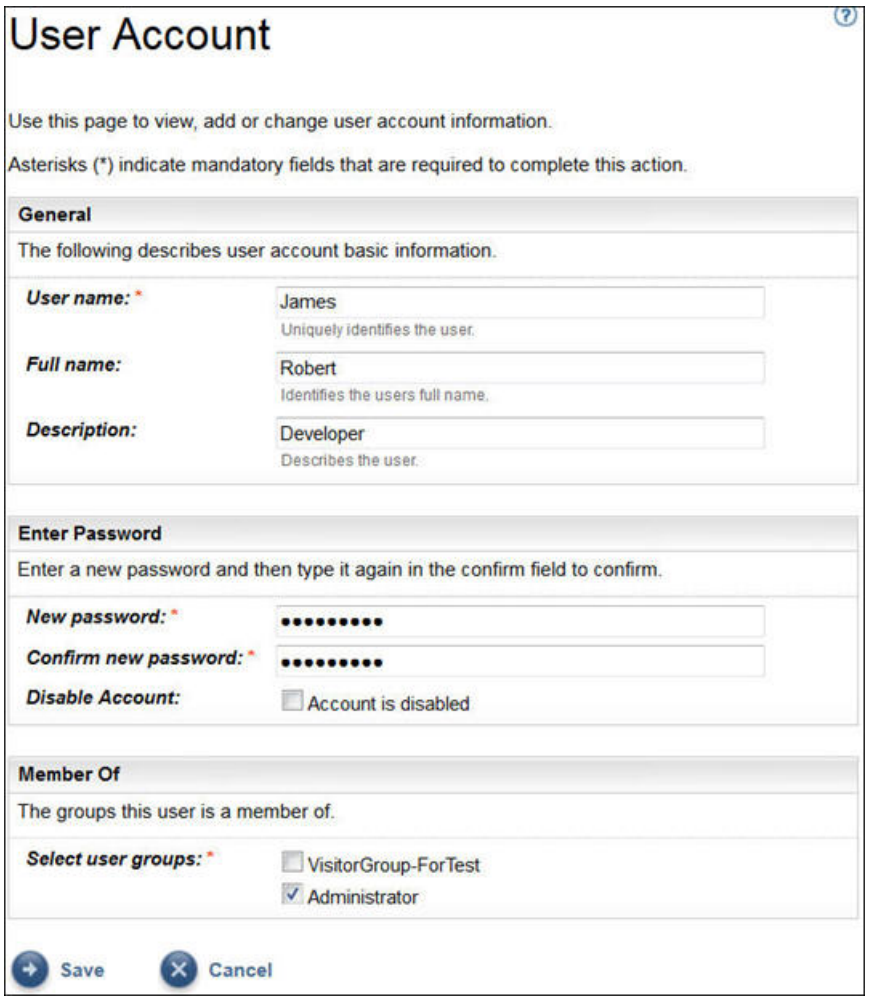

Figura 109. Añadir cuenta de usuario

3. En el campo **Nombre de usuario**, especifique un nombre para esta cuenta de usuario.
4. Opcional: En el campo **Nombre completo**, especifique el nombre completo del usuario de esta cuenta.
5. Opcional: En el campo **Descripción**, especifique una descripción para esta cuenta de usuario.
6. En el campo **Nueva contraseña**, especifique una contraseña para esta cuenta de usuario.

   La contraseña debe ajustarse a las reglas siguientes:

   - Debe tener como mínimo 8 caracteres de largo
   - Debe contener al menos un carácter alfabético y uno no alfabético
   - No puede contener el nombre de usuario
   - No puede ser igual que ninguna de las ocho contraseñas anteriores
   - Se debe cambiar al menos cada 30 días (de forma predeterminada) o según se haya especificado en la sección "Modificar la duración de la contraseña" en la página 102, pero no se puede cambiar más de una vez en un día.
7. En el campo **Confirmar contraseña**, vuelva a especificar la contraseña para esta cuenta de usuario.

   Las dos contraseñas que introduzca se comparan para confirmar que coinciden antes de guardar la contraseña.

   Nota: La contraseña se debe cambiar la primera vez que se inicie sesión en esta cuenta de usuario.
8. Si desea deshabilitar esta cuenta de usuario, seleccione el recuadro **La cuenta está deshabilitada**.

   Deshabilitar la cuenta permite impedir que se utilice sin necesidad de suprimirla.

   Nota: No puede deshabilitar la cuenta **admin** ni cambiar el grupo de la cuenta **admin**.

9. Seleccione los grupos de usuarios para esta cuenta de usuario. Debe seleccionar al menos un grupo de usuarios. El usuario tendrá el nivel de autorización que tengan definido los grupos que seleccione.
10. Pulse **Guardar** para guardar la cuenta de usuario.

    Se muestra la página **Cuentas de usuario y grupos de usuarios** con la nueva cuenta de usuario en la lista.

Modificar cuentas de usuario y grupos de usuarios

Puede modificar las cuentas de usuario y los grupos de usuarios existentes.

Modificar cuentas de usuario

Puede modificar las cuentas de usuario existentes.

Acerca de esta tarea

Para modificar una cuenta de usuario, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Cuentas de usuario**.

   Se muestra la página **Cuentas de usuario y grupos de usuarios**.
2. Pulse en la pestaña **Cuentas** y después pulse el icono **Editar** junto a la cuenta de usuario.

   Se muestra la página **Cuenta de usuario**.
3. En el panel **General**, puede modificar la información básica para esta cuenta de usuario.
4. En el panel **Introducir contraseña**, puede cambiar la contraseña y la información de administración de contraseñas. También puede deshabilitar esta cuenta de usuario.

   La contraseña debe ajustarse a las reglas siguientes:

   - Debe tener como mínimo 8 caracteres de largo
   - Debe contener al menos un carácter alfabético y uno no alfabético
   - No puede contener el nombre de usuario
   - No puede ser igual que ninguna de las ocho contraseñas anteriores
   - Se debe cambiar al menos cada 90 días, pero no se puede cambiar más de una vez al día.

   Nota: La contraseña se debe cambiar la primera vez que se inicie sesión en esta cuenta de usuario.
5. Si desea deshabilitar esta cuenta de usuario, seleccione **La cuenta está deshabilitada**.

   Deshabilitar la cuenta permite impedir que se utilice sin necesidad de suprimirla. Para obtener información sobre cómo suprimir una cuenta de usuario, consulte “Suprimir cuentas de usuario y grupos de usuarios” en la página 142.

   Nota: No puede deshabilitar la cuenta **admin** ni cambiar el grupo de la cuenta **admin**.

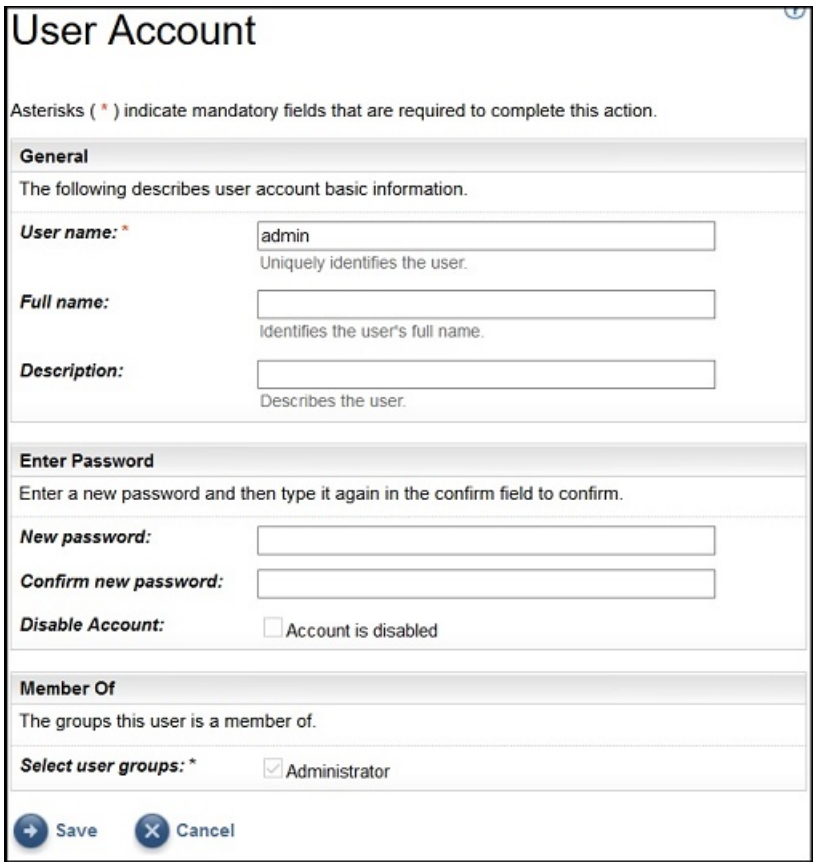

Figura 110. Modificar cuenta de usuario administrador

6. En el panel **Miembro de** puede cambiar los grupos de usuarios a los que pertenece esta cuenta de usuario. La cuenta de usuario debe ser miembro de al menos un grupo de usuarios.
7. Pulse **Guardar** para guardar los cambios.
   En la página **Cuentas de usuario y grupos de usuarios** se muestra la información modificada.

Modificar grupos de usuarios

Puede modificar los grupos de usuarios existentes.

Antes de empezar

Nota: No puede cambiar el grupo **Administrador**.

Acerca de esta tarea

Para modificar un grupo de usuarios, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Cuentas de usuario**.
   Se muestra la página **Cuentas de usuario y grupos de usuarios**.
2. Pulse en la pestaña **Grupos** y después pulse el icono **Editar** junto al grupo de usuarios.
   Se muestra la página **Grupo de usuarios**.
3. En el panel **General**, puede modificar la información básica para este grupo de usuarios.
4. En el panel **Nivel de autorización de los miembros**, puede decidir si este grupo de usuarios tiene autorización de *Administrador*, *Descubrimiento* o solo de *Lectura*.

5. Si ha especificado el nivel de autorización *Descubrimiento* en **Nivel de autorización de miembro**, puede cambiar los conjuntos de alcances que este grupo de usuarios está autorizado a descubrir en el panel **Restringir a los conjuntos de alcances seleccionados**.
6. Pulse **Guardar** para guardar los cambios.

   En la página **Cuentas de usuario y grupos de usuarios** se muestra la información modificada.

Suprimir cuentas de usuario y grupos de usuarios

Puede suprimir las cuentas de usuario y los grupos de usuarios existentes.

Suprimir cuentas de usuario

Puede suprimir las cuentas de usuario existentes.

Acerca de esta tarea

Nota: La cuenta de usuario **admin** no se puede suprimir.

Para suprimir una cuenta de usuario, siga estos pasos:

Procedimiento

1. En el panel de navegación, pulse **Administración** > **Cuentas de usuario**.

   Se muestra la página **Cuentas de usuario y grupos de usuarios**.
2. Pulse la pestaña **Cuentas** y después pulse el icono Suprimir junto a la cuenta de usuario que desea suprimir.
3. Pulse **Aceptar** para confirmar que desea suprimir la cuenta de usuario.

Suprimir grupos de usuarios

Puede suprimir los grupos de usuarios existentes.

Acerca de esta tarea

Nota: El grupo de usuarios **Administrador** no se puede suprimir.

Para suprimir un grupo de usuarios, siga estos pasos:

Procedimiento

1. Pulse **Administración** > **Cuentas de usuario**.

   Se muestra la página **Cuentas de usuario y grupos de usuarios**.
2. Pulse en la pestaña **Grupos** y después pulse el icono Suprimir junto al grupo de usuarios que desea suprimir.
3. Pulse **Aceptar** para confirmar que desea suprimir el grupo de usuarios.

   Nota: Un grupo de usuarios solo puede suprimirse si no tiene usuarios asignados.

Accesibilidad

Technical Support Appliance no interfiere con las funciones de accesibilidad de los navegadores admitidos. Para obtener una lista completa de las funciones de accesibilidad, visite la página de soporte de accesibilidad del navegador admitido que esté utilizando. Para obtener una lista de navegadores admitidos, consulte “Navegadores web necesarios” en la página 5.

Las publicaciones para este producto están disponibles en formato Adobe PDF (Portable Document Format) y deben cumplir los estándares de accesibilidad. Si tiene alguna dificultad a la hora de utilizar los archivos PDF y desea solicitar alguna publicación en formato basado en web, envíe una solicitud a la dirección siguiente:

icfeedbk@us.ibm.com

También puede enviar una solicitud por correo postal a la dirección siguiente:

International Business Machines Corporation
Information Development
3605 Hwy 52 North
Rochester, MN, EE. UU. 55901

En la solicitud, indique el título de la publicación, "Guía de configuración de IBM Technical Support Appliance" en la línea de asunto de la nota.

Cuando envía información a IBM, otorga a IBM el derecho no exclusivo de utilizar o distribuir la información de la forma que considere adecuada, sin incurrir en ninguna obligación para con usted.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en EE. UU.

Es posible que IBM no ofrezca los productos, servicios o características descritos en este documento en otros países. Consulte a su representante local de IBM para obtener información sobre los productos y servicios disponibles en su zona. Las referencias a un producto, programa o servicio de IBM no pretenden afirmar ni implicar que únicamente pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ningún derecho de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal descrito en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE. UU.

Para consultas sobre licencias relacionadas con información de DBCS (juego de caracteres de doble byte), póngase en contacto con el Departamento de Propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

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

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO PERO NO LIMITÁNDOSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO. Algunos países no permiten la renuncia a garantías explícitas o implícitas en determinadas transacciones, por lo que puede que esta declaración no sea aplicable en su caso.

Esta información puede incluir imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar en cualquier momento mejoras o cambios en los productos o programas descritos en esta publicación sin previo aviso.

Cualquier referencia incluida en esta información a sitios web que no sean de IBM solo se proporciona para su comodidad y en ningún modo constituye una aprobación de dichos sitios web. Los materiales de dichos sitios web no forman parte de los materiales para este producto de IBM, y el uso de dichos sitios web se hace bajo responsabilidad del usuario.

IBM puede utilizar o distribuir cualquier información que se le proporcione en la forma que considere adecuada, sin incurrir por ello en ninguna obligación para con el remitente.

Los datos de rendimiento que contiene este documento se han determinado en un entorno controlado. Por tanto, los resultados que se obtengan en otros entornos operativos pueden variar considerablemente. Algunas medidas se han tomado en sistemas a nivel de desarrollo y no se garantiza que estas medidas sean las mismas en los sistemas disponibles en general. Además, es posible que se hayan estimado algunas medidas mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deberían verificar los datos aplicables a su entorno específico.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes de disponibilidad pública. IBM no ha comprobado estos productos y no puede confirmar la precisión de su rendimiento, compatibilidad, ni contemplar ninguna otra reclamación relacionada con los productos que no son de IBM. Las preguntas relacionadas con las funciones de los productos que no son de IBM deberán dirigirse a los proveedores de estos productos.

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.

Esta información se proporciona solo a efectos de planificación. La información contenida está sujeta a cambios antes de que estén disponibles los productos descritos.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas comerciales o marcas registradas de International Business Machines Corp. en muchas jurisdicciones en todo el mundo. Otros nombres de producto o servicio pueden ser marcas registradas de IBM u otras compañías. Encontrará una lista actualizada de las marcas registradas de IBM en el sitio web www.ibm.com/legal/copytrade.shtml, en el apartado "Copyright and trademark information".

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows, Hyper-V y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

Java™ y todas las marcas registradas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle o sus filiales.

VMware, el logotipo de VMware, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server y VMware vSphere son marcas comerciales o marcas registradas de VMware, Inc. o sus filiales en los Estados Unidos o en otras jurisdicciones.

Número Pieza:

(1P) P/N: