



PlateSpin[®] Protect 11.0.1

Guía del usuario

2 de septiembre de 2014

Información legal

ESTE DOCUMENTO Y EL SOFTWARE DESCRITO EN EL MISMO SE FACILITAN DE ACUERDO CON Y SUJETOS A LOS TÉRMINOS DE UN ACUERDO DE LICENCIA O DE UN ACUERDO DE NO DIVULGACIÓN. EXCEPTO EN LA FORMA ESTABLECIDA EXPRESAMENTE EN EL MENCIONADO ACUERDO DE LICENCIA O ACUERDO DE NO DIVULGACIÓN, NETIQ CORPORATION PROPORCIONA ESTE DOCUMENTO Y EL SOFTWARE DESCRITO EN EL MISMO "TAL COMO ESTÁN" SIN NINGÚN TIPO DE GARANTÍA, YA SEA EXPRESA O IMPLÍCITA, INCLUIDA SIN LIMITACIÓN, CUALQUIER GARANTÍA EXPRESA DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN EN PARTICULAR. ALGUNOS ESTADOS O JURISDICCIONES NO PERMITEN LAS EXENCIONES DE GARANTÍA EXPRESAS O IMPLÍCITAS EN DETERMINADAS TRANSACCIONES; POR TANTO, ESTE ENUNCIADO PODRÍA NO SER DE APLICACIÓN EN SU CASO.

A efectos de claridad, cualquier módulo, adaptador u otro material similar ("Módulo") se concede bajo licencia de acuerdo con los términos y condiciones del Acuerdo de licencia del usuario final correspondiente a la versión aplicable del producto o software de NetIQ con el que se relaciona o interactúa y, al acceder al Módulo, copiarlo o usarlo, usted se compromete a quedar vinculado por dichos términos. Si no está de acuerdo con los términos del Acuerdo de licencia del usuario final, entonces no está autorizado para usar, acceder a o copiar el Módulo, y deberá destruir todas las copias del Módulo y ponerse en contacto con NetIQ para recibir más instrucciones.

Se prohíbe prestar, vender, alquilar o entregar este documento y el software descrito en este documento de ninguna forma sin el permiso previo por escrito de NetIQ Corporation, excepto en la medida permitida por la ley. Excepto según se establece en el mencionado acuerdo de licencia o acuerdo de no divulgación, se prohíbe la reproducción, almacenamiento en un sistema de recuperación o transmisión por cualquier medio, ya sea electrónico, mecánico o de otro tipo, de cualquier parte de este documento o del software descrito en este documento sin el permiso previo por escrito de NetIQ Corporation. Algunas empresas, nombres y datos mencionados en este documento se utilizan con fines ilustrativos y puede que no representen a empresas, personas o datos reales.

Este documento podría incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información contenida en este documento. Estos cambios pueden incorporarse en nuevas ediciones de este documento. NetIQ Corporation puede realizar mejoras o cambios en el software descrito en este documento en cualquier momento.

Derechos restringidos del Gobierno de los Estados Unidos: si el software y la documentación se adquieren por parte de o en nombre del gobierno de los Estados Unidos o por parte de un contratista o subcontratista (en cualquier nivel) principal del gobierno de los Estados Unidos, de conformidad con 48 C.F.R. 227.7202-4 (para adquisiciones del Departamento de Defensa [DOD]) y con 48 C.F.R. 2.101 y 12.212 (para adquisiciones que no sean del DOD), los derechos del gobierno sobre el software y la documentación, incluidos los derechos de uso, modificación, reproducción, publicación, actuación, visualización o divulgación estarán sujetos en todas sus vertientes a los derechos y restricciones de licencia comercial establecidos en el presente acuerdo de licencia.

© 2014 NetIQ Corporation. Reservados todos los derechos.

Para obtener información acerca de las marcas comerciales de NetIQ, consulte <https://www.netiq.com/company/legal/>.

Concesión de la licencia

Las licencias de PlateSpin Protect 10.4 no se pueden utilizar con versiones anteriores de PlateSpin Protect.

Software de otros fabricantes

Consulte la página *PlateSpin Third-Party License Usage and Copyright* (https://www.netiq.com/documentation/platespin_licensing/platespin_licensing_qs/data/platespin_licensing_qs.html) (Uso de licencias y copyright de otros fabricantes de PlateSpin) para obtener información sobre el software de otros fabricantes que se usa en PlateSpin Protect.

Tabla de contenido

Acerca de NetIQ Corporation	7
Acerca de esta guía	9
1 Descripción general del producto	11
1.1 Acerca de PlateSpin Protect	11
1.2 Configuraciones compatibles	11
1.2.1 Cargas de trabajo Windows compatibles	11
1.2.2 Cargas de trabajo Linux compatibles	13
1.2.3 Contenedores de máquina virtual admitidos	14
1.2.4 Firmware de sistema admitido	14
1.3 Seguridad y privacidad	14
1.3.1 Seguridad de los datos de la carga de trabajo durante la transmisión	15
1.3.2 Seguridad de las comunicaciones entre los clientes y el servidor	15
1.3.3 Seguridad de las credenciales	15
1.3.4 Autorización y autenticación de usuarios	15
1.4 Rendimiento	15
1.4.1 Acerca de las características de rendimiento del producto	16
1.4.2 Compresión de datos	16
1.4.3 Regularización del ancho de banda	16
1.4.4 Especificaciones de RPO, RTO y TTO	17
1.4.5 Capacidad de ampliación	17
2 Configuración de la aplicación de PlateSpin Protect	19
2.1 Licencia del producto	19
2.1.1 Obtención de un código de activación de licencia	19
2.1.2 Activación de licencia en línea	19
2.1.3 Activación de licencia sin conexión	20
2.2 Configuración de la autorización y la autenticación de usuarios	21
2.2.1 Acerca de la autorización y autenticación de usuarios de PlateSpin Protect	21
2.2.2 Gestión del acceso y los permisos de PlateSpin Protect	22
2.2.3 Gestión de los grupos de seguridad de PlateSpin Protect y los permisos de la carga de trabajo	24
2.3 Requisitos de acceso y comunicación en la red de protección	25
2.3.1 Requisitos de acceso y comunicación para las cargas de trabajo	25
2.3.2 Requisitos de acceso y comunicación para los contenedores	27
2.3.3 Requisitos de apertura de puertos para los hosts de servidores de PlateSpin	27
2.3.4 Protección en redes públicas y privadas mediante NAT	28
2.3.5 Anulación de la shell bash por defecto para ejecutar comandos en cargas de trabajo Linux	28
2.3.6 Requisitos de clústeres DRS VMware como contenedores	29
2.4 Configuración de las opciones por defecto de PlateSpin Protect	29
2.4.1 Configuración de notificaciones automáticas por correo electrónico de eventos e informes	29
2.4.2 Configuración de idiomas para versiones internacionales de PlateSpin Protect	33
2.4.3 Configuración del comportamiento del servidor de PlateSpin mediante parámetros de configuración XML	34
2.4.4 Configuración de la compatibilidad con VMware vCenter Site Recovery Manager	36

3	Activación y ejecución	39
3.1	Apertura de la interfaz Web de PlateSpin Protect	39
3.2	Elementos de la interfaz Web de PlateSpin Protect	40
3.2.1	Barra de navegación	41
3.2.2	Panel de resumen visual	41
3.2.3	Panel de tareas y eventos	42
3.3	Cargas de trabajo y comandos de carga de trabajo	42
3.3.1	Comandos de protección y recuperación de cargas de trabajo	43
3.4	Gestión de varias instancias de PlateSpin Protect y PlateSpin Forge	44
3.4.1	Uso de la consola de gestión de PlateSpin Protect	45
3.4.2	Acerca de las tarjetas de consola de gestión de PlateSpin Protect	45
3.4.3	Adición de instancias de PlateSpin Protect y PlateSpin Forge a la consola de gestión	46
3.4.4	Gestión de tarjetas en la consola de gestión	46
3.5	Generación de informes de carga de trabajo y de protección de la carga de trabajo	48
4	Protección de la carga de trabajo	49
4.1	Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo	49
4.2	Adición de contenedores (destinos de protección)	51
4.3	Adición de cargas de trabajo para su protección	52
4.4	Configuración de los detalles de protección y preparación de la réplica	53
4.4.1	Detalles de protección de la carga de trabajo	54
4.5	Inicio de la protección de la carga de trabajo	56
4.6	Cancelación de comandos	57
4.7	Failover (conmutación por fallo)	58
4.7.1	Detección de cargas de trabajo sin conexión	58
4.7.2	Realización de failover	59
4.7.3	Uso de la función de prueba de failover	60
4.8	Failback (conmutación a configuración previa)	60
4.8.1	Failback automatizado a una plataforma de máquina virtual	61
4.8.2	Failback semiautomatizado a un equipo físico	64
4.8.3	Failback semiautomatizado a una máquina virtual	65
4.9	Reprotección de una carga de trabajo	66
5	Elementos básicos de la protección de la carga de trabajo	67
5.1	Consumo de licencia de carga de trabajo	67
5.2	Directrices para las credenciales de carga de trabajo y contenedor	68
5.3	Configuración de inquilinos múltiples de Protect en VMware	68
5.3.1	Uso de herramientas para definir funciones de VMware	69
5.3.2	Asignación de funciones en vCenter	71
5.4	Transferencia de datos	74
5.4.1	Métodos de transferencia	74
5.4.2	Cifrado de datos	75
5.5	Niveles de protección	76
5.6	Puntos de recuperación	77
5.7	Método de réplica inicial (completa o incremental)	77
5.8	Control de servicios y daemons	79
5.9	Uso de los guiones freeze y thaw en todas las réplicas (Linux)	79
5.10	Volúmenes	80
5.11	Redes	82
5.12	Failback a equipos físicos	82
5.12.1	Descarga de la imagen ISO de arranque de PlateSpin	82

5.12.2	Incorporación de controladores de dispositivo adicionales en la imagen ISO de arranque	83
5.12.3	Registro de equipos físicos como destinos de failback con PlateSpin Protect	84
5.13	Temas avanzados sobre la protección de la carga de trabajo.	85
5.13.1	Protección de clústeres de Windows.	85
5.13.2	Uso de funciones de protección de la carga de trabajo mediante la API de servicios Web de PlateSpin Protect	87
6	Herramientas auxiliares para trabajar con equipos físicos	91
6.1	Gestión de controladores de dispositivo	91
6.1.1	Empaquetado de controladores de dispositivo para sistemas Windows.	91
6.1.2	Empaquetado de controladores de dispositivo para sistemas Linux.	92
6.1.3	Carga de controladores a la base de datos de controladores de dispositivos de PlateSpin Protect.	92
6.1.4	Uso de la función de traductor de ID de plug-and-play (PnP)	95
7	Solución de problemas	103
7.1	Solución de problemas con el inventario de cargas de trabajo (Windows)	103
7.1.1	Realización de pruebas de conectividad	105
7.1.2	Inhabilitación del software antivirus.	106
7.1.3	Habilitación de permisos y acceso a archivos y recursos compartidos.	106
7.2	Solución de problemas con el inventario de cargas de trabajo (Linux)	107
7.3	Solución de problemas durante el comando de preparación de réplica (Windows)	108
7.3.1	Directiva de grupo y derechos de usuario	108
7.4	Solución de problemas de réplica de la carga de trabajo	109
7.5	Solución de problemas de reenvío de tráfico en las cargas de trabajo	111
7.6	Solución de problemas con la ayuda en línea	111
7.7	Generación y visualización de informes de diagnóstico	111
7.8	Eliminación de cargas de trabajo	112
7.9	Limpieza de la carga de trabajo después de la protección	112
7.9.1	Limpieza de las cargas de trabajo Windows	112
7.9.2	Limpieza de las cargas de trabajo Linux	113
7.10	Compresión de las bases de datos de PlateSpin Protect	115
A	Distribuciones de Linux compatibles con Protect	117
A.1	Análisis de la carga de trabajo Linux	117
A.1.1	Determinación de la cadena de versión	117
A.1.2	Determinación de la arquitectura.	118
A.2	Controlador "blkwatch" compilado previamente para Protect (Linux)	118
B	Sincronización del almacenamiento local del nodo de clúster	129
	Glosario	131

Acerca de NetIQ Corporation

NetIQ, una empresa de Attachmate, es líder global en gestión de seguridad y sistemas. Con más de 12.000 clientes en más de 60 países, las soluciones de NetIQ maximizan las inversiones en tecnología y ofrecen mejoras en los procesos de TI para conseguir ahorros de costes considerables. El catálogo de la empresa incluye galardonados productos de administración para automatización de procesos de TI, administración de sistemas, gestión de la seguridad, auditoría y control de configuraciones, administración de empresas y gestión de comunicaciones unificadas. Para obtener más información, visite www.netiq.com.

Cómo ponerse en contacto con la asistencia para ventas

Para cualquier pregunta sobre nuestros productos, precios y capacidades, póngase en contacto con su representante local. Si no puede contactar con su representante local, comuníquese con nuestro equipo de Asistencia para ventas.

Oficinas mundiales: www.netiq.com/about_netiq/officelocations.asp

Estados Unidos y Canadá: 888-323-6768

Correo electrónico: info@netiq.com

sitio Web de iFolder: www.netiq.com

Cómo ponerse en contacto con el personal de asistencia técnica

Para obtener información sobre problemas con productos específicos, póngase en contacto con nuestro equipo de asistencia técnica.

Oficinas mundiales: www.netiq.com/Support/contactinfo.asp

Norteamérica y Sudamérica: 1-713-418-5555

Europa, Oriente Medio y África: +353 (0) 91-782 677

Correo electrónico: support@netiq.com

sitio Web de iFolder: www.netiq.com/support

Cómo ponerse en contacto con la asistencia para documentación

Nuestro objetivo es proporcionar documentación que satisfaga sus necesidades. Si tiene sugerencias de mejoras, haga clic en **Add Comment** (Agregar comentario) en la parte de abajo de cualquier página de las versiones HTML de la documentación publicada en www.netiq.com/documentation. Si lo desea, también puede enviar un correo electrónico a Documentation-Feedback@netiq.com. Agradecemos sus comentarios y estamos deseando oír sus sugerencias.

Cómo contactar con la comunidad de usuarios en línea

Qmunity, la comunidad de NetIQ en línea, es una red de colaboración que le pone en contacto con sus colegas y con otros expertos de NetIQ. Qmunity le ayuda a dominar los conocimientos que necesita para hacer realidad todo el potencial de su inversión en TI de la que depende, al proporcionarle información inmediata, enlaces útiles a recursos prácticos y acceso a los expertos de NetIQ. Para obtener más información, visite la página <http://community.netiq.com>.

Acerca de esta guía

Esta guía proporciona información sobre el uso de PlateSpin Protect.

- ♦ Capítulo 1, “Descripción general del producto”, en la página 11
- ♦ Capítulo 2, “Configuración de la aplicación de PlateSpin Protect”, en la página 19
- ♦ Capítulo 3, “Activación y ejecución”, en la página 39
- ♦ Capítulo 4, “Protección de la carga de trabajo”, en la página 49
- ♦ Capítulo 5, “Elementos básicos de la protección de la carga de trabajo”, en la página 67
- ♦ Capítulo 6, “Herramientas auxiliares para trabajar con equipos físicos”, en la página 91
- ♦ Capítulo 7, “Solución de problemas”, en la página 103
- ♦ Apéndice A, “Distribuciones de Linux compatibles con Protect”, en la página 117
- ♦ Apéndice B, “Sincronización del almacenamiento local del nodo de clúster”, en la página 129
- ♦ “Glosario” en la página 131

Usuarios a los que va dirigida

Esta guía está dirigida al personal de TI, como administradores y operadores de centros de datos, que usan PlateSpin Protect en sus proyectos habituales de protección de la carga de trabajo.

Comentarios

Nos gustaría recibir sus comentarios y sugerencias acerca de este manual y del resto de la documentación incluida con este producto. Utilice la función de *comentarios del usuario* situada en la parte superior e inferior de las páginas de la documentación en línea.

Documentación adicional

Esta guía forma parte de la documentación de PlateSpin Protect. Para consultar una lista completa de las publicaciones de esta versión, visite el sitio Web de documentación en línea del producto:

Documentación en línea de PlateSpin Protect 11 (https://www.netiq.com/documentation/platespin_protect_11/)

Actualizaciones de la documentación

Encontrará la versión más reciente de esta guía en el [sitio Web de documentación en línea de PlateSpin Protect 11](https://www.netiq.com/documentation/platespin_protect_11/) (https://www.netiq.com/documentation/platespin_protect_11/):

Recursos adicionales

Recomendamos utilizar los siguientes recursos adicionales en Internet:

- ♦ [Comunidad de usuarios de NetIQ](https://www.netiq.com/communities/) (<https://www.netiq.com/communities/>): una comunidad Web con diversos temas de debate.

- ♦ [Base de datos de asistencia de NetIQ \(https://www.netiq.com/support/kb/\)](https://www.netiq.com/support/kb/): una recopilación de artículos técnicos detallados en profundidad.
- ♦ [Foros de asistencia de NetIQ \(https://forums.netiq.com/forum.php\)](https://forums.netiq.com/forum.php): un sitio Web donde los usuarios de los productos pueden hablar de la funcionalidad de los productos de NetIQ y recibir consejos de otros usuarios.
- ♦ [MyNetIQ \(https://www.netiq.com/f/mynetiql/\)](https://www.netiq.com/f/mynetiql/): un sitio Web que ofrece información y servicios para los productos PlateSpin, como acceso a la mejor documentación técnica, registros en seminarios virtuales y descargas de versiones de prueba de productos.

Asistencia técnica

Encontrará más información acerca de las directivas y procedimientos de asistencia técnica de NetIQ en su [Guía de asistencia técnica \(https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and\)](https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and).

Estos recursos le permitirán recibir asistencia específica para PlateSpin Protect:

- ♦ Teléfono en Canadá y Estados Unidos: 1-800-858-4000
- ♦ Teléfono fuera de Estados Unidos: 1-801-861-4000
- ♦ Correo electrónico: support@platespin.com
- ♦ Información específica del producto: [asistencia de PlateSpin Protect \(https://www.netiq.com/support/kb/product.php?id=SG_XPLATESPINPROTECT_1_2\)](https://www.netiq.com/support/kb/product.php?id=SG_XPLATESPINPROTECT_1_2)

1 Descripción general del producto

En esta sección se incluye la información siguiente:

- ♦ [Sección 1.1, “Acerca de PlateSpin Protect”, en la página 11](#)
- ♦ [Sección 1.2, “Configuraciones compatibles”, en la página 11](#)
- ♦ [Sección 1.3, “Seguridad y privacidad”, en la página 14](#)
- ♦ [Sección 1.4, “Rendimiento”, en la página 15](#)

1.1 Acerca de PlateSpin Protect

PlateSpin Protect es un software de continuidad empresarial y recuperación de desastres que protege las cargas de trabajo físicas y virtuales (sistemas operativos, middleware y datos) mediante tecnología de virtualización. En caso de interrupción del servicio o de fallo del servidor operativo, se pueden activar rápidamente una réplica virtualizada de una carga de trabajo en el *contenedor* de destino (un host de máquina virtual) y seguir ejecutándose con normalidad hasta que se restaure el entorno operativo.

PlateSpin Protect le permite:

- ♦ Recuperar rápidamente cargas de trabajo en caso de fallo
- ♦ Proteger múltiples cargas de trabajo al mismo tiempo
- ♦ Probar la carga de trabajo de failover sin interferir con el entorno operativo
- ♦ Devolver cargas de trabajo de failover a su infraestructura original o a una completamente nueva, ya sea física o virtual
- ♦ Aprovechar las soluciones de almacenamiento externo existentes, como SAN

1.2 Configuraciones compatibles

- ♦ [Sección 1.2.1, “Cargas de trabajo Windows compatibles”, en la página 11](#)
- ♦ [Sección 1.2.2, “Cargas de trabajo Linux compatibles”, en la página 13](#)
- ♦ [Sección 1.2.3, “Contenedores de máquina virtual admitidos”, en la página 14](#)
- ♦ [Sección 1.2.4, “Firmware de sistema admitido”, en la página 14](#)

1.2.1 Cargas de trabajo Windows compatibles

PlateSpin Protect admite la mayoría de las cargas de trabajo basadas en Windows.

Se admite tanto la réplica en el nivel de archivos como en el nivel de bloques, con ciertas restricciones. Consulte la [Sección 5.4, “Transferencia de datos”, en la página 74](#).

Tabla 1-1 Cargas de trabajo Windows compatibles

Sistema operativo	Observaciones
Cargas de trabajo de servidor	
Windows Server 2012 R2 Windows Server 2012	
Windows Server 2008 R2 (64 bits) Windows Server 2008 (64 bits)	Incluidos controladores de dominio (DC) y las ediciones Small Business Server (SBS)
Windows Server 2003 R2 (64 bits) Windows Server 2003 R2 (32 bits) Windows Server 2003 con el último SP (64 bits) Windows Server 2003 con el último SP (32 bits)	Windows 2003 requiere el SP1 o superior para la réplica basada en bloques.
Clústeres de Windows	Consulte "Protección de clústeres de Windows" en la página 85 para conocer las configuraciones específicas de clúster admitidas.
Cargas de trabajo de estación de trabajo	
Windows 8.1 Windows 8	<p>Advertencia: debe seleccionar el plan de energía <i>Alto rendimiento</i> en el origen con Windows 8 para que las funciones de failover y failback de la carga de trabajo funcionen correctamente.</p> <p>Para configurar este plan de energía desde el panel de control de Windows:</p> <ol style="list-style-type: none"> 1. Seleccione <i>Todos los elementos de Panel de control > Opciones de energía</i>. 2. En el recuadro de diálogo <i>Elegir o personalizar un plan de energía</i>, seleccione <i>Mostrar planes adicionales > Alto rendimiento</i>. 3. Cierre el panel de control.
<p>Versiones internacionales admitidas: alemán, chino simplificado, chino tradicional, francés y japonés.</p> <p>Compatibilidad con firmware de carga de trabajo (UEFI y BIOS): PlateSpin Protect duplica la compatibilidad de Microsoft con cargas de trabajo Windows basadas en UEFI o BIOS. Transfiere las cargas de trabajo (se admiten transferencias por bloques y archivos) del origen al destino, al tiempo que aplica el firmware compatible a los sistemas operativos correspondientes de origen y destino. El procedimiento es idéntico para el failback a un equipo físico. Cuando se inicia cualquier transición (failover o failback) entre sistemas UEFI y BIOS, Protect la analiza e informa sobre su validez.</p> <p>Nota: si protege una carga de trabajo basada en UEFI y quiere seguir usando el mismo modo de arranque de firmware durante todo el ciclo de vida del producto protegido, tendrá que usar como destino un contenedor vSphere 5.0 o superior.</p>	

A continuación, se muestran algunos ejemplos del comportamiento de Protect para proteger y realizar un failback entre sistemas basados en UEFI y en BIOS:

- ♦ Al transferir una carga de trabajo basada en UEFI a un contenedor VMware vSphere 4.x (que no es compatible con UEFI), Protect pasa el firmware UEFI de la carga de trabajo en el momento del failover a firmware BIOS. Después, cuando se selecciona el failback en un equipo físico basado en UEFI, Protect revierte la transición del firmware de BIOS a UEFI.
- ♦ Si intenta realizar el failback de una carga de trabajo protegida de Windows 2003 en un equipo físico basado en UEFI, Protect analiza la opción e informa de que no es válida (es decir, la transición del firmware de BIOS a UEFI no se admite, ya que Windows 2003 no admite el modo de arranque UEFI).
- ♦ Si se protege un origen basado en UEFI en un destino basado en BIOS, Protect migra los discos de arranque del sistema UEFI, en formato GPT, a discos MBR. El failback de esta carga de trabajo BIOS a un equipo físico basado en UEFI convierte los discos de arranque de nuevo al formato GPT.

1.2.2 Cargas de trabajo Linux compatibles

PlateSpin Protect admite varias distribuciones de Linux.

La réplica se realiza a nivel de bloque, para lo que el software PlateSpin requiere un módulo `blkwatch` compilado para la distribución de Linux específica que se desea proteger.

Algunas versiones de Linux admitidas requieren compilar el módulo `blkwatch` de PlateSpin para su núcleo específico. Estas cargas de trabajo se identifican explícitamente.

Tabla 1-2 Cargas de trabajo Linux compatibles

Sistema operativo	Observaciones
Cargas de trabajo de servidor Linux	
Red Hat Enterprise Linux (RHEL) 6.2	Solo transferencia basada en bloques.
Red Hat Enterprise Linux (RHEL) 4 (32 bits)	Solo transferencia basada en bloques.
Novell Open Enterprise Server (OES) 11 SP1 y SP2	Nota: no se admite la versión por defecto del núcleo, la 3.0.13, de OES 11 SP2. Actualice a la versión del núcleo 3.0.27 o posterior antes de realizar un inventario de la carga de trabajo. Solo transferencia basada en bloques.

Sistemas de archivos de Linux admitidos

Se admiten los sistemas de archivos EXT2, EXT3, EXT4, REISERFS y NSS (cargas de trabajo OES 2), solo para la transferencia basada en bloques.

Nota: los volúmenes cifrados de las cargas de trabajo del origen se descifran en la máquina virtual de failover.

1.2.3 Contenedores de máquina virtual admitidos

Tabla 1-3 Plataformas admitidas como contenedor de máquina virtual

Contenedor	Notas
Clúster DRS VMware en vSphere 5.5	<ul style="list-style-type: none">♦ La configuración de DRS debe ser Partially Automated (Parcialmente automatizada) o Fully Automated (Totalmente automatizada. No debe definirse en Manual).♦ Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 5.5 y solo se puede gestionar en vCenter 5.5.
Clúster DRS VMware en vSphere 5.1	<ul style="list-style-type: none">♦ La configuración de DRS debe ser Partially Automated (Parcialmente automatizada) o Fully Automated (Totalmente automatizada. No debe definirse en Manual).♦ Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 5.1 y solo se puede gestionar en vCenter 5.1.
Clúster DRS VMware en vSphere 4.1	<ul style="list-style-type: none">♦ La configuración de DRS debe ser Partially Automated (Parcialmente automatizada) o Fully Automated (Totalmente automatizada. No debe definirse en Manual).♦ Como contenedor de máquina virtual, el clúster puede usar una combinación de servidores ESX 4.1 y ESXi 4.1 y solo se puede gestionar en vCenter 4.1.

1.2.4 Firmware de sistema admitido

PlateSpin Protect duplica la compatibilidad con UEFI de Microsoft. Para obtener más información, consulte la [Sección 1.2.1, “Cargas de trabajo Windows compatibles”](#), en la página 11.

1.3 Seguridad y privacidad

PlateSpin Protect incluye numerosas funciones para ayudarle a proteger los datos y a aumentar la seguridad.

- ♦ [Sección 1.3.1, “Seguridad de los datos de la carga de trabajo durante la transmisión”](#), en la página 15
- ♦ [Sección 1.3.2, “Seguridad de las comunicaciones entre los clientes y el servidor”](#), en la página 15
- ♦ [Sección 1.3.3, “Seguridad de las credenciales”](#), en la página 15
- ♦ [Sección 1.3.4, “Autorización y autenticación de usuarios”](#), en la página 15

1.3.1 Seguridad de los datos de la carga de trabajo durante la transmisión

Para hacer la transferencia de los datos de la carga de trabajo más segura, puede configurar la protección de la carga de trabajo para que se cifren los datos. Si el cifrado está habilitado, los datos que se replican por la red se cifran mediante AES (Estándar de cifrado avanzado).

Si es necesario, puede configurar el servidor de PlateSpin para que utilice un algoritmo de cifrado de datos compatible con FIPS (Federal Information Processing Standards, normas federales de procesamiento de la información, publicación 140-2). Consulte la sección sobre “cómo habilitar la compatibilidad con algoritmos de cifrado de datos compatibles con FIPS (opcional)” en la *Guía de instalación*.

El cifrado se puede habilitar o inhabilitar de forma individual en cada carga de trabajo. Consulte [“Detalles de protección de la carga de trabajo”](#) en la página 54.

1.3.2 Seguridad de las comunicaciones entre los clientes y el servidor

Puesto que la instalación del servidor de PlateSpin habilita SSL en el host del servidor de PlateSpin, la transmisión de datos segura entre el navegador Web y el servidor de PlateSpin ya está configurada como HTTPS (protocolo seguro de transferencia de hipertexto). La instalación también añade un certificado autofirmado si no se encuentra ninguno válido.

1.3.3 Seguridad de las credenciales

Las credenciales que usa para acceder a varios sistemas (como las cargas de trabajo y los destinos de failback) se almacenan en la base de datos de PlateSpin Protect y, por lo tanto, quedan protegidas por las mismas medidas de seguridad que el host del servidor de PlateSpin.

Asimismo, las credenciales se incluyen en los diagnósticos, a los que pueden acceder los usuarios acreditados. Debe asegurarse de que solo el personal autorizado gestione los proyectos de protección de la carga de trabajo.

1.3.4 Autorización y autenticación de usuarios

PlateSpin Protect proporciona un mecanismo completo y seguro de autorización y autenticación de usuarios basado en funciones de usuario. Este mecanismo controla el acceso a las aplicaciones y las operaciones que pueden realizar los usuarios. Consulte la [Sección 2.2, “Configuración de la autorización y la autenticación de usuarios”](#), en la página 21.

1.4 Rendimiento

- ♦ [Sección 1.4.1, “Acerca de las características de rendimiento del producto”](#), en la página 16
- ♦ [Sección 1.4.2, “Compresión de datos”](#), en la página 16
- ♦ [Sección 1.4.3, “Regularización del ancho de banda”](#), en la página 16
- ♦ [Sección 1.4.4, “Especificaciones de RPO, RTO y TTO”](#), en la página 17
- ♦ [Sección 1.4.5, “Capacidad de ampliación”](#), en la página 17

1.4.1 Acerca de las características de rendimiento del producto

Las características de rendimiento del producto PlateSpin Protect dependen de varios factores; por ejemplo:

- ♦ Los perfiles de hardware y software de las cargas de trabajo de origen.
- ♦ Los perfiles de hardware y software de los contenedores de destino.
- ♦ El perfil de hardware y software del host del servidor de PlateSpin.
- ♦ El ancho de banda, la configuración y las condiciones específicas de la red.
- ♦ El número de cargas de trabajo protegidas.
- ♦ El número de volúmenes protegidos.
- ♦ El tamaño de los volúmenes protegidos.
- ♦ La densidad de archivos (el número de archivos por unidad de capacidad) en los volúmenes de las cargas de trabajo.
- ♦ Los niveles de E/S de origen (el nivel de ocupación de las cargas de trabajo).
- ♦ El número de réplicas simultáneas.
- ♦ Si el cifrado de datos está habilitado o inhabilitado.
- ♦ Si la compresión de datos está habilitada o inhabilitada.

En los planes de protección de la carga de trabajo a gran escala, debe realizar una protección de prueba de una carga de trabajo típica, ejecutar algunas réplicas y usar el resultado como comparativa para ajustar con precisión las medidas de forma regular durante todo el proyecto.

1.4.2 Compresión de datos

Si fuera necesario, PlateSpin Protect puede comprimir los datos de la carga de trabajo antes de transferirlos por la red. De esta forma, se reduce la cantidad total de datos transferidos durante las réplicas.

Los índices de compresión dependen del tipo de archivos de los volúmenes de las cargas de datos de origen, y pueden variar del 0.9 (100 MB de datos comprimidos en 90 MB) al 0.5 (100 MB comprimidos en 50 MB), aproximadamente.

Nota: la compresión de datos usa la potencia del procesador de la carga de trabajo de origen.

La compresión de datos se puede configurar de forma individual en cada carga de trabajo o en niveles de protección. Consulte [“Niveles de protección” en la página 76](#).

1.4.3 Regularización del ancho de banda

PlateSpin Protect permite controlar la cantidad de ancho de banda de la red que consume la comunicación directa entre el origen y el destino durante la protección de la carga de trabajo. Es posible especificar una velocidad de rendimiento para cada contrato de protección. De esta forma, se proporciona un método para evitar que el tráfico de réplica congestione la red de producción y se reduce la carga total del servidor de PlateSpin.

La regularización del ancho de banda se puede configurar de forma individual en cada carga de trabajo o en niveles de protección. Consulte [“Niveles de protección” en la página 76](#).

1.4.4 Especificaciones de RPO, RTO y TTO

- ♦ **Objetivos de punto de recuperación (RPO):** describe la cantidad de pérdida de datos aceptable medida en tiempo. El RPO se determina por el tiempo entre réplicas incrementales de una carga de trabajo protegida y se ve afectado por los niveles actuales de utilización de PlateSpin Protect, la velocidad y el ámbito de los cambios en la carga de trabajo, la velocidad de la red y la programación de réplica seleccionada.
- ♦ **Objetivos de tiempo de recuperación (RTO):** describe el tiempo necesario para una operación de failover (devolver una carga de trabajo de failover en línea para sustituir temporalmente una carga de trabajo de producción protegida).

El RTO para conmutar una carga de trabajo a su réplica virtual se ve afectado por el tiempo que se tarda en configurar y ejecutar la operación de failover (de 10 a 45 minutos). Consulte [“Failover \(conmutación por fallo\)” en la página 58](#).

- ♦ **Objetivos de tiempo de prueba (TTO):** describe el tiempo necesario para probar la recuperación tras fallos con cierta certeza de restauración de servicios.

Use la función *Test Failover* (Probar failover) para ejecutar distintos escenarios y generar datos comparativos. Consulte [“Uso de la función de prueba de failover” en la página 60](#).

Uno de los factores que afectan al RPO, el RTO y el TTO es el número de operaciones de failover simultáneas necesarias. Si hay solo una carga de trabajo en failover, habrá más memoria y recursos de CPU disponibles que si hay varias cargas en failover, que deben compartir los recursos de su infraestructura subyacente.

Es preciso determinar los tiempos de failover medios de las cargas de trabajo en su entorno. Para ello, se realizan pruebas de failover varias veces y se usan los datos comparativos en los planes de recuperación de datos generales. Consulte [“Generación de informes de carga de trabajo y de protección de la carga de trabajo” en la página 48](#).

1.4.5 Capacidad de ampliación

La capacidad de ampliación engloba (y depende de) las siguientes características principales de su producto PlateSpin Protect:

- ♦ **Cargas de trabajo por servidor:** el número de cargas de trabajo por servidor de PlateSpin puede variar entre 10 y 50, en función de diversos factores, incluidos los requisitos de RPO y las características de hardware del host del servidor.
- ♦ **Protecciones por contenedor:** el número máximo de protecciones por contenedor está relacionado (pero no coincide) con las especificaciones de VMware en referencia al número máximo de máquinas virtuales admitidas por cada host ESXi. Algunos factores adicionales incluyen las estadísticas de recuperación (incluidas réplicas y failovers al mismo tiempo) y las especificaciones del fabricante de hardware.

Recomendamos realizar pruebas, ajustar incrementalmente la capacidad estimada y usar estos datos para determinar la capacidad máxima de ampliación.

2 Configuración de la aplicación de PlateSpin Protect

En esta sección se incluye información acerca de lo siguiente:

- ♦ Sección 2.1, “Licencia del producto”, en la página 19
- ♦ Sección 2.2, “Configuración de la autorización y la autenticación de usuarios”, en la página 21
- ♦ Sección 2.3, “Requisitos de acceso y comunicación en la red de protección”, en la página 25
- ♦ Sección 2.4, “Configuración de las opciones por defecto de PlateSpin Protect”, en la página 29

2.1 Licencia del producto

Esta sección proporciona información sobre cómo activar el software de PlateSpin Protect.

- ♦ Sección 2.1.1, “Obtención de un código de activación de licencia”, en la página 19
- ♦ Sección 2.1.2, “Activación de licencia en línea”, en la página 19
- ♦ Sección 2.1.3, “Activación de licencia sin conexión”, en la página 20

2.1.1 Obtención de un código de activación de licencia

Para asignar una licencia de producto, debe disponer de un código de activación de licencia. Si no tiene un código de activación de licencia, solicite uno en el [sitio Web del Centro de servicios al cliente \(http://www.netiq.com/center/\)](http://www.netiq.com/center/). Se le enviará un código de activación de licencia por correo electrónico.

La primera vez que entre en PlateSpin Protect, el navegador le redirigirá automáticamente a la página de activación de la licencia. Tiene dos opciones para activar su licencia de producto: [Activación de licencia en línea](#) o [Activación de licencia sin conexión](#).

2.1.2 Activación de licencia en línea

Para la activación en línea, PlateSpin Protect debe contar con acceso a Internet.

Nota: los servidores proxy HTTP pueden provocar fallos durante la activación en línea. Se recomienda la activación sin conexión para los usuarios en entornos que usen un servidor proxy HTTP.

- 1 En la interfaz Web de PlateSpin Protect, haga clic en *Settings > Licenses > Add License* (Configuración > Licencias > Añadir licencia). Se muestra la página License Activation (Activación de licencia).

- 2 Seleccione *Online Activation* (Activación en línea), especifique la dirección de correo electrónico que proporcionó al realizar el pedido y el código de activación que recibió y haga clic en *Activate* (Activar).

El sistema obtiene la licencia necesaria por Internet y activa el producto.

2.1.3 Activación de licencia sin conexión

Para la activación sin conexión, se debe obtener una clave de licencia por Internet mediante un equipo que tenga acceso a Internet.

Nota: para obtener una clave de licencia, debe disponer de una cuenta de Novell. Si es cliente actual de PlateSpin y no tiene una cuenta del Centro de servicios al cliente de Novell, debe crear una en primer lugar. Use su nombre de usuario actual de PlateSpin (una dirección de correo electrónico válida registrada en PlateSpin) como entrada para el nombre de usuario de la cuenta del centro de servicios al cliente.

- 1 Haga clic en *Settings > License* (Activación > Licencia) y, seguidamente, en *Add license* (Añadir licencia). Se muestra la página de activación de licencia.
- 2 Seleccione *Offline Activation* (Activación sin conexión) y copie el ID de hardware mostrado.
- 3 Use un navegador Web en un equipo que tenga acceso a Internet y diríjase al [sitio Web de activación de productos de PlateSpin](http://www.platespin.com/productactivation/ActivateOrder.aspx) (<http://www.platespin.com/productactivation/ActivateOrder.aspx>). Entre con su nombre de usuario de Novell.
- 4 Cumplimente los campos adecuados:
 - ♦ el código de activación que recibió;
 - ♦ la dirección de correo electrónico que proporcionó al realizar el pedido
 - ♦ el ID de hardware que copió en el [Paso 2](#).
- 5 Haga clic en *Activate* (Activar).
El sistema genera un archivo de clave de licencia y le pide que lo guarde.
- 6 Guarde el archivo de licencia generado, transféralo al host del producto que no tiene conexión a Internet y úselo para activar el producto.

2.2 Configuración de la autorización y la autenticación de usuarios

En esta sección se incluye la siguiente información:

- ♦ [Sección 2.2.1, “Acerca de la autorización y autenticación de usuarios de PlateSpin Protect”, en la página 21](#)
- ♦ [Sección 2.2.2, “Gestión del acceso y los permisos de PlateSpin Protect”, en la página 22](#)
- ♦ [Sección 2.2.3, “Gestión de los grupos de seguridad de PlateSpin Protect y los permisos de la carga de trabajo”, en la página 24](#)

2.2.1 Acerca de la autorización y autenticación de usuarios de PlateSpin Protect

El mecanismo de autorización y autenticación de usuarios de PlateSpin Protect se basa en funciones de usuario y controla el acceso a la aplicación, así como las operaciones que los usuarios pueden realizar. El mecanismo se basa en la autenticación integrada de Windows (IWA) y su interacción con los servicios de información de Internet (IIS).

El mecanismo de acceso basado en funciones permite implementar la autorización y autenticación de usuarios de varias formas:

- ♦ Restringiendo el acceso a la aplicación a usuarios concretos
- ♦ Permitiendo solo operaciones específicas para usuarios concretos
- ♦ Otorgando a cada usuario acceso a cargas de trabajo concretas para realizar operaciones definidas por la función asignada

Cada instancia de PlateSpin Protect dispone del siguiente conjunto de grupos de usuarios para el sistema operativo que define las funciones relacionadas:

- ♦ **Administradores de protección de la carga de trabajo:** cuenta con acceso ilimitado a todas las funciones y características de la aplicación. Los administradores locales forman parte implícita de este grupo.
- ♦ **Usuarios avanzados de protección de la carga de trabajo:** tienen acceso a la mayoría de funciones y características de la aplicación, con algunos límites como restricciones en la capacidad para modificar la configuración del sistema relativa a las licencias y la seguridad.
- ♦ **Operadores de protección de la carga de trabajo:** tienen acceso a un subconjunto limitado de funciones y características del sistema; suficiente para realizar las operaciones cotidianas.

Si un usuario intenta conectarse a PlateSpin Protect, las credenciales proporcionadas a través del navegador se validan mediante IIS. Si el usuario no es miembro de una de las funciones de protección de la carga de trabajo, la conexión se rechaza.

Tabla 2-1 Funciones de protección de la carga de trabajo y detalles de permisos

Detalles de la función de protección de la carga de trabajo	Administradores	Usuarios avanzados	Operadores
Añadir carga de trabajo	Permitido	Permitido	Denegado
Eliminar carga de trabajo	Permitido	Permitido	Denegado
Configurar la protección	Permitido	Permitido	Denegado

Detalles de la función de protección de la carga de trabajo	Administradores	Usuarios avanzados	Operadores
Preparar la réplica	Permitido	Permitido	Denegado
Ejecutar una réplica (completa)	Permitido	Permitido	Permitido
Ejecutar una carga incremental	Permitido	Permitido	Permitido
Pausar/Reanudar una programación	Permitido	Permitido	Permitido
Probar failover	Permitido	Permitido	Permitido
Failover	Permitido	Permitido	Permitido
Cancelar el failover	Permitido	Permitido	Permitido
Abortar	Permitido	Permitido	Permitido
Descartar (tarea)	Permitido	Permitido	Permitido
Configuración (todo)	Permitido	Denegado	Denegado
Ejecutar informes/diagnóstico	Permitido	Permitido	Permitido
Failback	Permitido	Denegado	Denegado
Volver a proteger	Permitido	Permitido	Denegado

Además, el software PlateSpin Protect proporciona un mecanismo basado en *grupos de seguridad* que define qué usuarios deben tener acceso a qué cargas de trabajo en el inventario de cargas de trabajo de PlateSpin Protect.

Para configurar correctamente un acceso a PlateSpin Protect basado en funciones, hay que llevar a cabo dos tareas:

1. Añadir usuarios a los grupos de usuarios necesarios, como se detalla en la [Tabla 2-1](#) (consulte la documentación de Windows).
2. Crear grupos de seguridad de nivel de aplicación que asocien estos usuarios a cargas de trabajo específicas (consulte [“Gestión de los grupos de seguridad de PlateSpin Protect y los permisos de la carga de trabajo”](#) en la página 24).

2.2.2 Gestión del acceso y los permisos de PlateSpin Protect

En las secciones siguientes se proporciona más información:

- ♦ [“Adición de usuarios a PlateSpin Protect”](#) en la página 23
- ♦ [“Asignación de una función de protección de carga de trabajo a un usuario de PlateSpin Protect”](#) en la página 23

Adición de usuarios a PlateSpin Protect

Emplee el procedimiento descrito en esta sección para añadir a un nuevo usuario de PlateSpin Protect.

Si desea proporcionar permisos de función específicos a un usuario existente del host del servidor de PlateSpin, consulte [“Asignación de una función de protección de carga de trabajo a un usuario de PlateSpin Protect”](#) en la página 23.

- 1 En el host del servidor de PlateSpin, acceda a la consola de grupos y usuarios locales del sistema (*Inicio > Ejecutar > lusrmgr.msc > Intro*).
- 2 Haga clic con el botón derecho en el nodo *Users* (Usuarios), seleccione *New User* (Nuevo usuario), especifique los datos necesarios y haga clic en *Create* (Crear).

Ya puede asignar una función de protección de carga de trabajo al usuario recién creado. Consulte [“Asignación de una función de protección de carga de trabajo a un usuario de PlateSpin Protect”](#) en la página 23.

Asignación de una función de protección de carga de trabajo a un usuario de PlateSpin Protect

Antes de asignar una función a un usuario, determine el conjunto de permisos más adecuado para él. Consulte la [Tabla 2-1, “Funciones de protección de la carga de trabajo y detalles de permisos”](#), en la página 21.

- 1 En el host del servidor de PlateSpin, acceda a la consola de grupos y usuarios locales del sistema (*Inicio > Ejecutar > lusrmgr.msc > Intro*).
- 2 Haga clic en el nodo *Users* (Usuarios) y doble clic en el usuario correspondiente en el panel derecho.
- 3 En la pestaña *Member Of* (Miembro de), haga clic en *Add* (Añadir), busque el grupo de protección de carga de trabajo deseado y asígnesele al usuario.

Puede que el cambio tarde varios minutos en tener efecto. Para intentar aplicar los cambios manualmente, reinicie el servidor llevando a cabo estos pasos:

- 1 Acceda al subdirectorío `bin\RestartPlateSpinServer` del servidor de PlateSpin.
- 2 Haga doble clic en el ejecutable `RestartPlateSpinServer.exe`.
Se abrirá un indicador de comandos para solicitar confirmación.
- 3 Confirme escribiendo `Y` y pulse `Intro`.

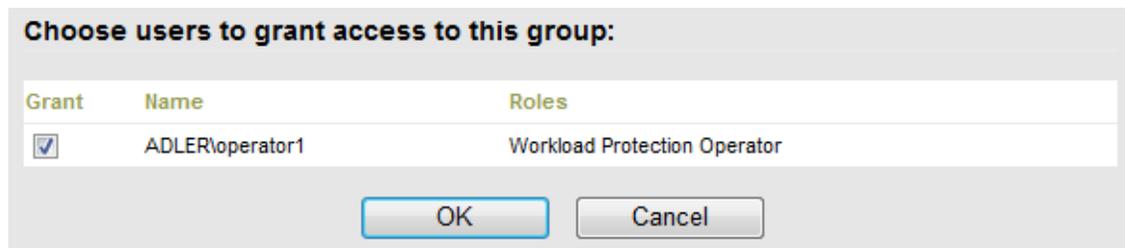
Ya puede añadir al usuario a un grupo de seguridad de PlateSpin Protect y asociarlo a un conjunto específico de cargas de trabajo. Consulte [“Gestión de los grupos de seguridad de PlateSpin Protect y los permisos de la carga de trabajo”](#) en la página 24.

2.2.3 Gestión de los grupos de seguridad de PlateSpin Protect y los permisos de la carga de trabajo

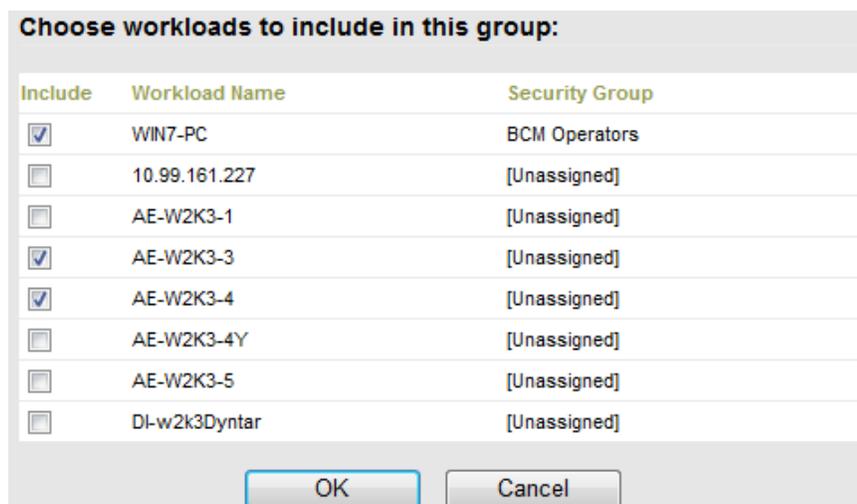
PlateSpin Protect proporciona un mecanismo de acceso de nivel de aplicación detallado que permite a usuarios concretos realizar tareas específicas de protección de la carga de trabajo en cargas de trabajo determinadas. Esto se realiza configurando *grupos de seguridad*.

- 1 Asigne un usuario de PlateSpin Protect a la función de protección de la carga de trabajo cuyos permisos se adapten mejor a dicha función en su organización. Consulte [“Asignación de una función de protección de carga de trabajo a un usuario de PlateSpin Protect”](#) en la página 23.
- 2 Acceda a PlateSpin Protect como administrador en la interfaz Web de PlateSpin Forge y haga clic en *Settings > Permissions* (Configuración > Permisos).
Se abre la página Security Groups (Grupos de seguridad).
- 3 Haga clic en *Create Security Group* (Crear grupo de seguridad).
- 4 En el campo *Security Group Name* (Nombre del grupo de seguridad), indique un nombre para el grupo de seguridad.
- 5 Haga clic en *Add Users* (Añadir usuarios) y seleccione los usuarios necesarios para este grupo de seguridad.

Si desea añadir a un usuario de PlateSpin Protect que se haya añadido recientemente al host del servidor de PlateSpin, puede que no esté disponible de inmediato en la interfaz de usuario. En tal caso, haga clic primero en *Refresh User Accounts* (Actualizar cuentas del usuario).



- 6 Haga clic en *Add Workloads* (Añadir cargas de trabajo) y seleccione las cargas de trabajo necesarias:



Solo los usuarios de este grupo de seguridad tendrán acceso a las cargas de trabajo seleccionadas.

7 Haga clic en *Crear*.

La página se vuelve a cargar muestra el nuevo grupo en la lista de grupos de seguridad.

Para editar un grupo de seguridad, haga clic en su nombre en la lista de grupos de seguridad.

2.3 Requisitos de acceso y comunicación en la red de protección

En esta sección se incluye la información siguiente:

- ♦ [Sección 2.3.1, “Requisitos de acceso y comunicación para las cargas de trabajo”, en la página 25](#)
- ♦ [Sección 2.3.2, “Requisitos de acceso y comunicación para los contenedores”, en la página 27](#)
- ♦ [Sección 2.3.3, “Requisitos de apertura de puertos para los hosts de servidores de PlateSpin”, en la página 27](#)
- ♦ [Sección 2.3.4, “Protección en redes públicas y privadas mediante NAT”, en la página 28](#)
- ♦ [Sección 2.3.5, “Anulación de la shell bash por defecto para ejecutar comandos en cargas de trabajo Linux”, en la página 28](#)
- ♦ [Sección 2.3.6, “Requisitos de clústeres DRS VMware como contenedores”, en la página 29](#)

2.3.1 Requisitos de acceso y comunicación para las cargas de trabajo

Los requisitos de software, redes y cortafuegos siguientes se aplican a las cargas de trabajo que pretende proteger mediante PlateSpin Protect.

Tabla 2-2 *Requisitos de acceso y comunicación para las cargas de trabajo*

Tipo de carga de trabajo	Requisitos previos	Puertos necesarios (por defecto)
Todas las cargas de trabajo	Compatible con ping (petición y respuesta de eco ICMP)	
Todas las cargas de trabajo Windows	Microsoft .NET Framework versión 2.0 o 3.5 SP1	

Tipo de carga de trabajo	Requisitos previos	Puertos necesarios (por defecto)
Windows 7; Windows Server 2008;	<ul style="list-style-type: none"> ◆ Credenciales de cuenta de administrador o de administrador del dominio incorporadas (no es suficiente solo ser miembro del grupo de administradores). En Vista, la cuenta debe estar habilitada (está inhabilitada por defecto). 	TCP 3725 NetBIOS 137 - 139
Windows Vista	<ul style="list-style-type: none"> ◆ El Firewall de Windows debe estar configurado para permitir la opción <i>Compartir archivos e impresoras</i>. Use una de estas opciones: <ul style="list-style-type: none"> ◆ Opción 1, uso del Firewall de Windows: use el elemento básico del Panel de control <i>Firewall de Windows</i> (<i>firewall.cpl</i>) y seleccione <i>Compartir archivos e impresoras</i> en la lista de excepciones. - O bien - ◆ Opción 2, uso del Firewall con seguridad avanzada: use la utilidad <i>Firewall de Windows con seguridad avanzada</i> (<i>wf.msc</i>) con la opción <i>Reglas de entrada</i> habilitada y definida como <i>Permitir</i>: <ul style="list-style-type: none"> ◆ <i>Compartir archivos e impresoras (solicitud eco: ICMPv4In)</i> ◆ <i>Compartir archivos e impresoras (solicitud eco: ICMPv6In)</i> ◆ <i>Compartir archivos e impresoras (datagrama NB de entrada)</i> ◆ <i>Compartir archivos e impresoras (nombre NB de entrada)</i> ◆ <i>Compartir archivos e impresoras (sesión NB de entrada)</i> ◆ <i>Compartir archivos e impresoras (SMB de entrada)</i> ◆ <i>Compartir archivos e impresoras (administrador de trabajos de impresión: RPC)</i> ◆ <i>Compartir archivos e impresoras (administrador de trabajos de impresión: RPC-EPMAP)</i> 	SMB (TCP 139, 445 y UDP 137, 138) TCP 135/445
Windows Server 2003 (incluidos SP1 Standard, SP2 Enterprise y R2 SP2 Enterprise)	<p>Nota: después de habilitar los puertos necesarios, ejecute el comando siguiente en el indicador del servidor para habilitar la administración remota de PlateSpin:</p> <pre>netsh firewall set service RemoteAdmin enable</pre> <p>Para obtener más información sobre netsh, consulte el artículo de Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx).</p>	<ul style="list-style-type: none"> ◆ TCP: 3725, 135, 139, 445 ◆ UDP: 137, 138, 139

Tipo de carga de trabajo	Requisitos previos	Puertos necesarios (por defecto)
Windows Server 2000; Windows XP	<ul style="list-style-type: none"> Instrumental de administración de Windows (WMI) instalado <p>WMI (RPC/DCOM) puede usar los puertos TCP 135 y 445, así como puertos aleatorios o asignados de forma dinámica por encima del 1024. Si se producen problemas al añadir la carga de trabajo, puede colocar de forma temporal la carga de trabajo en una zona desmilitarizada o abrir temporalmente los puertos bloqueados por el cortafuegos mientras se añade la carga de trabajo en PlateSpin Protect.</p> <p>Para obtener información adicional, como instrucciones para limitar el rango de puertos para DCOM y RPC, consulte los siguientes artículos técnicos de Microsoft.</p> <ul style="list-style-type: none"> Uso de DCOM con servidores de seguridad (http://msdn.microsoft.com/en-us/library/ms809327.aspx) Cómo configurar la asignación dinámica de puertos RPC para trabajar con servidores de seguridad (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) Cómo configurar DCOM para que funcione en un Firewall basado en NAT (http://support.microsoft.com/kb/248809) 	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 y UDP 137, 138) RPC (TCP 135)
Todas las cargas de trabajo Linux	Servidor de shell segura (SSH)	TCP 22, 3725

2.3.2 Requisitos de acceso y comunicación para los contenedores

Los requisitos de software, redes y cortafuegos siguientes se aplican a los contenedores de carga de trabajo admitidos.

Tabla 2-3 Requisitos de acceso y comunicación para los contenedores

Sistema	Requisitos previos	Puertos necesarios (por defecto)
Todos los contenedores	Compatible con ping (petición y respuesta de eco ICMP)	
VMware ESX/ESXi 4.1	<ul style="list-style-type: none"> Cuenta de VMware con función de administrador 	HTTPS (TCP 443)
VMware ESXi 5.0	<ul style="list-style-type: none"> API de servicios Web de VMware y API de gestión de archivos 	
vCenter Server	El usuario con acceso debe tener asignados los permisos y las funciones correspondientes. Consulte la documentación de la versión específica de VMware para obtener más información.	HTTPS (TCP 443)

2.3.3 Requisitos de apertura de puertos para los hosts de servidores de PlateSpin

Los requisitos de apertura de puertos siguientes se aplican a los hosts de servidores de PlateSpin.

Tabla 2-4 Requisitos de apertura de puertos para los hosts de servidores de PlateSpin

Puerto (por defecto)	Observaciones
TCP 80	Para comunicaciones HTTP
TCP 443	Para comunicaciones HTTPS (si SSL está habilitado)

2.3.4 Protección en redes públicas y privadas mediante NAT

En ciertos casos, un origen, un destino o el propio PlateSpin Protect pueden estar situados en una red (privada) interna protegida por un dispositivo de traducción de direcciones de red (NAT) que no puede comunicarse con su equivalente durante la protección.

PlateSpin Protect permite resolver este problema, según cuál de los hosts siguientes esté ubicado tras el dispositivo NAT:

- ♦ **Servidor de PlateSpin:** en la herramienta *PlateSpin Server Configuration*, registre las direcciones IP adicionales asignadas al host. Consulte [“Configuración de la aplicación para que funcione con NAT” en la página 28](#).
- ♦ **Contenedor de destino:** cuando intente descubrir un contenedor (por ejemplo, VMware ESX), especifique la dirección IP pública (o externa) del host en los parámetros de descubrimiento.
- ♦ **Carga de trabajo:** si intenta añadir una carga de trabajo, especifique la dirección IP pública (externa) de la carga de trabajo en los parámetros de descubrimiento.
- ♦ **Máquina virtual en failover:** durante el failback, puede especificar una dirección IP alternativa para la carga de trabajo en failover en [Detalles de failback \(carga de trabajo en máquina virtual\) en la página 63](#).
- ♦ **Destino de failback:** durante un intento para registrar un destino de failback, cuando se le pida que proporcione la dirección IP del servidor de PlateSpin, proporcione la dirección local del host del servidor de protección o una de sus direcciones públicas (externas) registradas en la herramienta *PlateSpin Server Configuration* del servidor (consulte *Servidor de PlateSpin* más arriba).

Configuración de la aplicación para que funcione con NAT

Para habilitar el servidor de PlateSpin a fin de que funcione en entornos con NAT habilitada, debe registrar direcciones IP adicionales del servidor de PlateSpin en la base de datos de la herramienta *PlateSpin Server Configuration* que el servidor lee durante el inicio.

Para obtener información sobre el procedimiento de actualización, consulte [“Configuración del comportamiento del servidor de PlateSpin mediante parámetros de configuración XML” en la página 34](#).

2.3.5 Anulación de la shell bash por defecto para ejecutar comandos en cargas de trabajo Linux

El servidor de PlateSpin usa por defecto la shell `/bin/bash` para ejecutar comandos en una carga de trabajo de origen Linux.

Si se requiere, puede anular la shell por defecto modificando la clave de registro correspondiente en el servidor de PlateSpin.

Consulte el [artículo 7010676 de la KB \(https://www.netiq.com/support/kb/doc.php?id=7010676\)](https://www.netiq.com/support/kb/doc.php?id=7010676).

2.3.6 Requisitos de clústeres DRS VMware como contenedores

Para ser un destino de protección válido, el clúster DRS VMware debe añadirse al conjunto de contenedores (inventariarse) como clúster VMware. No debe intentar añadir un clúster DRS como conjunto de servidores ESX individuales. Consulte [“Adición de contenedores \(destinos de protección\)” en la página 51](#).

Además, el clúster DRS VMware debe cumplir los siguientes requisitos de configuración:

- ♦ DRS debe estar habilitado y establecido como `Partially Automated` (Parcialmente automatizado) o `Fully Automated` (Totalmente automatizado).
- ♦ Debe existir al menos un almacén de datos compartido entre todos los servidores ESX del clúster VMware.
- ♦ Debe existir al menos un vSwitch y un grupo virtual de puertos, o bien un conmutador distribuido de vNetwork, compartido entre todos los servidores ESX del clúster VMware.
- ♦ Las cargas de trabajo de failover (máquinas virtuales) de cada contrato de protección se sitúan exclusivamente en los almacenes de datos, vSwitch y grupos virtuales de puertos compartidos entre todos los servidores ESX del clúster VMware.

2.4 Configuración de las opciones por defecto de PlateSpin Protect

En esta sección se incluye la información siguiente:

- ♦ [Sección 2.4.1, “Configuración de notificaciones automáticas por correo electrónico de eventos e informes”, en la página 29](#)
- ♦ [Sección 2.4.2, “Configuración de idiomas para versiones internacionales de PlateSpin Protect”, en la página 33](#)
- ♦ [Sección 2.4.3, “Configuración del comportamiento del servidor de PlateSpin mediante parámetros de configuración XML”, en la página 34](#)
- ♦ [Sección 2.4.4, “Configuración de la compatibilidad con VMware vCenter Site Recovery Manager”, en la página 36](#)

2.4.1 Configuración de notificaciones automáticas por correo electrónico de eventos e informes

Es posible configurar PlateSpin Protect para que envíe automáticamente notificaciones de eventos e informes de réplica a direcciones de correo electrónico específicas. Esta función requiere que primero se especifique un servidor SMTP válido para que PlateSpin Protect lo use.

- ♦ [“Configuración de SMTP” en la página 30](#)
- ♦ [“Configuración de notificaciones automáticas sobre eventos por correo electrónico” en la página 30](#)
- ♦ [“Configuración de envío de informes de réplica automáticos por correo electrónico” en la página 32](#)

Configuración de SMTP

Use la interfaz Web de PlateSpin Protect para configurar los valores de SMTP (protocolo simple de transferencia de correo) del servidor usado para entregar las notificaciones de correo sobre eventos y los informes de réplica.

Figura 2-1 Configuración del protocolo simple de transferencia de correo (SMTP)



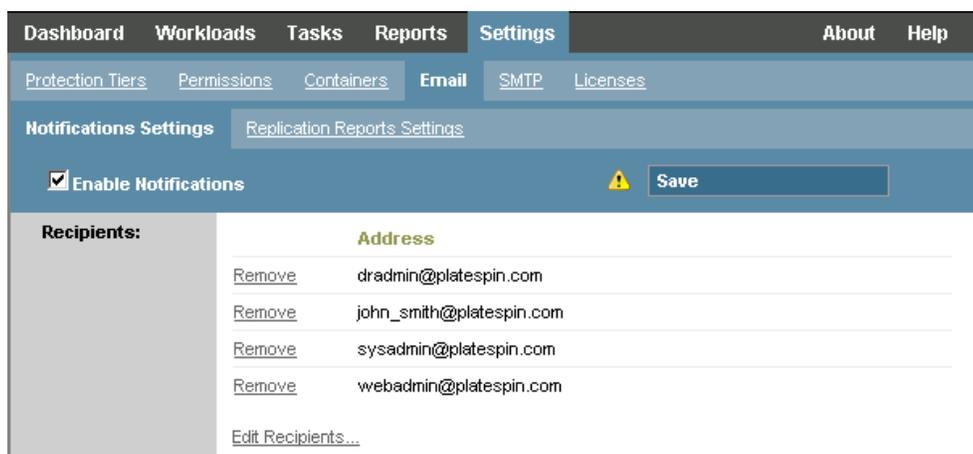
SMTP Settings		Save
SMTP Server Address:	<input type="text"/>	
Port:	<input type="text" value="25"/>	
Reply Address:	<input type="text"/>	
Username:	<input type="text"/>	
Password:	<input type="text"/>	
Confirm:	<input type="text"/>	

Para configurar los valores de SMTP:

- 1 En la interfaz Web de PlateSpin Protect, haga clic en *Settings* > *SMTP* (Configuración > SMTP).
- 2 Especifique los valores *Address* (Dirección), *Port* (Puerto, por defecto es el 25) y *Reply Address* (Dirección de respuesta) para recibir notificaciones por correo electrónico sobre eventos y progreso.
- 3 Indique un valor en *Username* (Nombre de usuario) y *Password* (Contraseña) y confirme la contraseña.
- 4 Haga clic en *Guardar*.

Configuración de notificaciones automáticas sobre eventos por correo electrónico

- 1 Configure un servidor SMTP para que lo use PlateSpin Protect. Consulte [“Configuración de SMTP” en la página 30](#).
- 2 En la interfaz Web de PlateSpin Protect, haga clic en *Settings* > *Email* > *Notification Settings* (Configuración > Correo electrónico > Configuración de notificación).
- 3 Seleccione la opción *Enable Notifications* (Habilitar notificaciones).
- 4 Haga clic en *Edit Recipients* (Editar destinatarios), indique las direcciones de correo electrónico necesarias separadas por comas y haga clic en *OK* (Aceptar).



5 Haga clic en *Guardar*.

Para suprimir direcciones de correo electrónico mostradas, haga clic en la opción *Remove* (Eliminar) situada junto a la dirección que desea suprimir.

Los eventos siguientes activan las notificaciones de correo electrónico:

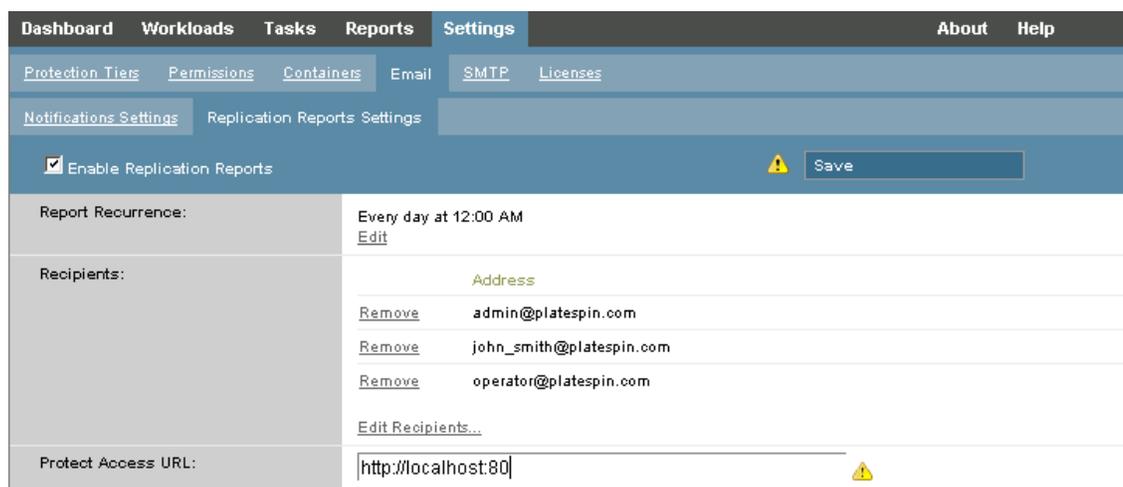
Evento	Observaciones
Carga de trabajo en línea detectada	Se genera cuando el sistema detecta que una carga de trabajo anteriormente sin conexión está ahora en línea. Se aplica a las cargas de trabajo cuyo estado de contrato no es <i>En pausa</i> .
Carga de trabajo sin conexión detectada	Se genera cuando el sistema detecta que una carga de trabajo anteriormente en línea está ahora sin conexión. Se aplica a las cargas de trabajo cuyo estado de contrato no es <i>En pausa</i> .
Réplica completa terminada correctamente	
Error en réplica completa	
Réplica completa perdida	Similar al evento Réplica incremental perdida.
Réplica incremental terminada correctamente	
Error en réplica incremental	

Evento	Observaciones
Réplica incremental perdida	Se genera cuando se produce una de estas circunstancias: <ul style="list-style-type: none"> ♦ Una réplica se pausa manualmente mientras se realiza una réplica incremental programada. ♦ El sistema intenta llevar a cabo una réplica incremental programada mientras se efectúa una réplica activada manualmente. ♦ El sistema determina que el destino no tiene suficiente espacio en disco.
Prueba de failover terminada	Se genera al marcar manualmente una operación de prueba de failover como correcta o errónea.
Preparación de failover terminada	
Error al preparar el failover	
Failover terminado	
Error en failover	

Configuración de envío de informes de réplica automáticos por correo electrónico

Para configurar PlateSpin Protect de modo que envíe automáticamente informes de replicación por correo electrónico, lleve a cabo estos pasos:

- 1 Configure un servidor SMTP para que lo use PlateSpin Protect. Consulte [Configuración de SMTP \(en la página 30\)](#).
- 2 En la interfaz Web de PlateSpin Protect, haga clic en *Settings > Email > Replication Reports Settings* (Configuración > Correo electrónico > Configuración de informes de réplica).
- 3 Seleccione la opción *Enable Replication Reports* (Habilitar informes de réplica).
- 4 En la sección *Report Recurrence* (Recurrencia de informes), haga clic en *Configure* (Configurar) y especifique el patrón de recurrencia necesario para los informes.
- 5 En la sección *Recipients* (Destinatarios), haga clic en *Edit Recipients* (Editar destinatarios), indique las direcciones de correo electrónico necesarias separadas por comas y haga clic en *OK* (Aceptar).



6 (Opcional) En la sección *Protect Access URL* (URL de acceso a Protect), especifique una URL si no usa la dirección por defecto para el servidor de PlateSpin (por ejemplo, si el host del servidor de PlateSpin tiene más de una NIC o si está protegida por un servidor NAT). Esta URL afecta al título del informe y a la función para acceder a contenido relevante en el servidor mediante hiperenlaces dentro de los informes enviados por correo electrónico.

7 Haga clic en *Guardar*.

Para obtener información sobre otros tipos de informes que se pueden generar y ver a pedido, consulte [“Generación de informes de carga de trabajo y de protección de la carga de trabajo”](#) en la [página 48](#).

2.4.2 Configuración de idiomas para versiones internacionales de PlateSpin Protect

PlateSpin Protect proporciona compatibilidad con otros idiomas para alemán, chino simplificado, chino tradicional, francés y japonés.

Para usar la interfaz Web de PlateSpin Protect y la ayuda integrada en uno de estos idiomas, este debe añadirse al navegador Web y trasladarse a la parte superior del orden de preferencia:

- 1 Acceda a la configuración de idiomas del navegador Web:
 - ♦ **Internet Explorer:** haga clic en *Herramientas > Opciones de Internet > pestaña General > Idiomas*.
 - ♦ **Firefox:** haga clic en *Herramientas > Opciones > pestaña Contenido > Idiomas*.
- 2 Añada el idioma requerido y súbalo a la parte superior de la lista.
- 3 Guarde la configuración e inicie la aplicación cliente conectándose con el servidor de PlateSpin . Consulte [“Apertura de la interfaz Web de PlateSpin Protect”](#) en la [página 39](#).

Nota: (para usuarios de las versiones en chino tradicional y chino simplificado) si se intenta conectar con el servidor de PlateSpin con un navegador que no cuente con una versión específica para el chino, podrían producirse errores en el servidor Web. Para un funcionamiento correcto, use la configuración del navegador para añadir una versión específica del chino (por ejemplo, Chino [zh-cn] o Chino [zh-tw]). No use una versión neutral como Chino [zh].

El idioma de una pequeña parte de los mensajes del sistema generados por el servidor de PlateSpin depende del idioma de la interfaz del sistema operativo seleccionada en el host del servidor de PlateSpin:

- 1 Acceda al host del servidor de PlateSpin.
- 2 Inicie el applet Configuración regional y de idioma (haga clic en *Inicio > Ejecutar*, escriba `intl.cpl` y pulse Intro) y haga clic en la pestaña *Idiomas* (Windows Server 2003) o *Teclados e idiomas* (Windows Server 2008), según el caso.
- 3 Si aún no lo está, instale el paquete de idioma necesario. Puede que tenga que acceder al medio del instalación del sistema operativo.
- 4 Seleccione el idioma requerido como idioma de interfaz del sistema operativo. Cuando se le pida, salga de la sesión o reinicie el sistema.

2.4.3 Configuración del comportamiento del servidor de PlateSpin mediante parámetros de configuración XML

Algunos aspectos del comportamiento del servidor de PlateSpin se controlan mediante parámetros de configuración que se establecen en una página Web de configuración del host del servidor de PlateSpin (https://servidor_de_PlateSpin/platespinconfiguration/).

En circunstancias normales, estos valores no se deben modificar a no ser que se lo indique el servicio técnico de PlateSpin. En esta sección se explican varios casos de uso habituales y se incluye información sobre el procedimiento requerido.

Lleve a cabo el siguiente procedimiento para modificar y aplicar cualquier parámetro de configuración:

- 1 Desde cualquier navegador Web, abra https://servidor_PlateSpin/platespinconfiguration/.
- 2 Localice el parámetro de servidor necesario y cambie su valor.
- 3 Guarde la configuración y salga de la página.

No es necesario rearrancar ni reiniciar servicios después de realizar el cambio en la herramienta de configuración.

Los temas siguientes proporcionan información sobre soluciones específicas en las que puede que tenga que cambiar el comportamiento del producto mediante un valor de configuración XML.

- ♦ [“Optimización de transferencia de datos en conexiones WAN” en la página 34](#)
- ♦ [“Configuración de la compatibilidad con SRM” en la página 35](#)

Optimización de transferencia de datos en conexiones WAN

Puede optimizar el rendimiento de la transferencia de datos y realizar ajustes más precisos para las conexiones WAN. Para ello, debe modificar los parámetros de configuración que el sistema lee de los ajustes que se realizan en una herramienta de configuración situada en el host del servidor de PlateSpin. Para el procedimiento genérico, consulte [“Configuración del comportamiento del servidor de PlateSpin mediante parámetros de configuración XML” en la página 34](#).

Use estos valores para optimizar las transferencias de datos en una red WAN. Estos valores son globales y afectan a todas las réplicas basadas en archivos y VSS.

Nota: si se modifican estos valores, puede afectar negativamente al tiempo que tarda la réplica en redes de alta velocidad, como Gigabit Ethernet. Antes de modificar cualquiera de estos valores, consulte al servicio técnico de PlateSpin.

La [Tabla 2-5](#) muestra los parámetros de configuración con los valores por defecto y los recomendados para un funcionamiento óptimo en un entorno WAN de alta latencia.

Tabla 2-5 Parámetros de configuración por defecto y optimizados de https://servidor_de_PlateSpin/platespinconfiguration/

Parámetro	Valor por defecto	Valor optimizado
<code>fileTransferMinCompressionLimit</code> Especifica el umbral de compresión de nivel de paquete en bytes.	0 (inhabilitado)	Máx. 65536 (64 KB)
<code>fileTransferCompressionThreadsCount</code> Controla el número de hilos usados para la compresión de datos de nivel de paquete. Si la compresión está inhabilitada, este parámetro se ignora. Dado que la compresión depende de la CPU, este valor puede tener efecto en el rendimiento.	2	N/D
<code>fileTransferSendReceiveBufferSize</code> Ajuste de tamaño de la ventana de TCP/IP para las conexiones de transferencia de archivos. Controla el número de bytes enviado sin reconocimiento TCP. Si el valor se define en 0, se usa el tamaño por defecto de la ventana TCP (8 KB). En caso de tamaños personalizados, especifique el tamaño en bytes. Use la fórmula siguiente para determinar el valor oportuno: $((\text{VELOCIDAD_ENLACE}(\text{Mb/s})/8) * \text{RETRASO}(\text{s})) * 1000 * 1000$ Por ejemplo, para un enlace de 100 Mb/s con una latencia de 10 ms, el tamaño de buffer adecuado sería: $(100/8) * 0.01 * 1000 * 1000 = 125000 \text{ bytes}$	0 (8192 bytes)	Máx. 5242880 (5 MB)

Configuración de la compatibilidad con SRM

Las cargas de trabajo replicadas por PlateSpin Protect y gestionadas en VMware vCenter Site Recovery Manager (SRM) pueden interactuar sin problemas si configura el producto para admitir SRM. Parte de la configuración requiere un cambio en los parámetros de configuración XML del servidor de PlateSpin. Para obtener información sobre estos cambios de configuración, consulte la sección completa: [Sección 2.4.4, “Configuración de la compatibilidad con VMware vCenter Site Recovery Manager”](#), en la página 36.

2.4.4 Configuración de la compatibilidad con VMware vCenter Site Recovery Manager

Puede usar PlateSpin Protect para proteger las cargas de trabajo de forma local y, después, usar algún método adicional para replicarlas a una ubicación remota, como una red SAN. Por ejemplo, puede usar VMware vCenter Site Recovery Manager (SRM) para replicar todo el almacén de datos de máquinas virtuales de destino replicadas a un sitio remoto. En tal caso, se necesario realizar pasos de configuración específicos para garantizar que las máquinas virtuales de destino se pueden replicar y tienen un comportamiento correcto cuando se activan en el sitio remoto.

La configuración para la compatibilidad de con SRM consta de los siguientes ajustes:

- ♦ Configurar un valor para conservar la imagen ISO y los discos de PlateSpin Protect en el mismo almacén de datos que los archivos `.vmtx` y `..vmdk` de VMware.
- ♦ Preparar el entorno de PlateSpin Protect para copiar VMware Tools en el destino de failover. Esto implica la creación y copia manual de algunos archivos, además de realizar algunos ajustes de configuración para acelerar el proceso de instalación de VMware Tools.

Lleve a cabo los pasos siguientes para asegurarse de que los archivos de carga de trabajo se mantienen en el mismo almacén de datos:

- 1 En cualquier navegador Web, abra `https://Servidor_de_PlateSpin/platespinconfiguration/` para mostrar la página Web de configuración.
- 2 En la página Web de configuración, localice el parámetro de servidor `CreatePSFilesInVmDatastore` y cambie su valor a `true` (verdadero).

Nota: la persona que configure el [contrato de réplica](#) será la responsable de asegurarse de que se especifica el mismo almacén de datos para todos los archivos de disco de la máquina virtual de destino.

- 3 Guarde la configuración y salga de la página.

Los paquetes de configuración de VMware Tools se pueden copiar en el destino de failover durante la réplica, de forma que el servicio de configuración los pueda instalar al arrancar la máquina virtual. Esto se produce de forma automática si el destino de failover es capaz de ponerse en contacto con el servidor de Protect. En los casos en los que esto no sea posible, debe preparar el entorno antes de la réplica llevando a cabo estos pasos:

- 1 Recupere los paquetes de VMware Tools de un host ESX:
 - 1a Copie de forma segura (`scp`) la imagen `windows.iso` del directorio `/usr/lib/vmware/isoimages` en un host VMware al que se pueda acceder en una carpeta temporal local.
 - 1b Abra la imagen ISO, extraiga los paquetes de configuración y guárdelos en una ubicación a la que se pueda acceder:
 - ♦ **VMware 5.0 y 5.1:** los paquetes de configuración son `setup.exe` y `setup64.exe`.
 - ♦ **VMware 4.0 y 4.1:** los paquetes de configuración son `VMware Tools.msi` y `VMware Tools64.msi`.
- 2 Cree paquetes OFX a partir de los paquetes de configuración que ha extraído del servidor de VMware:
 - 2a Comprima el paquete que desee, asegurándose de que el archivo de configuración se encuentra en la raíz del archivo de reserva `.zip`.
 - 2b Cambie el nombre del archivo de reserva `.zip` a `1.package` para que se pueda usar como paquete OFX.

Nota: si desea crear un paquete OFX para más de un paquete de configuración, recuerde que cada paquete de instalación debe tener su propio archivo de reserva .zip exclusivo.

Puesto que todos los paquetes deben tener el mismo nombre (1.package), si desea guardar varios archivos de reserva .zip como paquetes OFX, debe hacerlo en distintos subdirectorios exclusivos.

- 3 Copie el paquete OFX oportuno (1.package) a %ProgramFiles(x86)%\PlateSpin\Packages\%GUID% en el servidor de PlateSpin. El valor de %GUID% depende de la versión del servidor de VMware y de la arquitectura de VMware Tools.

En la tabla siguiente se muestran las versiones del servidor, la arquitectura de VMware Tools y el identificador GUID que debe copiar en el paquete en el directorio correcto:

Versión del servidor de VMware	Arquitectura de VMware Tools	GUID
4.0	x86	D052CBAC-0A98-4880-8BCC-FE0608F0930F
4.0	x64	80B50267-B30C-4001-ABDF-EA288D1FD09C
4.1	x86	F2957064-65D7-4bda-A52B-3F5859624602
4.1	x64	80B1C53C-6B43-4843-9D63-E9911E9A15D5
5.0	x86	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5.0	x64	F7C9BC91-7733-4790-B7AF-62E074B73882
5.1	x86	34DD2CBE-183E-492f-9B36-7A8326080755
5.1	x64	AD4FDE1D-DE86-4d05-B147-071F4E1D0326

Aceleración del proceso de configuración

Cuando se arranca un destino de failover, se lanza el servicio de configuración para preparar el uso de la máquina virtual, pero se mantiene inactivo varios minutos a la espera de los datos del servidor de PlateSpin o buscando VMware Tools en el CD ROM. Para reducir este tiempo de espera,

- 1 En la página Web de configuración, localice el ajuste `ConfigurationServiceValues` y cambie el valor de su ajuste secundario `WaitForFloppyTimeoutInSecs` a cero (0).
- 2 En la página Web de configuración, localice el parámetro de servidor `ForceInstallVMToolsCustomPackage` y cambie su valor a `true` (verdadero).

Con estos ajustes realizados, el proceso de configuración tarda menos de 15 minutos: el destino se arranca (hasta dos veces), VMware Tools se instala y SRM accede a las herramientas para ayudarle a configurar la conectividad del sitio remoto.

3 Activación y ejecución

Esta sección proporciona información sobre las funciones esenciales de PlateSpin Protect y su interfaz.

- ♦ Sección 3.1, “Apertura de la interfaz Web de PlateSpin Protect”, en la página 39
- ♦ Sección 3.2, “Elementos de la interfaz Web de PlateSpin Protect”, en la página 40
- ♦ Sección 3.3, “Cargas de trabajo y comandos de carga de trabajo”, en la página 42
- ♦ Sección 3.4, “Gestión de varias instancias de PlateSpin Protect y PlateSpin Forge”, en la página 44
- ♦ Sección 3.5, “Generación de informes de carga de trabajo y de protección de la carga de trabajo”, en la página 48

3.1 Apertura de la interfaz Web de PlateSpin Protect

La mayor parte de la interacción con el dispositivo se realiza a través del cliente Web basado en navegador de PlateSpin Protect.

Los navegadores compatibles son:

- ♦ *Google Chrome*, versión 34.0 y posteriores
- ♦ *Microsoft Internet Explorer*, versión 11.0 y posteriores
- ♦ *Mozilla Firefox*, versión 29.0 y posteriores

Nota: JavaScript (Active Scripting) debe estar habilitado en el navegador:

- ♦ **Chrome:** en el menú de Chrome, seleccione **Configuración > Mostrar opciones avanzadas > Configuración de contenido > Permitir que todos los sitios ejecuten JavaScript**.
- ♦ **IE:** en el menú Herramientas, seleccione **Opciones de Internet > Seguridad**, haga clic en **Nivel personalizado**, avance hasta **Active scripting** y seleccione **Habilitar**, haga clic en **Sí** en el recuadro de diálogo de advertencia y haga clic en **Aceptar**, > **Aplicar** y de nuevo en **Aceptar**.
- ♦ **Firefox:** haga clic en **Herramientas > Opciones > Contenido** y seleccione la opción **Habilitar JavaScript**.

Para utilizar la interfaz Web de PlateSpin Protect y la ayuda integrada en uno de los idiomas admitidos, consulte la [Sección 2.4.2, “Configuración de idiomas para versiones internacionales de PlateSpin Protect”, en la página 33](#).

Para lanzar la interfaz Web de PlateSpin Protect:

- 1 Abra un navegador Web y diríjase a:
`https://<nombre_de_host | dirección_IP>/Protect`

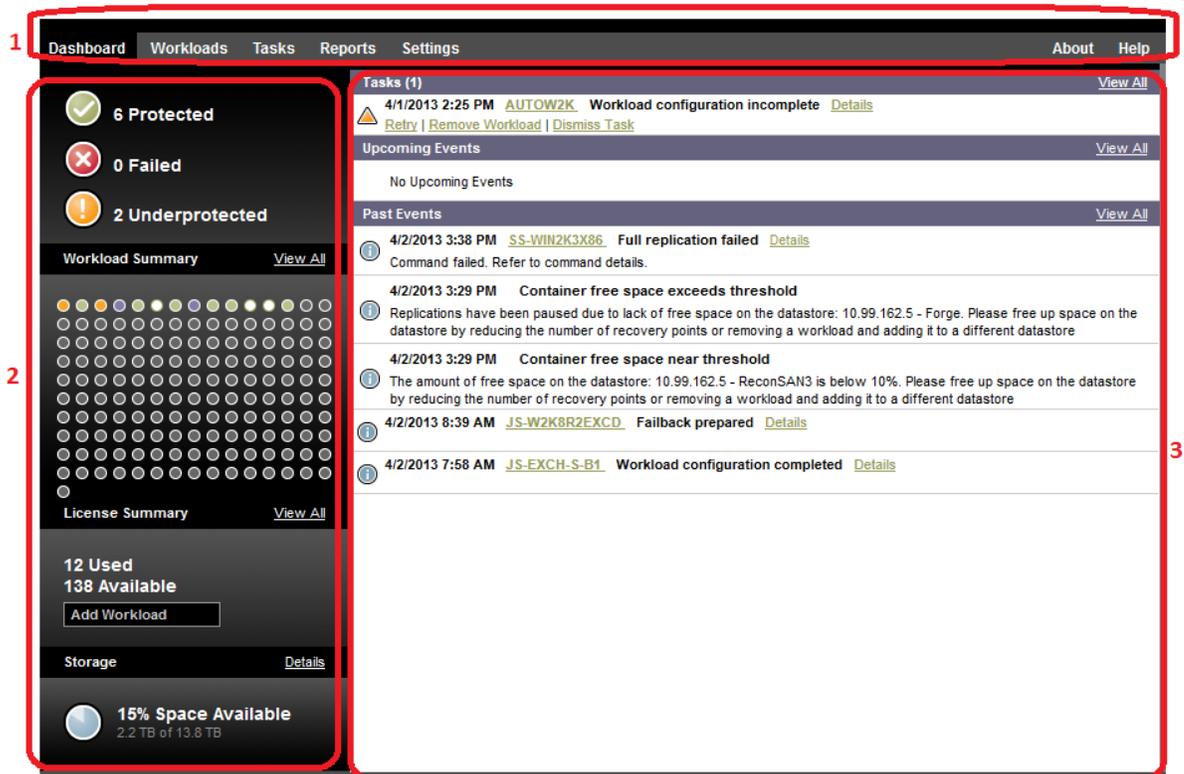
Sustituya <nombre_de_host | dirección_IP> con el nombre de host o la dirección IP del host del servidor de PlateSpin.

Si SSL no está habilitado, use http en la URL.

3.2 Elementos de la interfaz Web de PlateSpin Protect

La ventana por defecto de la interfaz Web de PlateSpin Protect es la página Dashboard (Consola), que contiene elementos para navegar a distintas áreas funcionales de la interfaz y llevar a cabo las operaciones de protección y recuperación de la carga de trabajo.

Figura 3-1 Página Dashboard (Consola) por defecto de la interfaz Web de PlateSpin Protect



La página Dashboard (Consola) está formada por los elementos siguientes:

1. **Barra de navegación:** se encuentra en la mayoría de las páginas de la interfaz Web de PlateSpin Protect.
2. **Panel de resumen visual:** proporciona un vista de nivel superior del estado general del inventario de la carga de trabajo de PlateSpin Protect.
3. **Panel de tareas y eventos:** proporciona información sobre los eventos y tareas que requieren la atención del usuario.

En los temas siguientes se proporcionan más detalles:

- ♦ Sección 3.2.1, “Barra de navegación”, en la página 41
- ♦ Sección 3.2.2, “Panel de resumen visual”, en la página 41
- ♦ Sección 3.2.3, “Panel de tareas y eventos”, en la página 42

3.2.1 Barra de navegación

La barra de navegación incluye los enlaces siguientes:

- ♦ **Dashboard (Consola):** muestra la página por defecto, Dashboard (Consola).
- ♦ **Workloads (Cargas de trabajo):** muestra la página de cargas de trabajo. Consulte [“Cargas de trabajo y comandos de carga de trabajo”](#) en la página 42.
- ♦ **Tasks (Tareas):** muestra la página de tareas, donde aparecen los elementos que requieren la intervención del usuario.
- ♦ **Reports (Informes):** muestra la página de informes. Consulte [“Generación de informes de carga de trabajo y de protección de la carga de trabajo”](#) en la página 48.
- ♦ **Settings (Configuración):** muestra la página de configuración, que proporciona acceso a las siguientes opciones de configuración:
 - ♦ **Protection Tiers (Niveles de protección):** consulte [“Niveles de protección”](#) en la página 76.
 - ♦ **Permissions (Permisos):** consulte [“Configuración de la autorización y la autenticación de usuarios”](#) en la página 21.
 - ♦ **Contenedores:** consulte [“Adición de contenedores \(destinos de protección\)”](#) en la página 51.
 - ♦ **Email/SMTP (Correo electrónico/SMTP):** consulte [“Configuración de notificaciones automáticas por correo electrónico de eventos e informes”](#) en la página 29.
 - ♦ **Licenses/License Designations (Licencias/Designación de licencias):** consulte [“Licencia del producto”](#) en la página 19.

3.2.2 Panel de resumen visual

El panel de resumen visual proporciona una vista de nivel superior de todas las cargas de trabajo con licencia y de la cantidad de espacio de almacenamiento disponible.

Las cargas de trabajo en inventario se representan en tres categorías:

- ♦ **Protected (Protegidas):** indica el número de cargas de trabajo protegidas de forma activa.
- ♦ **Failed (Con error):** indica el número de cargas de trabajo protegidas que tienen errores según el análisis del sistema del nivel de protección de dicha carga.
- ♦ **Underprotected (Con protección insuficiente):** indica el número de cargas de trabajo protegidas que requieren la atención del usuario.

El área en el centro del panel izquierdo representa un resumen gráfico de la página de cargas de trabajo. Usa los siguientes iconos de punto para representar los distintos estados de las cargas de trabajo:

Tabla 3-1 Representación de la carga de trabajo por iconos de puntos

● Sin protección	● Con protección insuficiente
○ Sin protección – Error	● Con error
● Protegida	● Ha caducado
● No se usa	

Los iconos se muestran en orden alfabético según el nombre de la carga de trabajo. Pase el ratón por los iconos para mostrar el nombre de la carga de trabajo o haga clic en el icono para mostrar la página de detalles de la carga de trabajo correspondiente.

Storage (Almacenamiento) proporciona información sobre el espacio del almacén de contenedores disponible en PlateSpin Protect.

3.2.3 Panel de tareas y eventos

El panel de tareas y eventos muestra las tareas más recientes, los eventos pasados más recientes y los próximos eventos futuros.

Los eventos se registran siempre que se produce cualquier cosa relevante para el sistema o para la carga de trabajo. Por ejemplo, un evento puede ser que se añada una nueva carga de trabajo protegida, el inicio o el error de réplica de una carga de trabajo o el fallo de una carga de trabajo protegida. Algunos eventos generan notificaciones automáticas por correo electrónico si SMTP está configurado. Consulte [“Configuración de notificaciones automáticas por correo electrónico de eventos e informes” en la página 29.](#)

Las tareas son comandos especiales relacionados con eventos que requieren la intervención del usuario. Por ejemplo, al completar un comando de prueba de failover, el sistema genera un evento asociado con dos tareas: `Mark Test as Success` (Marcar prueba como correcta) y `Mark Test as Failure` (Marcar prueba como error). Cuando se hace clic en una de estas tareas, se cancela la operación de prueba de failover y se escribe un evento correspondiente en el historial. Otro ejemplo es el evento `FullReplicationFailed`, que se muestra asociado a una tarea `StartFull`. Encontrará una lista completa de las tareas actuales en la pestaña *Tasks* (Tareas).

En el panel de tareas y eventos de la consola, cada categoría muestra un máximo de tres entradas. Para ver todas las tareas o los eventos pasados y futuros, haga clic en *View All* (Ver todo) en la sección oportuna.

3.3 Cargas de trabajo y comandos de carga de trabajo

La página *Workloads* (Cargas de trabajo) muestra una tabla con una fila para cada carga de trabajo en inventario. Haga clic en el nombre de una carga de trabajo para mostrar la página *Workload Details* (Detalles de la carga de trabajo) a fin de ver o editar las configuraciones relevantes a la carga de trabajo y su estado.

Figura 3-2 Página Workloads (Cargas de trabajo)

The screenshot shows the 'Workloads' page in the PlateSpin Protect interface. At the top, there are navigation tabs: Dashboard, Workloads (selected), Tasks, Reports, Settings, About, and Help. Below the tabs is a dropdown menu for 'All Workloads' and an 'Add Workload' button. The main content is a table with the following columns: Tasks, Online, Workload, Protection Tier, Schedule, Replication Status, Last Replication, Next Replication, and Last Test Failover. The table lists several workloads, including 'DI-RHEL5-1x64.platespin.com', 'DI-Sles10-SP3.platespin.com', 'DI-machine.platespin.com', 'DI-Sles11-sro-multi.platespin.com', 'RS-W2K3SP12NDDI', 'DI-RHEL5u4.platespin.com', 'failback', and 'doris'. Below the table are 'Select All' and 'Deselect All' links. Underneath is a 'Workload Commands' section with buttons for: Configure, Prepare Replication, Run Replication, Run Incremental, Pause Schedule, Resume Schedule, Test Failover, Prepare for Failover, Run Failover, Cancel Failover, Failback, and Remove Workload. At the bottom right, the server time is shown as 'Thursday, June 03, 2010 1:28 PM - Eastern Daylight Time'.

Nota: todas las marcas horarias muestran la zona horaria del host del servidor de PlateSpin. Puede ser distinta a la zona horaria de la carga de trabajo protegida o del host en el que se ejecute la interfaz Web de PlateSpin Protect. En la parte inferior derecha de la ventana del cliente se muestra la fecha y la hora del servidor.

3.3.1 Comandos de protección y recuperación de cargas de trabajo

Los comandos reflejan el flujo de trabajo de protección y recuperación de la carga de trabajo. Para realizar un comando para una carga de trabajo, seleccione la casilla de verificación correspondiente de la izquierda. Los comandos aplicables dependen del estado actual de la carga de trabajo.

Figura 3-3 Comandos de cargas de trabajo

This screenshot shows the 'Workloads' page with a different workload selected. The table shows two workloads: 'VM-SRC2' (which is not online and has an 'Unprotected' status) and 'VM-SRC5' (which is online, has an 'Hourly' schedule, and is in an 'Idle' replication status). The 'VM-SRC5' row is highlighted, and its checkbox is checked. The 'Workload Commands' section below the table shows the same set of buttons as in Figure 3-2, but the 'Failback' button is highlighted in a darker color, indicating it is the applicable command for the selected workload.

En la tabla siguiente se resumen los comandos de cargas de trabajo y se describen sus funciones.

Tabla 3-2 Comandos de protección y recuperación de cargas de trabajo

Comando de carga de trabajo	Descripción
<i>Configure</i> (Configurar)	Inicia la configuración de protección de la carga de trabajo con parámetros aplicables a una carga de trabajo en inventario.
<i>Prepare Replication</i> (Preparar réplica)	Instala el software de transferencia de datos requerido en el origen y crea una carga de trabajo de failover (una máquina virtual) en el contenedor de destino en preparación de la réplica de la carga de trabajo.
<i>Run Replication</i> (Ejecutar réplica)	Inicia la réplica de la carga de trabajo de acuerdo con los parámetros especificados (réplica completa).
<i>Run Incremental</i> (Ejecutar incremental)	Realiza una transferencia incremental de los datos cambiados desde el origen al destino situado fuera del contrato de protección de la carga de trabajo.
<i>Pause Schedule</i> (Pausar programación)	Suspende la protección. Todas las réplicas programadas se omiten hasta que se reanuda la programación.
<i>Resume Schedule</i> (Reanudar programación)	Reanuda la protección según los valores de protección guardados.
<i>Test Failover</i> (Probar failover)	Arranca y configura la carga de trabajo de failover en un entorno aislado dentro del contenedor para realizar pruebas.
<i>Prepare for Failover</i> (Preparar para failover)	Arranca la carga de trabajo de failover para preparar una operación de failover.
<i>Run Failover</i> (Ejecutar failover)	Arranca y configura la carga de trabajo de failover, por lo que se hace cargo de los servicios empresariales de una carga de trabajo con errores.
<i>Cancel Failover</i> (Cancelar failover)	Aborta el proceso de failover.
<i>Failback</i>	Tras una operación de failover, devuelve la carga de trabajo de failover a su infraestructura original o a una nueva (virtual o física).
<i>Remove Workload</i> (Eliminar carga de trabajo)	Elimina una carga de trabajo del inventario.

3.4 Gestión de varias instancias de PlateSpin Protect y PlateSpin Forge

PlateSpin Protect incluye una aplicación de cliente basada en Web, la consola de gestión de PlateSpin Protect, que proporciona acceso centralizado a varias instancias de PlateSpin Protect y PlateSpin Forge.

En un centro de datos con más de una instancia de PlateSpin Protect, puede designar una de las instancias como gestora y ejecutar la consola de gestión desde ahí. Las demás instancias se añaden en la gestora, lo que proporciona un único punto de control e interacción.

- ♦ [Sección 3.4.1, “Uso de la consola de gestión de PlateSpin Protect”, en la página 45](#)
- ♦ [Sección 3.4.2, “Acerca de las tarjetas de consola de gestión de PlateSpin Protect”, en la página 45](#)

- ♦ Sección 3.4.3, “Adición de instancias de PlateSpin Protect y PlateSpin Forge a la consola de gestión”, en la página 46
- ♦ Sección 3.4.4, “Gestión de tarjetas en la consola de gestión”, en la página 46

3.4.1 Uso de la consola de gestión de PlateSpin Protect

- 1 Abra un navegador Web en un equipo que tenga acceso a las instancias de PlateSpin Protect y diríjase a:

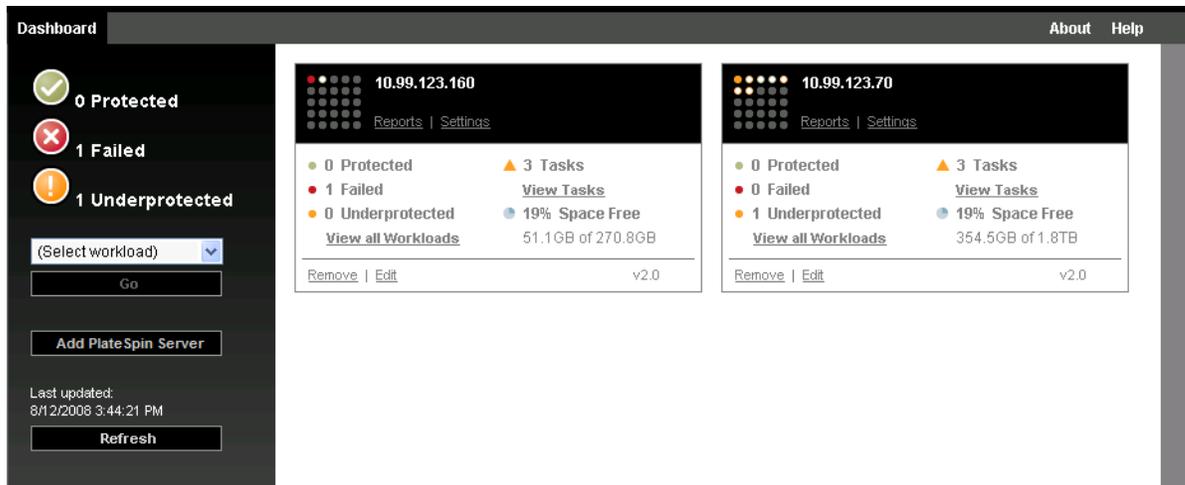
`https://<dirección_IP | nombre_de_host>/console`

Sustituya `<dirección_IP | nombre_de_host>` con la dirección IP o el nombre de host del host del servidor de PlateSpin designado como gestor.

- 2 Inicie sesión con su nombre de usuario de y contraseña.

Se muestra la página por defecto de la consola, Dashboard (Consola).

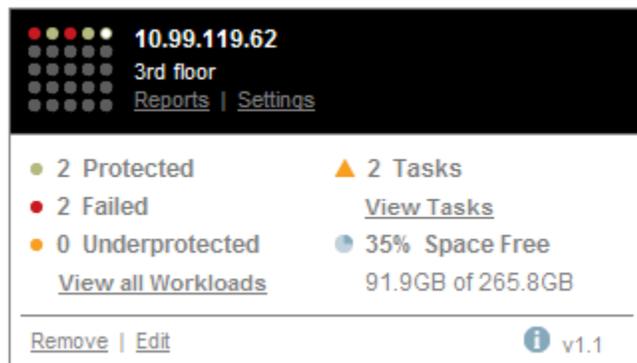
Figura 3-4 Página por defecto de la consola de gestión



3.4.2 Acerca de las tarjetas de consola de gestión de PlateSpin Protect

Las instancias individuales de PlateSpin Protect y PlateSpin Forge se representan mediante tarjetas cuando se añaden a la consola de gestión.

Figura 3-5 Tarjeta de instancia de PlateSpin Forge



Las tarjetas muestran información básica sobre la instancia específica de PlateSpin Protect o PlateSpin Forge, por ejemplo:

- ♦ Dirección IP/nombre de host
- ♦ Ubicación
- ♦ Número de versión
- ♦ Número de cargas de trabajo
- ♦ Estado de las cargas de trabajo
- ♦ Capacidad de almacenamiento
- ♦ Espacio libre restante

Los hiperenlaces de cada tarjeta permiten desplazarse a las páginas de cargas de trabajo, informes, configuración y tareas de la instancia concreta. También hay hiperenlaces que permiten editar la configuración de una tarjeta o eliminar una tarjeta de la pantalla.

3.4.3 Adición de instancias de PlateSpin Protect y PlateSpin Forge a la consola de gestión

Cuando se añade una instancia de PlateSpin Protect o Forge a la consola de gestión, se crea una tarjeta nueva en esta.

Nota: si entra en la consola de gestión mientras ejecuta una instancia de PlateSpin Protect o PlateSpin Forge, dicha instancia no se añade automáticamente a la consola. Debe añadirla manualmente.

Para añadir una instancia de PlateSpin Protect o Forge a la consola:

- 1 En la ventana principal de la consola, haga clic en *Add PlateSpin Server* (Añadir servidor de PlateSpin).
Se muestra la página *Add/Edit* (Añadir/Editar).
- 2 Especifique la URL del host del servidor de PlateSpin o de la máquina virtual de Forge. Si SSL está habilitado, use el protocolo HTTPS.
- 3 (Opcional) Marque la casilla de verificación *Use Management Console Credentials* (Usar credenciales de la consola de gestión) para usar las mismas credenciales que se usan en la consola. Si el campo *Domain \ Username* (Dominio \ Nombre de usuario) está seleccionado, la consola lo completa de forma automática.
- 4 En el campo *Domain \ Username* (Dominio \ Nombre de usuario), indique un nombre de dominio y un nombre de usuario válidos para la instancia de PlateSpin Protect o PlateSpin Forge que va a añadir. En el campo *Password* (Contraseña), indique la contraseña correspondiente.
- 5 (Opcional) Especifique un valor descriptivo o identificativo en los campos *Display Name* (Nombre de visualización, máximo de 15 caracteres), *Location* (Ubicación, máximo de 20 caracteres) y *Notes* (Notas, máximo de 400 caracteres) que requiera.
- 6 Haga clic en *Add/Save* (Añadir/Guardar).
Se añade una tarjeta nueva a la consola.

3.4.4 Gestión de tarjetas en la consola de gestión

Es posible modificar los detalles de una tarjeta en la consola de gestión.

- 1 Haga clic en el hiperenlace *Edit* (Editar) de la tarjeta que desee editar.

Se muestra la página *Add/Edit* (Añadir/Editar) de la consola.

2 Realice los cambios que desee y haga clic en *Add/Save* (Añadir/Guardar).

Se muestra la página principal actualizada de la consola.

Para eliminar una tarjeta de la consola de gestión:

1 Haga clic en el hipervínculo *Remove* (Eliminar) de la tarjeta que desee eliminar.

Se muestra un mensaje de confirmación.

2 Haga clic en *Aceptar*.

La tarjeta individual se elimina de la consola.

3.5 Generación de informes de carga de trabajo y de protección de la carga de trabajo

PlateSpin Protect permite generar informes que proporcionan información analítica sobre los contratos de protección de la carga de trabajo a lo largo del tiempo.

Se admiten los siguientes tipos de informes:

- ♦ **Workload Protection (Protección de la carga de trabajo):** informa sobre los eventos de réplica de todas las cargas de trabajo en un intervalo de tiempo que se puede seleccionar.
- ♦ **Replication History (Historial de réplica):** informa sobre el tipo de réplica, su tamaño, el tiempo empleado y la velocidad de transferencia de la carga de trabajo seleccionada en un intervalo de tiempo que también se puede seleccionar.
- ♦ **Replication Window (Ventana de réplica):** informa sobre la dinámica de las réplicas completas o incrementales. Se puede resumir por *Average* (Promedio), *Most Recent* (Más recientes), *Sum* (Suma) y *Peak* (Máximo).
- ♦ **Current Protection Status (Estado de protección actual):** informa sobre estadísticas de *Target RPO* (RPO de destino), *Actual RPO* (RPO real), *Actual TTO* (TTO real), *Actual RTO* (RTO real), *Last Test Failover* (Última prueba de failover), *Last Replication* (Última réplica) y *Test Age* (Antigüedad de la prueba).
- ♦ **Events (Eventos):** informa sobre los eventos del sistema de todas las cargas de trabajo en un intervalo de tiempo que se puede seleccionar.
- ♦ **Scheduled Events (Eventos programados):** informa solo sobre los eventos de protección de la carga de trabajo futuros.

Figura 3-6 Opciones de un informe de historial de réplica

The screenshot shows the 'Reports' section of the PlateSpin Protect interface. The 'Replication History' report is selected. The interface includes a navigation bar with 'Dashboard', 'Workloads', 'Tasks', 'Reports', and 'Settings'. Below the navigation bar, there is a search bar with the text 'What are the replication events relevant to my workload?'. The report filters are set to 'Custom' with a date range from '4/4/2011 12:00:00 AM' to '4/18/2011 4:15:41 PM'. The workload is set to 'SES-2K8-1'. There are checkboxes for 'All Replication Events' and 'Diagnostics View'. The main content area displays a table with the following data:

Date	Replication Event	Total Time	Transfer Time	Transfer Size	Transfer Speed
4/17/2011 4:01 AM	Incremental replication did not run as scheduled because the workload was busy	--	--	.0 MB	0.00 Mbps
4/17/2011 4:00 AM	Incremental replication did not run as scheduled because the workload was busy	--	--	.0 MB	0.00 Mbps
4/10/2011 4:01 AM	Incremental replication did not run as scheduled because the workload was busy	--	--	.0 MB	0.00 Mbps
4/10/2011 4:00 AM	Incremental replication did not run as scheduled because the workload was busy	--	--	.0 MB	0.00 Mbps

At the bottom of the table, there are links for 'Printable View' and 'Export To Xml'. The footer of the interface shows the date and time: 'Monday, April 18, 2011 4:15 PM - Eastern Daylight Time'.

Para generar un informe:

- 1 En la interfaz Web de PlateSpin Protect, haga clic en *Reports* (Informes).
Se muestra una lista de tipos de informes.
- 2 Haga clic en el nombre del tipo de informe que desee.

4 Protección de la carga de trabajo

PlateSpin Protect crea una réplica de la carga de trabajo de producción y la actualiza de forma periódica según la programación que defina.

La réplica, o la *carga de trabajo de failover*, es una máquina virtual en el contenedor de máquinas virtuales de PlateSpin Protect que se hace cargo de la función empresarial de la carga de trabajo de producción en caso de que se produzca una interrupción en el sitio de producción.

- ♦ Sección 4.1, “Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo”, en la página 49
- ♦ Sección 4.2, “Adición de contenedores (destinos de protección)”, en la página 51
- ♦ Sección 4.3, “Adición de cargas de trabajo para su protección”, en la página 52
- ♦ Sección 4.4, “Configuración de los detalles de protección y preparación de la réplica”, en la página 53
- ♦ Sección 4.5, “Inicio de la protección de la carga de trabajo”, en la página 56
- ♦ Sección 4.6, “Cancelación de comandos”, en la página 57
- ♦ Sección 4.7, “Failover (conmutación por fallo)”, en la página 58
- ♦ Sección 4.8, “Failback (conmutación a configuración previa)”, en la página 60
- ♦ Sección 4.9, “Reprotección de una carga de trabajo”, en la página 66

4.1 Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo

PlateSpin Protect define el flujo de trabajo siguiente para la protección y recuperación de la carga de trabajo:

- 1 Preparación:** este paso incluye los pasos de preparación para garantizar que las cargas de trabajo, los contenedores y el entorno cumplen los criterios necesarios.
 - 1a** Asegúrese de que PlateSpin Protect admite la carga de trabajo.
Consulte “[Configuraciones compatibles](#)” en la página 11.
 - 1b** Asegúrese de que las cargas de trabajo y los contenedores cumplen los requisitos previos de acceso y red.
Consulte “[Requisitos de acceso y comunicación en la red de protección](#)” en la página 25.
 - 1c** (Solo Linux)
 - ♦ (Condicional) Si tiene previsto proteger una carga de trabajo Linux compatible con un núcleo no estándar, personalizado o reciente, reconstruya el módulo `blkwatch` PlateSpin, que se necesita para la réplica de datos en el nivel de bloques.
Consulte el artículo 7005873 de la KB (<https://www.netiq.com/support/kb/doc.php?id=7005873>).

- ♦ (Recomendado) Prepare instantáneas LVM para la transferencia de datos en el nivel de bloques. Asegúrese de que cada grupo de volúmenes tiene espacio libre suficiente para las instantáneas LVM (al menos un 10 % de la suma de todas las particiones).

Consulte el [artículo 7005872 de la KB \(https://www.netiq.com/support/kb/doc.php?id=7005872\)](https://www.netiq.com/support/kb/doc.php?id=7005872).

- ♦ (Opcional) Prepare los guiones `freeze` y `thaw` para ejecutarlos en la carga de trabajo de origen en cada réplica.

Consulte [“Uso de los guiones freeze y thaw en todas las réplicas \(Linux\)” en la página 79](#).

2 Inventario: este paso implica añadir cargas de trabajo y contenedores a la base de datos del servidor de PlateSpin.

Las cargas de trabajo que desee proteger y los contenedores que alojen cargas de trabajo de failover deben inventariarse correctamente. Puede añadir cargas de trabajo y contenedores en cualquier orden. Sin embargo, cada contrato de protección requiere una carga de trabajo definida y un contenedor inventariados por el servidor de PlateSpin. Consulte [“Adición de contenedores \(destinos de protección\)” en la página 51](#) y [“Adición de cargas de trabajo para su protección” en la página 52](#).

3 Definición del contrato de protección: en este paso, se definen los detalles y especificaciones de un contrato de protección y se prepara la réplica.

Consulte [“Configuración de los detalles de protección y preparación de la réplica” en la página 53](#).

4 Inicialización de la protección: en este paso se comienza el contrato de protección según sus requisitos.

Consulte [“Inicio de la protección de la carga de trabajo” en la página 56](#).

5 Pasos opcionales del ciclo vital de la protección: estos pasos quedan fuera de la programación automatizada de réplicas, pero se suelen usar en distintas situaciones o podrían ser necesarias para la estrategia de continuidad empresarial.

- ♦ *Incremental manual.* Es posible ejecutar una réplica incremental manual, fuera del contrato de protección de la carga de trabajo, haciendo clic en *Run Incremental* (Ejecutar incremental).
- ♦ *Prueba.* Es posible probar la función de failover en un ambiente y de forma controlada. Consulte [Uso de la función de prueba de failover](#).

6 Failover: este paso realiza un failover de la carga de trabajo protegida a la réplica que se ejecuta en el contenedor de máquina virtual. Consulte [“Failover \(conmutación por fallo\)” en la página 58](#).

7 Failback: este paso corresponde a la fase de reanudación empresarial después de sufrir problemas con la carga de trabajo de producción. Consulte [“Failback \(conmutación a configuración previa\)” en la página 60](#).

8 Reprotección: este paso permite volver a definir el contrato de protección original para la carga de trabajo. Consulte [“Reprotección de una carga de trabajo” en la página 66](#)

La mayoría de estos pasos se representan mediante comandos de la carga de trabajo en la página Workloads (Cargas de trabajo). Consulte [“Cargas de trabajo y comandos de carga de trabajo” en la página 42](#).

Después de una operación de failback correcta, aparece disponible el comando *Reprotect* (Volver a proteger).

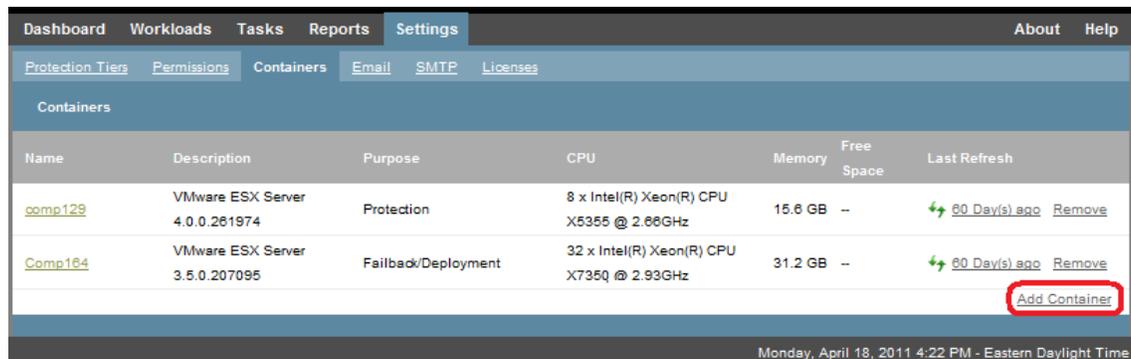
4.2 Adición de contenedores (destinos de protección)

Un contenedor es una infraestructura de protección que actúa como el host de una réplica actualizada regularmente de una carga de trabajo protegida. La infraestructura puede ser un servidor VMware ESX Server o un clúster DRS de VMware.

Para proteger una carga de trabajo, debe disponer de una y de un contenedor que estén en el inventario del servidor de PlateSpin (o que se hayan *añadido* a este).

Para añadir un contenedor:

- 1 En la interfaz Web de PlateSpin Protect, haga clic en *Settings > Containers > Add Container* (Configuración > Contenedores > Añadir contenedor).



- 2 Especifique los parámetros siguientes:

- ♦ **Tipo:** seleccione el tipo de contenedor (*VMware ESX Server* o *VMware DRS Cluster*). Asegúrese de que el contenedor sea compatible.

Para obtener más información, consulte la “[Contenedores de máquina virtual admitidos](#)” en la página 14.

- ♦ **Nombre de host o IP:** introduzca el nombre de host o la dirección IP del contenedor.
- ♦ **Nombre de host o IP de vCenter:** (solo clústeres DRS) introduzca el nombre de host o la dirección IP del servidor de vCenter.
- ♦ **Nombre de clúster:** (solo clústeres DRS) introduzca el nombre del clúster DRS necesario.

Al intentar añadir o actualizar un clúster DRS, la operación de descubrimiento subyacente podría fallar si:

- ♦ Un clúster no contiene hosts ESX.
- ♦ Un nombre de clúster no es único en el servidor vCenter (aunque tenga una vía de inventario única).
- ♦ Ninguno de los miembros del clúster es accesible (por ejemplo, porque el servidor de vCenter está en modo de mantenimiento).
- ♦ **Nombre de usuario/contraseña:** proporcione las credenciales de administrador para acceder al host necesario. Consulte “[Directrices para las credenciales de carga de trabajo y contenedor](#)” en la página 68.
- ♦ **Finalidad:** (solo contenedores de máquina virtual) seleccione el elemento oportuno (*Protection*, *Failback/Deployment* [Protección, Failback/Implantación] o ambos). Si selecciona ambos (*Protection* [Protección] y *Failback/Deployment* [Failback/Implantación]), el contenedor estará disponible para su selección como destino en las operaciones de protección y en las de failback/implantación.

3 Haga clic en *Añadir*.

PlateSpin Protect vuelve a cargar la página Containers (Contenedores) y muestra un indicador de proceso para el contenedor que se añade . Al completarse, el icono del indicador de proceso se transforma en el icono *Refresh* (Actualizar) .

Para actualizar un contenedor, haga clic en el icono *Refresh* (Actualizar)  junto al contenedor que desee actualizar. Se volverá a realizar el inventario del contenedor.

Para eliminar un contenedor, haga clic en *Remove* (Eliminar) junto al contenedor que desee eliminar.

4.3 Adición de cargas de trabajo para su protección

Las cargas de trabajo, los objetos básicos de protección de un almacén de datos, son sistemas operativos junto con su middleware y sus datos desacoplados de su infraestructura física o virtual subyacente.

Para proteger una carga de trabajo, debe disponer de una y de un contenedor que estén en el inventario del servidor de PlateSpin (o que se hayan *añadido* a este).

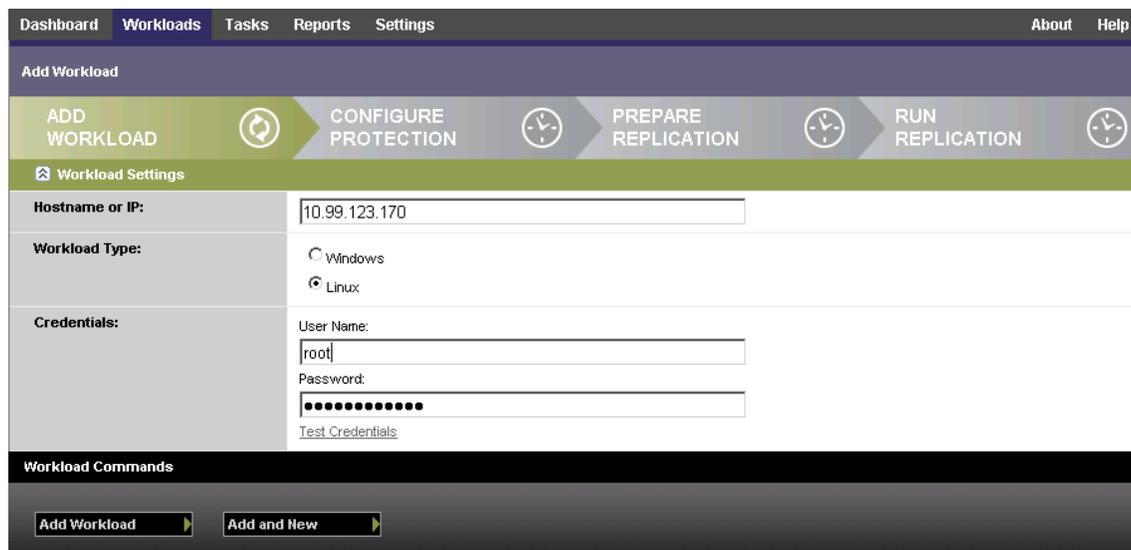
Para añadir una carga de trabajo:

1 Siga los pasos preparatorios necesarios.

Consulte el [Paso 1](#) en “Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo” en la [página 49](#).

2 En la página Dashboard (Consola) o Workloads (Cargas de trabajo), haga clic en *Add Workload* (Añadir carga de trabajo).

En la interfaz Web de PlateSpin Protect se muestra la página Add Workload (Añadir carga de trabajo).



3 Especifique los detalles necesarios de la carga de trabajo:

- ♦ **Workload Settings (Configuración de la carga de trabajo):** especifique el nombre de host o la dirección IP de la carga de trabajo, el sistema operativo y las credenciales del administrador.

Use el formato de credencial necesario. Consulte [“Directrices para las credenciales de carga de trabajo y contenedor” en la página 68](#).

Para asegurarse de que PlateSpin Protect puede acceder a la carga de trabajo, haga clic en *Test Credentials* (Probar credenciales).

- 4 Haga clic en *Add Workload* (Añadir carga de trabajo).

PlateSpin Protect vuelve a abrir la página Workloads (Cargas de trabajo) y muestra un indicador de proceso para la carga de trabajo que se carga . Espere a que se complete el proceso. Cuando se completa, se muestra un evento *Workload Added* (Carga de trabajo añadida) en la consola y la nueva carga está disponible en la página Workloads (Cargas de trabajo).

Si aún no ha añadido ningún contenedor, añada uno para preparar la protección de la carga de trabajo. Si ya lo ha hecho, pase a [“Configuración de los detalles de protección y preparación de la réplica” en la página 53](#).

4.4 Configuración de los detalles de protección y preparación de la réplica

Los detalles de protección controlan los valores de protección y recuperación de la carga de trabajo, así como el comportamiento en todo el ciclo vital de una carga de trabajo protegida. En cada fase del flujo de trabajo de protección y recuperación (consulte la [“Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo” en la página 49](#)), se leen los valores relevantes de los detalles de protección.

Para configurar los detalles de protección de la carga de trabajo:

- 1 Añada una carga de trabajo. Consulte [“Adición de cargas de trabajo para su protección” en la página 52](#).
- 2 Añada un contenedor. Consulte [“Adición de contenedores \(destinos de protección\)” en la página 51](#).
- 3 En la página Workloads (Cargas de trabajo), seleccione la carga de trabajo necesaria y haga clic en *Configure* (Configurar).

También puede hacer clic en el nombre de la carga de trabajo.

Nota: si el inventario de PlateSpin Protect aún no tiene ningún contenedor, el sistema solicitará que añada uno. Para ello, haga clic en *Add Container* (Añadir contenedor) en la parte inferior.

- 4 Seleccione una opción en *Initial Replication Method* (Método de réplica inicial). Esto indica si desea que los datos de volumen se transfieran por completo desde la carga de trabajo a la máquina virtual de failover o se sincronicen con los volúmenes de una máquina virtual existente. Consulte [“Método de réplica inicial \(completa o incremental\)” en la página 77](#).
- 5 Asigne un destino de protección. Puede ser un contenedor o, si ha seleccionado *Incremental Replication* (Réplica incremental) como método de réplica inicial, una carga de trabajo *preparada*. Consulte [“Método de réplica inicial \(completa o incremental\)” en la página 77](#).

Nota: si el inventario solo tiene un contenedor, la carga de trabajo se asignará a él automáticamente.

- 6 Configure los detalles de protección de cada conjunto de valores según sus necesidades de continuidad empresarial. Consulte [“Detalles de protección de la carga de trabajo” en la página 54](#).
- 7 Corrija los posibles errores de validación que se muestren en la interfaz Web de PlateSpin Protect.

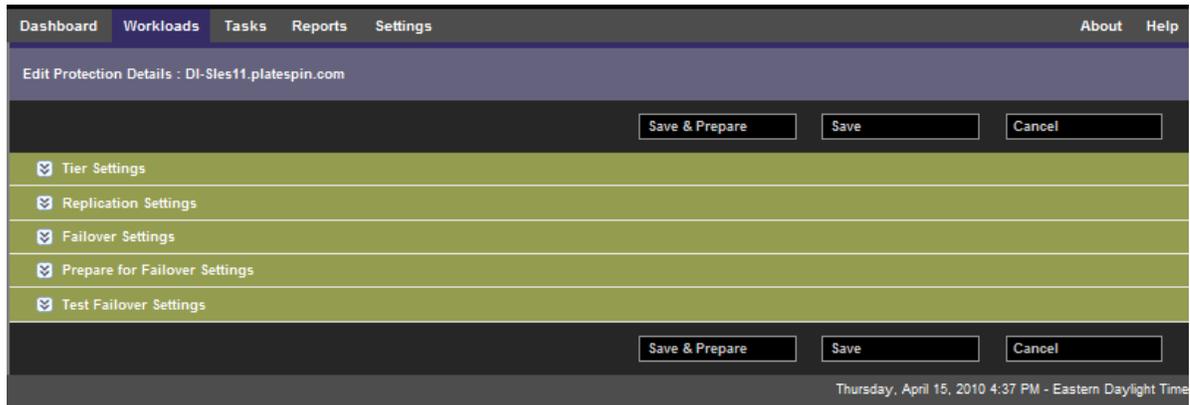
8 Haga clic en *Guardar*.

También puede hacer clic en *Save & Prepare* (Guardar y preparar). De esta forma, se guarda la configuración y, simultáneamente, se ejecuta el comando *Prepare Replication* (Preparar réplica), que instala los controladores de transferencia de datos en la carga de trabajo de origen si fuera necesario y crea la réplica inicial de la máquina virtual de la carga de trabajo.

Espere a que se complete el proceso. Cuando se completa, se muestra un evento *Workload configuration completed* (Configuración de la carga de trabajo terminada) en la consola.

4.4.1 Detalles de protección de la carga de trabajo

Los detalles de protección de la carga de trabajo se representan mediante cinco conjuntos de parámetros:



Puede expandir o comprimir cada conjunto haciendo clic en el icono situado a la izquierda.

A continuación se describen los cinco conjuntos de parámetros:

Tabla 4-1 Detalles de protección de la carga de trabajo

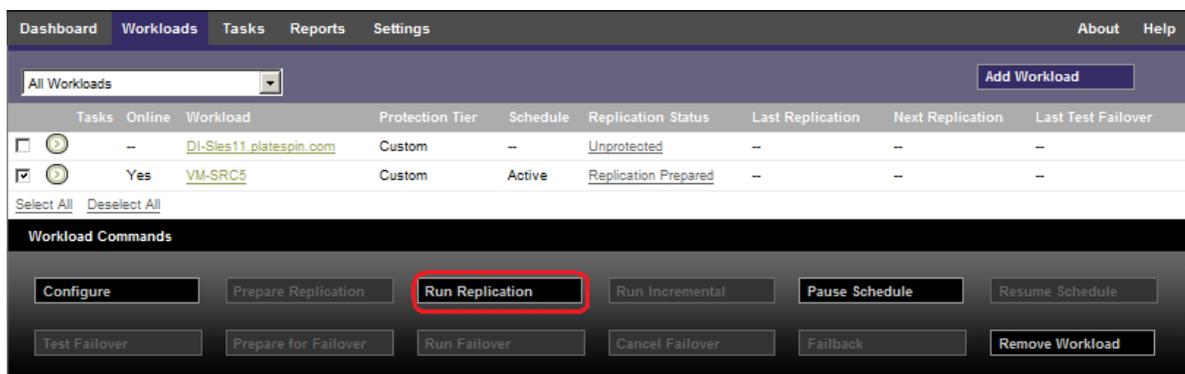
Conjunto de parámetros (configuración)	Detalles
Tier (nivel)	Indica el nivel de protección que usa la protección actual. Consulte “Niveles de protección” en la página 76 .

Conjunto de parámetros (configuración)	Detalles
Replication (Réplica)	<p>Transfer Method (Método de transferencia): (Windows) permite seleccionar un mecanismo de transferencia de datos y la seguridad mediante cifrado. Consulte “Transferencia de datos” en la página 74.</p> <p>Transfer Encryption (Cifrado de transferencia): para habilitar el cifrado, seleccione la opción <i>Encrypt Data Transfer</i> (Transferencia de datos de cifrado). Consulte “Seguridad y privacidad” en la página 14.</p> <p>Source Credentials (Credenciales de origen): necesarias para acceder a la carga de trabajo. Consulte “Directrices para las credenciales de carga de trabajo y contenedor” en la página 68.</p> <p>Number of CPUs (Número de CPU): permite especificar el número necesario de CPU virtuales asignadas a la carga de trabajo de failover. Solo es aplicable si el método seleccionado para la réplica inicial es <i>Full</i> (Completa).</p> <p>Replication Network (Red de réplica): permite separar el tráfico de réplica según las redes virtuales definidas en el contenedor de máquina virtual. Consulte “Redes” en la página 82.</p> <p>Configuration File Datastore (Almacén de datos de archivo de configuración): permite seleccionar un almacén de datos asociado con el contenedor de máquina virtual para almacenar los archivos de configuración de la máquina virtual. Consulte “Puntos de recuperación” en la página 77.</p> <p>Protected Volumes (Volúmenes protegidos): use estas opciones para seleccionar volúmenes que proteger y para asignar sus réplicas a almacenes de datos específicos en el contenedor de máquina virtual.</p> <p>Thin Disk option (Opción de disco ligero): habilita la función de disco virtual de provisión ligera, por la que un disco virtual aparece en la máquina virtual con un tamaño determinado, pero solo consume la cantidad de espacio de disco que realmente necesitan los datos de dicho disco.</p> <p>Services/Daemons to Stop During Replication (Servicios y daemons que se deben detener durante la réplica): permite seleccionar los servicios de Windows o los daemons de Linux que se detendrán automáticamente durante la réplica. Consulte “Control de servicios y daemons” en la página 79.</p>
Failover	<p>VM Memory (Memoria de la máquina virtual): permite especificar la cantidad de memoria asignada a la carga de trabajo de failover.</p> <p>Hostname and Domain/Workgroup affiliation (Nombre de host y afiliación de dominio/grupo de trabajo): use estas opciones para controlar la identidad y la afiliación de dominio/grupo de trabajo de la carga de trabajo de failover cuando esté activa. Para la afiliación del dominio, se necesitan las credenciales del administrador del dominio.</p> <p>Network Connections (Conexiones de red): use estas opciones para controlar la configuración de LAN de la carga de trabajo de failover. Consulte “Redes” en la página 82.</p> <p>Service/Daemon States to Change (Estados de servicio/daemon para cambiar): permite controlar el estado de inicio de servicios de aplicaciones (Windows) o daemon (Linux) específicos. Consulte “Control de servicios y daemons” en la página 79.</p>

Conjunto de parámetros (configuración)	Detalles
Prepare for Failover (Preparar para failover)	Permite controlar la configuración de red temporal de la carga de trabajo de failover durante la operación opcional de preparación para failover. Consulte “Redes” en la página 82 .
Test Failover (Probar failover)	<p>VM Memory (Memoria de la máquina virtual): permite asignar la RAM necesaria a la carga de trabajo temporal.</p> <p>Hostname (Nombre de host): permite asignar un nombre de host a la carga de trabajo temporal.</p> <p>Domain/Workgroup (Dominio/Grupo de trabajo): permite afiliar la carga de trabajo temporal con un dominio o un grupo de trabajo. Para la afiliación del dominio, se necesitan las credenciales del administrador del dominio.</p> <p>Network Connections (Conexiones de red): controla la configuración LAN de la carga de trabajo temporal. Consulte “Redes” en la página 82.</p> <p>Service/Daemon States to Change (Estados de servicio/daemon para cambiar): permite controlar el estado de inicio de servicios de aplicaciones (Windows) o daemon (Linux) específicos. Consulte “Control de servicios y daemons” en la página 79.</p>

4.5 Inicio de la protección de la carga de trabajo

La protección de la carga de trabajo se inicia mediante el comando *Run Replication* (Ejecutar réplica):



Puede ejecutar el comando Run Replication (Ejecutar réplica) después de:

- ◆ Añadir una carga de trabajo
- ◆ Configurar los detalles de protección de la carga de trabajo
- ◆ Preparar la réplica inicial

Cuando esté listo para continuar:

- 1 En la página Workloads (Cargas de trabajo), seleccione la carga de trabajo necesaria y haga clic en *Run Replication* (Ejecutar réplica).
- 2 Haga clic en *Ejecutar*.
PlateSpin Protect inicia la ejecución y muestra un indicador de proceso para el paso *Copy data* (Copiar datos) .

Nota: después de proteger una carga de trabajo:

- ♦ Si se cambia el tamaño de un volumen con protección de nivel de bloques, se invalida la protección. El procedimiento correcto consiste en: 1.º, eliminar la protección de la carga de trabajo; 2.º, cambiar el tamaño de los volúmenes según se precise; y 3.º, restablecer la protección volviendo a añadir la carga de trabajo, configurando sus detalles de protección e iniciando las réplicas.
- ♦ Cualquier modificación significativa de la carga de trabajo protegida requiere que la protección se vuelva a establecer. Un ejemplo es cuando se añaden volúmenes o tarjetas de red a la carga de trabajo protegida.

4.6 Cancelación de comandos

Es posible cancelar un comando después de ejecutarlo y mientras está en curso en la página Command Details (Detalles del comando) de dicho comando.

Para acceder a la página Command Details (Detalles del comando) de cualquier comando en curso:

- 1 Diríjase a la página Workloads (Cargas de trabajo).
- 2 Localice la carga de trabajo requerida y haga clic en el enlace que representa el comando que se está ejecutando en esa carga de trabajo.

<input type="checkbox"/>		No	CL-2K8R2-VM1	Custom	Active		Idle	3/5/2012 12:23 AM	4/11/2012 12:00 AM	--
<input type="checkbox"/>		Yes	DL-Sies11x64-Src	every 4 hours	Active		Fallover Prepared	3/29/2012 8:13 AM	4/9/2012 12:00 PM	3/23/2012 3:32 PM
<input type="checkbox"/>		--	ma-cl-slessp2.site	every 4 hours	--		Live	3/15/2012 2:49 PM	--	3/9/2012 2:44 PM
<input type="checkbox"/>		Yes	VISTACLIENT	Custom	Active		Running Incremental	3/28/2012 10:21 AM	4/9/2012 12:00 PM	3/23/2012 5:14 PM
<input type="checkbox"/>		--	CL-VISTASP1-SRC	every 4 hours	--		Live	2/22/2012 2:55 PM	--	--
<input type="checkbox"/>		Yes	CL-XPX64-SRC	Custom	Active		Idle	4/9/2012 10:17 AM	4/9/2012 12:00 PM	3/23/2012 5:15 PM

En la interfaz Web de PlateSpin Protect se muestra la página Command Details (Detalles del comando):

Running Incremental
Status: Running
Duration: 3d 21h 31m 37s
Step: Copy data (2%)
Setting Up Controller (1%)

Last Full Replication: 2/17/2012 3:53 PM
Last Incremental Replication: 3/28/2012 10:21 AM
Last Test Fallover: 3/23/2012 5:14 PM
Schedule: Active
Replication History: [View](#)
Tasks: --

Command Summary

Events:	Event	Details	User	Date
	Incremental replication started		DEV-MORTAZAA\PlateSpin	4/5/2012 2:00 PM

Status: Running
 Controller installation has not finished in a timely fashion. A controller has already been installed on 10.99.123.164.

Start Time: 4/5/2012 2:00 PM
Duration: 3d 21h 31m 37s

Steps:

Step	Status	Start Time	End Time	Duration	Diagnostics
Revert to snapshot	Completed	4/5/2012 2:00 PM	4/5/2012 2:01 PM	1m 7s	--
Copy data	Running (2%)	4/5/2012 2:01 PM	--	3d 21h 30m 30s	--

Diagnostics: [Generate](#)

Workload Commands

[Abort](#) [Configure](#) [Pause Schedule](#)

- 3 Haga clic en *Abort* (Abortar).

4.7 Failover (conmutación por fallo)

Si se produce un *failover*, la función empresarial de una carga de trabajo con errores pasa a estar controlada por una carga de trabajo de failover de un contenedor de máquina virtual de PlateSpin Protect.

- ♦ [Sección 4.7.1, “Detección de cargas de trabajo sin conexión”, en la página 58](#)
- ♦ [Sección 4.7.2, “Realización de failover”, en la página 59](#)
- ♦ [Sección 4.7.3, “Uso de la función de prueba de failover”, en la página 60](#)

4.7.1 Detección de cargas de trabajo sin conexión

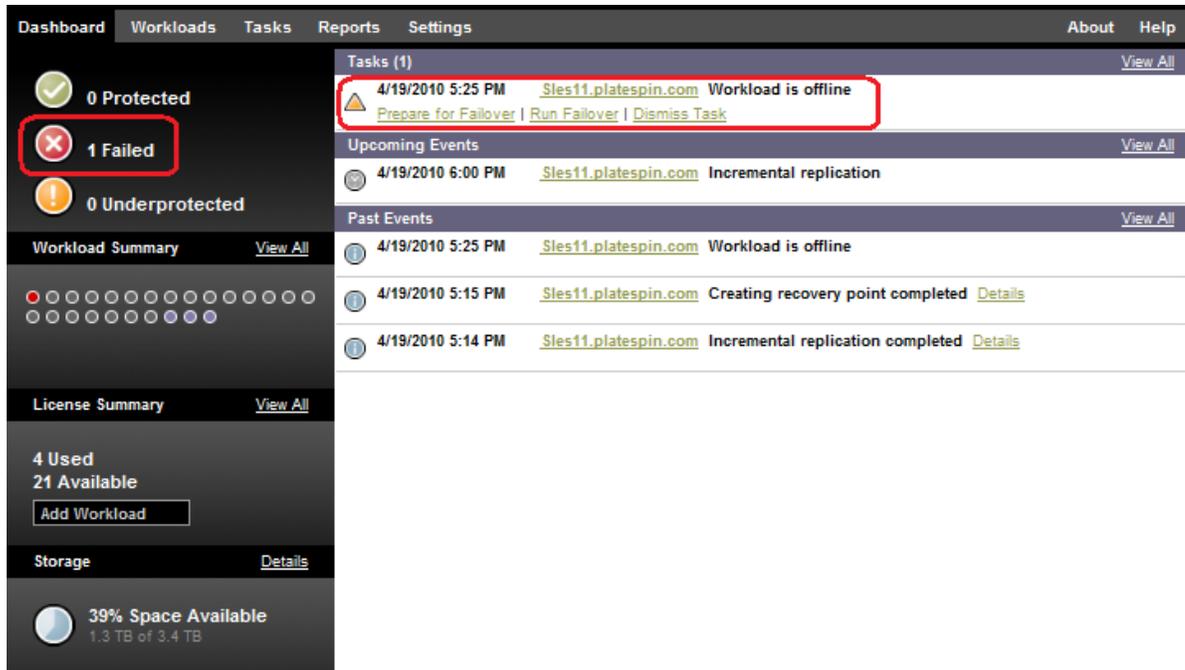
PlateSpin Protect supervisa de manera constante las cargas de trabajo protegidas. Si se produce un error al intentar supervisar una carga de trabajo un número predefinido de veces, PlateSpin Protect genera un evento *Workload is offline* (Carga de trabajo sin conexión). Los criterios para determinar y registrar un error de carga de trabajo forman parte de la configuración de nivel de la protección de la carga de trabajo (consulte la fila [Tier \(nivel\)](#) en [“Detalles de protección de la carga de trabajo” en la página 54](#)).

Si se han configurado las notificaciones en los valores de SMTP, PlateSpin Protect envía de forma simultánea una notificación por correo electrónico a los destinatarios especificados. Consulte [“Configuración de notificaciones automáticas por correo electrónico de eventos e informes” en la página 29](#).

Si se detecta un error de carga de trabajo mientras el estado de la réplica es *Idle* (Inactiva), puede continuar con el comando *Run Failover* (Ejecutar failover). Si se produce un error de carga de trabajo mientras se realiza una réplica incremental, el trabajo se detiene. En tal caso, cancele el comando (consulte [“Cancelación de comandos” en la página 57](#)) y continúe con el comando *Run Failover* (Ejecutar failover). Consulte [“Realización de failover” en la página 59](#).

En la ilustración siguiente, se muestra la página Dashboard (Consola) de la interfaz Web de PlateSpin Protect cuando detecta un error de carga de trabajo. Fíjese en las tareas aplicables del panel de tareas y eventos:

Figura 4-1 Página Dashboard (Consola) al detectar un error de carga de trabajo (Workload is offline)



4.7.2 Realización de failover

La configuración de failover, incluida la identidad de red de la carga de trabajo de failover y los valores LAN, se guardan junto a los detalles de protección de la carga de trabajo en el momento de la configuración. Consulte la fila [Failover](#) en “[Detalles de protección de la carga de trabajo](#)” en la [página 54](#).

Puede usar los métodos siguientes para realizar un failover:

- Seleccione la carga de trabajo requerida en la página Workloads (Cargas de trabajo) y haga clic en *Run Failover* (Ejecutar failover).
- Haga clic en el hipervínculo del comando correspondiente del evento *Workload is offline* (Carga de trabajo sin conexión) del panel de tareas y eventos. Consulte la [Figura 4-1](#).
- Ejecute el comando *Prepare for Failover* (Preparar failover) para arrancar la máquina virtual de failover previamente. Siga teniendo la opción de cancelar el failover (algo útil si el failover reaparece).

Use uno de estos métodos para iniciar el proceso de failover y seleccione un punto de recuperación para aplicar a la carga de trabajo de failover (consulte “[Puntos de recuperación](#)” en la [página 77](#)). Haga clic en *Execute* (Ejecutar) y supervise el progreso. Cuando se complete, el estado de réplica de la carga de trabajo debe indicar *Live* (Activa).

Para probar la carga de trabajo de failover o el proceso de failover como parte o de un ejercicio de recuperación tras fallos planificado, consulte “[Uso de la función de prueba de failover](#)” en la [página 60](#).

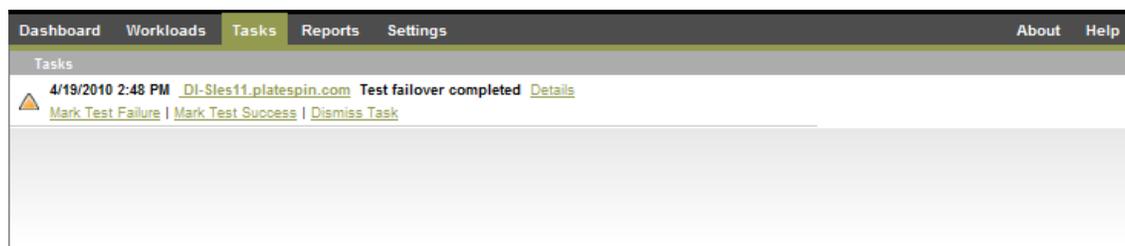
4.7.3 Uso de la función de prueba de failover

PlateSpin Protect proporciona la capacidad para probar la función de failover y la integridad de la carga de trabajo de failover. Para ello, se usa el comando *Test Failover* (Probar failover), que arranca la carga de trabajo de failover en un entorno de redes restringido para realizar pruebas.

Cuando se ejecuta el comando, PlateSpin Protect aplica a la carga de trabajo de failover la configuración de prueba de failover guardada en los detalles de protección de la carga de trabajo (consulte la fila [Test Failover \(Probar failover\)](#) en “[Detalles de protección de la carga de trabajo](#)” en la [página 54](#)).

- 1 Defina un intervalo de tiempo oportuno para la prueba y asegúrese de que no hay ninguna réplica en curso. El estado de la réplica de la carga de trabajo debe ser *Idle* (Inactiva).
- 2 En la página Workloads (Cargas de trabajo), seleccione la carga de trabajo requerida, haga clic en *Test Failover* (Probar failover), seleccione un punto de recuperación (consulte “[Puntos de recuperación](#)” en la [página 77](#)) y haga clic en *Execute* (Ejecutar).

Cuando se completa, PlateSpin Protect genera un evento correspondiente y una tarea con un conjunto de comandos aplicables:



- 3 Verifique la integridad y la funcionalidad empresarial de la carga de trabajo de failover. Use el cliente de VMware vSphere para acceder a la carga de trabajo de failover en el contenedor de máquina virtual.
- 4 Marque la prueba como *errónea* o *correcta*. Use los comandos correspondientes de la tarea: *Mark Test Failure* (Marcar prueba como errónea) o *Mark Test Success* (Marcar prueba como correcta). La acción seleccionada se guarda en el historial de eventos asociado con la carga de trabajo a fin que los informes la puedan recuperar. *Dismiss Task* (Descartar tarea) descarta la tarea y el evento.

Cuando se completen las tareas *Mark Test Failure* (Marcar prueba como errónea) o *Mark Test Success* (Marcar prueba como correcta), PlateSpin Protect descargará los valores temporales que se aplicaron a la carga de trabajo de failover y la protección volverá al estado en el que se encontraba antes de la prueba.

4.8 Failback (conmutación a configuración previa)

El paso lógico siguiente tras un failover, es una operación de failback. Con ella se transfiere la carga de trabajo de failover a su infraestructura original o, si fuera necesario, a una nueva.

Los métodos de failback admitidos dependen del tipo de infraestructura de destino y del grado de automatización del proceso de failback:

- ♦ **Failback automatizado a una máquina virtual:** compatible con plataformas VMware ESX y clústeres DRS VMware.
- ♦ **Failback semiautomatizado a un equipo físico:** compatible con todos los equipos físicos.
- ♦ **Failback semiautomatizado a una máquina virtual:** compatible con plataformas Xen en SLES y Microsoft Hyper-V.

En los temas siguientes se proporciona más información:

- ♦ [Sección 4.8.1, “Failback automatizado a una plataforma de máquina virtual”, en la página 61](#)
- ♦ [Sección 4.8.2, “Failback semiautomatizado a un equipo físico”, en la página 64](#)
- ♦ [Sección 4.8.3, “Failback semiautomatizado a una máquina virtual”, en la página 65](#)

4.8.1 Failback automatizado a una plataforma de máquina virtual

Los contenedores siguientes se admiten como destinos de failback automatizados:

Destino	Notas
Clúster DRS VMware en vSphere 5.15	<ul style="list-style-type: none">♦ La configuración de DRS debe ser Partially Automated (Parcialmente automatizada) o Fully Automated (Totalmente automatizada. No debe definirse en Manual).♦ Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 5.5 y solo se puede gestionar en vCenter 5.5.
Clúster DRS VMware en vSphere 5.1	<ul style="list-style-type: none">♦ La configuración de DRS debe ser Partially Automated (Parcialmente automatizada) o Fully Automated (Totalmente automatizada. No debe definirse en Manual).♦ Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 5.1 y solo se puede gestionar en vCenter 5.1.
Clúster DRS VMware en vSphere 5.0	<ul style="list-style-type: none">♦ La configuración de DRS debe ser Partially Automated (Parcialmente automatizada) o Fully Automated (Totalmente automatizada. No debe definirse en Manual).♦ Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 5.0 y solo se puede gestionar en vCenter 5.0.
Clúster DRS VMware en vSphere 4.1	<ul style="list-style-type: none">♦ La configuración de DRS debe ser Partially Automated (Parcialmente automatizada) o Fully Automated (Totalmente automatizada. No debe definirse en Manual).♦ Como contenedor de máquina virtual, el clúster puede usar una combinación de servidores ESX 4.1 y ESXi 4.1 y solo se puede gestionar en vCenter 4.1.
VMware ESXi 4.1, 5.0, 5.1	Las versiones ESXi deben disponer de una licencia pagada. La protección no se admite en estos sistemas si funcionan con una licencia gratuita.
VMware ESX 4.1	

Lleve a cabo estos pasos para ejecutar un failback automatizado de una carga de trabajo de failover en un contenedor VMware de destino.

- 1 Tras un failover, seleccione la carga de trabajo en la página Workloads (Cargas de trabajo) y haga clic en *Failback*.
El sistema solicita que se realicen las siguientes selecciones.
- 2 Especifique los siguientes conjuntos de parámetros:
 - ♦ **Workload Settings (Configuración de la carga de trabajo)**: especifique el nombre de host o la dirección IP de la carga de trabajo de failover y proporcione las credenciales del nivel de administrador. Use el formato de credencial necesario (consulte [“Directrices para las credenciales de carga de trabajo y contenedor” en la página 68](#)).

- ♦ **Failback Target Settings (Configuración de destino de failback):** especifique los parámetros siguientes:
 - ♦ **Replication Method (Método de réplica):** seleccione el ámbito de la réplica de datos. Si selecciona *Incremental*, debe *preparar* un destino. Consulte [“Método de réplica inicial \(completa o incremental\)”](#) en la página 77.
 - ♦ **Target Type (Tipo de destino):** Seleccione *Virtual Target* (Destino virtual). Si aún no tiene un contenedor de failback, haga clic en *Add Container* (Añadir contenedor) y añada al inventario un contenedor compatible.
- 3 Haga clic en *Save and Prepare* (Guardar y preparar) y supervise el progreso en la pantalla Command Details (Detalles del comando).
 Cuando se complete correctamente, PlateSpin Protect cargará la pantalla Ready for Failback (Preparado para el failback), donde se le pide que especifique los detalles de la operación de failback.
 - 4 Configure los detalles del failback. Consulte [“Detalles de failback \(carga de trabajo en máquina virtual\)”](#) en la página 63.
 - 5 Haga clic en *Save and Failback* (Guardar y failback) y supervise el progreso en la página Command Details (Detalles del comando). Consulte la [Figura 4-2](#).
 PlateSpin Protect ejecutará el comando. Si ha seleccionado *Reprotect after Failback* (Volver a proteger después del failback) en el conjunto de parámetros posterior al failback, se muestra un comando *Reprotect* (Volver a proteger) en la interfaz Web de PlateSpin Protect.

Figura 4-2 Detalles del comando de failback

The screenshot displays the 'Running Failback' command details for VM-SRC18. The status is 'Running' with a duration of 42m 22s. The current step is 'Copy data' at 91% completion. A progress bar shows 'Uninstalling VMware Tools (1%)'. The Command Summary table is as follows:

Step	Status	Start Time	End Time	Duration	Diagnostics
Copy data	Running (91%)	4/20/2010 7:55 PM	--	42m 17s	--

Below the table is the 'Replication Transfer Summary' section:

Average Transfer Speed:	40.88 Mbps
Total Data Transferred:	5.5 GB
Total Files Transferred:	27138
Total Folders Transferred:	4063
Duration:	19m 25s

Detalles de failback (carga de trabajo en máquina virtual)

Los detalles del failback se representan mediante tres conjuntos de parámetros que se pueden configurar al realizar una operación de carga de trabajo de failback en una máquina virtual.

Tabla 4-2 Detalles de failback (máquina virtual)

Conjunto de parámetros (configuración)	Detalles
Failback	<p>Transfer Method (Método de transferencia): permite seleccionar un mecanismo de transferencia de datos y la seguridad mediante cifrado. Consulte “Transferencia de datos” en la página 74.</p> <p>Failback Network (Red de failback): permite dirigir el tráfico de failback por una red dedicada basada en las redes virtuales definidas en el contenedor de máquina virtual. Consulte “Redes” en la página 82.</p> <p>VM Datastore (Almacén de datos de máquina virtual): permite seleccionar un almacén de datos asociado con el contenedor de failback para la carga de trabajo de destino.</p> <p>Volume Mapping (Asignación de volumen): si el método de réplica inicial especificado es el incremental, permite seleccionar volúmenes de origen y asignarlos a volúmenes del destino de failback para su sincronización.</p> <p>Services/Daemons to stop (Servicios/Daemons que se deben detener): permite seleccionar los servicios de Windows o los daemons de Linux que se detendrán automáticamente durante el failback. Consulte “Control de servicios y daemons” en la página 79.</p> <p>Alternative Address for Source (Dirección alternativa para el origen): acepta la introducción de una dirección IP adicional para la máquina virtual en failover, si fuera aplicable. Consulte “Protección en redes públicas y privadas mediante NAT” en la página 28.</p>
Carga de trabajo	<p>Número de CPU: permite especificar el número necesario de CPU virtuales asignadas a la carga de trabajo de destino.</p> <p>VM Memory (Memoria de la máquina virtual): permite asignar la RAM necesaria a la carga de trabajo de destino.</p> <p>Hostname, Domain/Workgroup (Nombre de host, Dominio/Grupo de trabajo): use estas opciones para controlar la identidad y la afiliación de dominio/grupo de trabajo de la carga de trabajo de destino. Para la afiliación del dominio, se necesitan las credenciales del administrador del dominio.</p> <p>Network Connections (Conexiones de red): use estas opciones para especificar la asignación de red de la carga de trabajo de destino basada en las redes virtuales del contenedor de máquina virtual subyacente.</p> <p>Service States to Change (Estados de servicio que se deben cambiar): permite controlar el estado de inicio de servicios de aplicaciones (Windows) o daemon (Linux) específicos. Consulte “Control de servicios y daemons” en la página 79.</p>

Conjunto de parámetros (configuración)	Detalles
Después del failback	<p>Reprotect Workload (Volver a proteger la carga de trabajo): use esta opción si tiene previsto volver a crear el contrato de protección de la carga de trabajo de destino después de la distribución. Se mantiene así un historial continuo de eventos para la carga de trabajo y se asigna o de designa automáticamente una licencia de carga de trabajo.</p> <ul style="list-style-type: none"> ♦ Reprotect after Failback (Volver a proteger después del failback): seleccione esta opción si tiene previsto volver a crear un contrato de protección para la carga de trabajo de destino. Cuando se completa el failback, hay un comando <i>Reprotect</i> (Volver a proteger) disponible en el interfaz Web de PlateSpin Protect para la carga de trabajo a la que se ha aplicado el failback. ♦ No reprotect (No volver a proteger): seleccione esta opción si no tiene previsto volver a crear un contrato de protección para la carga de trabajo de destino. Para proteger la carga de trabajo a la que se ha aplicado el failback cuando se complete el proceso, tendrá que volver a incluirla en el inventario y reconfigurar sus detalles de protección.

4.8.2 Failback semiautomatizado a un equipo físico

Use estos pasos para efectuar un failback de una carga de trabajo en un equipo físico después de un failover. El equipo físico puede ser la infraestructura original o una nueva.

- 1 Registre el equipo físico necesario en el servidor de PlateSpin. Consulte [“Failback a equipos físicos” en la página 82](#).
- 2 Si faltan controladores o estos no son compatibles, cargue los controladores necesarios en la base de datos de controladores del dispositivo PlateSpin Protect. Consulte [“Gestión de controladores de dispositivo” en la página 91](#).
- 3 Tras un failover, seleccione la carga de trabajo en la página Workloads (Cargas de trabajo) y haga clic en *Failback*.
- 4 Especifique los siguientes conjuntos de parámetros:
 - ♦ **Workload Settings (Configuración de la carga de trabajo):** especifique el nombre de host o la dirección IP de la carga de trabajo de failover y proporcione las credenciales del nivel de administrador. Use el formato de credencial necesario (consulte [“Directrices para las credenciales de carga de trabajo y contenedor” en la página 68](#)).
 - ♦ **Failback Target Settings (Configuración de destino de failback):** especifique los parámetros siguientes:
 - ♦ **Replication Method (Método de réplica):** seleccione el ámbito de la réplica de datos. Consulte [“Método de réplica inicial \(completa o incremental\)” en la página 77](#).
 - ♦ **Target Type (Tipo de destino):** seleccione la opción *Physical Target* (Destino físico) y el equipo físico que registró en el [Paso 1](#).

- 5 Haga clic en *Save and Prepare* (Guardar y preparar) y supervise el progreso en la pantalla Command Details (Detalles del comando).

Cuando se complete correctamente, PlateSpin Protect cargará la pantalla Ready for Failback (Preparado para el failback), donde se le pide que especifique los detalles de la operación de failback.

- 6 Configure los detalles del failback y haga clic en *Save and Failback* (Guardar y failback). Supervise el progreso en la pantalla Command Details (Detalles del comando).

4.8.3 Failback semiautomatizado a una máquina virtual

Este tipo de failback sigue un proceso similar al [Failback semiautomatizado a un equipo físico](#) para un destino de máquina virtual distinto al contenedor de VMware con compatibilidad nativa. Durante este proceso, se indica al sistema que considere un destino de máquina virtual como si fuera un equipo físico.

El failback semiautomatizado en una máquina virtual se admite en las siguientes plataformas de máquina virtual de destino:

- ♦ Xen en SLES 10 SP2
- ♦ Microsoft Hyper-V Server 2008 (*no R2*)

También es posible efectuar un failback semiautomatizado en un contenedor que cuente con compatibilidad de totalmente automatizada (destinos de VMware ESX y de clústeres DRS).

4.9 Reprotección de una carga de trabajo

La operación de *reprotección*, el paso lógico siguiente después de un *failback*, completa el ciclo vital de protección de la carga de trabajo y lo inicia de nuevo. Tras una operación de failback correcta, aparece el comando *Reprotect* (Volver a proteger) disponible en la interfaz Web de PlateSpin Protect y el sistema aplica los mismos detalles de protección que se indicaron durante la configuración inicial del contrato de protección.

Nota: el comando *Reprotect* (Volver a proteger) solo está disponible si se seleccionó la opción *Reprotect* (Volver a proteger) en los detalles del failback. Consulte [“Failback \(conmutación a configuración previa\)” en la página 60](#).

El resto del flujo de trabajo que cubre el ciclo vital de protección es igual que las operaciones de protección de la carga de trabajo normales; puede repetirlo todas las veces que sea necesario.

5 Elementos básicos de la protección de la carga de trabajo

En esta sección se proporciona información sobre las distintas áreas funciones de un contrato de protección de la carga de trabajo.

- ♦ [Sección 5.1, “Consumo de licencia de carga de trabajo”, en la página 67](#)
- ♦ [Sección 5.2, “Directrices para las credenciales de carga de trabajo y contenedor”, en la página 68](#)
- ♦ [Sección 5.3, “Configuración de inquilinos múltiples de Protect en VMware”, en la página 68](#)
- ♦ [Sección 5.4, “Transferencia de datos”, en la página 74](#)
- ♦ [Sección 5.5, “Niveles de protección”, en la página 76](#)
- ♦ [Sección 5.6, “Puntos de recuperación”, en la página 77](#)
- ♦ [Sección 5.7, “Método de réplica inicial \(completa o incremental\)”, en la página 77](#)
- ♦ [Sección 5.8, “Control de servicios y daemons”, en la página 79](#)
- ♦ [Sección 5.9, “Uso de los guiones freeze y thaw en todas las réplicas \(Linux\)”, en la página 79](#)
- ♦ [Sección 5.10, “Volúmenes”, en la página 80](#)
- ♦ [Sección 5.11, “Redes”, en la página 82](#)
- ♦ [Sección 5.12, “Failback a equipos físicos”, en la página 82](#)
- ♦ [Sección 5.13, “Temas avanzados sobre la protección de la carga de trabajo”, en la página 85](#)

5.1 Consumo de licencia de carga de trabajo

La licencia del producto PlateSpin Protect le da derecho a proteger un número específico de cargas de trabajo. Cada vez que se añade una carga de trabajo para proteger, el sistema consume una licencia de carga de trabajo del repositorio de licencias. Es posible recuperar una licencia consumida si elimina una carga de trabajo, hasta un máximo de cinco veces.

Para obtener información sobre las licencias del producto y su activación, consulte [“Licencia del producto” en la página 19](#).

5.2 Directrices para las credenciales de carga de trabajo y contenedor

PlateSpin Protect debe disponer de acceso de administrador a las cargas de trabajo y una configuración de funciones apropiada para los contenedores. A lo largo del flujo de trabajo de protección y recuperación de la carga de trabajo, PlateSpin Protect le solicita que especifique credenciales que se deben proporcionar en un formato específico.

Tabla 5-1 Credenciales de carga de trabajo y contenedor

Para descubrir	Credenciales	Observaciones
Todas las cargas de trabajo Windows	Credenciales de administrador local o de dominio	Para el nombre de usuario, use este formato: <ul style="list-style-type: none">♦ Para equipos miembros del dominio: <i>autoridad\principal</i>♦ Para equipos miembros del grupo de trabajo: <i>nombre de host\principal</i>
Clústeres de Windows	Credenciales de administrador del dominio	
Todas las cargas de trabajo Linux	Nombre de usuario y contraseña de nivel de usuario Root	Las cuentas que no sean de usuario Root se deben configurar correctamente para que puedan usar <code>sudo</code> . Consulte el artículo 7920711 de la KB .
VMware ESX/ESXi 4.1; ESXi 5.0, ESXi 5.1, ESXi 5.5	Una cuenta de VMware con una configuración de funciones adecuada. Consulte la Sección 5.3.1, “Uso de herramientas para definir funciones de VMware” , en la página 69.	Si ESX se ha configurado para la autenticación de dominios de Windows, también puede utilizar las credenciales de dominio de Windows.
VMware vCenter Server	Una cuenta de VMware con una configuración de funciones adecuada. Consulte la Sección 5.3.1, “Uso de herramientas para definir funciones de VMware” , en la página 69.	

5.3 Configuración de inquilinos múltiples de Protect en VMware

PlateSpin Protect incluye funciones de usuario únicas (y una herramienta para crearlas en un centro de datos VMware) que hacen posible que usuarios de VMware no administrativos (o “usuarios habilitados”) lleven a cabo operaciones del ciclo de vida de Protect en el entorno VMware. Estas funciones hacen posible que usted, como proveedor de servicios, segmente su clúster VMware para permitir múltiples inquilinos. Esto implica la existencia de varias instancias de contenedores de Protect en el centro de datos para acomodar a clientes de Protect o “inquilinos” que deseen mantener sus datos y el hecho de que existen por separado e inaccesibles para los demás clientes del centro de datos.

En esta sección se incluye la información siguiente:

- ♦ [Sección 5.3.1, “Uso de herramientas para definir funciones de VMware”](#), en la página 69
- ♦ [Sección 5.3.2, “Asignación de funciones en vCenter”](#), en la página 71

5.3.1 Uso de herramientas para definir funciones de VMware

PlateSpin Protect requiere ciertos privilegios para acceder a la infraestructura de VMware (los “contenedores” de VMware) y realizar tareas en ella, con el fin de que el flujo de trabajo y las funciones de Protect sean posibles en ese entorno. Puesto que existen muchos de estos privilegios necesarios, NetIQ ha creado un archivo que define los privilegios mínimos obligatorios y los agrega a tres funciones personalizadas de VMware:

- ♦ Administrador de máquinas virtuales de PlateSpin
- ♦ Administrador de infraestructuras de PlateSpin
- ♦ Usuario de PlateSpin

Este archivo de definiciones, `PlateSpinRole.xml`, está incluido en la instalación del servidor de PlateSpin Protect. Un ejecutable adjunto, `PlateSpin.VMwareRoleTool.exe`, accede al archivo para permitir la creación de estas funciones personalizadas de PlateSpin en un entorno vCenter de destino.

En esta sección se incluye la información siguiente:

- ♦ [“Sintaxis básica de la línea de comandos” en la página 69](#)
- ♦ [“Parámetros e indicadores adicionales de línea de comandos” en la página 69](#)
- ♦ [“Ejemplo de uso de la herramienta” en la página 70](#)
- ♦ [“\(Opción\) Definición manual de las funciones de PlateSpin en vCenter” en la página 70](#)

Sintaxis básica de la línea de comandos

Desde la ubicación en la que se haya instalado la herramienta de funciones, ejecute la herramienta desde la línea de comandos empleando esta sintaxis básica:

```
PlateSpin.VMwareRoleTool.exe /host=[host name/IP] /user=[user name] /role=[the  
role definition file name and location] /create
```

Nota: el archivo de definición de funciones se encuentra por defecto en la misma carpeta que la herramienta de definición de funciones.

Parámetros e indicadores adicionales de línea de comandos

Aplique los siguientes parámetros según sea necesario al utilizar `PlateSpin.VMwareRoleTool.exe` para crear o actualizar funciones en vCenter:

<code>/crear</code>	(Obligatorio) Crea las funciones definidas mediante el parámetro <code>/role</code> .
<code>/get_all_privileges</code>	Muestra todos los privilegios definidos en el servidor.

Indicadores opcionales

<code>/interactive</code>	Ejecuta la herramienta con opciones interactivas que permiten crear funciones individuales, comprobar la compatibilidad de funciones o indicar todas las funciones compatibles.
<code>/password=[contraseña]</code>	Proporciona la contraseña de VMware (omite la solicitud de contraseña)
<code>/verbose</code>	Visualizar información detallada

Ejemplo de uso de la herramienta

Uso: `PlateSpin.VMwareRoleTool.exe /host=houston_sales /user=pedrom /role=PlateSpinRole.xml /create`

Acciones resultantes:

1. La herramienta de definición de funciones se ejecuta en el servidor de vCenter `houston_sales`, que tiene un administrador con el nombre de usuario `pedrom`.
2. En ausencia del parámetro `/password`, la herramienta solicita la contraseña de usuario, que deberá introducir.
3. La herramienta accede al archivo de definición de funciones, `PlateSpinRole.xml`, que se encuentra en el mismo directorio que el ejecutable de la herramienta (no era necesario definir su vía).
4. La herramienta encuentra el archivo de definición y recibe la instrucción (`/create`) de crear las funciones definidas en el contenido de ese archivo en el entorno vCenter.
5. La herramienta accede al archivo de definición y crea las nuevas funciones (incluidos los privilegios mínimos apropiados para el acceso limitado definido) dentro de vCenter.
Las nuevas funciones personalizadas se [asignarán posteriormente a los usuarios en vCenter](#).

(Opción) Definición manual de las funciones de PlateSpin en vCenter

Puede usar el cliente de vCenter para crear y asignar manualmente las funciones personalizadas de PlateSpin. Esto requiere crear las funciones con los privilegios enumerados definidos en `PlateSpinRole.xml`. Si la creación se realiza manualmente, no existen restricciones sobre el nombre de la función. La única restricción es que los nombres de funciones creadas como equivalentes a aquellas en el archivo de definición tengan los privilegios mínimos apropiados del archivo de definición.

Para obtener información sobre cómo crear funciones personalizadas en vCenter, consulte el documento sobre [cómo administrar funciones y permisos de VMWare VirtualCenter](http://www.vmware.com/pdf/vi3_vc_roles.pdf) (http://www.vmware.com/pdf/vi3_vc_roles.pdf) en el centro de recursos técnicos de VMware.

5.3.2 Asignación de funciones en vCenter

Al configurar un entorno de múltiples inquilinos, deberá aprovisionar un solo servidor de Protect por cliente o “inquilino”. Le asignará a este servidor de Protect un usuario habilitado con funciones especiales de VMware para Protect. Este usuario habilitado creará el contenedor de Protect. Como proveedor de servicios, mantendrá las credenciales del usuario y no las revelará al cliente inquilino.

La siguiente tabla indica las funciones que debe definir para el usuario habilitado. También incluye más información sobre la finalidad de la función:

Contenedor de vCenter para asignación de funciones	Aspectos específicos de asignación de funciones	Instrucciones de propagación	Más información
Raíz del árbol de inventario de vCenter	Asigne al usuario habilitado la función <i>Administrador de infraestructuras de PlateSpin</i> (o equivalente).	Por razones de seguridad, defina el permiso como no propagable.	Esta función es necesaria para supervisar las tareas que lleva a cabo el software de Protect y finalizar cualquier sesión de VMware inactiva.
Todos los objetos del centro de datos a los que el usuario habilitado necesite acceder	Asigne al usuario habilitado la función <i>Administrador de infraestructuras de PlateSpin</i> (o equivalente).	Por razones de seguridad, defina el permiso como no propagable.	Esta función es necesaria para permitir el acceso a los almacenes de datos del centro de datos para cargar o descargar archivos. Defina el permiso como no propagable.
Todos los clústeres que se vayan a añadir a Protect como contenedores y todos los hosts incluidos en los clústeres	Asigne al usuario habilitado la función <i>Administrador de infraestructuras de PlateSpin</i> (o equivalente).	La propagación queda sujeta al criterio del administrador de VMware.	Para asignarlo a un host, propague el permiso desde el objeto de clúster o cree un permiso adicional en cada host del clúster. Si la función se asigna en el objeto de clúster y se propaga, no será necesario realizar cambios adicionales al añadir un nuevo host al clúster. Sin embargo, propagar el permiso tiene implicaciones respecto a la seguridad.
Todos los repositorios de recursos a los que necesite acceder el usuario habilitado	Asigne al usuario habilitado la función <i>Administrador de máquinas virtuales de PlateSpin</i> (o equivalente).	La propagación queda sujeta al criterio del administrador de VMware.	Aunque puede asignar el acceso a cualquier cantidad de repositorios de recursos en cualquier ubicación del árbol, debe asignar esta función al usuario habilitado en al menos un repositorio de recursos.
Todas las carpetas de máquinas virtuales a las que necesite acceder el usuario habilitado	Asigne al usuario habilitado la función <i>Administrador de máquinas virtuales de PlateSpin</i> (o equivalente).	La propagación queda sujeta al criterio del administrador de VMware.	Aunque puede asignar el acceso a cualquier cantidad de carpetas de máquinas virtuales en cualquier ubicación del árbol, debe asignar esta función al usuario habilitado en al menos una carpeta.

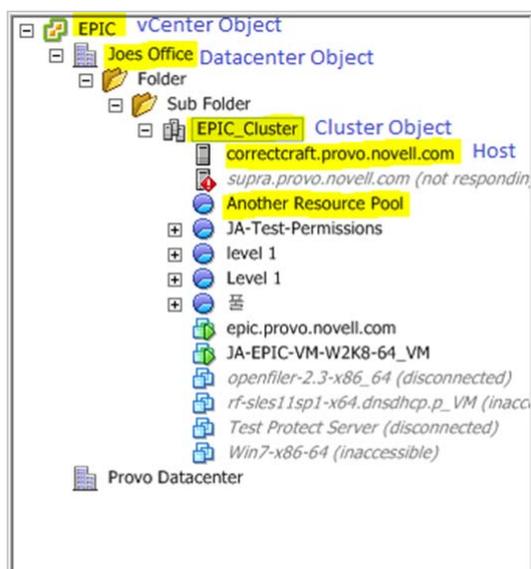
Contenedor de vCenter para asignación de funciones	Aspectos específicos de asignación de funciones	Instrucciones de propagación	Más información
<p>Todas las redes a las que necesite acceder el usuario habilitado</p> <p>Redes virtuales distribuidas con dvSwitch y dvPortgroup</p>	<p>Asigne al usuario habilitado la función <i>Administrador de máquinas virtuales de PlateSpin</i> (o equivalente).</p>	<p>La propagación queda sujeta al criterio del administrador de VMware.</p>	<p>Aunque puede asignar el acceso a cualquier cantidad de redes en cualquier ubicación del árbol, debe asignar esta función al usuario habilitado en al menos una carpeta.</p> <ul style="list-style-type: none"> ◆ Para asignar la función correcta a dvSwitch, propague la función en el centro de datos (lo que implicará que un objeto adicional reciba la función) o sitúe dvSwitch en una carpeta y asigne la función a dicha carpeta. ◆ Para que un grupo de puertos estándar se muestre como red disponible en la interfaz de Protect, cree una definición para él en cada host del clúster.
<p>Todos los almacenes de datos y clústeres de almacenes de datos a los que necesite acceder el usuario habilitado</p>	<p>Asigne al usuario habilitado la función <i>Administrador de máquinas virtuales de PlateSpin</i> (o equivalente).</p>	<p>La propagación queda sujeta al criterio del administrador de VMware.</p>	<p>El usuario habilitado debe tener esta función asignada en al menos un almacén de datos o clúster de almacenes de datos.</p> <p>Para los clústeres de almacenes de datos, el permiso debe propagarse a los almacenes de datos que contenga. En caso de no proporcionar acceso a un miembro individual del clúster, fallarán tanto la preparación como las réplicas completas.</p>

La siguiente tabla muestra la función que puede asignar al cliente o usuario inquilino.

Contenedor de vCenter para asignación de funciones	Aspectos específicos de asignación de funciones	Instrucciones de propagación	Más información
Todos los repositorios de recursos y las carpetas en las que se vayan a crear las máquinas virtuales del cliente	Asigne al usuario inquilino la función <i>Usuario de PlateSpin</i> (o equivalente).	La propagación queda sujeta al criterio del administrador de VMware.	<p>Este inquilino pertenece al grupo de administradores de PlateSpin en el servidor de PlateSpin Protect y también está en el servidor de vCenter.</p> <p>Si el inquilino va tener la posibilidad de modificar los recursos empleados por la máquina virtual (es decir, redes, imágenes ISO, etc.), proporcione a este usuario los permisos necesarios sobre dichos recursos. Por ejemplo, si desea permitir que el cliente modifique la red a la que está conectada su máquina virtual, el usuario debe tener asignada la función de solo lectura (o superior) en todas las redes a las que pueda acceder el cliente.</p>

A continuación se muestra una infraestructura virtual en la consola de vCenter. Los objetos etiquetados en azul tienen asignada la función Administrador de infraestructuras. Los objetos etiquetados en verde tienen asignada la función Administrador de máquinas virtuales. El árbol no muestra carpetas de máquinas virtuales, redes ni almacenes de datos. A estos objetos se les asigna la función *Administrador de máquinas virtuales de PlateSpin*.

Figura 5-1 Funciones asignadas en vCenter



Implicaciones de seguridad de la asignación de funciones de VMware

El software de PlateSpin emplea un usuario habilitado únicamente para realizar operaciones del ciclo de vida de protección. Desde su perspectiva como proveedor de servicios, los usuarios finales nunca tienen acceso a las credenciales del usuario habilitado y no pueden acceder al mismo conjunto de recursos de VMware. En un entorno en el que haya varios servidores de Protect configurados para usar el mismo entorno vCenter, Protect impide cualquier posibilidad de acceso entre distintos clientes. Algunas de las principales implicaciones de seguridad son las siguientes:

- ♦ Con la función *Administrador de infraestructuras de PlateSpin* asignada al objeto de vCenter, todos los usuarios habilitados podrán ver las tareas realizadas por cualquier otro usuario (pero no actuar sobre ellas).
- ♦ Puesto que no existe ninguna forma de establecer permisos en carpetas o subcarpetas de almacenes de datos, todos los usuarios habilitados con permisos en un almacén de datos tendrán acceso a todos los discos de los demás usuarios habilitados almacenados en él.
- ♦ Con la función *Administrador de infraestructuras de PlateSpin* asignada al objeto de clúster, todos los usuarios habilitados podrán activar o desactivar HA o DRS en todo el clúster.
- ♦ Con la función *Usuario de PlateSpin* asignada al objeto de clúster de almacenamiento, todos los usuarios habilitados podrán activar o desactivar SDRS en todo el clúster.
- ♦ Establecer la función *Administrador de infraestructuras de PlateSpin* en el objeto de clúster DRS y propagarla permite que el usuario habilitado vea todas las máquinas virtuales situadas en el repositorio de recursos por defecto o la carpeta de máquinas virtuales por defecto. Además, la propagación requiere que el administrador establezca explícitamente que el usuario habilitado tenga una función de “no acceso” en cada repositorio de recursos o carpeta de máquinas virtuales donde no deba tener acceso.
- ♦ Establecer la función *Administrador de infraestructuras de PlateSpin* en el objeto vCenter permite que el usuario habilitado finalice las sesiones de cualquier otro usuario conectado a vCenter.

Nota: recuerde que en estas situaciones, cada usuario habilitado es en realidad una instancia diferente del software de PlateSpin.

5.4 Transferencia de datos

En los temas siguientes se proporciona información sobre los mecanismos y opciones de la transferencia de datos de las cargas de trabajo a sus réplicas.

- ♦ [Sección 5.4.1, “Métodos de transferencia”, en la página 74](#)
- ♦ [Sección 5.4.2, “Cifrado de datos”, en la página 75](#)

5.4.1 Métodos de transferencia

Un método de transferencia describe la forma en la que los datos se replican desde una carga de trabajo de origen a un destino. PlateSpin Protect proporciona distintas funciones de transferencia de datos, que dependen del sistema operativo de la carga de trabajo protegida.

- ♦ [“Métodos de transferencia admitidos para las cargas de trabajo Windows” en la página 75](#)
- ♦ [“Métodos de transferencia admitidos para las cargas de trabajo Linux” en la página 75](#)

Métodos de transferencia admitidos para las cargas de trabajo Windows

En el caso de las cargas de trabajo Windows, PlateSpin Protect proporciona mecanismos para transferir los datos del volumen de la carga de trabajo en el nivel de bloques o de archivos.

- Réplica en el nivel de bloques de Windows:** los datos se replican en el nivel de bloques de un volumen. Para este método de transferencia, PlateSpin Protect proporciona dos mecanismos que difieren en el rendimiento y en su impacto en la continuidad. Puede pasar de un mecanismo a otro según precise.
 - ♦ **Réplica con el componente basado en bloques:** esta opción usa un componente de software dedicado para la transferencia de datos en el nivel de bloques y aprovecha el servicio de instantánea de volumen de Microsoft (VSS) con aplicaciones y servicios que admiten VSS. La instalación del componente en la carga de trabajo protegida es automática.

Nota: para instalar o desinstalar el componente basado en bloques es necesario reorganizar la carga de trabajo protegida. No es necesario reorganizar al proteger clústeres de Windows con la transferencia de datos en el nivel de bloques. Cuando se configuran los detalles de protección de la carga de trabajo, es posible instalar el componente más tarde y retrasar el reorganización necesario hasta la primera réplica.

- ♦ **Réplica sin el componente basado en bloques:** esta opción usa un mecanismo de hash junto con Microsoft VSS para realizar un seguimiento de los cambios en los volúmenes protegidos.

Con esta opción no es necesario reorganizar, pero su rendimiento es inferior a la del componente basado en bloques.
- Réplica en el nivel de archivos de Windows:** los datos se replican archivo a archivo (solo en Windows).

Métodos de transferencia admitidos para las cargas de trabajo Linux

Para las cargas de trabajo Linux, PlateSpin Protect proporciona un mecanismo de transferencia de los datos del volumen de la carga de trabajo solo en el nivel de bloques. La transferencia de datos se realiza con ayuda de un componente en el nivel de bloques que aprovecha las instantáneas LVM, si están disponible (es la opción por defecto y la recomendada). Consulte el [artículo 7005872 de la KB \(https://www.netiq.com/support/kb/doc.php?id=7005872\)](https://www.netiq.com/support/kb/doc.php?id=7005872).

El componente basado en bloques de Linux incluido en la distribución de PlateSpin Protect está compilado previamente para los núcleos estándar, no de depuración de las distribuciones de Linux compatibles. Si tiene un núcleo no estándar, personalizado o reciente, puede reconstruir el componente basado en bloques para dicho núcleo concreto. Consulte el [artículo 7005873 de la KB \(https://www.netiq.com/support/kb/doc.php?id=7005873\)](https://www.netiq.com/support/kb/doc.php?id=7005873).

La distribución o eliminación del componente es transparente, no afecta a la continuidad y no requiere intervención del usuario ni reorganizar.

5.4.2 Cifrado de datos

Para hacer más segura la transferencia de los datos de la carga de trabajo, PlateSpin Protect permite cifrar la réplica de datos. Si el cifrado está habilitado, las transferencias del origen al destino a través de la red se cifran mediante el estándar AES (Advanced Encryption Standard, estándar de cifrado avanzado) o 3DES si se habilita el cifrado FIPS (ver la sección sobre “cómo habilitar la compatibilidad con algoritmos de cifrado de datos compatibles con FIPS (opcional)” en la *Guía de instalación y actualización*).

Nota: el cifrado de datos afecta al rendimiento y podría ralentizar la transferencia de datos de forma significativa.

5.5 Niveles de protección

Un nivel de protección es un conjunto personalizable de parámetros de protección de la carga de trabajo que definen lo siguiente:

- ♦ La frecuencia y periodicidad de las réplicas.
- ♦ Si la transmisión de datos se cifrará.
- ♦ Si los datos se comprimirán y cómo se hará.
- ♦ Si se debe regular el ancho de banda disponible con una velocidad de transmisión especificada durante la transferencia de datos.
- ♦ Los criterios para que el sistema considere que una carga de trabajo está sin conexión (es errónea).

Los niveles de protección son parte integral de cada contrato de protección de la carga de trabajo. Durante la etapa de configuración de un contrato de protección de la carga de trabajo, es posible seleccionar uno de los numerosos niveles de protección incorporados y personalizar sus atributos según requiera el contrato específico.

También puede crear niveles de protección personalizados por adelantado:

- 1 En la interfaz Web de PlateSpin Protect, haga clic en *Settings > Protection Tiers > Create Protection Tier* (Configuración > Niveles de protección > Crear nivel de protección).
- 2 Especifique los parámetros del nuevo nivel de protección:

Name (Nombre)	Escriba el nombre que desea usar para el nivel.
Incremental Recurrence (Recurrencia incremental)	Permite especificar la frecuencia de las réplicas incrementales y el patrón de periodicidad incremental. Puede escribir directamente en el campo <i>Start of recurrence</i> (Inicio de la recurrencia) o hacer clic en el icono de calendario para seleccionar una fecha. Seleccione <i>None</i> (Ninguno) en <i>Recurrence Pattern</i> (Patrón de recurrencia) para no usar nunca una réplica incremental.
Full Recurrence (Recurrencia completa)	Permite especificar la frecuencia de las réplicas completas y el patrón de periodicidad completa.
Blackout Window (Ventana de interrupción)	Use este valor para forzar una interrupción de la réplica (para suspender las réplicas programadas durante las horas punta de uso o para evitar conflictos entre software que admite VSS y el componente VSS de transferencia de datos del nivel de bloques de PlateSpin). Para especificar una ventana de interrupción, haga clic en <i>Edit</i> (Editar) y seleccione un patrón de recurrencia de interrupción (diario, semanal, etc.), así como las horas de inicio y finalización del período de interrupción. Nota: las horas de inicio y finalización de la interrupción se basan en el reloj del sistema del servidor de PlateSpin.

Compression Level (Nivel de compresión)	<p>Estos valores controlan si los datos de la carga de trabajo se comprimirán antes de la transmisión y cómo se realizará esta compresión. Consulte “Compresión de datos” en la página 16.</p> <p>Seleccione una de las opciones disponibles. <i>Fast</i> (Rápida) es la opción que consume menos recursos de CPU en el origen, pero da como resultado una tasa de compresión inferior; <i>Maximum</i> (Máxima) es la que consume más, pero produce una tasa de compresión más alta. <i>Optimal</i> (Óptima), la opción intermedia, es la recomendada.</p>
Bandwidth Throttling (Regularización del ancho de banda)	<p>Estos valores controlan la regularización del ancho de banda. Consulte “Regularización del ancho de banda” en la página 16.</p> <p>Para regular las réplicas con una velocidad específica, indique el valor de rendimiento necesario en Mb/s e indique el patrón temporal.</p>
Recovery Points to Keep (Puntos de recuperación que conservar)	<p>Permite especificar el número de puntos de recuperación que se debe conservar para las cargas de trabajo que usan este nivel de protección. Consulte “Puntos de recuperación” en la página 77.</p>
Workload Failure (Error de carga de trabajo)	<p>Permite especificar el número de intentos de detección de la carga de trabajo antes de que se considere que hay un error.</p>
Workload Detection (Detección de carga de trabajo)	<p>Permite especificar el intervalo de tiempo (en segundos) entre intentos de detección de la carga de trabajo.</p>

5.6 Puntos de recuperación

Un punto de recuperación es una instantánea de un momento concreto de una carga de trabajo. Permite restaurar la carga de trabajo replicada a un estado específico.

Cada carga de trabajo protegida tiene al menos un punto de recuperación y puede tener un máximo de 32.

Advertencia: los puntos de recuperación que se van acumulando pueden causar que se agote el espacio de almacenamiento de PlateSpin Protect.

5.7 Método de réplica inicial (completa o incremental)

En las operaciones de protección y failback de la carga de trabajo, el parámetro Initial Replication (Réplica inicial) determina el ámbito de los datos transferidos de un origen a un destino.

- ♦ **Todos:** una transferencia del volumen completo se realiza desde la carga de trabajo de producción a su réplica (la carga de trabajo de failover), o de la carga de trabajo de failover a su infraestructura virtual o física original.
- ♦ **Replicación:** solo se transfieren las diferencias de un origen a su destino, siempre que tengan un sistema operativo y perfiles de volumen similares.
 - ♦ Durante la protección: la carga de trabajo de producción se compara con una máquina virtual existente en el contenedor de máquina virtual. La máquina virtual existente puede ser una de las siguientes:
 - ♦ Una máquina virtual de recuperación de la carga de trabajo anteriormente protegida; si se ha deseleccionado la opción *Delete VM* (Suprimir máquina virtual) del comando *Remove Workload* (Eliminar carga de trabajo).

- ♦ Una máquina virtual que se importa manualmente al contenedor de máquina virtual, como una máquina virtual de carga de trabajo que se traslada físicamente en un medio extraíble del sitio de producción a un sitio de recuperación remoto.

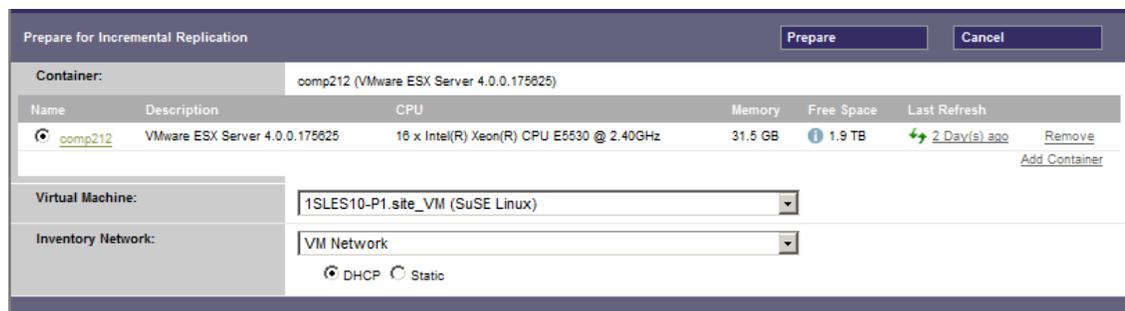
Para obtener más información, consulte la documentación de VMware.

- ♦ Durante el failback a un equipo virtual: la carga de trabajo de failover se compara con una máquina virtual existente en un contenedor de failback.
- ♦ Durante el failback en un equipo físico: la carga de trabajo de failover se compara con una carga de trabajo en el equipo físico de destino, si este está registrado con PlateSpin Protect (consulte [“Failback semiautomatizado a un equipo físico” en la página 64](#)).

Durante la protección de la carga de trabajo y el failback a un host de máquina virtual, si se selecciona *Incremental* como método de réplica inicial, debe examinar, localizar y preparar la máquina virtual de destino para la sincronización con el origen de la operación seleccionada.

- 1 Continúe con el comando de carga de trabajo requerido, por ejemplo, *Configure (Protection Details)* [Configurar (detalles de protección)] o *Failback*.
- 2 En la opción *Initial Replication Method* (Método de réplica inicial), seleccione *Incremental Replication* (Réplica incremental).
- 3 Haga clic en *Prepare Workload* (Preparar carga de trabajo).

La interfaz Web de PlateSpin Protect muestra la página Prepare for Incremental Replication (Preparar para réplica incremental).



- 4 Seleccione el contenedor requerido, la máquina virtual y la red de inventario que se debe usar para comunicarse con la máquina virtual. Si el contenedor de destino especificado es un clúster DRS de VMware, también puede especificar un repositorio de recursos de destino al que el sistema debe asignar la carga de trabajo.
- 5 Haga clic en *Prepare* (Preparar).

Espere a que el proceso se complete y a que la interfaz de usuario vuelva al comando original y seleccione la carga de trabajo preparada.

Nota: (solo en réplicas de datos de nivel de bloques) una réplica inicial incremental lleva mucho más tiempo que las réplicas siguientes. Esto se debe a que el sistema debe comparar los volúmenes del origen y del destino bloque a bloque. Las réplicas siguientes dependen de los cambios detectados por el componente basado en bloques mientras supervisa una carga de trabajo en ejecución.

5.8 Control de servicios y daemons

PlateSpin Protect permite controlar los servicios y daemons:

- ♦ **Control de servicios/daemons de origen:** durante la transferencia de datos, es posible detener automáticamente los servicios de Windows o los daemons de Linux que se ejecutan en la carga de trabajo de origen. De esta forma se garantiza que la carga de trabajo se replica en un estado más coherente que si se dejan en ejecución.

Por ejemplo, para las cargas de trabajo Windows, puede detener los servicios del software antivirus o los servicios del software de copia de seguridad VSS de otros fabricantes.

Para obtener un control adicional de los orígenes Linux durante la réplica, puede ejecutar guiones personalizados en las cargas de trabajo Linux durante cada réplica. Consulte [“Uso de los guiones freeze y thaw en todas las réplicas \(Linux\)” en la página 79](#).

- ♦ **Control del estado de inicio/control de ejecución del destino:** puede seleccionar el estado de inicio (Windows) o el nivel de ejecución (Linux) de los servicios/daemons de la máquina virtual de failover. Cuando se realiza una operación de failover o de prueba de failover, puede especificar los servicios o daemons que desea que se ejecuten o que se detengan cuando la carga de trabajo de failover se active.

Los servicios habituales que podría ser útil asignar a un estado de inicio inhabilitado son los específicos del proveedor enlazados a su infraestructura física subyacente y que no se necesitan en una máquina virtual.

5.9 Uso de los guiones freeze y thaw en todas las réplicas (Linux)

En los sistemas Linux, PlateSpin Protect proporciona la capacidad de ejecutar automáticamente guiones personalizados, *freeze* y *thaw*, que complementan la función automática de control de daemons.

El guion *freeze* se ejecuta al principio de la réplica, mientras que el guion *thaw* se ejecuta al final.

Puede usar esta capacidad para complementar la función de control automatizado de daemons proporcionada en la interfaz de usuario (consulte [“Control de servicios/daemons de origen:” en la página 79](#)). Por ejemplo, puede ser útil usar esta función para congelar temporalmente determinados daemons, en lugar de apagarlos durante las réplicas.

Para implementar la función, lleve a cabo el siguiente procedimiento antes de configurar la protección de la carga de trabajo Linux:

1 Cree los archivos siguientes:

- ♦ `platespin.freeze.sh`: un guion de shell que se ejecuta al principio de la réplica.
- ♦ `platespin.thaw.sh`: un guion de shell que se ejecuta al final de la réplica.
- ♦ `platespin.conf`: un archivo de texto donde se definen los argumentos necesarios, junto con un valor de tiempo límite.

La sintaxis requerida para el contenido del archivo `platespin.conf` es:

```
[ServiceControl]
FreezeArguments=<argumentos>
ThawArguments=<argumentos>
TimeOut=<tiempo límite>
```

Sustituya <argumentos> por los argumentos del comando necesarios, separados por espacio, y <tiempo límite> por un valor de tiempo límite en segundos. Si no se especifica un valor, se usa el tiempo límite por defecto (60 segundos).

- 2 Guarde los guiones y el archivo `.conf` en la carga de trabajo de origen de Linux en el directorio siguiente:

```
/etc/platespin
```

5.10 Volúmenes

Al añadir una carga de trabajo para proteger, PlateSpin Protect realiza un inventario de los medios de almacenamiento de la carga de trabajo de origen y configura automáticamente las opciones de la interfaz Web de PlateSpin Protect para que especifique los volúmenes que necesita para la protección.

PlateSpin Protect admite varios tipos de almacenamientos, incluidos los discos dinámicos Windows, LVM (solo la versión 2), RAID y SAN.

Para las cargas de trabajo Linux, PlateSpin Protect proporciona las siguientes funciones adicionales:

- ♦ El almacenamiento sin volúmenes, como una partición de intercambio asociada con la carga de trabajo de origen, se vuelve a crear en la carga de trabajo de failover.
- ♦ El diseño de los grupos de volúmenes y de los volúmenes lógicos se conserva para que se pueda volver a crear durante el failback.
- ♦ (Cargas de trabajo OES 2) Los diseños EVMS de las cargas de trabajo de origen se conservan y se vuelven a crear en el contenedor de máquina virtual. Los repositorios NSS se copian del origen a la máquina virtual de recuperación.

En las ilustraciones siguientes se muestra el conjunto de parámetros Replication Settings (Configuración de réplica) para una carga de trabajo Linux con varios volúmenes y dos volúmenes lógicos en un grupo de volúmenes.

Figura 5-2 Volúmenes, volúmenes lógicos y grupos de volúmenes de una carga de trabajo Linux protegida

Tier Settings																	
Replication Settings																	
Encrypt Data Transfer:	No																
Source Credentials:	root																
Number of CPUs:	1																
Replication Network:	DHCP - VM Network																
Recovery Point Datastore:	Storage2 (669.7 GB free)																
Protected Volumes:	<table border="1"> <thead> <tr> <th>Include</th> <th>Name</th> <th>Total Size</th> <th>Datastore</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>/usr</td> <td>2.9 GB</td> <td>Storage2</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>/boot</td> <td>2.0 GB</td> <td>Storage2</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>/new2 (EXT3)</td> <td>151.9 MB</td> <td>Storage2</td> </tr> </tbody> </table>	Include	Name	Total Size	Datastore	<input checked="" type="checkbox"/>	/usr	2.9 GB	Storage2	<input checked="" type="checkbox"/>	/boot	2.0 GB	Storage2	<input checked="" type="checkbox"/>	/new2 (EXT3)	151.9 MB	Storage2
	Include	Name	Total Size	Datastore													
	<input checked="" type="checkbox"/>	/usr	2.9 GB	Storage2													
	<input checked="" type="checkbox"/>	/boot	2.0 GB	Storage2													
<input checked="" type="checkbox"/>	/new2 (EXT3)	151.9 MB	Storage2														
Protected Logical Volumes:	<table border="1"> <thead> <tr> <th>Include</th> <th>Name</th> <th>Total Size</th> <th>Volume Group</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>/LogicalVolume1 (EXT3)</td> <td>484.2 MB</td> <td>group</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>/LogicalVolume2 (EXT3)</td> <td>193.7 MB</td> <td>group</td> </tr> </tbody> </table>	Include	Name	Total Size	Volume Group	<input checked="" type="checkbox"/>	/LogicalVolume1 (EXT3)	484.2 MB	group	<input checked="" type="checkbox"/>	/LogicalVolume2 (EXT3)	193.7 MB	group				
	Include	Name	Total Size	Volume Group													
	<input checked="" type="checkbox"/>	/LogicalVolume1 (EXT3)	484.2 MB	group													
<input checked="" type="checkbox"/>	/LogicalVolume2 (EXT3)	193.7 MB	group														
Volume Groups:	<table border="1"> <thead> <tr> <th>Include</th> <th>Name</th> <th>Total Size</th> <th>Datastore</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>group</td> <td>1016.0 MB</td> <td>Storage2</td> </tr> </tbody> </table>	Include	Name	Total Size	Datastore	<input checked="" type="checkbox"/>	group	1016.0 MB	Storage2								
Include	Name	Total Size	Datastore														
<input checked="" type="checkbox"/>	group	1016.0 MB	Storage2														
Non-volume Storage:	--																
Daemons to Stop During Replication:	--																
Failover Settings																	
Prepare for Failover Settings																	
Test Failover Settings																	
Recovery Points																	
Workload Details																	

En la ilustración siguiente se muestran las opciones de protección de volúmenes de una carga de trabajo OES 2 con opciones que incidan que el diseño EVMS debe conservarse y volver a crearse para la carga de trabajo de failover:

Figura 5-3 Opciones relativas a los volúmenes de Replication Settings (carga de trabajo OES 2)

Protected Logical Volumes:	<table border="1"> <thead> <tr> <th>Include</th> <th>Name</th> <th>Used Space</th> <th>Free Space</th> <th>Volume Group / EVMS Volume</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>/(REISERFS)</td> <td>2.2 GB</td> <td>2.2 GB</td> <td>system</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>/boot (EXT2)</td> <td>13.0 MB</td> <td>55.3 MB</td> <td>/dev/evms/sda1</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>/opt/novell/nss/mnt/pools/NEWPOOL (NSSFS)</td> <td>23.3 MB</td> <td>999.6 MB</td> <td>NEWPOOL</td> </tr> </tbody> </table>	Include	Name	Used Space	Free Space	Volume Group / EVMS Volume	<input checked="" type="checkbox"/>	/(REISERFS)	2.2 GB	2.2 GB	system	<input checked="" type="checkbox"/>	/boot (EXT2)	13.0 MB	55.3 MB	/dev/evms/sda1	<input checked="" type="checkbox"/>	/opt/novell/nss/mnt/pools/NEWPOOL (NSSFS)	23.3 MB	999.6 MB	NEWPOOL
	Include	Name	Used Space	Free Space	Volume Group / EVMS Volume																
	<input checked="" type="checkbox"/>	/(REISERFS)	2.2 GB	2.2 GB	system																
	<input checked="" type="checkbox"/>	/boot (EXT2)	13.0 MB	55.3 MB	/dev/evms/sda1																
<input checked="" type="checkbox"/>	/opt/novell/nss/mnt/pools/NEWPOOL (NSSFS)	23.3 MB	999.6 MB	NEWPOOL																	
Non-volume Storage:	<table border="1"> <thead> <tr> <th>Include</th> <th>Partition</th> <th>Is Swap</th> <th>Total Size</th> <th>Datastore / Volume Group</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>/dev/system/swap</td> <td>Yes</td> <td>1.48 GB</td> <td>system</td> </tr> </tbody> </table>	Include	Partition	Is Swap	Total Size	Datastore / Volume Group	<input checked="" type="checkbox"/>	/dev/system/swap	Yes	1.48 GB	system										
Include	Partition	Is Swap	Total Size	Datastore / Volume Group																	
<input checked="" type="checkbox"/>	/dev/system/swap	Yes	1.48 GB	system																	
Volume Groups:	<table border="1"> <thead> <tr> <th>Include</th> <th>Name</th> <th>Total Size</th> <th>Datastore</th> <th>Thin Disk</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>system</td> <td>5.9 GB</td> <td>dev-comp124:storage</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Include	Name	Total Size	Datastore	Thin Disk	<input checked="" type="checkbox"/>	system	5.9 GB	dev-comp124:storage	<input type="checkbox"/>										
Include	Name	Total Size	Datastore	Thin Disk																	
<input checked="" type="checkbox"/>	system	5.9 GB	dev-comp124:storage	<input type="checkbox"/>																	
EVMS Volumes:	<table border="1"> <thead> <tr> <th>Include</th> <th>Name</th> <th>Datastore</th> <th>Total Size</th> <th>Datastore</th> <th>Thin Disk</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>/dev/evms/sda1</td> <td></td> <td>70.6 MB</td> <td>dev-comp124:storage</td> <td><input type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>NEWPOOL</td> <td></td> <td>1023.0 MB</td> <td>dev-comp124:storage</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Include	Name	Datastore	Total Size	Datastore	Thin Disk	<input checked="" type="checkbox"/>	/dev/evms/sda1		70.6 MB	dev-comp124:storage	<input type="checkbox"/>	<input checked="" type="checkbox"/>	NEWPOOL		1023.0 MB	dev-comp124:storage	<input type="checkbox"/>		
Include	Name	Datastore	Total Size	Datastore	Thin Disk																
<input checked="" type="checkbox"/>	/dev/evms/sda1		70.6 MB	dev-comp124:storage	<input type="checkbox"/>																
<input checked="" type="checkbox"/>	NEWPOOL		1023.0 MB	dev-comp124:storage	<input type="checkbox"/>																
Daemons to Stop During Replication:	Add Daemons																				

5.11 Redes

PlateSpin Protect permite controlar la identidad de red y la configuración LAN de la carga de trabajo de failover para evitar que el tráfico de réplica interfiera con el tráfico principal de la LAN o la WAN.

Puede especificar configuraciones de red distintas en los detalles de protección de la carga de trabajo para usarlas en distintas etapas del flujo de trabajo de protección y recuperación de la carga de trabajo:

- ♦ **Replication (Réplica):** (conjunto de parámetros [Replication \(Réplica\)](#)) para separar el tráfico de réplica normal del tráfico de producción.
- ♦ **Failover:** (conjunto de parámetros [Failover](#)) para que la carga de trabajo de failover entre a formar parte de la red de producción cuando se active.
- ♦ **Prepare for Failover (Preparar para failover):** (parámetro de red [Prepare for Failover \(Preparar para failover\)](#)) para la configuración de red durante la etapa opcional de preparación para failover.
- ♦ **Test Failover (Probar failover):** (conjunto de parámetros [Test Failover \(Probar failover\)](#)) para la configuración de red que se aplica a la carga de trabajo de failover durante le etapa de prueba de failover.

5.12 Failback a equipos físicos

Si la infraestructura de destino necesaria para una operación de failback es un equipo físico, debe registrarlo en PlateSpin Protect.

El registro de un equipo físico se realiza arrancando el equipo físico de destino con la imagen ISO de arranque de PlateSpin.

- ♦ [Sección 5.12.1, “Descarga de la imagen ISO de arranque de PlateSpin”, en la página 82](#)
- ♦ [Sección 5.12.2, “Incorporación de controladores de dispositivo adicionales en la imagen ISO de arranque”, en la página 83](#)
- ♦ [Sección 5.12.3, “Registro de equipos físicos como destinos de failback con PlateSpin Protect”, en la página 84](#)

5.12.1 Descarga de la imagen ISO de arranque de PlateSpin

Es posible descargar las imágenes ISO de arranque de PlateSpin (`bootofx.x2p.iso` para destinos basados en firmware BIOS y `bootofx.x2p.uefi.iso` para destinos basados en firmware UEFI) del área de PlateSpin Protect en [Novell Downloads \(http://download.novell.com\)](http://download.novell.com) (Descargas de Novell) mediante una búsqueda con los parámetros siguientes:

- ♦ *Product or Technology* (Producto o tecnología): PlateSpin Protect
- ♦ *Select Version* (Seleccionar versión): PlateSpin Protect11.0
- ♦ *Date Range* (Intervalo de fechas): All Dates (Todas la fechas)

5.12.2 Incorporación de controladores de dispositivo adicionales en la imagen ISO de arranque

Puede usar una utilidad personalizada para incorporar controladores de dispositivo de Linux en la imagen de arranque de PlateSpin antes de grabarla en un CD:

- 1 Obtenga o compile los archivos de controlador *.ko oportunos del fabricante del hardware de destino.

Importante: asegúrese de que los controladores son válidos para el núcleo incluido con el archivo ISO (para sistemas x86: 3.0.93-0.8-pae, para sistemas x64: 3.0.93-0.8-default) y son válidos para la arquitectura de destino. Consulte el [artículo 7005990 de la KB](#).

- 2 Monte la imagen en un equipo Linux (se necesitan credenciales de usuario `Root`). Utilice la siguiente sintaxis de comando:

```
mount -o loop <vía-a-ISO> <punto_de_montaje>
```

- 3 Copie el guion `rebuildiso.sh`, situado en el subdirectorio `/tools` del archivo ISO montado, a un directorio de trabajo temporal. Cuando termine, desmonte el archivo ISO (ejecute el comando `umount <punto_de_montaje>`).

- 4 Cree otro directorio de trabajo para los archivos de controladores necesarios y guárdelos en dicho directorio.

- 5 En el directorio donde haya guardado el guión `rebuildiso.sh`, ejecute `rebuildiso.sh` como usuario `Root`, empleando la siguiente sintaxis:

```
./rebuildiso.sh <ARGS> [-v] -m32|-m64 -i <archivo_ISO>
```

La siguiente tabla muestra las posibles opciones de línea de comandos para este comando:

Opción	Descripción
<code>-i <archivo_ISO></code>	<code><archivo_ISO></code> es el archivo ISO que desee modificar, enumerar, etc.
<code>-v</code>	Si se utiliza con el argumento <code>-l</code> , la opción hace que se utilice <code>modinfo</code> para obtener información detallada sobre el controlador.
<code>-o</code>	Si se utiliza con el argumento <code>-c</code> o el argumento <code>-d</code> , la antigua copia del archivo ISO no se sobrescribirá.
<code>-m32</code>	Especifica una inyección <code>initrd</code> de 32 bits
<code>-m64</code>	Especifica una inyección <code>initrd</code> de 64 bits

La tabla siguiente indica los posibles argumentos que se pueden usar con este comando. Debe emplearse al menos uno de los argumentos en el comando:

Argumento	Descripción
<code>-d <vía></code>	<code><vía></code> especifica el directorio que contiene los controladores (es decir, archivos *.ko) que desee inyectar. Al completarse el comando, el archivo ISO se actualiza con los controladores añadidos.
<code>-c <vía></code>	<code><vía></code> especifica la ubicación en la que se encuentra un archivo <code>ConfigureTakeControl.xml</code> .

Argumento	Descripción
-l [<i>tipo</i>]	<p><tipo> especifica un subconjunto de controladores que desee enumerar. El valor por defecto incluye todos los tipos.</p> <p>Se presupone que los tipos de controladores enumerados que comiencen con una barra inclinada (/) se encuentran en <directorio_módulo_núcleo>/kernel/</p> <p>Se presupone que los tipos de controladores sin una barra inclinada (/) se encuentran en <directorio_módulo_núcleo>/kernel/drivers/</p> <p>Ejemplos de subconjunto de controladores:</p> <pre>-l scsi -l 'net video' -l '/net net'</pre> <p>Uso especial de este argumento:</p> <p>Si desea enumerar los subdirectorios disponibles de cada subconjunto, utilice el argumento de la forma siguiente: -l INDEX</p>

Ejemplos de sintaxis

- ♦ Para enumerar un índice de controladores de 32 bits:

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -l INDEX
```
- ♦ Para enumerar los controladores encontrados en la carpeta /misc:

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -l misc
```
- ♦ Para inyectar los controladores de 32 bits de la carpeta /oem-drivers:

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -d oem-drivers
```
- ♦ Para inyectar los controladores de 64 bits de una carpeta /oem-drivers y también un archivo ConfigureTakeControl.xml personalizado:

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m64 -c ConfigureTakeControl.xml -d oem-drivers
```

5.12.3 Registro de equipos físicos como destinos de failback con PlateSpin Protect

- 1 Grabe la imagen ISO de arranque de PlateSpin en un CD o guárdela en el medio desde el que arranca el destino.
- 2 Asegúrese de que el puerto del conmutador de red conectado al destino tiene definido el valor *Auto Full Duplex* (Transmisión dúplex automática).
- 3 Use el CD de arranque para arrancar el equipo físico de destino y espere a que se abra la ventana del indicador de comandos.
- 4 (Solo en Linux) En sistemas de 64 bits, en el indicador de arranque inicial, escriba lo siguiente:
 - ♦ ps64 (para sistemas con hasta 512 MB de RAM)
 - ♦ ps64_512m (para sistemas con más de 512 MB de RAM)
- 5 Pulse Intro.

- 6 Cuando se le pida, introduzca el nombre de host o la dirección IP del host del servidor de PlateSpin.
- 7 Proporcione las credenciales de administrador para el host del servidor de PlateSpin especificando una autoridad. Para la cuenta de usuario, use este formato:
dominio\usuario o *nombre_de_host\usuario*
Las tarjetas de red disponibles se detectan y se muestran según sus direcciones MAC.
- 8 Si DHCP está disponible en la NIC que se va a usar, pulse Intro para continuar. Si DHCP no está disponible, seleccione la NIC requerida para configurarse con una dirección IP estática.
- 9 Introduzca un nombre de host para el equipo físico o pulse la tecla Intro para aceptar los valores por defecto.
- 10 Cuando se le pida que indique si desea usar HTTPS, introduzca **Y** (Sí), si ha habilitado SSL, o **N** (No), si no lo ha hecho.

Después de unos minutos, el equipo físico estará disponible en la configuración de failback de la interfaz Web de PlateSpin Protect.

5.13 Temas avanzados sobre la protección de la carga de trabajo

- ♦ [Sección 5.13.1, “Protección de clústeres de Windows”, en la página 85](#)
- ♦ [Sección 5.13.2, “Uso de funciones de protección de la carga de trabajo mediante la API de servicios Web de PlateSpin Protect”, en la página 87](#)

5.13.1 Protección de clústeres de Windows

admite la protección de servicios empresariales de un clúster de Microsoft Windows. Las tecnologías de agrupación en clúster admitidas son:

- ♦ Clúster de failover de Microsoft basado en servidor Windows 2008 R2

En esta sección se incluye la información siguiente:

- ♦ [“Protección de la carga de trabajo” en la página 86](#)
- ♦ [“Failover de protección” en la página 87](#)
- ♦ [“Failback de protección” en la página 87](#)

Nota: para obtener información sobre la reconstrucción del entorno Windows 2008/2008R2 Failover Cluster después de que se haya protegido mediante PlateSpin Forge durante el failover/failback, consulte el [artículo de la KB](#) donde se describe el procedimiento.

Protección de la carga de trabajo

La protección de un clúster se logra mediante réplicas incrementales de los cambios del nodo activo transmitidas a un clúster de un nodo virtual, que se puede usar para solucionar problemas de la infraestructura de origen.

La cobertura de asistencia técnica para las migraciones de clúster de la versión actual está sujeta a las condiciones siguientes:

- ♦ Cuando se realiza una operación *Add Workload* (Añadir carga de trabajo), debe definir el nodo activo; es decir, el nodo posee actualmente el recurso de quórum del clúster. El nodo activo se identifica mediante la dirección IP del clúster (*dirección IP virtual*). Al especificar la dirección IP de un nodo individual, dicho nodo se incorpora al inventario como una carga de trabajo Windows normal no de clúster.
- ♦ Es preciso colocar un recurso de quórum de clúster junto al grupo de recursos del clúster (servicio) que se va a proteger.

Cuando se usa la transferencia basada en bloques, los componentes del controlador basado en bloques no se instalan en los nodos del clúster. La transferencia basada en bloques se produce cuando se usa una sincronización sin controlador con una réplica basada en MD5. Dado que el controlador basado en bloques no se instala, no es necesario rearrancar los nodos del clúster de origen.

Nota: la transferencia basada en bloques no se admite para proteger clústeres de Microsoft Windows.

Si se produce un failover de nodo entre réplicas incrementales de un clúster protegido y si el nuevo perfil del nodo activo es similar al nodo activo que ha fallado, el contrato de protección continúa según esté programado. En caso contrario, el comando falla. Los perfiles de los nodos de clúster se consideran similares si:

- ♦ Tienen el mismo número de volúmenes.
- ♦ Cada volumen es exactamente del mismo tamaño en cada nodo.
- ♦ Tienen un número idéntico de conexiones de red.
- ♦ Los números de serie de los volúmenes locales (volumen del sistema y volumen reservado para el sistema) deben ser iguales en cada nodo del clúster.

Si las unidades locales de cada nodo del clúster tienen distintos números de serie, no podrá ejecutar una réplica incremental después de que el nodo activo cambie en caso de un fallo del nodo. Por ejemplo, el nodo activo es Nodo 1 y cambia a Nodo 2).

Existen dos opciones para admitir clústeres en esta situación para Protect 11.0.1:

- ♦ (Recomendado) Use la utilidad *Gestor de volúmenes* personalizada para cambiar los números de serie del volumen local a fin de que coincidan en todos los nodos del clúster. Para obtener más información, consulte el [Apéndice B, "Sincronización del almacenamiento local del nodo de clúster", en la página 129](#).
- ♦ (Condicional y opcional) Si se produce este error:

```
Volume mappings does not contain source serial number: xxxx-xxxx,
```

puede que se deba a un cambio en el nodo activo antes de ejecutar la réplica incremental. En tal caso, puede ejecutar una réplica completa para asegurarse de que el clúster vuelve a estar protegido. Las réplicas incrementales deben funcionar de nuevo después de la réplica completa.

Si decide que no desea hacer coincidir los números de serie de los volúmenes de cada nodo del clúster, es necesario realizar una réplica completa antes de cada réplica incremental cada vez que el nodo activo realice un failover a un nuevo nodo del clúster.

Si se produce un failover del nodo antes de que se complete el proceso de copia durante una réplica completa o incremental, el comando se cancela y se muestra un mensaje que indica que es necesario volver a ejecutar la réplica.

Para proteger un clúster de Windows, siga el flujo de trabajo de protección de la carga de trabajo habitual (consulte [“Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo” en la página 49](#)).

Failover de protección

Cuando la operación de failover se completa y el equipo de failover vuelve a estar conectado, observará un clúster multinodo con un nodo activo (los demás nodos no estarán disponibles).

Para realizar el failover (o para probarlo) en un clúster de Windows, el clúster debe ser capaz de conectarse a un controlador de dominio. Para aprovechar la función de failover de prueba, debe proteger el controlador de dominio junto con el clúster. Durante la prueba, active el controlador de dominio, seguido por la carga de trabajo del clúster de Windows (en una red aislada).

Failback de protección

En esta versión solo se admiten operaciones de failback que usen la réplica completa para un clúster de Windows.

Si configura el failback como una réplica completa en un destino físico, puede usar uno de estos métodos:

- ♦ Asigne todos los discos del equipo de failover a un único disco local del destino de failback.
- ♦ Añada otro disco (`Disco 2`) al equipo de failback físico. A continuación, puede configurar la operación de failback para que restaure el volumen del sistema de failover al `Disco 1` y los discos adicionales de failover (los discos compartidos anteriores) al `Disco 2`. Esto permite que el disco del sistema se restaure en un disco de almacenamiento del mismo tamaño que el de origen original.

Cuando se complete el failback, puede unir otros nodos al clúster recién restaurado.

5.13.2 Uso de funciones de protección de la carga de trabajo mediante la API de servicios Web de PlateSpin Protect

Puede usar la función de protección de cargas de trabajo según el programa mediante la API `protectionservices` desde las aplicaciones. Puede usar cualquier lenguaje de programación o de guiones que admita un cliente HTTP y el entorno de serialización JSON.

```
https://<nombre de host | dirección_IP>/protectionservices
```

Sustituya `<nombre_de_host | dirección_IP>` con el nombre de host o la dirección IP del host del servidor de PlateSpin. Si SSL no está habilitado, use `https` en el URI.

Figura 5-4 API de la página principal del servidor de Protect

PlateSpin Protect Server API

Version 4.0.0.1161

Documentation

Getting started

- [Getting started with API](#)
- [Security and authentication](#)
- [Developer Guidelines](#)
- [Troubleshooting](#)
- [FAQ](#)

How to

- [Steps to protect workload](#)
- [Working with workload](#)
- [Working with container](#)
- [Working with security groups](#)
- [Working with protection tiers](#)
- [Limitations of the API](#)
- [Samples](#)
- [Glossary](#)

REST Resources (auto-generated)

- [Containers](#)
- [Workloads](#)
- [Configuration](#)
- [Operations](#)
- [Protection Tiers](#)
- [Security Groups](#)

Resource representations

This section specifies the representations of the resources which this API operates on. The representations are made up of fields, each with a name and value, encoded using a JSON dictionary. The values may be numeric or string literals, lists, or dictionaries, each of which are represented in the obvious way in JSON. These representations typically nest. For example, the representation of a Containers will include representations of the Container which inhabit it, which in turn include representations of the Virtual Machine. Many of the models specify that the representation includes a uri field whose value is the URI of the resource being represented. This is present to support URI discovery in nested representations.

Para crear un guion de operaciones habituales de protección de la carga de trabajo, use las muestras con referencias escritas en Python como guía. También se proporciona una aplicación Microsoft Silverlight, junto con su código fuente, como referencia.

Descripción general de la API

PlateSpin Protect presenta una vista previa de tecnología API basada en REST que los desarrolladores pueden usar para crear sus propias aplicaciones que funcionen con el producto. La API incluye información sobre las operaciones siguientes:

- ♦ descubrir contenedores
- ♦ descubrir cargas de trabajo
- ♦ configurar la protección
- ♦ ejecutar aplicaciones, operaciones de failover y de failback
- ♦ consultar el estado de la carga de trabajo y del contenedor
- ♦ consultar el estado de las operaciones en ejecución
- ♦ consultar los grupos de seguridad y sus niveles de protección

Los administradores de Protect pueden utilizar una muestra de Jscript (<https://localhost/protectionservices/Documentation/Samples/protect.js>) desde la línea de comandos para acceder al producto a través de la API. La muestra puede servir como ayuda para escribir guiones para trabajar con el producto. Mediante la utilidad de línea de comandos, puede realizar las operaciones siguientes:

- ♦ añadir una única carga de trabajo

- ♦ añadir un único contenedor
- ♦ ejecutar las operaciones de réplica, failover y failback
- ♦ añadir varias cargas de trabajo y contenedores a la vez

Nota: para obtener más información sobre esta operación, consulte la documentación de la API en <https://localhost/protectionservices/Documentation/AddWorkloadsAndContainersFromCsvFile.htm>.

- ♦ eliminar todas las cargas de trabajo a la vez
- ♦ eliminar todos los contenedores a la vez

La página principal de la API REST de PlateSpin Protect (<https://localhost/protectionservices/> o <https://<página del servidor>/protectionservices/>) incluye enlaces a contenido que puede resultar útil para desarrolladores y administradores.

Esta vista previa de tecnología se desarrollará por completo con nuevas funciones en versiones posteriores.

6 Herramientas auxiliares para trabajar con equipos físicos

La distribución de PlateSpin Protect incluye herramientas que puede usar para trabajar con equipos físicos como destinos de failback.

- ♦ [Sección 6.1, “Gestión de controladores de dispositivo”, en la página 91](#)

6.1 Gestión de controladores de dispositivo

PlateSpin Protect incluye una biblioteca de controladores de dispositivo e instala de forma automática los controladores oportunos en las cargas de trabajo de destino. Si falta algún controlador o no es compatible, o bien si necesita controladores concretos para una infraestructura de destino, puede que tenga que añadir (cargar) controladores a la base de datos de controladores de PlateSpin Protect o PlateSpin Forge.

En las secciones siguientes se proporcionan más detalles:

- ♦ [Sección 6.1.1, “Empaquetado de controladores de dispositivo para sistemas Windows”, en la página 91](#)
- ♦ [Sección 6.1.2, “Empaquetado de controladores de dispositivo para sistemas Linux”, en la página 92](#)
- ♦ [Sección 6.1.3, “Carga de controladores a la base de datos de controladores de dispositivos de PlateSpin Protect”, en la página 92](#)
- ♦ [Sección 6.1.4, “Uso de la función de traductor de ID de plug-and-play \(PnP\)”, en la página 95](#)

6.1.1 Empaquetado de controladores de dispositivo para sistemas Windows

Para empaquetar los controladores de dispositivo de Windows a fin de cargarlos en la base de datos de controladores de PlateSpin Protect:

- 1 Prepare todos los archivos de controlador interdependientes (*.sys, *.inf, *.dll, etc.) para la infraestructura y dispositivo de destino. Si ha obtenido controladores específicos del fabricante en archivos de reserva .zip o ejecutables, extráigalos primero.
- 2 Guarde los archivos de controlador en carpetas independientes, con una carpeta por dispositivo.

Los controladores ya están listos para cargarse. Consulte [“Carga de controladores a la base de datos de controladores de dispositivos de PlateSpin Protect” en la página 92](#).

Nota: para no tener problemas durante la operación de protección del trabajo y la carga de trabajo de destino, cargue solo controladores firmados digitalmente para:

- ♦ Todos los sistemas Windows de 64 bits
 - ♦ Las versiones de 32 bits de los sistemas Windows Vista y Windows Server 2008, así como Windows 7
-

6.1.2 Empaquetado de controladores de dispositivo para sistemas Linux

Para empaquetar los controladores de dispositivo de Linux para cargarlos en la base de datos de controladores de PlateSpin Protect, puede usar una utilidad personalizada incluida en una de las imágenes ISO de arranque de PlateSpin.

- 1 En una estación de trabajo Linux, cree un directorio para los archivos de controlador de dispositivo. Todos los controladores del directorio deben ser para el mismo núcleo y la misma arquitectura.

- 2 Descargue la imagen de arranque y móntela.

Por ejemplo, si la imagen ISO se ha copiado en el directorio `/root`, indique este comando para destinos con firmware BIOS:

```
# mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.iso /mnt/ps
```

o este comando para destinos con firmware UEFI:

```
# mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.uefi.iso /mnt/ps
```

- 3 En el subdirectorio `/tools` de la imagen ISO montada, copie el archivo de reserva `packageModules.tar.gz` en otro directorio de trabajo y extráigalo.

Por ejemplo, para un archivo `.gz` que se encuentre en el directorio de trabajo actual, indique este comando:

```
tar -xvzf packageModules.tar.gz
```

- 4 Introduzca el directorio de trabajo y ejecute el comando siguiente:

```
./PackageModules.sh -d <vía_a_directorio_de_controlador> -o <nombre de paquete>
```

Sustituya `<vía_a_directorio_de_controlador>` por la vía real al directorio en el que ha guardado los archivos de controlador, y `<nombre de paquete>` por el nombre real del paquete, con el formato siguiente:

```
Nombrecontrolador-versióncontrolador-distribución-versiónnúcleo-  
arquitectura.pkg
```

Por ejemplo, `bnx2x-1.48.107-RHEL4-2.6.9-11.EL-i686.pkg`

El paquete ya está listo para cargarse. Consulte [“Carga de controladores a la base de datos de controladores de dispositivos de PlateSpin Protect”](#) en la página 92.

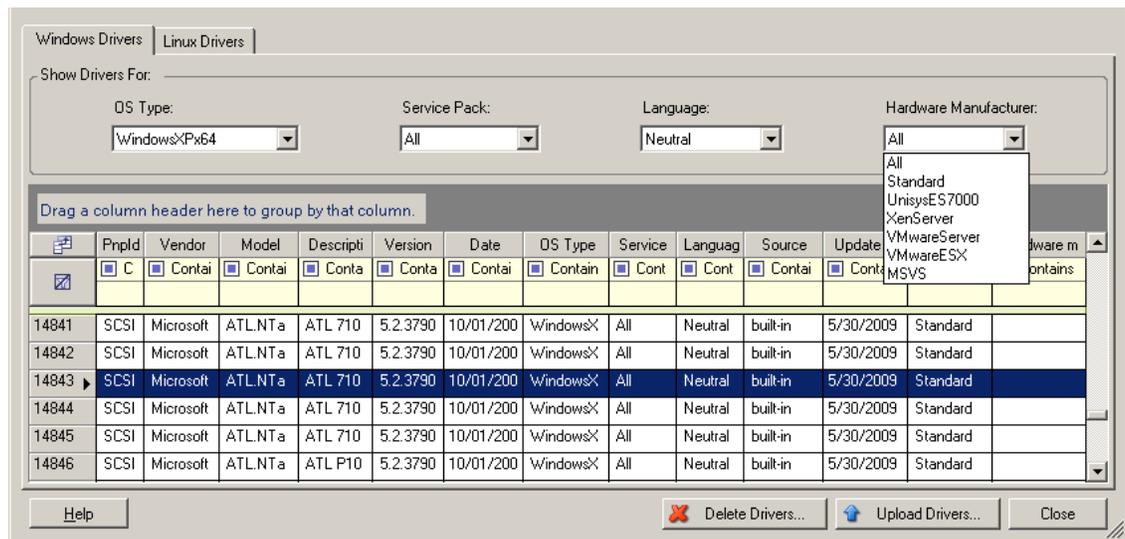
6.1.3 Carga de controladores a la base de datos de controladores de dispositivos de PlateSpin Protect

Use PlateSpin Driver Manager para cargar controladores de dispositivo a la base de datos de controladores.

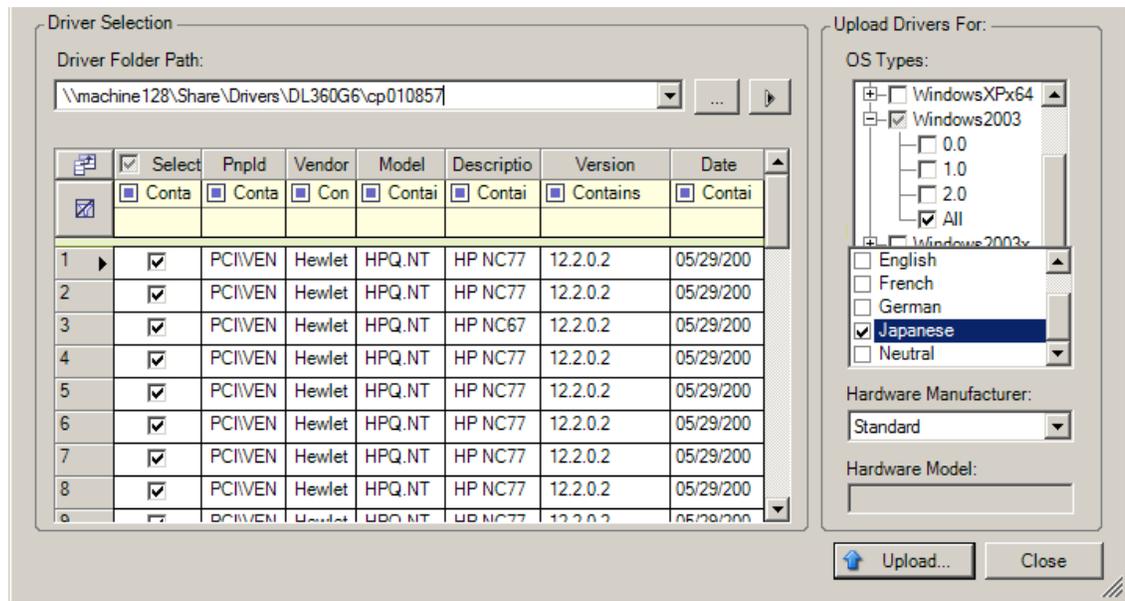
Nota: durante la carga, PlateSpin Protect no valida los controladores con los tipos de sistema operativo ni con sus especificaciones de bits. Asegúrese de cargar solo controladores adecuados para la infraestructura de destino.

Procedimiento de carga de controladores de dispositivo (Windows)

- 1 Obtenga y prepare los controladores necesarios del dispositivo. Consulte [Empaquetado de controladores de dispositivo para sistemas Windows](#).
- 2 En el host del servidor de PlateSpin, en \Archivos de programa\PlateSpin Protect Server\DriverManager, inicie el programa `DriverManager.exe` y seleccione la pestaña *Windows Drivers* (Controladores de Windows).



- 3 Haga clic en *Upload Drivers* (Cargar controladores), diríjase a la carpeta que contiene los archivos de controlador necesarios y seleccione el tipo de sistema operativo aplicable, el idioma y las opciones del fabricante del hardware.



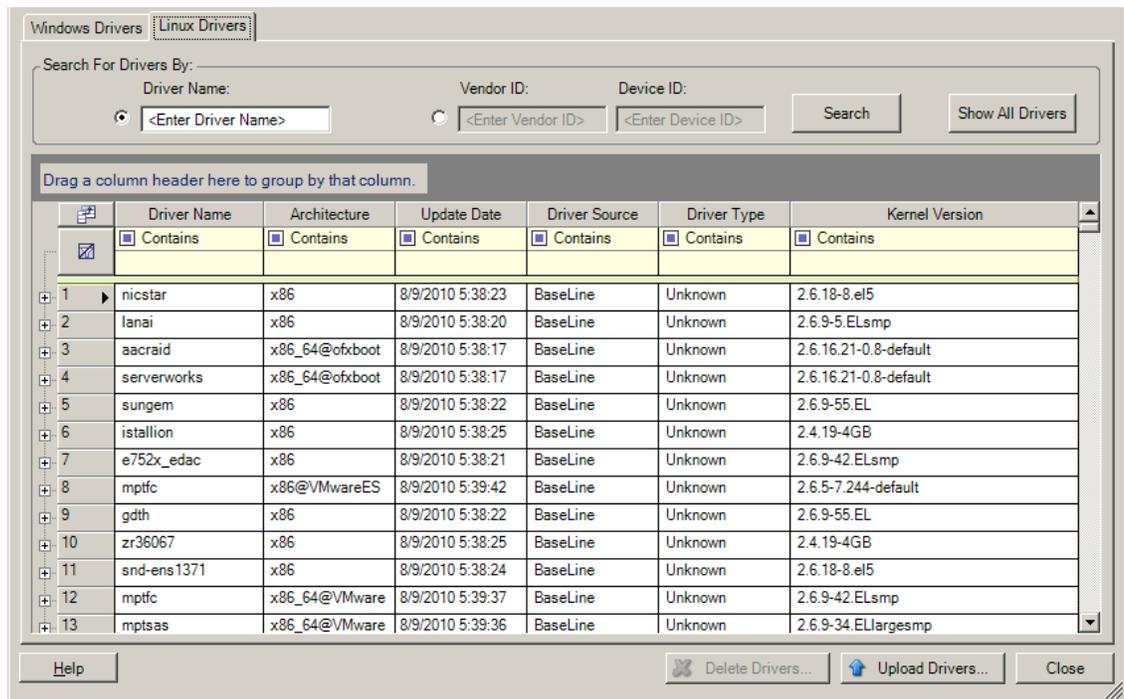
Seleccione *Standard* (Estándar) en la opción *Hardware Manufacturer* (Fabricante del hardware), a no ser que los controladores se hayan diseñado específicamente para alguno de los entornos de destino mostrados.

- 4 Haga clic en *Upload* (Cargar) y confirme la selección cuando se le solicite.

El sistema carga los controladores seleccionados en la base de datos de controladores.

Procedimiento de carga de controladores de dispositivo (Linux)

- 1 Obtenga y prepare los controladores necesarios del dispositivo. Consulte [Empaquetado de controladores de dispositivo para sistemas Linux](#).
- 2 Haga clic en *Tools > Manage Device Drivers* (Herramientas > Gestionar controladores de dispositivo) y seleccione la pestaña *Linux Drivers* (Controladores Linux):



- Haga clic en *Upload Drivers* (Cargar controladores), diríjase a la carpeta que contiene el paquete de controlador requerido (*.pkg) y haga clic en *Upload All Drivers* (Cargar todos los controladores).

El sistema carga los controladores seleccionados en la base de datos de controladores.

6.1.4 Uso de la función de traductor de ID de plug-and-play (PnP)

“Plug-and-play” (PnP) hace referencia a la función del sistema operativo Windows que permite la conectividad, la configuración y la gestión con dispositivos plug-and-play nativos. En Windows, la función facilita el descubrimiento de dispositivos de hardware que admiten PnP conectados a un bus PnP. A los dispositivos compatibles con PnP se les asigna un conjunto de cadenas de identificación de dispositivo según su fabricante. Estas cadenas se programan en el dispositivo cuando se fabrica y resultan fundamentales para la forma de funcionar de PnP: forman parte del origen de información de Windows utilizado para emparejar el dispositivo con un controlador válido.

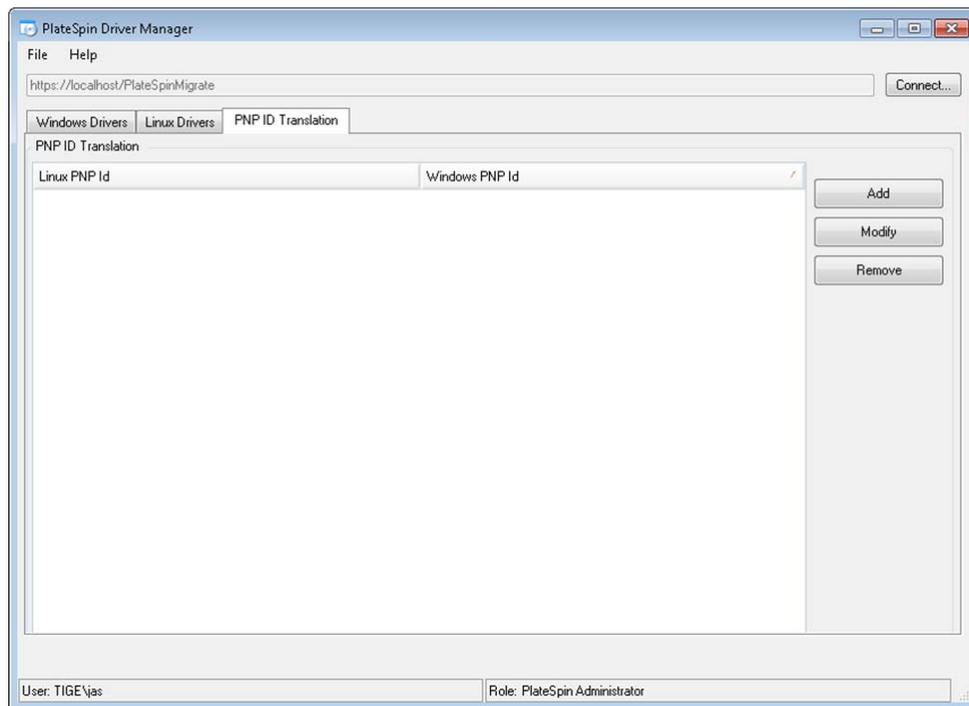
Cuando el servidor de PlateSpin descubre cargas de trabajo y su hardware disponible, el descubrimiento incluye estos ID de PnP. El almacenamiento de estos datos forma parte de los detalles de la carga de trabajo. PlateSpin usa los ID para determinar qué controlador, si hubiera alguno, debe incluirse durante la operación de failover/failback. El servidor de PlateSpin conserva una base de

datos de ID de PnP para los controladores asociados con cada sistema operativo admitido. Dado que Windows y Linux usan formatos distintos para los ID de PnP, una carga de trabajo Windows descubierta por el disco de protección de RAM de Linux contiene ID de PnP con el estilo de Linux.

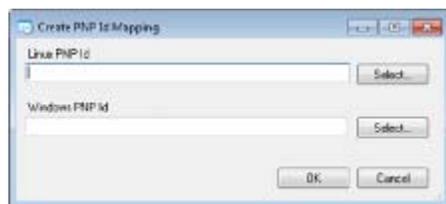
Estos ID reciben un formato coherente, por lo que PlateSpin puede aplicar una transformación estándar a cada uno de ellos para determinar su ID de PnP de Windows correspondiente. La traducción se produce de forma automática en el producto PlateSpin. La función permite al usuario o a un técnico de asistencia añadir, editar o eliminar asignaciones personalizadas de PnP.

Lleve a cabo estos pasos para utilizar la función de traducción de ID PnP:

- 1 Lance la herramienta PlateSpin Driver Manager y conéctese al servidor de PlateSpin.
- 2 En Driver Manager, seleccione la pestaña *PNP ID Translation* (Traducción de IP de PnP) para abrir la lista correspondiente, que incluye las asignaciones actuales conocidas de los ID de PnP personalizadas.



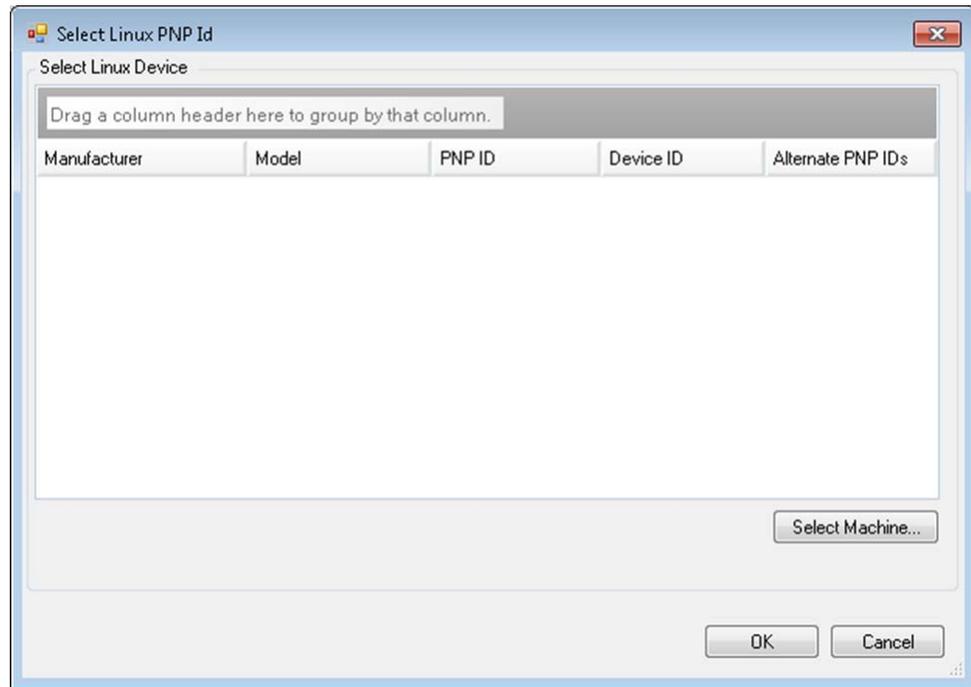
- 3 En la página de la lista, haga clic en *Add* (Añadir) para abrir el recuadro de diálogo *Create PNP ID Mapping* (Crear asignación de ID de PnP).



- 4 En el campo *Linux PNP ID* (ID de PnP de Linux), añada un ID de PnP de Linux.
 - 4a (Condicional) Si lo conoce, escriba el ID de PnP de Linux que desea usar.
O bien

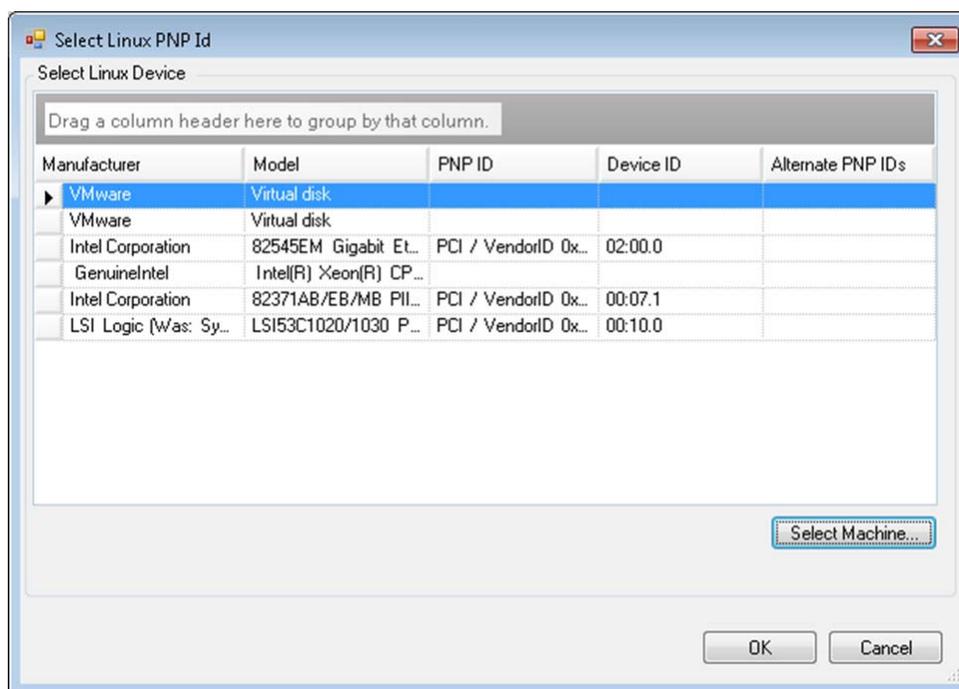
4b (Condicional) Seleccione un ID de una carga de trabajo descubierta anteriormente.

4b1 Junto al campo *Linux PnP ID* (ID de PnP de Linux), haga clic en *Select* (Seleccionar) para abrir el recuadro de diálogo *Select Linux PnP ID* (Seleccionar ID de PnP de Linux).

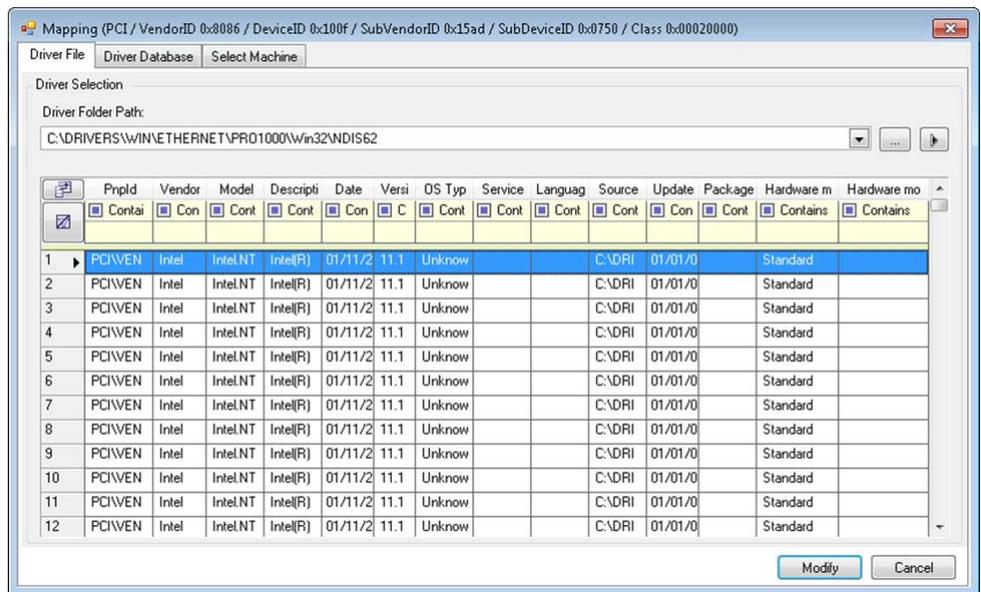


4b2 En el recuadro de diálogo, haga clic *Select Machine* (Seleccionar equipo) para mostrar una lista de los equipos descubiertos anteriormente por el disco RAM de Linux de PlateSpin.

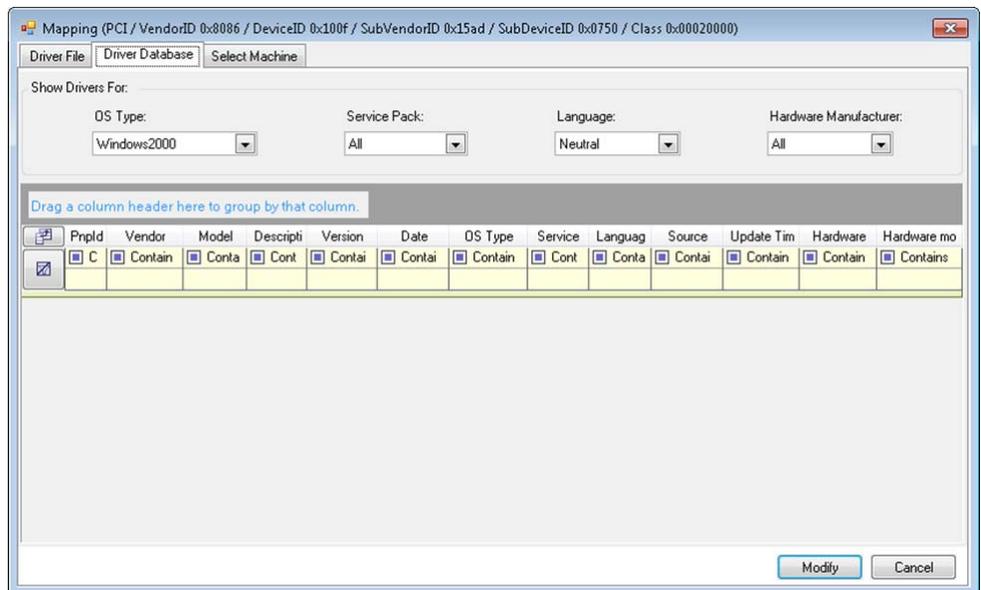
4b3 Resalte uno de los dispositivos de la lista y haga clic en *Select* (Seleccionar) para completar la lista del recuadro de diálogo *Select Linux PnP ID* (Seleccionar ID de PnP de Linux).



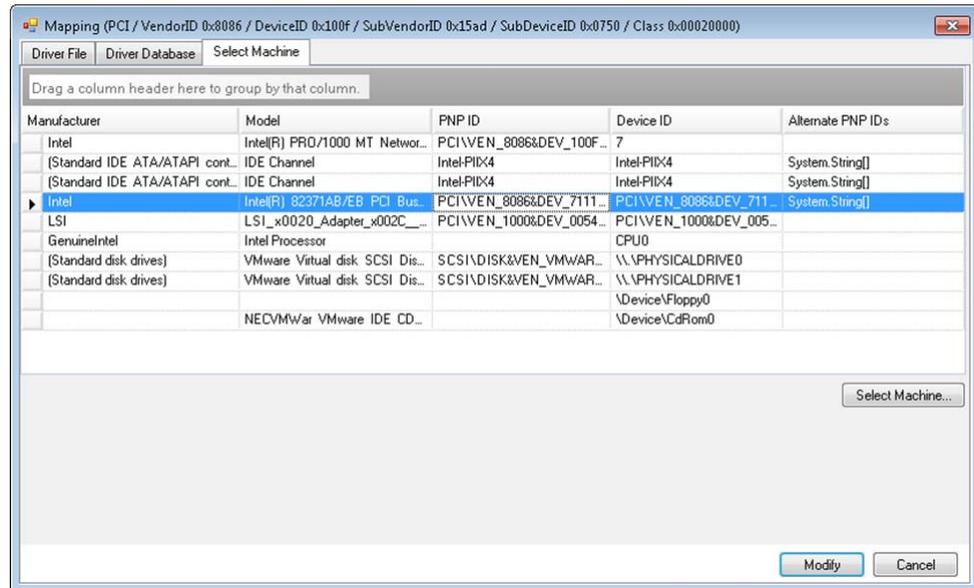
- 4b4** Seleccione un dispositivo de la lista y haga clic en *OK* (Aceptar) para aplicar la transformación estándar al ID de PnP y mostrarla en el recuadro de diálogo *Create PnP ID Mapping* (Crear asignación de ID de PnP).
- 5** En el campo *Windows PNP ID* (ID de PnP de Windows), añada un ID de PnP de Windows:
- 5a** (Condicional) Si lo conoce, escriba el ID de PnP de Windows que desea usar.
O bien
- 5b** (Condicional) Junto al campo *Windows PNP ID* (ID de PnP de Windows), haga clic en *Select* (Seleccionar) para abrir una herramienta de asignación que presenta tres métodos para asignar el ID de PnP de Windows:
- ♦ En la pestaña *Driver File* (Archivo de controlador), busque y seleccione un archivo de controlador de Windows (es decir un archivo con la extensión *.inf), seleccione el ID de PnP que desee y haga clic en *Modify* (Modificar).



- ♦ En la pestaña *Driver Database* (Base de datos de controladores), busque y seleccione la base de datos de controladores actual, seleccione el ID de PnP correcto y seleccione *Modify* (Modificar).

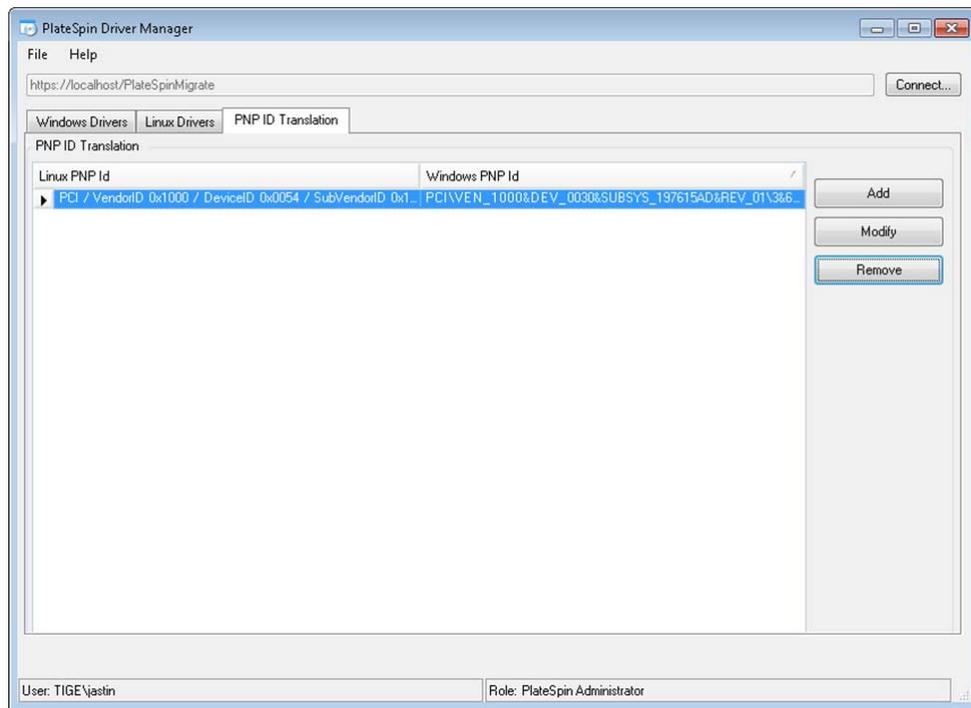


- ♦ En la pestaña *Select Machine* (Seleccionar equipo), haga clic en *Select Machine* (Seleccionar equipo) y en la lista de equipos Windows descubiertos con la función de descubrimiento activa, seleccione un equipo, haga clic en *OK* (Aceptar) para mostrar sus dispositivos, seleccione el ID de PnP que desee y haga clic en *Modify* (Modificar).



Importante: si selecciona un ID de PnP de Windows que no tenga un paquete de controlador asociado instalado, podría producirse un error durante la operación de failover/failback.

- 6 En el recuadro de diálogo *Create PnP ID Mapping* (Crear asignación de ID de PnP), confirme que se han seleccionado el ID de PnP de Linux y de Windows correctos y haga clic en *OK* (Aceptar) para abrir la página *PNP ID Translation* (Traducción de ID de PnP) de PlateSpin Driver Manager.



- 7 (Opcional) Para modificar o eliminar la asignación en la lista PNP ID Translation (Traducción de ID de PnP), seleccione el patrón de asignación y haga clic en *Remove* (Eliminar) o en *Modify* (Modificar), según la operación que desee llevar a cabo.

Remove (Eliminar) simplemente suprime la asignación (después de mostrar un recuadro de diálogo de confirmación).

Para modificar:

- 7a Haga clic en *Modify* (Modificar) para abrir el recuadro de diálogo Create PNP ID Mapping (Crear asignación de ID de PnP).
- 7b Repita el [Paso 5 en la página 98](#) para modificar el ID de PnP de Windows.

Nota: no es posible seleccionar ni modificar el ID de PnP de Linux.

7 Solución de problemas

En esta sección se incluye la información siguiente:

- ♦ Sección 7.1, “Solución de problemas con el inventario de cargas de trabajo (Windows)”, en la página 103
- ♦ Sección 7.2, “Solución de problemas con el inventario de cargas de trabajo (Linux)”, en la página 107
- ♦ Sección 7.3, “Solución de problemas durante el comando de preparación de réplica (Windows)”, en la página 108
- ♦ Sección 7.4, “Solución de problemas de réplica de la carga de trabajo”, en la página 109
- ♦ Sección 7.5, “Solución de problemas de reenvío de tráfico en las cargas de trabajo”, en la página 111
- ♦ Sección 7.6, “Solución de problemas con la ayuda en línea”, en la página 111
- ♦ Sección 7.7, “Generación y visualización de informes de diagnóstico”, en la página 111
- ♦ Sección 7.8, “Eliminación de cargas de trabajo”, en la página 112
- ♦ Sección 7.9, “Limpieza de la carga de trabajo después de la protección”, en la página 112
- ♦ Sección 7.10, “Compresión de las bases de datos de PlateSpin Protect”, en la página 115

7.1 Solución de problemas con el inventario de cargas de trabajo (Windows)

Podría ser necesario solucionar los siguientes problemas comunes durante el inventario de cargas de trabajo.

Problemas o mensajes	Solución
El dominio de las credenciales no es válido o está vacío.	<p>Este error se produce cuando el formato de las credenciales es incorrecto.</p> <p>Pruebe a realizar el descubrimiento con una cuenta de administrador local con el formato de credenciales <code>nombredehost\AdministradorLocal</code></p> <p>O bien, pruebe a realizar el descubrimiento con una cuenta de administrador de dominio con el formato de credenciales <code>dominio\AdministradorDeDominio</code></p>

Problemas o mensajes	Solución
No es posible conectar con el servidor Windows... Se deniega el acceso.	<p>No se ha usado una cuenta al intentar añadir una carga de trabajo. Use una cuenta de administrador o añada al usuario al grupo de administradores y vuelva a intentarlo.</p> <p>Este mensaje podría indicar también un error de conectividad WMI. Intente las distintas soluciones posibles siguientes y realice la "Prueba de conectividad de WMI" en la página 105 de nuevo. Si la prueba es correcta, pruebe a añadir de nuevo la carga de trabajo.</p> <ul style="list-style-type: none"> ◆ "Solución de problemas de la conectividad DCOM" en la página 105 ◆ "Solución de problemas de conectividad del servicio RPC" en la página 106
No es posible conectar con el servidor Windows... No se encuentra la vía de red.	<p>Error de conectividad de red. Realice las pruebas de "Realización de pruebas de conectividad" en la página 105. Si una prueba falla, asegúrese de que PlateSpin Protect y la carga de trabajo se encuentran en la misma red. Vuelva a configurar la red e inténtelo de nuevo.</p>
"Discover Server Details {hostname}" Failed Progress: 0% Status: NotStarted (Error en los detalles del servidor de descubrimiento {hostname}. Progreso: 0%. Estado: sin iniciar).	<p>Este error se puede producir por varias razones, y cada una de ellas tiene una solución distinta:</p> <ul style="list-style-type: none"> ◆ En entornos donde se use un servidor proxy local con autenticación, omita el servidor proxy o añada los permisos adecuados. Consulte el artículo 7920339 de la KB (https://www.netiq.com/support/kb/doc.php?id=7920339) para obtener más detalles. ◆ Si las directivas locales o de dominio restringen los permisos necesarios, siga los pasos descritos en el artículo 7920862 de la KB (https://www.netiq.com/support/kb/doc.php?id=7920862).
Se produce un error en el descubrimiento de la carga de trabajo con el mensaje: Could not find file output.xml (No se encuentra el archivo output.xml). O bien Network path not found (No se encuentra la vía de red) O (al intentar descubrir un clúster de Windows) Inventory failed to discover. Inventory result returned nothing. (Error de descubrimiento de inventario. No hay resultados para el inventario).	<p>Hay varias razones posibles para el error Could not find file output.xml:</p> <ul style="list-style-type: none"> ◆ El software antivirus del origen podría estar interfiriendo con el directorio. Inhabilite el software antivirus para determinar si es la causa del problema. Consulte "Inhabilitación del software antivirus" en la página 106. ◆ El uso compartido de archivos e impresoras para redes de Microsoft podría no estar habilitado. Habilítelo en las propiedades de la tarjeta de interfaz de red. ◆ Podría no ser posible acceder a los recursos compartidos Admin\$ del origen. Asegúrese de que PlateSpin Protect puede acceder a estos recursos compartidos. Consulte "Habilitación de permisos y acceso a archivos y recursos compartidos" en la página 106. ◆ El servicio de servidor o de estación de trabajo podría no estar en ejecución. Si fuera el caso, habilítelo y defina el modo de inicio automático. ◆ El servicio de registro remoto de Windows está inhabilitado. Inicie el servicio y defina el tipo de inicio automático.

En las siguientes secciones encontrará más información sobre cómo resolver problemas en cargas de trabajo Windows:

- ♦ [Sección 7.1.1, “Realización de pruebas de conectividad”, en la página 105](#)
- ♦ [Sección 7.1.2, “Inhabilitación del software antivirus”, en la página 106](#)
- ♦ [Sección 7.1.3, “Habilitación de permisos y acceso a archivos y recursos compartidos”, en la página 106](#)

7.1.1 Realización de pruebas de conectividad

- ♦ [“Prueba de conectividad de red” en la página 105](#)
- ♦ [“Prueba de conectividad de WMI” en la página 105](#)
- ♦ [“Solución de problemas de la conectividad DCOM” en la página 105](#)
- ♦ [“Solución de problemas de conectividad del servicio RPC” en la página 106](#)

Prueba de conectividad de red

Realice esta prueba de conectividad de red básica para determinar si PlateSpin Protect puede comunicarse con la carga de trabajo que intenta proteger.

- 1 Acceda al host del servidor de PlateSpin.
- 2 Abra un indicador de comandos y haga ping con la carga de trabajo:

```
ping IP_de_carga_de_trabajo
```

Prueba de conectividad de WMI

- 1 Acceda al host del servidor de PlateSpin.
- 2 Haga clic en *Inicio > Ejecutar*, escriba `wbemtest` y pulse *Intro*.
- 3 Haga clic en *Conectar*.
- 4 En el *espacio de nombre*, escriba el nombre de la carga de trabajo que intenta descubrir y añádale `\root\cimv2`. Por ejemplo, si el nombre de host es `win2k`, escriba:
`\\win2k\root\cimv2`
- 5 Introduzca las credenciales oportunas, ya sea con el formato `nombredelhost\AdministradorLocal` o `dominio\AdministradorDeDominio`.
- 6 Haga clic en *Conectar* para probar la conexión WMI.

Si aparece un mensaje de error, no es posible establecer una conexión WMI entre PlateSpin Protect y la carga de trabajo.

Solución de problemas de la conectividad DCOM

- 1 Entre en la carga de trabajo que desea proteger.
- 2 Haga clic en *Inicio > Ejecutar*.
- 3 Escriba `dcomcnfg` y pulse *Intro*.

4 Compruebe la conectividad:

- ♦ En sistemas Windows (XP/Vista/2003/2008/7), se abre la ventana Servicios de componentes. En la carpeta *Equipos* del árbol de la consola de la herramienta administrativa Servicios de componentes, haga clic con el botón derecho en el equipo cuya conectividad DCOM desee comprobar y haga clic en *Propiedades*. Haga clic en la pestaña *Propiedades predeterminada* y asegúrese de que *Habilitar COM distribuido en este equipo* está seleccionado.
- ♦ En un equipo Windows 2000 Server, se muestra el recuadro de diálogo Configuración DCOM. Haga clic en la pestaña *Propiedades predeterminada* y asegúrese de que *Habilitar COM distribuido en este equipo* está seleccionado.

5 Si DCOM no está habilitado, habilítelo y reanque el servidor o reinicie el servicio instrumental de administración de Windows (WMI). A continuación, pruebe a añadir de nuevo la carga de trabajo.

Solución de problemas de conectividad del servicio RPC

Hay tres bloqueos potenciales para el servicio RPC:

- ♦ El servicio de Windows
- ♦ Un cortafuegos de Windows
- ♦ Un cortafuegos de red

Para el servicio de Windows, asegúrese de que el servicio RPC se está ejecutando en la carga de trabajo. Para acceder al panel de servicios, ejecute `services.msc` desde un indicador de comandos. Para un cortafuegos de Windows, añada una excepción para RPC. Para los cortafuegos de hardware, puede probar las siguientes estrategias:

- ♦ Coloque PlateSpin Protect y la carga de trabajo en el mismo lado del cortafuegos
- ♦ Abra puertos específicos entre PlateSpin Protect y la carga de trabajo (consulte [“Requisitos de acceso y comunicación en la red de protección” en la página 25](#)).

7.1.2 Inhabilitación del software antivirus

En ocasiones, el software antivirus puede bloquear algunas de las funciones de PlateSpin Protect relacionadas con WMI y el registro remoto. Para garantizar que el inventario de cargas de trabajo se lleve a cabo correctamente, quizá sea necesario inhabilitar primero el servicio de antivirus en alguna carga de trabajo. Asimismo, el software antivirus podría bloquear a veces el acceso a algunos archivos, o permitir el acceso solo a algunos procesos o ejecutables. Esto podría obstruir la réplica de datos basada en archivos. En tal caso, cuando se configura la protección de la carga de trabajo, es posible seleccionar los servicios que se inhabilitarán, como aquellos instalados y usados por el software antivirus. Estos servicios solo se inhabilitan durante la transferencia de archivos y se reinician cuando el proceso se completa. Esta acción no es necesaria durante las réplicas de datos en el nivel de bloques.

7.1.3 Habilitación de permisos y acceso a archivos y recursos compartidos

Para proteger correctamente una carga de trabajo, PlateSpin Protect necesita distribuir e instalar correctamente software dentro de la carga de trabajo. Al distribuir estos componentes a una carga de trabajo, así como durante el proceso para añadir una carga de trabajo, PlateSpin Protect usa los

recursos compartidos administrativos de la carga de trabajo. Para realizar esta tarea, PlateSpin Protect necesita acceso administrativo a los recursos compartidos, ya sea con la cuenta del administrador local o con una cuenta de administración de dominio.

Para garantizar que los recursos compartidos administrativos están habilitados:

- 1 Haga clic con el botón derecho en *Mi PC* en el escritorio y seleccione *Administrar*.
- 2 Expanda *Herramientas del sistema > Carpetas compartidas > Recursos compartidos*.
- 3 En el directorio *Carpetas compartidas*, debe ser una entrada *Admin\$*, junto a otros recursos compartidos.

Tras confirmar que los recursos compartidos están habilitados, asegúrese de que se puede acceder a ellos desde el host del servidor de PlateSpin:

- 1 Acceda al host del servidor de PlateSpin.
- 2 Haga clic en *Inicio > ejecutar*, escriba `\\<host_servidor>\Admin$` y haga clic en *Aceptar*.
- 3 Si se le solicita, use las mismas credenciales que usó para añadir la carga de trabajo en el inventario de carga de trabajo de PlateSpin Protect.
El directorio se abre y debería poder examinar y modificar su contenido.
- 4 Repita el proceso para todos los recursos compartidos con la excepción de *IPC\$*.

Windows usa el recurso compartido *IPC\$* para la validación de credenciales y la autenticación. No está asignado a una carpeta ni archivo en la carga de trabajo, por lo que la prueba siempre falla. Sin embargo, el recurso compartido seguirá siendo visible.

PlateSpin Protect no modifica el contenido actual del volumen; sin embargo, crea su propio directorio, para el que necesita acceso y permisos.

7.2 Solución de problemas con el inventario de cargas de trabajo (Linux)

Problemas o mensajes	Solución
No es posible conectar ni con el servidor SSH que se ejecuta en <dirección_IP> ni con los servicios Web de la infraestructura virtual de VMware en <dirección_IP>/sdk	<p>Este mensaje se puede deber a diversos motivos:</p> <ul style="list-style-type: none">◆ No es posible acceder a la carga de trabajo.◆ SSH no se está ejecutando en la carga de trabajo.◆ El cortafuegos está activado y los puertos necesarios no se han abierto.◆ No se admite el sistema operativo específico de la carga de trabajo. <p>Para los requisitos de red y acceso de una carga de trabajo, consulte "Requisitos de acceso y comunicación en la red de protección" en la página 25.</p>

Problemas o mensajes	Solución
Acceso denegado	Este problema de autenticación indica un nombre de usuario o una contraseña no válidos. Para obtener información sobre las credenciales de acceso de la carga de trabajo adecuados, consulte “Directrices para las credenciales de carga de trabajo y contenedor” en la página 68.

7.3 Solución de problemas durante el comando de preparación de réplica (Windows)

Problemas o mensajes	Solución
Error de autenticación al verificar la conexión del controlador al configurar el controlador en el origen.	Esta directiva debe permitir la cuenta usada para añadir una carga de trabajo. Consulte “Directiva de grupo y derechos de usuario” en la página 108.
Error al determinar si .NET Framework está instalado (con la excepción Falló la relación de confianza entre esta estación de trabajo y el dominio primario.).	Compruebe si el servicio de registro remoto del origen está habilitado e iniciado. Consulte también “Solución de problemas con el inventario de cargas de trabajo (Windows)” en la página 103.

7.3.1 Directiva de grupo y derechos de usuario

Debido a la forma en la que PlateSpin Protect interactúa con el sistema operativo de la carga de trabajo de origen, es necesario que la cuenta del administrador que se usa para añadir una carga de trabajo tenga derechos de usuario determinados en el equipo de origen. En la mayoría de los casos, estos valores son los usados por defecto en la directiva de grupo; sin embargo, si el entorno se ha bloqueado, puede que se hayan eliminado las siguientes asignaciones de derechos de usuario:

- ♦ Desviar comprobación de recorrido
- ♦ Reemplazar un testigo de nivel de proceso
- ♦ Actuar como parte del sistema operativo

A fin de verificar que se han definido estos valores de la directiva de grupo, puede ejecutar `gpresult /v` en la línea de comandos del equipo de origen, o bien `RSOP.msc`. Si la directiva no se ha definido, o si se ha inhabilitado, se puede habilitar mediante la directiva de seguridad local del equipo o mediante cualquier directiva de grupo de dominio que se aplique al equipo.

Puede activar la directiva de inmediato mediante el comando `gpupdate /force` (en Windows 2003/XP) o mediante `secedit /refreshpolycymachine_policy /enforce` (en Windows 2000).

7.4 Solución de problemas de réplica de la carga de trabajo

Problemas o mensajes	Solución
Error recuperable durante la réplica al <i>programar la toma de una instantánea del equipo virtual</i> o al <i>programar la reversión de la máquina virtual a una instantánea antes del inicio</i> .	Este problema se produce cuando el servidor se está cargando y el proceso tarda más de lo esperado. Espere a que se complete la réplica.
Problema de la carga de trabajo que requiere la intervención del usuario	Este mensaje puede estar provocado por distintos motivos. En la mayoría de los casos, el mensaje incluirá más detalles sobre la naturaleza y el área del problema (como la conectividad o las credenciales). Después de solucionar el problema, espere unos minutos. Si el mensaje persiste, póngase en contacto con el servicio técnico de PlateSpin.
Todas las cargas de trabajo sufren un error recuperable porque no tiene espacio suficiente en el disco.	Verifique el espacio libre. Si se necesita más espacio, elimine una carga de trabajo.
Velocidad de red lenta, por debajo de 1 MB.	Confirme que la configuración dúplex de la tarjeta de interfaz de red del equipo de origen está activada y que la configuración del conmutador conectado coincide. Es decir, si el conmutador está definido en automático, el origen no se puede definir con 100 MB.
Velocidad de red lenta, por encima de 1 MB.	Mida la latencia ejecutando el comando siguiente en la carga de trabajo de origen: <code>ping ip-t</code> (sustituya <i>ip</i> con la dirección IP del host del servidor de PlateSpin). Deje que se ejecuten 50 interacciones. La media indica la latencia. Consulte también “Optimización de transferencia de datos en conexiones WAN” en la página 34 .
No es posible iniciar la transferencia de archivos. El puerto 3725 ya está en uso. O bien	Asegúrese de que el puerto está abierto y a la escucha: Ejecute <code>netstat -ano</code> en la carga de trabajo. Compruebe el cortafuegos.
No es posible conectar con el puerto 3725.	Vuelva a intentar la réplica.

Problemas o mensajes	Solución
<p>Conexión del controlador no establecida.</p> <p>Error de réplica en el paso <i>Toma de control de la máquina virtual</i>.</p>	<p>Este error se produce si la información de conectividad de la réplica no es válida. El servidor DHCP no está disponible o la red virtual de réplica no se puede enrutar al host del servidor de PlateSpin.</p> <p>Cambie la IP de réplica a una IP estática y habilite el servidor DHCP.</p> <p>Asegúrese de que la red virtual seleccionada para la réplica se puede enrutar al host del servidor de PlateSpin.</p>
<p>El trabajo de réplica no se inicia (se bloquea al 0 %)</p>	<p>Este error se puede producir por varias razones, y cada una de ellas tiene una solución distinta:</p> <ul style="list-style-type: none"> ◆ En entornos donde se use un servidor proxy local con autenticación, omita el servidor proxy o añada los permisos adecuados para resolver el problema. Consulte el artículo 20339 de la KB (https://www.netiq.com/support/kb/doc.php?id=7920339) para obtener más detalles. ◆ Si las directivas locales o de dominio restringen los permisos necesarios, siga los pasos descritos en el artículo 7920862 de la KB (https://www.netiq.com/support/kb/doc.php?id=7920862). <p>Este problema es habitual si el host del servidor de PlateSpin está afiliado con un dominio y las directivas de dominios se aplican con restricciones. Consulte "Directiva de grupo y derechos de usuario" en la página 108.</p>
<p>Tras una actualización de Windows, algunos archivos de la carpeta C:\Windows\SoftwareDistribution no se transfieren al equipo de destino durante la réplica incremental basada en archivos.</p>	<p>Esta es una situación habitual en Microsoft Windows: con fines de optimización, algunos archivos se marcan para ser suprimidos en la clave de registro HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot, para evitar que se incluyan en las instantáneas VSS. Consulte el artículo de la red de desarrolladores de Microsoft sobre exclusión de archivos de las instantáneas para obtener más información.</p> <p>Normalmente, estos archivos se emplean para instalar las actualizaciones de Windows y luego se suprimen, pues dejan de ser necesarios después de la actualización. Si decide restaurar estos archivos, ejecute Windows Update en el equipo de destino después del failover para restablecer la carpeta SoftwareDistribution.</p>

7.5 Solución de problemas de reenvío de tráfico en las cargas de trabajo

En algunas situaciones, la réplica de una carga de trabajo que reenvía tráfico de red (por ejemplo, si la finalidad de la carga de trabajo es hacer de puente de red NAT, VPN o cortafuegos) puede mostrar una degradación significativa del rendimiento de la red. Esto está relacionado con un problema con los adaptadores VMXNET 2 y VMXNET 3 que tienen habilitada la funcionalidad LRO (Large Receive Offload, recepción de grandes cargas).

Para solucionar este problema, deberá inhabilitar LRO en el adaptador de red virtual. Para obtener más información, consulte el [artículo 7005495 de la KB](#).

7.6 Solución de problemas con la ayuda en línea

en algunos sistemas con configuración de seguridad del navegador mejorada (como Internet Explorer 8 en Windows Server 2008), los iconos Expandir y Comprimir (+ y -) del índice podrían no funcionar. Para solucionar el problema, habilite JavaScript en el navegador:

- ♦ **Internet Explorer:** haga clic en *Herramientas > Opciones de seguridad > pestaña Seguridad > zona Internet > Nivel personalizado* y seleccione la opción *Habilitar para Active Scripting*.
- ♦ **Firefox:** Haga clic en *Herramientas > Opciones > Contenido* y seleccione la opción *Habilitar JavaScript*.

7.7 Generación y visualización de informes de diagnóstico

En la interfaz Web de PlateSpin Protect, después de ejecutar un comando, puede generar informes detallados de diagnóstico sobre los detalles del comando.

- 1 Haga clic en *Command Details* (Detalles del comando) y en el enlace *Generate Diagnostics* (Generar diagnóstico).

The screenshot displays the 'Command Details' page for a replication task. The main heading is 'Running First Replication'. The status is 'Running' with a progress bar at 80%. The duration is 14h 49m 6s. The step is 'Copy data (80%)'. The command is 'Scheduling Target Machine for Preparing to Configure Operating System (15%)'. The page includes a 'Command Summary' table, a 'Replication Transfer Summary' table, and a 'Workload Commands' section. A red box highlights the 'Generate Diagnostics' link in the 'Diagnostics' column of the 'Steps' table.

Step	Status	Start Time	End Time	Duration	Diagnostics
Copy data	Running (80%)	3/31/2010 8:24 PM	--	14h 48m 53s	--

Replication Transfer Summary	
Average Transfer Speed:	298.80 Mbps
Total Data Transferred:	3.7 GB
Duration:	1m 42s

Tras un tiempo, la página se actualiza y muestra el enlace *View* (Ver) encima del enlace *Generated Diagnostics* (Generar diagnóstico).

- 2 Haga clic en *View* (Ver).
Se abre una página nueva con información de diagnóstico completa sobre el comando actual.
- 3 Guarde la página de diagnóstico y téngala lista por si necesita ponerse en contacto con el servicio de asistencia técnica.

7.8 Eliminación de cargas de trabajo

En algunas circunstancias, puede ser necesario eliminar una carga de trabajo del inventario de PlateSpin Protect y volver a añadirla más tarde.

- 1 En la página Workloads (Cargas de trabajo), seleccione la carga de trabajo que desea eliminar y haga clic en *Remove Workload* (Eliminar carga de trabajo).
(Condicional) Para las cargas de trabajo Windows protegidas anteriormente mediante la réplica de nivel de bloques, la interfaz Web de PlateSpin Protect pide que se indique si también se desean eliminar los componentes basados en bloques. Puede seleccionar lo siguiente:
 - ♦ **No eliminar los componentes:** los componentes no se eliminarán.
 - ♦ **Eliminar componentes, pero no reiniciar la carga de trabajo:** los componentes se eliminarán. Sin embargo, será preciso rearrancar la carga de trabajo para completar el proceso de desinstalación.
 - ♦ **Eliminar componentes y reiniciar la carga de trabajo:** los componentes se eliminarán y la carga de trabajo se rearrancará automáticamente. Asegúrese de llevar a cabo esta operación durante el tiempo de inactividad programado.
- 2 En la página de confirmación del comando, haga clic en *Confirm* (Confirmar) para ejecutar el comando.
Espere a que se complete el proceso.

7.9 Limpieza de la carga de trabajo después de la protección

Use estos pasos para limpiar todos los componentes de software de PlateSpin de la carga de trabajo de origen cuando se necesite, por ejemplo, cuando la protección tiene problemas o no se efectúa correctamente.

Las secciones siguientes contienen más información:

- ♦ [Sección 7.9.1, “Limpieza de las cargas de trabajo Windows”, en la página 112](#)
- ♦ [Sección 7.9.2, “Limpieza de las cargas de trabajo Linux”, en la página 113](#)

7.9.1 Limpieza de las cargas de trabajo Windows

Componente	Instrucciones de eliminación
Componente de transferencia basada en bloques de PlateSpin	Consulte el artículo 7005616 de la KB (https://www.netiq.com/support/kb/doc.php?id=7005616) .

Componente	Instrucciones de eliminación
Componente de transferencia basada en bloques de otros fabricantes (discontinuado)	<ol style="list-style-type: none"> Use el applet Agregar o quitar programas (ejecute <code>appwiz.cpl</code>) y elimine el componente. Según el origen, puede que tenga una de estas versiones: <ul style="list-style-type: none"> Réplica de datos SteelEye para Windows versión 6 actualización 2 SteelEye DataKeeper para Windows versión 7 Rearranque el equipo.
Componente de transferencia basada en archivos	En el nivel raíz de cada volumen protegido, elimine todos los archivos con el nombre <code>PlateSpinCatalog*.dat</code> .
Software de inventario de carga de trabajo	<p>En el directorio <code>Windows</code> de la carga de trabajo:</p> <ul style="list-style-type: none"> Elimine todos los archivos con el nombre <code>machinediscovery*</code>. Elimine el subdirectorio denominado <code>platespin</code>.
Software de controlador	<ol style="list-style-type: none"> Abra un indicador de comandos y cambie el directorio actual a: <ul style="list-style-type: none"> <code>\Archivos de programa\platespin*</code> (sistemas de 32 bits) <code>\Archivos de programa (x86)\platespin*</code> (sistemas de 64 bits) Ejecute el comando siguiente: <code>ofxcontroller.exe /uninstall</code> Elimine el directorio <code>platespin*</code>.

7.9.2 Limpieza de las cargas de trabajo Linux

Componente	Instrucciones de eliminación
Software de controlador	<ul style="list-style-type: none"> Elimine estos procesos: <ul style="list-style-type: none"> <code>pkill -9 ofxcontrollerd</code> <code>pkill -9 ofxjobexec</code> Elimine el paquete RPM del controlador OFX: <code>rpm -e ofxcontrollerd</code> En el sistema de archivos de la carga de trabajo, elimine el directorio <code>/usr/lib/ofx</code> con su contenido.

Componente	Instrucciones de eliminación
Software de transferencia de datos en el nivel de bloques	<ol style="list-style-type: none"> 1. Compruebe si el controlador está activo: <pre>lsmod grep blkwatch</pre> <p>Si el controlador sigue cargado en la memoria, el resultado debe contener una línea similar a la siguiente:</p> <pre>blkwatch_7616 70924 0</pre> 2. (Condicional) Si el controlador sigue cargado, elimínelo de la memoria: <pre>rmmmod blkwatch_7616</pre> 3. Elimine el controlador de la secuencia de arranque: <pre>blkconfig -u</pre> 4. Elimine los archivos del controlador suprimiendo el directorio siguiente con su contenido: <pre>/lib/modules/[Versión_Núcleo]/Platespin</pre> 5. Suprima el archivo siguiente: <pre>/etc/blkwatch.conf</pre>
Instantáneas LVM	<p>Las instantáneas LVM usadas en las réplicas continuas recibe un nombre según la convención <i>nombre_del_volumen-PS-snapshot</i>. Por ejemplo, una instantánea del volumen LogVol01 se llamará LogVol01-PS-snapshot.</p> <p>Para eliminar estas instantáneas LVM:</p> <ol style="list-style-type: none"> 1. Genere una lista de instantáneas de la carga de trabajo requerida de una de estas formas: <ul style="list-style-type: none"> ♦ Use la interfaz Web de PlateSpin Protect para generar un informe de tarea para la tarea con errores. El informe debe contener información sobre las instantáneas LVM y sus nombres. - O bien - ♦ En la carga de trabajo Linux requerida, ejecute el comando siguiente para mostrar una lista de todos los volúmenes e instantáneas: <pre># lvsdisplay -a</pre> 2. Anote los nombres y ubicaciones de las instantáneas que desea eliminar. 3. Elimine las instantáneas mediante el comando siguiente: <pre>lvremove nombre_de_instantánea</pre>
Archivos de mapas de bits (bitmap)	<p>Para cada volumen protegido, elimine el archivo <code>.blocks_bitmap</code> correspondiente de la raíz del volumen.</p>
Herramientas	<p>En la carga de trabajo de origen, en <code>/sbin</code>, elimine los siguientes archivos:</p> <ul style="list-style-type: none"> ♦ <code>bmaputil</code> ♦ <code>blkconfig</code>

7.10 Compresión de las bases de datos de PlateSpin Protect

Cuando las bases de datos de PlateSpin Protect (OFX, PortabilitySuite y Protection) alcanzan una capacidad predeterminada, se produce una limpieza periódica de dichas bases. Si precisa regular aún más el tamaño o el contenido de estas bases de datos, Protect proporciona una utilidad (PlateSpin.DBCleanup.exe) para limpiarlas en más profundidad o comprimirlas. En el [artículo 7006458 de la KB \(https://www.netiq.com/support/kb/doc.php?id=7006458\)](https://www.netiq.com/support/kb/doc.php?id=7006458) se explica dónde se encuentra la herramienta y las opciones disponibles, en caso de que decida usarla para operaciones de base de datos sin conexión.

A Distribuciones de Linux compatibles con Protect

El software de PlateSpin ForgeProtect incluye versiones compiladas previamente del controlador `blkwatch` para muchas distribuciones de Linux que no son de depuración (32 bits y 64 bits). En esta sección se incluye la información siguiente:

- ♦ [Sección A.1, “Análisis de la carga de trabajo Linux”, en la página 117](#)
- ♦ [Sección A.2, “Controlador “blkwatch” compilado previamente para Protect \(Linux\)”, en la página 118](#)

A.1 Análisis de la carga de trabajo Linux

Antes de determinar si PlateSpin Protect cuenta con un controlador `blkwatch` para esa distribución, debe obtener más información sobre el núcleo de la carga de trabajo Linux a fin de que pueda usarlo como término de búsqueda en la lista de distribuciones compatibles. En esta sección se incluye la información siguiente:

- ♦ [Sección A.1.1, “Determinación de la cadena de versión”, en la página 117](#)
- ♦ [Sección A.1.2, “Determinación de la arquitectura”, en la página 118](#)

A.1.1 Determinación de la cadena de versión

Puede determinar la cadena de versión del núcleo de la carga de trabajo Linux ejecutando el comando siguiente en el terminal de Linux de la carga de trabajo:

```
uname -r
```

Por ejemplo, si ejecuta `uname -r`, podría producirse el siguiente resultado:

```
3.0.76-0.11-default
```

Si busca en la lista de distribuciones, observará que hay dos entradas que coinciden con esta cadena:

- ♦ `SLES11SP3-GA-3.0.76-0.11-default-x86`
- ♦ `SLES11SP3-GA-3.0.76-0.11-default-x86_64`

El resultado de la búsqueda indica que el producto tiene controladores para las arquitecturas de 32 bits (`x86`) y de 64 bits (`x86_64`).

A.1.2 Determinación de la arquitectura

Puede determinar la arquitectura de la carga de trabajo Linux ejecutando el comando siguiente en el terminal de Linux de la carga de trabajo:

```
uname -m
```

Por ejemplo, si ejecuta `uname -m`, podría producirse el siguiente resultado:

```
x86_64
```

Con esta información es posible determinar si la carga de trabajo tienen una arquitectura de 64 bits.

A.2 Controlador “blkwatch” compilado previamente para Protect (Linux)

A continuación se muestra una lista de las distribuciones de Linux que no son de depuración para las que Protect cuenta con un controlador `blkwatch`. Puede buscar en la lista para determinar si la cadena de versión y la arquitectura del núcleo de la carga de trabajo Linux coinciden con una distribución compatible de la lista. Si encuentra la cadena de versión y la arquitectura, PlateSpin Protect tiene una versión precompilada del controlador `blkwatch`.

Si la búsqueda no da resultados, puede crear un controlador `blkwatch` personalizado. Para ello, siga los pasos descritos en el artículo [7005873 de la KB](#).

Sintaxis de los elementos de la lista

Los elementos de la lista tienen un formato con la siguiente sintaxis:

```
<Distribución>-<Parche>-<Cadena_versión_núcleo>-<Arquitectura_núcleo>
```

Por ejemplo, para una distribución de SLES 9 SP1 con la cadena de versión del núcleo 2.6.5-7.139-bigsmpt en la arquitectura de 32 bits (x86), el elemento aparece en la lista con este formato:

```
SLES9-SP1-2.6.5-7.139-bigsmpt-x86
```

Lista de distribuciones

```
RHEL4-GA-2.6.9-5.EL-x86  
RHEL4-GA-2.6.9-5.EL-x86_64  
RHEL4-GA-2.6.9-5.ELhugemem-x86  
RHEL4-GA-2.6.9-5.ELsmp-x86  
RHEL4-GA-2.6.9-5.ELsmp-x86_64  
RHEL4-U1-2.6.9-11.EL-x86  
RHEL4-U1-2.6.9-11.EL-x86_64  
RHEL4-U1-2.6.9-11.ELhugemem-x86  
RHEL4-U1-2.6.9-11.ELsmp-x86  
RHEL4-U1-2.6.9-11.ELsmp-x86_64  
RHEL4-U2-2.6.9-22.EL-x86  
RHEL4-U2-2.6.9-22.EL-x86_64  
RHEL4-U2-2.6.9-22.ELhugemem-x86  
RHEL4-U2-2.6.9-22.ELsmp-x86
```

RHEL4-U2-2.6.9-22.ELsmp-x86_64
RHEL4-U3-2.6.9-34.EL-x86
RHEL4-U3-2.6.9-34.EL-x86_64
RHEL4-U3-2.6.9-34.ELhugemem-x86
RHEL4-U3-2.6.9-34.ELlargesmp-x86_64
RHEL4-U3-2.6.9-34.ELsmp-x86
RHEL4-U3-2.6.9-34.ELsmp-x86_64
RHEL4-U4-2.6.9-42.EL-x86
RHEL4-U4-2.6.9-42.EL-x86_64
RHEL4-U4-2.6.9-42.ELhugemem-x86
RHEL4-U4-2.6.9-42.ELlargesmp-x86_64
RHEL4-U4-2.6.9-42.ELsmp-x86
RHEL4-U4-2.6.9-42.ELsmp-x86_64
RHEL4-U5-2.6.9-55.EL-x86
RHEL4-U5-2.6.9-55.EL-x86_64
RHEL4-U5-2.6.9-55.ELhugemem-x86
RHEL4-U5-2.6.9-55.ELlargesmp-x86_64
RHEL4-U5-2.6.9-55.ELsmp-x86
RHEL4-U5-2.6.9-55.ELsmp-x86_64
RHEL4-U6-2.6.9-67.EL-x86
RHEL4-U6-2.6.9-67.EL-x86_64
RHEL4-U6-2.6.9-67.ELhugemem-x86
RHEL4-U6-2.6.9-67.ELlargesmp-x86_64
RHEL4-U6-2.6.9-67.ELsmp-x86
RHEL4-U6-2.6.9-67.ELsmp-x86_64
RHEL4-U7-2.6.9-78.EL-x86
RHEL4-U7-2.6.9-78.EL-x86_64
RHEL4-U7-2.6.9-78.ELhugemem-x86
RHEL4-U7-2.6.9-78.ELlargesmp-x86_64
RHEL4-U7-2.6.9-78.ELsmp-x86
RHEL4-U7-2.6.9-78.ELsmp-x86_64
RHEL4-U8-2.6.9-89.EL-x86
RHEL4-U8-2.6.9-89.EL-x86_64
RHEL4-U8-2.6.9-89.ELhugemem-x86
RHEL4-U8-2.6.9-89.ELlargesmp-x86_64
RHEL4-U8-2.6.9-89.ELsmp-x86
RHEL4-U8-2.6.9-89.ELsmp-x86_64
RHEL4-U9-2.6.9-100.EL-x86
RHEL4-U9-2.6.9-100.EL-x86_64
RHEL4-U9-2.6.9-100.ELhugemem-x86
RHEL4-U9-2.6.9-100.ELlargesmp-x86_64
RHEL4-U9-2.6.9-100.ELsmp-x86
RHEL4-U9-2.6.9-100.ELsmp-x86_64
RHEL5-GA-2.6.18-8.e15-x86
RHEL5-GA-2.6.18-8.e15-x86_64
RHEL5-GA-2.6.18-8.e15PAE-x86
RHEL5-U1-2.6.18-53.e15-x86

RHEL5-U1-2.6.18-53.el5-x86_64
RHEL5-U1-2.6.18-53.el5PAE-x86
RHEL5-U10-2.6.18-371.el5-x86
RHEL5-U10-2.6.18-371.el5-x86_64
RHEL5-U10-2.6.18-371.el5PAE-x86
RHEL5-U2-2.6.18-92.el5-x86
RHEL5-U2-2.6.18-92.el5-x86_64
RHEL5-U2-2.6.18-92.el5PAE-x86
RHEL5-U3-2.6.18-128.el5-x86
RHEL5-U3-2.6.18-128.el5-x86_64
RHEL5-U3-2.6.18-128.el5PAE-x86
RHEL5-U4-2.6.18-164.el5-x86
RHEL5-U4-2.6.18-164.el5-x86_64
RHEL5-U4-2.6.18-164.el5PAE-x86
RHEL5-U5-2.6.18-194.el5-x86
RHEL5-U5-2.6.18-194.el5-x86_64
RHEL5-U5-2.6.18-194.el5PAE-x86
RHEL5-U6-2.6.18-238.el5-x86
RHEL5-U6-2.6.18-238.el5-x86_64
RHEL5-U6-2.6.18-238.el5PAE-x86
RHEL5-U7-2.6.18-274.el5-x86
RHEL5-U7-2.6.18-274.el5-x86_64
RHEL5-U7-2.6.18-274.el5PAE-x86
RHEL5-U8-2.6.18-308.el5-x86
RHEL5-U8-2.6.18-308.el5-x86_64
RHEL5-U8-2.6.18-308.el5PAE-x86
RHEL5-U9-2.6.18-348.el5-x86
RHEL5-U9-2.6.18-348.el5-x86_64
RHEL5-U9-2.6.18-348.el5PAE-x86
RHEL6-GA-2.6.32-71.el6.i686-x86
RHEL6-GA-2.6.32-71.el6.x86_64-x86_64
RHEL6-U1-2.6.32-131.0.15.el6.i686-x86
RHEL6-U1-2.6.32-131.0.15.el6.x86_64-x86_64
RHEL6-U2-2.6.32-220.el6.i686-x86
RHEL6-U2-2.6.32-220.el6.x86_64-x86_64
RHEL6-U3-2.6.32-279.el6.i686-x86
RHEL6-U3-2.6.32-279.el6.x86_64-x86_64
RHEL6-U4-2.6.32-358.el6.i686-x86
RHEL6-U4-2.6.32-358.el6.x86_64-x86_64
RHEL6-U5-2.6.32-431.el6.i686-x86
RHEL6-U5-2.6.32-431.el6.x86_64-x86_64
SLES10-GA-2.6.16.21-0.8-bigsmpt-x86
SLES10-GA-2.6.16.21-0.8-default-x86
SLES10-GA-2.6.16.21-0.8-default-x86_64
SLES10-GA-2.6.16.21-0.8-smp-x86
SLES10-GA-2.6.16.21-0.8-smp-x86_64
SLES10-GA-2.6.16.21-0.8-xen-x86

SLES10-GA-2.6.16.21-0.8-xen-x86_64
SLES10-GA-2.6.16.21-0.8-xenpae-x86
SLES10-SP1-2.6.16.46-0.12-bigsmp-x86
SLES10-SP1-2.6.16.46-0.12-default-x86
SLES10-SP1-2.6.16.46-0.12-default-x86_64
SLES10-SP1-2.6.16.46-0.12-smp-x86
SLES10-SP1-2.6.16.46-0.12-smp-x86_64
SLES10-SP1-2.6.16.46-0.12-xen-x86
SLES10-SP1-2.6.16.46-0.12-xen-x86_64
SLES10-SP1-2.6.16.46-0.12-xenpae-x86
SLES10-SP2-2.6.16.60-0.21-bigsmp-x86
SLES10-SP2-2.6.16.60-0.21-default-x86
SLES10-SP2-2.6.16.60-0.21-default-x86_64
SLES10-SP2-2.6.16.60-0.21-smp-x86
SLES10-SP2-2.6.16.60-0.21-smp-x86_64
SLES10-SP2-2.6.16.60-0.21-xen-x86
SLES10-SP2-2.6.16.60-0.21-xen-x86_64
SLES10-SP2-2.6.16.60-0.21-xenpae-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-bigsmp-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-default-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-default-x86_64
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-smp-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-smp-x86_64
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-xen-x86
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-xen-x86_64
SLES10-SP2_LTSS_U2-2.6.16.60-0.42.54.1-xenpae-x86
SLES10-SP3-2.6.16.60-0.54.5-bigsmp-x86
SLES10-SP3-2.6.16.60-0.54.5-default-x86
SLES10-SP3-2.6.16.60-0.54.5-default-x86_64
SLES10-SP3-2.6.16.60-0.54.5-smp-x86
SLES10-SP3-2.6.16.60-0.54.5-smp-x86_64
SLES10-SP3-2.6.16.60-0.54.5-xen-x86
SLES10-SP3-2.6.16.60-0.54.5-xen-x86_64
SLES10-SP3-2.6.16.60-0.54.5-xenpae-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-bigsmp-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-default-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-default-x86_64
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-smp-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-smp-x86_64
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-xen-x86
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-xen-x86_64
SLES10-SP3_LTSS_U1-2.6.16.60-0.113.1-xenpae-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-bigsmp-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-default-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-default-x86_64
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-smp-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-smp-x86_64

SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-xen-x86
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-xen-x86_64
SLES10-SP3_LTSS_U2-2.6.16.60-0.123.1-xenpae-x86
SLES10-SP4-2.6.16.60-0.85.1-bigsmp-x86
SLES10-SP4-2.6.16.60-0.85.1-default-x86
SLES10-SP4-2.6.16.60-0.85.1-default-x86_64
SLES10-SP4-2.6.16.60-0.85.1-smp-x86
SLES10-SP4-2.6.16.60-0.85.1-smp-x86_64
SLES10-SP4-2.6.16.60-0.85.1-xen-x86
SLES10-SP4-2.6.16.60-0.85.1-xen-x86_64
SLES10-SP4-2.6.16.60-0.85.1-xenpae-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-bigsmp-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-default-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-default-x86_64
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-smp-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-smp-x86_64
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-xen-x86
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-xen-x86_64
SLES10-SP4_LTSS_U1-2.6.16.60-0.105.1-xenpae-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-bigsmp-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-default-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-default-x86_64
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-smp-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-smp-x86_64
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-xen-x86
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-xen-x86_64
SLES10-SP4_LTSS_U2-2.6.16.60-0.107.1-xenpae-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-bigsmp-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-default-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-default-x86_64
SLES10-SP4_U4-2.6.16.60-0.93.1-smp-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-smp-x86_64
SLES10-SP4_U4-2.6.16.60-0.93.1-xen-x86
SLES10-SP4_U4-2.6.16.60-0.93.1-xen-x86_64
SLES10-SP4_U4-2.6.16.60-0.93.1-xenpae-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-bigsmp-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-default-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-default-x86_64
SLES10-SP4_U5-2.6.16.60-0.97.1-smp-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-smp-x86_64
SLES10-SP4_U5-2.6.16.60-0.97.1-xen-x86
SLES10-SP4_U5-2.6.16.60-0.97.1-xen-x86_64
SLES10-SP4_U5-2.6.16.60-0.97.1-xenpae-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-bigsmp-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-default-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-default-x86_64
SLES10-SP4_U6-2.6.16.60-0.99.1-smp-x86

SLES10-SP4_U6-2.6.16.60-0.99.1-smp-x86_64
SLES10-SP4_U6-2.6.16.60-0.99.1-xen-x86
SLES10-SP4_U6-2.6.16.60-0.99.1-xen-x86_64
SLES10-SP4_U6-2.6.16.60-0.99.1-xenpae-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-bigsmp-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-default-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-default-x86_64
SLES10-SP4_U7-2.6.16.60-0.101.1-smp-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-smp-x86_64
SLES10-SP4_U7-2.6.16.60-0.101.1-xen-x86
SLES10-SP4_U7-2.6.16.60-0.101.1-xen-x86_64
SLES10-SP4_U7-2.6.16.60-0.101.1-xenpae-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-bigsmp-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-default-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-default-x86_64
SLES10-SP4_U8-2.6.16.60-0.103.1-smp-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-smp-x86_64
SLES10-SP4_U8-2.6.16.60-0.103.1-xen-x86
SLES10-SP4_U8-2.6.16.60-0.103.1-xen-x86_64
SLES10-SP4_U8-2.6.16.60-0.103.1-xenpae-x86
SLES11-GA-2.6.27.19-5-default-x86
SLES11-GA-2.6.27.19-5-default-x86_64
SLES11-GA-2.6.27.19-5-pae-x86
SLES11-SP1-2.6.32.12-0.6-default-x86
SLES11-SP1-2.6.32.12-0.6-default-x86_64
SLES11-SP1-2.6.32.12-0.6-pae-x86
SLES11-SP1_LTSS_U1-2.6.32.59-0.9-default-x86
SLES11-SP1_LTSS_U1-2.6.32.59-0.9-default-x86_64
SLES11-SP1_LTSS_U1-2.6.32.59-0.9-pae-x86
SLES11-SP1_LTSS_U2-2.6.32.59-0.13-default-x86
SLES11-SP1_LTSS_U2-2.6.32.59-0.13-default-x86_64
SLES11-SP1_LTSS_U2-2.6.32.59-0.13-pae-x86
SLES11-SP1_U14-2.6.32.54-0.3-default-x86
SLES11-SP1_U14-2.6.32.54-0.3-default-x86_64
SLES11-SP1_U14-2.6.32.54-0.3-pae-x86
SLES11-SP1_U15-2.6.32.59-0.3-default-x86
SLES11-SP1_U15-2.6.32.59-0.3-default-x86_64
SLES11-SP1_U15-2.6.32.59-0.3-pae-x86
SLES11-SP1_U16-2.6.32.59-0.7-default-x86
SLES11-SP1_U16-2.6.32.59-0.7-default-x86_64
SLES11-SP1_U16-2.6.32.59-0.7-pae-x86
SLES11SP2-GA-3.0.13-0.27-default-x86
SLES11SP2-GA-3.0.13-0.27-default-x86_64
SLES11SP2-GA-3.0.13-0.27-pae-x86
SLES11SP2-GA-3.0.13-0.27-xen-x86
SLES11SP2-GA-3.0.13-0.27-xen-x86_64
SLES11SP2-LTSS_U1-3.0.101-0.7.19-default-x86

SLES11SP2-LTSS_U1-3.0.101-0.7.19-default-x86_64
SLES11SP2-LTSS_U1-3.0.101-0.7.19-pae-x86
SLES11SP2-LTSS_U1-3.0.101-0.7.19-xen-x86
SLES11SP2-LTSS_U1-3.0.101-0.7.19-xen-x86_64
SLES11SP2-LTSS_U2-3.0.101-0.7.21-default-x86
SLES11SP2-LTSS_U2-3.0.101-0.7.21-default-x86_64
SLES11SP2-LTSS_U2-3.0.101-0.7.21-pae-x86
SLES11SP2-LTSS_U2-3.0.101-0.7.21-xen-x86
SLES11SP2-LTSS_U2-3.0.101-0.7.21-xen-x86_64
SLES11SP2-U1-3.0.26-0.7-default-x86
SLES11SP2-U1-3.0.26-0.7-default-x86_64
SLES11SP2-U1-3.0.26-0.7-pae-x86
SLES11SP2-U1-3.0.26-0.7-xen-x86
SLES11SP2-U1-3.0.26-0.7-xen-x86_64
SLES11SP2-U10-3.0.74-0.6.8-default-x86
SLES11SP2-U10-3.0.74-0.6.8-default-x86_64
SLES11SP2-U10-3.0.74-0.6.8-pae-x86
SLES11SP2-U10-3.0.74-0.6.8-xen-x86
SLES11SP2-U10-3.0.74-0.6.8-xen-x86_64
SLES11SP2-U11-3.0.74-0.6.10-default-x86
SLES11SP2-U11-3.0.74-0.6.10-default-x86_64
SLES11SP2-U11-3.0.74-0.6.10-pae-x86
SLES11SP2-U11-3.0.74-0.6.10-xen-x86
SLES11SP2-U11-3.0.74-0.6.10-xen-x86_64
SLES11SP2-U12-3.0.80-0.5-default-x86
SLES11SP2-U12-3.0.80-0.5-default-x86_64
SLES11SP2-U12-3.0.80-0.5-pae-x86
SLES11SP2-U12-3.0.80-0.5-xen-x86
SLES11SP2-U12-3.0.80-0.5-xen-x86_64
SLES11SP2-U13-3.0.80-0.7-default-x86
SLES11SP2-U13-3.0.80-0.7-default-x86_64
SLES11SP2-U13-3.0.80-0.7-pae-x86
SLES11SP2-U13-3.0.80-0.7-xen-x86
SLES11SP2-U13-3.0.80-0.7-xen-x86_64
SLES11SP2-U14-3.0.93-0.5-default-x86
SLES11SP2-U14-3.0.93-0.5-default-x86_64
SLES11SP2-U14-3.0.93-0.5-pae-x86
SLES11SP2-U14-3.0.93-0.5-xen-x86
SLES11SP2-U14-3.0.93-0.5-xen-x86_64
SLES11SP2-U15-3.0.101-0.5-default-x86
SLES11SP2-U15-3.0.101-0.5-default-x86_64
SLES11SP2-U15-3.0.101-0.5-pae-x86
SLES11SP2-U15-3.0.101-0.5-xen-x86
SLES11SP2-U15-3.0.101-0.5-xen-x86_64
SLES11SP2-U16-3.0.101-0.7.15-default-x86
SLES11SP2-U16-3.0.101-0.7.15-default-x86_64
SLES11SP2-U16-3.0.101-0.7.15-pae-x86

SLES11SP2-U16-3.0.101-0.7.15-xen-x86
SLES11SP2-U16-3.0.101-0.7.15-xen-x86_64
SLES11SP2-U17-3.0.101-0.7.17-default-x86
SLES11SP2-U17-3.0.101-0.7.17-default-x86_64
SLES11SP2-U17-3.0.101-0.7.17-pae-x86
SLES11SP2-U17-3.0.101-0.7.17-xen-x86
SLES11SP2-U17-3.0.101-0.7.17-xen-x86_64
SLES11SP2-U2-3.0.31-0.9-default-x86
SLES11SP2-U2-3.0.31-0.9-default-x86_64
SLES11SP2-U2-3.0.31-0.9-pae-x86
SLES11SP2-U2-3.0.31-0.9-xen-x86
SLES11SP2-U2-3.0.31-0.9-xen-x86_64
SLES11SP2-U3-3.0.34-0.7-default-x86
SLES11SP2-U3-3.0.34-0.7-default-x86_64
SLES11SP2-U3-3.0.34-0.7-pae-x86
SLES11SP2-U3-3.0.34-0.7-xen-x86
SLES11SP2-U3-3.0.34-0.7-xen-x86_64
SLES11SP2-U4-3.0.38-0.5-default-x86
SLES11SP2-U4-3.0.38-0.5-default-x86_64
SLES11SP2-U4-3.0.38-0.5-pae-x86
SLES11SP2-U4-3.0.38-0.5-xen-x86
SLES11SP2-U4-3.0.38-0.5-xen-x86_64
SLES11SP2-U5-3.0.42-0.7-default-x86
SLES11SP2-U5-3.0.42-0.7-default-x86_64
SLES11SP2-U5-3.0.42-0.7-pae-x86
SLES11SP2-U5-3.0.42-0.7-xen-x86
SLES11SP2-U5-3.0.42-0.7-xen-x86_64
SLES11SP2-U6-3.0.51-0.7.9-default-x86
SLES11SP2-U6-3.0.51-0.7.9-default-x86_64
SLES11SP2-U6-3.0.51-0.7.9-pae-x86
SLES11SP2-U6-3.0.51-0.7.9-xen-x86
SLES11SP2-U6-3.0.51-0.7.9-xen-x86_64
SLES11SP2-U7-3.0.58-0.6.2-default-x86
SLES11SP2-U7-3.0.58-0.6.2-default-x86_64
SLES11SP2-U7-3.0.58-0.6.2-pae-x86
SLES11SP2-U7-3.0.58-0.6.2-xen-x86
SLES11SP2-U7-3.0.58-0.6.2-xen-x86_64
SLES11SP2-U8-3.0.58-0.6.6-default-x86
SLES11SP2-U8-3.0.58-0.6.6-default-x86_64
SLES11SP2-U8-3.0.58-0.6.6-pae-x86
SLES11SP2-U8-3.0.58-0.6.6-xen-x86
SLES11SP2-U8-3.0.58-0.6.6-xen-x86_64
SLES11SP2-U9-3.0.74-0.6.6-default-x86
SLES11SP2-U9-3.0.74-0.6.6-default-x86_64
SLES11SP2-U9-3.0.74-0.6.6-pae-x86
SLES11SP2-U9-3.0.74-0.6.6-xen-x86
SLES11SP2-U9-3.0.74-0.6.6-xen-x86_64

SLES11SP3-GA-3.0.76-0.11-default-x86
SLES11SP3-GA-3.0.76-0.11-default-x86_64
SLES11SP3-GA-3.0.76-0.11-pae-x86
SLES11SP3-GA-3.0.76-0.11-xen-x86
SLES11SP3-GA-3.0.76-0.11-xen-x86_64
SLES11SP3-U1-3.0.82-0.7-default-x86
SLES11SP3-U1-3.0.82-0.7-default-x86_64
SLES11SP3-U1-3.0.82-0.7-pae-x86
SLES11SP3-U1-3.0.82-0.7-xen-x86
SLES11SP3-U1-3.0.82-0.7-xen-x86_64
SLES11SP3-U2-3.0.93-0.8-default-x86
SLES11SP3-U2-3.0.93-0.8-default-x86_64
SLES11SP3-U2-3.0.93-0.8-pae-x86
SLES11SP3-U2-3.0.93-0.8-xen-x86
SLES11SP3-U2-3.0.93-0.8-xen-x86_64
SLES11SP3-U3-3.0.101-0.8-default-x86
SLES11SP3-U3-3.0.101-0.8-default-x86_64
SLES11SP3-U3-3.0.101-0.8-pae-x86
SLES11SP3-U3-3.0.101-0.8-xen-x86
SLES11SP3-U3-3.0.101-0.8-xen-x86_64
SLES11SP3-U4-3.0.101-0.15-default-x86
SLES11SP3-U4-3.0.101-0.15-default-x86_64
SLES11SP3-U4-3.0.101-0.15-pae-x86
SLES11SP3-U4-3.0.101-0.15-xen-x86
SLES11SP3-U4-3.0.101-0.15-xen-x86_64
SLES11SP3-U5-3.0.101-0.21-default-x86
SLES11SP3-U5-3.0.101-0.21-default-x86_64
SLES11SP3-U5-3.0.101-0.21-pae-x86
SLES11SP3-U5-3.0.101-0.21-xen-x86
SLES11SP3-U5-3.0.101-0.21-xen-x86_64
SLES11SP3-U6-3.0.101-0.29-default-x86
SLES11SP3-U6-3.0.101-0.29-default-x86_64
SLES11SP3-U6-3.0.101-0.29-pae-x86
SLES11SP3-U6-3.0.101-0.29-xen-x86
SLES11SP3-U6-3.0.101-0.29-xen-x86_64
SLES11SP3-U7-3.0.101-0.31-default-x86
SLES11SP3-U7-3.0.101-0.31-default-x86_64
SLES11SP3-U7-3.0.101-0.31-pae-x86
SLES11SP3-U7-3.0.101-0.31-xen-x86
SLES11SP3-U7-3.0.101-0.31-xen-x86_64
SLES11SP3-U8-3.0.101-0.35-default-x86
SLES11SP3-U8-3.0.101-0.35-default-x86_64
SLES11SP3-U8-3.0.101-0.35-pae-x86
SLES11SP3-U8-3.0.101-0.35-xen-x86
SLES11SP3-U8-3.0.101-0.35-xen-x86_64
SLES9-GA-2.6.5-7.97-bigsmpt-x86
SLES9-GA-2.6.5-7.97-default-x86

SLES9-GA-2.6.5-7.97-default-x86_64
SLES9-GA-2.6.5-7.97-smp-x86
SLES9-GA-2.6.5-7.97-smp-x86_64
SLES9-SP1-2.6.5-7.139-bigsmp-x86
SLES9-SP1-2.6.5-7.139-default-x86
SLES9-SP1-2.6.5-7.139-default-x86_64
SLES9-SP1-2.6.5-7.139-smp-x86
SLES9-SP1-2.6.5-7.139-smp-x86_64
SLES9-SP2-2.6.5-7.191-bigsmp-x86
SLES9-SP2-2.6.5-7.191-default-x86
SLES9-SP2-2.6.5-7.191-default-x86_64
SLES9-SP2-2.6.5-7.191-smp-x86
SLES9-SP2-2.6.5-7.191-smp-x86_64
SLES9-SP3-2.6.5-7.244-bigsmp-x86
SLES9-SP3-2.6.5-7.244-default-x86
SLES9-SP3-2.6.5-7.244-default-x86_64
SLES9-SP3-2.6.5-7.244-smp-x86
SLES9-SP3-2.6.5-7.244-smp-x86_64
SLES9-SP4-2.6.5-7.308-bigsmp-x86
SLES9-SP4-2.6.5-7.308-default-x86
SLES9-SP4-2.6.5-7.308-default-x86_64
SLES9-SP4-2.6.5-7.308-smp-x86
SLES9-SP4-2.6.5-7.308-smp-x86_64

B Sincronización del almacenamiento local del nodo de clúster

En esta sección se detalla el procedimiento que puede usar para cambiar los números de serie del volumen local para hacer coincidir los nodos del clúster de Windows que desea proteger. La información incluye el uso de la utilidad Gestor de volúmenes (`VolumeManager.exe`) para sincronizar el almacenamiento local del nodo de clúster.

Para descargar y ejecutar la utilidad:

- 1 En el [sitio de descargas de NetIQ](#), buque el producto Protect 11 y haga clic en **Submit Query** (Enviar consulta).
- 2 En la pestaña de productos, seleccione **PlateSpin Protect 11.0** y haga clic en **proceed to download** (Continuar para descargar).
- 3 En la página de descarga, haga clic en **download** (Descargar) en la línea `VolumeManager.exe` o seleccione en enlace similar del gestor de descargas.
- 4 Descargue la utilidad y cópiela en una ubicación a la que pueda acceder en cada nodo del clúster.
- 5 En el nodo activo del clúster, abra un indicador de comandos de administración, diríjase a la ubicación de la utilidad de descarga y ejecute el comando siguiente:

```
VolumeManager.exe -l
```

Se muestra una lista de los volúmenes locales y sus números de serie respectivos. Por ejemplo:

```
Volume Listing:
```

```
-----
```

```
DriveLetter (*:) VolumeId="System Reserved" SerialNumber: AABB-CCDD
```

```
DriveLetter (C:) VolumeId=C:\ SerialNumber: 1122-3344
```

Anote estos números de serie o siga mostrándolos para compararlos más tarde.

- 6 Compruebe que todos los números de serie del almacenamiento local del nodo activo coinciden con los números correspondientes de los demás nodos del clúster.
 - 6a En cada nodo del clúster, ejecute el comando `VolumeManager.exe -l` para obtener sus números de serie de volumen.
 - 6b Compare los números de serie de almacenamiento local del nodo activo ([Paso 5](#)) con los números correspondientes del nodo ([Paso 6a](#)).
 - 6c (Condicional) Si hay diferencias en los números de serie entre el nodo activo y este nodo, anote el número de serie que desea copiar en este nodo y ejecute el comando siguiente para establecerlo. Después compruebe el número de serie.

```
VolumeManager -s <IDVolumen> <número-serie>
```

A continuación se muestran dos ejemplos de cómo se debe usar este comando:

- ♦ `VolumeManager -s "Reservado para el sistema" AAAA-AAAA`
- ♦ `VolumeManager -s C:\ 1111-1111`

- 6d** Cuando haya cambiado correctamente todos los números de serie del volumen de un nodo del clúster, debe reiniciar dicho nodo.
- 6e** Repita del [Paso 6a](#) al [Paso 6d](#) en cada nodo del clúster.
- 7** (Condicional) Si el clúster ya se ha protegido en un entorno de PlateSpin, se recomienda ejecutar una réplica completa en el nodo activo para asegurarse de que los cambios se propagan a la base de datos.

Glosario

Carga de trabajo. El objeto básico de protección de un almacén de datos. Un sistema operativo junto con su middleware y los datos, desacoplado de su infraestructura física o virtual subyacente.

Carga de trabajo de failover. Una réplica virtual arrancable de una carga de trabajo protegida.

Contenedor. Infraestructura de protección de carga de trabajo de PlateSpin Protect, como un host de máquina virtual.

Contrato de protección. Un conjunto de valores activos pertenecientes a todo el ciclo vital de protección de una carga de trabajo (*añadir al inventario, réplicas* iniciales y continuas, *failover, failback* y *volver a proteger*).

Destino. Una carga de trabajo o su infraestructura que es el resultado de un comando de PlateSpin Protect. Por ejemplo, en la protección inicial de una carga de trabajo, el destino es la carga de trabajo de failover del contenedor. En una operación de failback, es la infraestructura original de la carga de trabajo de producción o un contenedor admitido que se haya incluido en el inventario de PlateSpin Protect.

Véase [Origen](#).

Evento. Un mensaje del servidor de PlateSpin que contiene información sobre pasos importantes en todo el ciclo vital de protección de la carga de trabajo.

Failback. Restauración de la función empresarial de una carga de trabajo errónea en su entorno original cuando la función empresarial de una carga de trabajo de failover temporal de PlateSpin Protect ya no es necesaria.

Failover. Tomar el control de la función empresarial de una carga de trabajo errónea por parte de una carga de trabajo de failover de un contenedor de máquina virtual de PlateSpin Protect.

Incremental. 1. (Nombre) una transferencia programada individual o una transferencia manual de las diferencias entre una carga de trabajo protegida y su réplica (la carga de trabajo de failover).

2. (Adjetivo) Describe el ámbito de la *réplica (1)*, donde la réplica inicial de una carga de trabajo se crea de forma diferenciada según las diferencias entre la carga de trabajo y su equivalente preparada.

Nivel de protección. Un conjunto personalizable de parámetros de protección de la carga de trabajo que define la frecuencia de las réplicas y criterios por los que el sistema considerará que una carga de trabajo es errónea.

Objetivo de punto de recuperación (RPO). La pérdida de datos tolerable medida en tiempo y definida por un intervalo configurable entre las réplicas incrementales de una carga de trabajo protegida.

Objetivo de tiempo de recuperación (RTO). Una medida del tiempo de inactividad tolerable de la carga de trabajo definido por el tiempo que una operación de failover tarda en completarse.

Objetivos de tiempo de prueba (TTO). Una medida de la facilidad con la que se puede probar un plan de recuperación tras fallos. Es similar al RTO, pero incluye el tiempo necesario para que un usuario pruebe la carga de trabajo de failover.

Origen. Una carga de trabajo o su infraestructura que sirve como punto de partida de una operación de PlateSpin Protect. Por ejemplo, en la protección inicial de una carga de trabajo, el origen es la carga de trabajo de producción. En una operación de failback, es la carga de trabajo de failover del contenedor.

Véase [Destino](#).

Preparación para failover. Una operación de PlateSpin Protect que arranca la carga de trabajo de failover para preparar una operación de failover completa.

Probar failover. Una operación de PlateSpin Protect que arranca una carga de trabajo de failover en un entorno de redes aislado para realizar pruebas sobre la funcionalidad del failover y para verificar la integridad de la carga de trabajo de failover.

Programación de réplica. La programación que se configura para controlar la frecuencia y el ámbito de las réplicas.

Punto de recuperación. Una instantánea de un momento que permite restaurar una carga de trabajo replicada a un estado anterior.

Réplica. 1. *Réplica inicial*, la creación de una copia base inicial de una carga de trabajo. Se puede llevar a cabo como *réplica completa* (se transfieren todos los datos de la carga de trabajo a una máquina virtual de failover vacía), o como *réplica incremental* (consulte [Incremental](#) (2)).

2. Transferencia de los datos cambiados de una carga de trabajo protegida a su réplica en el contenedor.

Volver a proteger. Un comando de PlateSpin Protect que restablece un contrato de protección para una carga de trabajo después de las operaciones de failover y failback.