PlateSpin® Protect 11.2 SP1

Guía del usuario

Diciembre de 2017

Información legal

Para obtener información acerca de la información legal, las marcas comerciales, las renuncias de responsabilidad, las garantías, la exportación y otras restricciones de uso, los derechos del gobierno estadounidense, la directiva de patentes y el cumplimiento de la norma FIPS, consulte el sitio https://www.microfocus.com/about/legal/.

Concesión de la licencia

Las licencias adquiridas para PlateSpin Protect 11 y versiones posteriores no se pueden usar para PlateSpin Protect 10.3 o versiones anteriores.

Tabla de contenido

Acerca de esta guía 9

Parte I Planificación 11

1 Planificación del entorno de PlateSpin 13

1.1 Configuraciones compatibles . . . 13
1.1.1 Cargas de trabajo Windows compatibles . . . 14
1.1.2 Cargas de trabajo Linux compatibles . . . 15
1.1.3 Contenedores de máquina virtual compatibles . . . 17
1.1.4 Arquitecturas de cargas de trabajo compatibles . . . 19
1.1.5 Almacenamiento admitido . . . 21
1.1.6 Idiomas admitidos . . . 22
1.1.7 Navegadores Web compatibles . . . 23
1.2 Métodos de transferencia de datos admitidos . . . 23
1.2.1 Métodos de transferencia de datos compatibles para cargas de trabajo Windows . . . 23
1.2.2 Método de transferencia compatible para cargas de trabajo Linux . . . 24
1.3 Seguridad y privacidad . . . 24
1.3.1 Cifrado de datos durante la transmisión . . . 24
1.3.2 Seguridad de las comunicaciones entre los clientes y el servidor . . . 25
1.3.3 Seguridad de las credenciales . . . 25
1.3.4 Autorización y autenticación de usuarios . . . 25
1.3.5 Autenticación de Windows para la base de datos de Microsoft SQL Server . . . 25
1.3.6 Cortafuegos y configuración del puerto . . . 25
1.4 Rendimiento . . . 27
1.4.1 Acerca de las características de rendimiento del producto . . . 28
1.4.2 Especificaciones de RPO, RTO y TTO . . . 28
1.4.3 Compresión de datos . . . 29
1.4.4 Regularización del ancho de banda . . . 29
1.4.5 Capacidad de ampliación . . . 30
1.4.6 Servidor de base de datos . . . 30
1.5 Requisitos de acceso y comunicación en la red de protección . . . 31
1.5.1 Requisitos de red para la interfaz Web del host del servidor de PlateSpin . . . 31
1.5.2 Requisitos de red para los contenedores . . . 31
1.5.3 Requisitos de red para las cargas de trabajo . . . 32
1.5.4 Requisitos para la autenticación de Windows para la base de datos de Microsoft SQL Server . . . 34
1.5.5 Requisitos para la protección en redes públicas y privadas mediante NAT . . . 35
1.5.6 Requisitos para que el servidor de PlateSpin funcione con NAT . . . 36
1.5.7 Anulación de la shell bash por defecto para ejecutar comandos en cargas de trabajo Linux . . . 36

2 Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo 37

Parte II Gestión del servidor de PlateSpin 39

3 Uso de las herramientas de PlateSpin 41

3.1 Lanzamiento de la interfaz Web . . . 41

3.2 Descripción general de la consola . . . 42
3.2.1 Barra de navegación . . . 43
3.2.2 Panel de resumen visual . . . 43
3.2.3 Panel de tareas y eventos . . . 44
3.3 Descripción general de las cargas de trabajo . . . 45
3.4 Comandos de protección y recuperación de cargas de trabajo . . . 45
3.5 Otras herramientas de gestión del servidor de PlateSpin . . . 47
3.5.1 Configuración de PlateSpin . . . 47
3.5.2 Utilidad Protect Agent . . . 48
3.5.3 Herramienta VMware Role . . . 48

4 Gestión de licencias 49

4.1 Activación de la licencia del producto . . . 49
4.1.1 Activación de licencia en línea . . . 49
4.1.2 Activación de licencia sin conexión . . . 50
4.2 Acerca del consumo de licencias de carga de trabajo . . . 50
4.3 Visualización de la información de licencia . . . 51
4.4 Adición de una licencia . . . 52
4.5 Supresión de una licencia . . . 52
4.6 Generación de un informe de licencias para la asistencia técnica . . . 52

5 Configuración de la autorización y la autenticación de usuarios 53

5.1 Acerca del acceso basado en funciones de PlateSpin Protect . . . 53
5.2 Gestión del acceso y los permisos de PlateSpin Protect . . . 54
5.2.1 Adición de usuarios a PlateSpin Protect . . . 55
5.2.2 Asignación de una función de protección de carga de trabajo a un usuario de PlateSpin Protect . . . 55
5.3 Gestión de los grupos de seguridad de PlateSpin Protect y los permisos de la carga de trabajo . . . 56
5.4 Configuración de inquilinos múltiples de Protect en VMware . . . 57
5.4.1 Definición de funciones de VMware para varios inquilinos . . . 57
5.4.2 Asignación de funciones en vCenter . . . 61

6 Configuración de la aplicación del servidor de PlateSpin 65

6.1 Configuración de idiomas para versiones internacionales . . . 65
6.1.1 Establecimiento del idioma en el sistema operativo . . . 65
6.1.2 Establecimiento del idioma en el navegador Web . . . 66
6.2 Configuración de los servicios de notificación por correo electrónico para eventos e informes de réplica . . . 67
6.2.1 Configuración de SMTP para el servicio de notificación por correo electrónico . . . 67
6.2.2 Habilitación de las notificaciones de eventos . . . 68
6.2.3 Habilitación de informes de réplica . . . 69
6.3 Configuración de direcciones IP alternativas para el servidor de PlateSpin . . . 70
6.4 Optimización de transferencia de datos en conexiones WAN . . . 71
6.4.1 Ajuste de parámetros . . . 71
6.4.2 Ajuste de FileTransferSendReceiveBufferSize . . . 73
6.5 Optimización del rendimiento del entorno de réplica . . . 74
6.6 Establecimiento de método de rearranque para el servicio de configuración . . . 75
6.7 Configuración de la compatibilidad con VMware vCenter Site Recovery Manager . . . 76
6.7.1 Configuración de archivos de carga de trabajo en el mismo almacén de datos . . . 76
6.7.2 Configuración de herramientas de VMware para los destinos de failover . . . 77
6.7.3 Aceleración del proceso de configuración . . . 78

7 Configuración de la interfaz Web de PlateSpin 79

7.1 Creación y gestión de etiquetas de cargas de trabajo . . . 79
7.1.1 Creación de una etiqueta de carga de trabajo . . . 79
7.1.2 Edición de una etiqueta de carga de trabajo . . . 80
7.1.3 Adición de una etiqueta a una carga de trabajo . . . 80
7.1.4 Eliminación de una etiqueta de una carga de trabajo . . . 81
7.1.5 Supresión de una etiqueta de carga de trabajo . . . 81
7.2 Configuración de las frecuencias de actualización de la interfaz Web . . . 81
7.3 Personalización del aspecto de la interfaz Web . . . 82

8 Gestión de varios servidores de PlateSpin en la consola de gestión 83

8.1 Uso de la consola de gestión de PlateSpin Protect . . . 83
8.2 Acerca de las tarjetas de consola de gestión de PlateSpin Protect . . . 84
8.3 Adición de instancias de PlateSpin Protect y PlateSpin Forge a la consola de gestión . . . 85
8.4 Edición de tarjetas en la consola de gestión . . . 86
8.5 Eliminación de tarjetas en la consola de gestión . . . 86

A Cambio de marca de la interfaz Web de PlateSpin Protect 87

A.1 Cambio de marca de la interfaz Web mediante parámetros de configuración . . . 87
A.1.1 Elementos configurables de la interfaz Web . . . 88
A.1.2 Parámetros configurables de la interfaz Web . . . 88
A.2 Cambio de marca del nombre del producto en el Registro de Windows . . . 90

Parte III Preparación de los destinos y los orígenes de protección 93

9 Preparación de contenedores (destinos de protección) 95

9.1 Acerca de los contenedores (destinos de protección) . . . 95
9.1.1 Contenedores compatibles . . . 95
9.1.2 Requisitos de acceso a la red para contenedores . . . 95
9.1.3 Directrices de los parámetros para los contenedores . . . 95
9.2 Adición de contenedores (destinos de protección) . . . 96
9.3 Actualización de los detalles del contenedor . . . 98
9.4 Eliminación de contenedores (destinos de protección) . . . 98

10 Preparación de cargas de trabajo (orígenes de protección) 99

10.1 Acerca de las cargas de trabajo (orígenes de protección) . . . 99
10.1.1 Cargas de trabajo compatibles . . . 99
10.1.2 Requisitos de acceso a la red para las cargas de trabajo de origen . . . 100
10.1.3 Directrices de parámetros para las cargas de trabajo de origen . . . 100
10.2 Adición de cargas de trabajo (orígenes de protección) . . . 100
10.3 Etiquetado de cargas de trabajo . . . 101
10.4 Actualización de los detalles de la carga de trabajo . . . 102
10.5 Eliminación de cargas de trabajo . . . 103

11 Preparación de controladores de dispositivos para los destinos de failback físicos 105

11.1 Gestión de controladores de dispositivo . . . 105
11.1.1 Empaquetado de controladores de dispositivo para cargas de trabajo Windows . . . 105
11.1.2 Empaquetado de controladores de dispositivo para cargas de trabajo Linux . . . 106

11.1.3 Carga de paquetes de controladores a la base de datos de controladores de dispositivo de PlateSpin . . . 106
11.2 Gestión de las asignaciones de ID de PnP de PlateSpin . . . 109

12 Preparación para proteger cargas de trabajo Linux 117

12.1 Verificación de los controladores basados en bloques para Linux . . . 117
12.2 Preparación de instantáneas para la transferencia a nivel de bloques (Linux) . . . 117
12.2.1 Configuración de instantáneas LVM para la réplica del volumen de Linux . . . 118
12.2.2 Configuración de instantáneas NSS para la réplica del repositorio NSS . . . 118
12.3 Uso de los guiones freeze y thaw en todas las réplicas (Linux) . . . 119

13 Preparación para proteger clústeres de Windows 121

13.1 Planificación para proteger la carga de trabajo de clúster . . . 121
13.1.1 Requisitos para la protección del clúster . . . 122
13.1.2 Transferencia basada en bloques para los clústeres . . . 123
13.1.3 Impacto del failover del nodo de clúster en la réplica . . . 125
13.1.4 Similitud del nodo de clúster . . . 126
13.1.5 Configuración de la protección . . . 127
13.2 Configuración de descubrimiento del nodo activo de Windows . . . 127
13.3 Configuración del método de transferencia basada en bloques para clústeres . . . 128
13.4 Adición de valores de búsqueda de nombres de recursos . . . 128
13.5 Tiempo límite de arbitraje de quórum . . . 129
13.6 Configuración de los números de serie del volumen local . . . 129
13.7 Failover de PlateSpin . . . 129
13.8 Failback de PlateSpin . . . 130

14 Solución de problemas de descubrimiento e inventario de cargas de trabajo 131

14.1 Resolución de problemas de descubrimiento para cargas de trabajo Windows . . . 131
14.1.1 Problemas comunes y soluciones . . . 131
14.1.2 Modificación del retraso del inicio de pulsación del controlador OFX . . . 133
14.1.3 Realización de pruebas de conectividad . . . 133
14.1.4 Inhabilitación del software antivirus . . . 135
14.1.5 Habilitación de permisos y acceso a archivos y recursos compartidos . . . 135
14.2 Resolución de problemas de descubrimiento para cargas de trabajo Linux . . . 136
14.3 Resolución de problemas de descubrimiento de hosts de destino . . . 136

B Distribuciones de Linux compatibles con Protect 137

B.1 Análisis de la carga de trabajo Linux . . . 137
B.1.1 Determinación de la cadena de versión . . . 137
B.1.2 Determinación de la arquitectura . . . 137
B.2 Controladores blkwatch precompilados para distribuciones Linux . . . 138
B.2.1 Sintaxis de los elementos de la lista . . . 138
B.2.2 Lista de distribuciones . . . 138
B.2.3 Otras distribuciones de Linux que usan controladores blkwatch . . . 138

C Sincronización de números de serie en el almacenamiento local del nodo de clústeres 141

D Utilidad Protect Agent 143

D.1 Uso de la utilidad Protect Agent para Windows . . . 143
D.2 Uso de Protect Agent con controladores de transferencia basada en bloques . . . 144

Parte IV Protección de cargas de trabajo 149

15 Protección y recuperación de cargas de trabajo 151

15.1 Requisitos previos para proteger las cargas de trabajo . . . 151
15.2 Configuración de los detalles de protección y preparación de la réplica . . . 151
15.2.1 Detalles de protección de la carga de trabajo . . . 153
15.3 Inicio de la protección de la carga de trabajo . . . 156
15.4 Cancelación de comandos . . . 157
15.5 Failover . . . 157
15.5.1 Detección de cargas de trabajo sin conexión . . . 157
15.5.2 Realización de failover . . . 158
15.5.3 Uso de la función de prueba de failover . . . 159
15.6 Failback . . . 160
15.6.1 Failback automatizado a una plataforma de máquina virtual . . . 160
15.6.2 Failback semiautomatizado a un equipo físico . . . 163
15.6.3 Failback semiautomatizado a una máquina virtual . . . 164
15.7 Reprotección de una carga de trabajo . . . 164

16 Elementos básicos de la protección de la carga de trabajo 167

16.1 Directrices para las credenciales de carga de trabajo y contenedor . . . 167
16.2 Niveles de protección . . . 168
16.3 Puntos de recuperación . . . 170
16.4 Método de réplica inicial (completa o incremental) . . . 170
16.5 Control de servicios y daemons . . . 171
16.6 Almacenamiento de volúmenes . . . 172
16.7 Redes . . . 175
16.8 Failback a equipos físicos . . . 175
16.8.1 Descarga de la imagen ISO OFX de arranque de PlateSpin . . . 175
16.8.2 Incorporación de controladores de dispositivo adicionales en la imagen ISO de arranque . . . 176
16.8.3 Registro de equipos físicos como destinos de failback con PlateSpin Protect . . . 177
16.9 Protección de clústeres de Windows . . . 178
16.9.1 Failover de PlateSpin . . . 178
16.9.2 Failback de PlateSpin . . . 179

17 Generación de informes 181

17.1 Acerca de los informes de Protect . . . 182
17.2 Generación de informes de carga de trabajo y de protección de la carga de trabajo . . . 182
17.3 Generación de informes de diagnóstico . . . 183

18 Solución de problemas de protección y recuperación de cargas de trabajo 185

18.1 Optimización del rendimiento de una conexión . . . 185
18.2 Solución de problemas de reenvío de tráfico en las cargas de trabajo . . . 185
18.3 Solución de problemas del servicio de configuración . . . 186
18.3.1 Comprensión de las causas del problema . . . 186
18.3.2 ¿Qué se puede hacer para resolver el problema? . . . 187
18.3.3 Sugerencias adicionales para la solución de problemas . . . 190
18.4 Solución de problemas de réplica al preparar la carga de trabajo (Windows) . . . 191
18.4.1 Directiva de grupo y derechos de usuario . . . 191
18.4.2 Dos o más volúmenes tienen el mismo número de serie de volumen . . . 191
18.5 Solución de problemas de réplica de la carga de trabajo . . . 192
18.6 Solución de problemas de failover o failback de la carga de trabajo . . . 194

18.7 Compresión de las bases de datos de PlateSpin Protect 195
18.8 Limpieza de la carga de trabajo después de la protección 195
18.8.1 Limpieza de las cargas de trabajo Windows 195
18.8.2 Limpieza de las cargas de trabajo Linux 196

Parte V Herramientas de PlateSpin 199

E Uso de funciones de protección de la carga de trabajo mediante la API del servidor de PlateSpin Protect 201

E.1 Descripción general de la API 201
E.2 Documentación de la API del servidor de PlateSpin Protect 201
E.3 Muestras y otras referencias 202

F Uso de la herramienta de prueba de red iPerf para optimizar el rendimiento de red para productos de PlateSpin 205

F.1 Introducción 205
F.2 Cálculos 206
F.3 Configuración 207
F.4 Metodología 208
F.5 Expectativas 209

Acerca de esta guía

La *Guía del usuario* proporciona información sobre el uso de PlateSpin Protect. Proporciona información conceptual, una descripción general de la interfaz del usuario e instrucciones detalladas para las tareas comunes. También define la terminología e incluye información para solucionar problemas.

A quién va dirigida

Este documento está dirigido a administradores y operadores de centros de datos que usan PlateSpin Protect en su solución habitual de protección de cargas de trabajo y recuperación tras fallos.

Documentación adicional

Para obtener la versión más reciente de esta guía y otros recursos de documentación de PlateSpin Protect, visite el sitio Web de documentación de PlateSpin Protect (https://www.netiq.com/documentation/platespin-protect/).

Además de en inglés, la documentación en línea está disponible en estos idiomas: alemán, chino simplificado, chino tradicional, español, francés y japonés.

Información de contacto

Nos gustaría recibir sus comentarios y sugerencias acerca de este manual y del resto de la documentación incluida con este producto. Puede utilizar el enlace para **comentar sobre el tema** de la parte inferior de cualquier página de la documentación en línea o enviar un correo electrónico a Documentation-Feedback@microfocus.com.

Para problemas específicos de productos, póngase en contacto con Atención al cliente de Micro Focus en https://www.microfocus.com/support-and-services/.

Planificación

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

- Capítulo 1, “Planificación del entorno de PlateSpin”, en la página 13
- Capítulo 2, “Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo”, en la página 37

1 Planificación del entorno de PlateSpin

Use los datos de esta sección para planificar el entorno de protección y recuperación de PlateSpin.

- Sección 1.1, “Configuraciones compatibles”, en la página 13
- Sección 1.2, “Métodos de transferencia de datos admitidos”, en la página 23
- Sección 1.3, “Seguridad y privacidad”, en la página 24
- Sección 1.4, “Rendimiento”, en la página 27
- Sección 1.5, “Requisitos de acceso y comunicación en la red de protección”, en la página 31

1.1 Configuraciones compatibles

PlateSpin Protect admite la mayoría de las versiones de los sistemas operativos Microsoft Windows, SUSE Linux Enterprise Server y Red Hat Enterprise Linux. También admite determinadas versiones de los sistemas operativos Novell Open Enterprise Server, Oracle Enterprise Linux y CentOS.

En esta sección se describen todas las configuraciones de plataforma admitidas por PlateSpin Protect, así como el software, el hardware, los entornos de virtualización necesarios para la protección y la recuperación de las cargas de trabajo. Algunas configuraciones, como se indica, requieren una gestión especial para configurar y recuperar las cargas de trabajo. Asegúrese de revisar la información de referencia en toda la documentación en línea o en los artículos de la base de conocimientos antes de intentar configurar la carga de trabajo.

Nota: aunque las configuraciones que no se mencionan en este documento no se admiten, muchas de las mejoras que se realizan a PlateSpin Protect son consecuencia directa de las sugerencias de nuestros clientes. Puede ayudarnos a garantizar que nuestro producto satisfaga todas sus necesidades. Si tiene interés en una configuración de plataforma que no aparezca en la lista, póngase en contacto con el servicio de asistencia técnica. Agradecemos sus comentarios y estamos deseando oír sus sugerencias.

- Sección 1.1.1, “Cargas de trabajo Windows compatibles”, en la página 14
- Sección 1.1.2, “Cargas de trabajo Linux compatibles”, en la página 15
- Sección 1.1.3, “Contenedores de máquina virtual compatibles”, en la página 17
- Sección 1.1.4, “Arquitecturas de cargas de trabajo compatibles”, en la página 19
- Sección 1.1.5, “Almacenamiento admitido”, en la página 21
- Sección 1.1.6, “Idiomas admitidos”, en la página 22
- Sección 1.1.7, “Navegadores Web compatibles”, en la página 23

1.1.1 Cargas de trabajo Windows compatibles

PlateSpin Protect admite cargas de trabajo de las versiones del sistema operativo Microsoft Windows indicadas en la Tabla 1-1

Se admite tanto la réplica en el nivel de archivos como en el nivel de bloques, con ciertas restricciones. Consulte Sección 1.2, “Métodos de transferencia de datos admitidos”, en la página 23.

Nota: no se admite la protección de cargas de trabajo de escritorio (estaciones de trabajo).

Tabla 1-1 *Cargas de trabajo Windows compatibles*

Sistema operativo	Notas
Servidores	
Windows Server 2016	Para la protección de servidores Windows Server 2016 se requiere VMware 6.0 o posterior.
Windows Server 2012 R2 Windows Server 2012	Incluidos los controladores de dominio (DC) y las ediciones Small Business Server (SBS) Para obtener información sobre la conversión de controladores de dominio de Active Directory, consulte el artículo 7920501 de la base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7920501).
Windows Server 2008 R2 (64 bits) Windows Server 2008 (64 bits) Windows Server 2008 con el último Service Pack (32 bits)	Incluidos los controladores de dominio (DC) y las ediciones Small Business Server (SBS) Para obtener información sobre la conversión de controladores de dominio de Active Directory, consulte el artículo 7920501 de la base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7920501).
Windows Server 2003 R2 (64 bits) Windows Server 2003 R2 (32 bits) Windows Server 2003 con el último Service Pack (64 bits) Windows Server 2003 con el último Service Pack (32 bits)	Windows 2003 requiere el SP1 o superior para la réplica basada en bloques.

Sistema operativo	Notas
Clústeres	
Clúster de failover de Microsoft basado en Windows Server 2016	Para la protección de clústeres de Windows Server 2016 se requiere VMware 6.0 o posterior.
Clúster de failover de Microsoft basado en Windows Server 2012 R2	Modelos compatibles: *quórum Nodo y mayoría discos* y *Sin mayoría: quórum solo de disco.*
Clúster de failover de Microsoft basado en Windows Server 2008 R2	La compatibilidad incluye la transferencia de datos basada en bloques con un controlador (solo en las SAN de Fibre Channel) o sin un controlador para las réplicas incrementales de clústeres. No se admite la réplica basada en archivos. **Advertencia:** no intente utilizar el controlador basado en bloques en clústeres con unidades iSCSI compartidas, ya que el clúster terminaría siendo inservible. Consulte “Preparación para proteger clústeres de Windows” en la página 121.
Servidor de clúster de Windows basado en Windows Server 2003 R2	Modelo compatible: *clúster de dispositivo de quórum estándar.* La compatibilidad solo incluye las transferencias de datos basadas en bloques sin controlador para las réplicas incrementales de clústeres. No se admite la réplica basada en archivos. Consulte “Preparación para proteger clústeres de Windows” en la página 121.
Hosts de Hyper-V	
Windows Server 2012 R2 con función Hyper-V Windows Server 2012 con función Hyper-V	Protege un servidor Windows que funciona como host de Hyper-V y sus volúmenes. Protege las máquinas virtuales individuales por separado.

Requisitos de configuración de Windows

Actualizaciones de Windows

Asegúrese de aplicar las actualizaciones de Windows en el sistema de origen antes de ejecutar la primera réplica completa.

Controlador de dominio y software antivirus

Si el equipo Windows es un controlador de dominio, asegúrese también de inhabilitar el software antivirus en el sistema durante la réplica.

1.1.2 Cargas de trabajo Linux compatibles

PlateSpin Protect admite cargas de trabajo de las distribuciones del sistema operativo Linux indicadas en la Tabla 1-2

La réplica de las cargas de trabajo Linux protegidas se produce solo en el nivel de bloques. Consulte “Requisito para controladores `blkwatch` en la página 17.

Tabla 1-2 *Cargas de trabajo Linux compatibles*

Sistema operativo	Versiones	Notas
Servidores		
Red Hat Enterprise Linux (RHEL)	7.0 a 7.3 6.0 a 6.9 5.x. 4.x.	Consulte “Distribuciones de Linux compatibles con Protect” en la página 137 para obtener una lista de las versiones del núcleo de Linux compatibles y de las arquitecturas para las distribuciones de RHEL. PlateSpin Protect no admite el sistema de archivos XFS versión 5 (v5) de RHEL 7.3 y distribuciones basadas en RHEL 7.3. Para las cargas de trabajo Red Hat Enterprise Linux 6.7, Oracle Linux 6.7 y CentOS 6.7 con volúmenes LVM, la réplica incremental solo se admite para la versión más reciente del núcleo (`2.6.32-642.13.1.el6.x86_64`) para la distribución RHEL 6.7. Es el mismo núcleo que se utiliza en la distribución RHEL 6.8.
SUSE Linux Enterprise Server (SLES)	11 SP1 a 11 SP4 10.x. 9.x.	Consulte “Distribuciones de Linux compatibles con Protect” en la página 137 para obtener una lista de las versiones del núcleo de Linux compatibles y de las arquitecturas para las distribuciones de SLES. La versión del núcleo 3.0.13 de SLES 11 SP3 no es compatible. Actualice a la versión del núcleo 3.0.27 o posterior antes de realizar un inventario de la carga de trabajo.
Open Enterprise Server (OES)	2015 SP1 11 SP1 a 11 SP3 2 SP3 Consulte SUSE Linux Enterprise Server (SLES).	Para OES 2015 SP1, Protect es compatible con repositorios NSS de 32 bits de hasta 8 TB de tamaño. No se admiten repositorios NSS de 64 bits. Consulte “Distribuciones de Linux compatibles con Protect” en la página 137 para obtener una lista de las versiones del núcleo de Linux compatibles y de las arquitecturas para las distribuciones de SLES. No se admite la versión por defecto del núcleo, la 3.0.13, en OES 11 SP2. Actualice a la versión del núcleo 3.0.27 o posterior antes de realizar un inventario de la carga de trabajo.

Sistema operativo	Versiones	Notas
Oracle Linux (OL) (anteriormente Oracle Enterprise Linux [OEL])	Consulte Red Hat Enterprise Linux (RHEL).	Consulte “Distribuciones de Linux compatibles con Protect” en la página 137 para obtener una lista de las versiones del núcleo de Linux compatibles y de las arquitecturas para las distribuciones de RHEL. Hay controladores blkwatch disponibles para el núcleo estándar Red Hat Compatible Kernel (RHCK) y el Unbreakable Enterprise Kernel (UEK) en OEL 6 U7 y versiones posteriores, como se indica en la “Lista de distribuciones” en la página 138 Para PlateSpin Protect 11.2 y versiones anteriores no se admiten las cargas de trabajo que usen el núcleo UEK. Para Oracle Linux 6 U7, los controladores blkwatch para la versión 2.6.32-573 del núcleo no admiten la réplica incremental para cargas de trabajo con volúmenes LVM. Actualice el núcleo y utilice los controladores de RHEL 6 U7 para el núcleo 2.6.32-642.
CentOS	Consulte Red Hat Enterprise Linux (RHEL).	Consulte “Distribuciones de Linux compatibles con Protect” en la página 137 para obtener una lista de las versiones del núcleo de Linux compatibles y de las arquitecturas para las distribuciones de RHEL. CentOS 7.*x* requiere VMware 5.5 o posterior.

Requisitos de configuración para cargas de trabajo Linux

Requisito para controladores `blkwatch`

La transferencia de datos basada en bloques para una carga de trabajo Linux requiere un controlador `blkwatch` compilado para la distribución de Linux concreta que se va a proteger. El software de PlateSpin Protect incluye versiones compiladas previamente del controlador `blkwatch` para muchas distribuciones de Linux que no son de depuración (32 bits y 64 bits). También es posible crear un controlador personalizado. Para obtener más información, consulte “Distribuciones de Linux compatibles con Protect” en la página 137.

1.1.3 Contenedores de máquina virtual compatibles

Un contenedor de máquinas virtuales es una infraestructura de protección que actúa como el host de una réplica virtual arrancable y actualizada regularmente de una carga de trabajo protegida.

- “Plataformas VMware compatibles” en la página 18
- “Compatibilidad de clústeres DRS de VMware como contenedores” en la página 19
- “Compatibilidad con VMware vCenter Site Recovery Manager” en la página 19
- “Compatibilidad con multitenencia de Protect en VMware” en la página 19

Plataformas VMware compatibles

Consulte la Tabla 1-3 para obtener una lista de las plataformas VMware compatibles. Las plataformas se admiten como contenedores de protección y como contenedores de failback.

Nota: la protección de cargas de trabajo en un contenedor de máquinas virtuales de destino está sujeta a que el proveedor del host admita el sistema operativo invitado del host. Para obtener información sobre los hosts de VMware de destino, consulte la *Guía de compatibilidad de VMware* (http://www.vmware.com/resources/compatibility/).

La infraestructura de contenedor puede ser un servidor VMware ESXi o un clúster DRS de VMware. Para obtener información sobre los requisitos de configuración de los clústeres DRS de VMware, consulte “Compatibilidad de clústeres DRS de VMware como contenedores” en la página 19.

Tabla 1-3 *Plataformas admitidas como contenedor de máquina virtual*

Contenedor	Versiones	Notas
VMware vCenter o ESXi	6.5	Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 6.5 y solo se puede gestionar en vCenter 6.5.
VMware vCenter o ESXi	6.0 (GA2, U2, U3)	Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 6.0 y solo se puede gestionar en vCenter 6.0.
VMware vCenter o ESXi	5.5 (GA2, U2, U3)	Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 5.5 y solo se puede gestionar en vCenter 5.5.
VMware vCenter o ESXi	5.1 (GA2, U2, U3)	Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 5.1 y solo se puede gestionar en vCenter 5.1.
VMware vCenter o ESXi	4.1 (GA2, U3)	Como contenedor de máquina virtual, el clúster DRS debe contener solo servidores ESXi 4.1 y solo se puede gestionar en vCenter 4.1.

Nota: los hosts de VMware ESXi deben disponer de una licencia pagada. La protección no se admite en estos sistemas si funcionan con una licencia gratuita.

Compatibilidad de clústeres DRS de VMware como contenedores

Para poder ser un destino de protección válido, el clúster DRS de 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 96.

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). No debe definirse como **Manual.**
- Debe compartirse al menos un almacén de datos entre todos los hosts de VMware del clúster VMware.
- Debe existir al menos un vSwitch y un grupo virtual de puertos, o bien un conmutador distribuido de vNetwork, común para todos los hosts de VMware del clúster VMware.
- Las cargas de trabajo de failover (máquinas virtuales) de cada contrato de protección deben situarse exclusivamente en los almacenes de datos, vSwitch y los grupos virtuales de puertos compartidos entre todos los hosts de VMware del clúster VMware.

Compatibilidad con VMware vCenter Site Recovery Manager

PlateSpin Protect admite la copia de máquinas virtuales replicadas en un sitio de recuperación remoto mediante VMware vCenter Site Recovery Manager (SRM). Consulte la Sección 6.7, “Configuración de la compatibilidad con VMware vCenter Site Recovery Manager”, en la página 76.

Compatibilidad con multitenencia de Protect en VMware

PlateSpin Protect admite la multitenencia en VMware. Varios servidores de Protect pueden compartir la misma interfaz final del clúster de VMware. Consulte “Configuración de inquilinos múltiples de Protect en VMware” en la página 57.

1.1.4 Arquitecturas de cargas de trabajo compatibles

PlateSpin Protect admite las arquitecturas de equipos basados en x86 siguientes:

- “Procesador y arquitectura de sistema operativo” en la página 19
- “Núcleos y zócalos para máquinas virtuales de destino” en la página 20
- “CPU virtuales para máquinas virtuales de destino” en la página 20
- “Firmware UEFI y BIOS” en la página 20

Procesador y arquitectura de sistema operativo

PlateSpin Protect admite la protección y recuperación de arquitecturas x64 y x86 para cargas de trabajo físicas y virtuales en su centro de datos:

- 64 bits
- 32 bits

Núcleos y zócalos para máquinas virtuales de destino

Para los contenedores de máquinas virtuales compatibles que usen VMware 5.1 y versiones superiores con un nivel mínimo de hardware de máquina virtual 8, PlateSpin Protect permite especificar el número de zócalos y de núcleos por zócalo para la carga de trabajo de failover. El total de núcleos se calcula automáticamente. Este parámetro se aplica durante la primera instalación de una carga de trabajo con el valor de réplica inicial de **Full** (Réplica completa).

Nota: el número máximo de núcleos que puede usar la carga de trabajo depende de factores externos, como el sistema operativo invitado, la versión del hardware de la máquina virtual, la licencia de VMware para el host de ESXi y la capacidad de cálculo máxima del host de ESXi para vSphere. Consulte *ESXi/ESX Configuration Maximums* (Máximos de configuración ESXi/ESX, en la Base de conocimientos de VMware 1003497) (https://kb.vmware.com/kb/1003497).

Algunas distribuciones de un sistema operativo invitado podrían no respetar la configuración de núcleos o de núcleos por zócalo. Por ejemplo, los sistemas operativos invitados que usan SLES 10 SP4 y OES 2 SP3 conservan la configuración de núcleos y zócalos original de la instalación, mientras que otras distribuciones de SLES, RHEL y OES sí respetan la configuración.

CPU virtuales para máquinas virtuales de destino

Para contenedores de máquinas virtuales que usen VMware 4.1, PlateSpin Protect permite especificar el número necesario de vCPU (CPU virtuales) que se deben asignar a la carga de trabajo de failover. Este parámetro se aplica durante la primera instalación de una carga de trabajo con el valor de réplica inicial de **Full** (Réplica completa). Cada vCPU se presenta al sistema operativo invitado en el contenedor de máquinas virtuales como un único núcleo con un solo zócalo.

Firmware UEFI y BIOS

PlateSpin Protect admite las interfaces de firmware UEFI y BIOS para cargas de trabajo Windows y Linux.

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, debe usar como destino un contenedor vSphere 5.0 o más reciente.

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 una operación de failback de una carga de trabajo Windows 2003 protegida en un equipo físico basado en UEFI, Protect analiza la opción y le informa de que no es válida. Es decir, la transición del firmware de BIOS a UEFI no se admite debido a 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.

En cargas de trabajo Windows, PlateSpin Protect duplica la compatibilidad de Microsoft con cargas de trabajo Windows basadas en UEFI o BIOS. Transfiere las cargas de trabajo del origen al destino, al tiempo que aplica el firmware compatible a los sistemas operativos correspondientes de origen y destino. Se admiten tanto las transferencias basadas en bloques como las basadas en archivos. 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.

1.1.5 Almacenamiento admitido

PlateSpin Protect admite las siguientes configuraciones de almacenamiento para las cargas de trabajo Windows y Linux.

- "Discos de almacenamiento" en la página 21
- "Esquemas de particionamiento" en la página 21
- "Sistemas de archivos de Windows" en la página 22
- "Sistemas de archivos Linux" en la página 22
- "Características del almacenamiento en Linux" en la página 22

Discos de almacenamiento

PlateSpin Protect admite varios tipos de discos de almacenamiento de origen, incluidos los discos básicos, los discos dinámicos Windows, LVM2, RAID y SAN.

Puede especificar si los discos virtuales de la réplica de máquina virtual protegida se provisionan de forma ligera o pesada.

Nota: las advertencias siguientes se aplican a los discos de almacenamiento:

- **Discos dinámicos de Windows:** PlateSpin Protect no admite los discos dinámicos Windows en el destino.

  Para los discos dinámicos, el almacenamiento no sigue la estrategia de asignación "igual que el origen". Tanto los volúmenes dinámicos simples como los distribuidos residirán en la carga de trabajo de destino como discos de volúmenes básicos simples. El disco de destino se particiona como GPT si el tamaño total combinado de los discos miembro del volumen dinámico supera el límite de tamaño de la partición MBR. Para obtener más información, consulte el artículo de *Microsoft TechNet: Understanding the 2 TB limit in Windows Storage* (https://blogs.technet.microsoft.com/askcore/2010/02/18/understanding-the-2-tb-limit-in-windows-storage/) (Explicación del límite de 2 TB en el almacenamiento de Windows).
- **RAID de software de Linux:** PlateSpin Protect no admite cargas de trabajo de Linux con volúmenes en RAID de software.

Esquemas de particionamiento

PlateSpin Protect admite los esquemas de particionamiento MBR (registro de arranque maestro) y GPT (tabla de particiones GUID) para cargas de trabajo Windows y Linux. Las cargas de trabajo y el almacenamiento para la protección deben configurarse en discos particionados con MBR o GPT. Aunque GPT permite hasta 128 particiones por cada disco, PlateSpin Protect solo admite 57 o menos particiones GPT por disco.

Sistemas de archivos de Windows

PlateSpin Protect solo admite el sistema de archivos NTFS en cualquier sistema Windows compatible.

Sistemas de archivos Linux

PlateSpin Protect admite los sistemas de archivos EXT2, EXT3, EXT4, REISERFS, XFS y NSS (solo Open Enterprise Server), solo con transferencia basada en bloques.

Nota: no se admite el sistema de archivos XFS v5 para Red Hat Enterprise Linux 7.3 ni distribuciones basadas en esa versión.

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

Características del almacenamiento en Linux

Para las cargas de trabajo Linux, PlateSpin Protect proporciona la siguiente compatibilidad de almacenamiento adicional:

- 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.
- Los volúmenes de disco en bruto LVM se admiten en configuraciones de tipo "igual que el origen" en las cargas de trabajo Linux.
- (OES 11) Los diseños de gestión de volúmenes de Linux de Novell (NLVM) de las cargas de trabajo de origen se conservan y se vuelven a crear en el contenedor de máquinas virtuales. Los repositorios NSS se copian del origen a la máquina virtual de recuperación.
- (OES 2) Los diseños EVMS de las cargas de trabajo de origen se conservan y se vuelven a crear en el contenedor de máquinas virtuales. Los repositorios NSS se copian del origen a la máquina virtual de recuperación.

1.1.6 Idiomas admitidos

Además de en inglés, PlateSpin Protect proporciona compatibilidad con otros idiomas para la instalación y el uso en equipos configurados en:

- Chino simplificado (zh-cn)
- Chino tradicional (zn-tw)
- Francés (fr)
- Alemán (de)
- Japonés (ja)

Sugerencia: las demás versiones internacionales tienen compatibilidad limitada. En idiomas distintos a los indicados podría verse afectada la actualización de los archivos del sistema.

Hay disponible documentación en línea traducida en estos idiomas, además de en español (es).

Para utilizar la interfaz Web en uno de esos idiomas, consulte “Configuración de idiomas para versiones internacionales” en la página 65.

1.1.7 Navegadores Web compatibles

La mayor parte de la interacción con el producto se realiza a través de la interfaz Web.

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.

Para utilizar la interfaz Web de PlateSpin Protect en uno de los idiomas admitidos, consulte “Configuración de idiomas para versiones internacionales” en la página 65.

1.2 Métodos de transferencia de datos admitidos

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

- Sección 1.2.1, “Métodos de transferencia de datos compatibles para cargas de trabajo Windows”, en la página 23
- Sección 1.2.2, “Método de transferencia compatible para cargas de trabajo Linux”, en la página 24

1.2.1 Métodos de transferencia de datos compatibles para 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 archivos de Windows:** (solo en Windows) los datos se replican archivo a archivo.
- **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. Aprovecha el Servicio de instantáneas de volumen de Microsoft (VSS) y las aplicaciones y servicios que admite 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 rearrancar la carga de trabajo protegida. No es necesario rearrancar 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 rearranque 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. La réplica compara cada bloque del disco y copia solo los cambios.

  Con esta opción no es necesario rearrancar, pero su rendimiento es inferior a la del componente basado en bloques.

1.2.2 Método de transferencia compatible para cargas de trabajo Linux

Para cargas de trabajo Linux, PlateSpin Protect admite solo la transferencia de datos basada en bloques con un controlador block-watch (`blkwatch`).

Nota: la distribución o eliminación del controlador `blkwatch` es transparente, no afecta a la continuidad y no requiere intervención del usuario ni rearrancar.

La distribución de PlateSpin Protect incluye controladores `blkwatch` precompilados para cargas de trabajo con núcleos estándares no de depuración de las distribuciones Linux compatibles. Consulte la Sección B.2, “Controladores blkwatch precompilados para distribuciones Linux”, en la página 138.

Si las cargas de trabajo tienen un núcleo no estándar, personalizado o más reciente, puede crear un controlador `blkwatch` personalizado para el núcleo específico. Consulte el artículo 7005873 de la base de conocimientos: *How to Build a Custom Block-Based Linux Kernel Driver* (https://www.netiq.com/support/kb/doc.php?id=7005873) (Cómo crear un controlador de núcleo de Linux personalizado basado en bloques).

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, “Cifrado de datos durante la transmisión”, en la página 24
- Sección 1.3.2, “Seguridad de las comunicaciones entre los clientes y el servidor”, en la página 25
- Sección 1.3.3, “Seguridad de las credenciales”, en la página 25
- Sección 1.3.4, “Autorización y autenticación de usuarios”, en la página 25
- Sección 1.3.5, “Autenticación de Windows para la base de datos de Microsoft SQL Server”, en la página 25
- Sección 1.3.6, “Cortafuegos y configuración del puerto”, en la página 25

1.3.1 Cifrado de datos durante la transmisión

El cifrado de transferencia hace que la transmisión de los datos de la carga de trabajo sea más segura durante la réplica de la carga de trabajo. Si el cifrado está habilitado, la transferencia de datos en red del origen al destino se cifra mediante el estándar avanzado de cifrado (AES).

Nota: el cifrado de datos afecta al rendimiento y podría ralentizar la transferencia de datos hasta en un 30 %.

Es posible habilitar o inhabilitar el cifrado individualmente para cada carga de trabajo. Para ello, se selecciona la opción **Encrypt Data Transfer** (Cifrar transferencia de datos). Consulte la “Detalles de protección de la carga de trabajo” en la página 153.

1.3.2 Seguridad de las comunicaciones entre los clientes y el servidor

El servidor de PlateSpin habilita SSL en el host del servidor de PlateSpin, de forma que la transmisión de datos sea segura entre el navegador Web y el servidor de PlateSpin con 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

PlateSpin Protect protege las credenciales mediante una conexión SSL para las comunicaciones y la biblioteca de cifrado de Windows para cifrar las contraseñas.

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 “Configuración de la autorización y la autenticación de usuarios” en la página 53.

1.3.5 Autenticación de Windows para la base de datos de Microsoft SQL Server

PlateSpin Protect proporciona la capacidad para usar la autenticación de Windows para acceder a la base de datos de Microsoft SQL Server. Consulte “Requisitos para la autenticación de Windows para la base de datos de Microsoft SQL Server” en la página 34.

1.3.6 Cortafuegos y configuración del puerto

La Tabla 1-4 muestra los puertos por defecto que se usan en PlateSpin Protect. Si configura puertos personalizados, deberá abrirlos. Para las comunicaciones entre el servidor de PlateSpin y las máquinas de origen y de destino que gestiona, asegúrese de abrir también los puertos adecuados en los cortafuegos presentes entre ellos. El tráfico de las comunicaciones es bidireccional (entrante y saliente). Consulte también “Requisitos de acceso y comunicación en la red de protección” en la página 31.

Tabla 1-4 *Puertos por defecto usados por PlateSpin Protect*

Número de puerto	Protocolo	Función	Detalles
80	TCP	HTTP	(No seguro) Se usa para la comunicación HTTP entre el host del servidor de PlateSpin y los equipos de origen y de destino que gestiona. Abra este puerto en el host del servidor de PlateSpin, en las cargas de trabajo de origen y de destino y en los hosts ESXi de VMware.
443	TCP	HTTPS	(Seguro) Se usa para la comunicación HTTPS, en caso de que SSL esté habilitado, entre el host del servidor de PlateSpin y los equipos de origen y de destino. Abra este puerto en el host del servidor de PlateSpin, en las cargas de trabajo de origen y de destino, en los hosts ESXi de VMware y en el servidor host de vCenter.
3725	TCP	Transferencia de datos	Se usa para transferir datos entre los equipos de origen y de destino, incluida la transferencia basada en archivos y la transferencia basada en bloques. Abra este puerto en los equipos de origen y de destino para todas las cargas de trabajo. Los cortafuegos entre un origen y su destino también deben permitir el puerto TCP 3725. Consulte “Configuraciones compatibles” en la página 13.
135 445	TCP	RPC/DCOM	Se usa para la comunicación RPC/DCOM en los equipos Windows durante el proceso de descubrimiento y al tomar el control del equipo de origen y rearrancarlo. Abra estos puertos para la comunicación entre las máquinas de origen y de destino para todas las cargas de trabajo Windows. Consulte “Cargas de trabajo Windows compatibles” en la página 14.
137 138 139	TCP	NetBIOS	Se usa para la comunicación NetBIOS (servicio de nombre, servicio de datagrama y servicio de sesión). Abra estos puertos para la comunicación entre las máquinas de origen y de destino para todas las cargas de trabajo Windows. Consulte “Cargas de trabajo Windows compatibles” en la página 14.
137 138	UDP	SMB	Se usa para la comunicación SMB a fin de transferir el archivo de la carpeta de toma de control y transferir los archivos del servidor de PlateSpin al equipo de origen. Abra estos puertos en el host del servidor de PlateSpin y en las cargas de trabajo de origen.
139 445	TCP	SMB	
22	TCP		Se usa para la comunicación SSH y SCP en equipos Linux durante el proceso de descubrimiento. Abra este puerto en las máquinas de origen y de destino para todas las cargas de trabajo Linux. Consulte “Cargas de trabajo Linux compatibles” en la página 15.

Número de puerto	Protocolo	Función	Detalles
25	TCP	SMTP	Se usa para el tráfico SMTP si la notificación por correo electrónico está habilitada. Abra este puerto en el host del servidor de PlateSpin y en el host de transmisión de correo.
25	UDP	SMTP	
1433	TCP	SQL	Se usa para la comunicación de Microsoft SQL Server con fines de autenticación y para el intercambio de datos con un dispositivo SQL Server remoto. Abra los puertos SQL en el host del servidor de PlateSpin y en el host remoto de SQL Server, así como en todos los cortafuegos que haya entre ellos. Para obtener más información sobre los requisitos de puertos de SQL Server, consulte el artículo *Configure the Firewall to Allow Server Access* (Configuración del cortafuegos para permitir el acceso del servidor) en Microsoft Developers Network.
1434	TCP	SQL	Se usa para la conexión del administrador dedicada de Microsoft SQL Server.
1434	UDP	SQL	Se usa para las instancias con nombre de Microsoft SQL Server. Este puerto puede ser necesario si usa instancias con nombre en un servidor SQL Server remoto.
49152 a 65.535	TCP	SQL	Se usa para Microsoft SQL Server o RPC para LSA, SAM y Netlogon. Si ha configurado Microsoft SQL Server para que use un puerto TCP específico, debe abrir dicho puerto en el cortafuegos. Consulte “Requisitos para la autenticación de Windows para la base de datos de Microsoft SQL Server” en la página 34.

1.4 Rendimiento

- Sección 1.4.1, “Acerca de las características de rendimiento del producto”, en la página 28
- Sección 1.4.2, “Especificaciones de RPO, RTO y TTO”, en la página 28
- Sección 1.4.3, “Compresión de datos”, en la página 29
- Sección 1.4.4, “Regularización del ancho de banda”, en la página 29
- Sección 1.4.5, “Capacidad de ampliación”, en la página 30
- Sección 1.4.6, “Servidor de base de datos”, en la página 30

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 Especificaciones de RPO, RTO y TTO

En su entorno de protección, tendrá expectativas diferentes para los puntos de recuperación y los tiempos de recuperación necesarios para distintas cargas de trabajo.

- **Objetivos de punto de recuperación (RPO):** el valor de RPO describe la cantidad tolerable de pérdida de datos definido en tiempo en caso de que se produzca una interrupción importante del servicio de TI. El RPP se define como un intervalo configurable entre las réplicas incrementales de una carga de trabajo protegida.

  El RPO 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):** el valor de RTO describe el tiempo de inactividad tolerable de la carga de trabajo definido por el tiempo que una operación de failover tarda en completarse. La operación de failover devuelve una carga de trabajo de failover en línea para sustituir temporalmente una carga de trabajo de producción protegida.

  El RTO se ve afectado por el tiempo que se tarda en configurar y ejecutar la operación de failover (de 10 a 45 minutos). Consulte “Failover” en la página 157.
- **Objetivos de tiempo de prueba (TTO):** el valor de TTO describe el tiempo necesario para probar la recuperación tras fallos con cierta certeza de restauración de servicios. Es similar al RTO, pero incluye el tiempo necesario para que un usuario pruebe la carga de trabajo de failover.

  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 159.

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.

Cuando se prueba la respuesta de failover, se deben tener en cuenta los valores reales asociados con los ajustes RPO, RTO y TTO configurados:

- **Punto de recuperación real (RPA):** el RPA es la pérdida de datos real medida en tiempo y definida según el intervalo real medido entre réplicas incrementales de una carga de trabajo protegida que se produce durante una prueba de failover. El RPA también se denomina *Objetivo de punto de recuperación real* (RPO real).
- **Tiempo de recuperación real (RTA):** el RTA es una medida del tiempo de inactividad real de la carga de trabajo definido por el tiempo que una operación de failover tarda en completarse. El RTA también se denomina *Objetivo de tiempo de recuperación real* (RTO real).
- **Tiempo de prueba real (TTA):** el TTA es una medida del tiempo real en el que se puede probar un plan de recuperación tras fallos. Es similar al RTO real, pero incluye el tiempo necesario para que un usuario pruebe la carga de trabajo de failover. El TTA también se denomina *Objetivo de tiempo de prueba real* (RTO real).

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 182.

1.4.3 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 168.

1.4.4 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 168.

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 simultáneas) 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.

1.4.6 Servidor de base de datos

PlateSpin Protect incluye Microsoft SQL Server Express Edition. Las capacidades de SQL Server Express son suficientes para un único servidor de PlateSpin que proteja hasta 50 cargas de trabajo (consulte la Sección 1.4.5, “Capacidad de ampliación”, en la página 30).

Nota: Microsoft SQL Server Express tiene un límite de tamaño de base de datos de 10 GB y solo puede utilizar un núcleo de CPU a la vez. Para obtener más información sobre los requisitos y las limitaciones de SQL Server Express, consulte la documentación de Microsoft SQL Server 2014 Express (https://www.microsoft.com/en-us/download/details.aspx?id=42299).

La instancia de base de datos del servidor de PlateSpin puede crecer hasta 0,5 GB por mes y cada carga de trabajo, según el número de réplicas incrementales que se hayan programado. Se recomienda archivar o descartar periódicamente los datos de informes históricos para dejar espacio a los nuevos datos de informes.

En un clúster DRS de VMware, asegúrese de equilibrar los destinos de protección entre varios hosts en el clúster para conseguir un rendimiento óptimo.

Es recomendable configurar el servidor de PlateSpin para que utilice una instancia de la base de datos en el servidor de base de datos existente de Microsoft SQL Server Standard Edition o Enterprise Edition en los siguientes entornos:

- Distribuciones de varios servidores de PlateSpin que utilicen el mismo servidor de base de datos de Microsoft SQL Server remoto para las instancias de base de datos.
- Distribuciones en las que sea importante conservar todo el historial de los datos de informes.

Aunque varios servidores de PlateSpin pueden utilizar el mismo servidor de base de datos remoto, cada servidor requiere una instancia de base de datos independiente.

Para configurar una instancia de base de datos remota para el servidor de PlateSpin, consulte “Configuración del servidor de base de datos de Microsoft SQL Server remoto” en la *Guía de instalación y actualización de PlateSpin Protect*.

1.5 Requisitos de acceso y comunicación en la red de protección

Antes de configurar las cargas de trabajo para la protección y la recuperación, asegúrese de configurar la red con los valores de acceso y de comunicaciones descritos en esta sección.

- Sección 1.5.1, “Requisitos de red para la interfaz Web del host del servidor de PlateSpin”, en la página 31
- Sección 1.5.2, “Requisitos de red para los contenedores”, en la página 31
- Sección 1.5.3, “Requisitos de red para las cargas de trabajo”, en la página 32
- Sección 1.5.4, “Requisitos para la autenticación de Windows para la base de datos de Microsoft SQL Server”, en la página 34
- Sección 1.5.5, “Requisitos para la protección en redes públicas y privadas mediante NAT”, en la página 35
- Sección 1.5.6, “Requisitos para que el servidor de PlateSpin funcione con NAT”, en la página 36
- Sección 1.5.7, “Anulación de la shell bash por defecto para ejecutar comandos en cargas de trabajo Linux”, en la página 36

1.5.1 Requisitos de red para la interfaz Web del host del servidor de PlateSpin

En la Tabla 1-5 se describen los puertos que deben estar abiertos en el host del servidor de PlateSpin para permitir el acceso a la interfaz Web.

Tabla 1-5 *Requisitos de apertura de puertos para el host del servidor de PlateSpin*

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

1.5.2 Requisitos de red para los contenedores

La Tabla 1-6 describe los requisitos de software, redes y cortafuegos para los contenedores de cargas de trabajo admitidos.

Tabla 1-6 *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)	
Todos los contenedores de VMware. Consulte “Contenedores de máquina virtual compatibles” en la página 17.	◆ Cuenta de VMware con función de administrador ◆ API de servicios Web de VMware y API de gestión de archivos	HTTPS (TCP 443)

Sistema	Requisitos previos	Puertos necesarios (por defecto)
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)

1.5.3 Requisitos de red para las cargas de trabajo

La Tabla 1-7 describe los requisitos de software, redes y cortafuegos para las cargas de trabajo que pretende proteger mediante PlateSpin Protect.

Tabla 1-7 *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. Consulte "Cargas de trabajo Windows compatibles" en la página 14.	◆ Microsoft .NET Framework 3.5 Service Pack 1 ◆ Microsoft .NET Framework 4.0 Para el descubrimiento, las cargas de trabajo de origen deben ejecutar Microsoft .NET Framework 2 SP2 o versiones posteriores.	
Todas las cargas de trabajo de clúster de Windows Server. Consulte Clústeres en "Cargas de trabajo Windows compatibles" en la página 14.	Asegúrese de que el servidor de PlateSpin puede resolver la búsqueda directa de DNS y la búsqueda inversa de las direcciones IP del clúster de Windows Server y en sus nodos de clúster. Es posible actualizar el servidor DNS o actualizar el archivo `hosts` local (`%systemroot%\system32\drivers\etc\hosts`) en el host del servidor de PlateSpin.	

Tipo de carga de trabajo	Requisitos previos	Puertos necesarios (por defecto)
Todas las cargas de trabajo Windows. Consulte "Cargas de trabajo Windows compatibles" en la página 14.	◆ Credenciales de cuenta de `administrador` o de administrador del dominio incorporadas (no es suficiente solo ser miembro del grupo de administradores). ◆ El Firewall de Windows debe estar configurado para permitir la opción **Compartir archivos e impresoras.** Use una de estas opciones: ◆ **Opción 1, uso del Firewall de Windows:** use el elemento básico del Panel de control **Firewall de Windows** (`firewall.cpl`) y seleccione **Compartir archivos e impresoras** en la lista de excepciones. - O bien - ◆ **Opción 2, uso del Firewall con seguridad avanzada:** use la utilidad Firewall de Windows con seguridad avanzada (`wf.msc`) con la opción **Reglas de entrada** habilitada y definida como `Permitir`: ◆ **Compartir archivos e impresoras (solicitud eco: ICMPv4In)** ◆ **Compartir archivos e impresoras (solicitud eco: ICMPv6In)** ◆ **Compartir archivos e impresoras (datagrama NB de entrada)** ◆ **Compartir archivos e impresoras (nombre NB de entrada)** ◆ **Compartir archivos e impresoras (sesión NB de entrada)** ◆ **Compartir archivos e impresoras (SMB de entrada)** ◆ **Compartir archivos e impresoras (administrador de trabajos de impresión: RPC)** ◆ **Compartir archivos e impresoras (administrador de trabajos de impresión: RPC-EPMAP)**	TCP 3725 NetBIOS (TCP 137 - 139) SMB (TCP 139, 445 y UDP 137, 138) RPC (TCP 135, 445)
Windows Server 2003 (incluidos SP1 Standard, SP2 Enterprise y R2 SP2 Enterprise).	**Nota:** después de habilitar los puertos necesarios, ejecute el comando siguiente en el indicador del servidor para habilitar la administración remota de PlateSpin: `netsh firewall set service RemoteAdmin enable` Para obtener más información sobre netsh, consulte el artículo de Microsoft TechNet *La utilidad de línea de comandos Netsh* (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx).	TCP 3725, 135, 139, 445 UDP 137, 138, 139

Tipo de carga de trabajo	Requisitos previos	Puertos necesarios (por defecto)
Todas las cargas de trabajo Linux. Consulte “Cargas de trabajo Linux compatibles” en la página 15.	Servidor de shell segura (SSH)	TCP 22, 3725

1.5.4 Requisitos para la autenticación de Windows para la base de datos de Microsoft SQL Server

PlateSpin Protect proporciona la capacidad para usar la autenticación de Windows para acceder a la base de datos de Microsoft SQL Server. Debe configurar Active Directory y abrir puertos en el cortafuegos para permitir la autenticación.

Para habilitar la autenticación de Windows en las base de datos de SQL:

1. Asegúrese de que configura Microsoft SQL Server de forma que permita tanto conexiones TCP/IP como conexiones de conducto nombrado.
2. (Condicional) Si tiene previsto usar la autenticación de Windows para acceder a la base de datos de Microsoft SQL Server, debe configurar lo siguiente en Active Directory:
   - Debe añadir el servidor de base de datos Microsoft SQL Server al dominio.
   - Necesita dos cuentas de usuario de dominio para la instalación de PlateSpin Protect.
     - **Un usuario de dominio con el conjunto de funciones `sysadmin`:** este usuario con derechos de administración de SQL es necesario para crear bases de datos, tablas y otros objetos de esquema.
     - **Un usuario de servicio de PlateSpin:** el usuario de servicio puede ser un usuario de dominio con pocos privilegios del dominio. Sin embargo, el usuario de servicio debe ser un administrador local en el servidor de PlateSpin Protect y debe tener asignado dicho permiso antes de la instalación.

       Si la contraseña del usuario de Windows cambia, debe actualizarla para el usuario de servicio de PlateSpin y el grupo de aplicaciones de IIS. Para evitar esta situación, puede ser conveniente utilizar un usuario de Windows cuya contraseña no caduque nunca.

   Nota: si usa la autenticación de Windows, deberá entrar como usuario del dominio con derechos de administración de SQL cuando actualice el servidor de PlateSpin.
3. Abra los puertos siguientes en el cortafuegos para admitir la autenticación en SQL Server:
   - **Puertos 49152-65535/TCP:** permiten el tráfico de RPC para LSA, SAM y Netlogon.
   - **Puerto 1433/TCP:** permite el tráfico de Microsoft SQL Server.
   - **Puertos personalizados:** si configura SQL Server para que use un puerto TCP personalizado, debe abrir dicho puerto en el cortafuegos.

   Nota: si no usa puertos dinámicos, debe especificar el puerto dedicado en el campo **Database Server** (Servidor de base de datos).

4 (Condicional) Si desea usar puertos dedicados con PlateSpin Protect, debe abrirlos en el cortafuegos:

4a En el servidor de base de datos, determine qué puertos deben abrirse:

4a1 En Administrador de configuración de SQL Server, seleccione **Protocolos para SQLExpress > TCP/IP**, haga clic con el botón secundario y seleccione **Propiedades.**

4a2 En el recuadro de diálogo seleccione la pestaña **Direcciones IP.**

4a3 En **IPAll** (o en el protocolo que desee), si **Puerto TCP** o **Puertos TCP dinámicos** tienen cualquier valor distinto a 0, abra los puertos especificados en el cortafuegos. Estos son los puertos que se usan para conectarse a SQL Server.

Por ejemplo, si el campo **Puertos TCP dinámicos** tiene el valor 60664 y el campo **Puerto TCP** tiene el valor 1555, debe habilitar los puertos 60664 y 1555 en las reglas del cortafuegos de SQL Server.

4b Abra los puertos en el cortafuegos.

Nota: si tiene un valor definido para los puertos dinámicos, puede que su servidor no aparezca en la lista de servidores SQL cuando haga clic en **Examinar.** En tal caso, deberá especificar el servidor manualmente en el campo de entrada **Database Server** (Servidor de base de datos) de la instalación de PlateSpin Protect.

Por ejemplo, si el nombre del servidor es `MISQLSERVER`, el nombre de la instancia de la base de datos es `SQLEXPRESS` y el puertos dedicado definido para el puerto dinámico es `60664`, deberá indicar el texto siguiente y seleccionar el tipo de autenticación que desee:

```
MISQLSERVER\SQLEXPRESS,60664
```

Debe abrir los puertos en el cortafuegos.

1.5.5 Requisitos para la 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:** con la herramienta de configuración de PlateSpin, registre las direcciones IP adicionales asignadas al host del servidor de PlateSpin. Consulte “Requisitos para que el servidor de PlateSpin funcione con NAT” en la página 36.
- **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 161).
- **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 PlateSpin o una de sus direcciones públicas (externas) registradas en la base de datos de configuración de PlateSpin del servidor. Consulte “Requisitos para que el servidor de PlateSpin funcione con NAT” en la página 36.

1.5.6 Requisitos para que el servidor de PlateSpin funcione con NAT

El servidor de PlateSpin necesita direcciones IP adicionales para poder funcionar en entornos que tengan habilitada la traducción de direcciones de red (NAT, por sus siglas en inglés). Consulte “Requisitos para que el servidor de PlateSpin funcione con NAT” en la página 36.

1.5.7 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 base de conocimientos *Linux Default Shell Override Procedure* (https://www.netiq.com/support/kb/doc.php?id=7010676) (Procedimiento de sustitución de shell por defecto de Linux).

2 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. La mayoría de estos pasos se representan mediante comandos de la carga de trabajo en la página Workloads (Cargas de trabajo). Consulte “Comandos de protección y recuperación de cargas de trabajo” en la página 45.

Tabla 2-1 *Ciclo de vida de protección y recuperación*

Tarea	Acción	Observaciones
Preparación Asegúrese de que las cargas de trabajo, los contenedores y el entorno cumplen los criterios necesarios.		
	1. Asegúrese de que PlateSpin Protect admite la carga de trabajo.	Consulte “Configuraciones compatibles” en la página 13.
	2. Asegúrese de que las cargas de trabajo y los contenedores de máquina virtual cumplen los requisitos previos de acceso y red.	Consulte “Requisitos de acceso y comunicación en la red de protección” en la página 31.
Inventario 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.		
	3. Añada los contenedores de destino al servidor de PlateSpin.	Consulte “Adición de contenedores (destinos de protección)” en la página 96.
	4. Añada las cargas de trabajo de destino al servidor de PlateSpin.	Consulte “Adición de cargas de trabajo (orígenes de protección)” en la página 100.
	5. Para un destino de protección física, prepare los controladores del dispositivo.	Consulte Capítulo 11, “Preparación de controladores de dispositivos para los destinos de failback físicos”, en la página 105.
	6. Para una carga de trabajo Linux, prepare la protección de la carga de trabajo:	Consulte Capítulo 12, “Preparación para proteger cargas de trabajo Linux”, en la página 117.
	7. Para cargas de trabajo de clúster de Windows Server, prepare la protección de la carga de trabajo de clúster.	Consulte Capítulo 13, “Preparación para proteger clústeres de Windows”, en la página 121.

Tarea	Acción	Observaciones
Definir el contrato de protección		
	8. Defina la información y las especificaciones de un contrato de protección.	Consulte “Configuración de los detalles de protección y preparación de la réplica” en la página 151.
	9. Prepare la réplica.	
Iniciar la protección		
	10. Comience el contrato de protección según sus requisitos.	Consulte “Inicio de la protección de la carga de trabajo” en la página 156.
Tareas del ciclo de vida de protección (opcionales) 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.		
	11. *Incremental manual*. Es posible ejecutar una réplica incremental manual, fuera del contrato de protección de la carga de trabajo.	Seleccione la carga de trabajo y haga clic en **Run Incremental** (Ejecutar réplica incremental).
	12. *Prueba*. Es posible probar la función de failover en un ambiente y de forma controlada.	Consulte Uso de la función de prueba de failover.
Failover		
	13. 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” en la página 157.
Failback		
	14. Este paso corresponde a la fase de reanudación empresarial después de sufrir problemas con la carga de trabajo de producción.	Consulte “Failback” en la página 160.
Reprotección		
	15. 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 164. Después de una operación de failback correcta, aparece disponible el comando **Reprotect** (Volver a proteger).

Gestión del servidor de PlateSpin

Esta sección proporciona la información que necesita para activar su licencia de PlateSpin Protect y personalizar el producto de PlateSpin para su entorno. Familiarícese con las herramientas de PlateSpin y las opciones de configuración. Puede volver a esta sección cuando lo necesite para gestionar las licencias o los usuarios, o bien para personalizar la configuración.

- Capítulo 3, “Uso de las herramientas de PlateSpin”, en la página 41
- Capítulo 4, “Gestión de licencias”, en la página 49
- Capítulo 5, “Configuración de la autorización y la autenticación de usuarios”, en la página 53
- Capítulo 6, “Configuración de la aplicación del servidor de PlateSpin”, en la página 65
- Capítulo 7, “Configuración de la interfaz Web de PlateSpin”, en la página 79
- Capítulo 8, “Gestión de varios servidores de PlateSpin en la consola de gestión”, en la página 83
- Apéndice A, “Cambio de marca de la interfaz Web de PlateSpin Protect”, en la página 87

3 Uso de las herramientas de PlateSpin

La mayor parte de la interacción con el producto se realiza a través de la interfaz Web. También puede configurar los parámetros globales para la aplicación de servidor de PlateSpin mediante la página de configuración de PlateSpin basada en Web.

- Sección 3.1, “Lanzamiento de la interfaz Web”, en la página 41
- Sección 3.2, “Descripción general de la consola”, en la página 42
- Sección 3.3, “Descripción general de las cargas de trabajo”, en la página 45
- Sección 3.4, “Comandos de protección y recuperación de cargas de trabajo”, en la página 45
- Sección 3.5, “Otras herramientas de gestión del servidor de PlateSpin”, en la página 47

3.1 Lanzamiento de la interfaz Web

1. (Opcional) Configure el servidor de PlateSpin y el navegador Web para utilizar uno de los idiomas admitidos en lugar del inglés. Consulte “Configuración de idiomas para versiones internacionales” en la página 65.
2. Abra un navegador Web compatible y diríjase a:

   `https://Servidor_de_PlateSpin/Protect`

   Sustituya *`Servidor_de_PlateSpin`* por el nombre de host DNS o la dirección IP del host del servidor de PlateSpin.

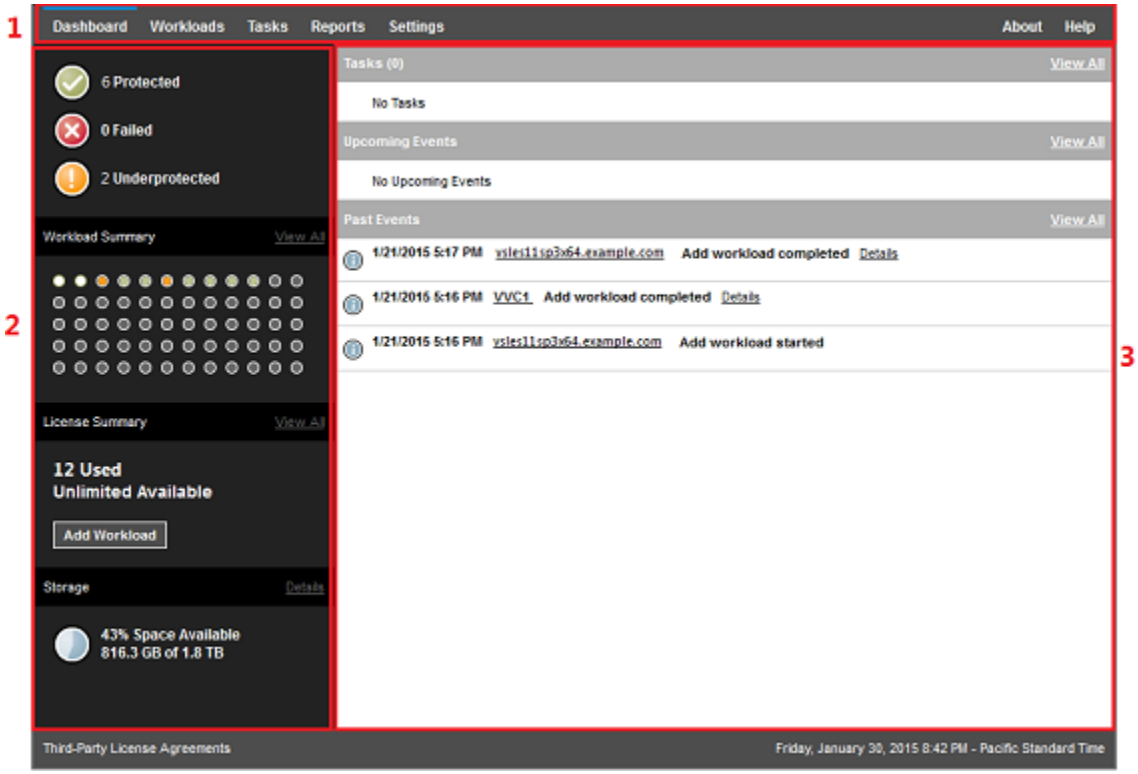
   Si SSL no está habilitado, use `http` en la URL.
3. Entre con las credenciales del administrador para el host del servidor de PlateSpin.

   Para obtener información sobre cómo configurar usuarios adicionales para PlateSpin, consulte la Capítulo 5, “Configuración de la autorización y la autenticación de usuarios”, en la página 53.

3.2 Descripción general de la consola

La página Dashboard (Consola) de la interfaz Web de PlateSpin Protect 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 43
- Sección 3.2.2, “Panel de resumen visual”, en la página 43
- Sección 3.2.3, “Panel de tareas y eventos”, en la página 44

Nota: es posible modificar determinados elementos de la interfaz Web para que se adapten a la marca de su organización. Para obtener más información, consulte “Cambio de marca de la interfaz Web de PlateSpin Protect” en la página 87.

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 “Descripción general de las cargas de trabajo” en la página 45.
- **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 182.
- **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 168.
  - **Workload Tags (Etiquetas de carga de trabajo):** consulte la “Creación y gestión de etiquetas de cargas de trabajo” en la página 79.
  - **Permissions (Permisos):** consulte “Configuración de la autorización y la autenticación de usuarios” en la página 53.
  - **Containers (Contenedores):** Consulte “Adición de contenedores (destinos de protección)” en la página 96.
  - **Notification Settings (Configuración de notificación):** “Habilitación de las notificaciones de eventos” en la página 68.
  - **Replication Reports Settings (Configuración de informes de réplica):** “Habilitación de informes de réplica” en la página 69
  - **SMTP:** consulte “Configuración de SMTP para el servicio de notificación por correo electrónico” en la página 67.
  - **Licenses (Licencias):** consulte la “Activación de la licencia del producto” en la página 49.

3.2.2 Panel de resumen visual

El panel Visual Summary (Resumen visual) indica el estado de protección de alto nivel de las cargas de trabajo del inventario, el estado de cada carga de trabajo con licencia, un resumen de uso de las licencias y la cantidad de espacio de almacenamiento disponible.

Estado de protección

El estado de protección general de las cargas de trabajo del inventario se representa mediante tres categorías:

- **Protected (Protegidas):** indica el número de cargas de trabajo protegidas de forma activa.
- **Failed (Erróneo):** 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.

Resumen de la carga de trabajo

La sección Workload Summary (Resumen de la carga de trabajo) muestra el estado de cada carga de trabajo con licencia que aparece en la página Workloads (Cargas de trabajo). El número máximo de iconos de punto de estado de las cargas de trabajo coincide con el número de licencias de cargas de trabajo instaladas en el servidor de PlateSpin. En caso de las licencias ilimitadas, el resumen muestra 96 iconos de puntos. En la Tabla 3-1 se describen los distintos estados de las cargas de trabajo representados mediante iconos de punto.

Los iconos representan a las cargas de trabajo y se muestran en orden alfabético. 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.

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

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

Resumen de licencia

La sección License Summary (Resumen de licencia) muestra el número de licencias instaladas y el número de licencias usadas actualmente por las cargas de trabajo.

Almacenamiento

La sección **Storage** (Almacenamiento) proporciona información sobre la cantidad total de espacio de almacenamiento del contenedor para PlateSpin Protect, así como el espacio que hay actualmente en uso.

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 los servicios de notificación por correo electrónico para eventos e informes de réplica” en la página 67.

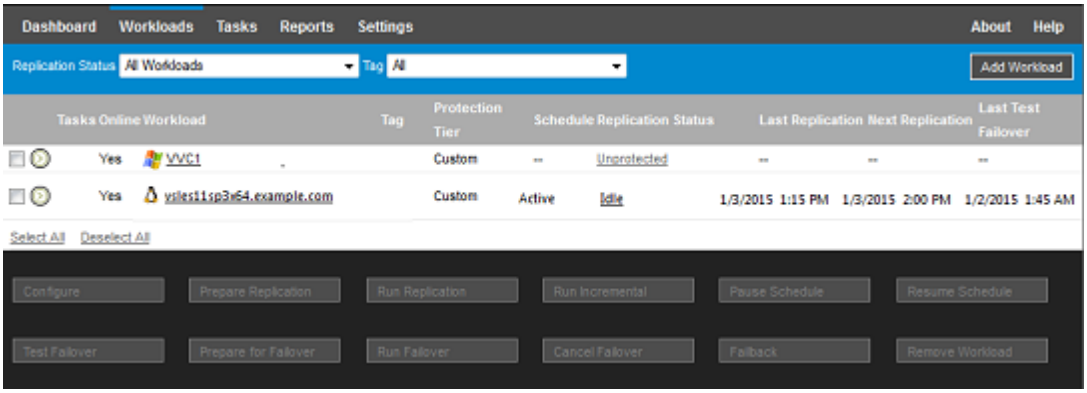
Las tareas son comandos especiales relacionados con eventos que requieren la intervención del usuario. Por ejemplo, al completar un comando de prueba de failover, el sistema genera un evento asociado con dos tareas: `Mark Test as Success` (Marcar prueba como correcta) y `Mark Test as Failure` (Marcar 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 Descripción general de las cargas 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. La lista de cargas de trabajo muestra información sobre la disponibilidad de la carga de trabajo (si está en línea o sin conexión), la etiqueta, el nivel de protección, el estado de réplica y los tiempos de ejecución, así como de la hora del último failover de prueba.

Figura 3-2 *Página Workloads (Cargas de trabajo)*

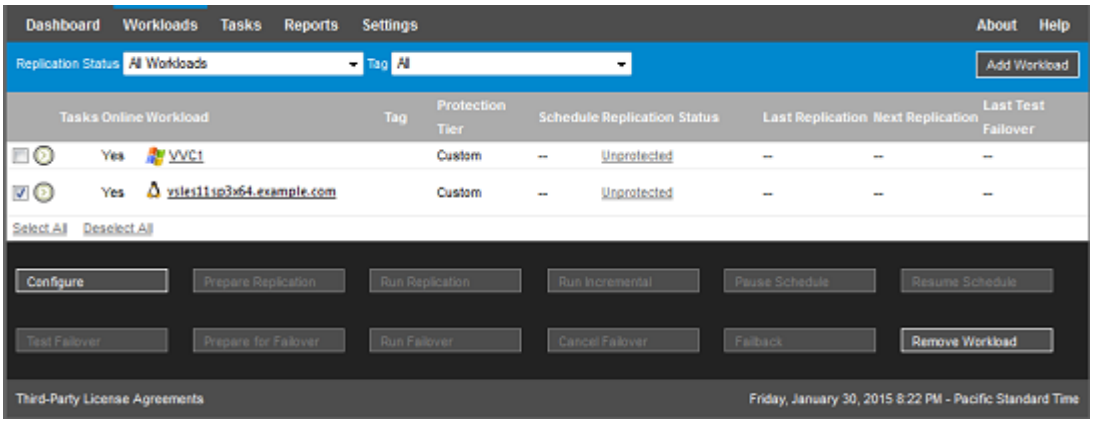


Nota: todas las marcas horarias muestran la zona horaria del host del servidor de PlateSpin. Puede ser distinta a la zona horaria de la carga de trabajo protegida o del host en el que se ejecute la interfaz Web. En la parte inferior derecha de la ventana del cliente se muestra la fecha y la hora del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

3.4 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*



En la Tabla 3-2 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
Configure (Configurar)	Inicia la configuración de protección de la carga de trabajo con parámetros aplicables a una carga de trabajo en inventario.
Prepare Replication (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.
Run Replication (Ejecutar réplica)	Inicia la réplica de la carga de trabajo de acuerdo con los parámetros especificados (réplica completa).
Run Incremental (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.
Pause Schedule (Pausar programación)	Suspende la protección. Todas las réplicas programadas se omiten hasta que se reanuda la programación.
Resume Schedule (Reanudar programación)	Reanuda la protección según los valores de protección guardados.
Test Failover (Probar failover)	Arranca y configura la carga de trabajo de failover en un entorno aislado dentro del contenedor para realizar pruebas.
Prepare for Failover (Preparar para failover)	Arranca la carga de trabajo de failover para preparar una operación de failover.
Run Failover (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.
Cancel Failover (Cancelar failover)	Aborta el proceso de failover.
Failback	Tras una operación de failover, devuelve la carga de trabajo de failover a su infraestructura original o a una nueva (virtual o física).
Reprotect (Volver a proteger)	Después de una operación de failback correcta, la opción Reprotect (Volver a proteger) está disponible.

Comando de carga de trabajo	Descripción
Remove Workload (Eliminar carga de trabajo)	Elimina una carga de trabajo del inventario.

3.5 Otras herramientas de gestión del servidor de PlateSpin

- Sección 3.5.1, “Configuración de PlateSpin”, en la página 47
- Sección 3.5.2, “Utilidad Protect Agent”, en la página 48
- Sección 3.5.3, “Herramienta VMware Role”, en la página 48

3.5.1 Configuración de PlateSpin

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 en:

`https://Servidor_de_PlateSpin/platespinconfiguration/`

Nota: en circunstancias normales, estos valores no se deben modificar a no ser que se lo indique el servicio técnico de PlateSpin.

Para cambiar y aplicar cualquier parámetro de configuración:

1. En cualquier navegador Web, abra

   `https://Servidor_de_PlateSpin/platespinconfiguration/`
2. Busque el parámetro de servidor necesario y cambie su valor.
3. Guarde la configuración y salga de la página.

   No es necesario rearrancar ni reiniciar los servicios de PlateSpin para aplicar los cambios.

Los temas siguientes proporcionan información sobre situaciones concretas en las que puede ser necesario cambiar el comportamiento del producto mediante los parámetros de configuración de PlateSpin:

- “Requisitos para que el servidor de PlateSpin funcione con NAT” en la página 36
- “Optimización de transferencia de datos en conexiones WAN” en la página 71
- “Optimización del rendimiento del entorno de réplica” en la página 74
- “Establecimiento de método de rearranque para el servicio de configuración” en la página 75
- “Configuración de la compatibilidad con VMware vCenter Site Recovery Manager” en la página 76
- “Cambio de marca de la interfaz Web mediante parámetros de configuración” en la página 87
- “Configuración de descubrimiento del nodo activo de Windows” en la página 127
- “Solución de problemas del servicio de configuración” en la página 186

3.5.2 Utilidad Protect Agent

La utilidad Protect Agent (ProtectAgent.cli.exe) es una utilidad de línea de comandos que se puede usar para instalar, actualizar, realizar consultas o desinstalar controladores de transferencias basadas en bloques. Aunque siempre es necesario rearrancar cuando se instalan, se desinstalan o se actualizan controladores, la utilidad Protect Agent permite controlar mejor cuándo se produce la acción y, por lo tanto, cuándo se producirá el rearranque del servidor. Por ejemplo, puede usar la utilidad para instalar los controladores durante el tiempo de inactividad planificado, en lugar de hacerlo durante la primera réplica. Consulte el Apéndice D, “Utilidad Protect Agent”, en la página 143.

3.5.3 Herramienta VMware Role

La herramienta VMware Role (PlateSpin.VMwareRoleTool.exe) es una utilidad de línea de comandos que puede utilizar para crear funciones de usuario exclusivas para un centro de datos de VMware como asistencia para la multitenencia. Con las funciones puede otorgar a los usuarios de VMware no administrativos (o "usuarios habilitados") permiso para realizar operaciones del ciclo de vida de Protect en el entorno de VMware. Consulte la Sección 5.4, “Configuración de inquilinos múltiples de Protect en VMware”, en la página 57.

4 Gestión de licencias

Después de activar una licencia para el producto, puede supervisar la disponibilidad de las licencias de la carga de trabajo, añadir nuevas licencias y eliminar las licencias caducadas.

- Sección 4.1, “Activación de la licencia del producto”, en la página 49
- Sección 4.2, “Acerca del consumo de licencias de carga de trabajo”, en la página 50
- Sección 4.3, “Visualización de la información de licencia”, en la página 51
- Sección 4.4, “Adición de una licencia”, en la página 52
- Sección 4.5, “Supresión de una licencia”, en la página 52
- Sección 4.6, “Generación de un informe de licencias para la asistencia técnica”, en la página 52

4.1 Activación de la licencia del producto

La licencia del producto PlateSpin Protect le da derecho a proteger un número específico o ilimitado de cargas de trabajo.

Para asignar una licencia de producto a PlateSpin Protect, debe disponer de un código de activación de licencia. Si no tiene un código de activación de licencia, solicite uno en el Centro de servicios al cliente (http://www.netiq.com/customercenter/). Un representante de Atención al cliente se pondrá en contacto con usted y le proporcionará el código de activación de la licencia.

Nota: si es cliente de PlateSpin y no dispone de una cuenta en el Centro de servicios al cliente, primero debe crear una con la misma dirección de correo electrónico que especificó en la orden de compra. Consulte Creación de cuenta (https://www.netiq.com/selfreg/jsp/createAccount.jsp).

Tiene dos opciones para activar su licencia de producto: en línea o sin conexión.

- Sección 4.1.1, “Activación de licencia en línea”, en la página 49
- Sección 4.1.2, “Activación de licencia sin conexión”, en la página 50

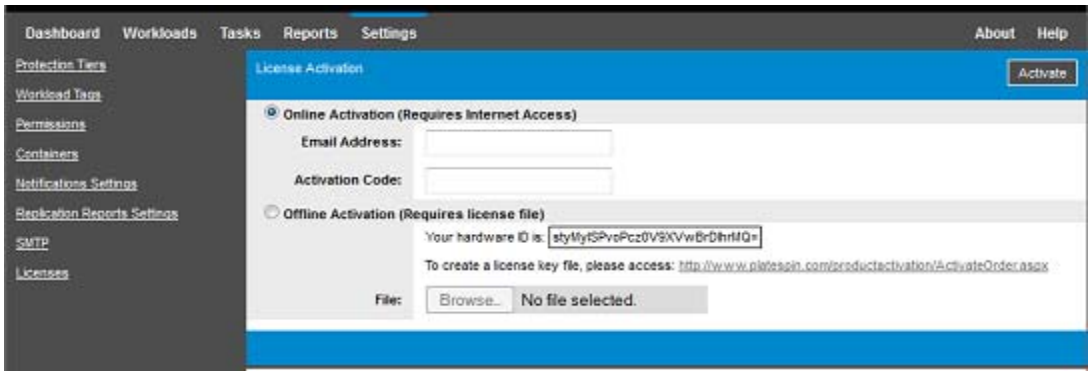
4.1.1 Activación de licencia en línea

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.

Para configurar la activación de licencias en línea:

1. En la interfaz Web, seleccione **Settings > Licenses** (Configuración > Licencias) y haga clic en **Add License** (Añadir licencia).



2 Seleccione **Online Activation** (Activación en línea).

3 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.

4.1.2 Activación de licencia sin conexión

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

1 En la interfaz Web, seleccione **Settings > Licenses** (Configuración > Licencias) y haga clic en **Add License** (Añadir 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 del producto PlateSpin (http://www.platespin.com/productactivation/ActivateOrder.aspx). Entre con su nombre de usuario y su contraseña del Centro de servicios al cliente.

4 Use el ID de hardware para crear un archivo de clave de licencia. Para este proceso se requiere la información siguiente:

   - 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 Guarde el archivo de licencia generado, transfiéralo al host del producto que no tiene conexión a Internet y úselo para activar el producto.

6 En la página License Activation (Activación de licencia) de la interfaz Web, indique la vía al archivo o busque su ubicación y haga clic en **Activate** (Activar).

   El archivo de clave de licencia se guarda y el producto se activa según este archivo.

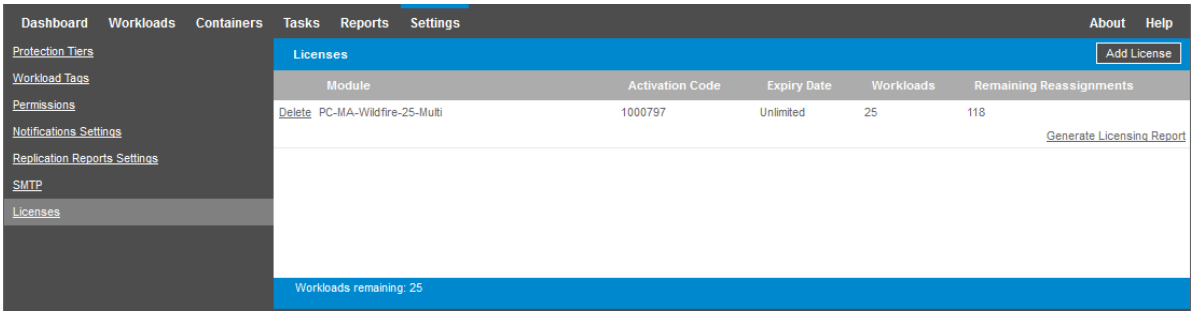
4.2 Acerca del consumo de licencias de carga de trabajo

La licencia del producto PlateSpin Protect le da derecho a proteger un número específico o ilimitado 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.

En la página Dashboard (Consola) de la interfaz Web de PlateSpin Protect, la sección License Summary (Resumen de licencia) muestra el número actual de licencias instaladas y consumidas.

La página Licenses (**Settings** > **Licenses**, Configuración > Licencias) muestra todas las licencias instaladas con el número actual de licencias de carga de trabajo consumidas y las reasignaciones restantes disponibles para esas licencias. La página también muestra el número total de licencias de carga de trabajo sin usar para el servidor de PlateSpin.

Figura 4-1 *Recuento de licencias y reasignaciones restantes*



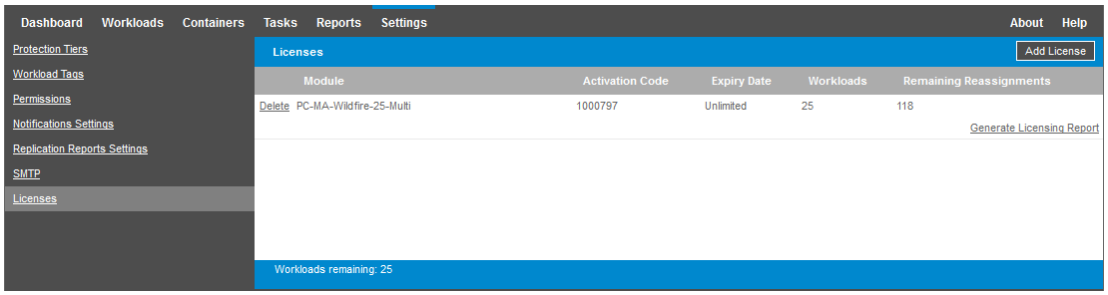
4.3 Visualización de la información de licencia

La página Dashboard (Consola) del producto proporciona un resumen de licencias donde se muestra el número total de licencias instaladas y consumidas.

Puede ver información acerca de las licencias de carga de trabajo instaladas en un servidor de PlateSpin en la página Licenses (Licencias). Para cada licencia, puede ver el número actual de licencias de carga de trabajo usadas y el número actual de reasignaciones restantes disponibles de las licencias usadas.

Para ver información de licencias:

1. En la interfaz Web, seleccione **Settings > Licenses** (Configuración > Licencias).



2. Consulte la información de la licencia:
   - Código de activación
   - Fecha de caducidad
   - Cargas de trabajo
   - Reasignaciones restantes
3. Consulte en **Workloads remaining** (Cargas de trabajo restantes) el número de licencias no utilizadas disponibles.

4.4 Adición de una licencia

Para activar una licencia nueva se emplea el mismo proceso que para activar la primera licencia. Consulte las secciones siguientes para obtener información:

- Sección 4.1.1, “Activación de licencia en línea”, en la página 49
- Sección 4.1.2, “Activación de licencia sin conexión”, en la página 50

4.5 Supresión de una licencia

Puede suprimir una licencia caducada en la página Licenses (Licencias).

1. En la interfaz Web, seleccione **Settings > Licenses** (Configuración > Licencias).
2. Consulte la información de la licencia.
3. Haga clic en la opción **Delete** (Suprimir) situada junto a la licencia caducada y confirme la acción.

4.6 Generación de un informe de licencias para la asistencia técnica

Si tiene problemas de licencias, el servicio de asistencia técnica podría pedirle que genere un informe de licencias. Este informe de diagnóstico contiene información codificada del producto sobre las licencias que tiene activadas para el servidor de PlateSpin.

1. En la interfaz Web, seleccione **Settings > Licenses** (Configuración > Licencias).
2. Bajo la lista de licencias, haga clic en **View Licensing Report** (Ver informe de licencias).

   Se abre el archivo `LicenseReport.txt` en una pestaña o una ventana nueva del navegador, en función de los ajustes de su navegador.
3. Guarde el archivo `LicenseReport.txt` con el nombre `LicenseReport.psl` en su equipo local.

5 Configuración de la autorización y la autenticación de usuarios

En esta sección se incluye la siguiente información:

- Sección 5.1, “Acerca del acceso basado en funciones de PlateSpin Protect”, en la página 53
- Sección 5.2, “Gestión del acceso y los permisos de PlateSpin Protect”, en la página 54
- Sección 5.3, “Gestión de los grupos de seguridad de PlateSpin Protect y los permisos de la carga de trabajo”, en la página 56
- Sección 5.4, “Configuración de inquilinos múltiples de Protect en VMware”, en la página 57

5.1 Acerca del acceso basado en funciones 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:** cuentan 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 5-1 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
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 un acceso basado en funciones adecuado a PlateSpin Protect:

1. Añada usuarios a los grupos de usuarios necesarios que se describen en la Tabla 5-1. Consulte la documentación de Windows.
2. Cree 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 56.

5.2 Gestión del acceso y los permisos de PlateSpin Protect

En las secciones siguientes se proporciona más información:

- Sección 5.2.1, “Adición de usuarios a PlateSpin Protect”, en la página 55
- Sección 5.2.2, “Asignación de una función de protección de carga de trabajo a un usuario de PlateSpin Protect”, en la página 55

5.2.1 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 55.

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) y seleccione **New User** (Nuevo usuario).
3. Especifique la información necesaria 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 55.

5.2.2 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 5-1, “Funciones de protección de la carga de trabajo y detalles de permisos”, en la página 54.

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).
4. Busque el grupo de protección de la carga de trabajo requerido y asígnelo al usuario.

Puede que el cambio tarde varios minutos en tener efecto. Para intentar aplicar los cambios manualmente, reinicie el servidor mediante el archivo ejecutable `RestartPlateSpinServer.exe`.

Para reiniciar el servidor de PlateSpin:

1. Antes de intentar reiniciar el servidor de PlateSpin, ponga en pausa todos los contratos o verifique que no hay ninguna réplica ni operación de failover o de failback en curso. No continúe hasta que todas las cargas de trabajo estén inactivas.
2. En el host del servidor de PlateSpin, diríjase a `.\bin\RestartPlateSpinServer`.
3. Haga doble clic en el ejecutable `RestartPlateSpinServer.exe`.

   Se abrirá un indicador de comandos para solicitar confirmación.
4. 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 56.

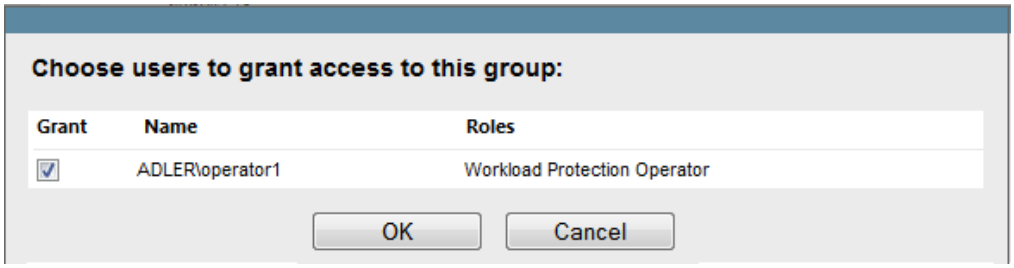
5.3 Gestión de los grupos de seguridad de PlateSpin Protect y los permisos de la carga de trabajo

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*.

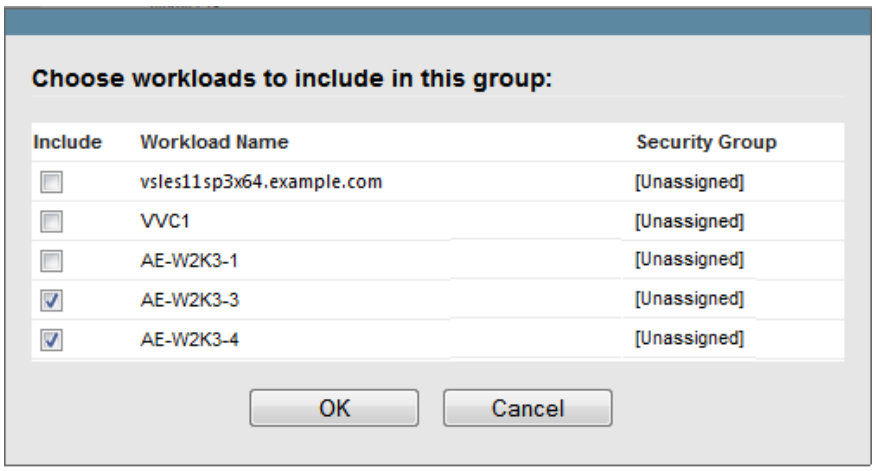
1. Asigne un usuario de PlateSpin Protect a la función de protección de la carga de trabajo cuyos permisos se adapten mejor a dicha función en su organización. Consulte "Asignación de una función de protección de carga de trabajo a un usuario de PlateSpin Protect" en la página 55.
2. Acceda a PlateSpin Protect como administrador en la interfaz Web de PlateSpin Protect 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 **Create** (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.

5.4 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 la multitenencia. 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 5.4.1, “Definición de funciones de VMware para varios inquilinos”, en la página 57
- Sección 5.4.2, “Asignación de funciones en vCenter”, en la página 61

5.4.1 Definición de funciones de VMware para varios inquilinos

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. El archivo `PlateSpinRole.xml` define los privilegios mínimos necesarios y los agrega a tres funciones personalizadas de VMware respectivamente:

- Gestor de máquinas virtuales de PlateSpin
- Gestor de infraestructuras de PlateSpin
- Usuario de PlateSpin

Este archivo está incluido en la instalación del servidor de PlateSpin Protect. Un ejecutable complementario, `PlateSpin.VMware.Role.Tool.exe`, accede al archivo para permitir la creación de estas funciones personalizadas de PlateSpin en un entorno vCenter de destino.

Por defecto, el archivo de definición de funciones (`PlateSpinRole.xml`) y la herramienta de definición de funciones (`PlateSpin.VMwareRoleTool.exe`) se encuentran en la carpeta `VMwareRolesTool`:

`<directorio-instalación>\PlateSpin Protect Server\bin\VMwareRolesTool`

En esta sección se incluye la información siguiente:

- “Sintaxis básica de la línea de comandos” en la página 58
- “Parámetros e indicadores adicionales de línea de comandos” en la página 58
- “Ejemplo de uso de la herramienta” en la página 58
- “(Opcional) Definición manual de las funciones de PlateSpin en vCenter” en la página 59
- “Uso de vCenter para ver privilegios de funciones personalizadas de PlateSpin” en la página 59

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.VMware.Role.Tool.exe /host=[host name or IP address of vCenter or ESX host] /user=[user name] /role=[PlateSpinRole.xml] /create
```

Donde `PlateSpinRole.xml` es el nombre de archivo de la definición de función.

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.VMware.Role.Tool.exe` para crear o actualizar funciones en vCenter:

Parámetros

`/create`	(Obligatorio) Crea las funciones definidas mediante el parámetro `/role`.
`/get_all_prvileges`	Muestra todos los privilegios definidos en el servidor.
`/get_compatible_roles`	Muestra todas las funciones que son compatibles con la función definida por `/role`.
`/check_role=[`*`nombre de función`*`]`	Compruebe que la función indicada es compatible con la función definida por `/role`.

Indicadores opcionales

`/interactive`	Ejecuta la herramienta con opciones interactivas que permiten crear funciones individuales, comprobar la compatibilidad de funciones o indicar todas las funciones compatibles. Para obtener información sobre cómo usar la herramienta en modo interactivo, consulte *VMware Role Tool to Verify Permissions to Roles* (Herramienta de funciones de VMware para verificar permisos para funciones, artículo 7018547 de la base de conocimientos) (https://www.netiq.com/support/kb/doc.php?id=7018547).
`/password=[contraseña]`	Proporciona la contraseña de VMware (omite la solicitud de contraseña).
`/verbose`	Muestra información detallada.

Ejemplo de uso de la herramienta

Uso: `PlateSpin.VMware.Role.Tool.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.

(Opcional) 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) en el centro de recursos técnicos de VMware.

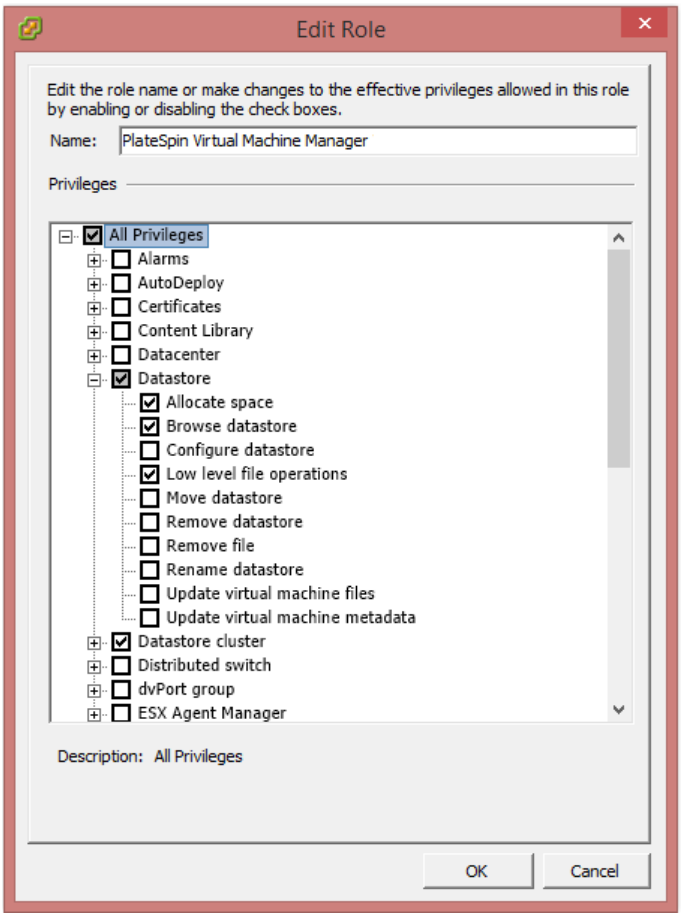
Uso de vCenter para ver privilegios de funciones personalizadas de PlateSpin

Puede usar el cliente de vCenter para ver los privilegios mínimos establecidos para las funciones personalizadas de PlateSpin.

1 En vCenter, seleccione una función personalizada:
   - Gestor de máquinas virtuales de PlateSpin
   - Gestor de infraestructuras de PlateSpin
   - Usuario de PlateSpin

2 Haga clic en **Edit** (Editar) para ver la configuración de los privilegios en el recuadro de diálogo Edit Role (Editar función).

Por ejemplo, la ilustración siguiente muestra algunos de los privilegios definidos para la función Gestor de máquinas virtuales de PlateSpin.



5.4.2 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 *Administrador de infraestructuras de PlateSpin* (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 *Administrador de infraestructuras de PlateSpin* (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 *Administrador de infraestructuras de PlateSpin* (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 *Administrador de máquinas virtuales de PlateSpin* (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 *Administrador de máquinas virtuales de PlateSpin* (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.

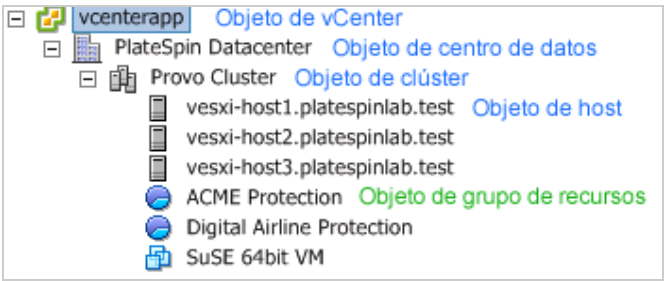
Contenedor de vCenter para asignación de funciones	Aspectos específicos de asignación de funciones	Instrucciones de propagación	Más información
Todas las redes a las que necesite acceder el usuario habilitado Redes virtuales distribuidas con dvSwitch y dvPortgroup	Asigne al usuario habilitado la función *Administrador de máquinas virtuales de PlateSpin* (o equivalente).	La propagación queda sujeta al criterio del administrador de VMware.	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. ◆ 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.
Todos los almacenes de datos y clústeres de almacenes de datos a los que necesite acceder el usuario habilitado	Asigne al usuario habilitado la función *Administrador de máquinas virtuales de PlateSpin* (o equivalente).	La propagación queda sujeta al criterio del administrador de VMware.	El usuario habilitado debe tener esta función asignada en al menos un almacén de datos o clúster de almacenes de datos. 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..

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 *Usuario de PlateSpin* (o equivalente).	La propagación queda sujeta al criterio del administrador de VMware.	Este inquilino pertenece al grupo de administradores de PlateSpin en el servidor de PlateSpin Protect y también está en el servidor de vCenter. 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.

A continuación se muestra una infraestructura virtual en la consola de vCenter. Los objetos de vCenter, centro de datos, clúster y host etiquetados en azul tienen asignada la función de administrador de infraestructuras. Los objetos de conjunto de recursos etiquetados en verde tienen asignada la función de 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.

---

6 Configuración de la aplicación del servidor de PlateSpin

En esta sección se describen los requisitos de instalación y configuración de PlateSpin Protect.

- Sección 6.1, “Configuración de idiomas para versiones internacionales”, en la página 65
- Sección 6.2, “Configuración de los servicios de notificación por correo electrónico para eventos e informes de réplica”, en la página 67
- Sección 6.3, “Configuración de direcciones IP alternativas para el servidor de PlateSpin”, en la página 70
- Sección 6.4, “Optimización de transferencia de datos en conexiones WAN”, en la página 71
- Sección 6.5, “Optimización del rendimiento del entorno de réplica”, en la página 74
- Sección 6.6, “Establecimiento de método de rearranque para el servicio de configuración”, en la página 75
- Sección 6.7, “Configuración de la compatibilidad con VMware vCenter Site Recovery Manager”, en la página 76

6.1 Configuración de idiomas para versiones internacionales

Además de en inglés, PlateSpin Protect proporciona compatibilidad con otros idiomas:

- Chino simplificado
- Chino tradicional
- Francés
- Alemán
- Japonés

Para gestionar el servidor de PlateSpin en uno de estos idiomas, configure el código de idioma para el sistema operativo en el host del servidor de PlateSpin y en su navegador Web.

- Sección 6.1.1, “Establecimiento del idioma en el sistema operativo”, en la página 65
- Sección 6.1.2, “Establecimiento del idioma en el navegador Web”, en la página 66

6.1.1 Establecimiento del idioma en el sistema operativo

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.

Para cambiar el idioma del sistema operativo:

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.

6.1.2 Establecimiento del idioma en el navegador Web

Para usar la interfaz Web de PlateSpin Protect 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:
   - **Chrome:**
     1. En el menú de Chrome, seleccione **Configuración** y haga clic en **Mostrar configuración avanzada.**
     2. Desplácese hasta **Idiomas** y haga clic en **Configuración de idioma y de introducción de texto**.
   - **Firefox:**
     1. En el menú **Herramientas,** seleccione **Opciones** y, seguidamente, seleccione la pestaña **Contenido.**
     2. En **Idiomas,** haga clic en **Seleccionar.**
   - **Internet Explorer:**
     1. En el menú **Herramientas,** seleccione **Opciones** y, seguidamente, seleccione la pestaña **General.**
     2. En **Apariencia,** haga clic en **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 “Lanzamiento de la interfaz Web” en la página 41.

Nota: (para usuarios 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]`.

6.2 Configuración de los servicios de notificación por correo electrónico para eventos e informes de réplica

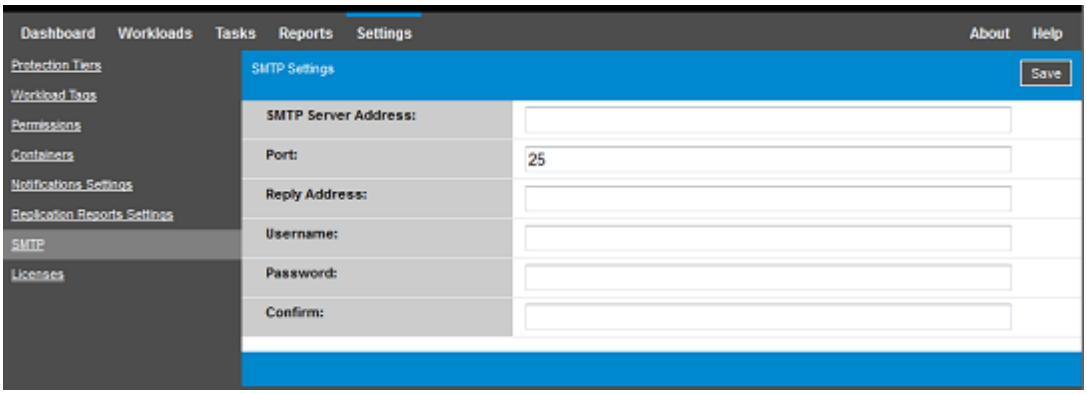
Es posible configurar PlateSpin Protect para que envíe automáticamente notificaciones de eventos e informes de réplica a direcciones de correo electrónico específicas de los destinatarios oportunos. Esta función requiere que primero se especifique un servidor SMTP válido para que PlateSpin Protect lo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

- Sección 6.2.1, “Configuración de SMTP para el servicio de notificación por correo electrónico”, en la página 67
- Sección 6.2.2, “Habilitación de las notificaciones de eventos”, en la página 68
- Sección 6.2.3, “Habilitación de informes de réplica”, en la página 69

6.2.1 Configuración de SMTP para el servicio de notificación por correo electrónico

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 6-1 *Configuración del protocolo simple de transferencia de correo (SMTP)*



Para configurar los valores de SMTP:

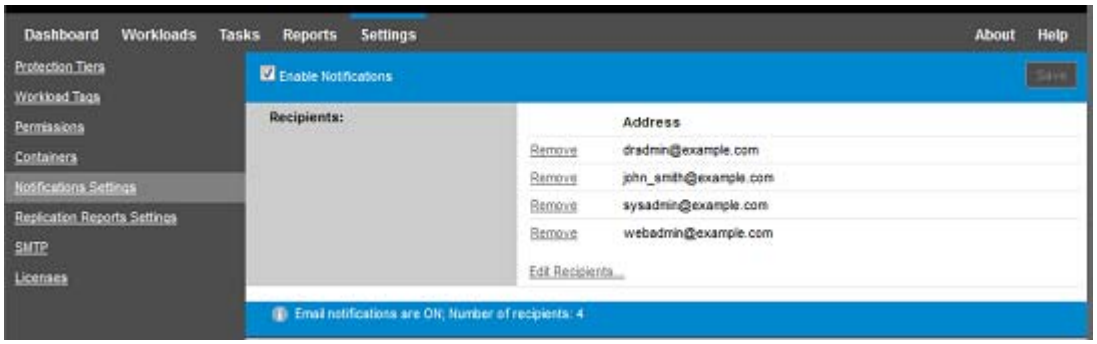
1. En la interfaz Web de PlateSpin Protect, haga clic en **Settings > SMTP** (Configuración > SMTP).
2. Especifique los valores del servidor SMTP para recibir notificaciones de eventos y de progreso por correo electrónico:
   - **Address** (Dirección)
   - **Port** (Puerto, por defecto es el 25)
   -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

6.2.2 Habilitación de las notificaciones de eventos

Los eventos se añaden siempre al registro de eventos de la aplicación del sistema, con los tipos de entrada de registro Advertencia, Error e Información. También puede habilitar que se envíen automáticamente las notificaciones de evento a los destinatarios apropiados.

1. Configure un servidor SMTP para que lo use PlateSpin Protect.

   Consulte “Configuración de SMTP para el servicio de notificación por correo electrónico” en la página 67.
2. En la interfaz Web de PlateSpin Protect, haga clic en **Settings > Notification Settings** (Configuración > 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 **Save** (Guardar).

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

Los tipos de eventos mostrados en la Tabla 6-1 pueden activar las notificaciones por correo electrónico si estas están habilitadas.

Nota: aunque las entradas del registro de eventos tienen ID exclusivos, no existe garantía de que los ID sigan igual en versiones futuras.

Tabla 6-1 *Tipos de eventos organizados por tipos de entrada de registro*

Tipos de eventos	Observaciones
Tipo de entrada de registro: Advertencia	
`FullReplicationMissed`	Similar al evento `Réplica incremental perdida`.

Tipos de eventos	Observaciones
`IncrementalReplicationMissed`	Se genera cuando se produce una de estas circunstancias: ◆ 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.
`WorkloadOfflineDetected`	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 **En pausa.**
Tipo de entrada de registro: Error	
`FailoverFailed`	
`FullReplicationFailed`	
`IncrementalReplicationFailed`	
`PrepareFailoverFailed`	
Tipo de entrada de registro: Información	
`FailoverCompleted`	
`FullReplicationCompleted`	
`IncrementalReplicationCompleted`	
`PrepareFailoverCompleted`	
`TestFailoverCompleted`	Se genera al marcar manualmente una operación de prueba de failover como correcta o errónea.
`WorkloadOnlineDetected`	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 **En pausa.**

6.2.3 Habilitación de informes de réplica

Puede habilitar que se envíen informes de réplica automáticamente a los destinatarios apropiados.

1 Configure un servidor SMTP para que lo use PlateSpin Protect.

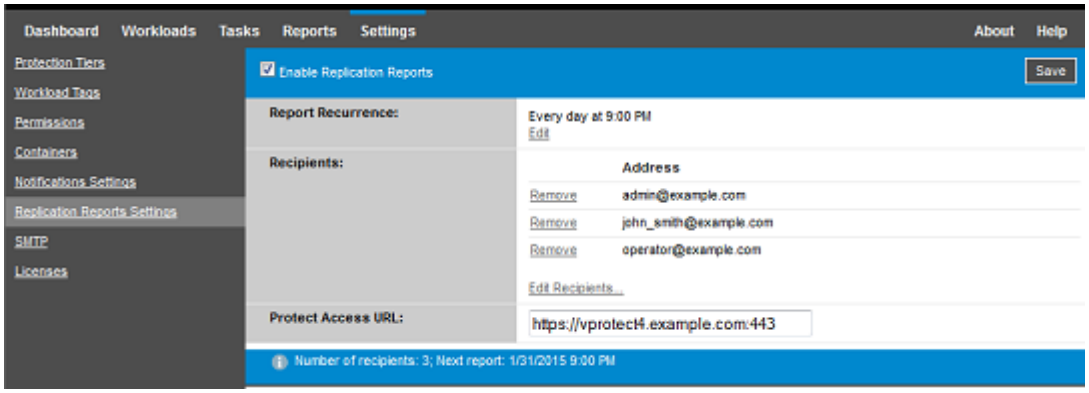
Consulte “Configuración de SMTP para el servicio de notificación por correo electrónico” en la página 67.

2 En la interfaz Web de PlateSpin Protect, haga clic en **Settings > 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 **Edit** (Editar) y especifique el patrón de recurrencia oportuno para los informes. Puede hacer clic en **Close** (Cerrar) para comprimir la sección.

5 En la sección **Recipients** (Destinatarios), haga clic en **Edit Recipients** (Editar destinatarios), indique las direcciones de correo electrónico oportunas, separadas por comas, y haga clic en **OK** (Aceptar). Puede hacer clic en la opción **Remove** (Eliminar) situada junto a una dirección de correo electrónico para suprimir el destinatario de la lista.



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 **Save** (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 182.

6.3 Configuración de direcciones IP alternativas para el servidor de PlateSpin

Puede añadir direcciones IP alternativas al parámetro `AlternateServerAddresses` de la configuración de PlateSpin a fin de habilitar el servidor de PlateSpin para que funcione en entornos con NAT habilitada.

Para añadir direcciones IP alternativas para el servidor de PlateSpin:

1 En cualquier navegador Web, abra

`https://`*`Servidor_de_PlateSpin`*`/platespinconfiguration/`

2 Busque el parámetro `AlternateServerAddresses` y añada direcciones IP para el servidor de PlateSpin.

3 Guarde la configuración y salga de la página.

No es necesario rearrancar ni reiniciar los servicios de PlateSpin para aplicar los cambios.

6.4 Optimización de transferencia de datos en conexiones WAN

Puede optimizar el rendimiento de la trasferencia 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 obtener más información, consulte la Sección 3.5.1, “Configuración de PlateSpin”, en la página 47.

- Sección 6.4.1, “Ajuste de parámetros”, en la página 71
- Sección 6.4.2, “Ajuste de FileTransferSendReceiveBufferSize”, en la página 73

6.4.1 Ajuste de parámetros

Use los parámetros de configuración de transferencia de archivos 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 6-2 muestra los parámetros de configuración de la página de configuración de PlateSpin (`https://Servidor_de_PlateSpin/platespinconfiguration/`) que controlan las velocidades de transferencia de archivos con los valores por defecto y máximos. Es posible modificar estos valores mediante pruebas de ensayo y error a fin de optimizar el funcionamiento en entornos WAN de alta latencia.

Tabla 6-2 *Parámetros de configuración por defecto y optimizados de transferencia de archivos*

Parámetro	Valor por defecto	Valor máximo
`AlwaysUseNonVSSFileTransferForWindows2003`	False	
`FileTransferCompressionThreadsCount` Controla el número de hilos usados para la compresión de datos de nivel de paquete. Si la compresión está inhabilitada, este ajuste se ignora. Dado que la compresión depende de la CPU, este valor puede tener efecto en el rendimiento.	2	N/D
`FileTransferBufferThresholdPercentage` Determina la cantidad mínima de datos que se deben almacenar en el buffer antes de crear y enviar nuevos paquetes de red.	10	
`FileTransferKeepAliveTimeOutMilliSec` Especifica cuánto tiempo hay que esperar para empezar a enviar mensajes de mantenimiento de la conexión si se supera el tiempo límite de TCP.	120000	

Parámetro	Valor por defecto	Valor máximo
`FileTransferLongerThan24HoursSupport`	True	
`FileTransferLowMemoryThresholdInBytes` Determina cuándo considera el servidor que se encuentra en un estado de poca memoria, lo que provoca el aumento de comportamiento de red.	536870912	
`FileTransferMaxBufferSizeForLowMemoryInBytes` Especifica el tamaño del buffer interno usado en el estado de poca memoria.	5242880	
`FileTransferMaxBufferSizeInBytes` Especifica el tamaño del buffer interno para retener datos de paquetes.	31457280	
`FileTransferMaxPacketSizeInButes` Determina el tamaño máximo de los paquetes que se pueden enviar.	1048576	
`FileTransferMinCompressionLimit` Especifica el umbral de compresión de nivel de paquete en bytes.	0 (inhabilitado)	Máx. 65536 (64 KB)
`FileTransferPort`	3725	

`FileTransferSendReceiveBufferSize`
 	
Permite definir el tamaño máximo (en bytes) de los búferes de envío y recepción para las conexiones TCP de la red de réplicas. El tamaño del búfer afecta al tamaño de la ventana de recepción de TCP (RWIN), donde se define el número de bytes que se pueden enviar sin acuse de recibo de TCP. Este valor es relevante tanto para las transferencias basadas en archivos como para las basadas en bloques. Si se ajusta el tamaño del búfer según el ancho de banda y la latencia de la red, se mejora el rendimiento y se reduce el procesamiento de la CPU.
 	
Si el valor se define en cero (desactivado), 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:
 	
((VELOCIDAD_ENLACE en Mb/s / 8) * RETRASO en s)) * 1000 * 1024
 	
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 * 1024 = 128000 bytes`
 	
Para obtener información sobre el ajuste, consulte la Sección 6.4.2, “Ajuste de FileTransferSendReceiveBufferSize”, en la página 73.
	0 (8192 bytes)	Máx. 5242880 (5 MB)

Parámetro	Valor por defecto	Valor máximo
`FileTransferSendReceiveBufferSizeLinux` Especifica el valor de tamaño de la ventana de recepción de TCP/IP (RWIN) para las conexiones de transferencia de archivos en Linux. Controla el número de bytes enviado sin reconocimiento TCP. Cuando el valor se define en cero (desactivado), el valor para el tamaño de la ventana TCP/IP en Linux se calcula automáticamente a partir del parámetro `FileTransferSendReceiveBufferSize`. Si ambos parámetros se definen en cero (desactivados), el valor por defecto es 248 KB. En caso de tamaños personalizados, especifique el tamaño en bytes. **Nota:** en versiones anteriores, era preciso definir este parámetro en la mitad del valor deseado, pero ya no es necesario hacerlo.	0 (253952 bytes)	
`FileTransferShutDownTimeOutInMinutes`	1090	
`FileTransferTCPTimeOutMilliSec` Permite definir los valores de tiempo límite de envió y recepción de TCP.	30000	
`PostFileTransferActionsRequiredTimeInMinutes`	60	

6.4.2 Ajuste de FileTransferSendReceiveBufferSize

El parámetro FileTransferSendReceiveBufferSize permite definir el tamaño máximo (en bytes) de los búferes de envío y recepción para las conexiones TCP de la red de réplica. El tamaño del búfer afecta al tamaño de la ventana de recepción de TCP (RWIN), donde se define el número de bytes que se pueden enviar sin acuse de recibo de TCP. Este valor es relevante tanto para las transferencias basadas en archivos como para las basadas en bloques. Si se ajusta el tamaño del búfer según el ancho de banda y la latencia de la red, se mejora el rendimiento y se reduce el procesamiento de la CPU.

Puede ajustar el parámetro FileTransferSendReceiveBufferSize para optimizar la transferencia de bloques o archivos desde los servidores de origen a los de destino en el entorno de réplica. Defina el parámetro en la página de configuración de PlateSpin (`https://Servidor_de_PlateSpin/platespinconfiguration/`).

Para calcular el tamaño óptimo del búfer:

1. Determine la latencia (retraso) entre el servidor de origen y el de destino.

   El objetivo es descubrir cuál es la latencia para un tamaño de paquete que se asemeje lo máximo posible al MTU.

   1a Entre a la sesión en el servidor de origen como usuario administrador.

   1b Escriba lo siguiente en un indicador de comandos:

   ```
   # ping <target-server-ip-address> -f -l <MTU_minus_28> -n 10
   ```

   Habitualmente, la opción `-l` para el comando `ping` añade 28 bytes a los encabezados de la carga especificada para *dirección-ip-servidor-destino*. Por lo tanto, puede ser buena idea probar con un valor inicial de `MTU menos 28` como tamaño en bytes.

1c Modifique repetidamente la carga y vuelva a introducir el comando en el Paso 1b hasta que obtenga el mensaje siguiente:

`The packet needs to be fragmented` (Es necesario fragmentar el paquete).

1d Anote la latencia en segundos.

Por ejemplo, si la latencia es de 35 ms (milisegundos), anote 0,035 como latencia.

2 Calcule un valor de byte para el tamaño del búfer inicial:

```
Tamaño del búfer = (ancho de banda en Mb/s / 8) * latencia en segundos * 1000 * 1024
```

Use valores binarios para el ancho de banda de red. Es decir, 10 Gb/s = 10240 Mb/s y 1 Gb/s = 1024 Mb/s.

Por ejemplo, el cálculo para una red de 10 Gb/s con una latencia de 35 ms es:

```
Tamaño del búfer = (10240 / 8) * 0,035 * 1000 * 1024 = 45875200 bytes
```

3 (Opcional) Calcule un tamaño de búfer óptimo redondeando al alza a un múltiplo del tamaño máximo del segmento (TMS).

3a Determine el TMS:

```
TMS = tamaño de MTU en bytes - (tamaño de encabezado IP + tamaño de encabezado TCP)
```

El tamaño de encabezado IP es de 20 bytes. El tamaño de encabezado TCP es de 20 bytes más los bytes para las opciones como la marca horaria.

Por ejemplo, si el tamaño de MTU es 1470, el TMS será habitualmente de 1430.

```
TMS = 1470 bytes - (20 bytes + 20 bytes) = 1430 bytes
```

3b Calcule el tamaño óptimo del búfer:

```
Tamaño óptimo del búfer = (redondeoalza(tamaño búfer/TMS)) * TMS
```

Para continuar con el ejemplo:

```
Tamaño óptimo del búfer = (redondeoalza(45875200 / 1430) * 1430 *= 32081 * 1430 = 45875830
```

Se redondea al alza en lugar de a la baja porque de esta última manera se obtendría un múltiplo del TMS de menor tamaño que el tamaño del búfer de 45875200:

```
Tamaño no óptimo del búfer = 32080 * 1430 = 45874400
```

6.5 Optimización del rendimiento del entorno de réplica

Utilice los valores de los parámetros de configuración de toma de control e instantánea para optimizar el rendimiento de la réplica. Estos valores son globales y afectan a todas las réplicas.

La Tabla 6-3 muestra los parámetros de configuración de la página de configuración de PlateSpin (`https://`*`Servidor_de_PlateSpin`*`/platespinconfiguration/`) que controlan el entorno de réplica con los valores por defecto.

Tabla 6-3 *Parámetros de configuración por defecto para el entorno de réplica*

Parámetro	Valor por defecto
`TakeControlMemorySizeInMB` El tamaño de la memoria (en MB) que se debe establecer al tomar el control de la réplica.	768
`TakeControlCoresPerSocket` El número de núcleos virtuales por zócalo que se debe usar al tomar el control, cuando se arranca el destino en el LRD o `bootofx.iso`.	1
`TakeControlSockets` El número de zócalos virtuales que se utilizará para tomar el control cuando se arranca el destino en el LRD o en `bootofx.iso`.	1
`MaximumConcurrentReplications` El número de réplicas simultáneas que pueden ejecutarse al mismo tiempo.	25
`VssSnapshotCreationDelay` El número de segundos de retraso que deben transcurrir entre los reintentos al crear una instantánea VSS durante la réplica.	120
`VssSnapshotCreationRetryCount` El número máximo de intentos para crear una instantánea VSS durante la réplica antes de que falle el intento de réplica.	5

6.6 Establecimiento de método de rearranque para el servicio de configuración

Durante una acción de failover, el servicio de configuración optimiza los rearranques reduciendo al mínimo su número y controlando cuándo se producen. Si experimenta un bloqueo del servicio de configuración durante una acción de failover para una carga de trabajo Windows con el error `Configuration Service Not Started` (No se ha iniciado el servicio de configuración), es posible que deba permitir los rearranques cuando se pida durante la configuración. Puede configurar que se omita la optimización del rearranque en una sola carga de trabajo afectada, o configurar un valor `SkipRebootOptimization` global en el servidor de PlateSpin para omitir la optimización del rearranque en todas las cargas de trabajo Windows.

Para omitir la optimización del rearranque para una sola carga de trabajo Windows:

1. Entre como usuario administrador en la carga de trabajo de origen.
2. Añada un archivo a la unidad raíz del sistema (normalmente, `C:`) denominado `PlateSpin.ConfigService.LegacyReboot` sin extensión de archivo. En un indicador de comandos, introduzca:

   ```
   echo $null >> %SYSTEMDRIVE%\PlateSpin.ConfigService.LegacyReboot
   ```

3. Ejecute de nuevo la acción de failover de prueba o de failover que ha fallado.

Para omitir la optimización del rearranque para todas las cargas de trabajo Windows:

1. Entre al servidor de PlateSpin y abra la página de configuración del servidor de PlateSpin en:

   `https://Servidor_de_PlateSpin/platespinconfiguration/`
2. Busque el parámetro de configuración **ConfigurationServiceValues** y haga clic en **Edit** (Editar) para el parámetro.
3. Cambie el valor de **SkipRebootOptimization** de `false` (falso) a `true` (verdadero).
4. Haga clic en **Save** (Guardar).
5. Ejecute una réplica incremental o completa.

   La réplica también propaga los valores de configuración modificados a la máquina virtual de destino.
6. Ejecute de nuevo la operación de failover de prueba o de failover para las cargas de trabajo Windows afectadas.

6.7 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.

Las cargas de trabajo replicadas por PlateSpin Protect y gestionadas en VMware vCenter SRM pueden comportarse sin problemas si configura PlateSpin Protect para que admita SRM mediante los ajustes siguientes:

- Configurar un valor para conservar la imagen ISO y los discos de PlateSpin Protect en el mismo almacén de datos que los archivos `.vmx` 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.

- Sección 6.7.1, “Configuración de archivos de carga de trabajo en el mismo almacén de datos”, en la página 76
- Sección 6.7.2, “Configuración de herramientas de VMware para los destinos de failover”, en la página 77
- Sección 6.7.3, “Aceleración del proceso de configuración”, en la página 78

6.7.1 Configuración de archivos de carga de trabajo en el mismo almacén de datos

Para asegurarse de que los archivos de carga de trabajo se conservan 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.

6.7.2 Configuración de herramientas de VMware para los destinos de failover

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 PlateSpin. En los casos en los que esto no sea posible, debe preparar el entorno antes de la réplica.

Para preparar el entorno:

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.*x* y versiones posteriores:** los paquetes de configuración son `setup.exe` y `setup64.exe`.
- **VMware 4.*x*:** 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:

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`) al directorio `%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, como se muestra en la Tabla 6-4. Utilice el valor de GUID adecuado para copiar el paquete en el directorio correcto.

Tabla 6-4 GUID de los nombres de directorio de VMware Tools

Versión del servidor de VMware	Arquitectura de VMware Tools	GUID
6.5	x86	D61C0FCA-058B-42C3-9F02-898F568A3071
6.5	x64	5D3947B7-BE73-4A00-A549-B15E84B98803
6.0	x86	311E672E-05BA-4CAF-A948-B26DF0C6C5A6
6.0	x64	D7F55AED-DA64-423F-BBBE-F1215529AD03
5.5	x86	660C345A-7A91-458b-BC47-6A3914723EF7
5.5	x64	8546D4EF-8CA5-4a51-A3A3-6240171BE278
5.1	x86	34DD2CBE-183E-492f-9B36-7A8326080755
5.1	x64	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5.0	x86	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5.0	x64	F7C9BC91-7733-4790-B7AF-62E074B73882
4.1	x86	F2957064-65D7-4bda-A52B-3F5859624602
4.1	x64	80B1C53C-6B43-4843-9D63-E9911E9A15D5
4.0	x86	D052CBAC-0A98-4880-8BCC-FE0608F0930F
4.0	x64	80B50267-B30C-4001-ABDF-EA288D1FD09C

6.7.3 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.

7 Configuración de la interfaz Web de PlateSpin

La interfaz Web de PlateSpin permite configurar las etiquetas que se usarán para realizar un seguimiento de las asociaciones lógicas entre cargas de trabajo. Además, es posible controlar la frecuencia de actualización de la pantalla de varias páginas. Use los datos de esta sección para configurar la interfaz Web.

- Sección 7.1, “Creación y gestión de etiquetas de cargas de trabajo”, en la página 79
- Sección 7.2, “Configuración de las frecuencias de actualización de la interfaz Web”, en la página 81
- Sección 7.3, “Personalización del aspecto de la interfaz Web”, en la página 82

7.1 Creación y gestión de etiquetas de cargas de trabajo

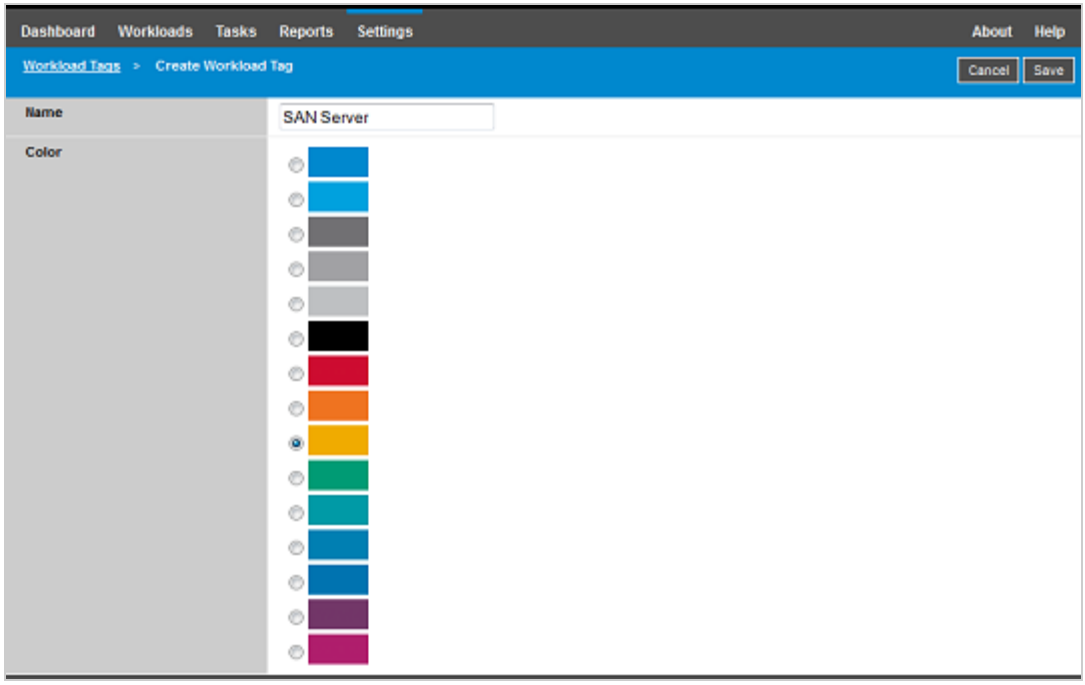
Si tiene un número elevado de cargas de trabajo para gestionar, examinar la lista y seleccionar cargas de trabajo similares para realizar acciones de operación simultáneas puede llevar mucho tiempo. Ordenar según un nombre o una característica puede servir de ayuda. Otra alternativa consiste en usar una etiqueta para configurar una asociación personalizada entre las cargas de trabajo que desea gestionar como grupo. Es posible ordenar fácilmente las cargas de trabajo por la columna Tag (Etiqueta), seleccionar las que tengan la etiqueta adecuada y ejecutar las operaciones disponibles en todas ellas al mismo tiempo.

Una etiqueta puede representar cualquier asociación lógica o física para una carga de trabajo que tenga sentido para usted. Puede asignar a cada etiqueta un color y un nombre exclusivos. Es posible crear tantas etiquetas únicas como se desee, aunque la elección de colores únicos es limitada. Cada carga de trabajo solo puede tener una etiqueta asociada. Cuando se exporta una carga de trabajo a un servidor nuevo, sus etiquetas se conservan.

- Sección 7.1.1, “Creación de una etiqueta de carga de trabajo”, en la página 79
- Sección 7.1.2, “Edición de una etiqueta de carga de trabajo”, en la página 80
- Sección 7.1.3, “Adición de una etiqueta a una carga de trabajo”, en la página 80
- Sección 7.1.4, “Eliminación de una etiqueta de una carga de trabajo”, en la página 81
- Sección 7.1.5, “Supresión de una etiqueta de carga de trabajo”, en la página 81

7.1.1 Creación de una etiqueta de carga de trabajo

1. En la interfaz Web de PlateSpin Protect, haga clic en **Settings** > **Workload Tags** > **Create Workload Tag** (Configuración > Etiquetas de carga de trabajo > Crear etiqueta de carga de trabajo).



2 Especifique un nombre de etiqueta exclusivo (con un máximo de 25 caracteres) y asocie un color a la descripción.

3 Haga clic en **Save** (Guardar) para añadir esta etiqueta nueva a la lista de etiquetas de carga de trabajo disponibles en la vista Workload Tags (Etiquetas de carga de trabajo) de la página Settings (Configuración).

7.1.2 Edición de una etiqueta de carga de trabajo

1 En la interfaz Web de PlateSpin Protect, haga clic en **Settings** > **Workload Tags** (Configuración > Etiquetas de carga de trabajo).

2 Edite cualquiera de las etiquetas disponibles. Haga clic en el nombre de la etiqueta, modifique su nombre o el color asociado y haga clic en **Save** (Guardar).

7.1.3 Adición de una etiqueta a una carga de trabajo

1 En la lista de cargas de trabajo, seleccione la carga activa que desee etiquetar y haga clic en **Configure** (Configurar) para abrir su página de configuración.

2 Expanda la sección **Tag** (Etiqueta) para ver el recuadro desplegable **Tag** (Etiqueta).

3 Seleccione el nombre de la etiqueta que desea asociar con la carga de trabajo y haga clic en **Save** (Guardar).

7.1.4 Eliminación de una etiqueta de una carga de trabajo

1. En la lista de cargas de trabajo, seleccione la carga y haga clic en **Configure** (Configurar) para abrir su página de configuración.
2. Expanda la sección **Tag** (Etiqueta) para ver el recuadro desplegable **Tag** (Etiqueta).
3. Seleccione la línea “vacía” en la lista de nombres de etiquetas disponibles y haga clic en **Save** (Guardar).

7.1.5 Supresión de una etiqueta de carga de trabajo

Es posible suprimir cualquier etiqueta que ya no use. No es posible suprimir una etiqueta si está asociada con cualquier carga de trabajo.

1. En la interfaz Web de PlateSpin Protect, haga clic en **Settings** > **Workload Tags** (Configuración > Etiquetas de carga de trabajo).
2. Anulación de la asociación de etiquetas de las cargas de trabajo.
3. Haga clic en la opción **Delete** (Suprimir) situada junto a la etiqueta y, seguidamente, en **OK** (Aceptar) para confirmar.

7.2 Configuración de las frecuencias de actualización de la interfaz Web

Varias páginas de la interfaz Web tienen intervalos de actualización que se pueden configurar, como se muestra en la Tabla 7-1. Puede modificar el valor del intervalo para adaptarlo a las necesidades de su entorno de PlateSpin.

Tabla 7-1 *Intervalos de actualización por defecto de la interfaz Web*

Parámetro de la interfaz Web	Intervalo de actualización por defecto (en segundos)
DashboardUpdateIntervalSeconds	60
WorkloadsUpdateIntervalSeconds	60
WorkloadTargetsUpdateIntervalSeconds	30
WorkloadDetailsUpdateIntervalSeconds	15
TasksUpdateIntervalSeconds	15

1. Abra el siguiente archivo en un editor de textos:

   `\Archivos de programa\PlateSpin Protect Server\Platespin Forge\web\web.config`
2. Modifique el valor de cualquiera de los valores de intervalo siguientes según necesite para su entorno de PlateSpin:

```
<add key="DashboardUpdateIntervalSeconds" value="60" /> <add
key="WorkloadsUpdateIntervalSeconds" value="60" /> <add
key="WorkloadTargetsUpdateIntervalSeconds" value="30" /> <add
key="WorkloadDetailsUpdateIntervalSeconds" value="15" /> <add
key="TasksUpdateIntervalSeconds" value="15" />
```

3 Guarde el archivo.

El valor nuevo se aplica en la siguiente sesión de la interfaz Web. No es necesario reiniciar el servicio ni el servidor de PlateSpin.

7.3 Personalización del aspecto de la interfaz Web

Puede modificar el aspecto de la interfaz Web de PlateSpin para que se adapte al de su identidad corporativa. Es posible modificar los colores, los logotipos y el nombre del producto. Para obtener más información, consulte el Apéndice A, “Cambio de marca de la interfaz Web de PlateSpin Protect”, en la página 87.

8 Gestión de varios servidores de PlateSpin en la consola de gestión

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 y PlateSpin Forge, puede designar una de las instancias como administrador 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 8.1, “Uso de la consola de gestión de PlateSpin Protect”, en la página 83
- Sección 8.2, “Acerca de las tarjetas de consola de gestión de PlateSpin Protect”, en la página 84
- Sección 8.3, “Adición de instancias de PlateSpin Protect y PlateSpin Forge a la consola de gestión”, en la página 85
- Sección 8.4, “Edición de tarjetas en la consola de gestión”, en la página 86
- Sección 8.5, “Eliminación de tarjetas en la consola de gestión”, en la página 86

8.1 Uso de la consola de gestión de PlateSpin Protect

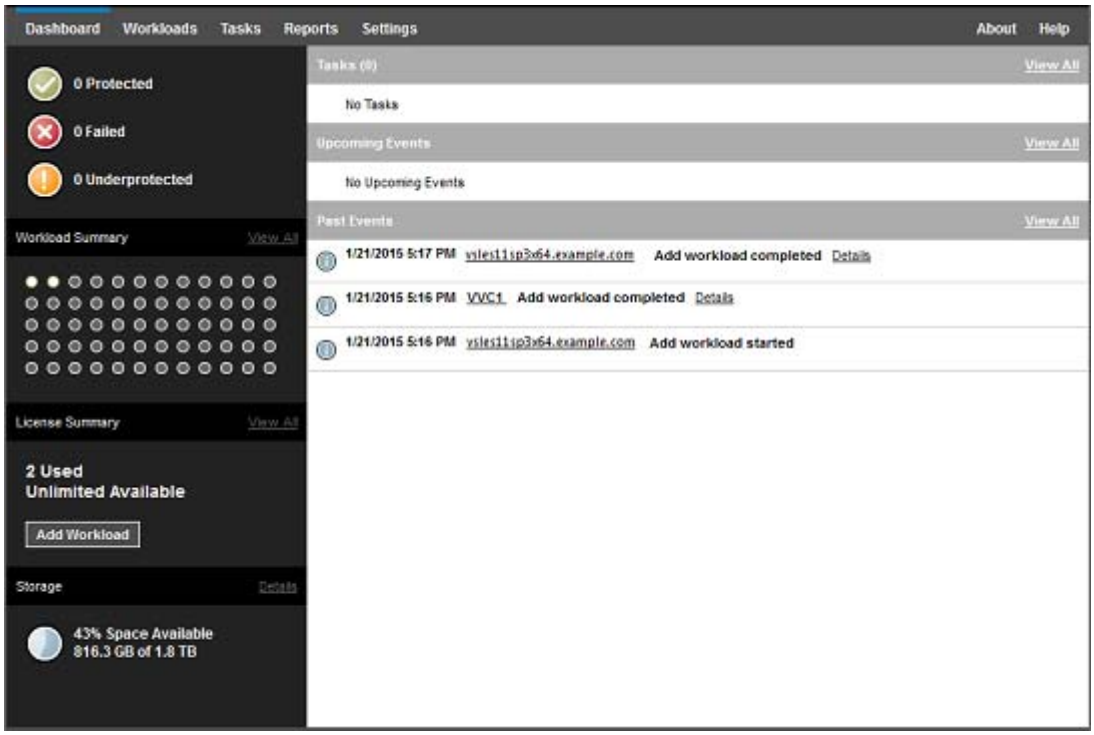
Para empezar a usar la consola de gestión:

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

   `https://`*Servidor_de_PlateSpin*`/console`

   Sustituya *Servidor_de_PlateSpin* con la dirección IP o el nombre de host DNS del host del servidor de PlateSpin designado como gestor.
2. Entre con su nombre de usuario y su contraseña de
3. (Entrada inicial) En la página de bienvenida, haga clic en **Add PlateSpin Server** (Añadir servidor de PlateSpin) y configure una instancia del servidor de PlateSpin como se describe en la Sección 8.3, “Adición de instancias de PlateSpin Protect y PlateSpin Forge a la consola de gestión”, en la página 85.

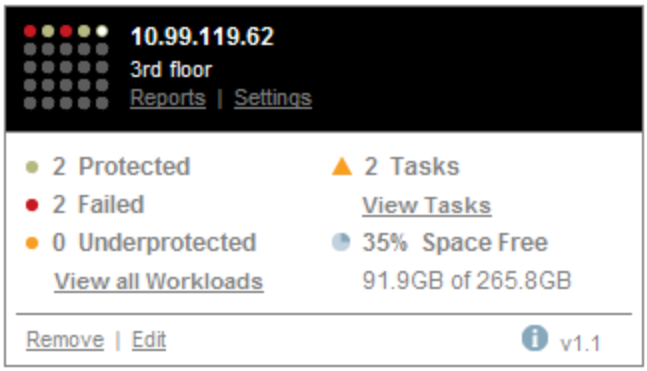
4 (Entradas posteriores) Consulte la consola.



8.2 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 8-1 *Tarjeta de instancia de PlateSpin Forge*



Las tarjetas muestran información básica sobre la instancia específica de PlateSpin Protect y 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.

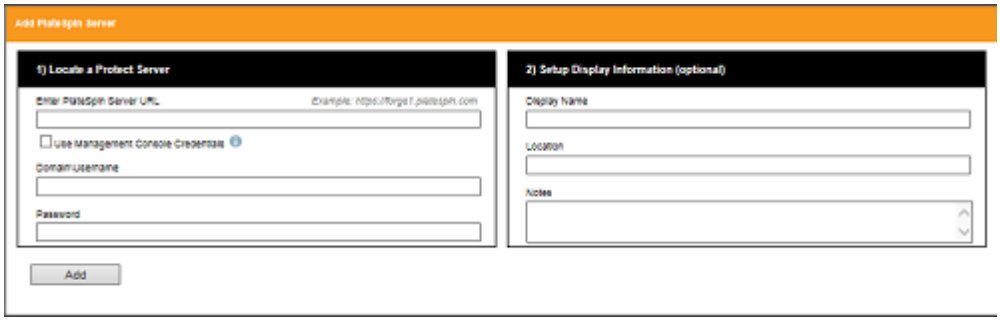
8.3 Adición de instancias de PlateSpin Protect y PlateSpin Forge a la consola de gestión

Cuando se añade una instancia de PlateSpin Protect o PlateSpin 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 PlateSpin Forge a la consola:

1. En la ventana principal de la consola, haga clic en **Add PlateSpin Server** (Añadir servidor de PlateSpin).



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 exclusivo de hasta 15 caracteres en **Display Name** (Nombre de visualización) para el servidor de PlateSpin, un valor de hasta 20 caracteres para **Location** (Ubicación) y las notas que necesite en **Notes** (Notas, hasta 400 caracteres).
6. Haga clic en **Add** (Añadir).

   Se añade una tarjeta nueva a la consola.

8.4 Edición de tarjetas en la consola de gestión

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

1. En la consola de gestión, busque la instancia de la tarjeta para el servidor de PlateSpin Protect o el servidor de PlateSpin Forge que desea modificar.
2. Haga clic en el hiperenlace **Edit** (Editar) de la tarjeta.

   Se muestra la página **Add/Edit** (Añadir/Editar) de la consola.
3. Realice los cambios que desee y haga clic en **Add/Save** (Añadir/Guardar).

   Se muestra la página principal actualizada de la consola.

8.5 Eliminación de tarjetas en la consola de gestión

Para eliminar una tarjeta de la consola de gestión:

1. En la consola de gestión, busque la instancia de la tarjeta para el servidor de PlateSpin Protect o el servidor de PlateSpin Forge que desea eliminar.
2. Haga clic en el hiperenlace **Remove** (Eliminar) de la tarjeta.

   Se muestra un mensaje de confirmación.
3. Haga clic en **OK** (Aceptar) para confirmar los datos.

   La tarjeta se elimina de la consola.

A Cambio de marca de la interfaz Web de PlateSpin Protect

Es posible modificar el aspecto de la interfaz Web para que coincida con el de su identidad corporativa, incluidos los colores, el logotipo y el nombre del producto. Incluso es posible eliminar los enlaces a las pestañas **About** (Acerca de) y **Help** (Ayuda) de la interfaz del producto.

Esta sección incluye información que le ayudará a cambiar la marca del producto:

- Sección A.1, “Cambio de marca de la interfaz Web mediante parámetros de configuración”, en la página 87
- Sección A.2, “Cambio de marca del nombre del producto en el Registro de Windows”, en la página 90

A.1 Cambio de marca de la interfaz Web mediante parámetros de configuración

Puede modificar el aspecto de la interfaz Web para que se adapte al aspecto propio de los sitios Web de su organización. Pera personalizar la marca de la interfaz Web, modifique los parámetros de configuración del host del servidor de PlateSpin.

Para modificar los parámetros de marca de interfaz Web:

1. En cualquier navegador Web, abra `https://servidor_de_PlateSpin/platespinconfiguration/` y entre como administrador.
2. Localice el parámetro del servidor requerido, haga clic en **Edit** (Editar) y cambie el valor.

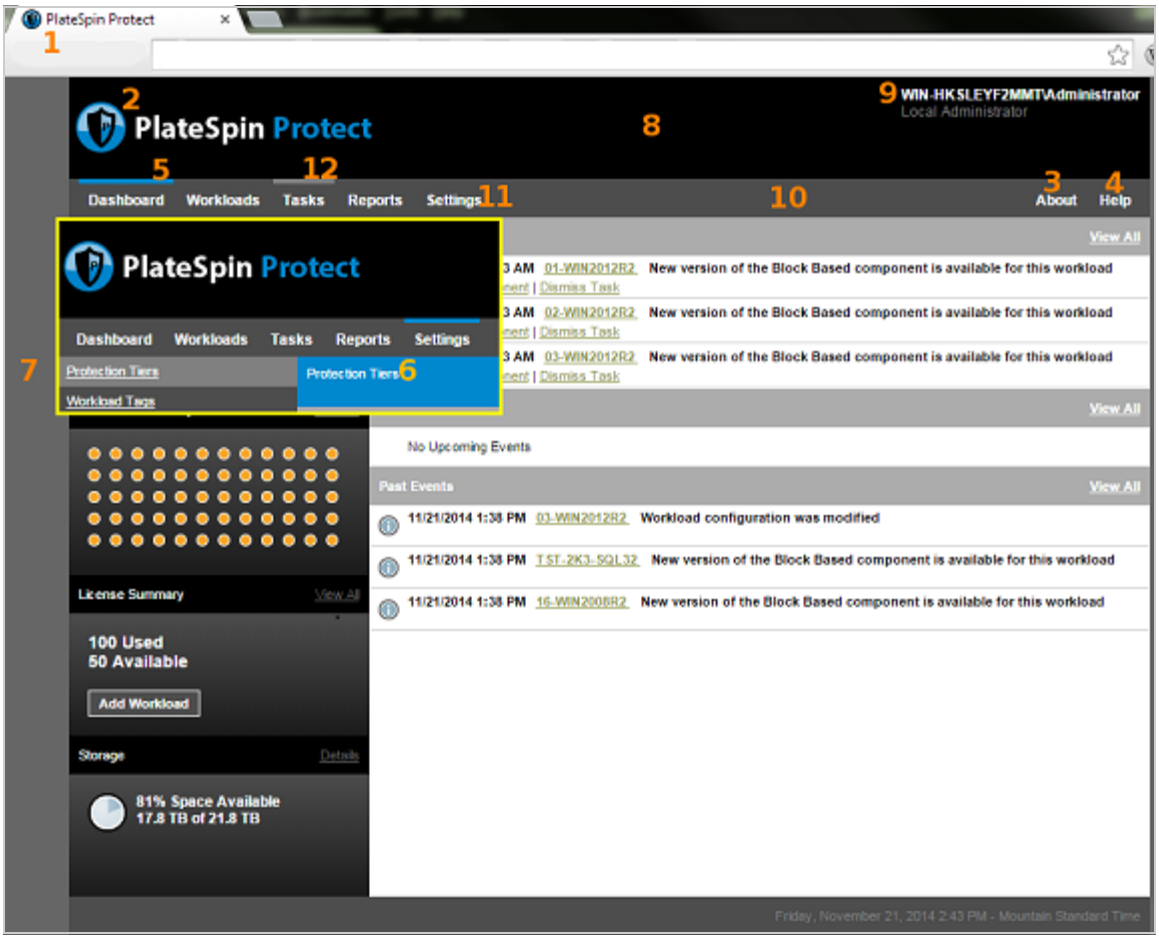
   Para obtener más información, consulte la Figura A-1 para ver los elementos configurables de la interfaz de usuario. Consulte la Tabla A-1 para ver el nombre del ajuste, la descripción y la información del valor por defecto para todos los elementos configurables.
3. Guarde la configuración y salga de la página.

   Aunque no es necesario rearrancar ni reiniciar los servicios después de realizar un cambio en la herramienta de configuración, dicho cambio podría tardar hasta 30 segundos en reflejarse en la interfaz.

A.1.1 Elementos configurables de la interfaz Web

El aspecto de la interfaz Web es coherente en todo el sistema. En la imagen de la consola de PlateSpin Protect de la Figura A-1 se identifican con indicadores numéricos los elementos que puede modificar. El recuadro muestra los elementos configurables del panel de configuración.

Figura A-1 *Interfaz Web de Protect con los elementos configurables etiquetados*



A.1.2 Parámetros configurables de la interfaz Web

En la tabla siguiente se muestran los elementos identificados de la interfaz (o “ID”) de la captura de pantalla de arriba, el nombre del ajuste, su descripción y el valor por defecto. Use la página de configuración del servidor de PlateSpin para cambiar estos valores (es decir, en la página de configuración, haga clic en **Edit** (Editar) en un valor de configuración) según el nuevo aspecto que desee.

Tabla A-1 *Parámetros de configuración de la interfaz de Web y valores por defecto*

ID	Configuración del nombre y la descripción	Valor por defecto

1	`WebUIFaviconUrl`
	
	Ubicación de un archivo de gráfico `.ico` válido. Especifique una de las opciones siguientes:
	
	◆ Una URL válida para el archivo `.ico` correspondiente en un equipo distinto.
	
	Por ejemplo: https://miservidor.ejemplo.com/dir1/dir2/icons/miempresa_favicon.ico
	
	◆ Una vía relativa en la raíz del servidor Web local en la que ha cargado el archivo `.ico` correspondiente.
	
	Por ejemplo, si crea la vía `miempresa\images\icons` en la raíz del servidor Web para almacenar los gráficos de iconos personalizados:
	
	`~/miempresa/images/icons/miempresa_favicon.ico`
	
	En este ejemplo, la vía real del sistema de archivos que contiene el archivo es `C:\Archivos de programa (x86)\PlateSpin Protect Server\PlateSpin Forge\web\miempresa\images\icons\miempresa_favicon.ico`.
		`~/doc/en/favicon.ico` [1]

2	`WebUILogoUrl`
	
	Ubicación del archivo de gráfico del logotipo del producto. Especifique una de las opciones siguientes:
	
	◆ Una URL válida para el archivo de gráficos correspondiente en un equipo distinto.
	
	Por ejemplo: https://miservidor.ejemplo.com/dir1/dir2/logos/miempresa_logo.png
	
	◆ Una vía relativa en la raíz del servidor Web local en la que ha cargado el archivo de gráficos correspondiente.
	
	Por ejemplo, si crea la vía `miempresa\images\logos` en la raíz del servidor Web para almacenar las imágenes de logotipos personalizados:
	
	`~/miempresa/images/logos/miempresa_logo.png`
	
	En este ejemplo, la vía real del sistema de archivos que contiene el archivo es `C:\Archivos de programa (x86)\PlateSpin Protect Server\PlateSpin Forge\web\miempresa\images\logos\miempresa_logo.png`.
		`~/Resources/protectLogo.png` [2]

3	`WebUIShowAboutTab` Alterna la visibilidad de la pestaña **About** (Acerca de). La puede activar (**True**, verdadero) o desactivar (**False**, falso).	True
4	`WebUIShowHelpTab` Alterna la visibilidad de la pestaña **Help** (Ayuda). La puede activar (**True**, verdadero) o desactivar (**False**, falso).	True

ID	Configuración del nombre y la descripción	Valor por defecto
5	`WebUISiteAccentColor`	#0088CE
	Color principal (valor RGB hexadecimal)	
6	`WebUISiteAccentFontColor`	#FFFFFF
	Color de la fuente que se mostrará con el color principal en la interfaz Web (valor RGB hexadecimal)	
7	`WebUISiteBackgroundColor`	#666666
	Color de segundo plano del sitio (valor RGB hexadecimal)	
8	`WebUISiteHeaderBackgroundColor`	#000000
	Color de segundo plano del encabezado del sitio (valor RGB hexadecimal)	
9	`WebUISiteHeaderFontColor`	#FFFFFF
	Color de fuente del encabezado del sitio en la interfaz Web (valor RGB hexadecimal)	
10	`WebUISiteNavigationBackgroundColor`	#4D4D4D
	Color de segundo plano de navegación del sitio en la interfaz Web (valor RGB hexadecimal)	
11	`WebUISiteNavigationFontColor`	#FFFFFF
	Color de la fuente de enlaces de navegación del sitio en la interfaz Web (valor RGB hexadecimal)	
12	`WebUISiteNavigationLinkHoverBackgroundColor`	#808080
	Color de segundo plano de enlaces de navegación del sitio en la interfaz Web (valor RGB hexadecimal)	

[1] La vía real del archivo es `C:\Archivos de programa (x86)\PlateSpin Protect Server\PlateSpin Forge\web\doc\en\favicon.ico`.

[2] La vía real del archivo es `C:\Archivos de programa (x86)\PlateSpin Protect Server\PlateSpin Forge\web\Resources\protectLogo.png`.

A.2 Cambio de marca del nombre del producto en el Registro de Windows

La cabecera situada en la parte superior de la interfaz del producto ofrece espacio para un logotipo corporativo y el nombre del propio producto. Es posible cambiar el logotipo, lo que suele incluir el nombre del producto, mediante un parámetro de configuración. Para cambiar o eliminar el nombre del producto en una pestaña del navegador, debe realizar un cambio en el Registro de Windows.

Para cambiar el nombre del producto:

1. En el servidor de PlateSpin, ejecute `regedit`.
2. En el Editor del Registro de Windows, diríjase a la clave de registro siguiente:

   `HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\ProtectServer\ProductName`

Nota: en algunos casos, la clave de registro se encuentra en esta ubicación:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\Protect`

3. Haga doble clic en la clave `ProductName` y cambie el valor de **Datos de valor** de la clave como prefiera. A continuación, haga clic en **Aceptar.**
4. Reinicie el servidor IIS para que se aplique el cambio de la interfaz.

Preparación de los destinos y los orígenes de protección

Antes de poder configurar los contratos de protección, debe identificar los contenedores de destino y las cargas de trabajo de origen previstos. Los detalles sobre los destinos y las cargas de trabajo se obtienen mediante un proceso de inventario.

- Capítulo 9, “Preparación de contenedores (destinos de protección)”, en la página 95
- Capítulo 10, “Preparación de cargas de trabajo (orígenes de protección)”, en la página 99
- Capítulo 11, “Preparación de controladores de dispositivos para los destinos de failback físicos”, en la página 105
- Capítulo 12, “Preparación para proteger cargas de trabajo Linux”, en la página 117
- Capítulo 13, “Preparación para proteger clústeres de Windows”, en la página 121
- Capítulo 14, “Solución de problemas de descubrimiento e inventario de cargas de trabajo”, en la página 131
- Apéndice B, “Distribuciones de Linux compatibles con Protect”, en la página 137
- Apéndice C, “Sincronización de números de serie en el almacenamiento local del nodo de clústeres”, en la página 141
- Apéndice D, “Utilidad Protect Agent”, en la página 143

9 Preparación 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. Al añadir un contenedor de destino, la base de datos de PlateSpin Protect se rellena con información de inventario detallada sobre el contenedor y sus recursos. El inventario proporciona los datos necesarios para determinar el uso del contenedor y configurar correctamente uno o varios contratos de protección de la carga de trabajo para el contenedor de destino.

- Sección 9.1, “Acerca de los contenedores (destinos de protección)”, en la página 95
- Sección 9.2, “Adición de contenedores (destinos de protección)”, en la página 96
- Sección 9.3, “Actualización de los detalles del contenedor”, en la página 98
- Sección 9.4, “Eliminación de contenedores (destinos de protección)”, en la página 98

9.1 Acerca de los contenedores (destinos de protección)

La interfaz Web de PlateSpin proporciona un inventario automatizado de las plataformas de contenedor de destino compatibles.

- Sección 9.1.1, “Contenedores compatibles”, en la página 95
- Sección 9.1.2, “Requisitos de acceso a la red para contenedores”, en la página 95
- Sección 9.1.3, “Directrices de los parámetros para los contenedores”, en la página 95

9.1.1 Contenedores compatibles

Antes de añadir un contenedor al servidor de PlateSpin, asegúrese de que la versión del contenedor de máquinas virtuales sea compatible. Consulte “Contenedores de máquina virtual compatibles” en la página 17.

9.1.2 Requisitos de acceso a la red para contenedores

Antes de comenzar las operaciones de inventario, asegúrese de que el servidor de PlateSpin puede comunicarse con las cargas de trabajo de origen y de destino. Consulte la Sección 1.5.2, “Requisitos de red para los contenedores”, en la página 31.

9.1.3 Directrices de los parámetros para los contenedores

En la Tabla 9-1 se proporcionan directrices para seleccionar el tipo de equipo, el formato de credenciales y la sintaxis de los parámetros de inventario para los hosts de destino mediante la interfaz Web.

Tabla 9-1 *Directrices de los parámetros de descubrimiento de la interfaz de Web para los contenedores de destino*

Para descubrir	Tipo de destino	Credenciales
Clúster de VMware vCenter	**Clúster DRS de VMware**	Credenciales de servicio Web de VMware vCenter (nombre de usuario y contraseña)
VMware ESXi Server	**ESX Server de VMware**	Cuenta de ESX con función de administrador O bien Credenciales del dominio Windows (solo versiones 4 y 4.1)

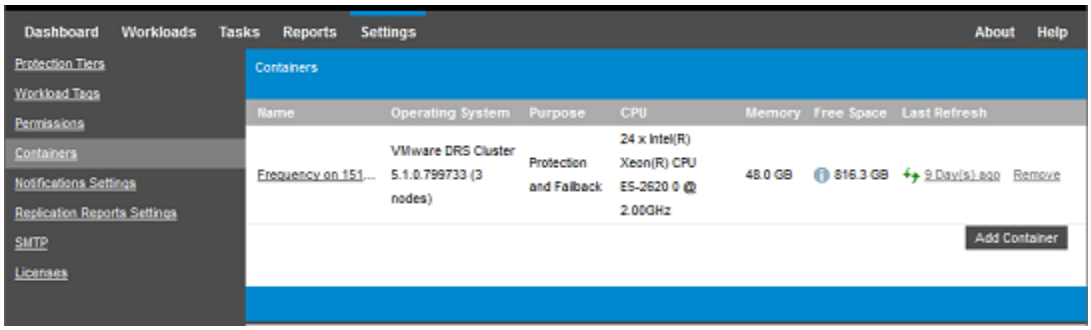
9.2 Adición de contenedores (destinos de protección)

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. PlateSpin Protect permite usar contenedores para la protección y la operación de failback.

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, seleccione **Settings > Containers > Add Container** (Configuración > Contenedores > Añadir contenedor).



2 Especifique el tipo de contenedor:

- **ESX Server de VMware**
- **Clúster DRS de VMware**

3 Dependiendo del tipo de destinos de que haya seleccionado en los pasos anteriores, especifique la información de acceso oportuna.

Tabla 9-2 *Opciones para un destino de clúster DRS de VMware*

Opción	Descripción
Nombre de host o IP de vCenter	Indique el nombre de host o la dirección IP del servidor de vCenter.

Opción	Descripción
Nombre de host o IP de vCenter	Indique el nombre de host o la dirección IP del servidor de vCenter.

- **Clúster DRS de VMware:** consulte la Tabla 9-3.
- **VMware ESX Server:** consulte la Tabla 9-4.

Tabla 9-3 *Opciones para un destino de clúster DRS de VMware*

Opción	Descripción
Nombre de host o IP de vCenter	Indique el nombre de host o la dirección IP del servidor de vCenter.

Opción	Descripción
Nombre de host o IP de vCenter	Indique el nombre de host o la dirección IP del servidor de vCenter.

Tabla 9-4 *Opciones para el destino de VMware ESX Server*

Opción	Descripción
Nombre de host o IP	Especifique el nombre de host o la dirección IP de VMware ESX Server.
Usuario y contraseña	Especifique las credenciales de administrador para acceder al contenedor de destino. Consulte "Directrices para las credenciales de carga de trabajo y contenedor" en la página 167.

4 Haga clic en **Test Credentials** (Probar credenciales) para validar los valores de la credenciales especificadas.

5 Seleccione el propósito del contenedor de máquinas virtuales:

- **Protección**
- **Failback**
- **Protección y failback**

Si selecciona tanto **Protección** como **Failback,** el contenedor estará disponible para su selección como destino en las operaciones de protección y en las de failback.

6 Haga clic en **Add** (Añadir) para añadir y descubrir detalles sobre el contenedor y mostrarlos en la página Containers (Contenedores).

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) .

9.3 Actualización de los detalles del contenedor

Debe actualizar periódicamente los detalles de los contenedores de destino antes de configurar o ejecutar un contrato de protección. La interfaz Web de PlateSpin permite actualizar los recursos descubiertos para los contenedores de destino virtuales.

Cuando se actualiza el destino, los recursos asociados se vuelven a descubrir automáticamente y se actualizan. Los contenedores se pueden actualizar de uno en uno.

Para actualizar los detalles de un contenedor de destino:

1. En la interfaz de PlateSpin, seleccione **Settings > Containers** (Configuración > Contenedores).
2. Haga clic en el icono **Refresh** (Actualizar) junto al contenedor que desee actualizar.

   Se volverá a realizar el inventario del contenedor.
3. Expanda los paneles de la página Container Details (Detalles del contenedor) para obtener información acerca de los cambios del inventario.

9.4 Eliminación de contenedores (destinos de protección)

Si elimina todos los contratos de protección de un contenedor de destino, puede eliminar (anular el descubrimiento) del contenedor de destino. También puede eliminar un contenedor que ya no se utilice.

Importante: antes de suprimir un contenedor de destino que esté en uso para el contrato de protección de carga de trabajo configurado, debe asegurarse de que todos los contratos afectados se han eliminado o se han reconfigurado para un contenedor de destino diferente.

Para eliminar un destino mediante la interfaz Web:

1. En la interfaz de PlateSpin, seleccione **Settings > Containers** (Configuración > Contenedores).
2. En la página Containers (Contenedores), haga clic en la opción **Remove** (Eliminar) situada junto al contenedor que desea eliminar de Protect.

10 Preparación de cargas de trabajo (orígenes de protección)

Para cualquier contrato de protección es imprescindible disponer de una carga de trabajo de origen y de un contenedor de destino. Al añadir una carga de trabajo al servidor de PlateSpin Protect, la base de datos de PlateSpin se completa con información detallada de inventario acerca del equipo. Esta información proporciona los datos necesarios para determinar el uso del equipo y configurar correctamente un contrato de protección.

- Sección 10.1, “Acerca de las cargas de trabajo (orígenes de protección)”, en la página 99
- Sección 10.2, “Adición de cargas de trabajo (orígenes de protección)”, en la página 100
- Sección 10.3, “Etiquetado de cargas de trabajo”, en la página 101
- Sección 10.4, “Actualización de los detalles de la carga de trabajo”, en la página 102
- Sección 10.5, “Eliminación de cargas de trabajo”, en la página 103

10.1 Acerca de las cargas de trabajo (orígenes de protección)

La interfaz Web de PlateSpin proporciona un inventario automatizado de las configuraciones de cargas de trabajo de origen compatibles.

- Sección 10.1.1, “Cargas de trabajo compatibles”, en la página 99
- Sección 10.1.2, “Requisitos de acceso a la red para las cargas de trabajo de origen”, en la página 100
- Sección 10.1.3, “Directrices de parámetros para las cargas de trabajo de origen”, en la página 100

10.1.1 Cargas de trabajo compatibles

Antes de añadir una carga de trabajo al servidor de PlateSpin, asegúrese de que la versión del sistema operativo y el hardware de la carga de trabajo sean compatibles. Consulte los apartados siguientes en la Sección 1.1, “Configuraciones compatibles”, en la página 13:

- “Cargas de trabajo Windows compatibles” en la página 14
- “Cargas de trabajo Linux compatibles” en la página 15
- “Arquitecturas de cargas de trabajo compatibles” en la página 19
- “Almacenamiento admitido” en la página 21

10.1.2 Requisitos de acceso a la red para las cargas de trabajo de origen

Para obtener información sobre los requisitos de acceso a la red para el inventario de las cargas de trabajo Windows y Linux, consulte la Sección 1.5.3, “Requisitos de red para las cargas de trabajo”, en la página 32.

10.1.3 Directrices de parámetros para las cargas de trabajo de origen

En la Tabla 10-1 se proporcionan directrices para seleccionar el tipo de equipo, el formato de credenciales y la sintaxis de los parámetros de inventario para las cargas de trabajo.

Tabla 10-1 *Directrices de los parámetros de descubrimiento para cargas de trabajo*

Para descubrir	Tipo de máquina	Credenciales	Observaciones
Todas las cargas de trabajo Windows	**Windows**	Credenciales locales o de administrador de dominio.	Para el nombre de usuario, use este formato: ◆ Para equipos miembros del dominio: *autoridad\principal* ◆ Para equipos miembros del grupo de trabajo: *nombre de host\principal*
Todas las cargas de trabajo Linux	**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 `sudo`. Consulte el artículo 7920711 de la base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7920711).

10.2 Adición de cargas de trabajo (orígenes de 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).

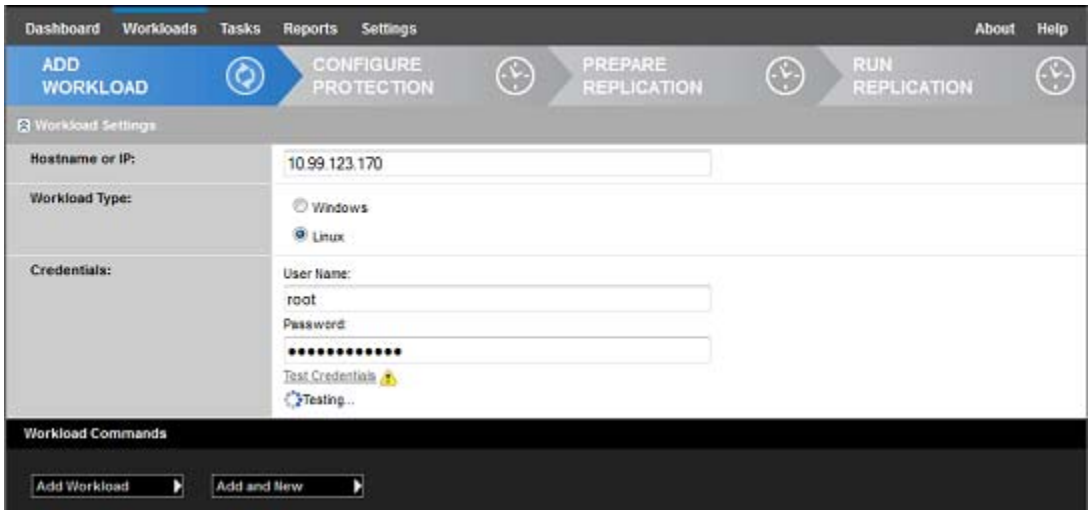
Para añadir una carga de trabajo:

1 Siga los pasos preparatorios necesarios.

Consulte el apartado Preparación en “Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo” en la página 37.

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

En la interfaz Web 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 167.

  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 que 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).

5 (Condicional) Si aún no ha añadido un contenedor para usarlo con esta carga de trabajo, añada uno a fin de preparar la protección de la carga de trabajo. Consulte "Preparación de contenedores (destinos de protección)" en la página 95.

6 Continúe con "Configuración de los detalles de protección y preparación de la réplica" en la página 151.

10.3 Etiquetado de cargas de trabajo

En la interfaz Web de PlateSpin, la página Workloads (Cargas de trabajo) puede mostrar una larga lista de cargas de trabajo. Buscar en esa lista para gestionar las cargas de trabajo similares puede llevar mucho tiempo. Para solucionar este problema, puede crear etiquetas para varias categorías de cargas de trabajo, departamentos u otras asociaciones lógicos correspondientes a su entorno.

Para obtener información sobre cómo crear, modificar o suprimir etiquetas de cargas de trabajo, consulte la Sección 7.1, "Creación y gestión de etiquetas de cargas de trabajo", en la página 79.

Después de crear etiquetas, estas están disponibles en la parte inferior de la página Edit Target Details (Editar detalles del destino), donde podrá asignar una etiqueta a las cargas de trabajo oportunas. La página Workloads (Cargas de trabajo) incluye la columna **Tag** (Etiqueta), donde se muestra cada etiqueta que haya asociado con una carga de trabajo. Puede ordenar esta columna para que las cargas de trabajo similares estén juntas. De ese modo, podrá localizar y ejecutar fácilmente operaciones sobre todas las cargas de trabajo etiquetadas al mismo tiempo.

Nota: al exportar una carga de trabajo con un valor de etiqueta a un nuevo servidor, la configuración de la etiqueta se mantendrá.

Para asociar una etiqueta a una carga de trabajo durante el paso de configuración de la protección:

1. En la interfaz Web de Protect, haga clic en **Workloads** (Cargas de trabajo).
2. En la lista de cargas de trabajo, seleccione la carga de trabajo que desee etiquetar y haga clic en **Configure Protection** (Configurar protección).
3. Configure la carga de trabajo.
4. En la sección Tag (Etiqueta) en la parte inferior de la página Edit Target Details (Editar detalles del destino), seleccione el nombre de la etiqueta que desea asociar con la carga de trabajo.
5. Haga clic en **Save** (Guardar).

Para añadir o modificar una etiqueta asociada con la carga de trabajo configurada:

1. En la interfaz Web de Protect, haga clic en **Workloads** (Cargas de trabajo).
2. En la lista de cargas de trabajo, haga clic en la que desee etiquetar para abrir la página Target Details (Detalles del destino).
3. Haga clic en **Editar**.
4. En la sección Tag (Etiqueta) en la parte inferior de la página Edit Target Details (Editar detalles del destino), seleccione el nombre de la etiqueta que desea asociar con la carga de trabajo.
5. Haga clic en **Guardar.**

Para disociar una etiqueta de una carga de trabajo:

1. En la interfaz Web de Protect, haga clic en **Workloads** (Cargas de trabajo).
2. En la lista de cargas de trabajo, seleccione la carga cuya etiqueta desee eliminar y haga clic en **Configure Protection** (Configurar protección).
3. En la sección Tag (Etiqueta) de la página de configuración, seleccione la cadena vacía y haga clic en **Save** (Guardar).

10.4 Actualización de los detalles de la carga de trabajo

La interfaz Web de PlateSpin no admite la actualización de los detalles de las cargas de trabajo descubiertas. Para actualizar los detalles de una carga de trabajo descubierta, debe eliminar la carga de trabajo y, a continuación, añadir y descubrir sus detalles de nuevo. Los detalles de configuración se pierden si la carga de trabajo se encuentra en un estado configurado cuando se elimina. Si hay una licencia de protección en uso, se elimina de la carga de trabajo y se devuelve al repositorio de licencias. Consulte la Sección 10.5, “Eliminación de cargas de trabajo”, en la página 103.

10.5 Eliminación de cargas de trabajo

En algunas circunstancias, puede ser necesario eliminar una carga de trabajo del inventario de 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).
2. (Condicional, Windows) Para las cargas de trabajo Windows protegidas anteriormente mediante la réplica de nivel de bloques, la interfaz Web 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.
3. En la página de confirmación del comando, haga clic en **Confirm** (Confirmar) para ejecutar el comando.

   Espere a que se complete el proceso.
4. (Condicional, Linux) Para las cargas de trabajo Linux, desinstale manualmente el controlador basado en bloques de la carga de trabajo de origen. Consulte Software de transferencia de datos en el nivel de bloques en Limpieza de las cargas de trabajo Linux.

11 Preparación de controladores de dispositivos para los destinos de failback físicos

PlateSpin Protect proporciona una biblioteca de controladores de dispositivos y de ID de Plug and Play (PnP) que se necesitan si dispone de equipos físicos como destinos de failback. Puede añadir controladores de dispositivos personalizados y asignaciones de ID de PnP mediante la herramienta PlateSpin Device Driver (`DeviceDriver.exe`).

- Sección 11.1, “Gestión de controladores de dispositivo”, en la página 105
- Sección 11.2, “Gestión de las asignaciones de ID de PnP de PlateSpin”, en la página 109

11.1 Gestión de controladores de dispositivo

PlateSpin Protect incluye una biblioteca de controladores de dispositivos que instala automáticamente los controladores correspondientes en las cargas de trabajo de destino. Si en el equipo de destino físico de failback 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.

- Sección 11.1.1, “Empaquetado de controladores de dispositivo para cargas de trabajo Windows”, en la página 105
- Sección 11.1.2, “Empaquetado de controladores de dispositivo para cargas de trabajo Linux”, en la página 106
- Sección 11.1.3, “Carga de paquetes de controladores a la base de datos de controladores de dispositivo de PlateSpin”, en la página 106

11.1.1 Empaquetado de controladores de dispositivo para cargas de trabajo Windows

Debe empaquetar los controladores de dispositivos de Windows a fin de prepararlos para la carga en la base de datos de controladores de PlateSpin Protect.

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

- Todos los sistemas Windows de 64 bits
- Las versiones de 32 bits de los sistemas Windows Server 2008

Para empaquetar controladores de dispositivos de Windows:

1. Prepare todos los archivos de controlador interdependientes (`*.sys`, `*.inf`, `*.dll`, etc.) para la infraestructura de destino y el dispositivo.

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.

El paquete ya está listo para cargarse. Consulte "Carga de paquetes de controladores a la base de datos de controladores de dispositivo de PlateSpin" en la página 106.

11.1.2 Empaquetado de controladores de dispositivo para cargas de trabajo Linux

Debe empaquetar los controladores de dispositivos de Linux a fin de prepararlos para la carga en la base de datos de controladores de PlateSpin Protect. En la imagen ISO de arranque de PlateSpin se incluye una utilidad personalizada para este propósito (`bootofx.x2p.iso`).

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 o con firmware UEFI:

   ```
   # mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.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 paquetes de controladores a la base de datos de controladores de dispositivo de PlateSpin" en la página 106.

11.1.3 Carga de paquetes de controladores a la base de datos de controladores de dispositivo de PlateSpin

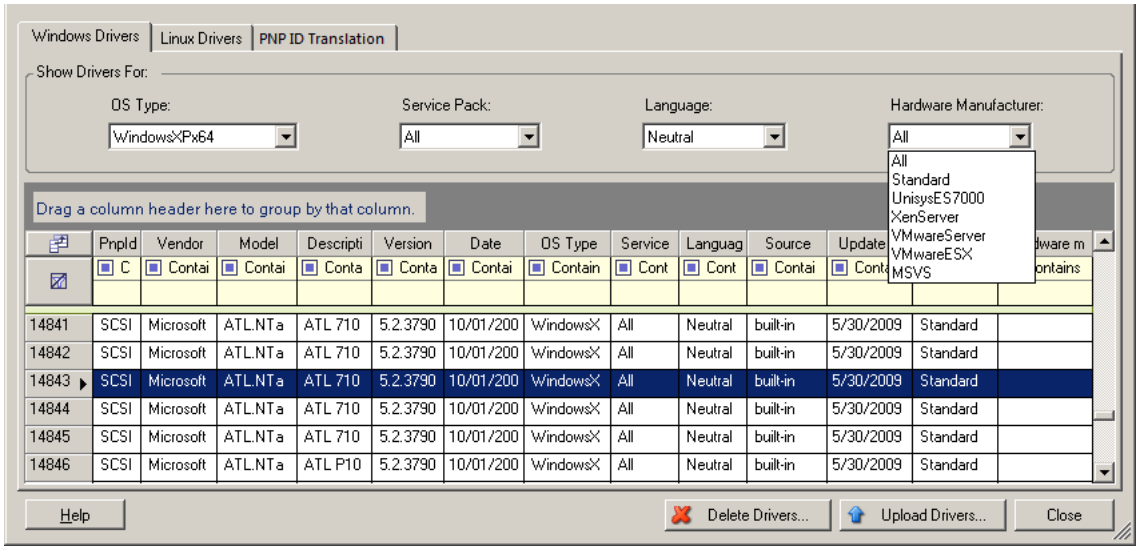
Use la herramienta PlateSpin Driver Manager para cargar controladores de dispositivo a la base de datos de controladores.

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

- "Procedimiento de carga de controladores de dispositivo (Windows)" en la página 107
- "Procedimiento de carga de controladores de dispositivo (Linux)" en la página 108

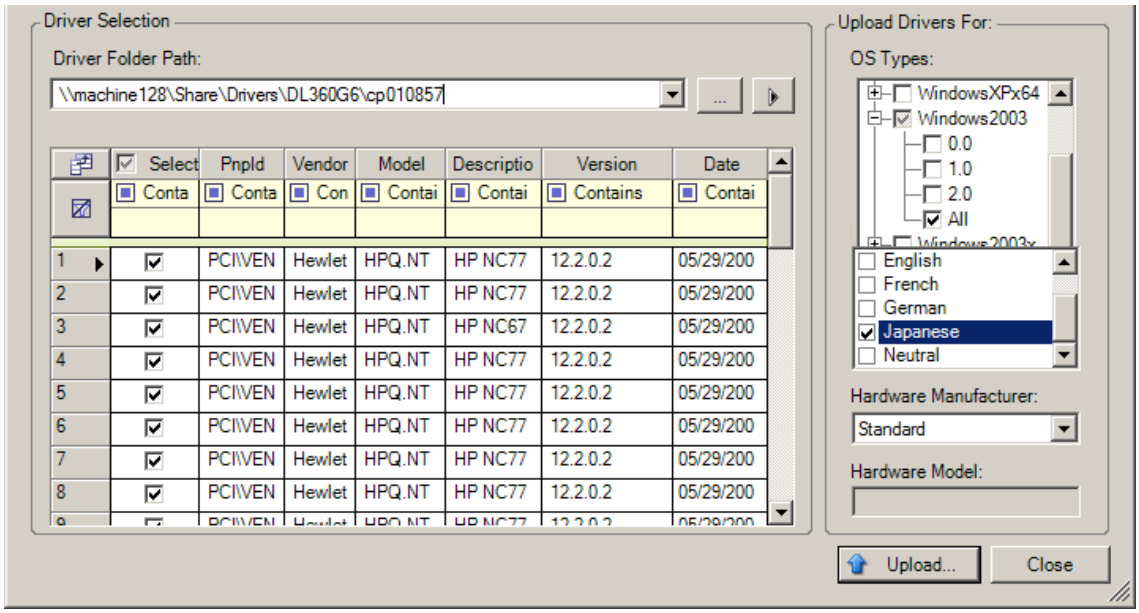
Procedimiento de carga de controladores de dispositivo (Windows)

1. Obtenga y prepare los controladores necesarios del dispositivo. Consulte "Empaquetado de controladores de dispositivo para cargas de trabajo Windows".
2. Entre como un usuario administrador al host del servidor de PlateSpin.
3. Lance la herramienta PlateSpin Driver Manager. Diríjase a `C:\Archivos de programa\PlateSpin Protect Server\DriverManager` e inicie el programa `DriverManager.exe`.
4. Seleccione **Tools** > **Manage Device Drivers** (Herramientas > Gestionar controladores de dispositivo) y seleccione la pestaña **Windows Drivers** (Controladores Windows).



5. En la parte inferior del recuadro de diálogo, haga clic en **Upload Drivers** (Cargar controladores).
6. En el recuadro de diálogo Driver Selection (Selección de controlador), 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.



7 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.

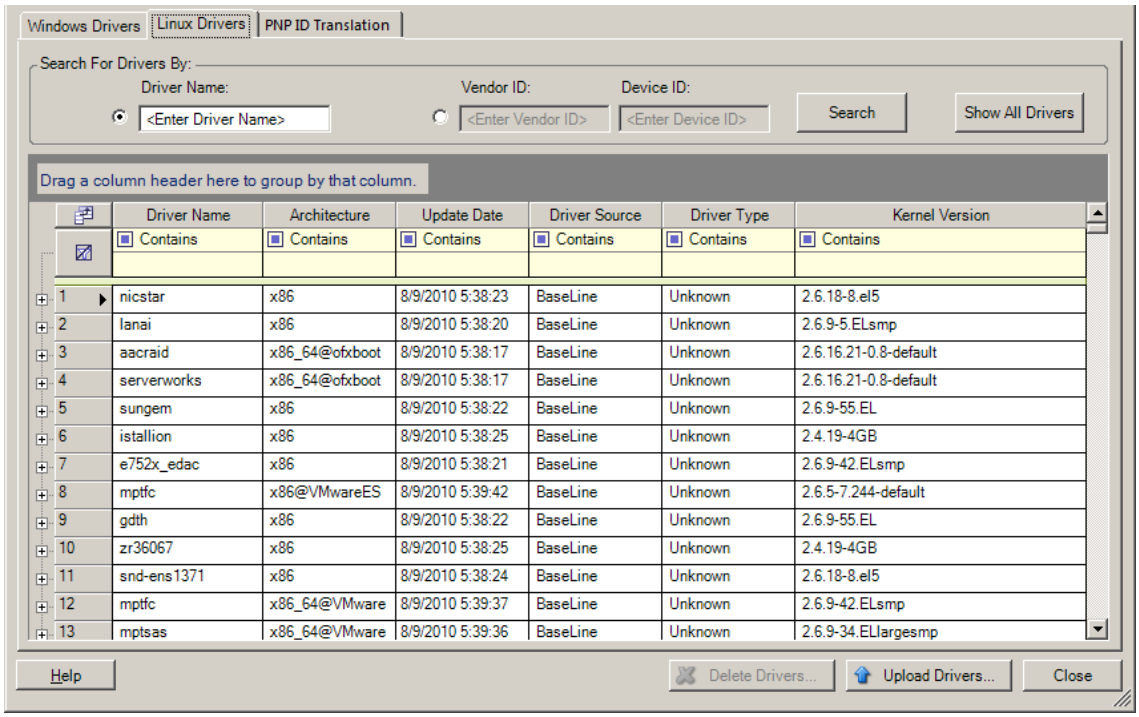
Procedimiento de carga de controladores de dispositivo (Linux)

1 Obtenga y prepare los controladores necesarios del dispositivo. Consulte "Empaquetado de controladores de dispositivo para cargas de trabajo Linux".

2 Entre como un usuario administrador al host del servidor de PlateSpin.

3 Lance la herramienta PlateSpin Driver Manager. Diríjase a `C:\Archivos de programa\PlateSpin Protect Server\DriverManager` e inicie el programa `DriverManager.exe`.

4 Seleccione **Tools** > **Manage Device Drivers** (Herramientas > Gestionar controladores de dispositivo) y seleccione la pestaña **Linux Drivers** (Controladores Linux).



5 En la parte inferior del recuadro de diálogo, haga clic en **Upload Drivers** (Cargar controladores).

6 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.

11.2 Gestión de las asignaciones de ID de PnP de PlateSpin

"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 RAM de Linux (LRD) para Protect contiene los ID de PnP con el estilo de Linux.

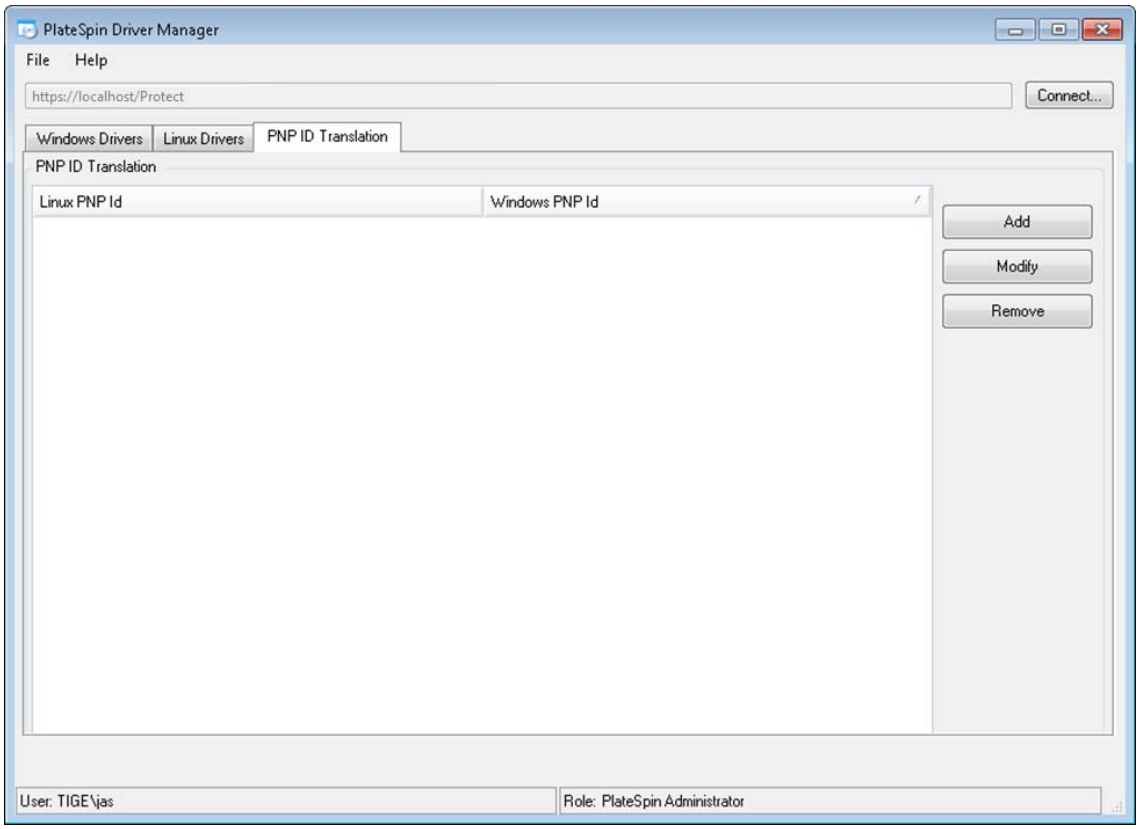
Estos ID reciben un formato coherente, por lo que PlateSpin puede aplicar una transformación estándar a cada uno de ellos para determinar su ID de PnP de Windows correspondiente. La traducción se produce de forma automática en el producto PlateSpin.

El usuario (o el equipo de asistencia técnica) puede usar la opción PNP ID Translation (Traducción de ID de PnP) de la herramienta PlateSpin Device Driver para añadir, editar o eliminar asignaciones personalizadas de ID de PnP.

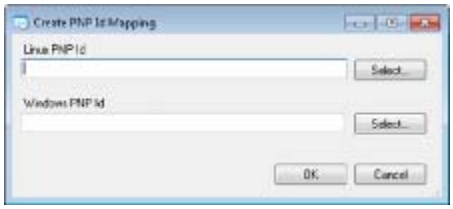
Para añadir asignaciones personalizadas de ID de PnP:

1. Entre como un usuario administrador al host del servidor de PlateSpin.
2. Lance la herramienta PlateSpin Driver Manager. Diríjase a `C:\Archivos de programa\PlateSpin Protect Server\DriverManager` e inicie el programa `DriverManager.exe`.
3. Conéctese con el servidor de PlateSpin.

   `https://localhost/Protect`
4. 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.



5 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).



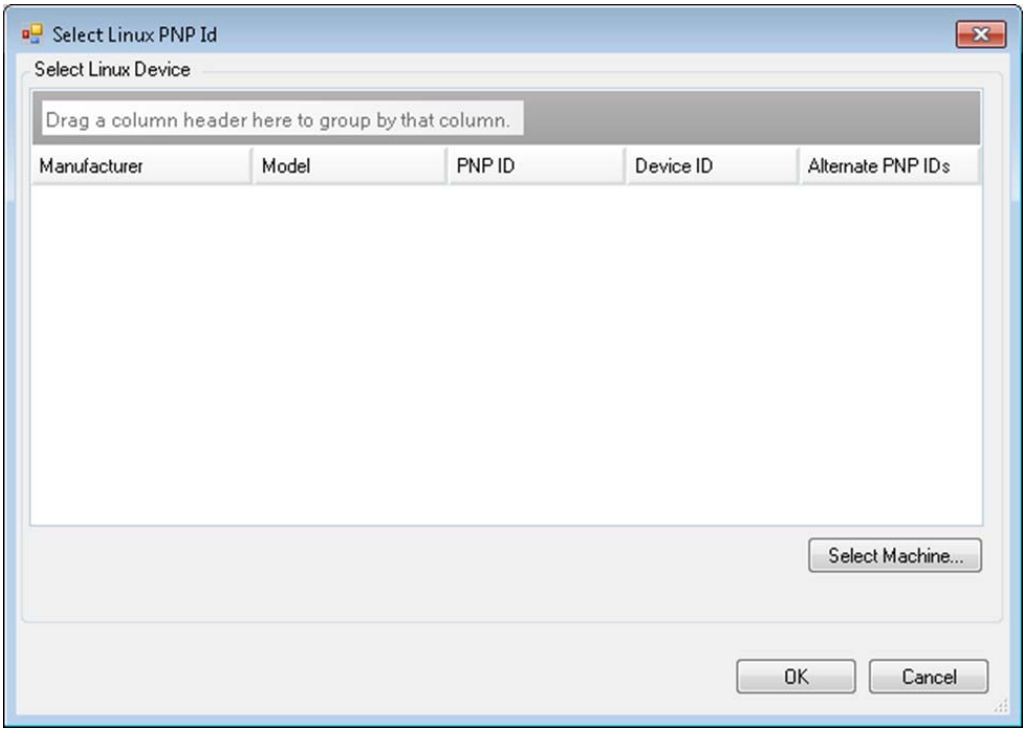
6 En el campo **Linux PNP ID** (ID de PnP de Linux), añada un ID de PnP de Linux.

6a (Condicional) Si lo conoce, escriba el ID de PnP de Linux que desea usar.

o bien

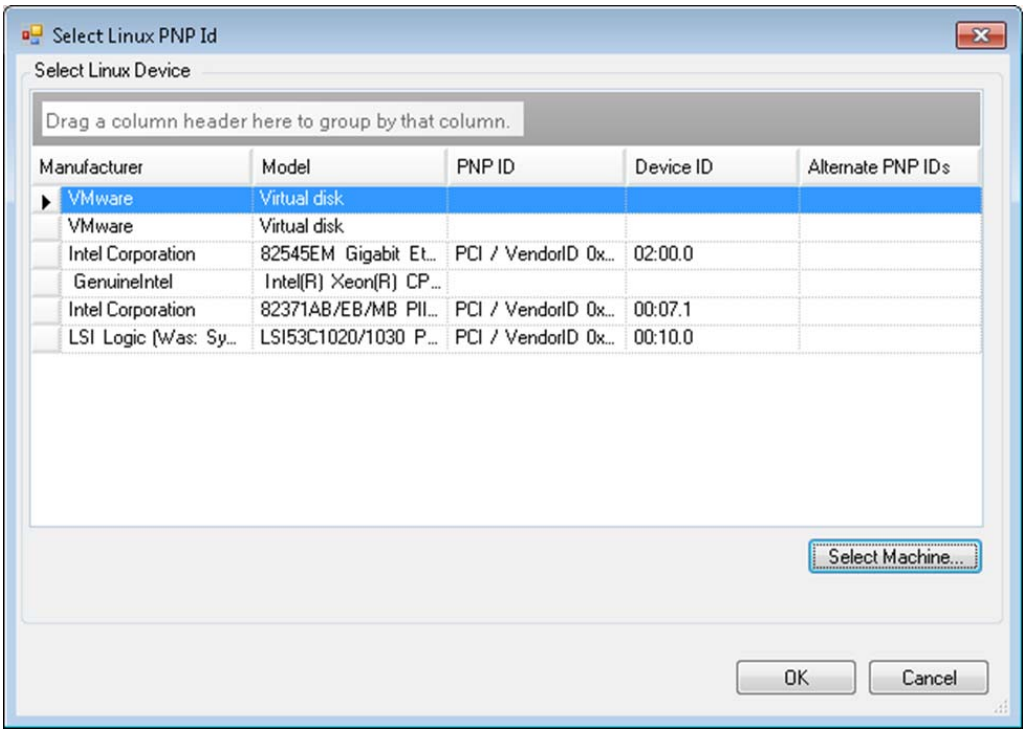
6b (Condicional) Seleccione un ID de una carga de trabajo descubierta anteriormente.

6b1 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).



6b2 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.

6b3 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).



6b4 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).

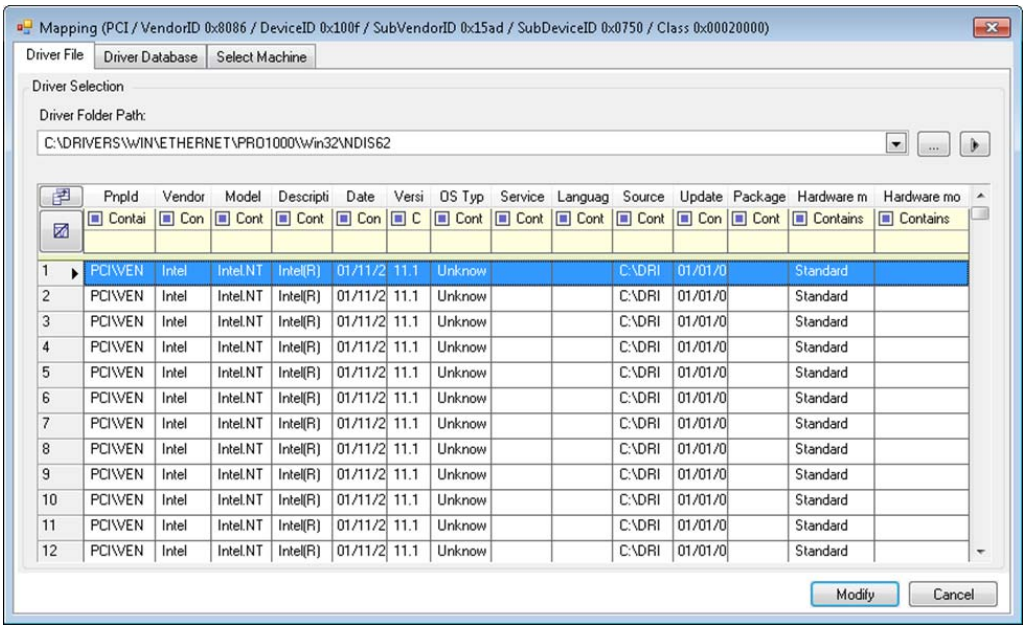
7 En el campo **Windows PNP ID** (ID de PnP de Windows), añada un ID de PnP de Windows:

7a (Condicional) Si lo conoce, escriba el ID de PnP de Windows que desea usar.

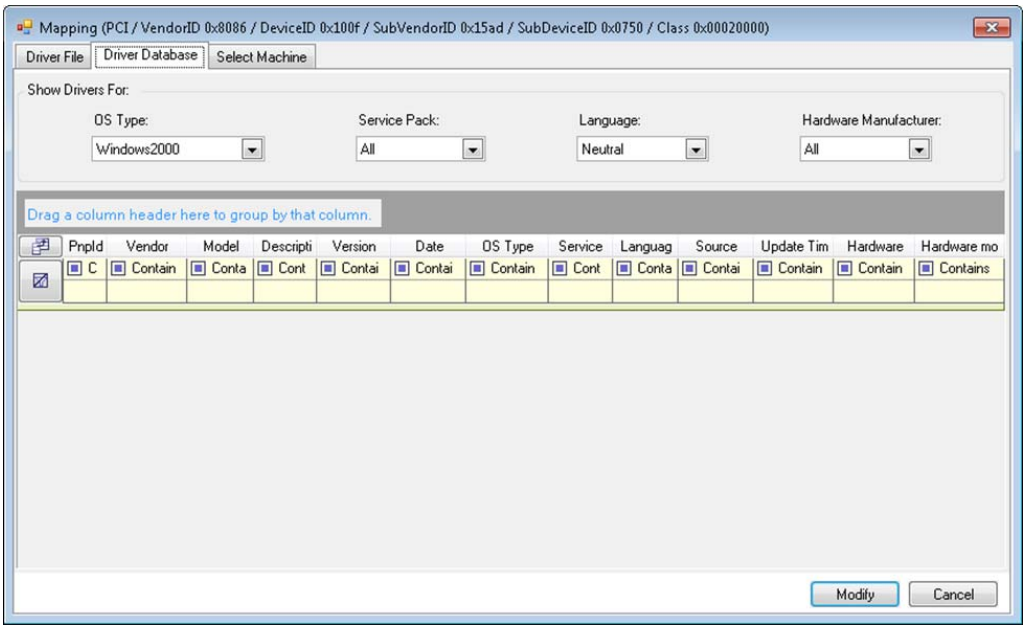
o bien

7b (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:

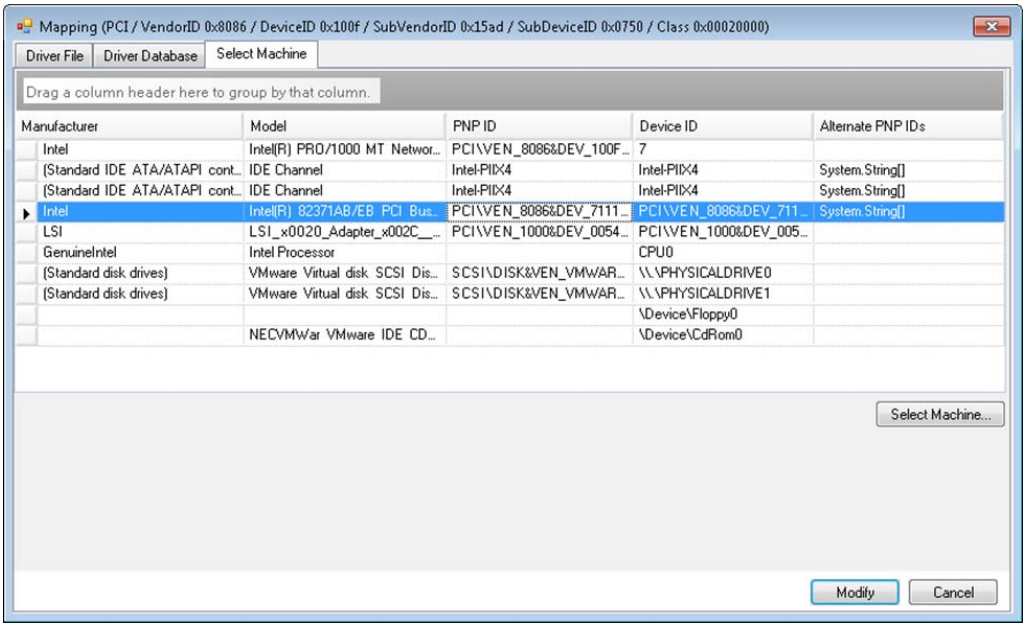
- En la pestaña **Driver File** (Archivo de controlador), busque y seleccione un archivo de controlador de Windows (es decir un archivo con la extensión `*.inf`), seleccione el ID de PnP que desee y haga clic en **Modify** (Modificar).



- 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).

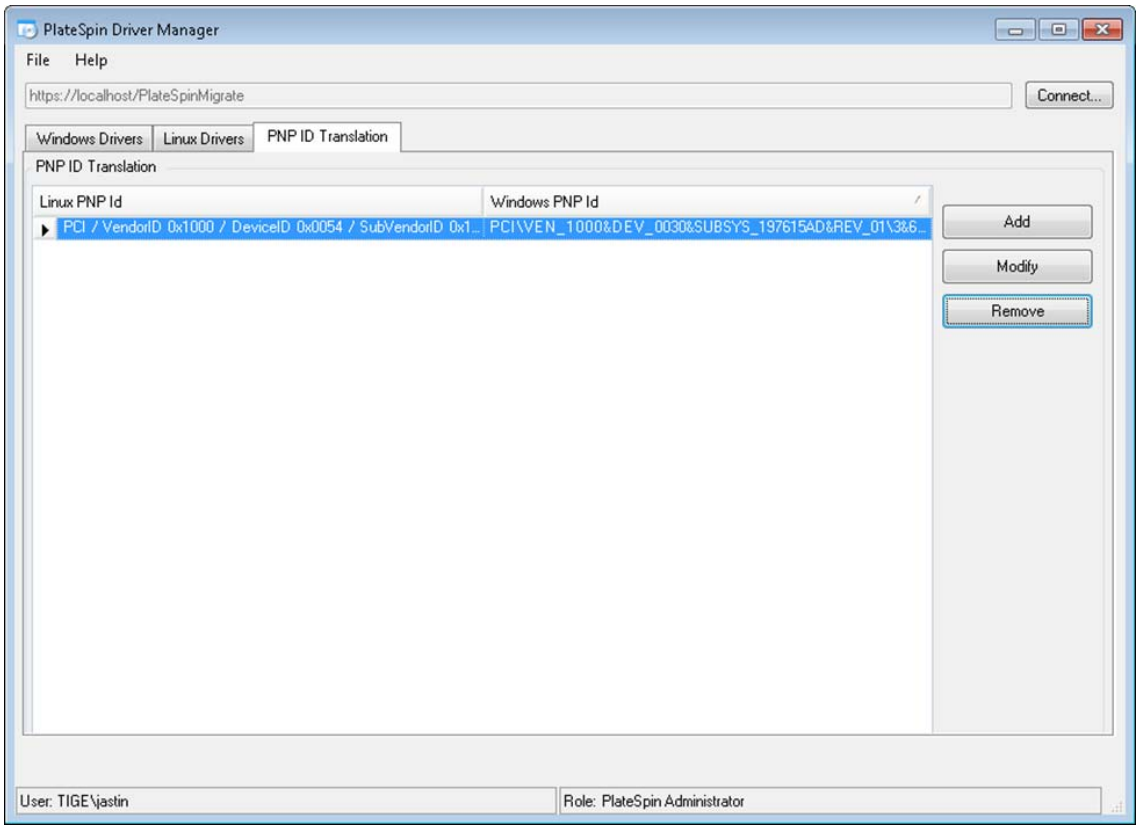


- En la pestaña **Select Machine** (Seleccionar equipo), haga clic en **Select Machine** (Seleccionar equipo) y en la lista de equipos Windows descubiertos con la función de descubrimiento activa, seleccione un equipo, haga clic en **OK** (Aceptar) para mostrar sus dispositivos, seleccione el ID de PnP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

8 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.



9 (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:

9a Haga clic en **Modify** (Modificar) para abrir el recuadro de diálogo Create PNP ID Mapping (Crear asignación de ID de PnP).

9b Repita el Paso 7 en la página 112 para modificar el ID de PnP de Windows.

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

---

12 Preparación para proteger cargas de trabajo Linux

Realice las tareas descritas en esta sección para preparar las cargas de trabajo Linux para la protección en PlateSpin Protect.

- Sección 12.1, “Verificación de los controladores basados en bloques para Linux”, en la página 117
- Sección 12.2, “Preparación de instantáneas para la transferencia a nivel de bloques (Linux)”, en la página 117
- Sección 12.3, “Uso de los guiones freeze y thaw en todas las réplicas (Linux)”, en la página 119

12.1 Verificación de los controladores basados en bloques para Linux

Compruebe que hay disponible un módulo blkwatch para la distribución Linux de la carga de trabajo. Para obtener una lista de controladores preconfigurados, consulte “Distribuciones de Linux compatibles con Protect” en la página 137.

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 base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7005873).

12.2 Preparación de instantáneas para la transferencia a nivel de bloques (Linux)

Se recomienda que prepare instantáneas para la transferencia de datos a nivel de bloques. Asegúrese de que cada grupo de volúmenes tiene espacio libre suficiente para las instantáneas (al menos un 10 % de la suma de todas las particiones). Si no hay disponibles instantáneas, Protect bloquea y libera cada bloque uno a uno en la carga de trabajo de origen para la transferencia de datos.

- Sección 12.2.1, “Configuración de instantáneas LVM para la réplica del volumen de Linux”, en la página 118
- Sección 12.2.2, “Configuración de instantáneas NSS para la réplica del repositorio NSS”, en la página 118

12.2.1 Configuración de instantáneas LVM para la réplica del volumen de Linux

El controlador `blkwatch` aprovecha las instantáneas LVM si están disponibles. Copiar bloques de la instantánea ayuda a evitar posibles conflictos de archivos abiertos.

Para el almacenamiento LVM, consulte el artículo 7005872 de la base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7005872).

12.2.2 Configuración de instantáneas NSS para la réplica del repositorio NSS

Para las cargas de trabajo Linux en las que se ejecute Open Enterprise Server, la solución de instantáneas LVM no está disponible para los repositorios NSS. Durante la réplica de repositorios NSS, Protect bloquea y libera cada bloque uno a uno para la transferencia de datos. Para evitar posibles conflictos de archivos abiertos y mejorar el rendimiento de la réplica, puede aprovechar las instantáneas del repositorio NSS para la réplica.

Puede añadir un solo disco sin formato que se utilizará para todas las instantáneas del repositorio NSS, o puede añadir un disco sin formato independiente para cada repositorio NSS. El mejor rendimiento se produce cuando se añade un disco independiente para cada repositorio. Añada el disco antes de configurar la protección de la carga de trabajo. Prepare el disco que desea utilizar y PlateSpin configurará las instantáneas NSS para el repositorio durante la réplica.

Nota: por defecto, PlateSpin usa el disco gestionado NLVM que tenga mayor cantidad de espacio libre (espacio sin particiones) para las instantáneas del repositorio NSS. Si observa que las instantáneas del repositorio NSS para la réplica se encuentran en el mismo disco que el sistema de archivos raíz o en otro disco con un flujo constante de E/S, debe usar el archivo `/etc/platespin/platespin.conf` para dirigir las instantáneas NSS en un disco adecuado.

Para obtener información sobre cómo funcionan las instantáneas NSS en Open Enterprise Server, consulte "Guidelines for Using and Managing Pool Snapshots" (http://www.novell.com/documentation/oes2015/stor_nss_lx/data/br18up4.html) (Directrices para usar y gestionar instantáneas del repositorio) en la *NSS File System Administration Guide for Linux* (Guía de administración del sistema de archivos NSS para Linux).

Para configurar uno o varios discos que se utilicen para las instantáneas de repositorios NSS:

1. En la carga de trabajo de origen OES, añada un disco Linux sin formato que se utilizará para las instantáneas de todos los repositorios NSS. Como alternativa, puede crear un disco independiente para cada repositorio NSS.

   El tamaño del disco debe ser de alrededor del 20 % de la cantidad de datos usadas en el repositorio NSS. Ajuste el tamaño según la cantidad de cambio o de crecimiento de datos que pueda producirse durante el intervalo de tiempo que dure una réplica.

2. Para cada disco que cree en el Paso 1, inicialice el disco que NLVM debe gestionar.

   Puede utilizar los comandos de NSSMU o NLVM para inicializar el disco. El formato del dispositivo puede ser GPT o DOS.

   - Para usar NSSMU:
     1. Lance NSSMU y seleccione **Devices** (Dispositivos).
     2. Seleccione el nuevo disco y pulse F3 para inicializarlo.

- Para utilizar comandos de NLVM:
  1. En la línea de comandos de , escriba

     `NLVM init <device_name> [format]`

3 Debe especificar qué disco se usará para cada instantánea del repositorio NSS. Cree un archivo `platespin.conf` en la carga de trabajo de origen OES y asociar los repositorios NSS con los discos nuevos:

3a En un editor de textos, cree un archivo en `/etc/platespin/platespin.conf`.

3b Para cada repositorio NSS, añada la información del dispositivo y el tamaño en el parámetro `Customlocation` con la sintaxis siguiente:

`[Ubicaciónpersonalizada] /dev/pool/<nombreDelRepositorio>=<dispositivo>:<tamañoMáxPartición-en-MB>`

Por ejemplo, especifique la siguiente entrada para un repositorio denominado `NSSPOOL` para añadir las instantáneas en el dispositivo `sdc` con un tamaño máximo de 12228 MB.

`[Ubicaciónpersonalizada] /dev/pool/NSSPOOL=sdc:12288`

4 Guarde el archivo.

5 Continúe configurando la protección de la carga de trabajo OES de origen.

12.3 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 171). 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`

13 Preparación para proteger clústeres de Windows

PlateSpin Protect admite la protección de servicios empresariales de un clúster de Microsoft Windows. Los sistemas operativos de clúster de Microsoft Windows compatibles son:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows Server 2003 R2

Para obtener más información, consulte “Clústeres” en la Sección 1.1.1, “Cargas de trabajo Windows compatibles”, en la página 14.

Nota: el software de gestión de clúster de Windows proporciona control sobre el failover y el failback para los recursos que se ejecutan en sus nodos de clústeres. En este documento, esta acción se denomina *failover de nodo de clústeres* o *failback de nodo de clústeres*.

El servidor de PlateSpin proporciona control sobre el failover y el failback para la carga de trabajo protegida que representa el clúster. En este documento, esta acción se denomina *failover de PlateSpin* o *failback de PlateSpin*.

- Sección 13.1, “Planificación para proteger la carga de trabajo de clúster”, en la página 121
- Sección 13.2, “Configuración de descubrimiento del nodo activo de Windows”, en la página 127
- Sección 13.3, “Configuración del método de transferencia basada en bloques para clústeres”, en la página 128
- Sección 13.4, “Adición de valores de búsqueda de nombres de recursos”, en la página 128
- Sección 13.5, “Tiempo límite de arbitraje de quórum”, en la página 129
- Sección 13.6, “Configuración de los números de serie del volumen local”, en la página 129
- Sección 13.7, “Failover de PlateSpin”, en la página 129
- Sección 13.8, “Failback de PlateSpin”, en la página 130

13.1 Planificación para proteger la carga de trabajo de clúster

Si el descubrimiento del nodo activo está habilitado (opción por defecto) para el entorno de PlateSpin, la protección de un clúster de Windows 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. Si se inhabilita el descubrimiento del nodo activo, cada nodo de un clúster de Windows puede descubrirse y protegerse como nodos independientes.

Antes de configurar los clústeres de Windows para su protección, asegúrese de que el entorno cumple los requisitos previos y de que entiende las condiciones para proteger las cargas de trabajo de clúster.

- Sección 13.1.1, “Requisitos para la protección del clúster”, en la página 122
- Sección 13.1.2, “Transferencia basada en bloques para los clústeres”, en la página 123
- Sección 13.1.3, “Impacto del failover del nodo de clúster en la réplica”, en la página 125
- Sección 13.1.4, “Similitud del nodo de clúster”, en la página 126
- Sección 13.1.5, “Configuración de la protección”, en la página 127

13.1.1 Requisitos para la protección del clúster

La cobertura de asistencia técnica para la protección del clúster está sujeta a las condiciones descritas en la Tabla 13-1. Tenga en cuenta estos requisitos cuando configure la protección de los clústeres en su entorno de PlateSpin.

Tabla 13-1 *Requisitos de protección del clúster*

Requisito	Descripción
Descubrir el nodo activo como un clúster de Windows	El valor de configuración global de PlateSpin `DiscoverActiveNodeAsWindowsCluster` determina si los clústeres de Windows están protegidos como clústeres o equipos independientes: ◆ **True (Verdadero, opción por defecto):** el nodo activo se descubre como un clúster de Windows. ◆ **False (Falso):** los nodos individuales se pueden descubrir como equipos independientes. Consulte la Sección 13.2, “Configuración de descubrimiento del nodo activo de Windows”, en la página 127.
Valores de búsqueda del nombre del recurso	El valor de configuración global de PlateSpin `MicrosoftClusterIPAddressNames` determina los nombres de recurso del clúster que se pueden descubrir en el entorno de PlateSpin. debe configurar los valores de búsqueda que permiten diferenciar el nombre del recurso de dirección IP del clúster compartido del nombre de otros recursos de dirección IP que pueda haber en el clúster. Consulte la Sección 13.4, “Adición de valores de búsqueda de nombres de recursos”, en la página 128.

Requisito	Descripción
Modo de clúster de Windows	El valor de configuración global de PlateSpin `WindowsClusterMode` determina el método de transferencia de datos basada en bloques para las réplicas incrementales: ◆ **Por defecto:** sincronización sin controlador. ◆ **SingleNodeBBT:** transferencia basada en bloques basada en controlador. Consulte lo siguiente. ◆ “Transferencia basada en bloques para los clústeres” en la página 123 ◆ “Configuración del método de transferencia basada en bloques para clústeres” en la página 128
Nombre de host o dirección IP del nodo activo	Debe especificar el nombre de host o la dirección del nodo activo del clúster cuando realice una operación **Add Workload** (Añadir carga de trabajo). Debido a los cambios de seguridad efectuados por Microsoft, los clústeres de Windows ya no se pueden descubrir mediante el nombre del clúster virtual (es decir, con la dirección IP del clúster compartido).
Nombre de host resoluble	El servidor de PlateSpin también debe ser capaz de resolver el nombre de host de cada nodo del clúster según sus direcciones IP. **Nota:** se requieren una búsqueda directa y una búsqueda inversa de DNS para resolver el nombre de host por su dirección IP.
Recurso de quórum	es preciso coubicar un recurso de quórum de clúster en el nodo junto al grupo de recursos del clúster (servicio) que se va a proteger.
Similitud de los nodos de clúster	En el modo de clúster de Windows por defecto, la sincronización sin controlador puede continuar desde cualquier nodo que se convierta en el nodo activo si los nodos son similares. Si no coinciden, las réplicas solo se pueden producir en el nodo activo descubierto originalmente. Consulte “Similitud del nodo de clúster” en la página 126.
PowerShell 2.0	Windows PowerShell 2.0 debe estar instalado en todos los nodos del clúster.

13.1.2 Transferencia basada en bloques para los clústeres

La transferencia basada en bloques para los clústeres funciona de forma distinta que para los servidores independientes. La réplica inicial crea una copia completa o bien utiliza un método de sincronización sin controlador en el nodo activo del clúster. Las réplicas incrementales posteriores pueden utilizar un método sin controlador o uno basado en el controlador para la transferencia de datos basada en bloques.

Nota: Protect no admite la transferencia basada en archivos para los clústeres.

El valor de configuración global de PlateSpin `WindowsClusterMode` determina el método de transferencia de datos basada en bloques para las réplicas incrementales:

- **Por defecto:** sincronización sin controlador.
- **SingleNodeBBT:** transferencia basada en bloques basada en controlador. Use solo SAN de Fibre Channel.

Advertencia: no intente utilizar SingleNodeBBT en clústeres con unidades iSCSI compartidas, ya que el clúster terminaría siendo inservible.

En la Tabla 13-2 se describen y se comparan los dos métodos.

Tabla 13-2 *Comparación de los métodos de transferencia de datos basada en bloques para la réplica Incremental*

Consideración	BBT por defecto	BBT de un solo nodo
Método de transferencia de datos	Se usa la sincronización sin controlador con una réplica basada en MD5 en el nodo activo en ese momento.	Se usa un controlador BBT instalado en el nodo activo descubierto originalmente.
Rendimiento	Las réplicas incrementales serán potencialmente lentas.	Mejora considerablemente el rendimiento de las réplicas incrementales.
Controladores	◆ No hay ningún controlador BBT que instalar. ◆ No es necesario rearrancar en los nodos de clúster de origen.	◆ Utilice la utilidad Protect Agent para instalar un controlador BBT en el nodo activo descubierto originalmente del clúster. ◆ Reinicie el nodo para que se aplique el controlador. De esta forma, se inicia un failover a otro nodo del clúster. Después del rearranque, vuelva a convertir el nodo descubierto originalmente en el nodo activo. ◆ El mismo nodo debe permanecer activo para que las réplicas se produzcan y para usar la transferencia basada en bloques de un solo nodo. ◆ Después de instalar el controlador BBT, debe producirse una réplica completa o una réplica incremental sin controlador antes de que puedan comenzar las réplicas incrementales basadas en controlador.
Clústeres de Windows admitidos	Funciona con cualquier clúster compatible de Windows Server.	Funciona con clústeres de Windows Server 2008 R2 y versiones posteriores. Otros clústeres de Windows compatibles utilizan el método de sincronización sin controlador para la réplica.

Consideración	BBT por defecto	BBT de un solo nodo
Primera réplica incremental	Se usa la sincronización sin controlador en el nodo activo.	Si se ha completado una réplica completa después de instalar el controlador BBT, se utiliza una transferencia basada bloques basada en controlador en el nodo activo descubierto originalmente. De lo contrario, se usa una sincronización sin controlador en el nodo activo descubierto originalmente.
Réplicas incrementales posteriores	Se usa la sincronización sin controlador en el nodo activo.	Se usa una transferencia basada en bloques basada en controlador en el nodo activo descubierto originalmente. Si un clúster cambia de nodo, el método de sincronización sin controlador se utiliza para la primera réplica incremental después de que el nodo activo original vuelva a ser el nodo activo. Consulte “Impacto del failover del nodo de clúster en la réplica” en la página 125.

13.1.3 Impacto del failover del nodo de clúster en la réplica

En la Tabla 13-3 se describe el impacto de la operación de failover del nodo de clúster en la réplica y las acciones que debe realizar el administrador de Protect.

Tabla 13-3 *Impacto del failover del nodo de clúster en la réplica*

Failover o failback del nodo de clúster	BBT por defecto	BBT de un solo nodo
El failover del nodo de clúster se produce durante la primera réplica completa.	La réplica falla. La primera réplica completa debe completarse correctamente sin un failover del nodo de clúster. 1. Elimine el clúster de Protect. 2. (Opcional) Vuelva a convertir el nodo activo descubierto originalmente en el nodo activo. 3. Vuelva a añadir el clúster mediante el nodo activo. 4. Vuelva a ejecutar la primera réplica completa.	

Failover o failback del nodo de clúster	BBT por defecto	BBT de un solo nodo
Se produce un failover del nodo de clúster durante una réplica completa posterior o una réplica incremental posterior.	El comando de réplica se cancela y se muestra un mensaje que indica que es necesario volver a ejecutar la réplica. Si el perfil del nuevo nodo activo es similar al nodo activo erróneo, el contrato de protección continúa siendo válido. 1. Vuelva a ejecutar la réplica en el nodo activo en ese momento. Si el perfil del nuevo nodo activo es similar al del nodo activo erróneo, el contrato de protección solo continúa siendo válido en el nodo activo original. 1. Vuelva a convertir el nodo activo descubierto originalmente en el nodo activo. 2. Vuelva a ejecutar la réplica en el nodo activo.	El comando de réplica se cancela y se muestra un mensaje que indica que es necesario volver a ejecutar la réplica. El contrato de protección solo es válido en el nodo activo descubierto originalmente. 1. Vuelva a convertir el nodo activo descubierto originalmente en el nodo activo. 2. Vuelva a ejecutar la réplica en el nodo activo. Esta primera réplica incremental después de un evento de failover/failback de clúster utiliza automáticamente la sincronización sin controlador. Las réplicas incrementales posteriores utilizarán el controlador basado en bloques, tal y como especifica la BBT de un solo nodo.
El failover del nodo de clúster se produce entre réplicas.	Si el perfil del nuevo nodo activo es similar al nodo activo erróneo, el contrato de protección continúa según lo planificado para la siguiente réplica incremental. En caso contrario, el comando de la próxima réplica incremental falla. Si se produce un error en una réplica incremental programada: 1. Vuelva a convertir el nodo activo descubierto originalmente en el nodo activo. 2. Ejecute una réplica incremental.	La réplica incremental falla si el nodo activo cambia entre las réplicas. 1. Asegúrese de que el nodo activo descubierto originalmente vuelva a ser el nodo activo. 2. Ejecute una réplica incremental. Esta primera réplica incremental después de un evento de failover/failback de clúster utiliza automáticamente la sincronización sin controlador. Las réplicas incrementales posteriores utilizarán el controlador basado en bloques, tal y como especifica la BBT de un solo nodo.

13.1.4 Similitud del nodo de clúster

En el modo de clúster de Windows por defecto, los nodos de clúster deben tener perfiles similares para evitar interrupciones en el proceso de réplica. Los perfiles de los nodos de clústeres se consideran similares si se cumplen todas las condiciones siguientes:

- Los números de serie de los volúmenes locales de los nodos (volumen del sistema y volumen reservado para el sistema) deben ser iguales en cada nodo del clúster.

Nota: 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. Consulte “Sincronización de números de serie en el almacenamiento local del nodo de clústeres” en la página 141.

Si los volúmenes locales de cada nodo del clúster tienen números de serie distintos, no será posible ejecutar una réplica después de que se produzca un failover del nodo de clústeres. Por ejemplo, durante un failover del nodo de clústeres, el nodo activo Nodo 1 falla y el software del clúster convierte al Nodo 2 en el nodo activo. Si las unidades locales de los dos nodos tienen números de serie distintos, el comando de la próxima réplica para la carga de trabajo falla.

- Los nodos deben tener el mismo número de volúmenes.
- Cada volumen debe ser exactamente del mismo tamaño en cada nodo.
- Los nodos deben tener un número idéntico de conexiones de red.

13.1.5 Configuración de la protección

Para configurar la protección de un clúster de Windows, siga el flujo de trabajo de protección de la carga de trabajo habitual. Asegúrese de que proporciona el nombre de host o la dirección IP del nodo activo del clúster. Consulte “Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo” en la página 37.

13.2 Configuración de descubrimiento del nodo activo de Windows

Puede descubrir clústeres de Windows Server como clústeres o como equipos independientes individuales, según el valor de configuración global de PlateSpin `DiscoverActiveNodeAsWindowsCluster`.

Para descubrir clústeres de Windows como clústeres, defina el parámetro `DiscoverActiveNodeAsWindowsCluster` con el valor `True` (Verdadero). Se trata del ajuste por defecto. El descubrimiento de clústeres, el inventario y la protección de la carga de trabajo usan el nombre de host o la dirección IP del nodo activo de un clúster, en lugar del nombre del clúster o de un recurso compartido de administración. No se configuran cargas de trabajo separadas para los nodos no activos del clúster. Para consultar otros requisitos de protección de la carga de trabajo del clúster, consulte “Requisitos para la protección del clúster” en la página 122.

Para descubrir todos los clústeres de Windows como equipos independientes individuales, defina el parámetro `DiscoverActiveNodeAsWindowsCluster` con el valor `False` (Falso). Este ajuste permite al servidor de PlateSpin descubrir todos los nodos de un clúster de failover de Windows como máquinas independientes. Es decir, añade al inventario el nodo activo de un clúster y los nodos inactivos como si fueran cargas de trabajo Windows normales no conscientes del clúster.

Para habilitar o inhabilitar el descubrimiento de clústeres:

1. Diríjase a la página de configuración del servidor de PlateSpin en

   https://<*dirección-ip-servidor-platespin*>/PlateSpinConfiguration
2. Busque `DiscoverActiveNodeAsWindowsCluster` y haga clic en **Edit** (Editar).
3. En el campo **Value** (Valor), seleccione **True** (Verdadero) para habilitar el descubrimiento de clústeres, o bien seleccione **False** (Falso) para inhabilitarlo.
4. Haga clic en **Save** (Guardar).

13.3 Configuración del método de transferencia basada en bloques para clústeres

Las réplicas incrementales para clústeres de Windows pueden utilizar un método sin controlador (por defecto) o un método basado en controlador (SingleNodeBBT) para la transferencia de datos basada en bloques, según el valor de configuración global de PlateSpin `WindowsClusterMode`. Para obtener más información, consulte “Transferencia basada en bloques para los clústeres” en la página 123.

Para configurar WindowsClusterMode:

1. Diríjase a la página de configuración del servidor de PlateSpin en

   https://<*dirección-ip-servidor-platespin*>/PlateSpinConfiguration
2. Busque `WindowsClusterMode` y haga clic en **Edit** (Editar).
3. En el campo **Value** (Valor), seleccione **Default** (Por defecto) para utilizar la sincronización sin controlador en la réplica incremental, o bien seleccione **SingleNodeBBT** para utilizar controladores basados en bloques para la réplica incremental.
4. Haga clic en **Save** (Guardar).

13.4 Adición de valores de búsqueda de nombres de recursos

Para ayudar a identificar el nodo activo de un clúster de failover de Windows, PlateSpin Protect debe diferenciar el nombre del recurso de dirección IP del clúster compartido de los nombres de otros recursos de dirección IP que haya en el clúster. El recurso de dirección IP del clúster compartido se encuentra en el nodo activo del clúster.

El parámetro global `MicrosoftClusterIPAddressNames` de la página de configuración del servidor de PlateSpin incluye una lista de valores de búsqueda que se pueden usar en el descubrimiento para una carga de trabajo de clúster de Windows. Cuando se añade una carga de trabajo de clúster de Windows, se debe especificar la dirección IP del nodo activo actualmente del clúster. PlateSpin Protect busca los nombres de los recursos de dirección IP del clúster en ese nodo a fin de buscar uno que *empiece con* los caracteres especificados de cualquier valor en la lista. Por lo tanto, cada valor de búsqueda debe contener suficientes caracteres para diferenciar el recurso de dirección IP del clúster compartido en un clúster específico, pero debe ser lo suficientemente corto para poder aplicarse al descubrimiento en otros clústeres de Windows.

Por ejemplo, el valor de búsqueda `Clust IP Address` o `Clust IP` coinciden con los nombre de los recursos *Clust IP Address* para 10.10.10.201 y *Clust IP Address* para 10.10.10.101.

El nombre por defecto del recurso de dirección IP del clúster compartido es `Cluster IP Address` en inglés, o su equivalente si el nodo del clúster está configurado en otro idioma. Los valores de búsqueda por defecto de la lista `MicrosoftClusterIPAddressNames` incluyen el nombre del recurso `Cluster IP Address` en inglés, así como en cada uno de los idiomas compatibles.

Dado que el nombre del recurso de dirección IP del clúster compartido puede configurarlo el usuario, debe añadir otros valores de búsqueda a la lista, según se precise. Si cambia el nombre del recurso, debe añadir un valor de búsqueda correspondiente en la lista `MicrosoftClusterIPAddressNames`. Por ejemplo, si especifica el nombre de recurso `Win2012-CLUS10-IP-ADDRESS`, debe añadir ese valor a la lista. Si tiene varios clústeres que usen la misma convención de nombres, la entrada `Win2012-CLUS` coincidirá con todos los nombres de recursos que empiecen con esa secuencia de caracteres.

Para añadir valores de búsqueda en la lista `MicrosoftClusterIPAddressNames`:

1. Diríjase a la página de configuración del servidor de PlateSpin en https://<*dirección-ip-servidor-platespin*>/PlateSpinConfiguration
2. Busque `MicrosoftClusterIPAddressNames` y haga clic en **Edit** (Editar).
3. En el campo **Value** (Valor), añada uno o varios valores de búsqueda a la lista.
4. Haga clic en **Save** (Guardar).

13.5 Tiempo límite de arbitraje de quórum

Es posible definir la clave de registro QuorumArbitrationTimeMax para los clústeres de failover de Windows Server en el entorno de PlateSpin mediante el parámetro global `FailoverQuorumArbitrationTimeout` en la página de configuración del servidor de PlateSpin. El tiempo límite por defecto es de 60 segundos, en consonancia con el valor por defecto de Microsoft para este ajuste. Consulte *QuorumArbitrationTimeMax* (https://msdn.microsoft.com/en-us/library/aa369123%28v=vs.85%29.aspx?f=255&MSPPError=-2147217396) en el sitio Web de Microsoft Developer Network. El intervalo de tiempo límite especificado se respeta para el arbitraje de quórum durante el failover y el failback.

Para definir el tiempo límite de arbitraje de quórum para todos los clústeres de failover de Windows:

1. Diríjase a la página de configuración del servidor de PlateSpin en https://<*dirección-ip-del-servidor-de-platespin*>/PlatespinConfiguration
2. Busque `FailoverQuorumArbitrationTimeout` y haga clic en **Edit** (Editar).
3. En el campo **Value** (Valor), especifique el número máximo de segundos que se permitirá el arbitraje del quórum.
4. Haga clic en **Save** (Guardar).

13.6 Configuración de los números de serie del volumen local

Use la utilidad *Gestor de volúmenes* para cambiar los números de serie del volumen local a fin de que coincidan en todos los nodos del clúster. Consulte “Sincronización de números de serie en el almacenamiento local del nodo de clústeres” en la página 141.

13.7 Failover de PlateSpin

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

Para realizar el failover de PlateSpin (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).

13.8 Failback de PlateSpin

La operación de failback de PlateSpin requiere una réplica completa para las carga de trabajo de Windows Cluster.

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

- Asigne todos los discos del clúster de un nodo virtual de PlateSpin 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 de PlateSpin para que restaure el volumen del sistema de la máquina de failover al `Disco 1` y los discos adicionales de la máquina 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.

Después de completar un failback de PlateSpin, debe reconectar el almacenamiento compartido y reconstruir el entorno de clúster antes de poder reunir nodos adicionales al clúster recién restaurado.

Nota: si el clúster se encuentra en el estado **Ready To Reprotect** (Preparado para volver a proteger), asegúrese de reconstruir y restaurar primero el destino de failback para que se descubra como clúster. Debe desinstalar manualmente el controlador de clústeres de PlateSpin como parte del proceso de reconstrucción.

Para obtener información sobre la reconstrucción del entorno de clúster después de que se produzca un failover y un failback de PlateSpin, consulte los recursos siguientes:

- **Clúster de failover de Windows Server 2012 R2 (failback a reconstrucción física o virtual):** consulte el artículo 7016770 de la base de conocimientos (http://www.netiq.com/support/kb/doc.php?id=7016770).
- **Clúster de failover de Windows Server 2008 R2 (failback a reconstrucción física o virtual):** consulte el artículo 7015576 de la base de conocimientos (http://www.netiq.com/support/kb/doc.php?id=7015576).

---

14 Solución de problemas de descubrimiento e inventario de cargas de trabajo

Esta sección le ayudará a solucionar problemas habituales durante el descubrimiento y el inventario de cargas de trabajo.

- Sección 14.1, “Resolución de problemas de descubrimiento para cargas de trabajo Windows”, en la página 131
- Sección 14.2, “Resolución de problemas de descubrimiento para cargas de trabajo Linux”, en la página 136
- Sección 14.3, “Resolución de problemas de descubrimiento de hosts de destino”, en la página 136

14.1 Resolución de problemas de descubrimiento para cargas de trabajo Windows

Utilice la información de esta sección para solucionar y resolver problemas durante el inventario y descubrimiento de cargas de trabajo Windows:

- Sección 14.1.1, “Problemas comunes y soluciones”, en la página 131
- Sección 14.1.2, “Modificación del retraso del inicio de pulsación del controlador OFX”, en la página 133
- Sección 14.1.3, “Realización de pruebas de conectividad”, en la página 133
- Sección 14.1.4, “Inhabilitación del software antivirus”, en la página 135
- Sección 14.1.5, “Habilitación de permisos y acceso a archivos y recursos compartidos”, en la página 135

14.1.1 Problemas comunes y soluciones

Problemas o mensajes	Solución
`The domain in the credentials is invalid or blank` (El dominio de las credenciales no es válido o está vacío).	Este error se produce cuando el formato de las credenciales es incorrecto. Pruebe a realizar el descubrimiento con una cuenta de administrador local con el formato de credenciales `nombredehost\AdministradorLocal`. O bien, pruebe a realizar el descubrimiento con una cuenta de administrador de dominio con el formato de credenciales `dominio\AdministradorDeDominio`.

Problemas o mensajes	Solución
`Unable to connect to Windows server...Access is denied` (No es posible conectar con el servidor Windows... Se deniega el acceso).	Se ha usado una cuenta distinta a la del administrador al intentar añadir una carga de trabajo. Use una cuenta de administrador o añada al usuario al grupo de administradores y vuelva a intentarlo. 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 133 de nuevo. Si la prueba es correcta, pruebe a añadir de nuevo la carga de trabajo. ◆ "Solución de problemas de la conectividad DCOM" en la página 134 ◆ "Solución de problemas de conectividad del servicio RPC" en la página 134
`Unable to connect to Windows server...The network path was not found` (No es posible conectar con el servidor Windows... No se encuentra la vía de red).	Error de conectividad de red. Realice las pruebas de "Realización de pruebas de conectividad" en la página 133. 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.
`Discover Server Details {hostname}" Failed Progress: 0% Status: NotStarted` (Error en los detalles del servidor de descubrimiento {hostname}. Progreso: 0%. Estado: sin iniciar)	Este error se puede producir por varias razones, y cada una de ellas tiene una solución distinta: ◆ 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 base de conocimientos (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 base de conocimientos (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).	Hay varias razones posibles para el error `Could not find file output.xml`: ◆ 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 135. ◆ 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 Protect puede acceder a estos recursos compartidos. Consulte "Habilitación de permisos y acceso a archivos y recursos compartidos" en la página 135. ◆ 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.

14.1.2 Modificación del retraso del inicio de pulsación del controlador OFX

Para evitar errores de descubrimiento producidos por problemas de sincronización, se establece un retraso del inicio de pulsación por defecto de 15 segundos (15 000 ms) en el controlador OFX. El valor se puede configurar añadiendo la clave de registro `HeartbeatStartupDelayInMS` en la carga de trabajo de origen. Esta clave de registro no se configura por defecto.

Para habilitar un retraso de pulsación más corto o más largo:

1. En la carga de trabajo de origen, abra el Editor del Registro de Windows.
2. Diríjase a la siguiente ubicación en el Editor del Registro, según la arquitectura de sistema operativo de la carga de trabajo de origen:

   Vía para una carga de trabajo de origen de 64 bits:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\OperationsFramework\Controller
   ```

   Vía para una carga de trabajo de origen de 32 bits:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\OperationsFramework\Controller
   ```

3. Añada una clave denominada `HeartbeatStartupDelayInMS` de tipo `REG_SZ` y defina en ella el valor que desee en milisegundos. El valor por defecto debe ser 15000.

   ```
   REG_SZ: HeartbeatStartupDelayInMS Value: "15000"
   ```

4. Reinicie la carga de trabajo de origen.

14.1.3 Realización de pruebas de conectividad

- “Prueba de conectividad de red” en la página 133
- “Prueba de conectividad de WMI” en la página 133
- “Solución de problemas de la conectividad DCOM” en la página 134
- “Solución de problemas de conectividad del servicio RPC” en la página 134

Prueba de conectividad de red

Realice esta prueba de conectividad de red básica para determinar si 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 `nombredehost\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 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 rearranque 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 Protect y la carga de trabajo en el mismo lado del cortafuegos
- Abra puertos específicos entre Protect y la carga de trabajo (consulte “Requisitos de acceso y comunicación en la red de protección” en la página 31).

14.1.4 Inhabilitación del software antivirus

En ocasiones, el software antivirus puede bloquear algunas de las funciones de 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. Este bloqueo 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. Inhabilitar los servicios no es necesario durante las réplicas de datos en el nivel de bloques.

14.1.5 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, Protect usa los recursos compartidos administrativos de la carga de trabajo. Para realizar esta tarea, 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 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.

14.2 Resolución de problemas de descubrimiento para cargas de trabajo Linux

Problemas o mensajes	Solución
`Unable to connect neither to the SSH server running on <IP_address> nor to VMware Virtual Infrastructure web-services at <ip_address>/sdk` (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)	Este mensaje se puede deber a diversos motivos: ◆ 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. 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 31.
`Access denied` (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 167.

14.3 Resolución de problemas de descubrimiento de hosts de destino

Problemas o mensajes	Solución
Para ESXi 4.1, en el descubrimiento directo de host faltan grupos de puertos de la máquina virtual si los grupos de puertos dvSwitch comparten el mismo nombre.	Asegúrese de que los nombres del grupo de puertos sean exclusivos en el host de VMware de destino.

B Distribuciones de Linux compatibles con Protect

El software de PlateSpin Protect incluye versiones compiladas previamente del controlador `blkwatch` para muchas distribuciones de Linux que no son de depuración (32 bits y 64 bits).

- Sección B.1, “Análisis de la carga de trabajo Linux”, en la página 137
- Sección B.2, “Controladores blkwatch precompilados para distribuciones Linux”, en la página 138

B.1 Análisis de la carga de trabajo Linux

Antes de determinar si PlateSpin Protect cuenta con un controlador `blkwatch` para su distribución de Linux, debe obtener más información sobre el núcleo de la carga de trabajo Linux a fin de que pueda usarla como término de búsqueda en la lista de distribuciones compatibles.

- Sección B.1.1, “Determinación de la cadena de versión”, en la página 137
- Sección B.1.2, “Determinación de la arquitectura”, en la página 137

B.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).

B.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.

B.2 Controladores blkwatch precompilados para distribuciones Linux

PlateSpin Protect proporciona controladores blkwatch precompilados para muchas distribuciones Linux que no son de depuración. Puede buscar en List of Distributions (Lista de distribuciones) 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 base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7005873). Los controladores autocompilados solo se admiten para las versiones mayor y menor del núcleo de Linux que aparecen en la Lista de distribuciones, o como una versión con parche de estas. Si la versión mayor y menor del núcleo en la cadena de versión del núcleo de la carga de trabajo Linux coincide con una versión mayor y menor del núcleo de la lista, el controlador autocompilado se admite.

- Sección B.2.1, “Sintaxis de los elementos de la lista”, en la página 138
- Sección B.2.2, “Lista de distribuciones”, en la página 138
- Sección B.2.3, “Otras distribuciones de Linux que usan controladores blkwatch”, en la página 138

B.2.1 Sintaxis de los elementos de la lista

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

<Distribución>-<Parche>-<Cadena_vesión_núcleo>-<Arquitectura_núcleo>

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

```
SLES9-SP1-2.6.5-7.139-bigsmp-x86
```

B.2.2 Lista de distribuciones

Para obtener una lista de las distribuciones del núcleo compatibles, consulte el apartado “Lista de distribuciones” (https://www.netiq.com/documentation/platespin-protect-11-2-1/protect_user/data/blkwatch-drivers.html#blkwatch-dist-list) en la *Guía del usuario de PlateSpin Protect*.

B.2.3 Otras distribuciones de Linux que usan controladores blkwatch

PlateSpin Protect es compatible con otras distribuciones Linux que se indican en la Tabla B-1 si se basan en una versión compatible de Red Hat Enterprise Linux o SUSE Linux Enterprise Server. Puede utilizar el controlador blkwatch precompilado para la distribución Linux compatible.

Tabla B-1 *Compatibilidad del controlador blkwatch con otras distribuciones Linux*

Otra distribución Linux	Basado en una versión compatible para RHEL o SLES	Notas
CentOS	Red Hat Enterprise Linux	
Open Enterprise Server (OES)	SUSE Linux Enterprise Server 11 SP 1 o posterior	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 una posterior antes de realizar un inventario de la carga de trabajo.
Oracle Linux (OL) (anteriormente Oracle Enterprise Linux [OEL])	Red Hat Enterprise Linux	Hay disponibles controladores blkwatch para el núcleo estándar y para Unbreakable Enterprise Kernel (UEK), como se indica en la Sección B.2.2, “Lista de distribuciones”, en la página 138. Para otras distribuciones Oracle Linux, hay disponibles controladores precompilados solo para el núcleo compatible de Red Hat (RHCK) correspondiente. En PlateSpin Protect 11.2 y versiones anteriores no se admiten cargas de trabajo que usen Unbreakable Enterprise Kernel de Oracle Linux.

Para obtener una lista de las distribuciones del núcleo compatibles, consulte el apartado “Lista de distribuciones” (https://www.netiq.com/documentation/platespin-protect-11-2-1/protect_user/data/blkwatch-drivers.html#blkwatch-dist-list) en la *Guía del usuario de PlateSpin Protect*.

C Sincronización de números de serie en el almacenamiento local del nodo de clústeres

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 los números de serie en el almacenamiento local del nodo de clústeres.

Para descargar y ejecutar la utilidad:

1. Descargue el archivo `VolumeManager.exe` desde la página de descarga de PlateSpin Protect:
   - **1a** Diríjase a la página de descargas de Micro Focus (https://www.microfocus.com/support-and-services/download/).
   - **1b** Seleccione PlateSpin Protect en la lista **Buscar por producto** o escriba el nombre del producto en el campo correspondiente para localizar el producto y selecciónelo.
   - **1c** Si hay disponible una lista de versiones, seleccione PlateSpin Protect 11.2.1.
   - **1d** En la página de descripción general de la descarga, haga clic en **proceed to download** (Continuar a la descarga) y entre con las credenciales de su cuenta de cliente.
   - **1e** Haga clic en **accept** (Aceptar) para aceptar su conformidad con las leyes y normativas de exportación de EE. UU.
   - **1f** En la página Download (Descarga), haga clic en el enlace **download** (Descargar) situado junto al archivo `VolumeManager.exe` y, a continuación, guarde el archivo.
2. Copie el archivo descargado en una ubicación a la que se pueda acceder desde todos los nodos de clúster.
3. 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.
4. Compruebe que todos los números de serie del almacenamiento local del nodo activo coinciden con los números correspondientes de los demás nodos del clúster.
   - **4a** En cada nodo del clúster, ejecute el comando `VolumeManager.exe -l` para obtener sus números de serie de volumen.
   - **4b** Compare los números de serie de almacenamiento local del nodo activo (Paso 3) con los números correspondientes del nodo (Paso 4a).
   - **4c** (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`

4d Cuando haya cambiado correctamente todos los números de serie del volumen de un nodo del clúster, debe reiniciar dicho nodo.

4e Repita del Paso 4a al Paso 4d en cada nodo del clúster.

5 (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.

D Utilidad Protect Agent

Protect Agent es una utilidad de línea de comandos que se puede usar para instalar, actualizar, realizar consultas o desinstalar controladores de transferencia basados en bloques.

Aunque siempre es necesario rearrancar cuando se instalan, se desinstalan o se actualizan controladores, Protect Agent permite controlar mejor cuándo se produce la acción y, por lo tanto, cuándo se producirá el rearranque del servidor. Por ejemplo, puede usar Protect Agent para instalar los controladores durante el tiempo de inactividad planificado, en lugar de hacerlo durante la primera réplica.

- Sección D.1, “Uso de la utilidad Protect Agent para Windows”, en la página 143
- Sección D.2, “Uso de Protect Agent con controladores de transferencia basada en bloques”, en la página 144

D.1 Uso de la utilidad Protect Agent para Windows

Para descargar la utilidad Protect Agent para Windows en la carga de trabajo de origen:

1. Entre en el equipo Windows de origen como usuario administrador.
2. En un navegador web, lance la interfaz Web y entre.
3. Haga clic en la pestaña **Downloads** (Descargas).
4. Haga clic en el enlace de la aplicación Protect Agent para la plataforma de destino Windows y, a continuación, guarde el archivo `ProtectAgent.cli.exe` comprimido.
5. Extraiga el contenido del archivo para acceder al archivo ejecutable.
6. (Opcional) Para ver la ayuda de Protect Agent, introduzca

   ```
   Protect.Agent.cli.exe -h
   ```

La utilidad está disponible en el host del servidor de PlateSpin en un archivo comprimido. Extraiga el contenido del archivo para acceder al archivo ejecutable.

```
C:\Archivos de programa\PlateSpin Protect Server\bin\ProtectAgent
```

La sintaxis para ejecutar la utilidad de Protect Agent para Windows es:

```
ProtectAgent.cli.exe {command} [command_option] [/psserver=%IP%]
```

En la Tabla D-1 se describen los comandos, las opciones de los comandos y los parámetros disponibles para el comando `ProtectAgent.cli.exe`.

Tabla D-1 *Comandos, opciones de comandos y parámetros de la utilidad de Protect Agent para Windows*

Uso	Descripción
Comandos	
`h |? | help`	Muestra el uso y las opciones del comando.
`logs | view-logs`	Abre el directorio de registro de la aplicación.

Uso	Descripción

`status`
 	
`/status [/psserver=%IP%]`
	Muestra el estado de instalación de los controladores de PlateSpin en esta carga de trabajo.
	
	Si especifica el servidor de PlateSpin, se comprobará si hay actualizaciones del controlador en el servidor.

`din | driver-install`
 	
`/din [/psserver=%IP%]`
	Instala los controladores de PlateSpin.
	
	Si especifica el servidor de PlateSpin, se comprobará si hay actualizaciones del controlador en el servidor.

`dup | driver-upgrade`
 	
`/dup [/psserver=%IP%]`
	Actualiza los controladores de PlateSpin.
	
	Si especifica el servidor de PlateSpin, se comprobará si hay actualizaciones del controlador en el servidor.

`dun | driver-uninstall`
 	
`[/dun /psserver=%IP%]`
	Desinstala los controladores de PlateSpin.

`con | config`
 	
`/con /setting=<`*`nombre_valor`*`>:<`*`valor`*`>`
 	
Ejemplo:
 	
`ProtectAgent.cli.exe /config /setting=psserver:10.10.10.202`
	Especifica el nombre del ajuste y su valor, que deben cambiarse en el archivo de configuración de esta carga de trabajo.
	
	La opción `psserver` detiene el servicio del controlador OFX (`ofxcontroller`), modifica el archivo `OfxController.exe.config` con la nueva dirección IP y reinicia el servicio. Si modifica la dirección IP pública del servidor de PlateSpin, debe ejecutar este comando en cada una de las cargas de trabajo de origen que se configuren para el servidor.

Conmutador	
`/psserver=%IP%`	Descarga los controladores de transferencia basados en bloques del servidor especificado cuando se invocan las opciones `status`, `driver-install` o `driver-upgrade`.
Opción de comando	

`setting`
 	
`/setting=<`*`nombre_valor`*`>:<`*`valor`*`>`
	Especifica el nombre del ajuste y el valor del ajuste de configuración que debe modificarse.
	
	Los nombres de ajuste admitidos son:
	
	`psserver`
	`altAddress`
	`heartbeat`

D.2 Uso de Protect Agent con controladores de transferencia basada en bloques

Con la utilidad Protect Agent se incluye una copia de los controladores de transferencia basados en bloques. Alternativamente, es posible especificar el parámetro de línea de comandos `/psserver=` para descargar los controladores del servidor de PlateSpin cuando se invocan las opciones `status`, `driver-install` o `driver-upgrade`. Esto resulta de utilidad si el servidor tiene aplicado un parche con un paquete de controladores nuevo, pero la utilidad de línea de comandos de Protect Agent no tiene este parche.

Nota: para evitar confusiones, el método recomendado para usar Protect Agent es instalar, desinstalar o actualizar los controladores y luego rearrancar antes de realizar una réplica.

Deberá rearrancar la carga de trabajo de origen cada vez que instale, actualice o desinstale los controladores. El rearranque fuerza que el controlador en ejecución se detenga y que el nuevo controlador se aplica al reiniciar el sistema. Si no rearranca el sistema antes de la réplica, el origen seguirá actuando como si la operación no se hubiera completado. Por ejemplo, si instala controladores sin rearrancar el sistema, el origen actúa como si no se hubieran instalado controladores durante la réplica. De igual forma, si actualiza los controladores sin rearrancar, el origen seguirá usando el controlador en ejecución durante la réplica hasta que se rearranque el sistema.

Si la versión del controlador instalado es distinta a la del controlador en ejecución, la opción `status` recordará al usuario que debe rearrancar. Por ejemplo:

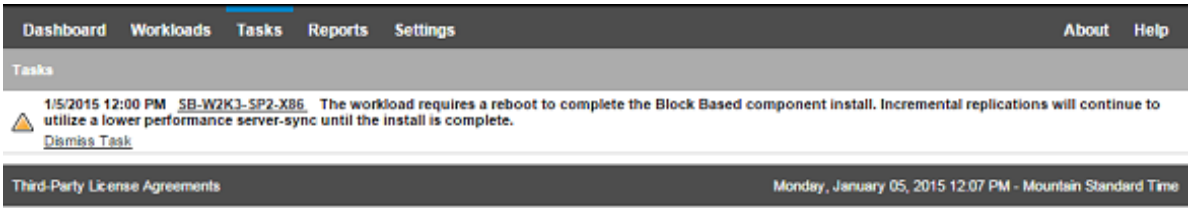
```
C:\ProtectAgent\ProtectAgent.cli.exe status
Step 1 of 2: Querying the PlateSpin controller service
   Done
Step 2 of 2: Querying the installed PlateSpin driver version
   Done

The task completed successfully
PlateSpin Controller Service Status
    Status: Running
    Version: 9.9.9.9
    Last Successful Contact: 1/5/2015 12:14:25 PM

PlateSpin Driver Status
    Installed Driver Version: 8.0.0.11
    Running Driver Version: Not running. Reboot to load the driver.
    Upgrade Available: No
```

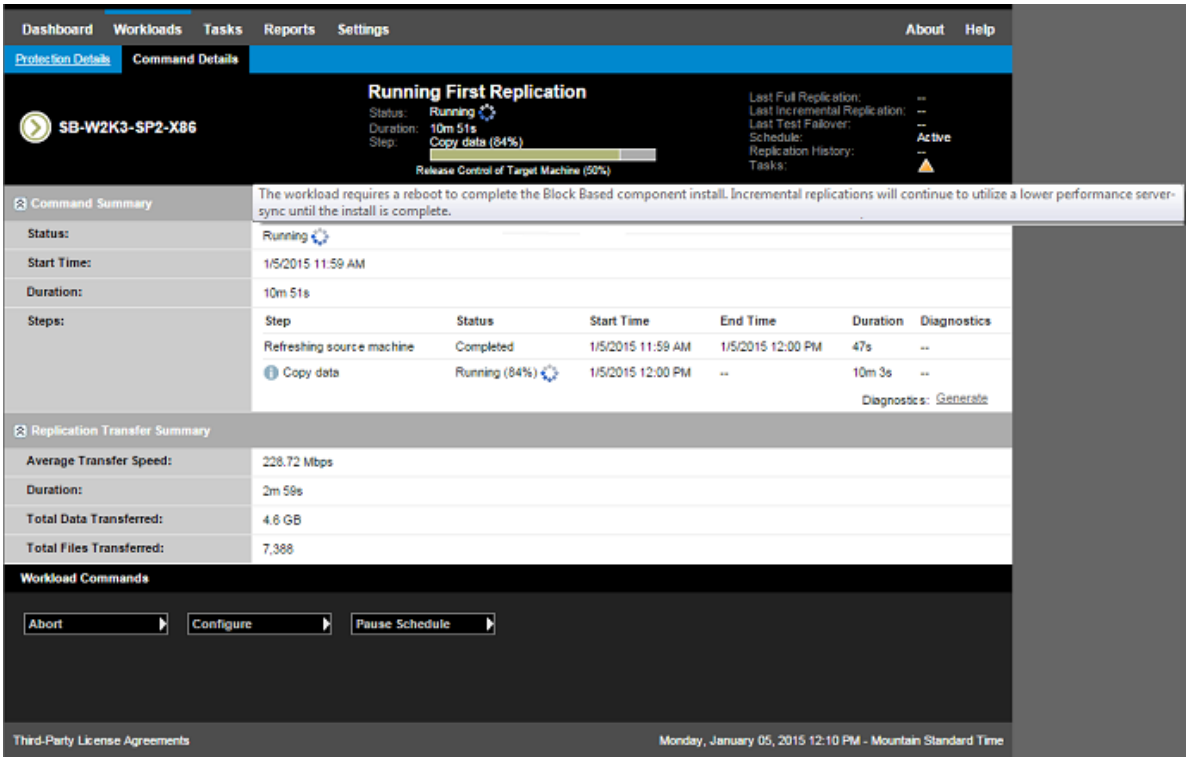
PlateSpin crea una tarea para advertir al usuario de que es necesario rearrancar a fin de completar la instalación o la actualización del controlador. La notificación aparece en la lista Tasks (Tareas, Figura D-1).

Figura D-1 *Tarea de notificación de rearranque*



Durante la réplica, la notificación aparece en la página Command Details (Detalles del comando, Figura D-2).

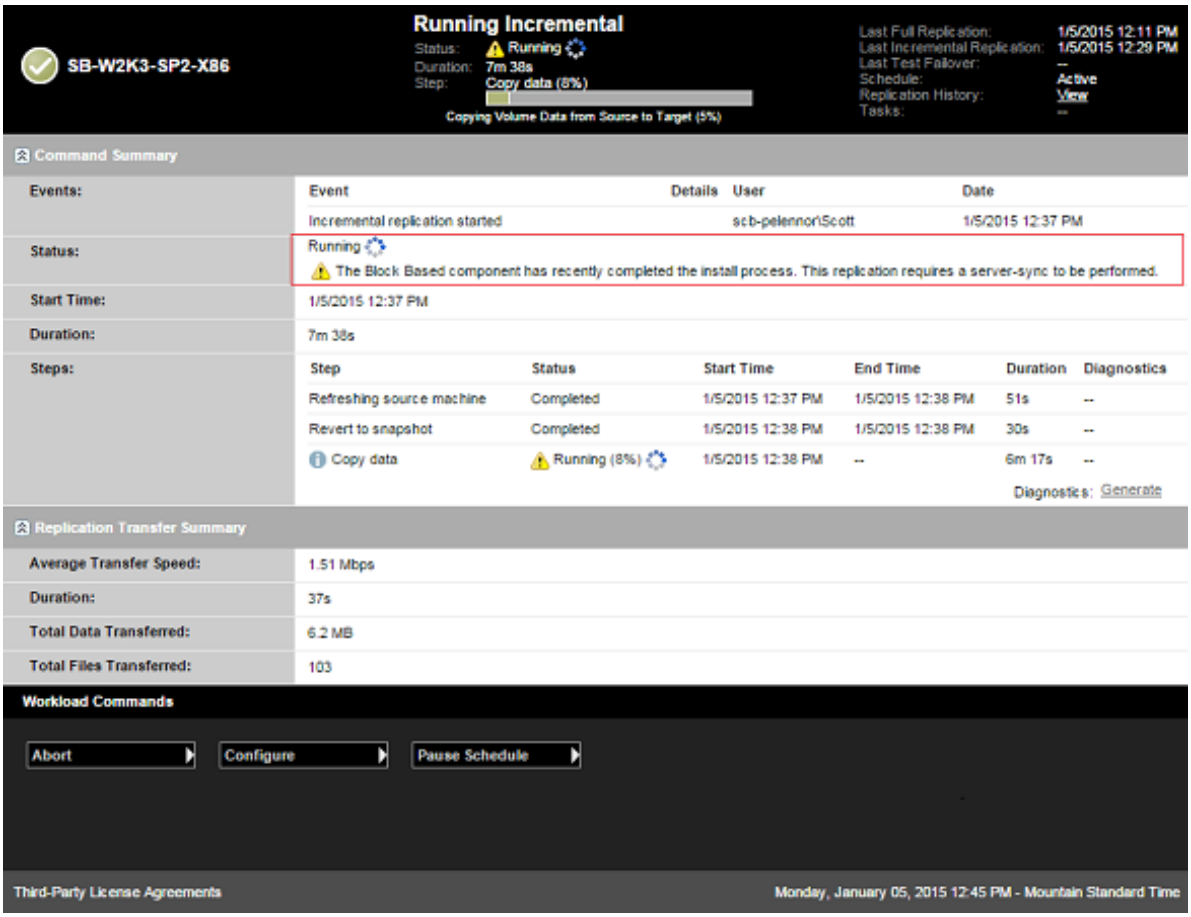
Figura D-2 *Notificación de rearranque durante la réplica*



Al rearrancar el equipo de origen se aplican y se inician los controladores instalados o actualizados. Si el controlador se ha instalado recientemente, después del rearranque será necesario realizar una réplica completa o una réplica de sincronización del servidor a fin de garantizar que se recogen todos

los cambios del origen. Este requisitos de réplica de sincronización del servidor se representa al usuario en el campo Status (Estado) como una advertencia (Figura D-3). Las réplicas incrementales posteriores se completarán sin advertencias según lo programado.

Figura D-3 *Notificación de sincronización del servidor requerida*



IV Protección de cargas de trabajo

Después de descubrir los destinos y las cargas de trabajo, estará en disposición de preparar la protección. Para ello, debe configurar contratos de protección para sus cargas de trabajo.

- Capítulo 15, “Protección y recuperación de cargas de trabajo”, en la página 151
- Capítulo 16, “Elementos básicos de la protección de la carga de trabajo”, en la página 167
- Capítulo 17, “Generación de informes”, en la página 181
- Capítulo 18, “Solución de problemas de protección y recuperación de cargas de trabajo”, en la página 185

15 Protección y recuperación de cargas 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 gestionada por 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 15.1, “Requisitos previos para proteger las cargas de trabajo”, en la página 151
- Sección 15.2, “Configuración de los detalles de protección y preparación de la réplica”, en la página 151
- Sección 15.3, “Inicio de la protección de la carga de trabajo”, en la página 156
- Sección 15.4, “Cancelación de comandos”, en la página 157
- Sección 15.5, “Failover”, en la página 157
- Sección 15.6, “Failback”, en la página 160
- Sección 15.7, “Reprotección de una carga de trabajo”, en la página 164

15.1 Requisitos previos para proteger las cargas de trabajo

Prepare los contenedores y las cargas de trabajo para la protección. Consulte la Parte III, “Preparación de los destinos y los orígenes de protección”, en la página 93.

En un dominio de Active Directory, siga estas prácticas recomendadas antes de ejecutar la primera réplica completa:

- Asegúrese de actualizar Windows (ejecute Windows Update) en la carga de trabajo de origen antes de ejecutar la primera réplica completa.
- Asegúrese de configurar el software antivirus con las exclusiones de archivos y carpetas recomendadas que se describen en el *artículo 822158 de la base de conocimientos de Microsoft: Recomendaciones para la detección de virus en equipos de empresa que ejecutan actualmente versiones compatibles de Windows* (https://support.microsoft.com/en-us/kb/822158).
- Si el equipo Windows es un controlador de dominio, asegúrese de inhabilitar el software antivirus en el sistema durante la réplica.

15.2 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 (añadir inventario, réplicas iniciales y posteriores,

failover, failback y reprotección), se leen los valores oportunos de los detalles de la protección. Consulte “Flujo de trabajo básico para la protección y la recuperación de la carga de trabajo” en la página 37. Esta recopilación de los valores activos actualmente pertenecientes al ciclo de vida completo de la protección de una carga de trabajo recibe el nombre de *contrato de protección* de la carga de trabajo.

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

1. Añada un contenedor. Consulte “Adición de contenedores (destinos de protección)” en la página 96.
2. Añada una carga de trabajo. Consulte “Adición de cargas de trabajo (orígenes de protección)” en la página 100.
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 170.
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 170.

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

   ---

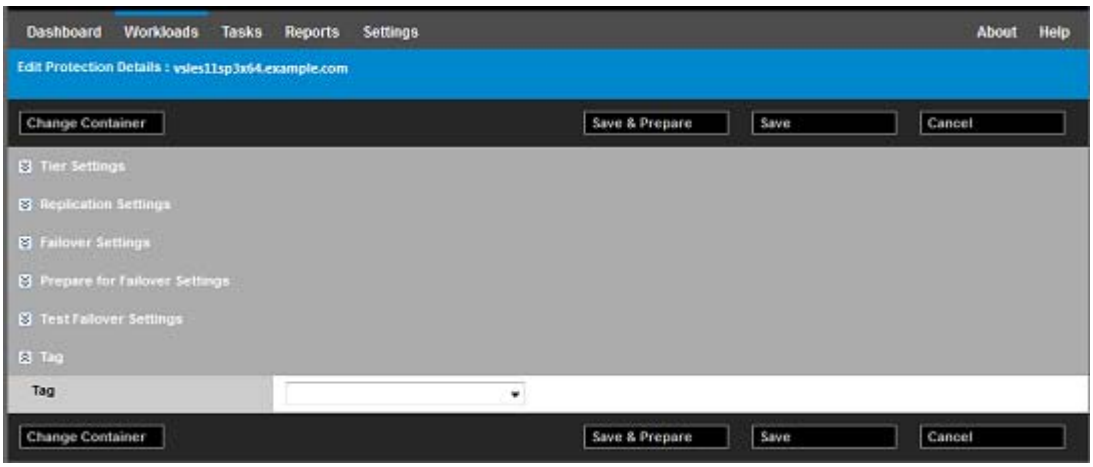
6. Configure los detalles de protección de cada conjunto de valores según sus necesidades de continuidad empresarial. Consulte “Detalles de protección de la carga de trabajo” en la página 153.
7. Corrija los posibles errores de validación que se muestren en la interfaz Web de PlateSpin Protect.
8. Haga clic en **Save** (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.

15.2.1 Detalles de protección de la carga de trabajo

Los detalles de protección de la carga de trabajo se representan mediante cinco conjuntos de parámetros, como se describe en la Tabla 15-1:



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

Tabla 15-1 *Detalles de protección de la carga de trabajo*

Configuración de parámetros	Detalles
Tier Settings (Valores de nivel)	
Protection Tier (Nivel de protección)	Permite especificar el nivel de protección que usa la protección actual. Consulte "Niveles de protección" en la página 168.
Replication Settings (Valores de réplica)	
Transfer Method (Método de transferencia)	(Windows) Seleccione un método de transferencia de datos basado en archivo o basado en bloques. Para obtener información sobre la réplica del nivel de bloque con componentes basados en bloques o sin ellos, consulte "Métodos de transferencia de datos admitidos" en la página 23. Para habilitar el cifrado, seleccione la opción **Encrypt Data Transfer** (Transferencia de datos de cifrado). Consulte "Cifrado de datos durante la transmisión" en la página 24.
Transfer Encryption (Cifrado de transferencia)	(Linux) Para habilitar el cifrado, seleccione la opción **Encrypt Data Transfer** (Transferencia de datos de cifrado). Consulte "Cifrado de datos durante la transmisión" en la página 24.
Source Credentials (Credenciales de origen)	Permite especificar las credenciales requeridas para acceder a la carga de trabajo. Consulte "Directrices para las credenciales de carga de trabajo y contenedor" en la página 167.

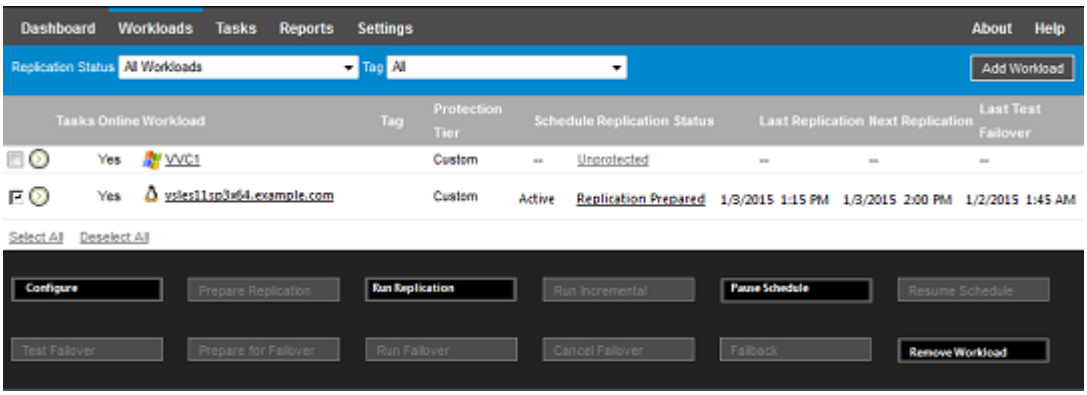
Configuración de parámetros	Detalles
CPU	(Contenedores de máquinas virtuales que usen VMware 5.1, 5.5 o 6.0 con un nivel mínimo de hardware de máquina virtual 8) Especifique el número de zócalos y de núcleos por zócalo para la carga de trabajo de failover. El total de núcleos se calcula automáticamente. Este parámetro se aplica durante la primera instalación de una carga de trabajo con el valor de réplica inicial de **Full** (Réplica completa). **Nota:** el número máximo de núcleos que puede usar la carga de trabajo depende de factores externos, como el sistema operativo invitado, la versión del hardware de la máquina virtual, la licencia de VMware para el host de ESXi y la capacidad de cálculo máxima del host de ESXi para vSphere (consulte *Máximos de configuración de vSphere 5.1* (http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf)). Algunas distribuciones de un sistema operativo invitado podrían no respetar la configuración de núcleos o de núcleos por zócalo. Por ejemplo, los sistemas operativos invitados que usan SLES 10 SP4 y OES 2 SP3 conservan la configuración de núcleos y zócalos original de la instalación, mientras que otras distribuciones de SLES, RHEL y OES sí respetan la configuración.
Number of CPUs (Número de CPU)	(Contenedores de máquinas virtuales que usen VMware 4.1) Especifique el número necesario de vCPU (CPU virtuales) que se deben asignar a la carga de trabajo de failover. Este parámetro se aplica durante la primera instalación de una carga de trabajo con el valor de réplica inicial de **Full** (Réplica completa). Cada vCPU se presenta al sistema operativo invitado en el contenedor de máquinas virtuales como un único núcleo con un solo zócalo.
Replication Network (Red de réplica)	Permite separar el tráfico de réplica según las redes virtuales definidas en el contenedor de máquinas virtuales. Consulte “Redes” en la página 175. Para este ajuste, también es posible especificar un valor de MTU para usarlo en la red de réplica de disco RAM de Linux (LRD) de PlateSpin Protect. Definir este valor puede ayudar a evitar el ruido en redes (por ejemplo, una VPN) que tengan un valor de MTU menor. El valor por defecto es una cadena vacía (no se muestra nada en el recuadro de texto). Cuando se configura la conectividad en el LRD, esto permite que el dispositivo de red defina su propio valor por defecto (que suele ser 1500). Si introduce un valor, PlateSpin Protect ajusta el valor de MTU al configurar la interfaz de red.
Allowed Networks (Redes permitidas)	Permite especificar una o varias interfaces de red (NIC o dirección IP) en el origen para usarlas en el tráfico de réplica.
Resource Pool for Target VM (Grupo de recursos para máquina virtual de destino)	(El contenedor de máquina virtual forma parte de un clúster DRS) Permite especificar la ubicación del grupo de recursos en la que se debe crear la máquina virtual de failover.
VM Folder for Target VM (Carpeta de máquina virtual para la máquina virtual de destino)	(El contenedor de máquina virtual forma parte de un clúster DRS) Permite especificar la ubicación de la carpeta de máquina virtual en la que se debe crear la máquina virtual de failover.
Configuration File Datastore (Almacén de datos de archivo de configuración)	Permite seleccionar un almacén de datos asociado con el contenedor de máquinas virtuales para almacenar los archivos de configuración de la máquina virtual. Consulte “Puntos de recuperación” en la página 170.

Configuración de parámetros	Detalles
Protected Volumes (Volúmenes protegidos)	Puede seleccionar los volúmenes que desea proteger y asignar sus réplicas a almacenes de datos específicos en el contenedor de máquinas virtuales.
Thin Disk (Opción de disco ligero)	Seleccione esta opción para habilitar 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.
Protected Logical Volumes (Volúmenes lógicos protegidos)	(Linux) Permite especificar uno o varios volúmenes LVM lógicos que se deben proteger para una carga de trabajo Linux o los grupos NSS en una carga de trabajo de Open Enterprise Server.
Non-volume Storage (Almacenamiento sin volumen)	(Linux) Permite especificar un área de almacenamiento (como una partición de intercambio) asociada con la carga de trabajo de origen. Este almacenamiento se vuelve a crear en la carga de trabajo de failover.
Volume Groups (Grupos de volúmenes)	(Linux) Permite especificar los grupos de volúmenes LVM que se deben proteger con los volúmenes LVM lógicos mostrados en la sección Protected Logical Volumes (Volúmenes lógicos protegidos) de la configuración.
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 171.
Failover Settings (Valores de failover)	
VM Memory (Memoria de la máquina virtual)	Permite especificar la cantidad de memoria asignada a la carga de trabajo de failover.
Hostname and Domain/Workgroup affiliation (Nombre de host y afiliación de dominio/grupo de trabajo)	Permite especificar 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.
Network Connections (Conexiones de red)	Permite especificar la configuración LAN de la carga de trabajo de failover. Consulte “Redes” en la página 175.
DNS Servers (Servidores DNS)	Permite especificar la dirección IP del servidor DNS primario y una DNS alternativa (opcional).
Services/Daemon States to Change (Estados de daemon o servicios para cambiar)	Permite especificar el estado de inicio de servicios de aplicaciones (Windows) o daemon (Linux) específicos. Consulte “Control de servicios y daemons” en la página 171.
Prepare for Failover Settings (Configuración de la preparación para failover)	
Temporary Failover Network (Red de failover temporal)	Permite especificar la configuración de LAN temporal de la carga de trabajo de failover durante la operación opcional de preparación para failover. Consulte “Redes” en la página 175.
Test Failover Settings (Valores de prueba de failover)	
VM Memory (Memoria de la máquina virtual)	Permite asignar la RAM necesaria a la carga de trabajo temporal.
Hostname (Nombre de host)	Permite asignar un nombre de host a la carga de trabajo temporal.

Configuración de parámetros	Detalles
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.
Network Connections (Conexiones de red)	Permite especificar la configuración LAN de la carga de trabajo temporal. Consulte “Redes” en la página 175.
DNS Servers (Servidores DNS)	Permite especificar la dirección IP del servidor DNS primario y una DNS alternativa (opcional).
Service/Daemon States to Change (Estados de servicio/daemon para cambiar)	Permite especificar el estado de inicio de servicios de aplicaciones (Windows) o daemons (Linux) específicos. Consulte “Control de servicios y daemons” en la página 171.
Tags (Etiquetas)	
Tag (Etiqueta)	(Opcional) Asigne una etiqueta a esta carga de trabajo. Consulte “Etiquetado de cargas de trabajo” en la página 101.

15.3 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 **Execute** (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. eliminar la protección de la carga de trabajo;
  2. cambiar el tamaño de los volúmenes según se precise; y
  3. 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.

15.4 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; por ejemplo, **Running Incremental** (Incremental en ejecución).

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

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

15.5 Failover

En una operación de *failover,* la carga de trabajo de failover incluida en un contenedor de máquinas virtuales de PlateSpin Protect asumirá la función empresarial de una carga de trabajo de producción que ha fallado.

- Sección 15.5.1, “Detección de cargas de trabajo sin conexión”, en la página 157
- Sección 15.5.2, “Realización de failover”, en la página 158
- Sección 15.5.3, “Uso de la función de prueba de failover”, en la página 159

15.5.1 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

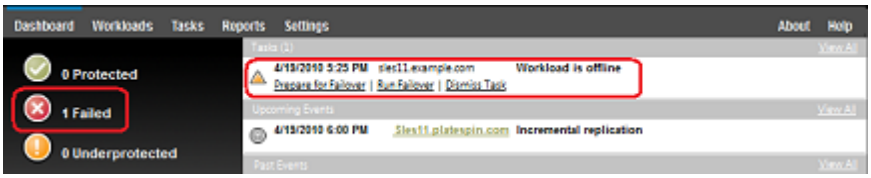
registrar un error de carga de trabajo forman parte de la configuración de nivel de la protección de la carga de trabajo. Consulte la fila “Tier Settings (Valores de nivel)” en “Detalles de protección de la carga de trabajo” en la página 153.

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 los servicios de notificación por correo electrónico para eventos e informes de réplica” en la página 67.

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 157) y continúe con el comando **Run Failover** (Ejecutar failover). Consulte “Realización de failover” en la página 158.

En la Figura 15-1 se muestra la página Dashboard (Consola) de la interfaz Web cuando detecta un error de carga de trabajo. Fíjese en las tareas aplicables del panel de tareas y eventos:

Figura 15-1 *Página Dashboard (Consola) al detectar un error de carga de trabajo (Workload is offline)*



15.5.2 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 “Failover Settings (Valores de failover)” en “Detalles de protección de la carga de trabajo” en la página 153.

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 hiperenlace del comando correspondiente del evento **Workload is offline** (Carga de trabajo sin conexión) del panel de tareas y eventos. Consulte la Figura 15-1.
- Ejecute el comando **Prepare for Failover** (Preparar failover) para arrancar la máquina virtual de failover previamente. Sigue 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 170). 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 159.

15.5.3 Uso de la función de prueba de failover

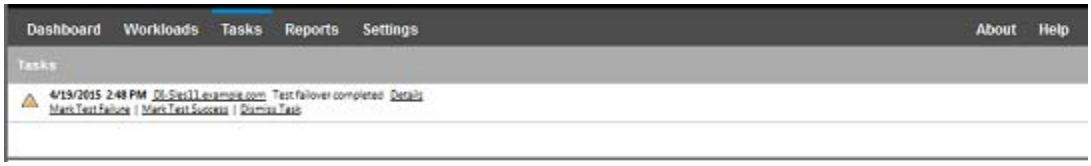
PlateSpin Protect proporciona la capacidad para probar la función de failover y la integridad de la carga de trabajo de failover. Esto se realiza mediante el comando **Test Failover** (Failover de prueba), que arranca la carga de trabajo de failover en un entorno de redes aislado para realizar pruebas sobre la funcionalidad del failover y para verificar la integridad de la carga de trabajo de failover.

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 “Test Failover Settings (Valores de prueba de failover)” en “Detalles de protección de la carga de trabajo” en la página 153.

Para usar la función de prueba de failover:

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 170) 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.

15.6 Failback

Una operación de *failback* restaura la función empresarial de una carga de trabajo de producción errónea en su entorno original cuando la función empresarial de una carga de trabajo de failover temporal ya no es necesaria. El paso lógico siguiente tras un failover es una operación de failback. Con ella se transfiere la carga de trabajo de failover 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 Microsoft Hyper-V.

En los temas siguientes se proporciona más información:

- Sección 15.6.1, “Failback automatizado a una plataforma de máquina virtual”, en la página 160
- Sección 15.6.2, “Failback semiautomatizado a un equipo físico”, en la página 163
- Sección 15.6.3, “Failback semiautomatizado a una máquina virtual”, en la página 164

15.6.1 Failback automatizado a una plataforma de máquina virtual

PlateSpin Protect admite el failback automatizado para los contenedores de failback en un servidor VMware ESXi Server admitido o en un clúster DRS de VMware. Consulte “Contenedores de máquina virtual compatibles” en la página 17.

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 167.
   - **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 170.
     - **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).

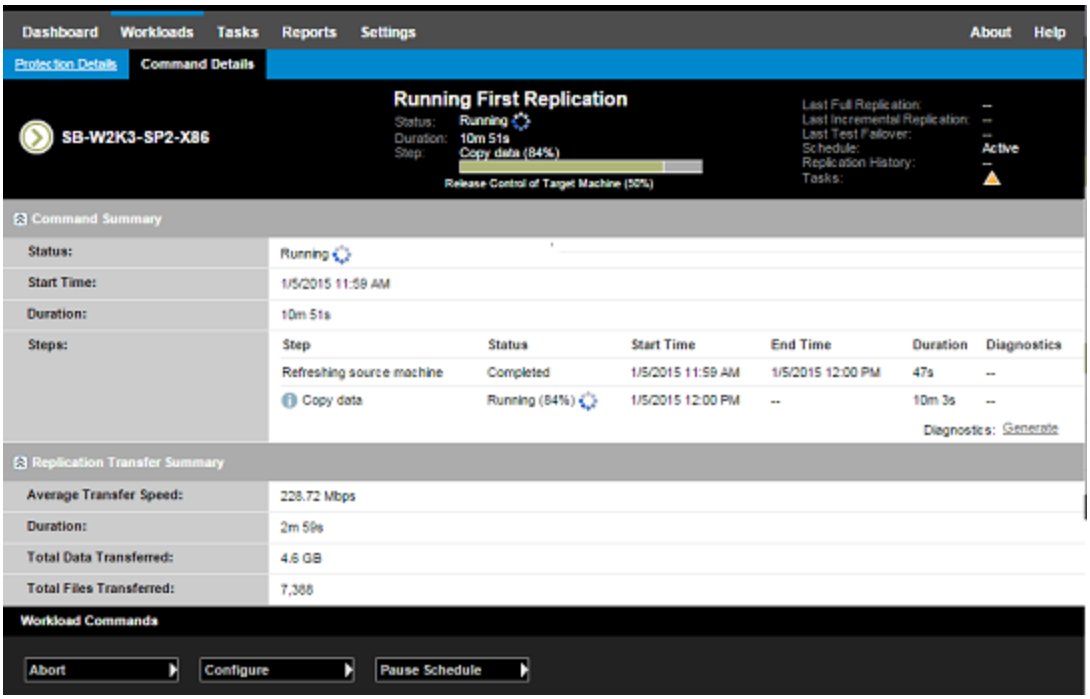
Cuando se complete correctamente, PlateSpin Protect cargará la pantalla Ready for Failback (Preparado para el failback), donde se le pide que especifique los detalles de la operación de failback.

4 Configure los detalles del failback. Consulte “Detalles de failback (carga de trabajo en máquina virtual)” en la página 161.

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 15-2.

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.

Figura 15-2 *Detalles del comando de failback*



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. Consulte la Tabla 15-2 para obtener más información sobre la configuración del parámetro.

Tabla 15-2 *Detalles de failback (carga de trabajo en máquina virtual)*

Configuración de parámetros	Detalles
Configuración de failback	
Transfer Method (Método de transferencia)	Permite seleccionar un mecanismo de transferencia de datos y la seguridad mediante cifrado. Consulte la “Cifrado de datos durante la transmisión” en la página 24.

Configuración de parámetros	Detalles
Failback Network (Red de failback)	Permite especificar la red que se debe usar para el tráfico de failback. Se trata de una red dedicada basada en redes virtuales definidas en el contenedor de máquinas virtuales. Consulte “Redes” en la página 175.
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.
Volume Mapping (Asignación de volumen)	Si el método de réplica inicial especificado es el incremental, seleccione los volúmenes de origen y asígnelos a volúmenes del destino de failback para su sincronización.
Services/Daemons to stop (Servicios/Daemons que se deben detener)	Permite especificar los servicios (Windows) o los daemons (Linux) de la aplicación que se detendrán automáticamente durante el failback. Consulte “Control de servicios y daemons” en la página 171.
Alternative Address for Source (Dirección alternativa para el origen)	Permite especificar una dirección IP adicional para la máquina virtual en failover, si fuera aplicable. Consulte “Requisitos para la protección en redes públicas y privadas mediante NAT” en la página 35.
Workload Settings (Configuración de la carga de trabajo)	
CPU	(Contenedores de máquinas virtuales que usen VMware 5.1, 5.5 u 6.0 con un nivel mínimo de hardware de máquina virtual 8) Especifique el número de zócalos y de núcleos por zócalo para la carga de trabajo virtual de failback. El total de núcleos se calcula automáticamente. Este parámetro se aplica durante la primera instalación de una carga de trabajo con el valor de réplica inicial de **Full** (Réplica completa). **Nota:** el número máximo de núcleos que puede usar la carga de trabajo depende de factores externos, como el sistema operativo invitado, la versión del hardware de la máquina virtual, la licencia de VMware para el host de ESXi y la capacidad de cálculo máxima del host de ESXi para vSphere (consulte *Máximos de configuración de vSphere 5.1* (http://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf)). Algunas distribuciones de un sistema operativo invitado podrían no respetar la configuración de núcleos o de núcleos por zócalo. Por ejemplo, los sistemas operativos invitados que usan SLES 10 SP4 y OES 2 SP3 conservan la configuración de núcleos y zócalos original de la instalación, mientras que otras distribuciones de SLES, RHEL y OES sí respetan la configuración.
Number of CPUs (Número de CPU)	(Contenedores de máquinas virtuales que usen VMware 4.1) Especifique el número necesario de vCPU (CPU virtuales) que se deben asignar a la carga de trabajo virtual de failback. Este parámetro se aplica durante la primera instalación de una carga de trabajo con el valor de réplica inicial de **Full** (Réplica completa). Cada vCPU se presenta al sistema operativo invitado en el contenedor de máquinas virtuales como un único núcleo con un solo zócalo.
VM Memory (Memoria de la máquina virtual)	Permite asignar la RAM necesaria a la carga de trabajo de destino.
Hostname, Domain/Workgroup (Nombre de host, Dominio/Grupo de trabajo)	Permite especificar la identidad y la afiliación de dominio o grupo de trabajo de la carga de trabajo de destino. Para la afiliación del dominio, se necesitan las credenciales del administrador del dominio.

Configuración de parámetros	Detalles
Network Connections (Conexiones de red)	Permite especificar la asignación de red de la carga de trabajo de destino basada en las redes virtuales del contenedor de máquina virtual subyacente.
Service States to Change (Estados de servicio que se deben cambiar)	Permite especificar el estado de inicio de servicios de aplicaciones (Windows) o daemons (Linux) específicos. Consulte “Control de servicios y daemons” en la página 171.
Post-Failback Settings (Configuración tras failback)	
Reprotect Workload (Volver a proteger la carga de trabajo)	Seleccione esta opción si tiene previsto volver a crear el contrato de protección de la carga de trabajo de destino después de la distribución. Con esta opción se conserva un historial continuo de eventos para la carga de trabajo y se asigna o de designa automáticamente una licencia de carga de trabajo.
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 **Reprotect** (Volver a proteger) disponible en el interfaz Web 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.

15.6.2 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 175.
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 “Preparación de controladores de dispositivos para los destinos de failback físicos” en la página 105.
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 167).
   - **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 170.
     - **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).

15.6.3 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.

Es posible efectuar una operación de failback semiautomatizada en un contenedor que cuente con compatibilidad de failback totalmente automatizada (destinos VMware ESX y de clústeres DRS).

También puede realizar una operación de failback semiautomatizada para las plataformas de máquina virtual de destino en hosts de Microsoft Hyper-V Server 2012.

Para iniciar las máquinas virtuales Hyper-V cuando se produzca el failover:

1 En un editor de texto, modifique todos los archivos `/etc/vmware/config` del host de Hyper-V añadiendo la línea siguiente:

```
vhv.allow = "TRUE"
```

2 En el cliente Web de vSphere, modifique la configuración de la máquina virtual de failover para la CPU:

- **2a** En la pestaña **Virtual Hardware** (Hardware virtual), seleccione **CPU.**
- **2b** En **Hardware virtualization** (Virtualización del hardware), seleccione **Expose hardware assisted virtualization to guest OS** (Exponer virtualización asistida de hardware para SO invitado).

3 En el cliente Web de vSphere, modifique la configuración de la máquina virtual de failover para el ID de CPU:

- **3a** En la pestaña **VM Options** (Opciones de la máquina virtual), expanda **Advanced** (Avanzadas) y seleccione **Edit configuration parameters** (Editar parámetros de configuración).
- **3b** Verifique los ajustes siguientes:

```
hypervisor.cpuid.v0 = FALSE
```

15.7 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 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” en la página 160.

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.

16 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 16.1, “Directrices para las credenciales de carga de trabajo y contenedor”, en la página 167
- Sección 16.2, “Niveles de protección”, en la página 168
- Sección 16.3, “Puntos de recuperación”, en la página 170
- Sección 16.4, “Método de réplica inicial (completa o incremental)”, en la página 170
- Sección 16.5, “Control de servicios y daemons”, en la página 171
- Sección 16.6, “Almacenamiento de volúmenes”, en la página 172
- Sección 16.7, “Redes”, en la página 175
- Sección 16.8, “Failback a equipos físicos”, en la página 175
- Sección 16.9, “Protección de clústeres de Windows”, en la página 178

16.1 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 16-1 *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: ◆ Para equipos miembros del dominio: *autoridad\principal* ◆ Para equipos miembros del grupo de trabajo: *nombre de host\principal*
Clústeres de Windows	Credenciales de administrador del dominio	Para equipos miembros del dominio: *autoridad\principal*

Para descubrir	Credenciales	Observaciones
Todas las cargas de trabajo Linux	Nombre de usuario y contraseña de usuario Root	Las cuentas que no sean de usuario Root se deben configurar correctamente para que puedan usar sudo. Consulte el artículo 7920711 de la base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7920711).
Host de VMware ESX o ESXi	Una cuenta de VMware con una configuración de funciones adecuada. Para configurar reglas de arquitectura multiempresa de Protect, consulte “Definición de funciones de VMware para varios inquilinos” en la página 57.	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. Para configurar reglas de arquitectura multiempresa de Protect, consulte “Definición de funciones de VMware para varios inquilinos” en la página 57.	

16.2 Niveles de protección

Un nivel de protección es un conjunto personalizado 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.

Para crear por adelantado niveles de protección personalizados:

1. En la interfaz Web, 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:

Parámetro	Acción
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 **Start of recurrence** (Inicio de la recurrencia) o hacer clic en el icono de calendario para seleccionar una fecha. Seleccione **None** (Ninguno) en Recurrence Pattern (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 esta 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 **Edit** (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)	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 29. Seleccione una de las opciones disponibles. **Fast** (Rápida) es la opción que consume menos recursos de CPU en el origen, pero da como resultado una tasa de compresión inferior; **Maximum** (Máxima) es la que consume más, pero produce una tasa de compresión más alta. **Optimal** (Óptima), la opción intermedia, es la recomendada.
Bandwidth Throttling (Regularización del ancho de banda)	Estos valores controlan la regularización del ancho de banda. Consulte “Regularización del ancho de banda” en la página 29. Para regular las réplicas con una velocidad específica, indique el valor de rendimiento necesario en Mb/s e indique el patrón temporal.
Recovery Points to Keep (Puntos de recuperación que conservar)	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 170.
Workload Failure (Error de carga de trabajo)	Permite especificar el número de intentos de detección de la carga de trabajo antes de que se considere que hay un error.
Workload Detection (Detección de carga de trabajo)	Permite especificar el intervalo de tiempo (en segundos) entre intentos de detección de la carga de trabajo.

16.3 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.

16.4 Método de réplica inicial (completa o incremental)

La *réplica inicial* es la creación de una copia base inicial de una carga de trabajo de producción en la carga de trabajo de failover (réplica virtual) en una operación de protección, o bien desde una carga de trabajo de failover a su infraestructura virtual o física original como preparación para una operación de failback para la carga de trabajo de producción.

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:** se realiza una transferencia de carga de trabajo completa según todos sus datos.
- **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 máquinas virtuales. 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.
  - **Durante un failback a una máquina 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 163).

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.

Para configurar un método de réplica inicial:

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 muestra la página Prepare for Incremental Replication (Preparar para réplica incremental).

4 Seleccione el contenedor requerido, la máquina virtual y la red 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 para 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.

16.5 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 119.

- **Control del estado de inicio o de la 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.

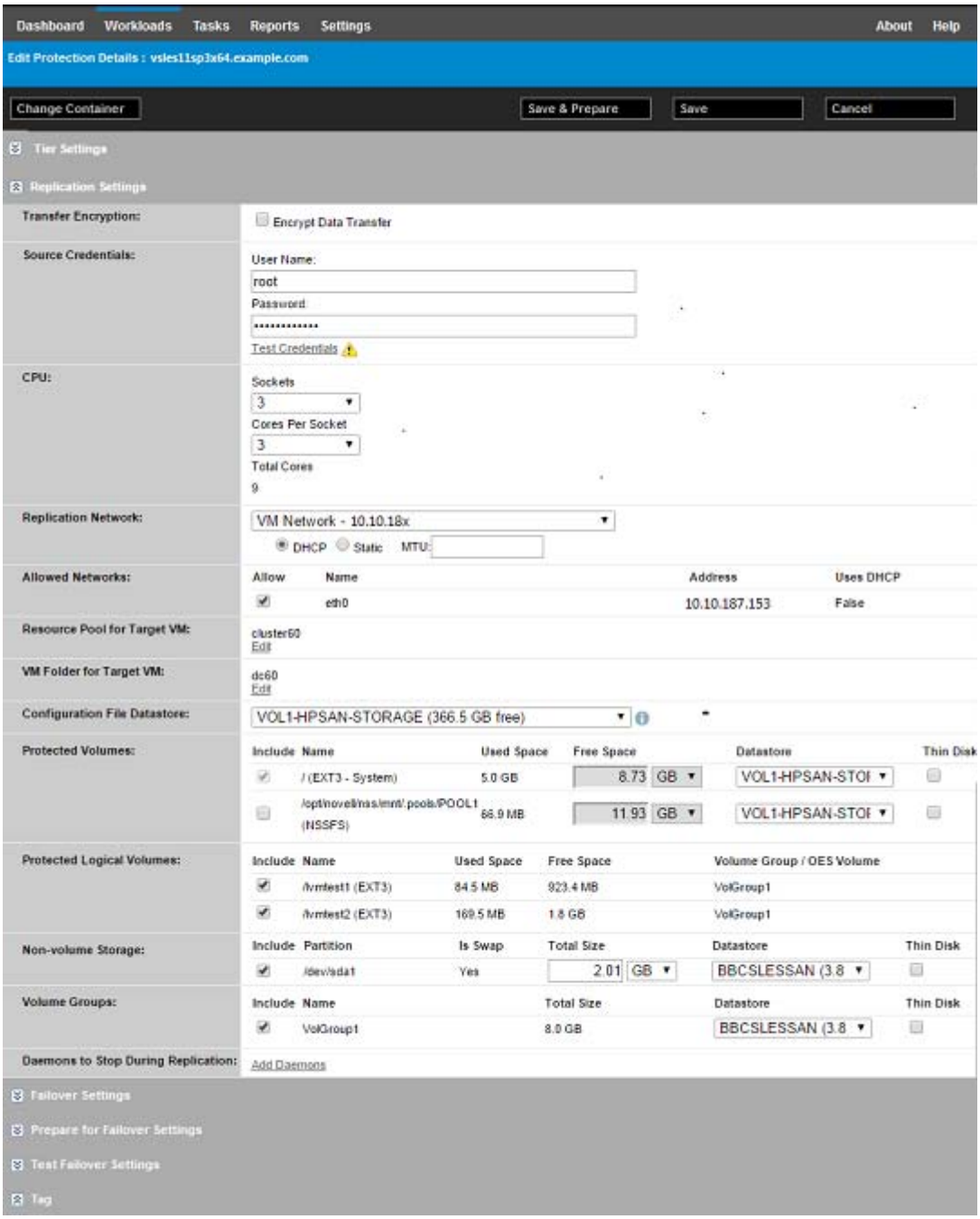
  Los servicios habituales que podría ser útil asignar a un estado de inicio `inhabilitado` son los específicos del proveedor enlazados a su infraestructura física subyacente y que no se necesitan en una máquina virtual.

16.6 Almacenamiento de 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 que se usan para especificar los volúmenes que necesita para la protección. Para obtener más información, consulte la Sección 1.1.5, “Almacenamiento admitido”, en la página 21.

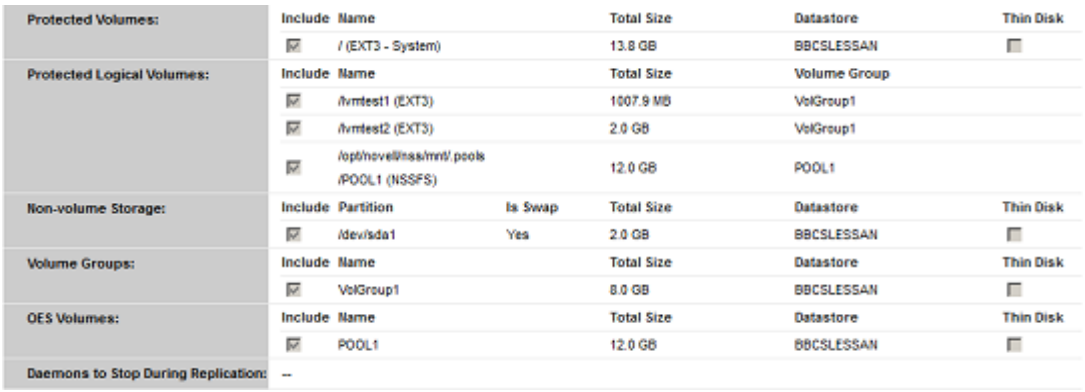
La Figura 16-1 muestra el conjunto de parámetros Replication Settings (Configuración de réplica) para una carga de trabajo Linux con varios volúmenes y dos volúmenes lógicos en un grupo de volúmenes.

Figura 16-1 *Volúmenes, volúmenes lógicos y grupos de volúmenes de una carga de trabajo Linux protegida*



La Figura 16-2 muestra las opciones de protección de volúmenes de una carga de trabajo OES 11 con opciones que indican que los diseños del volumen LVM2 y del grupo NSS deben conservarse y volver a crearse para la carga de trabajo de failover:

Figura 16-2 *Opciones relativas a los volúmenes de Replication Settings (carga de trabajo OES 11)*



La Figura 16-3 muestra las opciones de protección de volúmenes de una carga de trabajo OES 2 con opciones que indican que los diseños de EVMS y del grupo NSS deben conservarse y volver a crearse para la carga de trabajo de failover:

Figura 16-3 *Opciones relativas a los volúmenes de Replication Settings (carga de trabajo OES 2)*

16.7 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 Settings (Valores de réplica)) para separar el tráfico de réplica normal del tráfico de producción.
- **Failover:** (conjunto de parámetros Failover Settings (Valores de 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 Settings (Configuración de la preparación para failover)) para la configuración de red durante la etapa opcional de preparación para failover.
- **Test Failover (Probar failover):** (conjunto de parámetros Test Failover Settings (Valores de prueba de failover)) para la configuración de red que se aplica a la carga de trabajo de failover durante le etapa de prueba de failover.

16.8 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 OFX de arranque de PlateSpin.

- Sección 16.8.1, “Descarga de la imagen ISO OFX de arranque de PlateSpin”, en la página 175
- Sección 16.8.2, “Incorporación de controladores de dispositivo adicionales en la imagen ISO de arranque”, en la página 176
- Sección 16.8.3, “Registro de equipos físicos como destinos de failback con PlateSpin Protect”, en la página 177

16.8.1 Descarga de la imagen ISO OFX de arranque de PlateSpin

Puede descargar las imágenes ISO OFX de arranque de PlateSpin (`bootofx.x2p.iso` para destinos basados en firmware BIOS y para destinos basados en firmware UEFI) desde la página de descarga de software de PlateSpin Protect.

1. Diríjase a la página de descargas de Micro Focus (https://www.microfocus.com/support-and-services/download/).
2. Seleccione PlateSpin Protect en la lista **Buscar por producto** o escriba el nombre del producto en el campo correspondiente para localizar el producto y selecciónelo.
3. En la página de descripción general de la descarga, haga clic en **proceed to download** (Continuar a la descarga) y entre con las credenciales de su cuenta de cliente.
4. Haga clic en **accept** (Aceptar) para aceptar su conformidad con las leyes y normativas de exportación de EE. UU.
5. En la página Download (Descarga), haga clic en el enlace **download** (Descargar) situado junto al archivo `bootofx.x2p.iso` y, a continuación, guarde el archivo.

16.8.2 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.

Para usar esta utilidad:

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 base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7005990).

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

Argumento	Descripción
`-c <vía>`	<*vía*> especifica la ubicación en la que se encuentra un archivo `ConfigureTakeControl.xml`.

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

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
  ```

16.8.3 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
   ```

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.

16.9 Protección de clústeres de Windows

PlateSpin Protect admite la protección de servicios empresariales de un clúster de Microsoft Windows Server. Para obtener información sobre los requisitos y las opciones para proteger nodos en un clúster de Windows Server, consulte el Capítulo 13, “Preparación para proteger clústeres de Windows”, en la página 121.

- Sección 16.9.1, “Failover de PlateSpin”, en la página 178
- Sección 16.9.2, “Failback de PlateSpin”, en la página 179

16.9.1 Failover de PlateSpin

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

Para realizar el failover de PlateSpin (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).

16.9.2 Failback de PlateSpin

La operación de failback de PlateSpin requiere una réplica completa para las carga de trabajo de Windows Cluster.

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

- Asigne todos los discos del clúster de un nodo virtual de PlateSpin 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 de PlateSpin para que restaure el volumen del sistema de la máquina de failover al `Disco 1` y los discos adicionales de la máquina 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.

Después de completar un failback de PlateSpin, debe reconectar el almacenamiento compartido y reconstruir el entorno de clúster antes de poder reunir nodos adicionales al clúster recién restaurado.

Nota: si el clúster se encuentra en el estado **Ready To Reprotect** (Preparado para volver a proteger), asegúrese de reconstruir y restaurar primero el destino de failback para que se descubra como clúster. Debe desinstalar manualmente el controlador de clústeres de PlateSpin como parte del proceso de reconstrucción.

Para obtener información sobre la reconstrucción del entorno de clúster después de que se produzca un failover y un failback de PlateSpin, consulte los recursos siguientes:

- **Clúster de failover de Windows Server 2012 R2 (failback a reconstrucción física o virtual):** consulte el artículo 7016770 de la base de conocimientos (http://www.netiq.com/support/kb/doc.php?id=7016770).
- **Clúster de failover de Windows Server 2008 R2 (failback a reconstrucción física o virtual):** consulte el artículo 7015576 de la base de conocimientos (http://www.netiq.com/support/kb/doc.php?id=7015576).

---

17 Generación de informes

Puede generar informes sobre las cargas de trabajo descubiertas y los contratos de protección de cargas de trabajos mediante la interfaz Web de PlateSpin. Para obtener información sobre cómo generar un informe de licencias, consulte la Sección 4.6, “Generación de un informe de licencias para la asistencia técnica”, en la página 52.

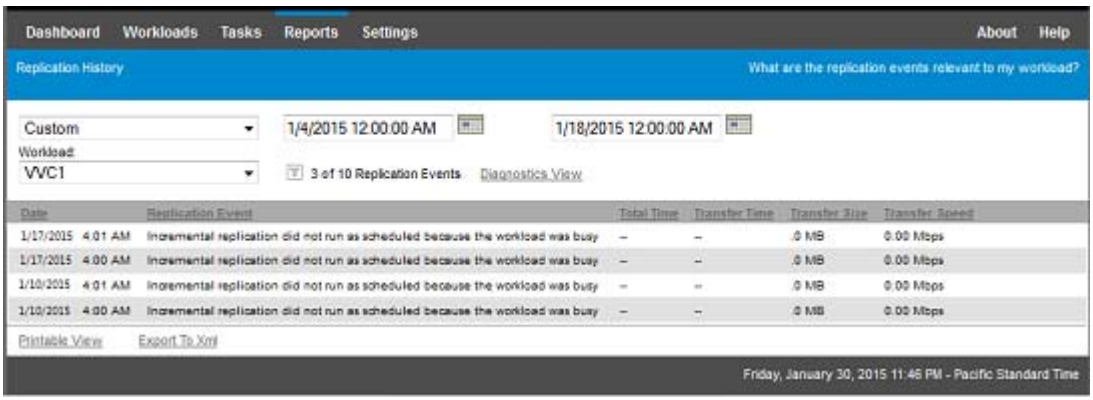
- Sección 17.1, “Acerca de los informes de Protect”, en la página 182
- Sección 17.2, “Generación de informes de carga de trabajo y de protección de la carga de trabajo”, en la página 182
- Sección 17.3, “Generación de informes de diagnóstico”, en la página 183

17.1 Acerca de los informes de Protect

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

- **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 17-1 *Opciones de un informe de historial de réplica*



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

Para generar un informe:

1. En la interfaz Web, 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.
3. Seleccione una o varias cargas de trabajo para las que desee crear el informe.
4. Configure el periodo de tiempo cuyo informe desee ver.
5. Especifique los parámetros adecuados para el informe.

6 Realice una de las siguientes acciones:

- Haga clic en **Printable View** (Vista para imprimir) para ver el informe en el navegador Web.
- Haga clic en **Export to XML** Exportar a XML y guarde el archivo XML en su equipo.

17.3 Generación 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, a continuación, haga clic en el enlace **Generate** (Generar) en la parte inferior derecha del panel.

   Tras un tiempo, la página se actualiza y muestra el enlace **Download** (Descargar) encima del enlace **Generated** (Generar).

2 Haga clic en **Download** (Descargar).

   En un archivo `.zip` se incluye información de diagnóstico completa sobre el comando actual.

3 Guarde el archivo y extraiga el diagnóstico para consultarlo.

4 Tenga preparado el archivo `.zip` si necesita ponerse en contacto con el servicio de asistencia técnica.

18 Solución de problemas de protección y recuperación de cargas de trabajo

Esta sección le ayudará a solucionar problemas habituales durante la protección y la recuperación de cargas de trabajo.

Para los problemas de descubrimiento e inventario en las cargas de trabajo de origen y los hosts de destino, consulte el Capítulo 14, “Solución de problemas de descubrimiento e inventario de cargas de trabajo”, en la página 131.

- Sección 18.1, “Optimización del rendimiento de una conexión”, en la página 185
- Sección 18.2, “Solución de problemas de reenvío de tráfico en las cargas de trabajo”, en la página 185
- Sección 18.3, “Solución de problemas del servicio de configuración”, en la página 186
- Sección 18.4, “Solución de problemas de réplica al preparar la carga de trabajo (Windows)”, en la página 191
- Sección 18.5, “Solución de problemas de réplica de la carga de trabajo”, en la página 192
- Sección 18.6, “Solución de problemas de failover o failback de la carga de trabajo”, en la página 194
- Sección 18.7, “Compresión de las bases de datos de PlateSpin Protect”, en la página 195
- Sección 18.8, “Limpieza de la carga de trabajo después de la protección”, en la página 195

18.1 Optimización del rendimiento de una conexión

Si experimenta un rendimiento lento, puede probar la conexión para comprobar si hay algún problema en ella o en el ancho de banda y resolverlo. Consulte el Apéndice F, “Uso de la herramienta de prueba de red iPerf para optimizar el rendimiento de red para productos de PlateSpin”, en la página 205.

18.2 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 base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7005495).

18.3 Solución de problemas del servicio de configuración

Después de una prueba de failover o una operación de failover, se produce un error en la máquina virtual de destino debido a problemas no específicos del servicio de configuración. El mensaje de error habitual es:

```
Configuration service in the target machine does not seem to have started. (Parece que el servicio de configuración de la máquina de destino no se ha iniciado)
```

Las sugerencias para solucionar problemas de esta sección explican los problemas habituales del servicio de configuración y formas alternativas para resolverlos.

- Sección 18.3.1, “Comprensión de las causas del problema”, en la página 186
- Sección 18.3.2, “¿Qué se puede hacer para resolver el problema?”, en la página 187
- Sección 18.3.3, “Sugerencias adicionales para la solución de problemas”, en la página 190

18.3.1 Comprensión de las causas del problema

El error del servicio de configuración indica que el servidor de PlateSpin no puede comunicarse con el servicio de configuración de la máquina virtual de destino. Analice el sistema para determinar la posible causa del problema.

- “Error al arrancar la máquina virtual de destino” en la página 186
- “La red no está configurada correctamente” en la página 186
- “No es posible leer ni escribir los mensajes de estado para los dispositivos de disquete” en la página 186

Error al arrancar la máquina virtual de destino

El sistema operativo debe cargarse en la máquina virtual de destino para que el servicio de configuración se inicie con normalidad. Un fallo del arranque indica que podría haber un conflicto del controlador, un error del cargador de arranque o posibles daños en el disco.

Si el sistema operativo no arranca en la máquina virtual de destino, se recomienda abrir un ticket de servicio en la Atención al cliente de Micro Focus.

La red no está configurada correctamente

La red debe configurarse correctamente para que el servicio de configuración de la carga de trabajo de destino pueda comunicarse con el servidor de PlateSpin.

Asegúrese de que ha configurado la red de manera que la carga de trabajo de destino pueda comunicarse con el servidor de PlateSpin. Consulte la Sección 1.5, “Requisitos de acceso y comunicación en la red de protección”, en la página 31.

No es posible leer ni escribir los mensajes de estado para los dispositivos de disquete

El servicio de configuración debe ser capaz de comunicarse con los dispositivos de disquete de las máquinas virtuales de VMware con el fin de leer y escribir los mensajes de estado para el servidor de PlateSpin.

En la máquina virtual de destino, compruebe que la máquina es capaz de comunicarse con los dispositivos de disquete:

1. En la máquina virtual, abra el archivo de registro (`C:\windows\platespin\configuration\data\log.txt`).
2. Cualquiera de los mensajes siguientes podría ser una indicación de que no es posible acceder al disco:

```
Failed (5) to write to file \\?\Volume{<guid-number>}\log.zip (Error [5] al escribir el
archivo \\?\Volume{<número-guid>}\log.zip)
CopyFile \\?\Volume{<guid-number>}\windows\platespin\configuration\data\result.txt to
\\?\Volume{<guid-number>}\result.txt failed (Error al copiar el archivo
\\?\Volume{<número-guid>}\windows\platespin\configuration\data\result.txt en
\\?\Volume{<número-guid>}\result.txt
The output floppy was not accessible after the timeout period (No es posible acceder al
disquete de salida después del tiempo límite)
```

18.3.2 ¿Qué se puede hacer para resolver el problema?

Para resolver un error del servicio de configuración, puede intentar alguna de las soluciones de esta sección.

- “Omitir las optimizaciones de rearranque de la máquina virtual de destino” en la página 187
- “Reducir el tráfico de lectura/escritura a los dispositivos de disquete” en la página 188
- “Cambiar el tipo de inicio para aumentar la demora” en la página 189
- “Configurar los servicios conflictivos para que no se ejecuten automáticamente durante el inicio” en la página 190

Omitir las optimizaciones de rearranque de la máquina virtual de destino

Protect intenta minimizar el número de rearranques que se producen en la máquina virtual de destino por defecto para acelerar el proceso de transición. Es posible que al permitir los rearranques adicionales mejore la capacidad de la máquina virtual de destino para comunicarse con el servidor de PlateSpin.

Para omitir las optimizaciones de rearranque:

1. Entre al servidor de PlateSpin y abra la página de configuración del servidor de PlateSpin en:

   `https://Servidor_de_PlateSpin/platespinconfiguration/`
2. Busque el parámetro **ConfigurationServiceValues**.
3. Edite el parámetro **ConfigurationServiceValues** y defina en la opción **SkipRebootOptimization** el valor `true` (verdadero).
4. Haga clic en **Save** (Guardar).
5. Ejecute una réplica incremental o completa.

   La réplica también propaga los valores de configuración modificados a la máquina virtual de destino.
6. Ejecute de nuevo la operación de failover de prueba o de failover para las cargas de trabajo afectadas.

Reducir el tráfico de lectura/escritura a los dispositivos de disquete

Puede reducir el número de veces que el servidor de PlateSpin intenta leer y escribir en los dispositivos de entrada de VMware o de salida de disquete si el registro de diagnóstico muestra el siguiente error:

`Information:1:Attempting floppy download` (Información:1:intento de descarga de disquete)

seguido de

`Verbose:1:Failed to copy file from remote URL` (Detallado:1:error al copiar el archivo de la URL remota)

-o bien-

`Exception: The remote server returned an error: (500) Internal Server Error` (Excepción: error en el servidor remoto: (500) Error del servidor interno)

Este error se debe a que VMware bloquea el recurso. Indica que el servidor de PlateSpin desasocia y vuelve a asociar el disquete cada vez que comprueba el estado. El bloqueo puede causar que la máquina virtual de destino no pueda leer ni escribir en el dispositivo de disquete. Consulte *Using the VMware vCenter Server 4.x,5.x and 6.0 Datastore Browser to Download or Copy a Powered-On Virtual Machine's .vmx and .nvram Files Fails (1019286)* (https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1019286) (Al usar el navegador de almacén de datos de VMware vCenter Server 4.x, 5.x y 6.0 para descargar o copiar, los archivos .vmx y .nvram de un máquina virtual encendida fallan [1019286])

Si experimenta problemas de bloqueo del dispositivo de disquete, puede aumentar los valores de sondeo del servicio de configuración en el servidor de PlateSpin:

vmwareConfigServicePollStartDelay

Este parámetro determina el tiempo que espera el servidor de PlateSpin para iniciar el sondeo del estado de la carga de trabajo de destino. El valor por defecto es 120 segundos (2 minutos).

vmwareConfigServicePollIntervalInMilliseconds

Este parámetro determina la frecuencia con la que el servidor de PlateSpin intenta comunicarse con la carga de trabajo de destino y leer o escribir en los dispositivos de disquete de VMware. El intervalo de sondeo por defecto es de 30 000 milisegundos (30 segundos).

vmwareConfigServicePollStartTimeout

Este parámetro determina el tiempo que espera el servidor de PlateSpin después de iniciar la máquina virtual de destino antes de mostrar un error en la interfaz Web. El valor por defecto es 420 segundos (7 minutos).

vmwareConfigServicePollUpdateTimeout

Este parámetro determina el tiempo que espera el servidor de PlateSpin después de cada intervalo de sondeo antes de mostrar un error en la interfaz Web. El valor por defecto es 300 segundos (5 minutos).

Los valores más altos de estos parámetros reducen la frecuencia con la que el servidor de PlateSpin intenta leer y escribir en los dispositivos de disquete de VMware de las máquinas virtuales de destino.

Para reducir el tráfico de lectura y escritura para los dispositivos de disquete de VMware:

1. Entre al servidor de PlateSpin y abra la página de configuración del servidor de PlateSpin en:

   `https://`*`Servidor_de_PlateSpin`*`/platespinconfiguration/`

2 Busque los parámetros de sondeo del servicio de configuración, modifique los valores según corresponda y haga clic en **Save** (Guardar).

   Por ejemplo:

   ```
   vmwareConfigServicePollStartDelay = 180 (3 minutos)
   vmwareConfigServicePollIntervalInMilliseconds = 300000 (5 minutos)
   vmwareConfigServicePollStartTimeout = 1200 (20 minutos)
   vmwareConfigServicePollUpdateTimeout = 900 (15 minutos)
   ```

   o bien

   ```
   vmwareConfigServicePollStartDelay = 300 (5 minutos)
   vmwareConfigServicePollIntervalInMilliseconds = 480000 (8 minutos)
   vmwareConfigServicePollStartTimeout = 1200 (20 minutos)
   vmwareConfigServicePollUpdateTimeout = 900 (15 minutos)
   ```

3 Ejecute una réplica incremental o completa.

   La réplica también propaga los valores de configuración modificados a la máquina virtual de destino.

4 Ejecute de nuevo la operación de failover de prueba o de failover para las cargas de trabajo afectadas.

Cambiar el tipo de inicio para aumentar la demora

El servicio de configuración podría aparecer antes de que se pueda acceder a los recursos. Puede cambiar el tipo de inicio del servicio configuración para aumentar la demora.

Para cambiar el tipo de inicio:

1 Entre al servidor de PlateSpin y abra la página de configuración del servidor de PlateSpin en:

   `https://Servidor_de_PlateSpin/platespinconfiguration/`

2 Busque el parámetro **windowsConfigServiceStartType**.

3 Cambie el valor **windowsConfigServiceStartType** a **AutoDelay**.

   Las opciones para **windowsConfigServiceStartType** son estas:

   - **GroupDelay** es el valor por defecto y añade el servicio de configuración al final de **ServiceGroupOrder** en el registro.
   - **AutoDelay** maximiza la cantidad de tiempo que el servicio espera antes de iniciarse (2 minutos después del arranque). Modifique también el valor del parámetro **ServicesPipeTimeoutForWindowsConfigService** en el Paso 4.
   - **NoDelay** es la opción más eficaz e inicia el servicio en cuando lo permite Windows. Sin embargo, no se recomienda por los posibles problemas de conexión a los recursos.

4 (AutoDelay) Cambie el valor del parámetro **ServicesPipeTimeoutForWindowsConfigService** a 180 segundos para tener en cuenta los 120 segundos que el servicio tardará en iniciarse después del arranque si AutoDelay está definido para el parámetro **windowsConfigServiceStartType** en el Paso 3.

5 Haga clic en **Save** (Guardar).

6 Ejecute una réplica incremental o completa.

   La réplica también propaga los valores de configuración modificados a la máquina virtual de destino.

7 Ejecute de nuevo la operación de failover de prueba o de failover para las cargas de trabajo afectadas.

Configurar los servicios conflictivos para que no se ejecuten automáticamente durante el inicio

Durante una acción de failover, un servicio de Windows interfiere con el montaje de los controladores del disquete.

Determine qué servicios de Windows están configurados para iniciarse en el rearranque. Se sabe que algunos servicios interfieren con la escritura del servicio de configuración en los disquetes; por ejemplo, algunos programas antivirus y de configuración inalámbrica. Debe configurar estos servicios para que no se ejecuten automáticamente en la prueba de failover o la operación de failover y, después, ejecutar de nuevo estas acciones.

También puede intentar inhabilitar todos los servicios no esenciales para la prueba de failover y la operación de failover en la página de configuración y, después, ejecutar de nuevo estas acciones.

18.3.3 Sugerencias adicionales para la solución de problemas

Si el servicio de configuración no puede contactar con el servidor de PlateSpin, el diagnóstico mostrará únicamente una parte de la realidad. También debe obtener los registros de la máquina virtual de destino:

- **Cargas de trabajo Windows:** los registros del servicio de configuración se encuentran en la carpeta `C:\windows\platespin\configuration\data`.
  - El archivo `log.txt` contiene toda la información de registro, pero el archivo `Config.ini` resulta útil para entender lo que se debe configurar.
  - El archivo `result.txt` contiene el estado de ejecución del servicio de configuración.
  - Si la máquina virtual de destino no puede leer el dispositivo de disquete de entrada, no contará con el archivo `Config.ini` combinado, lo que podría incluir información de configuración de la red personalizada para el entorno de red de failover.
  - Si el archivo `Config.ini` no tiene ninguna información relacionada con la red (como un `[NIC0]`), puede que el adaptador de red de la máquina virtual de destino tenga caracteres especiales en el nombre.

    Es un problema conocido que el archivo `Config.ini` podría no ser preciso hasta que se combina con el del dispositivo de disquete.
  - La máquina virtual de destino intenta rearrancar si no puede conectarse con el disquete de salida o el disquete de entrada (solo una vez). Si fuera el caso, verá el archivo `config.ini.floppyreboot`.
- **Cargas de trabajo Linux:** los registros del servicio de configuración se encuentran en la carpeta `/tmp`.
  - Los archivos de registro principales se denominan `file*.platespin.fileLogger`.

    Se recomienda examinar todas las carpetas de configuración de `/tmp`. Cree un archivo TAR con las carpetas de configuración junto con los archivos `file*.platespin.fileLogger` para enviarlo a la Atención al cliente de Micro Focus.
  - Otros archivos de configuración que hay que comprobar son los siguientes:

    ```
    /tmp/Ofx.RunCommand.Output*
    /tmp/*DiskHelper*
    /tmp/*VmTools*
    ```

- El archivo de configuración es `/usr/lib/psconfigservice/data/config.conf`.
- El archivo de registro de resultado final es `/usr/lib/psconfigservice/data/result.txt`.

18.4 Solución de problemas de réplica al preparar la carga de trabajo (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 191.
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 “Resolución de problemas de descubrimiento para cargas de trabajo Windows” en la página 131.

18.4.1 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.

Es posible actualizar la directiva de inmediato mediante el comando `gpudate /force`.

18.4.2 Dos o más volúmenes tienen el mismo número de serie de volumen

Problema: si intenta configurar una protección para un servidor Windows, se muestra el siguiente error:

```
[Source] Two or more volumes have the same serial number. Change the serial numbers so that they are unique and rediscover the machine. ([Origen] Dos o más volúmenes tienen el mismo número de serie. Cambie los números de serie para que sean exclusivos y vuelva a descubrir la máquina).
```

Solución: este problema puede producirse si el número de serie del volumen es el mismo para dos o más volúmenes. PlateSpin Protect requiere que los números de serie sean exclusivos.

Para solucionar este problema, modifique los números de serie de los volúmenes de datos según sea preciso y, a continuación, descubra de nuevo la máquina. Para obtener información sobre cómo usar las herramientas nativas de Windows para modificar los números de serie, consulte el artículo 7921101 de la base de conocimientos.

18.5 Solución de problemas de réplica de la carga de trabajo

Problemas o mensajes	Solución
Error recuperable durante la réplica en el paso **programar la toma de una instantánea del equipo virtual** o en el paso **programar la reversión de la máquina virtual a una instantánea antes del inicio**.	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.
La réplica incremental basada en archivos no se completa si el cifrado está habilitado	Después de habilitar el cifrado para una carga de trabajo Windows configurada para la transferencia de datos basada en archivos, el receptor de Windows podría bloquearse a final de la transferencia en el caso de las réplicas incrementales. El bloqueo se produce si el proceso de cifrado define de forma incorrecta la lectura del último byte de la transferencia como un valor distinto a cero, lo que indica que se están transfiriendo más archivos y que debe seguir leyendo la secuencia. Puede usar la transferencia de datos basada en bloques para las cargas de trabajo Windows si desea habilitar el cifrado para las transferencias de datos de 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.
La protección a través de WAN lleva mucho tiempo si el contenedor de máquinas virtuales contiene muchos almacenes de datos	en algunas circunstancias, el proceso de localizar la imagen ISO adecuada necesaria para arrancar el destino puede tardar más de lo esperado. Esto puede ocurrir cuando el servidor de PlateSpin está conectado al contenedor de máquinas virtuales a través de una red WAN y el contenedor tiene muchos almacenes de datos.
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.

Problemas o mensajes	Solución
Velocidad de red lenta, por encima de 1 MB.	Mida la latencia ejecutando el comando siguiente en la carga de trabajo de origen: `ping ip-t` (sustituya *ip* 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 71.

`No es posible iniciar la transferencia de archivos. El puerto 3725 ya está en uso.`
 	
O bien
 	
`No es posible conectar con el puerto 3725.`
	Asegúrese de que el puerto está abierto y a la escucha:
	
	Ejecute `netstat -ano` en la carga de trabajo.
	
	Compruebe el cortafuegos.
	
	Vuelva a intentar la réplica.

`Conexión del controlador no establecida.` Error de réplica en el paso **Toma de control de la máquina virtual.**	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. Cambie la IP de réplica a una IP estática y habilite el servidor DHCP. Asegúrese de que la red virtual seleccionada para la réplica se puede enrutar al host del servidor de PlateSpin.
El trabajo de réplica no se inicia (se bloquea al 0 %)	Este error se puede producir por varias razones, y cada una de ellas tiene una solución distinta: ◆ 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 7920339 de la base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7920339). ◆ Si las directivas locales o de dominio restringen los permisos necesarios, siga los pasos descritos en el artículo 7920862 de la base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7920862). 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 191.

Problemas o mensajes	Solución
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.	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* (http://msdn.microsoft.com/en-us/library/aa819132.aspx) para obtener más información. 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`.

18.6 Solución de problemas de failover o failback de la carga de trabajo

Problemas o mensajes	Solución
Los servicios de dominio de Active Directory no están disponibles después de una operación de failback (Windows).	Los servicios de dominio de Active Directory podrían no abrirse después de una operación de failover, si se producen errores de `chkdsk`. Hay dos causas de los errores de `chkdsk` que se pueden evitar: ◆ Los archivos de registro relacionados con las actualizaciones de Microsoft si el equipo de origen no se ha actualizado con todos los parches y actualizaciones recomendados de Microsoft cuando se realiza la primera réplica completa. ◆ Los archivos y carpetas del sistema que se deben excluir del software antivirus. Para evitar estos problemas, siga las prácticas recomendadas descritas en la Sección 15.1, “Requisitos previos para proteger las cargas de trabajo”, en la página 151 antes de ejecutar la primera réplica completa.
Durante el failback, se asignan NIC erróneas y el failback se bloquea.	Para permitir que el failback se complete correctamente, utilice una de las siguientes soluciones: ◆ Cambie la configuración de IP a las asignaciones esperadas, de forma que el destino se configure correctamente. ◆ Rearranque el hardware de "toma de control" en el LRD y repita los pasos para usarlo como destino de failback. Hay bastante probabilidad de que se asignen las interface Ethernet correctas a Protect la próxima vez. ◆ En la interfaz Web, si el failback parece bloquearse casi al final, es probable que el destino de failback no pueda comunicarse con el servidor de PlateSpin. Cambie los cables de red de la parte posterior del destino de failback para colocar la NIC correcta en las redes previstas. Esto permite que el destino de failback se comunique con el servidor de PlateSpin y que se complete el failback.

Problemas o mensajes	Solución
El failback X2P de cargas de trabajo Linux produce fallos de la interfaz gráfica de X-Server.	El problema está causado por una reconfiguración de la máquina virtual que ha pasado por el failover cuando se instaló VMware Tools. Para corregirlo, use el comando siguiente para buscar los archivos con la cadena `BeforeVMwareToolsInstall` en su nombre de archivo: `find / -iname '*BeforeVMwareToolsInstall'` Después de identificar todos estos archivos, devuélvalos a sus ubicaciones originales y vuelva a arrancar la carga de trabajo para corregir la interfaz de X Server.

18.7 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 base de conocimientos (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.

18.8 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.

- Sección 18.8.1, “Limpieza de las cargas de trabajo Windows”, en la página 195
- Sección 18.8.2, “Limpieza de las cargas de trabajo Linux”, en la página 196

18.8.1 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 base de conocimientos (https://www.netiq.com/support/kb/doc.php?id=7005616).
Componente de transferencia basada en bloques de otros fabricantes (discontinuado)	1. Use el applet Agregar o quitar programas (ejecute `appwiz.cpl`) y elimine el componente. Según el origen, puede que tenga una de estas versiones: ◆ Réplica de datos SteelEye para Windows versión 6 actualización 2 ◆ SteelEye DataKeeper para Windows versión 7 2. Rearranque el equipo.

Componente	Instrucciones de eliminación
Componente de transferencia basada en archivos	En el nivel raíz de cada volumen protegido, elimine todos los archivos con el nombre `PlateSpinCatalog*.dat`..
Software de inventario de carga de trabajo	En el directorio `Windows` de la carga de trabajo: ◆ Elimine todos los archivos con el nombre `machinediscovery*`. ◆ Elimine el subdirectorio denominado `platespin`.
Software de controlador	1. Abra un indicador de comandos en la carga de trabajo de origen y cambie el directorio actual a: ◆ `\Archivos de programa\platespin*` (sistemas de 32 bits) ◆ `\Archivos de programa (x86)\platespin*` (sistemas de 64 bits) 2. Ejecute el comando siguiente: `ofxcontroller.exe /uninstall` 3. Elimine el directorio `platespin*`..

18.8.2 Limpieza de las cargas de trabajo Linux

Componente	Instrucciones de eliminación
Software de controlador	◆ Elimine estos procesos: ◆ `pkill -9 ofxcontrollerd` ◆ `pkill -9 ofxjobexec` ◆ Elimine el paquete RPM del controlador OFX: `rpm -e ofxcontrollerd` ◆ En el sistema de archivos de la carga de trabajo, elimine el directorio `/usr/lib/ofx` con su contenido.

Componente	Instrucciones de eliminación

Software de transferencia de datos en el nivel de bloques	1. Compruebe si el controlador está activo:
	`lsmod | grep blkwatch`
	Si el controlador sigue cargado en la memoria, el resultado debe contener una línea similar a la siguiente:
	`blkwatch_7616 70924 0`
	2. (Condicional) Si el controlador sigue cargado, elimínelo de la memoria:
	`rmmod blkwatch_7616`
	3. Elimine el controlador de la secuencia de arranque:
	`blkconfig -u`
	4. Elimine los archivos del controlador suprimiendo el directorio siguiente con su contenido:
	`/lib/modules/`*`[Versión_Núcleo]`*`/Platespin`
	5. Suprima el archivo siguiente:
	`/etc/blkwatch.conf`

Instantáneas LVM	Las instantáneas LVM usadas en las réplicas continuas recibe un nombre según la convención *`nombre_del_volumen`*`-PS-snapshot`. Por ejemplo, una instantánea del volumen `LogVol01` se llamará `LogVol01-PS-snapshot`. Para eliminar estas instantáneas LVM: 1. Genere una lista de instantáneas de la carga de trabajo requerida de una de estas formas: ◆ Use la interfaz Web 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: `# lvdisplay -a` 2. Anote los nombres y ubicaciones de las instantáneas que desea eliminar. 3. Elimine las instantáneas mediante el comando siguiente: `lvremove` *nombre_de_instantánea*

Componente	Instrucciones de eliminación
Instantánea NSS	Una instantánea NSS creada y utilizada por PlateSpin para las réplicas siguientes. El nombre de la instantánea termina con el sufijo `PSSNP`. Para eliminar estas instantáneas NSS: 1. Genere una lista de instantáneas de la carga de trabajo requerida de una de estas formas: ◆ Use la interfaz Web para generar un informe de tarea para la tarea con errores. El informe debe contener información sobre las instantáneas NSS y sus nombres. **- O bien -** ◆ En la carga de trabajo Open Enterprise Server requerida, introduzca el comando siguiente para mostrar una lista de todas las instantáneas NSS: `# NLVM list snaps` **- O bien -** ◆ En la carga de trabajo Open Enterprise Server necesaria, lance NSSMU y seleccione **Snapshot** (Instantánea) para ver una lista de instantáneas. 2. Anote los nombres y ubicaciones de las instantáneas que desea eliminar. 3. En la carga de trabajo Open Enterprise Server, elimine las instantáneas adecuadas mediante uno de los siguientes métodos: ◆ Introduzca el siguiente comando: `NLVM delete snap` <*nombre_instantánea*> **- O bien -** ◆ Lance NSSMU y seleccione **Snapshot** (Instantánea). Para cada instantánea que desee suprimir, resalte la instantánea y pulse la tecla Suprimir.
Archivos de mapas de bits (bitmap)	Para cada volumen protegido, elimine el archivo `.blocks_bitmap` correspondiente de la raíz del volumen.
Herramientas	En la carga de trabajo de origen, en `/sbin`, elimine los siguientes archivos: ◆ `bmaputil` ◆ `blkconfig`

V Herramientas de PlateSpin

PlateSpin Protect proporciona herramientas adicionales para mejorar su entorno de protección.

- Apéndice E, “Uso de funciones de protección de la carga de trabajo mediante la API del servidor de PlateSpin Protect”, en la página 201
- Apéndice F, “Uso de la herramienta de prueba de red iPerf para optimizar el rendimiento de red para productos de PlateSpin”, en la página 205

E Uso de funciones de protección de la carga de trabajo mediante la API del servidor de PlateSpin Protect

Puede usar las funciones de protección de cargas de trabajo de PlateSpin Protect mediante programación a través de la API del servidor de PlateSpin Protect (`protectionservices`) desde las aplicaciones. Puede usar cualquier lenguaje de programación o de guiones que admita un cliente HTTP y el entorno de serialización JSON.

Nota: la API del servidor de Protect es experimental. La información de esta sección se proporciona como vista previa tecnológica.

- Sección E.1, “Descripción general de la API”, en la página 201
- Sección E.2, “Documentación de la API del servidor de PlateSpin Protect”, en la página 201
- Sección E.3, “Muestras y otras referencias”, en la página 202

E.1 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
- Dscubrir 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

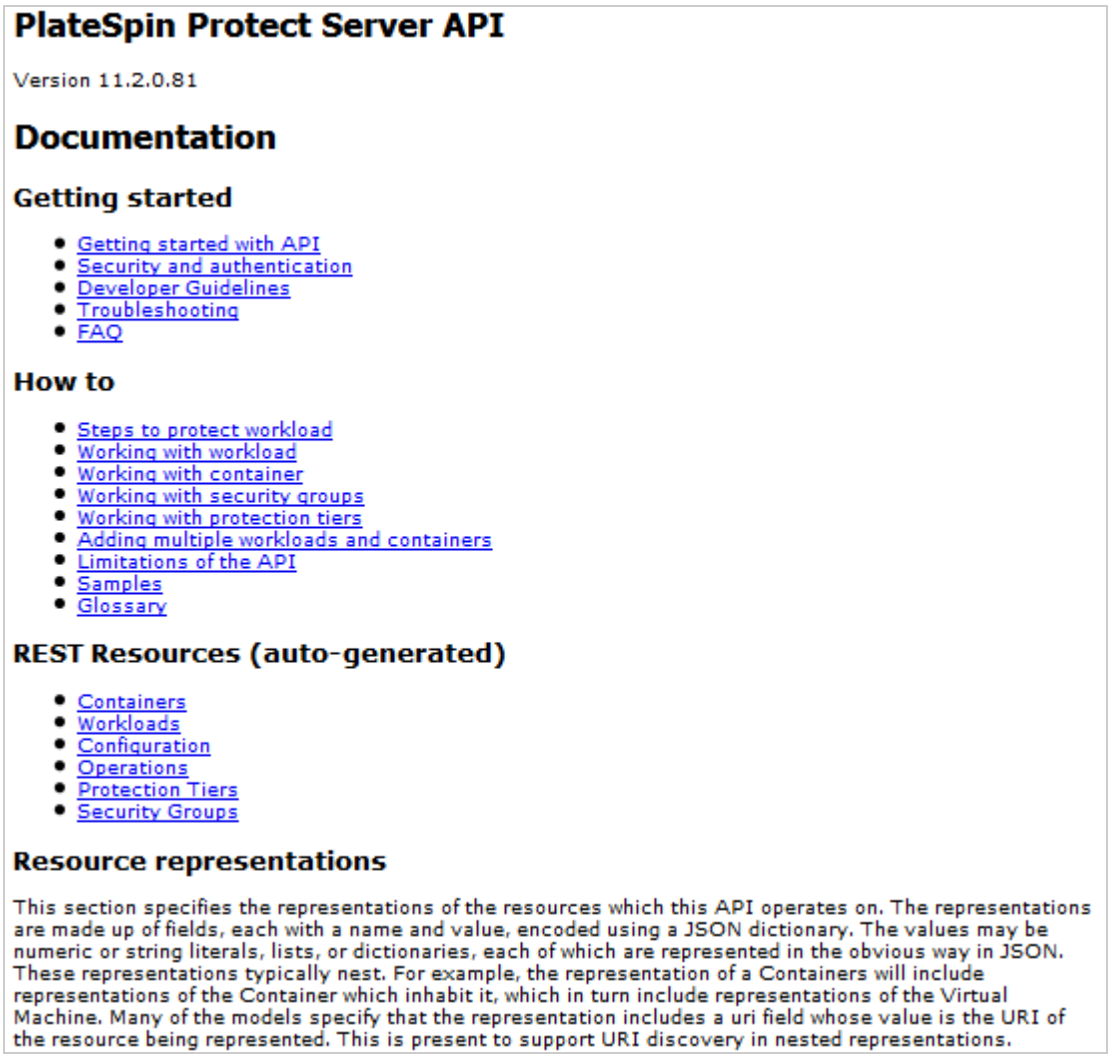
E.2 Documentación de la API del servidor de PlateSpin Protect

La página principal de la API del servidor de PlateSpin Protect para `protectionservices` proporciona documentación y ejemplos que pueden resultar de utilidad para desarrolladores y administradores. Para obtener más información, diríjase a la ubicación siguiente del host del servidor de PlateSpin:

`https://`*Servidor_de_PlateSpin*`/protectionservices/`

Sustituya *Servidor_de_PlateSpin* por 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 E-1 *Página principal de la API del servidor de Protect*



E.3 Muestras y otras referencias

Los administradores de Protect pueden utilizar una muestra de JScript desde la línea de comandos para acceder al producto a través de la API. En el host del servidor de PlateSpin, consulte las muestras en

https://localhost/protectionservices/Documentation/Samples/protect.js

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

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.

F Uso de la herramienta de prueba de red iPerf para optimizar el rendimiento de red para productos de PlateSpin

Antes de ejecutar una réplica, asegúrese de probar la conexión para comprobar si hay algún problema en ella o en el ancho de banda y resolverlo. En esta sección se describe cómo utilizar la herramienta de prueba de red iPerf de código abierto para optimizar el rendimiento de la conexión.

- Sección F.1, “Introducción”, en la página 205
- Sección F.2, “Cálculos”, en la página 206
- Sección F.3, “Configuración”, en la página 207
- Sección F.4, “Metodología”, en la página 208
- Sección F.5, “Expectativas”, en la página 209

F.1 Introducción

A fin de ayudar a los administradores de PlateSpin en su esfuerzo por lograr un mejor rendimiento de la red cuando se usan productos de PlateSpin, se proporciona la herramienta de prueba de red iPerf en el entorno de toma de control de LRD (disco RAM de Linux) de PlateSpin. Como se indica en la documentación de iPerf: “El principal objetivo de iPerf es ayudar a optimizar las conexiones TCP a través de una vía concreta. El problema de optimización fundamental para TCP es el tamaño de la ventana TCP, que controla la cantidad de datos que pueden estar presentes en la red en cualquier momento”.

El propósito de este Readme (Léame) es describir un método básico de optimización y pruebas de red en relación al uso de productos de PlateSpin. En primer lugar, debe calcular un tamaño de ventana TCP óptimo teórico. A continuación, use la herramienta iPerf para validar y ajustar con precisión el tamaño calculado y medir el rendimiento resultante. Este método también resulta útil para determinar el rendimiento real alcanzable para una red determinada.

Tanto la herramienta iPerf como los productos de PlateSpin ya usan el *tamaño de búfer de envío/recepción de TCP* para determinar la eventual elección interna del *tamaño de ventana TCP.* A partir de ahora, estos términos se utilizarán indistintamente.

Nota: hay muchos factores que afectan al rendimiento de la red. Hay disponible mucha información en Internet que puede ayudarle a comprenderlos. Uno de estos recursos es la *calculadora de rendimiento de red* (http://wintelguy.com/wanperf.pl), que permite calcular el rendimiento TCP máximo esperado según las características aplicables de la red del cliente. Se recomienda encarecidamente usar esta calculadora en línea para establecer correctamente las expectativas de rendimiento.

F.2 Cálculos

La optimización del tamaño de ventana TCP se basa en varios factores, incluida la velocidad del enlace de red y la latencia de la red. Para nuestros fines relativos a los productos de PlateSpin, la elección inicial del tamaño de ventana TCP para la optimización se basa en los cálculos estándar (ampliamente disponibles en Internet y en otros lugares) siguientes:

```
TamañoVentanaEnBytes = ((VELOCIDAD_ENLACE (Mb/s)/8) * RETRASO(s)) * 1000 * 1024
```

Por ejemplo, para un enlace de 54 Mb/s con una latencia de 150 ms, el tamaño de ventana inicial adecuado sería:

```
(54/8) * 0,15 * 1000 * 1024 = 1 036 800 bytes
```

Por ejemplo, para un enlace de 1000 Mb/s con una latencia de 10 ms, el tamaño de ventana inicial adecuado sería:

```
(1000/8) * 0,01 * 1000 * 1024 = 1 280 000 bytes
```

Para obtener un valor de latencia de la red, utilice el comando `ping` en el indicador de comandos (Windows) o el terminal (Linux). Aunque el tiempo de ida y vuelta (RTT) de `ping` es probablemente diferente a la latencia real, el valor obtenido es lo suficientemente parecido como para poder usarse en este método.

A continuación, se muestra un resultado de ejemplo de un comando `ping` de Windows, donde se observa una latencia de 164 ms de promedio:

```
ping 10.10.10.232 -n 5

Pinging 10.10.10.232 with 32 bytes of data:
Reply from 10.10.10.232: bytes=32 time=154ms TTL=61
Reply from 10.10.10.232: bytes=32 time=157ms TTL=61
Reply from 10.10.10.232: bytes=32 time=204ms TTL=61
Reply from 10.10.10.232: bytes=32 time=153ms TTL=61
Reply from 10.10.10.232: bytes=32 time=153ms TTL=61

Ping statistics for 10.10.10.232:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 153ms, Maximum = 204ms, Average = 164ms
```

A continuación, se muestra un resultado de ejemplo de un comando `ping` de Linux, donde se observa una latencia de 319 ms de promedio:

```
ping 10.10.10.232 -c 5

PING 10.10.10.232 (10.10.10.232) 56(84) bytes of data.
64 bytes from 10.10.10.232: icmp_seq=1 ttl=62 time=0.328 ms
64 bytes from 10.10.10.232: icmp_seq=2 ttl=62 time=0.280 ms
64 bytes from 10.10.10.232: icmp_seq=3 ttl=62 time=0.322 ms
64 bytes from 10.10.10.232: icmp_seq=4 ttl=62 time=0.349 ms
64 bytes from 10.10.10.232: icmp_seq=5 ttl=62 time=0.316 ms

--- 10.10.10.232 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.280/0.319/0.349/0.022 ms
```

En la práctica, debe utilizar las opciones `-n` o `-c` para especificar un número mayor de paquetes ping con el fin de medir el valor de latencia de forma más precisa.

F.3 Configuración

La herramienta iPerf se ejecuta en modo de servidor o cliente.

La sintaxis básica de uso del modo de servidor de `iperf` es:

```
iperf -s -w <win_size>
```

La sintaxis básica de uso del modo de cliente de `iperf` es:

```
iperf -c <server_ip> -w <win_size>
```

Se pretende medir y optimizar la red entre una carga de trabajo de origen y de destino. En muchos casos, pueden ser el origen y el destino reales en uso. Es posible realizar la prueba con una carga de trabajo diferente para el origen o el destino, siempre que la carga de sustitución tenga las mismas características de red que la original; por ejemplo, la misma NIC, la misma conexión de red, etc.

Nota: asegúrese de que no está probando el rendimiento desde el servidor de PlateSpin al origen o al destino, ya que ese tráfico es mínimo y no representa el que se produce durante una migración o una réplica.

Aunque es posible utilizar una carga de trabajo en directo (Windows o Linux) como servidor de destino o de iperf, en los pasos siguientes se proporciona el entorno más parecido a lo que ocurre en el momento de la migración o réplica, y se recomienda encarecidamente utilizarlos.

Para configurar y ejecutar `iperf` en el destino:

1. Arranque el destino mediante el LRD.
2. En la consola del LRD utilice el terminal auxiliar (se accede con Alt+F2) para hacer lo siguiente:
   - **2a** Configure la red con la opción 5.
   - **2b** Monte el medio de CD con la opción 6.
3. En la consola del LRD, cambie al terminal de depuración (se accede con Alt+F7) para ir a la ubicación de la herramienta iPerf:

   ```
   cd /mnt/cdrom/LRDTools/iperf_2.0.X/linux
   ```

4. Ejecute la herramienta iPerf en modo de servidor. Introduzca

   ```
   ./iperf -s -w <win_size>
   ```

Para configurar y ejecutar `iperf` en el origen:

1. Monte la imagen ISO del LRD mediante software o un medio físico.
2. Abra un indicador de comandos (Windows) o un terminal (Linux) y diríjase a la ubicación de la herramienta iPerf:

   ```
   cd <media>/LRDTools/iperf_2.0.X/
   ```

3. Según el sistema operativo, diríjase al subdirectorio `windows` o `linux`:

   ```
   cd windows
   ```

   ```
   -OR-
   ```

   ```
   cd linux
   ```

4 Ejecute la herramienta iPerf en modo de cliente. Introduzca

```
iperf -c <target_ip> -w <win_size>
```

Nota: puede descargar y usar `iperf3` para los cálculos, lo que resulta útil en ciertos escenarios en los que `iperf2` no es capaz de generar datos de rendimiento útiles. Aunque la sintaxis del comando y el resultado de `iperf3` difieren ligeramente, debe ser bastante sencillo adaptar e interpretar los últimos resultados, si es necesario.

F.4 Metodología

A partir de valor inicial de `win_size` determinado en la sección Cálculos, ejecute varias veces la herramienta iPerf con el valor calculado y con valores ligeramente mayores y menores y registre los resultados. Se recomienda aumentar y disminuir el valor de `win_size` en incrementos del 10 por ciento sobre el valor original.

Con el ejemplo anterior de 1 280 000 bytes, puede aumentar o disminuir el valor de `win_size` en incrementos de unos 100 000 bytes.

Nota: la opción `-w` de `iperf` permite especificar unidades como K (kilobytes) o M (megabytes).

Con el mismo ejemplo, para `-w` puede usar valores de `1,28 M`, `1,38 M`, `1,18 M`, etc., para el campo `win_size` en el paso 4. Por supuesto, se presupone que únicamente se repite el paso de ejecución para cada repetición de la herramienta iPerf.

El resultado de muestra de una repetición del cliente de iperf tiene un aspecto similar al siguiente:

```
iperf.exe -c 10.10.10.232 -w 1.1M

------------------------------------------------------------
Client connecting to 10.10.10.232, TCP port 5001
TCP window size: 1.10 MByte
------------------------------------------------------------
[296] local 10.10.10.224 port 64667 connected with 10.10.10.232 port 5001
[ ID] Interval       Transfer     Bandwidth
[296]  0.0-10.2 sec  11.3 MBytes  9.29 Mbits/sec
```

El resultado de muestra del servidor de destino de referencia tiene un aspecto similar al siguiente:

```
./iperf -s -w .6M

------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 1.20 MByte (WARNING: requested 614 Kbyte)
------------------------------------------------------------
[  4] local 10.10.10.232 port 5001 connected with 10.10.10.224 port 64667
[  4] 0.0-10.2 sec  11.3 MBytes  9.29 Mbits/sec
```

Nota:

- El cliente se desconecta del servidor después de una sola repetición, mientras que el servidor continúa a la escucha hasta que se detiene mediante Ctrl+C.
- El tamaño de la ventana especificado para un servidor Linux es la mitad del valor deseado, ya que Linux duplica de oficio el tamaño del búfer TCP pedido.

Utilice varias repeticiones para determinar el valor óptimo para el tamaño de ventana TCP. No olvide utilizar únicamente la mitad del valor deseado al especificar la opción `-w` en `iperf` en Linux.

Un mayor rendimiento indica que se acerca al tamaño de ventana TCP óptimo. Por último, a medida que se acerque al valor óptimo, utilice repeticiones más largas a fin de simular con mayor exactitud las condiciones de ejecución real. Para conseguir una repetición más larga, utilice la opción `-t <tiempo_en_segundos>` en `iperf`. Esta opción solo debe especificarse en el cliente.

Por ejemplo:

```
iperf.exe -c 10.10.10.232 -w 1.25M -t 60
```

Después de determinar un valor óptimo, configure este valor en el parámetro `FileTransferSendReceiveBufferSize` del servidor de PlateSpin correspondiente en:

https://<*mi_servidor_ps*>/PlatespinConfiguration/

Este valor global se aplica a todas las cargas de trabajo del servidor de PlateSpin, por lo que debe prestarse atención a las cargas de trabajo de grupo y sus respectivas redes de manera razonable a través de los servidores de PlateSpin disponibles.

F.5 Expectativas

Modificar el tamaño de la ventana TCP indirectamente mediante el tamaño del búfer de envío/recepción de TCP puede ser un método muy eficaz de aumentar el rendimiento de la red en algunos casos. A veces, es posible conseguir un rendimiento dos o tres veces superior al original, e incluso más. Sin embargo, es importante recordar que las características de la red pueden cambiar con el tiempo (y a menudo lo hacen) debido a cambios en los patrones de uso, el hardware, el software y otros elementos de infraestructura.

Se recomienda encarecidamente usar este método para calcular el valor óptimo a la misma hora del día y con los mismos patrones de uso de red que se utilizarán durante las tareas de migración o réplica en directo previstas. También se recomienda volver a calcular el valor periódicamente a fin de tener en cuenta las condiciones de red cambiantes.