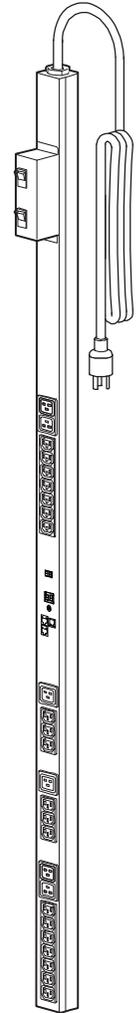


Guía del usuario

Unidad de distribución de alimentación de rack con control



Contenido

Introducción 1

Características del producto	1
Inicio	4
Establecimiento de la configuración de red	5
Recuperación de una pérdida de la contraseña	9

Panel frontal de la PDU de Rack 11

Interfaz de línea de comandos 15

Acerca de la interfaz de línea de comandos	15
Inicio de sesión en la Interfaz de línea de comandos	15
Acerca de la Pantalla principal.	18
Uso de la interfaz de línea de comandos	21
Sintaxis de un comando.	22
Códigos de respuesta de comando	24
Descripción de los comandos de la Tarjeta de administración de red.	25
Descripción de los comandos de dispositivo.	47

Interfaz Web 85

Exploradores Web aceptados	85
Inicio de sesión en la Interfaz Web.	86
Funciones de la interfaz Web.	89
Acerca de la ficha Inicio.	92

Administración del dispositivo 95

Acerca de la ficha Device Manager (Administrador del dispositivo) . . .	96
Ver el estado de la carga y la carga pico	96
Configuración de los umbrales de carga	97
Configuración del Nombre y la Ubicación de la PDU de Rack	98
Configuración del Retardo de inicio en frío	98
Restablecimiento de la Carga pico y los kWh.	99
Configuración y control de los grupos de tomas de corriente	99
Parámetros de toma de corriente para tomas de corriente y grupos de tomas de corriente	110
Programación de acciones de toma de corriente	115
Menú Outlet Manager (Administrador de tomas de corriente)	120

Entorno 121

Configuración de los sensores de temperatura y humedad	122
Configuración de las entradas de contacto seco	124

Registros 125

Uso de los registros de sucesos y de datos.	126
---	-----

Administración: Seguridad 135

Usuarios locales	136
Usuarios remotos	137
Configuración del servidor RADIUS	140
Tiempo de espera por inactividad	142

Administración: Notificación 143

Acciones de sucesos	144
Notificación activa, automática y directa	148



Administración: Funciones de red 157

Configuración de TCP/IP y de la comunicación	158
Ping de respuesta	164
Velocidad de puerto	164
DNS	165
Web	167
Consola	169
SNMP	171
Servidor FTP	176

Administración: Opciones generales 177

Identificación	178
Poner la fecha y la hora	179
Uso de un archivo .ini	181
Registro de sucesos y Unidades de temperatura	182
Restablecimiento de la PDU de rack	183
Configuración de los vínculos	184
Acerca de la Rack PDU	184

Cómo exportar los valores de configuración 185

Recuperación y exportación del archivo .ini	185
El suceso de carga y los mensajes de error	189

Transferencias de archivos 191

Cómo actualizar el firmware	191
Métodos de transferencia de archivos de firmware	193
Verificación de las actualizaciones	196

Resolución de problemas 198

PDU de Rack Problemas de acceso	198
---	-----

Apéndice A: Lista de comandos aceptados 200



Apéndice B: Manual de seguridad 205

Contenido y finalidad de este Apéndice	205
Funciones de seguridad.	206
Autenticación.	210
Cifrado.	212
Creación e instalación de certificados digitales	215
Cortafuegos	220
Uso del Rack PDU Security Wizard (Asistente para la seguridad de la PDU de rack)	221
Creación de un certificado raíz y de certificados de servidor.	224
Creación de un certificado de servidor y una solicitud de firma.	230
Creación de una clave de host SSH	233
Acceso a la interfaz de línea de comandos y seguridad.	236
Telnet y Secure Shell (SSH)	237
Acceso a la interfaz Web y seguridad: HTTP y HTTPS (con SSL).	238
Funciones y servidores RADIUS aceptados.	242
Configuración de la PDU de rack	243
Configuración del servidor RADIUS.	245

Índice 250

Introducción

Características del producto

La Dell® Managed Rack Power Distribution Unit (PDU) (Unidad de distribución de alimentación de rack con control) es un dispositivo de distribución de la alimentación autónomo y administrable por red. La PDU de Rack proporciona monitorización remota en tiempo real de las cargas conectadas. Alarmas definidas por el usuario advierten de las posibles sobrecargas de los circuitos. La PDU de Rack proporciona pleno control sobre las tomas de corriente mediante comandos remotos y parámetros de interfaz de usuario.

Se puede administrar una PDU de rack por medio de su interfaz Web, su interfaz de línea de comandos (CLI) o Simple Network Management Protocol (SNMP):

- Acceda a la interfaz Web utilizando Hypertext Transfer Protocol o utilizando HTTP seguro (HTTPS) con Secure Sockets Layer (SSL). Consulte [Inicio de sesión en la Interfaz Web](#).
- Acceda a la interfaz de línea de comandos a través de una conexión serie, Telnet o Secure Shell (SSH). Consulte [Acerca de la interfaz de línea de comandos](#).
- Utilice un explorador SNMP y la Dell Management Information Base (MIB) para administrar su PDU de rack.

Las PDU de rack cuentan con las siguientes características adicionales:

- Monitorización de la carga pico, y de la potencia y energía de todas las cargas conectadas.
- Monitorización del voltaje, la intensidad de corriente y la potencia por fases.
- Monitorización de la potencia para cada toma de corriente.
- Umbrales de alarma configurables que proporcionan alarmas de red y visuales que ayudan a evitar la sobrecarga de los circuitos.

- Cuatro niveles de cuentas de acceso de usuario: Administrador, Usuario de dispositivo, Usuario de sólo lectura y Usuario de tomas de corriente.
- Control independiente de las tomas de corriente.
- Retardos de la alimentación configurables.
- Hasta veinticuatro cuentas de usuario de tomas de corriente independientes.
- Registro de sucesos y datos. El registro de sucesos es accesible por Telnet, Secure CoPy (SCP), File Transfer Protocol (FTP), conexión serie o explorador Web (utilizando acceso HTTPS con SSL o utilizando acceso HTTP). El registro de datos es accesible por explorador Web, SCP o FTP.
- Notificaciones por correo electrónico de la PDU de rack y los sucesos del sistema.
- Capturas SNMP, mensajes Syslog y notificaciones por correo electrónico basados en el nivel de gravedad o categoría de la PDU de rack y los sucesos del sistema.
- Protocolos de seguridad para la autenticación y el cifrado.



La PDU de rack no ofrece protección contra la sobretensión momentánea. Para asegurarse de que el dispositivo esté protegido de los cortes del suministro eléctrico y de las sobretensiones momentáneas, conecte la PDU de rack a un sistema de alimentación ininterrumpible (SAI).

Prioridades de acceso para iniciar una sesión

Sólo un usuario puede iniciar una sesión en la PDU de rack cada vez. La prioridad de acceso, empezando por la prioridad más alta, será del modo siguiente:

- Acceso local a la interfaz de línea de comandos desde un ordenador con una conexión serie directa a la PDU de rack
- Acceso Telnet o Secure Shell (SSH) a la interfaz de línea de comandos desde un ordenador remoto
- Acceso Web



Véase [SNMP](#) para obtener información sobre cómo se controla el acceso SNMP a la PDU de rack.

Tipos de cuentas de usuario

La PDU de rack tiene cuatro niveles de acceso (Administrador, Usuario de dispositivo, Usuario de sólo lectura y Usuario de tomas de corriente), que están protegidos por requisitos de nombre de usuario y contraseña.

- Un Administrador puede utilizar todos los menús de la interfaz Web y todos los comandos de la interfaz de línea de comandos. Tanto el nombre de usuario como la contraseña predeterminados son **admin**.
- Un Usuario de dispositivo puede acceder sólo a lo siguiente:
 - En la interfaz Web, los menús de la ficha **Administrador del dispositivo**, la ficha **Entorno**, y los registros de sucesos y de datos, accesibles bajo los encabezamientos **Sucesos** y **Datos** en el menú de navegación izquierdo de la ficha **Registros**. Los registros de sucesos y datos no muestran ningún botón para borrar el registro.
 - En la interfaz de línea de comandos, las funciones y opciones equivalentes. Tanto el nombre de usuario como la contraseña predeterminados son **device**.
- Un Usuario de sólo lectura tiene las siguientes restricciones de acceso:
 - Acceso a través de la interfaz Web sólo.
 - Acceso a las mismas fichas y menús que un Usuario de dispositivo, pero sin la capacidad para cambiar configuraciones, controlar dispositivos, eliminar datos o utilizar las opciones de transferencia de archivos. Los enlaces a las opciones de configuración están visibles pero desactivados. Los registros de sucesos y datos no muestran ningún botón para borrar el registro.Tanto el nombre de usuario como la contraseña predeterminados son **readonly**.



Para establecer los valores de **Nombre de usuario** y **Contraseña** para los tres tipos de cuenta, véase [Configuración del acceso de usuario](#).

- Un Usuario de tomas de corriente tiene las siguientes restricciones de acceso:
 - Acceso a través de la interfaz Web y la interfaz de línea de comandos.
 - Acceso a los mismos menús que un Usuario de dispositivo, pero con una capacidad limitada para cambiar las configuraciones, controlar los dispositivos, eliminar datos o utilizar las opciones de transferencia de archivos. Los enlaces a las opciones de configuración están visibles pero están desactivados. El Usuario de tomas de corriente tiene acceso a la opción de menú **Outlet Control** (Control de tomas de corriente) que le permite controlar las tomas de corriente asignadas por el Administrador. Los usuarios de tomas de corriente no pueden borrar los registros de sucesos ni de datos.

El nombre de usuario y la contraseña se definen por el Administrador durante el proceso de adición de un nuevo Usuario de tomas de corriente.

Inicio

Para comenzar a utilizar la PDU de rack:

1. Instale la PDU de rack utilizando las *Instrucciones de instalación de la Rack Power Distribution Unit* que vienen con la PDU de rack.
2. Aplique alimentación y conéctela a su red. Siga las indicaciones de las *Instrucciones de instalación de la Rack Power Distribution Unit*.
3. Establezca la configuración de red. (consulte la sección [Establecimiento de la configuración de red](#)).
4. Comience a usar la PDU de rack por medio de una de las siguientes opciones:
 - [Interfaz Web](#)
 - [Interfaz de línea de comandos](#)
 - [Panel frontal de la PDU de Rack](#)

Establecimiento de la configuración de red

Debe configurar los siguientes parámetros TCP/IP para que la PDU de rack pueda funcionar en una red:

- Dirección IP de la PDU de rack
- Máscara de subred
- Puerta de enlace predeterminada



Si no se encuentra disponible una puerta de enlace predeterminada, utilice la dirección IP de un ordenador que esté ubicado en la misma subred que la PDU de rack y que esté normalmente en estado operativo. La PDU de rack utiliza la puerta de enlace predeterminada para efectuar una prueba de la red cuando hay muy poco tráfico.



No utilice la dirección de bucle de retroceso (127.0.0.1) como dirección de puerta de enlace predeterminada de la PDU de rack, ya que se desactiva la tarjeta y es necesario iniciar una sesión de comunicación serie local para restablecer los parámetros TCP/IP a sus valores predeterminados.

Métodos de configuración de TCP/IP

Utilice uno de los siguientes métodos para definir los parámetros de TCP/IP que necesita la PDU de rack:

- [Configuración de BOOTP y DHCP](#)
- [Interfaz de línea de comandos](#)

Configuración de BOOTP y DHCP

El valor de configuración de TCP/IP predeterminado **DHCP** da por sentado que hay disponible un servidor DHCP correctamente configurado que proporciona los valores de TCP/IP a las PDU de rack. También se puede configurar el parámetro para BOOTP.

Un archivo de configuración de usuario (INI) puede funcionar como archivo de inicio BOOTP o DHCP. Para obtener más información, consulte la sección [Uso de un archivo .ini](#).

BOOTP. Para que la PDU de rack pueda usar un servidor BOOTP para configurar sus parámetros TCP/IP, debe encontrar un servidor BOOTP configurado correctamente y que cumpla con RFC951.

En el archivo BOOTPTAB del servidor BOOTP, introduzca la dirección MAC, la dirección IP, la máscara de subred y la puerta de enlace predeterminada de la PDU de rack, y, opcionalmente, un nombre de archivo de inicio. Encontrará la dirección MAC en la parte inferior de la PDU de rack o en la hoja de Garantía de calidad que se incluye en el paquete.

Cuando se reinicia la PDU de rack, el servidor BOOTP le proporciona los valores de TCP/IP.

- Si se ha especificado un nombre de archivo de inicio, la PDU de rack intenta transferir ese archivo del servidor BOOTP mediante TFTP o FTP. La PDU de rack asume todos los valores especificados en el archivo de inicio.
- Si no se ha especificado un nombre de archivo de inicio, se pueden configurar de manera remota los demás parámetros de la PDU de rack por medio de la [Interfaz Web](#) o la [Interfaz de línea de comandos](#).



Para crear un archivo de inicio, consulte la documentación del servidor BOOTP.

DHCP. Se puede utilizar un servidor DHCP compatible con RFC2131/RFC2132 para configurar los parámetros de TCP/IP para la PDU de rack.



Esta sección resume la comunicación de la PDU de rack con un servidor DHCP. Para obtener más información sobre cómo un servidor DHCP puede configurar los parámetros de red de una PDU de rack, véase [Opciones de respuesta de DHCP](#).

1. La PDU de rack envía una solicitud de DHCP con los siguientes elementos de identificación:
 - Un identificador de clase de proveedor
 - Un identificador de cliente (de manera predeterminada, la dirección MAC de la PDU de rack)
 - Un identificador de clase de usuario (de manera predeterminada, la identificación del firmware de aplicación instalado en la PDU de rack)
2. Un servidor DHCP configurado correctamente responde con una oferta de DHCP que incluye todos los valores que necesita la PDU de rack para la comunicación en red. En la oferta de DHCP también se incluye la opción “Vendor Specific Information” (información específica del proveedor) (opción 43 de DHCP). La PDU de rack se puede configurar para que ignore las ofertas de DHCP que no encapsulen la cookie del proveedor en la opción 43 de DHCP utilizando el siguiente formato hexadecimal. (La PDU de rack no requiere esta cookie de manera predeterminada.)

```
Option 43 = 01 04 31 41 50 43
```

Donde:

- El primer byte (01) es el código.
- El segundo byte (04) es la longitud.
- Los bytes restantes (31 41 50 43) son la cookie del proveedor



Consulte la documentación del servidor DHCP para obtener información sobre cómo añadir el código en la opción “Vendor Specific Information” (información específica del proveedor).



Nota: Seleccionando la casilla de verificación **Requerir cookie específica del distribuidor para aceptar la dirección de DHCP** en la interfaz Web, se puede hacer necesario que el servidor DHCP proporcione una cookie de distribuidor, que suministra información a la PDU de rack (**Administración > Red>TCP/IP>configuración de ipv4**).

Interfaz de línea de comandos

1. Inicie una sesión en la interfaz de línea de comandos. Consulte [Inicio de sesión en la Interfaz de línea de comandos](#).
2. Póngase en contacto con el administrador de la red para obtener la dirección IP, la máscara de subred y la puerta de enlace predeterminada para la PDU de rack.
3. Utilice estos tres comandos para configurar los parámetros de red (el texto en cursiva indica una variable).

a. `tcpip -i suDirecciónIP`

b. `tcpip -s suMáscaradeSubred`

c. `tcpip -g suPuertadeenlacePredeterminada`

Para cada variable, escriba un valor numérico con el formato `xxx.xxx.xxx.xxx`.

Por ejemplo, para definir la dirección IP del sistema como 156.205.14.141, escriba el comando siguiente y pulse INTRO:

```
tcpip -i 156.205.14.141
```

4. Escriba `exit` (salir). La PDU de rack se reinicia para aplicar los cambios.

Recuperación de una pérdida de la contraseña

Puede utilizar un ordenador local (un ordenador que esté conectado a la PDU de rack u otro dispositivo a través del puerto serie) para acceder a la interfaz de línea de comandos.

1. Seleccione un puerto serie del ordenador local y desactive todos los servicios que utilicen ese puerto.
2. Conecte el cable serie suministrado en el puerto seleccionado del ordenador y en el puerto serie de la PDU de rack.
3. Ejecute un programa emulador de terminal (como, por ejemplo, HyperTerminal[®]) y configure el puerto seleccionado con los siguientes valores: 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada y sin control de flujo.
4. Pulse INTRO, varias veces si es necesario, para que aparezca el indicador **User Name** (Nombre de usuario). Si no aparece el indicador **User Name**, compruebe lo siguiente:
 - No hay ninguna otra aplicación que esté utilizando el puerto serie.
 - Los valores de configuración de terminal son correctos tal y como se especifica en el paso 3.
 - Se ha usado el cable correcto, tal y como se especifica en el paso 2.
5. Pulse el botón **Reset** (Restablecer). El indicador LED de estado parpadeará de forma alternativa entre naranja y verde. Vuelva a pulsar el botón **Reset** inmediatamente mientras el LED esté parpadeando para restablecer el nombre de usuario y la contraseña a sus valores predeterminados de forma temporal.
6. Pulse INTRO, varias veces si es necesario, para volver a mostrar el indicador **User Name** y, a continuación, utilice el valor **dell** como nombre de usuario y contraseña (si tarda más de 30 segundos en iniciar una sesión después de que vuelva a aparecer el indicador **User Name**, deberá repetir el paso 5 y volver a iniciar sesión).



7. En la interfaz de línea de comandos, utilice los siguientes comandos para cambiar los valores de **User Name** (Nombre de usuario) y **Password** (Contraseña), que ahora son **dell**:

```
user -an su nombre de administrador
```

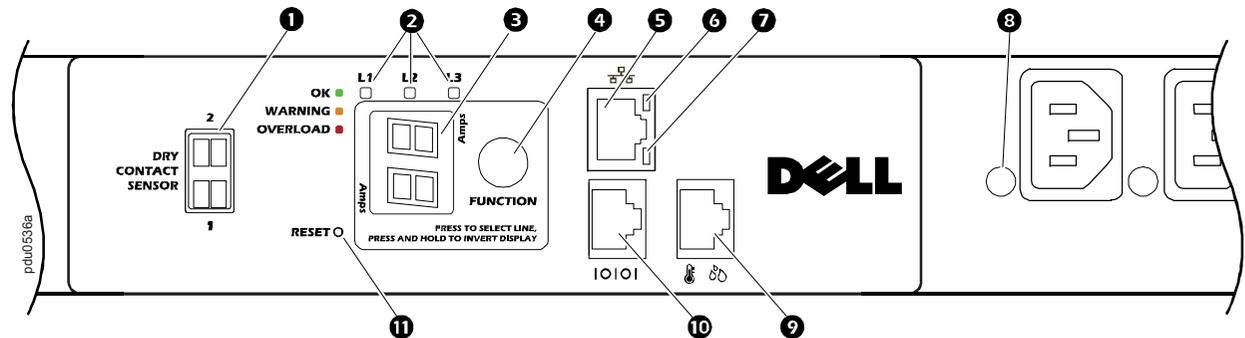
```
user -ap su contraseña de administrador
```

Por ejemplo, para cambiar el nombre de usuario de Administrador a **Don Adams**, escriba:

```
user -an Don Adams
```

8. Escriba **quit** o **exit** para cerrar la sesión, vuelva a conectar todos los cables serie que haya desconectado y reinicie los servicios que haya desactivado.

Panel frontal de la PDU de Rack



Ítem	Función
1 Entradas de contacto seco	Conector para dos dispositivos de contacto seco.
2 LEDs de fase Nota: en las PDU de rack monofásicas, sólo hay un LED.	<p>Cuando no hay ninguna alarma, la pantalla de LEDs muestra una corriente de fase, y un LED de fase en verde indica para qué fase. El sistema pasa cíclicamente por cada fase automáticamente, mostrando la corriente de fase durante tres segundos.</p> <p>Si hay una alarma para una fase, el LED de fase correspondiente se enciende y permanece encendido mientras se da la condición de alarma. El LED se ilumina en naranja para una alarma de Advertencia (Warning) y en rojo para una alarma Crítica. Si hay una alarma para más de una fase, el sistema automáticamente pasa cíclicamente por cada fase con una alarma, iluminando los LED de fase durante tres segundos.</p>

Ítem		Función
3	Pantalla de LEDs	Muestra la corriente de fase para el LED de fase iluminado en ese momento.
4	Botón Function (Función)	<ul style="list-style-type: none"> • Para mostrar manualmente la corriente de cada fase, pulse repetidamente el botón. La corriente se muestra durante 30 segundos o hasta que se vuelve a pulsar el botón. (Esta funcionalidad no está disponible en las PDU de rack monofásicas.) • Para mostrar la dirección IP, pulse el botón y manténgalo pulsado durante cinco segundos hasta que aparezca la IP; luego suelte. En la pantalla de LEDs, la dirección aparece de dos en dos dígitos y luego se repite el ciclo. • Para invertir la pantalla, pulse el botón y manténgalo pulsado durante diez segundos hasta que aparezca la configuración AA. Continúe sujetando el botón hasta que AA esté orientado de la forma deseada y luego suelte el botón.
5	Conector 10/100 Base-T	Puerto para conectar la PDU de rack a la red.
6	LED 10/100	Consulte LED 10/100 .
7	LED de estado de la red	Consulte LED de estado de la red .
8	LED de estado de la toma de corriente	Se ilumina en verde cuando la toma de corriente tiene electricidad. (cada toma de corriente tiene un LED de toma de corriente.)
9	Puerto de sensor de temp/ humedad	Puerto para conectar un sensor de temperatura de PDU de rack (G853N) o un sensor de temperatura/ humedad de PDU de rack (H621N).
10	Puerto serie RJ-45	Puerto para conectar la PDU de rack a un programa emulador de terminal para un acceso local a la interfaz de línea de comandos. Utilice el cable serie suministrado.
11	Botón Reset (Restablecer)	Para reiniciar la interfaz de la PDU de rack sin afectar a las salidas, pulse y suelte el botón Reset.

LEDde estado de la red

Estado	Descripción
Apagado	Existe una de las siguientes situaciones: <ul style="list-style-type: none">• La PDU de rack no recibe alimentación de entrada.• La PDU de rack no funciona correctamente. Es posible que tenga que ser reparada o sustituida.
Verde continuo	La PDU de rack tiene una configuración de TCP/IP válida.
Verde intermitente	La PDU de rack no tiene una configuración de TCP/IP válida.
Naranja continuo	Se ha detectado un fallo de hardware en la PDU de rack.
Naranja intermitente	La PDU de rack está efectuando solicitudes BOOTP.
Naranja y verde intermitentes (alternativamente)	Si el LED emite destellos lentamente, la PDU de rack está efectuando solicitudes DHCP. Si el LED emite destellos rápidamente, la PDU de rack está iniciándose.
<ol style="list-style-type: none">1. Si no utiliza un servidor BOOTP o DHCP, véase Establecimiento de la configuración de red para configurar los parámetros TCP/IP de la PDU de rack.2. Para utilizar un servidor DHCP, véase Configuración de TCP/IP y de la comunicación.	

LED 10/100

Estado	Descripción
Apagado	Existe una o más de las siguientes situaciones: <ul style="list-style-type: none">• La PDU de rack no recibe alimentación de entrada.• El cable que conecta la PDU de rack a la red está desconectado o es defectuoso.• El dispositivo que conecta la PDU de rack a la red está apagado.• La PDU de rack misma no funciona correctamente. Es posible que tenga que ser reparada o sustituida.
Verde constante	La PDU de rack está conectada a una red que está funcionando a 10 Megabits por segundo (Mbps).
Naranja constante	La PDU de rack está conectada a una red que está funcionando a 100 Mbps.
Verde intermitente	La PDU de rack está recibiendo o transmitiendo paquetes de datos a 10 Mbps.
Naranja intermitente	La PDU de rack está recibiendo o transmitiendo paquetes de datos a 100 Mbps.

Interfaz de línea de comandos

Acerca de la interfaz de línea de comandos

Se puede usar la interfaz de línea de comandos para administrar y ver el estado de la PDU de rack. Además, la interfaz de línea de comandos le permite crear scripts para un funcionamiento automatizado. Un administrador tiene acceso completo a la interfaz de línea de comandos, un usuario de dispositivo y un usuario de tomas de corriente tienen un acceso limitado y un usuario de sólo lectura tiene un acceso completamente restringido. (para obtener información adicional, consulte la sección [Tipos de cuentas de usuario](#).)

Se pueden configurar todos los parámetros de una PDU de rack (incluidos aquellos para los cuales no hay comandos ILC específicos) utilizando la ILC (interfaz de línea de comandos) para transferir un archivo INI a la PDU de rack. La ILC utiliza XMODEM para realizar la transferencia. Sin embargo, no se puede leer el archivo INI actual a través de XMODEM.

Inicio de sesión en la Interfaz de línea de comandos

Para acceder a la interfaz de línea de comandos, se puede utilizar una conexión local (serie) o una conexión remota (Telnet o SSH) con un ordenador en la misma red que la PDU de rack.

Acceso remoto a la interfaz de línea de comandos

Se puede acceder a la interfaz de línea de comandos a través de Telnet o SSH. De forma predeterminada, Telnet está activado. La activación de SSH desactiva Telnet.

Para activar o desactivar estos métodos de acceso, utilice la interfaz Web. En la ficha **Administración**, seleccione **Red** en la barra de menú superior y a continuación la opción **acceso** bajo **Consola** en el menú de navegación izquierdo.

Telnet para un acceso básico. Telnet proporciona la seguridad básica de la autenticación por nombre de usuario y contraseña, pero no la elevada seguridad que ofrece el cifrado.

Para utilizar Telnet para acceder a la interfaz de línea de comandos:

1. Desde un ordenador en la misma red que la PDU de rack, en un indicador de comando, escriba `telnet` y la dirección IP de la PDU de rack (por ejemplo, `telnet 139.225.6.133`, cuando la PDU de rack utiliza el puerto Telnet predeterminado 23), y pulse INTRO.
Si la PDU de rack utiliza un número de puerto no predeterminado (del 5000 al 32768), debe incluir dos puntos o un espacio, dependiendo de su cliente Telnet, entre la dirección IP (o nombre DNS) y el número de puerto. (Estos son comandos para uso general: algunos clientes no le permiten especificar el puerto como argumento y otros pueden requerir comandos adicionales.)
2. Introduzca el nombre de usuario y la contraseña (de manera predeterminada, **admin** y **admin** para un Administrador, o **device** y **device** para un Usuario de dispositivo).



Si no recuerda su nombre de usuario o contraseña, consulte [Recuperación de una pérdida de la contraseña](#).

SSH para un acceso de alta seguridad. Si utiliza la alta seguridad de SSL para la interfaz Web, use SSH para acceder a la interfaz de línea de comandos. SSH cifra los nombres de usuario, las contraseñas y los datos transmitidos. La interfaz, las cuentas de usuario y los derechos de acceso de usuario son los mismos, tanto si accede a la interfaz de línea de comandos mediante SSH como si lo hace a través de Telnet; sin embargo, para utilizar SSH, primero debe configurar SSH y tener instalado un programa cliente SSH en su ordenador.

Acceso local a la interfaz de línea de comandos

Para acceder localmente a la interfaz de línea de comandos, utilice un ordenador que esté conectado a la PDU de rack a través del puerto serie:

1. Seleccione un puerto serie del ordenador y desactive todos los servicios que utilicen ese puerto.
2. Conecte el cable serie suministrado del puerto serie seleccionado en el ordenador al puerto serie de la PDU de rack.
3. Ejecute un programa emulador de terminal (por ejemplo, HyperTerminal) y configure el puerto seleccionado con estos valores: 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada y sin control de flujo.
4. Pulse INTRO, y en los indicadores, introduzca su nombre de usuario y contraseña.

Acerca de la Pantalla principal

A continuación se da un ejemplo de la pantalla principal, que se muestra cuando se inicia una sesión en la interfaz de línea de comandos de una PDU de rack:

```
Dell Corporation                               Network Management Card AOS  vx.x.x
(c)Copyright 2009 All Rights Reserved  RPDUD                               vx.x.x
-----
Name      : Test Lab                               Date : 10/30/2009
Contact   : Don Adams                             Time : 5:58:30
Location  : Building 3                           User  : Administrator
Up Time   : 0 Days, 21 Hours, 21 Minutes         Stat  : P+ N+ A+

cli>
```

Campos de información de la pantalla principal:

- Dos campos identifican la versión del sistema operativo (AOS) y del firmware de aplicación (APP). El nombre del firmware de aplicación identifica el tipo de dispositivo que está conectado a la red. En el ejemplo anterior, se muestra el firmware de aplicación de la PDU de rack.

```
Network Management Card AOS vx.x.x  
RPDUD vx.x.x
```

- Tres campos identifican el nombre del sistema, la persona de contacto y la ubicación de la PDU de rack. (En la consola de control, utilice el menú **System** (Sistema) para establecer esos valores.)

```
Name (Nombre): Laboratorio de pruebas  
Contact (Contacto): Don Adams  
Location (Ubicación): Edificio 3
```

- El campo **Up time** (Tiempo de actividad) informa del tiempo que ha estado funcionando la PDU de rack desde la última vez que se encendió o reinició.

```
Up Time: 0 Days, 21 Hours, 21 Minutes
```

- Dos campos informan del momento en que se inició la sesión mostrando los valores de fecha (Date) y hora (Time).

```
Date (Fecha): 10/30/2009  
Time (Hora): 5:58:30
```

- El campo **User** (Usuario) informa de si se ha iniciado la sesión mediante la cuenta de **Administrator** (Administrador) o de **Device user** (Usuario de dispositivo). (La cuenta de **Usuario de sólo lectura** no puede acceder a la interfaz de línea de comandos.)

```
User (Usuario): Administrator (Administrador)
```

- El campo **Stat** (Estado) informa sobre el estado de la PDU de rack.

Stat : P+ N+ A+

P+	El sistema operativo Dell funciona correctamente.
-----------	---

IPv4 sólo	IPv6 sólo	IPv4 e IPv6*	Descripción
N+	N+	N4+ N6+	La red funciona correctamente.
N?	N6?	N4? N6?	Está en curso un ciclo de solicitud BOOTP.
N-	N6-	N4- N6-	La PDU de rack no ha podido conectarse a la red.
N!	N6!	N4! N6!	Otro dispositivo está utilizando la dirección IP de la PDU de rack.
* Los valores de N4 y N6 pueden ser diferentes uno de otro: por ejemplo, se puede tener N4- N6+.			

A+	La aplicación funciona correctamente.
A-	La aplicación tiene una suma de comprobación errónea.
A?	La aplicación se está inicializando.
A!	La aplicación no es compatible con el AOS.



Si no se muestra P+, póngase en contacto con [Personal de asistencia de Dell](#).

Uso de la interfaz de línea de comandos

En la interfaz de línea de comandos, se usan comandos para configurar la PDU de rack. Para utilizar un comando, escriba el comando y pulse INTRO. Los comandos y los argumentos son válidos en minúsculas, mayúsculas y en una combinación de ambas. Las opciones distinguen entre mayúsculas y minúsculas.

Mientras se usa la interfaz de línea de comandos, también se puede hacer lo siguiente:

- Escriba `?` y pulse INTRO para ver una lista de los comandos disponibles, que se basa en el tipo de cuenta.
- Para obtener información acerca de la finalidad y sintaxis de un comando en concreto, escriba el comando, un espacio, y `?` o la palabra `help`. Por ejemplo, para ver las opciones de configuración de RADIUS, escriba:

```
radius ?  
o  
radius help
```

- Pulse la tecla de flecha ARRIBA para ver el comando que se ha introducido más recientemente en la sesión. Utilice las teclas de flecha ARRIBA y ABAJO para desplazarse por una lista de hasta diez comandos anteriores.
- Escriba al menos una letra de un comando y pulse la tecla TAB para desplazarse por una lista de comandos válidos que coinciden con el texto que ha escrito en la línea de comandos.
- Escriba `exit` o `quit` para cerrar la conexión con la interfaz de línea de comandos.

Sintaxis de un comando

Ítem	Descripción
-	Las opciones van precedidas de un guión.
< >	Las definiciones de las opciones se encierran entre paréntesis angulares. Por ejemplo: -dp <contraseña de dispositivo>
[]	Si un comando acepta múltiples opciones o una opción acepta argumentos que se excluyen mutuamente, los valores pueden encerrarse entre corchetes.
	Una línea vertical entre elementos encerrados entre corchetes o paréntesis angulares indica que los elementos son mutuamente excluyentes. Debe utilizar uno de los elementos.

Ejemplo de un comando que admite múltiples opciones:

```
user [-an <nombre de administrador>] [-ap <contraseña de administrador>]
```

En este ejemplo, el comando `user` acepta la opción `-an`, que define el nombre de usuario del Administrador, y la opción `-ap`, que define la contraseña del Administrador. Para cambiar el nombre de usuario y la contraseña del Administrador a XYZ:

1. Escriba el comando `user`, una opción, y el argumento `XYZ`:

```
user -ap XYZ
```

2. Una vez ejecutado con éxito el primer comando, escriba el comando `user`, la segunda opción, y el argumento `XYZ`:

```
user -an XYZ
```

Ejemplo de un comando que acepta argumentos mutuamente excluyentes para una opción:

```
alarmcount -p [all | warning | critical]
```

En este ejemplo, la opción -p acepta sólo tres argumentos: all, warning, or critical (todas, de advertencia, o críticas). Por ejemplo, para ver el número de alarmas críticas activas, escriba:

```
alarmcount -p critical
```

El comando fallará si se escribe un argumento que no está especificado.

Códigos de respuesta de comando

Los códigos de respuesta de comando permiten que las operaciones en script detecten las condiciones de error de manera fiable sin tener que comprobar si coincide el texto de los mensajes de error:

La ILC informa de todas las operaciones de comando con el siguiente formato:

E [0-9] [0-9] [0-9] : Mensaje de error

Código	Mensaje	Código	Mensaje
E000	Success (Éxito)	E105	Command Prefill (Prerellenado de comando)
E001	Successfully Issued (Emitido con éxito)	E106	Data Not Available (Datos no disponibles)
E002	Reboot required for change to take effect (Se requiere reinicio para que el cambio surta efecto)	E107	Serial communication with the UPS has been lost (Se ha perdido la comunicación serie con el SAI)
E100	Command failed (El comando ha fallado)		
E101	Command not found (Comando no encontrado)		
E102	Parameter error (Error de parámetro)		
E103	Command line error (Error de línea de comando)		
E104	User level denial (Denegación a nivel de usuario)		

Descripción de los comandos de la Tarjeta de administración de red

?

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver una lista de todos los comandos de la ILC disponibles para su tipo de cuenta. Para ver el texto de ayuda de un comando en concreto, escriba el comando seguido de un signo de interrogación.

Ejemplo: Para ver una lista de las opciones que acepta el comando `alarmcount`, escriba:

```
alarmcount ?
```

about

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver información del hardware y el firmware. Esta información es útil en la resolución de problemas y le permite determinar si se necesita una actualización del firmware.

alarmcount

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción:

Opción	Argumentos	Descripción
-p	all (todas)	Permite ver el número de alarmas activas comunicadas por la PDU de rack. La información sobre las alarmas se proporciona en el registro de sucesos.
	warning (advertencia)	Permite ver el número de alarmas de advertencia activas.
	critical (críticas)	Permite ver el número de alarmas críticas activas.

Ejemplo: Para ver todas las alarmas de advertencia activas, escriba:

```
alarmcount -p warning
```

boot

Acceso: Administrador sólo

Descripción: Permite definir cómo obtendrá la PDU de rack sus valores de configuración de red, incluidos la dirección IP, la máscara de subred y la puerta de enlace predeterminada. Y a continuación configurar los parámetros de servidor BOOTP o DHCP.

Opción	Argumento	Descripción
-b <boot mode (modo de inicio)>	dhcp bootp manual	Define cómo se configurarán los parámetros TCP/IP cuando la PDU de rack se encienda, se restablezca o se reinicie. Véase Configuración de TCP/IP y de la comunicación para obtener información sobre cada uno de los valores de Modo de inicio.
-c	enable disable (activar o desactivar)	Sólo con los modos de inicio <code>dhcp</code> y <code>dhcpBootp</code> . Activa o desactiva el requisito de que el servidor DHCP proporcione la cookie de proveedor.

Generalmente no es necesario cambiar los valores predeterminados de estos tres parámetros:

- v <clase de proveedor>: DELL
- i <id de cliente>: La dirección MAC de la PDU de rack, que la identifica de manera única en la red
- u <clase de usuario>: El nombre del módulo de firmware de aplicación

Ejemplo: Para utilizar un servidor DHCP para obtener los valores de configuración de red:

1. Escriba `boot -b dhcp`
2. Active el requisito de que el servidor DHCP proporcione la cookie de proveedor:
`boot -c enable`

cd

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite navegar a una carpeta de la estructura de directorios de la PDU de rack.

Ejemplo 1: Para cambiar a la carpeta `ssh` y confirmar que se ha cargado un certificado de seguridad SSH en la PDU de rack:

1. Escriba `cd ssh` y pulse INTRO.
2. Escriba `dir` y pulse INTRO para listar los archivos almacenados en la carpeta SSH.

Ejemplo 2: Para volver a la carpeta principal del directorio, escriba:

```
cd ..
```

console

Acceso: Administrador sólo

Descripción: Define si los usuarios pueden acceder a la interfaz de línea de comandos utilizando Telnet, que está activado de manera predeterminada, o Secure Shell (SSH), que proporciona protección transmitiendo los nombres de usuario, las contraseñas y los datos de forma cifrada. Se puede cambiar el valor del puerto Telnet o SSH para obtener seguridad adicional. Otra posibilidad es desactivar el acceso de red a la interfaz de línea de comandos.

Opción	Argumento	Descripción
-S	disable telnet ssh	Permite configurar el acceso a la interfaz de línea de comandos o utilizar el comando disable (desactivar) para impedir el acceso. La activación de SSH activa SCP y desactiva Telnet.
-pt	<nº. de puerto telnet>	Permite definir el puerto Telnet utilizado para comunicarse con la PDU de rack (el 23 de manera predeterminada).
-ps	<nº. de puerto SSH>	Permite definir el puerto SSH utilizado para comunicarse con la PDU de rack (el 22 de manera predeterminada).
-b	2400 9600 19200 38400	Permite configurar la velocidad de la conexión del puerto serie (9600 bps de manera predeterminada).

Ejemplo 1: Para activar el acceso SSH a la interfaz de línea de comandos, escriba:
`console -S ssh`

Ejemplo 2: Para cambiar el puerto Telnet a 5000, escriba:
`console -pt 5000`

date

Acceso: Administrador sólo

Definición: Permite configurar la fecha utilizada por la PDU de rack.



Para configurar un servidor NTP para definir la fecha y hora para la PDU de rack, véase [Poner la fecha y la hora](#).

Opción	Argumento	Descripción
-d	<"cadena de caracteres de fecha">	Permite configurar la fecha actual. Utilice el formato de fecha especificado por el comando <code>date -f</code> .
-t	<00:00:00>	Permite configurar la hora actual, en horas, minutos y segundos. Utilice el formato de reloj de 24 horas.
-f	mm/dd/aa dd.mm.aaaa mmm-dd-aa dd-mmm-aa aaaa-mm-dd	Permite seleccionar el formato numérico en el que se muestran todas las fechas en esta interfaz de usuario. Cada letra m (mes), d (día) y a (año) representa un dígito. Los días y los meses de un sólo dígito se muestran con un cero inicial.
-z	<Diferencia de huso horario>	Permite establecer la diferencia con la hora GMT para especificar su huso horario. Esto le permite sincronizarse con otras personas de diferentes husos horarios.

Ejemplo 1: Para mostrar la fecha utilizando el formato aaaa-mm-dd, escriba:

```
date -f aaaa-mm-dd
```

Ejemplo 2: Para definir la fecha como 30 de octubre de 2009, utilizando el formato configurado en el ejemplo anterior, escriba:

```
date -d "2009-10-30"
```

Ejemplo 3: Para definir la hora como 5:21:03 de la tarde, escriba:

```
date -t 17:21:03
```

delete

Acceso: Administrador sólo

Descripción: Permite borrar un archivo del sistema de archivos.

Argumento	Descripción
<nombre de archivo>	Escriba el nombre del archivo para borrar.

dir

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver los archivos y carpetas almacenados en la PDU de rack.

dns

Acceso: Administrador sólo

Definición: Permite configurar los parámetros de DNS (Domain Name System).

Parámetro	Argumento	Descripción
-OM	enable disable	Permite anular el DNS manual.
-p	<Servidor DNS primario>	Permite establecer el servidor DNS primario.
-s	<Servidor DNS secundario>	Permite establecer el servidor DNS secundario.
-d	<nombre de dominio>	Permite establecer el nombre de dominio.
-n	<nombre de dominio IPv6>	Permite establecer el nombre de dominio IPv6.
-h	<nombre de host>	Permite establecer el nombre de host.

eventlog

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver la fecha y hora en que se ha recuperado el registro de sucesos, el estado de la PDU de rack, y el estado de los sensores conectados a la PDU de rack. Vea los sucesos del dispositivo más recientes y la fecha y hora en que han tenido lugar. Utilice las siguientes teclas para navegar por el registro de sucesos:

Tecla	Descripción
ESC	Cierra el registro de sucesos y regresa a la interfaz de línea de comandos.
INTRO	Actualiza la pantalla del registro. Utilice este comando para ver los sucesos que se han registrado después de la última vez que recuperó y mostró el registro.
BARRA ESPACIADORA	Permite ver la siguiente página del registro de sucesos.
B	Permite ver la página anterior del registro de sucesos. Este comando no está disponible en la página principal del registro de sucesos.
D	Borra el registro de sucesos. Siga las indicaciones para confirmar o denegar el borrado. Los sucesos eliminados no se pueden recuperar.

exit

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite salir de la sesión de la interfaz de línea de comandos.

format

Acceso: Administrador sólo

Descripción: Reformatea el sistema de archivos de la PDU de rack y borra todos los certificados de seguridad, claves de cifrado, valores de configuración y los registros de sucesos y de datos.



Para restablecer la PDU de rack a su configuración predeterminada, utilice el comando `resetToDef`.

FTP

Acceso: Administrador sólo

Descripción: Permite activar o desactivar el acceso al servidor FTP. También permite cambiar el valor del puerto al número de cualquier puerto sin usar del 5001 al 32768 para obtener seguridad adicional.

Opción	Argumento	Definición
-p	<número de puerto>	Define el puerto TCP/IP que utiliza el servidor FTP para comunicarse con la PDU de rack (el 21 de manera predeterminada). El servidor FTP utiliza el puerto especificado y el puerto un número menor que el puerto especificado.
-S	enable disable	Configura el acceso al servidor FTP.

Ejemplo: Para cambiar el puerto TCP/IP a 5001, escriba:

```
ftp -p 5001
```

help

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver una lista de todos los comandos de la ILC disponibles para su tipo de cuenta. Para ver el texto de ayuda de un comando en concreto, escriba el comando seguido de **help**.

Ejemplo 1: Para ver una lista de los comandos disponibles para un Usuario de dispositivo, escriba:

```
help
```

Ejemplo 2: Para ver una lista de las opciones que acepta el comando **alarmcount**, escriba:

```
alarmcount help
```

netstat

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver el estado de la red y todas las direcciones IPv4 e IPv6 activas.

ntp

Acceso: Administrador

Definición: Permite ver y configurar los parámetros de NTP (network time protocol).

Opción	Argumento	Definición
-OM	enable disable	Permite anular la configuración manual.
-p	<servidor NTP primario>	Especifica el servidor primario.
-s	<servidor NTP secundario>	Especifica el servidor secundario.

Ejemplo 1: Para activar la anulación de la configuración manual, escriba:

```
ntp -OM enable
```

Ejemplo 2: Para especificar el servidor NTP primario, escriba:

```
ntp -p 150.250.6.10
```

ping

Acceso: Administrador, Usuario de dispositivo

Descripción. Permite determinar si el dispositivo con la dirección IP o nombre DNS que se especifica está conectado a la red. Se envían cuatro consultas a la dirección.

Argumento	Descripción
<dirección IP o nombre DNS>	Escriba una dirección IP con el formato xxx.xxx.xxx.xxx, o el nombre DNS configurado por el servidor DNS.

Ejemplo: Para determinar si un dispositivo con una dirección IP de 150.250.6.10 está conectado a la red, escriba:

```
ping 150.250.6.10
```

portSpeed

Acceso: Administrador

Descripción:

Opción	Argumentos	Descripción
-s	auto 10H 10F 100H 100 F	Permite definir la velocidad de comunicación del puerto Ethernet. El comando <code>auto</code> permite que los dispositivos Ethernet negocien para transmitir a la mayor velocidad posible. Véase Velocidad de puerto para obtener más información sobre la configuración de la velocidad del puerto.

Ejemplo: Para configurar el puerto TCP/IP para comunicarse a 100 Mbps con comunicación semidúplex (comunicación en un solo sentido a la vez), escriba:

```
portspeed -s 100H
```

prompt

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite configurar el indicador de la interfaz de línea de comandos para que incluya o excluya el tipo de cuenta del usuario que está en una sesión actualmente. Cualquier usuario puede cambiar este parámetro; todas las cuentas de usuario se actualizarán para utilizar el nuevo valor.

Opción	Argumento	Descripción
-s	long (largo)	El indicador incluye el tipo de cuenta del usuario que está en una sesión actualmente.
	short (corto)	El valor predeterminado. El indicador tiene cuatro caracteres de largo: <code>ilc></code>

Ejemplo: Para incluir en el indicador de comando el tipo de cuenta del usuario que está en una sesión actualmente, escriba:

```
prompt -s long
```

quit

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite salir de la sesión de la interfaz de línea de comandos (funciona igual que el comando exit).

radius

Acceso: Administrador sólo

Descripción: Permite ver la configuración RADIUS existente, activar o desactivar la autenticación RADIUS y configurar los parámetros de autenticación básicos para hasta dos servidores RADIUS.



Para ver un resumen de la configuración de un servidor RADIUS y una lista de servidores RADIUS aceptados, consulte [Configuración del servidor RADIUS](#).

En la interfaz Web de la PDU de rackse dispone de parámetros de autenticación adicionales para los servidores RADIUS. Consulte [RADIUS](#) para obtener más información.

Para una información detallada sobre la configuración de su servidor RADIUS, consulte [Apéndice B: Manual de seguridad](#).

Opción	Argumento	Descripción
-a	local radiusLocal radius	Permite configurar la autenticación RADIUS: local : RADIUS se desactiva. La autenticación local se activa. radiusLocal : primero autenticación RADIUS, luego Local. Se activa RADIUS y la autenticación local. La autenticación se solicita primero al servidor RADIUS. Si el servidor RADIUS no responde, se usa autenticación local. radius : RADIUS se activa. La autenticación local se desactiva.

Opción	Argumento	Descripción
-p1 -p2	<IP de servidor>	El nombre de servidor o la dirección IP del servidor RADIUS primario o secundario. NOTA: Los servidores RADIUS utilizan el puerto 1812 de manera predeterminada para autenticar a los usuarios. Para utilizar un puerto diferente, añada dos puntos seguido del número del nuevo puerto al final del nombre o dirección IP del servidor RADIUS.
-s1 -s2	<secreto de servidor>	El secreto compartido entre el servidor RADIUS primario o secundario y la PDU de rack.
-t1 -t2	<tiempo de espera de servidor>	El tiempo en segundos que la PDU de rack espera a una respuesta del servidor RADIUS primario o secundario.

Ejemplo 1:

Para ver la configuración RADIUS existente de la PDU de rack, escriba **radius** y pulse INTRO.

Ejemplo 2: Para activar la autenticación RADIUS y la local, escriba:

```
radius -a radiusLocal
```

Ejemplo 3: Para configurar un tiempo de espera de 10 segundos para un servidor RADIUS secundario, escriba:

```
radius -t2 10
```

reboot

Acceso: Administrador sólo

Descripción: Reinicia la interfaz de la PDU de rack.

resetToDef

Acceso: Administrador sólo

Descripción:

Opción	Argumentos	Descripción
-p	all keepip (todo o mantener ip)	Permite restablecer todos los cambios en la configuración, incluyendo las acciones de sucesos, la configuración del dispositivo, y, de manera opcional, los valores de configuración TCP/IP.

Ejemplo: Para restablecer todos los cambios en la configuración excepto los valores de configuración TCP/IP para la PDU de rack, escriba:

```
resetToDef -p keepip
```

snmp, snmpv3

Acceso: Administrador sólo

Descripción: Permite activar o desactivar SNMP 1 o SNMP 3.

Opción	Argumentos	Descripción
-S	enable disable	Permite activar o mostrar la respectiva versión de SNMP, 1 ó 3.

Ejemplo: Para activar la versión 1 de SNMP, escriba:

```
snmp -S enable
```

system

Acceso: Administrador sólo

Descripción: Permite ver y establecer el nombre del sistema, el contacto, la ubicación y ver el tiempo de actividad así como la fecha y la hora, el usuario en sesión y el estado del sistema a alto nivel P, N, A (véase [Acerca de la Pantalla principal](#) para más información sobre el estado del sistema).

Opción	Argumento	Descripción
-n	<nombre del sistema>	Permite definir el nombre del dispositivo, el nombre de la persona responsable del dispositivo y la ubicación física del dispositivo. NOTA: Si se define un valor con más de una palabra, se debe encerrar el valor entre comillas.
-c	<contacto del sistema>	
-l	<ubicación del sistema>	

Ejemplo 1: Para configurar la ubicación del dispositivo como **Laboratorio de pruebas**, escriba:

```
system -l "Laboratorio de pruebas"
```

Ejemplo 2: Para configurar el nombre del sistema como **Don Adams**, escriba:

```
system -n "Don Adams"
```

tcpip

Acceso: Administrador sólo

Descripción: Permite ver y configurar manualmente estos parámetros de red para la PDU de rack:

Opción	Argumento	Descripción
-i	<dirección IP>	Escriba la dirección IP de la PDU de rack, utilizando el formato xxx.xxx.xxx.xxx
-s	<máscara de subred>	Escriba la máscara de subred para la PDU de rack.
-g	<puerta de enlace>	Escriba la dirección IP de la puerta de enlace predeterminada. No utilice la dirección de bucle invertido (127.0.0.1) como puerta de enlace predeterminada.
-d	<nombre de dominio>	Escriba el nombre DNS configurado por el servidor DNS.
-h	<nombre de host>	Escriba el nombre de host que va a utilizar la PDU de rack.

Ejemplo 1: Para ver la configuración de red de la PDU de rack, escriba `tcpip` y pulse INTRO.

Ejemplo 2: Para configurar manualmente una dirección IP de 150.250.6.10 para la PDU de rack, escriba:

```
tcpip -i 150.250.6.10
```

tcpip6

Acceso: Administrador sólo

Descripción: Permite activar IPv6 y ver y configurar manualmente estos parámetros de red para la PDU de rack:

Opción	Argumento	Descripción
-S	enable disable	Permite activar o desactivar IPv6.
-man	enable disable	Permite activar el direccionamiento manual para la dirección IPv6 de la PDU de rack.
-auto	enable disable	Permite activar que la PDU de rack configure automáticamente la dirección IPv6.
-i	<IPv6 address (dirección IPv6)>	Permite establecer la dirección IPv6 de la PDU de rack.
-g	<IPv6 gateway (puerta de enlace IPv6)>	Permite establecer la dirección IPv6 de la puerta de enlace predeterminada.
-d6	router stateful stateless never	Permite establecer el modo de DHCPv6: con los parámetros del router controlados, statefull (para la dirección y demás información, mantienen su estado), stateless (para la información que no sea la dirección, no se mantiene el estado), never (nunca).

Ejemplo 1: Para ver la configuración de red de la PDU de rack, escriba `tcpip6` y pulse INTRO.

Ejemplo 2: Para configurar manualmente un dirección IPv6 de `2001:0:0:0:0:FFD3:0:57ab` para la PDU de rack, escriba:

```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

user

Acceso: Administrador sólo

Descripción: Permite configurar el nombre de usuario, la contraseña y el tiempo de espera por inactividad para los tipos de cuenta Administrador, Usuario de dispositivo y Usuario de sólo lectura.



Para obtener información sobre los permisos concedidos a cada tipo de cuenta, véase [Tipos de cuentas de usuario](#).

Opción	Argumento	Descripción
-an -dn -rn	<nombre de administrador> <nombre de dispositivo> <nombre de sólo lectura>	Permite establecer un nombre de usuario sensible a mayúsculas y minúsculas para cada tipo de cuenta. La máxima longitud es de 10 caracteres.
-ap -dp -rp	<contraseña de administrador> <contraseña de dispositivo> <contraseña de sólo lectura>	Permite establecer una contraseña sensible a mayúsculas y minúsculas para cada tipo de cuenta. La máxima longitud es de 32 caracteres. Las contraseñas en blanco (contraseñas sin caracteres) no están permitidas.
-t	<minutos>	Configura el tiempo (3 minutos de manera predeterminada) que espera el sistema antes de cerrar la sesión de un usuario inactivo.

Ejemplo 1: Para cambiar el nombre de usuario del Administrador a XYZ, escriba:

```
user -an XYZ
```

Ejemplo 2: Para cambiar el tiempo antes de la desconexión a 10 minutos, escriba:

```
user -t 10
```

web

Acceso: Administrador sólo

Descripción: Posibilita el acceso a la interfaz Web utilizando HTTP o HTTPS.

Para obtener seguridad adicional, se puede cambiar el valor del puerto para HTTP y HTTPS a cualquier número de puerto no utilizado del 5000 al 32768. Los usuarios deben utilizar entonces dos puntos (:) en el campo de dirección del navegador para especificar el número de puerto. Por ejemplo, para un número de puerto de 5000 y una dirección IP de 152.214.12.114, escriba:

```
http://152.214.12.114:5000
```

Opción	Argumento	Definición
-S	disable http https	Permite configurar el acceso a la interfaz Web. Cuando se activa HTTPS, los datos se cifran durante la transmisión y se autentican mediante certificado digital.
-ph	<Nº. de puerto http>	Define el puerto TCP/IP utilizado por HTTP para comunicarse con la PDU de rack (el 80 de manera predeterminada).
-ps	<Nº. de puerto https>	Define el puerto TCP/IP utilizado por HTTPS para comunicarse con la PDU de rack (el 443 de manera predeterminada).

Ejemplo: Para impedir todo acceso a la interfaz Web, escriba:

```
web -S disable
```

xferINI

Acceso: Administrador sólo

Descripción: Permite utilizar XMODEM para cargar un archivo INI mientras accede a la interfaz de línea de comandos a través de una conexión serie. Una vez que se completa la carga:

- Si hay algún cambio en el sistema o la red, la interfaz de línea de comandos se reinicia y debe iniciar de nuevo una sesión.
- Si ha seleccionado una velocidad en baudios para la transferencia de archivos diferente de la predeterminada para la PDU de rack, debe restablecer la velocidad predeterminada para restablecer la comunicación con la PDU de rack.

xferStatus

Acceso: Administrador sólo

Descripción: Permite ver el resultado de la última transferencia de archivos.



Véase [Verificación de las actualizaciones](#) para obtener una descripción de los códigos de resultado de las transferencias.

Descripción de los comandos de dispositivo

devLowLoad

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de carga baja del dispositivo en kilovatios.

Ejemplo 1: Para ver el umbral de carga baja, escriba:

```
cli> devLowLoad
E000: Success (Éxito)
0.5 kW
```

Ejemplo 2: Para establecer en 1 kW el umbral de carga baja, escriba:

```
cli> devLowLoad 1.0
E000: Success (Éxito)
```

devNearOver

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de casi sobrecarga del dispositivo en kilovatios.

Ejemplo 1: Para ver el umbral de casi sobrecarga, escriba:

```
cli> devNearOver
E000: Success (Éxito)
20.5 kW
```

Ejemplo 2: Para establecer en 21,3 kW el umbral de casi sobrecarga, escriba:

```
cli> devNearOver 21.3
E000: Success (Éxito)
```

devOverLoad

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de sobrecarga del dispositivo en kilovatios.

Ejemplo 1: Para ver el umbral de sobrecarga, escriba:

```
cli> devOverLoad  
E000: Success (Éxito)  
25.0 kW
```

Ejemplo 2: Para establecer en 25,5 kW el umbral de sobrecarga, escriba:

```
cli> devOverLoad 25.5  
E000: Success (Éxito)
```

devReading

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite ver la potencia total en kilovatios o la energía total en kilovatios-hora del dispositivo.

Argumento	Definición
power (potencia)	Permite ver la potencia total en kilovatios
energy (energía)	Permite ver la energía total en kilovatios-hora

Ejemplo 1: Para ver la potencia total, escriba:

```
cli> devReading power
E000: Success (Éxito)
5.2 kW
```

Ejemplo 2: Para ver la energía total, escriba:

```
cli> devReading energy
E000: Success (Éxito)
200.1 kWh
```

devStartDly

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver la cantidad de tiempo (en segundos) a añadir al Retardo de encendido (Power On Delay) de cada toma de corriente después de que se aplique energía a la PDU de Rack. Los valores permitidos están dentro del rango de 1 a 300 segundos o never (que no se encienda nunca).

Ejemplo 1: Para ver el retardo de inicio en frío, escriba:

```
cli> devStartDly
E000: Success (Éxito)
5 seconds (segundos)
```

Ejemplo 2: Para establecer en seis segundos el retardo de inicio en frío, escriba:

```
cli> devStartDly 6
E000: Success (Éxito)
```

humLow

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de humedad baja como porcentaje de la humedad relativa.

Ejemplo 1: Para ver el umbral de humedad baja, escriba:

```
cli> humLow
E000: Success (Éxito)
10 %RH
```

Ejemplo 2: Para establecer el umbral de humedad baja, escriba:

```
cli> humLow 12
E000: Success (Éxito)
```

humMin

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de humedad mínima como porcentaje de la humedad relativa.

Ejemplo 1: Para ver el umbral de humedad mínima, escriba:

```
cli> humMin
E000: Success (Éxito)
6 %RH
```

Ejemplo 2: Para establecer el umbral de humedad mínima, escriba:

```
cli> humMin 8
E000: Success (Éxito)
```

humReading

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver el valor de humedad del sensor.

Ejemplo: Para ver el valor de humedad, escriba:

```
cli> humReading
E000: Success (Éxito)
25 %RH
```

inNormal

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite ver el estado normal de cada entrada de contacto seco.

Ejemplo: Para ver el estado normal de cada entrada de contacto seco, escriba:

```
cli> inNormal
E000: Success (Éxito)
1: Open (abierta)
2: Open (abierta)
```

inReading

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite ver el estado actual de cada entrada de contacto seco.

Ejemplo: Para ver el estado de las entradas de contacto seco, escriba:

```
cli> inReading
E000: Success (Éxito)
1: Open (abierta)
2: Open (abierta)
```

olAssignUsr

Acceso: Administrador

Descripción: Permite asignar control de las tomas de corriente a un usuario de tomas de corriente que existe en la base de datos local.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
<usuario>	Un usuario que existe en la base de datos local. (consulte la sección userAdd).

Ejemplo 1: Para asignar a un usuario llamado Bobby a las tomas de corriente 3, de la 5 a la 7, y 10, escriba:

```
cli> olAssignUsr 3,5-7,10 bobby
E000: Success (Éxito)
```

Ejemplo 2: Para asignar a un usuario llamado Billy a todas las tomas de corriente, escriba:

```
cli> olAssignUsr all billy
E000: Success (Éxito)
```

olCancelCmd

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Cancela todos los comandos pendientes para una toma de corriente o un grupo de tomas de corriente.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.

Ejemplo: Para cancelar todos los comandos para la toma de corriente 3, escriba:

```
cli> olCancelCmd 3
E000: Success (Éxito)
```

oIDlyOff

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Desactiva una toma de corriente o un grupo de tomas de corriente después del Retardo de apagado (Power Off Delay) (véase [oIOff](#)).

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección oIName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.

Ejemplo 1: Para desactivar las tomas de corriente 3, de la 5 a la 7, y 10, escriba:

```
cli> oIDlyOff 3,5-7,10
E000: Success (Éxito)
```

Ejemplo 2: Para desactivar todas las tomas de corriente, escriba:

```
cli> oIDlyOff all
E000: Success (Éxito)
```

oIDlyOn

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Activa una toma de corriente o un grupo de tomas de corriente después del Retardo de encendido (Power On Delay) (véase [oIDlyOnDelay](#)).

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección oIDName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.

Ejemplo 1: Para activar las tomas de corriente 3, de la 5 a la 7, y 10, escriba:

```
cli> oIDlyOn 3,5-7,10
E000: Success (Éxito)
```

Ejemplo 2: Para activar una toma de corriente con el nombre configurado de Outlet1, escriba:

```
cli> oIDlyOn outlet1
E000: Success (Éxito)
```

oIDlyReboot

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Aplica un ciclo de apagado-encendido a una toma de corriente o a un grupo de tomas de corriente. Las tomas de corriente especificadas se desactivarán basándose en el Retardo de apagado (Power Off Delay) configurado (véase [oIOffDelay](#)). Tras la Duración del reinicio (Reboot Duration) más larga (véase [oIRbootTime](#)) de las tomas de corriente seleccionadas, las tomas comenzarán a activarse basándose en los Retardos de encendido configurados (véase [oIOnDelay](#)) establecidos para las tomas especificadas.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección oIName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.

Ejemplo 1: Para aplicar un ciclo de apagado-encendido a las tomas de corriente 3, de la 5 a la 7, y 10, escriba:

```
cli> oIDlyReboot 3,5-7,10
E000: Success (Éxito)
```

Ejemplo 2: Para aplicar un ciclo de apagado-encendido a una toma de corriente con el nombre configurado de Outlet1, escriba:

```
cli> oIDlyReboot outlet1
E000: Success (Éxito)
```

olGroups

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente.

Descripción: Lista los grupos de sincronización de tomas de corriente (outlet synchronization groups) definidos en la PDU de rack. (Consulte la sección [Configuración y control de los grupos de tomas de corriente](#) para obtener más información.)

Ejemplo: Para listar los grupos de sincronización de tomas de corriente, escriba:

```
cli> olGroups
E000: Success (Éxito)
Outlet Group A:
159.215.6.141 -> Outlets: 2,4,5
159.215.6.143 -> Outlets: 2,8
Outlet Group B:
159.215.6.141 -> Outlets: 1
159.215.6.166 -> Outlets: 1
```

olLowLoad

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite establecer o ver el umbral de advertencia de carga baja de las tomas de corriente.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
<potencia>	El nuevo umbral de toma de corriente (vatios).

Ejemplo 1: Para establecer en 2 vatios el umbral de carga baja para todas las tomas de corriente, escriba:

```
cli> olLowLoad all 2
E000: Success (Éxito)
```

Ejemplo 2: Para ver el umbral de carga baja de las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> olLowLoad 3,5-7
E000: Success (Éxito)
3: BobbysServer: 2 W
5: BillysServer: 2 W
6: JoesServer: 2 W
7: JacksServer: 2 W
```

olName

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite establecer o ver el nombre configurado para una toma de corriente.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
<nuevonombre>	El nombre para una toma de corriente específica. Utilice únicamente letras y números.

Ejemplo: Para configurar el nombre para la toma de corriente 3 como BobbysServer, escriba:

```
cli> olName 3 BobbysServer
E000: Success (Éxito)
3: BobbysServer
5: BillysServer
6: JoesServer
7: JacksServer
```

olNearOver

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite establecer o ver el umbral de advertencia de casi sobrecarga de las tomas de corriente.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
<potencia>	El nuevo umbral de toma de corriente (vatios).

Ejemplo 1: Para ver el umbral de casi sobrecarga de las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> olNearOver 3,5-7
E000: Success (Éxito)
3: BobbysServer: 5 W
5: BillysServer: 6 W
6: JoesServer: 5 W
7: JacksServer: 4 W
```

Ejemplo 2: Para establecer el umbral de casi sobrecarga de las tomas de corriente 3 y de la 5 a la 7, en seis vatios, escriba:

```
cli> olNearOver 3,5-7 6
E000: Success (Éxito)
3: BobbysServer: 6 W
5: BillysServer: 6 W
6: JoesServer: 6 W
7: JacksServer: 6 W
```

o1Off

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite desactivar una toma de corriente o un grupo de tomas de corriente sin ningún retardo.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección o1Name).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.

Ejemplo 1: Para desactivar las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> o1off 3,5-7
E000: Success (Éxito)
```

o1OffDelay

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite establecer o ver el retardo de tiempo del comando Off Delayed (véase [o1DlyOff](#)) y de un comando Reboot Delayed (véase [o1DlyReboot](#)).

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica (consulte la sección o1Name).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
<tiempo>	Un tiempo para el retardo dentro de un rango de 1 a 7200 segundos (2 horas).

Ejemplo 1: Para establecer un retardo de 9 segundos para la desactivación de las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> o1OffDelay 3,5-7 9
E000: Success (Éxito)
```

Ejemplo 2: Para ver el retardo del comando Off Delayed para las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> o1OffDelay 3,5-7
E000: Success (Éxito)
3: BobbysServer: 9 sec
5: BillysServer: 9 sec
6: JoesServer: 9 sec
7: JacksServer: 9 sec
```

o1On

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite activar una toma de corriente o un grupo de tomas de corriente sin ningún retardo.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección o1Name).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.

Ejemplo 1: Para activar las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> o1On 3,5-7
E000: Success (Éxito)
```

o1OnDelay

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite establecer o ver el retardo de tiempo del comando On Delayed (véase [o1DlyOn](#)) y de un comando Reboot Delayed (véase [o1DlyReboot](#)).

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección o1Name).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
<tiempo>	Un tiempo para el retardo dentro de un rango de 1 a 7200 segundos (2 horas).

Ejemplo 1: Para establecer un retardo de 6 segundos para la activación de las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> o1OnDelay 3,5-7 6
E000: Success (Éxito)
```

Ejemplo 2: Para ver el retardo del comando On Delayed para las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> o1OnDelay 3,5-7
E000: Success (Éxito)
3: BobbysServer: 6 sec
5: BillysServer: 6 sec
6: JoesServer: 6 sec
7: JacksServer: 6 sec
```

olOverLoad

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite establecer o ver el umbral de advertencia de sobrecarga de las tomas de corriente.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
<potencia>	El nuevo umbral de toma de corriente (vatios).

Ejemplo 1: Para ver el umbral de sobrecarga de las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> olOverLoad 3,5-7
E000: Success (Éxito)
3: BobbysServer: 7 W
5: BillysServer: 8 W
6: JoesServer: 7 W
7: JacksServer: 6 W
```

Ejemplo 2: Para establecer el umbral de sobrecarga de las tomas de corriente 3 y de la 5 a la 7, en siete vatios, escriba:

```
cli> olOverLoad 3,5-7 7
E000: Success (Éxito)
3: BobbysServer: 7 W
5: BillysServer: 7 W
6: JoesServer: 7 W
7: JacksServer: 7 W
```

olRbootTime

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite establecer o ver la cantidad de tiempo que permanecerá desactivada una toma de corriente para un comando Reboot Delayed (véase [olDlyReboot](#)).

Ejemplo 1: Para ver el tiempo establecido para que las tomas de corriente 3 y de la 5 a la 7 permanezcan desactivadas durante un reinicio, escriba:

```
cli> olRbootTime 3,5-7
E000: Success (Éxito)
3: BobbysServer: 4 sec
5: BillysServer: 5 sec
6: JoesServer: 7 sec
7: JacksServer: 2 sec
```

Ejemplo 2: Para establecer el tiempo que las tomas de corriente 3 y de la 5 a la 7 permanezcan desactivadas durante un reinicio, escriba:

```
cli> olRebootTime 3,5-7 10
E000: Success (Éxito)
3: BobbysServer: 10 sec
5: BillysServer: 10 sec
6: JoesServer: 10 sec
7: JacksServer: 10 sec
```

olReading

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite ver la intensidad de corriente, la potencia o la energía de una toma de corriente o un grupo de tomas de corriente.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
current power energy	El nuevo umbral de toma de corriente (vatios).

Ejemplo 1: Para ver la intensidad de corriente de las tomas 3 y de la 5 a la 7, escriba:

```
cli> olReading 3,5-7 current
E000: Success (Éxito)
3: BobbysServer: 4 A
5: BillysServer: 5 A
6: JoesServer: 7 A
7: JacksServer: 2 A
```

Ejemplo 2: Para ver la potencia de la toma de corriente 3, escriba:

```
cli> olReading 3 power
E000: Success (Éxito)
3: BobbysServer: 40 W
```

Ejemplo 3: Para ver la energía de la toma de corriente JoesServer, escriba :

```
cli> olReading joesserver energy
E000: Success (Éxito)
6: JoesServer: 7,3 kWh
```

olReboot

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite aplicar un ciclo de apagado-encendido a una toma de corriente o un grupo de tomas de corriente sin ningún retardo. Si se especifica más de una toma de corriente, se aplicará el ciclo a esas tomas de corriente juntas.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.

Ejemplo: Para reiniciar las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> olReboot 3,5-7
E000: Success (Éxito)
```

olStatus

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite ver el estado de las tomas de corriente especificadas.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.

Ejemplo: Para ver el estado de las tomas de corriente 3 y de la 5 a la 7, escriba:

```
cli> olStatus 3,5-7
E000: Success (Éxito)
3: BobbysServer: On
5: BillysServer: Off
6: JoesServer: Off
7: JacksServer: On
```

olUnasgnUsr

Acceso: Administrador

Descripción: Permite retirar el control de tomas de corriente de un usuario de tomas de corriente que existe en la base de datos local.

Argumento	Descripción
all (todas)	Todas las tomas de corriente de dispositivo.
<nombre de toma de corriente>	El nombre configurado para una toma de corriente específica. (consulte la sección olName).
<nº. de toma de corriente>	Un solo número o un rango de números separados por un guión, o una lista de números de toma de corriente individuales y rangos de números separados por comas.
<usuario>	Un usuario que existe en la base de datos local. (consulte la sección userList).

Ejemplo 1: Para retirar a un usuario llamado Bobby del control de las tomas de corriente 3, de la 5 a la 7, y 10, escriba:

```
cli> olUnasgnUsr 3,5-7,10 bobby
E000: Success (Éxito)
```

Ejemplo 2: Para retirar a un usuario llamado Billy del control de todas las tomas de corriente, escriba:

```
cli> olUnasgnUsr all billy
E000: Success (Éxito)
```

phLowLoad

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de carga baja de fase en kilovatios. Para especificar las fases, elija entre las siguientes opciones. Escriba: **a11** (todas), una sola fase, un rango, o una lista de fases separadas por comas.

Ejemplo 1: Para establecer en 1 kW el umbral de carga baja para todas las fases, escriba:

```
cli> phLowLoad all 1
E000: Success (Éxito)
```

Ejemplo 2: Para ver el umbral de carga baja de las fases 1 a 3, escriba:

```
cli> phLowLoad 1-3
E000: Success (Éxito)
1: 1 A
2: 1 A
3: 1 A
```

phNearOver

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de casi sobrecarga de fase en kilovatios. Para especificar las fases, elija entre las siguientes opciones. Escriba: **a11** (todas), una sola fase, un rango, o una lista de fases separadas por comas.

Ejemplo 1: Para establecer en 10 kW el umbral de casi sobrecarga para todas las fases, escriba:

```
cli> phNearOver all 10  
E000: Success (Éxito)
```

Ejemplo 2: Para ver el umbral de casi sobrecarga de las fases 1 a 3, escriba:

```
cli> phNearOver 1-3  
E000: Success (Éxito)  
1: 10 A  
2: 10 A  
3: 10 A
```

phOverLoad

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de sobrecarga de fase en kilovatios. Para especificar las fases, elija entre las siguientes opciones. Escriba: **a11** (todas), una sola fase, un rango, o una lista de fases separadas por comas.

Ejemplo 1: Para establecer en 13 kW el umbral de sobrecarga para todas las fases, escriba:

```
cli> phOverLoad all 13
E000: Success (Éxito)
```

Ejemplo 2: Para ver el umbral de sobrecarga de las fases 1 a 3, escriba:

```
cli> phOverLoad 1-3
E000: Success (Éxito)
1: 13 A
2: 13 A
3: 13 A
```

phReading

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite ver la corriente, voltaje o potencia de una fase. Permite establecer o ver el umbral de casi sobrecarga de fase en kilovatios. Para especificar las fases, elija entre las siguientes opciones. Escriba: **a11** (todas), una sola fase, un rango, o una lista de fases separadas por comas.

Ejemplo 1: Para ver la medición de corriente de la fase 3, escriba:

```
cli> phReading 3 current
E000: Success (Éxito)
3: 4 A
```

Ejemplo 2: Para ver el voltaje de cada fase, escriba:

```
cli> phReading all voltage
E000: Success (Éxito)
1: 120 V
2: 120 V
3: 120 V
```

Ejemplo 3: Para ver la potencia de la fase 2, escriba:

```
cli> phReading 2 power
E000: Success (Éxito)
2: 40 W
```

phRestrictn

Acceso: Administrador

Descripción: Permite configurar o ver la función de restricción de sobrecarga para impedir que las tomas de corriente se activen cuando se viole el umbral de alarma de sobrecarga. Los argumentos aceptables son **none** (ninguna), **near** (casi) y **over** (sobre). Para especificar las fases, elija una de las siguientes opciones. Escriba: **all** (todas), una sola fase, un rango, o una lista de fases separadas por comas.

Ejemplo 1: Para poner la restricción de sobrecarga de la fase tres en ninguna, escriba:

```
cli> phRestrictn 3 none
E000: Success (Éxito)
```

Ejemplo 2: Para ver las restricciones de sobrecarga de todas las fases, escriba:

```
cli> phRestrictn all
E000: Success (Éxito)
1: over
2: near
3: none
```

prodInfo

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver información acerca de la PDU de Rack.

Ejemplo:

```
cli> prodInfo
E000: Success (Éxito)
AOS vX.X.X.X
Managed Rack PDU vX.X.X.X
Model:                DELL6xxx
Present Outlets:     12 (Tomas de corriente presentes)
Switched Outlets:    12 (tomas con interruptor)
Metered Outlets:     0 (tomas con medidor)
Max Current:         20 A (Máx corriente)
Phases:              1 (Fases)
```

sensorName

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el nombre asignado al puerto del sensor de temperatura/humedad de la PDU de Rack.

Ejemplo 1: Para poner el nombre del puerto en “Sensor1”, escriba:

```
cli> sensorName Sensor1  
E000: Success (Éxito)
```

Ejemplo 2: Para ver el nombre del puerto del sensor, escriba:

```
cli> sensorName  
E000: Success (Éxito)  
Sensor1
```

tempHigh

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de temperatura alta en Fahrenheit o Celsius.

Ejemplo 1: Para establecer el umbral de temperatura alta en 70° Fahrenheit, escriba:

```
cli> tempHigh F 70
E000: Success (Éxito)
```

Ejemplo 2: Para ver el umbral de temperatura alta en Celsius, escriba:

```
cli> tempHigh C
E000: Success (Éxito)
21 C
```

Ejemplo 3: Para ver el umbral de temperatura alta en Fahrenheit, escriba:

```
cli> tempHigh F
E000: Success (Éxito)
70 F
```

tempMax

Acceso: Administrador, Usuario de dispositivo

Descripción: Permite establecer o ver el umbral de temperatura máx en Fahrenheit o Celsius.

Ejemplo 1: Para establecer el umbral de temperatura máx en 80° Fahrenheit, escriba:

```
cli> tempMax F 80
E000: Success (Éxito)
```

Ejemplo 2: Para ver el umbral de temperatura máx en Celsius, escriba:

```
cli> tempMax C
E000: Success (Éxito)
27 C
```

Ejemplo 3: Para ver el umbral de temperatura máx en Fahrenheit, escriba:

```
cli> tempMax F
E000: Success (Éxito)
80 F
```

tempReading

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver el valor de temperatura del sensor en Fahrenheit o Celsius.

Ejemplo: Para ver el valor de temperatura en Fahrenheit, escriba:

```
cli> tempReading F
E000: Success (Éxito)
51.1 F
```

userAdd

Acceso: Administrador

Descripción: Permite añadir a un usuario de tomas de corriente a la base de datos de usuarios local.

Ejemplo: Para añadir a un usuario llamado Bobby, escriba:

```
cli> userAdd Bobby
E000: Success (Éxito)
```

userDelete

Acceso: Administrador

Descripción: Permite quitar a un usuario de tomas de corriente de la base de datos de usuarios local.

Ejemplo: Para quitar a un usuario llamado Bobby, escriba:

```
cli> userDelete Bobby
E000: Success (Éxito)
```

userList

Acceso: Administrador, Usuario de dispositivo y Usuario de tomas de corriente, pero sólo para las tomas a las cuales esté asignado el usuario.

Descripción: Permite listar los usuarios y las tomas de corriente asignadas a los mismos.

Ejemplo 1: Cuando haya iniciado una sesión como Administrador, escriba:

```
cli> userList
E000: Success (Éxito)
Local: admin: 1,2,3,4,5,6,7,8
Local: Bobby: 1,3
Local: Billy: 2,5
Local: Joe: 4,6
Local: Jack: 7,8
```

Ejemplo 2: Cuando haya iniciado una sesión como Billy, escriba:

```
cli> userList
E000: Success (Éxito)
Local: Billy: 2,5
```

userPasswd

Acceso: Administrador.

Descripción: Permite establecer la contraseña de un usuario de tomas de corriente.

Ejemplo: Para poner “abc123” como contraseña de Bobby, escriba:

```
cli> userPasswd Bobby abc123 abc123
E000: Success (Éxito)
```

whoami

Acceso: Administrador, Usuario de dispositivo, Usuario de tomas de corriente

Descripción: Permite ver el nombre de usuario del usuario activo.

Ejemplo:

```
cli> whoami
E000: Success (Éxito)
admin (administrador)
```

Exploradores Web aceptados

Se puede usar Microsoft® Internet Explorer® (IE) 7.x o superior (sólo en los sistemas operativos Windows®) o Mozilla® Firefox® 3.0.6 o superior (en todos los sistemas operativos) para acceder a la PDU de Rack a través de su interfaz Web. Es posible que otros exploradores que se encuentran corrientemente funcionen, pero no se han comprobado totalmente.

La PDU de Rack no puede funcionar con un servidor proxy. Antes de poder utilizar un explorador Web para acceder a la interfaz Web de la PDU de Rack, debe efectuar una de las siguientes acciones:

- Configurar el explorador Web para desactivar el uso de un servidor proxy para la PDU de Rack.
- Configurar el servidor proxy de manera que no actúe como proxy de la dirección IP específica de la PDU de Rack.

Inicio de sesión en la Interfaz Web

Información general

Se puede utilizar el nombre DNS o la dirección IP de sistema de la PDU de Rack para la dirección URL de la interfaz Web. Utilice su nombre de usuario y contraseña sensibles a mayúsculas y minúsculas para iniciar una sesión. Los nombres de usuario y contraseñas predeterminados difieren según el tipo de cuenta:

- **admin/admin** para un Administrador
- **device/device** para un Usuario de dispositivo
- **readonly/readonly** para un Usuario de sólo lectura

Para las cuentas de usuario de tomas de corriente no hay nombre de usuario ni contraseña predeterminados. Un administrador debe definir el nombre de usuario y contraseña y otras características de una cuenta para un Usuario de tomas de corriente. Consulte [Configuración de un usuario de tomas de corriente](#).



Si utiliza HTTPS (SSL/TLS) como protocolo de acceso, sus credenciales de inicio de sesión se comparan con la información de un certificado de servidor. Si el certificado se ha creado con el Security Wizard (Asistente para la seguridad) y se ha especificado una dirección IP como nombre común en el certificado, se debe utilizar una dirección IP para iniciar una sesión en la PDU de Rack. Si se ha especificado un nombre DNS como nombre común en el certificado, se debe utilizar un nombre DNS para iniciar una sesión.



Para obtener información sobre la página Web que aparece al iniciar una sesión en la interfaz Web, consulte la sección [Acerca de la ficha Inicio](#).

Formatos de las direcciones URL

Escriba el nombre DNS o la dirección IP de la PDU de Rack en el campo de dirección URL del explorador Web y pulse INTRO. Cuando se especifica un puerto de servidor Web no predeterminado en Internet Explorer, se debe incluir `http://` o `https://` en el URL.

Mensajes de error comunes del explorador cuando se inicia una sesión.

Mensaje de error	Causa del error	Explorador
“No está autorizado a ver esta página” o “Alguien está en una sesión en este momento...”	Otra persona está en una sesión.	Internet Explorer, Firefox
“Esta página no se puede mostrar”.	El acceso Web está desactivado o el URL no era correcto.	Internet Explorer
“No se puede conectar”.		Firefox

Ejemplos de formatos de URL.

- Para un nombre DNS de Web1:
 - `http://Web1` si HTTP es el modo de acceso.
 - `https://Web1` si HTTPS es el modo de acceso.
- Para una dirección IP de sistema de 139.225.6.133 y el puerto de servidor Web predeterminado (80):
 - `http://139.225.6.133` si HTTP es el modo de acceso.
 - `https://139.225.6.133` si HTTPS (HTTP con SSL) es el modo de acceso.
- Para una dirección IP de sistema de 139.225.6.133 y un puerto de servidor Web no predeterminado (5000):
 - `http://139.225.6.133:5000` si HTTP es el modo de acceso.
 - `https://139.225.6.133:5000` si HTTPS (HTTP con SSL) es el modo de acceso.
- Para una dirección IPv6 de sistema de 2001:db8:1::2c0:b7ff:fe00:1100 y un puerto de servidor Web no predeterminado (5000):
 - `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` si HTTP es el modo de acceso.

Funciones de la interfaz Web

Lea lo siguiente para familiarizarse con las funciones básicas de la interfaz Web de la PDU de Rack.

Fichas

Están disponibles las siguientes fichas:

- **Inicio:** Aparece cuando se inicia una sesión. Permite ver las alarmas activas, el estado de carga de la PDU de Rack, y los sucesos más recientes de la PDU de Rack. Para obtener más información, consulte la sección [Acerca de la ficha Inicio](#).
- **Administrador del dispositivo:** Permite ver el estado de carga, configurar los umbrales de carga, y ver y administrar las mediciones de carga pico de todos los dispositivos conectados, fases y tomas de corriente que correspondan. Permite administrar y controlar las tomas de corriente. Para obtener más información, consulte la sección [Acerca de la ficha Device Manager \(Administrador del dispositivo\)](#).
- **Entorno:** Permite ver los datos del sensor de temperatura y humedad, si está conectado un sensor a la PDU de Rack.
- **Registros:** Permite ver los registros de sucesos, de datos y del sistema.
- **Administración:** Permite configurar la seguridad, la conexión de red, la notificación y los parámetros generales.

Iconos de estado del dispositivo

Uno o más iconos y texto adjunto indican el estado operativo actual de la PDU de Rack:

	Crítica: Existe una alarma crítica, que requiere acción inmediata.
	Advertencia: Existe una condición de alarma que requiere atención y que podría poner en peligro los datos o el equipo si no se aborda.
	Sin alarmas: No hay ninguna alarma y la PDU de Rack funciona normalmente.

En la esquina superior derecha de cada página, la interfaz Web muestra los mismos iconos que se muestran en ese momento en la página Inicio para informar del estado de la PDU de Rack:

- El icono **Sin alarmas** si no existe ninguna alarma.
- Uno o ambos de los otros dos iconos (**Crítica** y **Advertencia**) si existe alguna alarma, y después de cada icono, la cantidad de alarmas activas de esa gravedad.

Para volver a la ficha **Inicio** para ver el resumen del estado de la PDU de Rack, incluidas las alarmas activas, haga clic en un icono de estado rápido de cualquier página de la interfaz.

Vínculos rápidos

En la parte inferior izquierda de la interfaz, hay tres vínculos (Links) configurables. A continuación se muestran los valores predeterminados:

- **Link 1:** dell.com
- **Link 2:** dell.com/home
- **Link 3:** dell.com/business



Para reconfigurar los vínculos, véase [Configuración de los vínculos](#).

Otras funciones de la interfaz Web

- La dirección IP aparece en la esquina superior izquierda.
- En la esquina superior derecha se encuentra un enlace de (**Ayuda**) sensible al contexto y un enlace de (**Cerrar sesión**).

Acerca de la ficha Inicio

Utilice la ficha Inicio para ver las alarmas activas, el estado de carga de la PDU de Rack, y los sucesos más recientes de la PDU de Rack.

Home | **Device Manager** | **Environment** | **Logs** | **Administration**

Overview | Alarm Status | Outlet Status No Alarms

Active Alarms

✓ No Alarms Present

Load Status

Device Load: 0.58 kW 
Phase L1 Load: 5.0 A  [More >](#)

Managed Rack PDU Parameters

Name: John Doe
Contact: Unknown
Location: Unknown
Model Number: DELL6605
Rating: 1 ø, 20 A
User: Administrator
UpTime: 25 Days 20 Hours 57 Minutes

Recent Device Events

Date	Time	Event
10/25/2010	19:45:54	Managed Rack PDU: Outlet #2 (Outlet 2) off.
10/25/2010	19:45:54	Managed Rack PDU: Outlet #1 (Outlet 1) off.
10/20/2000	19:22:58	Managed Rack PDU: Device low load cleared.
10/20/2000	19:22:56	Managed Rack PDU: Phase low load cleared on phase #1.
10/20/2000	19:18:59	Managed Rack PDU: Outlet #3 (Outlet 3) on.

[More Events >](#)

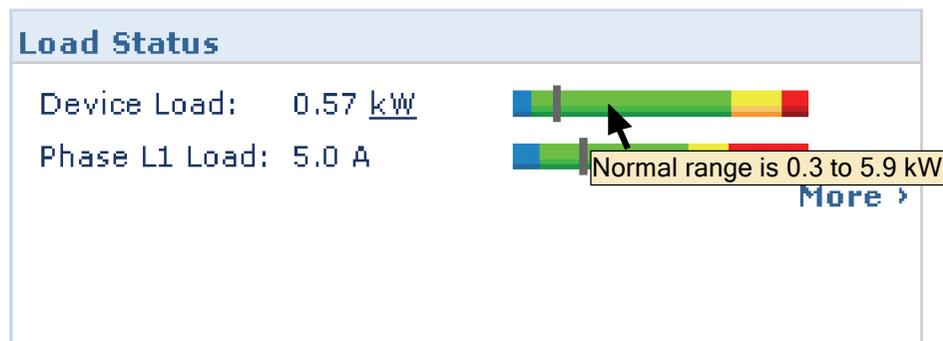
Link 1 | Link 2 | Link 3 Managed Rack PDU 

La vista Información general

Ruta: Inicio > Información general

La parte superior de la Información general indica el estado de alarma. Si hay una o más alarmas, el número y el tipo de las alarmas se indican con un enlace a la vista **Estado de alarma**, donde se pueden ver descripciones de cada alarma. Si no existe ninguna alarma, la Información general muestra “No hay alarmas”.

En la zona **Load Status** (Estado de carga), se muestra la carga del dispositivo en kW y de las fases en Amperios, según corresponda. El medidor verde, amarillo y rojo muestra el estado de carga actual: normal, casi sobrecarga o sobrecarga. Observe que si se ha configurado un umbral de carga baja, el medidor también incluirá un segmento azul a la izquierda de la parte verde. Ponga el cursor sobre los colores para ver los umbrales de carga configurados.



Haga clic en **Más** para ir a la ficha **Administrador del dispositivo** para configurar los umbrales y para ver y administrar la información de cargas pico.

En la zona de parámetros del dispositivo, se muestran el nombre, el contacto, la ubicación, la corriente nominal, el tipo de cuenta de usuario que está accediendo a la PDU de Rack y la cantidad de tiempo que lleva funcionando la PDU de Rack desde el último reinicio debido bien a un ciclo de apagado-encendido o a un reinicio de la Interfaz de administración. (Para obtener más información, consulte la sección [Restablecimiento de la PDU de rack.](#))

En la zona **Sucesos recientes del dispositivo**, se muestra, por orden cronológico inverso, los sucesos que han tenido lugar más recientemente y la fecha y hora en que han tenido lugar. Se muestra un máximo de cinco sucesos a la vez. Haga clic en **Más sucesos** para ir a la ficha **Registros** para ver el registro de sucesos entero.

La vista Estado de alarma

Ruta: Inicio > Estado de alarma

La vista **Estado de alarma** proporciona una descripción de todas las alarmas presentes.



Para obtener detalles sobre las violaciones de los umbrales de humedad y temperatura, haga clic en la ficha Entorno.

Administración del dispositivo

The screenshot displays the Dell Managed Rack PDU web interface. The top navigation bar includes 'Home', 'Device Manager', 'Environment', 'Logs', and 'Administration'. A 'No Alarms' indicator is visible in the top right corner. The left sidebar contains a menu with categories: 'Load Management' (device load, phase load, outlet load), 'Control', 'Configuration', 'Outlet Links', 'Outlet Groups' (information, group configuration), 'Scheduling', and 'Outlet Manager'. The main content area is titled 'Device Load Management' and shows the following information:

- Status:** Load: 0.58 kW, Peak Load: 0.59 kW, Energy: 64.3 kWh. A progress bar indicates the current load is within 2.42 kW of Near Overload.
- Configuration:** Name: John Doe, Location: Unknown.
- Warning Settings:** Overload Alarm: 3.7 kW [0.0 to 5.4], Near Overload Warning: 3.0 kW [0.0 to 5.4], Low Load Warning: 0.5 kW [0.0 to 5.4].
- Coldstart Delay:** Radio buttons for Immediate, Wait 6 Seconds [1 to 300] (selected), and Never.
- Reset Options:** Peak Load: Reset (last reset 06/12/2000 22:44:49), Kilowatt-Hours: Reset (last reset 04/24/2000 04:55:23).

Buttons for 'Apply' and 'Cancel' are located at the bottom of the configuration section. The footer of the interface includes 'Link 1 | Link 2 | Link 3', 'Managed Rack PDU', and the 'DELL' logo.

Acerca de la ficha Device Manager (Administrador del dispositivo)

Ruta: Device Manager (Administrador del dispositivo)

Utilice la ficha **Device Manager** (Administrador del dispositivo) para:

- Ver el estado de la carga de la PDU de Rack
- Configurar los umbrales de carga para todos los dispositivos conectados y fases que correspondan
- Administrar y controlar las tomas de corriente
- Configurar un nombre y una ubicación para la PDU de Rack
- Ver y administrar la medición de cargas pico
- Hacer clic en vínculos configurables por el usuario para abrir páginas web para los dispositivos específicos conectados a la PDU de Rack

Ver el estado de la carga y la carga pico

Ruta: Device Manager (Administrador del dispositivo) > *Load Management (Administración de la carga) opciones*

El indicador del medidor verde, amarillo y rojo muestra el estado actual de la carga: normal, casi sobrecarga o sobrecarga. Si se ha configurado un umbral de carga baja, el medidor incluirá un segmento azul a la izquierda de la parte verde. Al mostrarse la Carga del dispositivo (**Device Load**), el triángulo que se encuentra encima del medidor indica la carga pico.



Haga clic en **kW | BTU** en la esquina superior derecha para cambiar los valores de carga entre kilovatios y BTU (British Thermal Units).

Configuración de los umbrales de carga

Ruta: Device Manager (Administrador del dispositivo) > Load Management options (Administración de la carga) opciones

Para configurar los umbrales de carga:

1. Haga clic en la ficha **Device Manager** (Administrador del dispositivo).
2. Para configurar los umbrales de carga para el dispositivo o las fases, seleccione una opción del menú Load Management (Administración de la carga).
3. Establezca los umbrales de Alarma de sobrecarga (**Overload Alarm**), Advertencia de casi sobrecarga (**Near Overload Warning**) y Advertencia de carga baja (**Low Load Warning**).
4. Haga click en **Apply** (Aplicar).

Configuración del Nombre y la Ubicación de la PDU de Rack

Ruta: **Device Manager (Administrador del dispositivo) > Load Management (Administración de la carga) > Device Load (Carga del dispositivo)**

El nombre y la ubicación que se introducen aparecen en la ficha **Inicio**.



Se puede establecer el Nombre y la Ubicación a través de la ficha **Device Manager** o de la ficha **Administración**. Los cambios en una afectan a la otra.

1. Haga clic en la ficha **Device Manager** (Administrador del dispositivo), y a continuación en **device load** (Carga del dispositivo) en el menú **Load Management** (Administración de la carga).
2. Introduzca un nombre y una ubicación.
3. Haga clic en **Apply** (Aplicar).

Configuración del Retardo de inicio en frío

Ruta: **Device Manager (Administrador del dispositivo) > Device Load (Carga del dispositivo)**

El Retardo de inicio en frío (Coldstart Delay) es el número de segundos que se añaden al Retardo de encendido (Power On Delay) de cada toma de corriente antes de que la toma de corriente se active después de que se aplique energía a la PDU de rack. Los valores permitidos son: de 1 a 300 segundos, **Immediate** (Inmediato) o **Never** (Nunca) (que no se active nunca).

1. Haga clic en la ficha **Device Manager** (Administrador del dispositivo), y a continuación en **device load** (Carga del dispositivo) en el menú **Load Management** (Administración de la carga).
2. Seleccione una opción para **Coldstart Delay**.
3. Haga clic en **Apply** (Aplicar).

Restablecimiento de la Carga pico y los kWh

Ruta: **Device Manager (Administrador del dispositivo) > Device Load (Carga del dispositivo)**

1. Haga clic en la ficha **Device Manager** (Administrador del dispositivo), y a continuación en **device load** (Carga del dispositivo) en el menú **Load Management** (Administración de la carga).
2. Haga clic en las casillas de verificación **Peak Load** (Carga pico) y **Kilowatt-Hours** (Kilovatios-hora) según se desee.
3. Haga clic en **Apply** (Aplicar).

Configuración y control de los grupos de tomas de corriente

Grupos de tomas de corriente: terminología

Un grupo de tomas de corriente (*outlet group*) se compone de tomas de corriente que están vinculadas lógicamente entre sí en la misma PDU de Rack. Las tomas de corriente que están en un grupo de tomas de corriente se activan, se desactivan y se reinician de manera sincronizada:

- Un *grupo de tomas de corriente local* se compone de dos o más tomas de corriente de una PDU de Rack. Sólo las tomas de corriente de ese grupo están sincronizadas.
- Un *grupo de tomas de corriente global* se compone de una o más tomas de corriente de una PDU de Rack. Una toma de corriente se configura como *toma de corriente global*, la cual vincula lógicamente el grupo de tomas de corriente a grupos de tomas de corriente de hasta otras tres PDU de Rack. Todas las tomas de los grupos de tomas de corriente globales vinculados están sincronizadas.
 - En los grupos de tomas de corriente globales, el *grupo de tomas de corriente iniciador* es el grupo que emitió la acción.
 - En los grupos de tomas de corriente globales, un *grupo de tomas de corriente seguidor* es cualquier otro grupo de tomas de corriente que esté sincronizado con el grupo de tomas de corriente iniciador.

Cuando se aplica una acción de control de tomas de corriente a tomas que son miembros de un grupo de tomas de corriente, las tomas se sincronizan de la manera siguiente:

- En un grupo de tomas de corriente global, utilice los periodos de retardo y la duración del reinicio configurados para la toma de corriente global del grupo de tomas de corriente iniciador.
- En un grupo de tomas de corriente local, las tomas utilizan los periodos de retardo y la duración del reinicio de la toma de corriente con un número más bajo del grupo.

Finalidad y ventajas de los grupos de tomas de corriente

Utilizando grupos de tomas de corriente sincronizadas en las PDU de Rack, se puede asegurar que las tomas se activen, se desactiven y se reinicien de manera sincronizada. La sincronización de las acciones de grupo de control mediante grupos de tomas de corriente proporciona las siguientes ventajas.

- El apagado e inicio sincronizado de las fuentes de alimentación de los servidores con doble cable impide la información errónea de los fallos de alimentación durante un apagado o reinicio planificado del sistema.
- La sincronización de las tomas de corriente utilizando grupos de tomas de corriente proporciona una sincronización más precisa del apagado y el reinicio que depender de los periodos de retardo de las tomas individuales.
- Una toma de corriente global es visible para la interfaz de usuario de cualquier PDU de Rack a la que esté vinculada.

Requisitos del sistema para los grupos de tomas de corriente

Para establecer y utilizar grupos de control de tomas de corriente sincronizadas:

- Se necesita una red TCP/IP 10/100Base-T, con un hub o un conmutador Ethernet que tenga una fuente de alimentación no compartida por los ordenadores u otros dispositivos que se estén sincronizando.
- Si los grupos de tomas de corriente se deben sincronizar en múltiples PDU de Rack, esas PDU de Rack deben cumplir con los siguientes requisitos:
 - Deben estar en la misma subred.
 - Deben utilizar firmware que tenga el mismo número de versión tanto para el módulo del sistema operativo (AOS) como para el módulo de aplicación.
- Se necesita un ordenador que pueda iniciar operaciones de control sincronizado a través de la interfaz Web o la interfaz de línea de comandos de las PDU de Rack o a través de SNMP.
- Los grupos de tomas de corriente que se sincronicen deben tener la misma dirección IP de multidifusión (Multicast IP address). Asegúrese de que cada conmutador Ethernet que conecte PDUs de rack permita el tráfico de red multidifusión para esa dirección IP de multidifusión.

Reglas para la configuración de grupos de tomas de corriente

Para un sistema que utilice grupos de tomas de corriente, son aplicables las siguientes reglas:

- Una PDU de Rack puede tener más de un grupo de tomas de corriente, pero una toma de corriente sólo puede pertenecer a un grupo de tomas de corriente.
- Un grupo de tomas de corriente local que no tenga ninguna toma global debe componerse de dos o más tomas de corriente.
- Se puede sincronizar un grupo de tomas de corriente global en una PDU de Rack con un grupo de tomas de corriente global en cada una de otras tres PDU de Rack.
 - En un grupo de tomas de corriente global, sólo se puede designar una toma como toma de corriente global vinculada a grupos de tomas de corriente de otras PDU de Rack con fines de sincronización. Esa toma de corriente global puede ser la única toma de su grupo, o bien el grupo puede componerse de múltiples tomas.
 - Para vincular grupos de tomas de corriente de varias PDU de Rack para su sincronización, esas PDU de Rack deben tener el mismo nombre de multidifusión de dispositivo (Device Multicast Name) y la misma dirección de multidifusión de dispositivo (Device Multicast Address) y deben ejecutar la misma versión del firmware de PDU de Rack.
 - Una toma de corriente global de un grupo de tomas de corriente debe tener el mismo número de toma de corriente física que la toma de corriente global de cualquier otro grupo de tomas de corriente al que se vincule.
- Para crear y configurar grupos de tomas de corriente, se debe utilizar la interfaz Web o exportar los valores del archivo de configuración (.ini file) de una PDU de Rack configurada. La interfaz de línea de comandos le permite mostrar si una toma es miembro de un grupo de tomas de corriente y le permite aplicar acciones de control a un grupo de tomas de corriente, pero la interfaz de línea de comandos no le permite establecer ni configurar un grupo de tomas de corriente.

Habilitación de grupos de tomas de corriente

Haga click en la ficha **Device Manager** (Administrador del dispositivo) y seleccione **Group Configuration** (Configuración de grupos) en el menú de navegación izquierdo **Outlet Groups** (Grupos de tomas de corriente). Configure los siguientes parámetros, y haga clic en **Apply** (Aplicar).

Habilitación de la creación de grupos de tomas de corriente.

Parámetro	Descripción
Device Level Outlet Group (Grupo de tomas de corriente de nivel dispositivo)	Para crear un grupo de tomas de corriente, se debe habilitar este parámetro. Está inhabilitado de manera predeterminada.

Habilitación de la funcionalidad para grupos de tomas de corriente globales (grupos vinculados).

Parámetro	Descripción
Multicast Name (Nombre de multidifusión)	Para vincular grupos de tomas de corriente de múltiples PDU de Rack, se deben definir el mismo Nombre de multidifusión y la misma Dirección IP de multidifusión en cada una de esas PDU de Rack.
Multicast IP (IP de multidifusión)	NOTA: Se puede configurar un máximo de cuatro dispositivos con el mismo Nombre de multidifusión y la misma Dirección IP de multidifusión.

Habilitación del cifrado y autenticación de grupos de tomas de corriente.

Parámetro	Descripción
Authentication Phrase (Frase de autenticación)	Una frase de 15 a 32 caracteres ASCII que verifica que el dispositivo se está comunicando con otros dispositivos, que el mensaje no se ha cambiado durante la transmisión y que el mensaje se ha comunicado en el momento correcto. La frase de autenticación indica que no se ha retrasado y que no se ha copiado y enviado de nuevo después en un momento incorrecto.
Encryption Phrase (Frase de cifrado)	Una frase de 15 a 32 caracteres ASCII que asegura la privacidad de los datos (por medio de cifrado).

Establecimiento del puerto del grupo de tomas de corriente.

Parámetro	Descripción
Outlet Group Port (Puerto del grupo de tomas de corriente)	El número de puerto en el cual se comunicará el dispositivo con otros dispositivos.



Los dispositivos que intenten sincronizarse con Grupos de tomas de corriente de otros dispositivos deben tener todos la misma Frase de autenticación, la misma Frase de cifrado y el mismo Número de puerto de grupo. Estos valores están ocultos al usuario.

Creación de un grupo de tomas de corriente local

1. En la ficha **Device Manager** (Administrador del dispositivo), seleccione **Information** (Información) en el menú de navegación izquierdo **Outlet Groups** (Grupos de tomas de corriente).
2. Asegúrese de que los grupos de tomas de corriente están habilitados. (consulte la sección [Habilitación de grupos de tomas de corriente](#)).
3. Haga clic en **Create Local Outlet Group** (Crear grupo de tomas de corriente local).
4. Bajo **Select Local Outlets** (Seleccionar tomas de corriente locales), seleccione cada una de las tomas de corriente que van a estar en el grupo y asigne al grupo un nombre en el campo **Outlet Group Name** (Nombre del grupo de tomas de corriente). Se deben seleccionar al menos dos tomas de corriente.

Creación de múltiples grupos de tomas de corriente globales

Para establecer múltiples grupos de tomas de corriente globales que se vinculen a grupos de tomas de corriente de otras PDU de Rack:

1. En la ficha **Device Manager** (Administrador del dispositivo), seleccione **Information** (Información) en el menú de navegación izquierdo **Outlet Groups** (Grupos de tomas de corriente).
2. Asegúrese de que los grupos de tomas de corriente están habilitados y de que los parámetros de Multidifusión (nombre y dirección IP) son los mismos para todas las PDU de Rack que se van a vincular. (consulte la sección [Habilitación de grupos de tomas de corriente](#)).
3. Haga clic en **Create Global Outlet Groups** (Crear grupos de tomas de corriente globales).
4. Para cada grupo de tomas de corriente global que cree, seleccione una toma de corriente haciendo clic en su casilla de verificación. Luego haga clic en **Apply** (Aplicar). Por ejemplo, seleccione cinco tomas de corriente para crear cinco grupos de tomas de corriente, cada uno de los cuales se compone de una toma de corriente global.
5. Para añadir tomas de corriente a cualquiera de los grupos de tomas de corriente globales que ha creado, consulte [Edición o eliminación de un grupo de tomas de corriente](#).

Edición o eliminación de un grupo de tomas de corriente

1. En la ficha **Device Manager** (Administrador del dispositivo), seleccione **Information** (Información) en el menú de navegación izquierdo **Outlet Groups** (Grupos de tomas de corriente).
2. Bajo **Configured Outlet Groups** (Grupos de tomas de corriente configurados), haga clic en el número o el nombre del grupo de tomas de corriente para editar o eliminar.

3. Cuando se edita un grupo de tomas de corriente se pueden hacer cualquiera de las siguientes acciones:
 - Cambiar de nombre el grupo de tomas de corriente.
 - Añadir o quitar tomas de corriente haciendo clic en las casillas de verificación para marcarlas o quitarlas la marca.

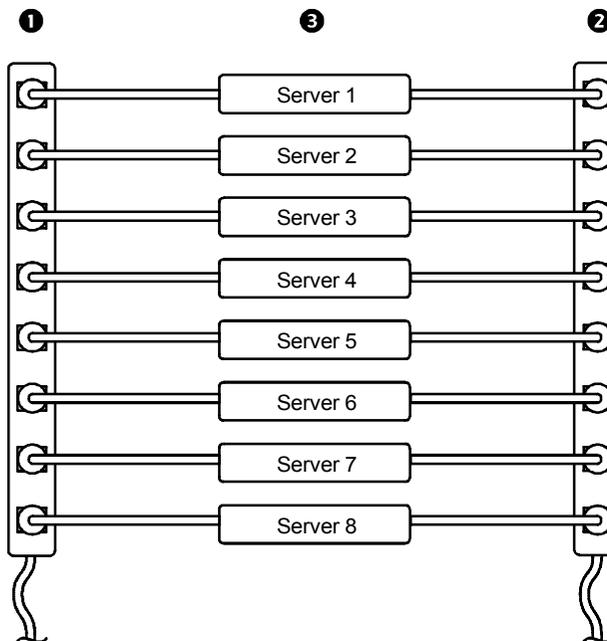


No se puede quitar una toma de corriente de un grupo de tomas de corriente que contenga sólo dos tomas de corriente a menos que la toma restante sea una toma global.

4. Para eliminar el grupo de tomas de corriente, haga clic en **Delete Outlet Group** (Eliminar grupo de tomas de corriente).

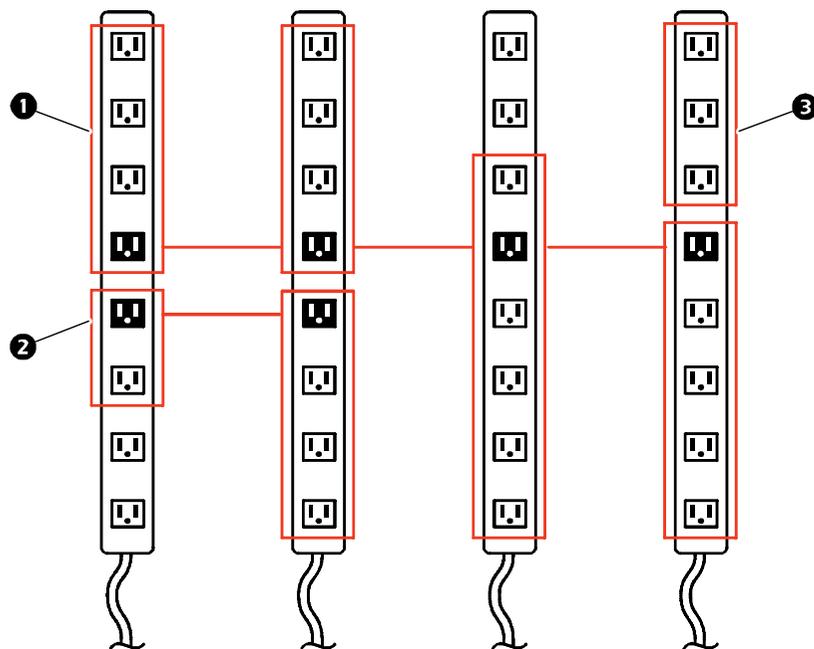
Configuraciones de grupos de tomas de corriente típicas

La siguiente configuración muestra dos PDU de Rack, cada una de ellas con ocho grupos de tomas de corriente. Cada grupo de tomas de corriente consta de una sola toma de corriente global. Cada grupo de tomas de corriente ❶ de la primera PDU de Rack está vinculado al grupo de tomas de corriente ❷ en la misma ubicación de la segunda PDU de Rack. Uno de los cables de un servidor con doble cable ❸ está conectado a cada toma de corriente de la primera PDU de Rack, y el otro cable está conectado a la toma de corriente correspondiente de la segunda PDU de Rack, asegurando que la alimentación de salida de ambas fuentes de alimentación al servidor se active o desactive de manera sincronizada en respuesta a una acción de control de tomas de corriente.



La siguiente configuración muestra tres conjuntos de tomas de corriente sincronizadas. Las tomas de corriente globales se muestran en negro. Los grupos de tomas de corriente están encerrados en rectángulos rojos.

1	Estos cuatro grupos de tomas de corriente globales sincronizan un total de 19 tomas de corriente.
2	Estos dos grupos de tomas de corriente globales sincronizan 6 tomas de corriente, 2 en un grupo y 4 en el otro.
3	Este grupo de tomas de corriente local sincroniza 3 tomas de corriente de la misma PDU de Rack.



Verificación de la instalación y configuración de los grupos de tomas de corriente globales

Para asegurarse de que su instalación cumple con todos los requisitos del sistema para grupos de tomas de corriente y de que ha configurado correctamente los grupos de tomas de corriente, seleccione **Information** (Información) en el menú de navegación izquierdo **Outlet Groups** (Grupos de tomas de corriente) de la interfaz Web para ver los grupos y sus conexiones:

- La sección **Configured Outlet Groups** (Grupos de tomas de corriente configurados) muestra lo siguiente:
 - Todos los grupos de tomas de corriente configurados en la PDU de Rack actual.
 - Las tomas de corriente en cada grupo por número de toma de corriente.
 - Todos los grupos de tomas de corriente de otras PDU de Rack con los cuales esté sincronizado un grupo de tomas de corriente global. Cada PDU de Rack se identifica por su dirección IP, y cada toma de corriente global se muestra en letra negrita.
- La sección **Global Outlet Overview** (Resumen de tomas de corriente globales) muestra lo siguiente:
 - La dirección IP de la PDU de Rack actual.
 - La dirección IP de todas las PDU de Rack que contengan tomas de corriente globales que estén disponibles para ser sincronizadas con grupos de tomas de corriente de otras PDU de Rack.
 - Todas las tomas de corriente globales configuradas en las PDU de Rack, independientemente de que estén sincronizadas o no con grupos de tomas de corriente de la PDU de Rack actual.

Parámetros de toma de corriente para tomas de corriente y grupos de tomas de corriente

Inicio de una acción de control



Si se aplica una acción de control de tomas de corriente a tomas de corriente o grupos de tomas de corriente, se utilizan los siguientes retardos para la acción:

- Con una toma de corriente individual (no en un grupo de tomas de corriente), la acción utiliza los periodos de retardo y duración del reinicio configurados para esa toma de corriente.
- Con un grupo de tomas de corriente global, la acción utiliza los periodos de retardo y duración del reinicio configurados para la toma de corriente global.
- Con un grupo de tomas de corriente local, la acción utiliza los periodos de retardo configurados para la toma de corriente con un número más bajo del grupo.

Para controlar las tomas de corriente de su PDU de Rack:

1. En la ficha **Device Manager** (Administrador del dispositivo), seleccione **Control** (Control) en el menú de navegación izquierdo.
2. Marque las casillas de verificación de cada toma de corriente individual o grupo de tomas de corriente para controlar, o seleccione la casilla de verificación **All Outlets** (Todas las tomas de corriente).
3. Seleccione una **Control Action** (Acción de control) en la lista y haga clic en **Next >>** (Siguiente). En la página de confirmación que explica la acción, elija aplicarla o cancelarla.

Acciones de control que se pueden seleccionar.

Opción	Descripción
No Action (sólo en la Interfaz Web)	No hacer nada.
On Immediate	Aplicar alimentación a las tomas de corriente seleccionadas.
On Delayed	Aplicar alimentación a cada toma de corriente seleccionada según su valor de Power On Delay (Retardo de encendido). [†]
Off Immediate	Retirar la alimentación de las tomas de corriente seleccionadas.
Off Delayed	Retirar la alimentación de cada toma de corriente seleccionada según su valor de Power Off Delay (Retardo de apagado). [†]
Reboot Immediate	Retirar la alimentación de cada toma de corriente seleccionada. Luego aplicar alimentación a cada una de esas tomas de corriente según su valor de Reboot Duration (Duración del reinicio). [†]
Reboot Delayed	Retirar la alimentación de cada toma de corriente seleccionada según su valor de Power Off Delay (Retardo de apagado). Esperar hasta que todas las tomas de corriente estén desactivadas (el valor más elevado de Reboot Duration), y luego aplicar alimentación a cada toma de corriente según su valor de Power On Delay (Retardo de encendido). [†]
<p>[†] Si está seleccionado un grupo de tomas de corriente local, sólo se utilizan los retardos y duración del reinicio configurados de la toma de corriente con el número más bajo del grupo. Si está seleccionado un grupo de tomas de corriente global, sólo se utilizan los retardos y duración del reinicio configurados de la toma de corriente global.</p>	

Opción	Descripción
Cancel Pending Commands	<p>Cancelar todos los comandos pendientes para las tomas de corriente seleccionadas y mantenerlas en su estado actual.</p> <p>NOTA: Para los grupos de tomas de corriente globales, sólo se puede cancelar un comando desde la interfaz del grupo de tomas de corriente iniciador. La acción cancelará el comando para el grupo de tomas de corriente iniciador y todos los grupos de tomas de corriente seguidores.</p>
<p>† Si está seleccionado un grupo de tomas de corriente local, sólo se utilizan los retardos y duración del reinicio configurados de la toma de corriente con el número más bajo del grupo. Si está seleccionado un grupo de tomas de corriente global, sólo se utilizan los retardos y duración del reinicio configurados de la toma de corriente global.</p>	

Configuración de los parámetros de toma de corriente y del nombre de toma de corriente

Están disponibles los siguientes parámetros:

Parámetro	Descripción
Name	Permite establecer el nombre para una o más tomas de corriente. El nombre se muestra al lado del número de toma de corriente en las pantallas de estado.
External Link	Permite definir un enlace HTTP o HTTPS con un sitio Web o una dirección IP. <ul style="list-style-type: none">• http://www.dell.com enlaza la toma de corriente con el sitio Web de Dell.• http://pdu_ip_address, donde <i>pdu_ip_address</i> es la dirección IP de la PDU de Rack y enlaza la toma de corriente con la interfaz Web de la PDU de Rack en la dirección IP, permitiendo que los usuarios autorizados inicien una sesión.
Power On Delay	Permite establecer el número de segundos que espera la PDU de Rack después de que se emite un comando antes de aplicar alimentación de una toma de corriente. NOTA: Para configurar una toma de corriente para que permanezca desactivada todo el tiempo, marque la casilla de verificación Never (Nunca) al lado de Power On Delay (Retardo de encendido).
Power Off Delay	Permite establecer el número de segundos que espera la PDU de Rack después de que se emite un comando antes de retirar la alimentación de una toma de corriente. NOTA: Para configurar una toma de corriente para que permanezca activada todo el tiempo, marque la casilla de verificación Never (Nunca) al lado de Power Off Delay (Retardo de apagado).
Reboot Duration	Permite establecer el número de segundos que permanece desactivada una toma de corriente antes de reiniciarse.

Para configurar los parámetros de toma de corriente o los nombres de toma de corriente, seleccione la ficha **Device Manager** (Administrador del dispositivo) y a continuación **Configuration** (Configuración) en el menú de navegación izquierdo. Haga clic en el botón **Configure Multiple Outlets** (Configurar múltiples tomas de corriente) en la sección **Outlet Configuration** (Configuración de tomas de corriente) o haga clic en el nombre de la toma de corriente.

- Configuración de los parámetros de toma de corriente para múltiples tomas de corriente:
 - Seleccione las casillas de verificación al lado de los números de las tomas de corriente que desea modificar, o seleccione la casilla de verificación **All Outlets** (Todas las tomas de corriente).
 - Introduzca valores para **Name** (Nombre) y **Link** (Vínculo), y haga clic en el botón **Apply** (Aplicar) inmediatamente debajo de la lista.
 - Introduzca valores para **Power On Delay** (Retardo de encendido), **Power Off Delay** (Retardo de apagado), o **Reboot Duration** (Duración del reinicio), y haga clic en el botón **Apply** (Aplicar) inmediatamente debajo de la lista.
- Configuración de los parámetros de toma de corriente para una sola toma de corriente:
 - Introduzca valores para **Name** (Nombre) y **Link** (Vínculo), y haga clic en el botón **Apply** (Aplicar) inmediatamente debajo de la lista.
 - Introduzca valores para **Power On Delay** (Retardo de encendido), **Power Off Delay** (Retardo de apagado), o **Reboot Duration** (Duración del reinicio), y haga clic en el botón **Apply** (Aplicar) inmediatamente debajo de la lista.

Programación de acciones de toma de corriente

Acciones que se pueden programar



Para configurar valores para **Power On Delay** (Retardo de encendido), **Power Off Delay** (Retardo de apagado) y **Reboot Duration** (Duración del reinicio) para cada toma de corriente, véase [Configuración de los parámetros de toma de corriente y del nombre de toma de corriente](#). Aunque se debe utilizar la interfaz Web para programar acciones de toma de corriente, se pueden establecer estos valores en la interfaz Web o la interfaz de línea de comandos.



Para que una acción se aplique a un grupo de tomas de corriente, debe tener habilitados los grupos de tomas de corriente al comienzo de la acción programada. Por ejemplo, si **Off Delayed** está programado para las 4:00 p.m., el Retardo de apagado (**Power Off Delay**) comienza a las 4:00 p.m. Aunque habilite los grupos de tomas de corriente durante ese **Power Off Delay** antes de cuando cualquiera de las tomas de corriente esté programada para desactivarse, la acción se aplicará sólo a la toma de corriente individual y no al grupo de tomas de corriente.

Para cualquier toma de corriente que se seleccione, se puede programar cualquiera de las acciones listadas en la tabla siguiente para que tenga lugar diariamente; a intervalos de una, dos, cuatro u ocho semanas; o sólo una vez.

Opción	Descripción
No Action	No hacer nada.
On Immediate	Aplicar alimentación a las tomas de corriente seleccionadas.
On Delayed	Aplicar alimentación a cada toma de corriente seleccionada según su valor de Power On Delay (Retardo de encendido). [†]
Off Immediate	Retirar la alimentación de las tomas de corriente seleccionadas.
Off Delayed	Retirar la alimentación de cada toma de corriente seleccionada según su valor de Power Off Delay (Retardo de apagado). [†]
Reboot Immediate	Retirar la alimentación de cada toma de corriente seleccionada. Luego aplicar alimentación a cada una de esas tomas de corriente según su valor de Reboot Duration (Duración del reinicio). [†]
Reboot Delayed	Retirar la alimentación de cada toma de corriente seleccionada según su valor de Power Off Delay (Retardo de apagado). Esperar hasta que todas las tomas de corriente estén desactivadas (el valor más elevado de Reboot Duration), y luego aplicar alimentación a cada toma de corriente según su valor de Power On Delay (Retardo de encendido). [†]
<p>[†] Si está seleccionado un grupo de tomas de corriente local, sólo se utilizan los retardos y duración del reinicio configurados de la toma de corriente con el número más bajo del grupo. Si está seleccionado un grupo de tomas de corriente global, sólo se utilizan los retardos y duración del reinicio configurados de la toma de corriente global.</p>	

[†] Si está seleccionado un grupo de tomas de corriente local, sólo se utilizan los retardos y duración del reinicio configurados de la toma de corriente con el número más bajo del grupo. Si está seleccionado un grupo de tomas de corriente global, sólo se utilizan los retardos y duración del reinicio configurados de la toma de corriente global.

Programación de un suceso de toma de corriente

1. En la interfaz Web, seleccione la ficha **Device Manager** (Administrador del dispositivo) y a continuación **Scheduling** (Programación) en el menú de navegación izquierdo.
2. En la página **Outlet Scheduling** (Programación de tomas de corriente), seleccione la frecuencia con la que tendrá lugar el suceso (**One-Time, Daily** o **Weekly**) (Una vez, Diariamente o Semanalmente), y haga clic en el botón **Next** (Siguiete).



Si selecciona **Weekly** (Semanalmente), puede elegir hacer que el suceso tenga lugar una vez cada semana o una vez cada dos, cuatro u ocho semanas.

3. En la página **Schedule a Daily Action** (Programar una acción diaria), en el cuadro de texto **Name of event** (Nombre del suceso), sustituya el nombre predeterminado, **Outlet Event**, por un nombre que identifique su nuevo suceso.

4. Utilice las listas desplegables para seleccionar el tipo de suceso y cuándo tendrá lugar.



El formato de fecha para los sucesos que ocurren una sola vez es *mm/dd*, y el formato de hora para todos los sucesos es *hh/mm*, especificándose la hora de dos dígitos en formato de 24 horas.

- Un suceso que está programado diariamente o a uno de los intervalos disponibles en la opción **Weekly** (Semanalmente) continúa teniendo lugar al intervalo programado hasta que se elimina o se desactiva el suceso.
- Se puede programar un suceso de una única vez para que tenga lugar sólo en una fecha de un periodo de 12 meses a partir de la fecha en que se realiza la programación. Por ejemplo, el 26 de diciembre de 2010, podría programar un suceso de una única vez para cualquier fecha desde la fecha actual hasta el 26 de diciembre de 2011.

5. Utilice las casillas de verificación para seleccionar las tomas de corriente que se verán afectadas por la acción. Se puede seleccionar una o más tomas de corriente individuales o **All Outlets** (Todas las tomas de corriente).
6. Haga clic en **Apply** (Aplicar) para confirmar la programación del suceso, o **Cancel** (Cancelar) para borrarlo.

Cuando se confirma el suceso, la página resumen se vuelve a mostrar, mostrándose el nuevo suceso en la lista de sucesos programados.

Modificación, desactivación, activación y eliminación de un suceso de toma de corriente programado

1. En la interfaz Web, seleccione la ficha **Device Manager** (Administrador del dispositivo) y a continuación **Scheduling** (Programación) en el menú de navegación izquierdo.
2. En la lista de sucesos en la sección **Scheduled Outlet Action** (Acción de toma de corriente programada) de la página **Scheduling** (Programación), haga clic en el nombre del suceso.
3. En la página **Daily/Weekly scheduled action detail** (Detalles de la acción programada diariamente/semanalmente), puede realizar cualquiera de las acciones siguientes:
 - Cambiar detalles del suceso, tales como el nombre del suceso, cuándo está programado que tenga lugar y qué tomas de corriente se ven afectadas.
 - Bajo **Status of event** (Estado del suceso) en la parte superior de la página puede realizar las siguientes tareas:
 - Desactivar el suceso, dejando todos los detalles configurados para que se pueda volver a activar posteriormente. Un suceso desactivado no tiene lugar. Un suceso se activa de manera predeterminada cuando se crea.
 - Activar el suceso, si se había puesto anteriormente en **Disable** (Desactivar).
 - Eliminar el suceso, quitando completamente el suceso del sistema. Los sucesos eliminados no se pueden recuperar.
4. Cuando termine de hacer cambios en esta página, haga clic en **Apply** (Aplicar) para confirmar los cambios o en **Cancel** (Cancelar).

Menú Outlet Manager (Administrador de tomas de corriente)

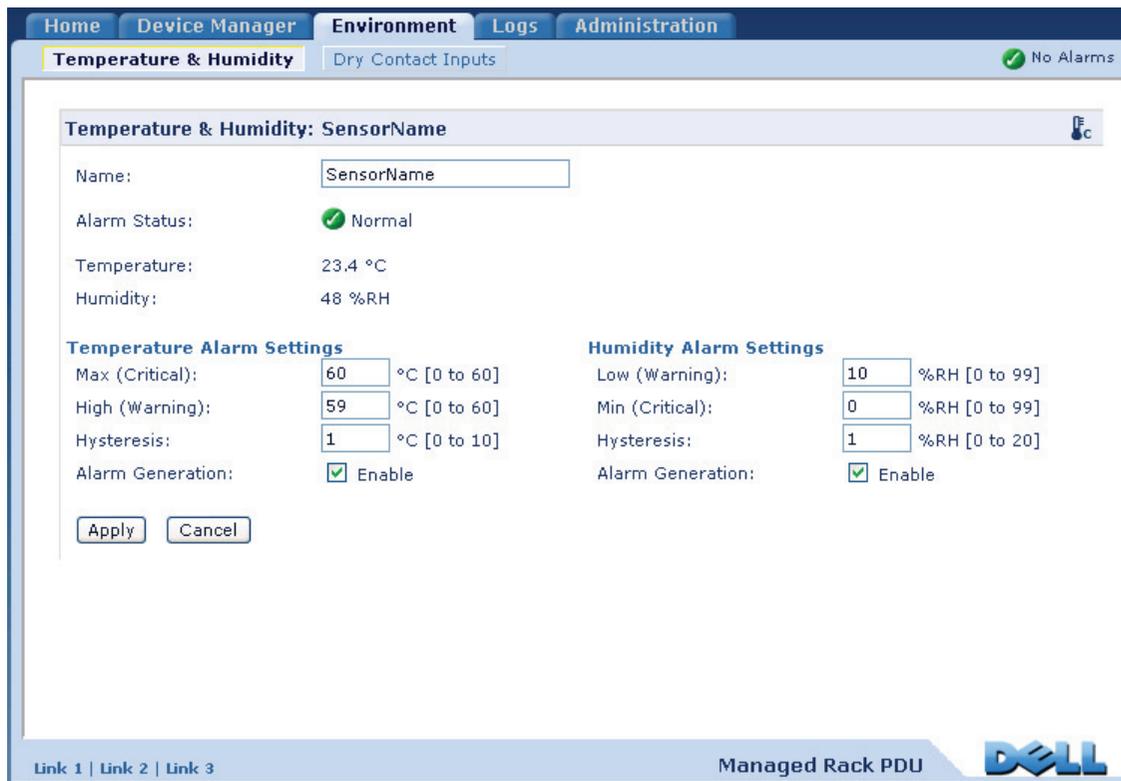
Permite crear y configurar cuentas de usuario de tomas de corriente. A las tomas de corriente individuales se les puede asignar un usuario con una Cuenta de usuario de tomas de corriente. Una Cuenta de usuario de tomas de corriente permite el control sólo de las tomas de corriente asignadas. La configuración de las tomas de corriente se permite a los que tienen derechos de Administrador. El Device Manager (Administrador del dispositivo) tiene derechos de configuración de las tomas de corriente limitados.

Configuración de un usuario de tomas de corriente

1. En la interfaz Web, seleccione la ficha **Device Manager** (Administrador del dispositivo) y a continuación **Outlet Manager** (Administrador de tomas de corriente) en el menú de navegación izquierdo.
2. Haga clic en el botón **Add New User** (Añadir nuevo usuario).
3. Introduzca la información para las siguientes opciones y haga clic en **Apply** (Aplicar) para confirmar los cambios.

Opción	Descripción
User Name	Permite establecer el nombre del usuario de tomas de corriente. "New User" está reservado y no está permitido. NOTA: Un nombre de usuario en naranja indica que la cuenta de usuario ha sido desactivada.
Password	Permite establecer la contraseña del usuario de tomas de corriente.
User Description	Permite establecer una identificación/descripción del usuario de tomas de corriente.
Account Status	Permite activar, desactivar o eliminar la cuenta del usuario de tomas de corriente.
Device outlet access	Permite seleccionar las tomas de corriente a las que puede acceder el usuario.

Entorno



Configuración de los sensores de temperatura y humedad

Ruta: Entorno > Temperatura y humedad

Por medio de la página **Temperatura y humedad**, cuando se tiene conectado a la PDU de Rack un sensor de temperatura o un sensor de temperatura y humedad, se pueden establecer umbrales para la generación de alarmas de Advertencia y Críticas (véase [Iconos de estado del dispositivo](#) para obtener detalles sobre cada tipo de alarma).

Para la temperatura:

- Si se alcanza el umbral de temperatura alta, el sistema genera una alarma de Advertencia.
- Si se alcanza el umbral de temperatura máxima, el sistema genera una alarma Crítica.

De modo similar, para la humedad:

- Si se alcanza el umbral de humedad baja, el sistema genera una alarma de Advertencia.
- Si se alcanza el umbral de humedad mínima, el sistema genera una alarma Crítica.



Haga clic en el símbolo de un termómetro en la esquina superior derecha para cambiar entre Fahrenheit y Celsius.

Para configurar los sensores de temperatura y humedad:

1. Introduzca los valores para los umbrales mínimo, máximo, alto y bajo.
2. Introduzca los valores de **Histéresis**. (Consulte [Histéresis](#) para más detalles.)
3. Active la generación de alarmas que se desee.
4. Haga clic en **Aplicar**.

Histéresis. Este valor especifica cuánto debe retroceder la temperatura o la humedad desde un umbral para que desaparezca la violación del umbral.

- Para las violaciones del umbral de temperatura máxima y alta, el punto de eliminación es el umbral menos la histéresis.
- Para las violaciones del umbral de humedad mínima y baja, el punto de eliminación es el umbral más la histéresis.

Aumente el valor de la histéresis de temperatura o la histéresis de humedad para evitar múltiples alarmas si la temperatura o la humedad que ha provocado una violación luego vacila ligeramente arriba y abajo. Si el valor de la histéresis es demasiado bajo, dicho vacilar puede provocar y eliminar una violación de un umbral repetidamente.

Ejemplo de temperatura que sube pero vacila: El umbral de temperatura máxima es de 29,44 °C y la histéresis de temperatura es de 1,7 °C. La temperatura sube por encima de 29,44 °C, violando el umbral. Luego vacila entre 28,89 °C y 30,00 °C repetidamente, pero no tiene lugar ningún suceso de desaparición de violación ni ninguna nueva violación. Para que la violación existente desapareciese, la temperatura tendría que caer por debajo de 27,78 °C (1,7 °C menos del umbral).

Ejemplo de humedad que baja pero vacila: El umbral de humedad mínima es del 18%, y la histéresis de humedad es del 8%. La humedad cae por debajo del 18%, violando el umbral. Luego vacila entre el 24% y el 13% repetidamente, pero no tiene lugar ningún suceso de desaparición de violación ni ninguna nueva violación. Para que la violación existente desapareciese, la humedad tendría que subir por encima del 26% (un 8% más del umbral).

Configuración de las entradas de contacto seco

Ruta: Entorno > Entradas de contacto seco

A través de la página **Entradas de contacto seco**, se puede ver el estado actual de los contactos secos, y configurar los mismos.

Parámetro	Descripción
Nombre	Un nombre para este contacto de entrada. <i>Máximo</i> : 20 caracteres.
Estado de alarma	Normal si este contacto de entrada no está comunicando una alarma, o la gravedad de la alarma, si este contacto de entrada está comunicando una alarma
Estado	El estado actual de este contacto de entrada: Cerrado o Abierto .
Generación de alarmas	Permite activar o desactivar este contacto de entrada. Cuando está desactivada, el contacto no genera ninguna alarma ni siquiera cuando está en la posición anormal
Estado normal	El estado normal (sin alarmas) de este contacto de entrada: Cerrado o Abierto .

Registros

The screenshot displays the Dell Managed Rack PDU web interface. At the top, there are navigation tabs: Home, Device Manager, Environment, Logs, and Administration. A 'No Alarms' indicator is visible in the top right corner. On the left side, there is a sidebar menu with categories: Events (log, reverse lookup, size), Data (log, graphing, interval, rotation, size), and Syslog (servers, settings, test). The main content area is titled 'Event Log Filtering' and includes a form for filtering events. The 'Event Time' section has two radio buttons: 'Last' (selected) with a dropdown set to '2 days', and 'From' with date and time pickers for '10/23/2010 20:33' and '10/25/2010 20:33'. Below the form are buttons for 'Apply', 'Clear Log', 'Filter Log', and 'Launch Log in New Window'. The 'Event Log' section contains a table with columns 'Date', 'Time', and 'Event'. The table lists several events from 10/25/2010, including user logins, sensor connections, and outlet status changes. At the bottom of the interface, there are links for 'Link 1 | Link 2 | Link 3', the text 'Managed Rack PDU', and the Dell logo.

Home Device Manager Environment **Logs** Administration

No Alarms

Events

- log
- reverse lookup
- size

Data

- log
- graphing
- interval
- rotation
- size

Syslog

- servers
- settings
- test

Event Log Filtering

Event Time: Last

From to

Event Log

Date	Time	Event
10/25/2010	20:27:48	System: Web user 'admin' logged in from 10.218.116.102.
10/25/2010	20:25:04	Managed Rack PDU: Sensor connected. Temperature/Humidity Sensor type.
10/25/2010	20:18:12	System: Web user 'admin' logged out from 10.218.116.102.
10/25/2010	20:07:50	System: Web user 'admin' logged in from 10.218.116.102.
10/25/2010	19:56:28	System: Web user 'admin' logged out from 10.218.116.102.
10/25/2010	19:45:54	Managed Rack PDU: Outlet #2 (Outlet 2) off.
10/25/2010	19:45:54	Managed Rack PDU: Outlet #1 (Outlet 1) off.
10/25/2010	19:45:31	System: Configuration change. Event log web display time selection.
10/25/2010	19:45:18	System: Set Time.
10/25/2010	19:45:25	System: Set Date.

Link 1 | Link 2 | Link 3

Managed Rack PDU

Uso de los registros de sucesos y de datos

Registro de sucesos

Ruta: Registros > Sucesos > opciones

Se puede ver, filtrar o eliminar el registro de sucesos. De manera predeterminada, el registro muestra todos los sucesos registrados durante los dos últimos días por orden cronológico inverso.

Para obtener listas de todos los sucesos configurables y su configuración actual, seleccione la ficha **Administración, Notificación** en la barra de menú superior, y **por suceso** bajo **Acciones de sucesos** en el menú de navegación izquierdo.



Consulte [Configuración por suceso](#).

Para mostrar el registro de sucesos (Registros > Sucesos > registro):

- De manera predeterminada, el registro de sucesos se ve como una página de la interfaz Web. El suceso más reciente se registra en la página 1. En la barra de navegación debajo del registro:
 - Haga clic en un número de página para abrir una página específica del registro.
 - Haga clic en **Anterior** o **Siguiente** para ver los sucesos registrados inmediatamente antes o después de los sucesos listados en la página abierta.
 - Haga clic en << para volver a la primera página o en >> para ver la última página del registro.
- Para ver los sucesos listados en una página, haga clic en **Iniciar registro en nueva ventana** desde la página de registro de sucesos para mostrar una vista de pantalla completa del registro.



En las opciones de su explorador, debe estar activado JavaScript® para que pueda utilizar el botón **Iniciar registro en nueva ventana**.



También se puede utilizar FTP o Secure CoPy (SCP) para ver el registro de sucesos. Consulte [Cómo utilizar FTP o SCP para recuperar archivos de registro](#).

Para filtrar el registro (Registros > Sucesos > registro):

- **Filtrado del registro por fecha y hora:** Para mostrar el registro de sucesos entero o para cambiar el número de días o semanas del cual el registro muestra los sucesos más recientes, seleccione **Últimos**. Seleccione un periodo de tiempo en el menú desplegable, luego haga clic en **Aplicar**. La configuración de filtrado se guarda hasta que se reinicie la PDU de Rack.

Para mostrar los sucesos registrados durante un intervalo de tiempo específico, seleccione **Desde**. Especifique la fecha y hora (utilizando el formato de reloj de 24 horas) inicial y final del periodo de tiempo del cual desea mostrar los sucesos y a continuación haga clic en **Aplicar**. La configuración de filtrado se guarda hasta que se reinicie la PDU de Rack.

- **Filtrado del registro por suceso:** Para especificar los sucesos que se muestran en el registro, haga clic en **Filtro de registro**. Quite la marca de la casilla de verificación de una categoría de sucesos o nivel de gravedad de alarma para retirarla de la vista. El texto en la esquina superior derecha de la página de registro de sucesos indica que está activo un filtro.

Como Administrador, haga clic en **Guardar como predeterminado** para guardar este filtro como vista predeterminada del registro para todos los usuarios. Si no se hace clic en **Guardar como predeterminado**, el filtro está activo hasta que se quite o hasta que se reinicie la PDU de Rack.

Para quitar un filtro activo, haga clic en **Filtro de registro** y a continuación en **Borrar filtro (Mostrar todo)**.



Los sucesos se procesan por el filtro utilizando lógica **OR** (disyuntiva).

- Los sucesos que no se seleccionan en la lista de **Filtrar por gravedad** no se muestran nunca en el registro de sucesos filtrado, aunque el suceso se dé en una categoría que se haya seleccionado en la lista de **Filtrar por categoría**.
- Los sucesos que no se seleccionan en la lista de **Filtrar por categoría** no se muestran nunca en el registro de sucesos filtrado, aunque dispositivos en esa categoría entren en un estado de alarma que se haya seleccionado en la lista de **Filtrar por gravedad**.

Para eliminar el registro (Registros > Sucesos > registro):

Para eliminar todos los sucesos registrados en el registro, haga clic en **Borrar registro** en la página Web que muestra el registro. Los sucesos eliminados no se pueden recuperar.



Para desactivar el registro de sucesos basado en su nivel de gravedad asignado o la categoría de suceso, véase [Configuración por suceso](#).

Para configurar búsqueda inversa (Registros > Sucesos > búsqueda inversa):

La búsqueda inversa está desactivada de forma predeterminada. Active esta función a menos que no tenga ningún servidor DNS configurado o tenga un rendimiento de red deficiente debido a un tráfico de red denso.

Con la búsqueda inversa activada, cuando se produce un suceso relacionado con la red, se registran en el registro de sucesos tanto la dirección IP como el nombre de dominio del dispositivo en red asociado con el suceso. Si no existe ninguna entrada de nombre de dominio para el dispositivo, sólo se registra con el suceso la dirección IP. Como los nombres de dominio generalmente cambian menos frecuentemente que las direcciones IP, la activación de la búsqueda inversa puede mejorar la capacidad para identificar las direcciones de dispositivos en red que estén provocando sucesos.

Para cambiar el tamaño del registro de sucesos (Registros > Sucesos > tamaño):

De manera predeterminada, el registro de sucesos almacena 400 sucesos. Se puede cambiar el número de sucesos que almacena el registro. Cuando se cambia el tamaño del registro de sucesos, se borran todas las entradas existentes del registro. Para evitar perder datos del registro, utilice FTP o SCP para recuperar el registro antes de introducir un nuevo valor en el campo **Tamaño de registro de sucesos**.



Consulte [Cómo utilizar FTP o SCP para recuperar archivos de registro](#).

Cuando el registro está lleno, se borran las entradas más antiguas.

Registro de datos

Ruta: Registros > Datos > opciones

El registro de datos registra la corriente y la potencia del dispositivo y las fases (en una PDU de Rack trifásica), según corresponda, así como la temperatura y la humedad y los datos de los contactos secos en el intervalo de tiempo especificado. Cada entrada se lista por la fecha y hora en que se han registrado los datos.

Para mostrar el registro de sucesos (Registros > Datos > registro):

- De manera predeterminada, el registro de datos se ve como una página de la interfaz Web. El dato más reciente se registra en la página 1. En el menú de navegación debajo del registro:
 - Haga clic en un número de página para abrir una página específica del registro.
 - Haga clic en **Anterior** o **Siguiente** para ver los datos registrados inmediatamente antes o después de los datos listados en la página abierta.
 - Haga clic en << para volver a la primera página del registro o en >> para ver la última página del mismo.
- Para ver los datos listados en una página, haga clic en **Iniciar registro en nueva ventana** desde la página de registro de datos para mostrar una vista de pantalla completa del registro.



En las opciones de su explorador debe estar activado JavaScript para que pueda utilizar el botón **Iniciar registro en nueva ventana**.



Otra posibilidad es utilizar FTP o SCP para ver el registro de datos. Consulte [Cómo utilizar FTP o SCP para recuperar archivos de registro](#).

Para filtrar el registro por fecha u hora (Registros > Datos > registro):

Para mostrar el registro de datos entero o para cambiar el número de días o semanas del cual el registro muestra los sucesos más recientes, seleccione **Últimos**.

Seleccione un periodo de tiempo en el menú desplegable, luego haga clic en **Aplicar**. La configuración de filtrado se guarda hasta que se reinicie el dispositivo.

Para mostrar los datos registrados durante un intervalo de tiempo específico, seleccione **Desde**. Especifique la fecha y hora (utilizando el formato de reloj de 24 horas) inicial y final del periodo de tiempo del cual desea mostrar los datos y a continuación haga clic en **Aplicar**. La configuración de filtrado se guarda hasta que se reinicie el dispositivo.

Para borrar el registro de datos:

Para borrar todos los datos registrados en el registro, haga clic en **Borrar registro de datos** en la página Web que muestra el registro. Los datos borrados no se pueden recuperar.

Para establecer el intervalo de recogida de datos (Registros > Datos > intervalo):

Defina, en el parámetro **Intervalo de registro**, la frecuencia con la que se muestrean y se almacenan los datos en el registro de datos, y vea el cálculo de los días de datos que puede almacenar el registro, basándose en el intervalo que haya seleccionado. Cuando el registro está lleno, se borran las entradas más antiguas. Para evitar el borrado automático de los datos más antiguos, active y configure la rotación de registro de datos, que se describe en la próxima sección.

Para configurar la rotación de registro de datos (Registros > Datos > rotación):

Permite establecer un depósito del registro de datos protegido por contraseña en un servidor FTP especificado. La activación de la rotación hace que el contenido del registro de datos se añada al archivo que se especifica por nombre y ubicación. Las actualizaciones de este archivo tienen lugar a los intervalos de carga que se especifican.

Parámetro	Descripción
Rotación de registro de datos	Permite activar o desactivar (la opción predeterminada) la rotación de registro de datos.
Dirección del servidor FTP	La ubicación del servidor FTP en el que se almacena el depósito de datos.
Nombre de usuario	El nombre de usuario que se requiere para enviar datos al archivo de depósito. Este usuario debe estar configurado para que tenga acceso de lectura y escritura al archivo de depósito de datos y al directorio (carpeta) en el que está almacenado.
Contraseña	La contraseña que se requiere para enviar datos al archivo de depósito.
Ruta del archivo	La ruta hasta el archivo de depósito.
Nombre de archivo	El nombre del archivo de depósito (archivo de texto ASCII).
Retardo X horas entre cargas.	El número de horas entre las cargas de datos en el archivo.
Cargar cada X minutos	El número de minutos entre los intentos de cargar datos en el archivo después de un fallo de carga.
Hasta X veces	El máximo número de veces que se intentará la carga después de un fallo inicial.
Hasta que la carga sea correcta	Se intenta cargar el archivo hasta que se haya completado la transferencia.

Para cambiar el tamaño del registro de datos (Registros > Datos > tamaño):

De manera predeterminada, el registro de datos almacena 1000 registros. Se puede cambiar el número de registros que almacena el registro. Cuando se cambia el tamaño del registro de datos, se borran todas las entradas existentes del registro. Para evitar perder registros, utilice FTP o SCP para recuperar el registro antes de introducir un nuevo valor en el campo **Tamaño de registro de datos**.



Consulte [Cómo utilizar FTP o SCP para recuperar archivos de registro](#).

Cuando el registro está lleno, se borran las entradas más viejas.

Cómo utilizar FTP o SCP para recuperar archivos de registro

Un Administrador o un Usuario de dispositivo puede utilizar FTP o SCP para recuperar un archivo de registro de sucesos (*event.txt*) o un archivo de registro de datos (*data.txt*) delimitado por tabulaciones e importarlo en una hoja de cálculo.

- El archivo informa de todos los sucesos o datos registrados desde la última vez que el registro se borró o (en el caso del registro de datos) se truncó debido a que alcanzó el máximo tamaño.
- El archivo incluye información que no muestra el registro de sucesos ni el registro de datos.
 - La versión del formato del archivo (primer campo).
 - La fecha y hora en que se recuperó el archivo
 - Los valores de **Nombre**, **Contacto** y **Ubicación** y la dirección IP de la PDU de Rack
 - El **Código de suceso**, único, de cada suceso registrado (sólo en el archivo *event.txt*)



La PDU de Rack utiliza años de cuatro dígitos para las entradas del registro. Es posible que tenga que seleccionar un formato de fecha de cuatro dígitos en su aplicación de hoja de cálculo para mostrar los cuatro dígitos.

Si está utilizando los protocolos de seguridad basados en cifrado para su sistema, utilice Secure CoPy (SCP) para recuperar el archivo de registro.

Si está utilizando métodos de autenticación no cifrados para la seguridad de su sistema, utilice FTP para recuperar el archivo de registro.



Consulte [Apéndice B: Manual de seguridad](#) para obtener información sobre los protocolos y métodos disponibles para establecer el tipo de seguridad que necesite.

Para utilizar SCP para recuperar los archivos. Para utilizar SCP para recuperar el archivo *event.txt*, use el comando siguiente:

```
scp nombreusuario@nombredehost_o_dirección_ip:event.txt ./event.txt
```

Para utilizar SCP para recuperar el archivo *data.txt*, use el comando siguiente:

```
scp nombreusuario@nombredehost_o_dirección_ip:data.txt ./data.txt
```

Para utilizar FTP para recuperar los archivos. Para utilizar FTP para recuperar el archivo *event.txt* o *data.txt*:

1. En un indicador de comando, escriba `ftp` y la dirección IP de la PDU de Rack, y pulse INTRO.

Si el valor de **Puerto** en la opción **Servidor FTP** (establecido a través del menú **Red** de la ficha **Administración**) se ha cambiado respecto a su valor predeterminado (**21**), debe utilizar el valor no predeterminado en el comando FTP. En los clientes FTP Windows, utilice el siguiente comando, incluidos los espacios. (En algunos clientes FTP, se debe utilizar dos puntos en vez de un espacio entre la dirección IP y el número de puerto.)

```
ftp>open dirección_ip número_de_puerto
```



Para establecer un valor de puerto no predeterminado para mejorar la seguridad del servidor FTP, consulte [Servidor FTP](#). Se puede especificar cualquier puerto del 5001 al 32768.

2. Use el **Nombre de usuario** y la **Contraseña** sensibles a mayúsculas y minúsculas de Administrador o Usuario de dispositivo para iniciar una sesión. Para Administrador, **admin** es el valor predeterminado tanto para **Nombre de usuario** como para **Contraseña**. Para el Usuario de dispositivo, los valores predeterminados son **device** para **Nombre de usuario** y para **Contraseña**.
3. Utilice el comando **get** para transmitir el texto de un registro a su unidad de disco local.

```
ftp>get event.txt
```

```
o
```

```
ftp>get data.txt
```

4. Escriba `quit` en el indicador `ftp>` para salir de FTP.

Administración: Seguridad

Home Device Manager Environment **Logs** Administration

Security Network Notification General ✓ No Alarms

Local Users

- administrator
- device
- read-only

Remote Users

- authentication
- RADIUS

Auto Log Off

Administrator

User Name:

Current Password:

New Password:

Confirm Password:

Link 1 | Link 2 | Link 3 Managed Rack PDU **DELL**

Usuarios locales

Configuración del acceso de usuario

Ruta: Administración > Seguridad > Usuarios locales > opciones

La cuenta de usuario de Administrador siempre tiene acceso a la PDU de Rack.

Las cuentas de Usuario de dispositivo y de Usuario de sólo lectura están activadas de manera predeterminada. Para desactivar las cuentas de Usuario de dispositivo y de Usuario de sólo lectura, seleccione la cuenta de usuario en el menú de navegación izquierdo, y a continuación quite la marca de la casilla de verificación **Activar**.

El nombre de usuario y la contraseña sensibles a mayúsculas y minúsculas para cada tipo de cuenta se establecen de la misma forma. La longitud máxima es de 64 caracteres para un nombre de usuario y de 64 caracteres para una contraseña. Las contraseñas en blanco (contraseñas sin caracteres) no están permitidas.



Para obtener información sobre los permisos concedidos a cada tipo de cuenta, véase [Tipos de cuentas de usuario](#).



Para las cuentas de usuario de tomas de corriente no hay nombre de usuario ni contraseña predeterminados. Un Administrador debe definir el nombre de usuario y contraseña y otras características de una cuenta para un Usuario de tomas de corriente. Consulte [Configuración de un usuario de tomas de corriente](#).

Tipo de cuenta	Nombre de usuario predeterminado	Contraseña predeterminada	Acceso permitido
Administrador	admin	admin	Interfaz Web e interfaz de línea de comandos
Usuario de dispositivo	device	device	
Usuario de sólo lectura	readonly	readonly	Sólo Interfaz Web

Usuarios remotos

Autenticación

Ruta: Administración > Seguridad > Usuarios remotos > Método de autenticación

Utilice esta opción para seleccionar la manera de administrar el acceso remoto a la PDU de Rack.



Para obtener información acerca de la autenticación local (no utilizando la autenticación centralizada de un servidor RADIUS), véase el [Apéndice B: Manual de seguridad](#).

La PDU de Rack admite las funciones de autenticación y autorización de RADIUS (Remote Authentication Dial-In User Service).

- Cuando un usuario accede a la PDU de Rack o a otro dispositivo habilitado para red que tiene RADIUS activado, se envía una solicitud de autenticación al servidor RADIUS para determinar el nivel de permiso del usuario.
- Los nombres de usuario RADIUS que se utilizan con la PDU de Rack están limitados a 32 caracteres.

Seleccione uno de los métodos siguientes:

- **Sólo autenticación local:** RADIUS se desactiva. La autenticación local se activa.
- **RADIUS, después autenticación local:** Se activa RADIUS y la autenticación local. La autenticación se solicita primero al servidor RADIUS. Si el servidor RADIUS no responde, se usa autenticación local.
- **RADIUS sólo:** RADIUS se activa. La autenticación local se desactiva.



Si está seleccionado **RADIUS sólo**, y el servidor RADIUS no está disponible, está identificado incorrectamente o está configurado incorrectamente, el acceso remoto no está disponible para ningún usuario. Debe utilizar una conexión serie con la interfaz de línea de comandos y cambiar el valor de **access** a **local** o **radiusLocal** para volver a obtener acceso. Por ejemplo, el comando para cambiar el valor de access a **local** sería:

```
radius -a local
```

RADIUS

Ruta: Administración > Seguridad > Usuarios remotos > RADIUS

Utilice esta opción para realizar las siguientes acciones:

- Listar los servidores RADIUS (un máximo de dos) disponibles para la PDU de Rack y el tiempo de espera para cada uno de ellos.
- Hacer clic en un vínculo, y configurar los parámetros para la autenticación por un nuevo servidor RADIUS.
- Hacer clic en un servidor RADIUS listado para mostrar y modificar sus parámetros.

Parámetro RADIUS	Definición
Servidor RADIUS	El nombre de servidor o la dirección IP (IPv4 o IPv6) del servidor RADIUS. Haga clic en un vínculo para configurar el servidor. NOTA: Los servidores RADIUS utilizan el puerto 1812 de manera predeterminada para autenticar a los usuarios. Para utilizar un puerto diferente, añada dos puntos seguido del número del nuevo puerto al final del nombre o dirección IP del servidor RADIUS.
Secreto	El secreto compartido entre el servidor RADIUS y la PDU de Rack.
Tiempo de espera	El tiempo en segundos que la PDU de Rack espera a una respuesta del servidor RADIUS.
Probar configuración	Introduzca el nombre de usuario y la contraseña de Administrador para probar la ruta del servidor RADIUS que ha configurado.
Omitir prueba y aplicar	No probar la ruta del servidor RADIUS.

Configuración del servidor RADIUS

Resumen del procedimiento de configuración

Debe configurar su servidor RADIUS para que funcione con la PDU de Rack.



Para obtener ejemplos del archivo de usuarios RADIUS con Vendor Specific Attributes (atributos específicos del vendedor) y un ejemplo de una entrada del archivo de diccionario del servidor RADIUS, véase el [Apéndice B: Manual de seguridad](#).

1. Añada la dirección IP de la PDU de Rack a la lista (archivo) de clientes del servidor RADIUS.
2. Los usuarios deben configurarse con atributos de tipo de servicio a menos que se definan atributos específicos del vendedor. Si no se configuran atributos de tipo de servicio, los usuarios tendrán acceso de sólo lectura (en la interfaz Web sólo).



Véase la documentación del servidor RADIUS para obtener información acerca del archivo de usuarios RADIUS, y vea un ejemplo en el [Apéndice B: Manual de seguridad](#).

3. Se pueden utilizar VSAs (Vendor Specific Attributes) en vez de los atributos de tipo de servicio proporcionados por el servidor RADIUS. Los VSA requieren una entrada en el diccionario y un archivo de usuarios RADIUS. En el archivo de diccionario, defina los nombres para las palabras clave ATTRIBUTE y VALUE, pero no para los valores numéricos. Si se cambian los valores numéricos, la autenticación y autorización RADIUS fallará. Los VSA tienen prioridad sobre los atributos RADIUS estándar.

Configuración de un servidor RADIUS en UNIX® con contraseñas shadow

Si se usan archivos de contraseñas shadow UNIX (/etc/passwd) con los archivos de diccionario RADIUS, se pueden utilizar los dos métodos siguientes para autenticar a los usuarios:

- Si todos los usuarios UNIX tienen privilegios administrativos, añada lo siguiente al archivo de “usuarios” RADIUS. Para permitir sólo Usuarios de dispositivo, cambie DELL-Service-Type a Device.

```
DEFAULT      Auth-Type = System
              DELL-Service-Type = Admin
```

- Añada nombres de usuario y atributos al archivo de “usuarios” RADIUS, y verifique la contraseña frente a /etc/passwd. El ejemplo siguiente es para los usuarios **bconners** y **thawk**:

```
bconners     Auth-Type = System
              DELL-Service-Type = Admin

thawk        Auth-Type = System
              DELL-Service-Type = Device
```

Servidores RADIUS admitidos

Se admiten FreeRADIUS y Microsoft IAS 2003. Es posible que otras aplicaciones RADIUS que se encuentran corrientemente funcionen, pero no se han comprobado totalmente.

Tiempo de espera por inactividad

Ruta: Administración > Seguridad > Cierre de sesión automático

Utilice esta opción para configurar el tiempo (3 minutos de manera predeterminada) que espera el sistema antes de cerrar la sesión de un usuario inactivo. Si se cambia este valor, se debe cerrar la sesión para que el cambio surta efecto.



Este temporizador continúa funcionando si un usuario cierra la ventana del explorador sin cerrar primero la sesión haciendo clic en **Cerrar sesión** en la parte superior derecha. Como se considera que ese usuario todavía está en una sesión, no puede iniciar una sesión ningún usuario hasta que expire el tiempo especificado como **Minutos de inactividad**. Por ejemplo, con el valor predeterminado de **Minutos de inactividad**, si un usuario cierra la ventana del explorador sin cerrar la sesión, no puede iniciar una sesión ningún usuario durante 3 minutos.

Administración: Notificación

The screenshot displays the Dell Managed Rack PDU Administration web interface. The top navigation bar includes tabs for Home, Device Manager, Environment, Logs, and Administration. The Administration tab is active, and the sub-tab 'Notification' is selected. A 'No Alarms' indicator is visible in the top right corner. The left sidebar contains a menu with sections: Event Actions (with sub-items 'by event' and 'by group'), E-mail (with sub-items 'server', 'recipients', and 'test'), and SNMP Traps (with sub-items 'trap receivers' and 'test'). The main content area is titled 'Event Actions for Individual Events' and contains a text instruction: 'To list all events in a main category by severity level, click the main category name. To list all events in a sub-category by severity level, click the sub-category name.' Below this instruction, there are two columns of links. The 'Device' column includes links for Communications, Device, Phase Load, Outlet Load, Outlet Control, and Sensor. The 'System' column includes links for Mass Configuration and Security. At the bottom of the interface, there are links for Link 1, Link 2, and Link 3, and the Dell logo.

Acciones de sucesos

Ruta: Administración > Notificación > Acciones de sucesos > opciones

Tipos de notificación

Se puede configurar que tengan lugar acciones de sucesos en respuesta a un suceso o un grupo de sucesos. Estas acciones notifican a los usuarios del suceso en cualquiera de las formas siguientes:

- Notificación activa y automática. Se contacta directamente con los usuarios o dispositivos de supervisión especificados.
 - Notificación por correo electrónico
 - Capturas de SNMP
 - Notificación Syslog
- Notificación indirecta
 - Registro de sucesos. Si no se configura ninguna notificación directa, los usuarios deben comprobar el registro para determinar los sucesos que han tenido lugar
 -  También puede registrar datos de rendimiento del sistema para usarlos para la supervisión del dispositivo. Véase [Registro de datos](#) para obtener información sobre cómo configurar y usar esta opción de registro de datos.
 - Consultas (operaciones SNMP GET)
 -  Para obtener más información, consulte la sección [SNMP](#). SNMP permite que un NMS realice consultas informativas. En SNMPv1, que no cifra los datos antes de la transmisión, la configuración del tipo de acceso SNMP más restrictivo, READ (LECTURA), permite las consultas informativas sin el riesgo de permitir cambios de configuración remotos.

Configuración de las acciones de sucesos

Parámetros de notificación. Para los sucesos que tienen un suceso de resolución asociado, también se pueden configurar los siguientes parámetros cuando se configuran los sucesos individualmente o por grupo, como se describe en las dos secciones siguientes. Para acceder a los parámetros, haga clic en el nombre del receptor o destinatario.

Parámetro	Descripción
Retardar x tiempo antes de enviar	Si persiste el suceso durante el tiempo especificado, se envía una notificación. Si desaparece la condición antes de que expire el tiempo, no se envía ninguna notificación.
Repetir a intervalos de x tiempo	La notificación se envía a los intervalos especificados (p. ej., cada 2 minutos).
Hasta x veces	Durante un suceso activo, la notificación se repite este número de veces.
Hasta que la condición desaparezca	La notificación se envía repetidamente hasta que la condición desaparece o se resuelve.

Configuración por suceso. Para definir acciones de sucesos para un suceso individual:

1. Seleccione la ficha **Administración, Notificación** en la barra de menú superior, y **por suceso** bajo **Acciones de sucesos** en el menú de navegación izquierdo.
2. En la lista de sucesos, examine las columnas marcadas para ver si la acción que desea ya está configurada. (De manera predeterminada, el registro está configurado para todos los sucesos.)

3. Para ver o cambiar la configuración actual, por ejemplo los destinatarios a los que se debe notificar por correo electrónico o buscar personas, o los Sistemas de administración de red (NMS) a los que se debe notificar mediante capturas SNMP, haga clic en el nombre del suceso.



Si no está configurado ningún servidor Syslog, los elementos relacionados con la configuración Syslog no se muestran.



Cuando se ven los detalles de la configuración de un suceso, se puede cambiar la configuración, activar o desactivar el registro de sucesos o Syslog, y desactivar la notificación para destinatarios de correo electrónico o receptores de capturas específicos, pero no se puede añadir ni quitar destinatarios ni receptores. Para añadir o quitar destinatarios o receptores, véase lo siguiente:

- [Identificación de los servidores Syslog](#)
- [Destinatarios de correo electrónico](#)
- [Receptores de capturas](#)

Configuración por grupo. Para configurar un grupo de sucesos simultáneamente:

1. Seleccione la ficha **Administración, Notificación** en la barra de menú superior, y **por grupo** bajo **Acciones de sucesos** en el menú de navegación izquierdo.
2. Elija cómo agrupar los sucesos para su configuración:
 - Elija **Agrupados por gravedad**, y a continuación seleccione todos los sucesos de uno o más niveles de gravedad. No se puede cambiar la gravedad de un suceso.
 - Elija **Agrupados por categoría**, y a continuación seleccione todos los sucesos de una o más categorías predefinidas.

3. Haga clic en **Siguiente>>** para desplazarse de una página a otra para hacer lo siguiente:
 - a. Seleccione acciones de sucesos para el grupo de sucesos.
 - Para elegir cualquier acción excepto **Registro** (la acción predeterminada), primero debe tener configurado por lo menos un destinatario o receptor pertinente.
 - Si elige **Registro** y ha configurado un servidor Syslog, seleccione **Registro de sucesos** o **Syslog** (o ambos) en la página siguiente.
 - b. Seleccione si deja activada para este grupo de sucesos la acción de suceso recién configurada o desactiva la acción.

Notificación activa, automática y directa

Notificación por correo electrónico

Información general de la configuración. Utilice Simple Mail Transfer Protocol (SMTP) para enviar correo electrónico a hasta cuatro destinatarios cuando tenga lugar un suceso.

Para usar la función Correo electrónico, debe definir los siguientes parámetros:

- La dirección IP de los servidores DNS (Domain Name System) primario y, opcionalmente, secundario



Consulte [DNS](#).

- La dirección IP o nombre DNS del **Servidor SMTP** y la **Dirección de remitente**



Consulte [SMTP](#).

- La dirección de correo electrónico de un máximo de cuatro destinatarios



Consulte [Destinatarios de correo electrónico](#).



Se puede utilizar el valor de **Dirección de destinatario** de la opción **destinatarios** para enviar correo electrónico a un buscaperonas de texto.

SMTP.

Ruta: Administración > Notificación > Correo electrónico > servidor

Parámetro	Descripción
Servidor SMTP local	La dirección IPv4/ IPv6 o nombre DNS del servidor SMTP local. NOTA: Esta definición sólo se requiere cuando Servidor SMTP está puesto en Local . Consulte Destinatarios de correo electrónico .
Dirección de remitente	El contenido del campo From (De) en los mensajes de correo electrónico enviados por la PDU de Rack: <ul style="list-style-type: none">• En el formato <i>usuario@ [dirección_IP]</i> (si se especifica una dirección IP como Servidor SMTP local)• En el formato <i>usuario@dominio</i> (si está configurado un DNS y el nombre DNS se especifica como Servidor SMTP local) en los mensajes de correo electrónico. NOTA: El Servidor SMTP local puede requerir que se utilice una cuenta de usuario válida en el servidor para este parámetro. Véase la documentación del servidor.

Destinatarios de correo electrónico.

Ruta: Administración > Notificación > Correo electrónico > destinatarios

Identifique hasta cuatro destinatarios de correo electrónico.

Parámetro	Descripción
Dirección de destinatario	<p>El nombre de usuario y de dominio del destinatario. Para utilizar el correo electrónico para enviar mensajes a un buscpersonas, utilice la dirección de correo electrónico de la cuenta de puerta de enlace del buscpersonas del destinatario (por ejemplo, myacct100@skytel.com). La puerta de enlace del buscpersonas generará la página.</p> <p>Para evitar la búsqueda DNS de la dirección IP del servidor de correo, utilice la dirección IP entre corchetes en vez del nombre de dominio de correo electrónico; p. ej., utilice jsmith@[xxx.xxx.x.xxx] en vez de jsmith@company.com. Esto es útil cuando las búsquedas DNS no funcionan correctamente.</p> <p>NOTA: El buscpersonas del destinatario debe poder utilizar mensajería de texto.</p>
Generación de correo electrónico	Activa (de manera predeterminada) o desactiva el envío de correo electrónico al destinatario.

Parámetro	Descripción
Servidor SMTP	<p>Seleccione uno de los métodos siguientes para enrutar el correo electrónico:</p> <ul style="list-style-type: none"> • Local: A través del servidor SMTP de la PDU de Rack. Este valor (recomendado) asegura que se envíe el correo electrónico antes del tiempo de espera de 20 segundos de la PDU de Rack, y, si es necesario, se reintente varias veces. Además realice una de las siguientes acciones: <ul style="list-style-type: none"> • Active el reenvío en el servidor SMTP de la PDU de Rack para que pueda enrutar el correo electrónico a servidores SMTP externos. Normalmente, los servidores SMTP no están configurados para reenviar el correo electrónico. Consulte con el administrador de su servidor SMTP antes de cambiar su configuración para permitir el reenvío. • Establezca una cuenta de correo electrónico especial para que la PDU de Rack reenvíe el correo electrónico a una cuenta de correo externa. • Destinatario: Directamente al servidor SMTP del destinatario. Con este valor, la PDU de Rack intenta enviar el correo electrónico sólo una vez. En un servidor SMTP remoto ocupado, el tiempo de espera puede impedir que se envíe parte del correo. <p>Cuando el destinatario utiliza el servidor SMTP de la PDU de Rack, este valor no tiene ningún efecto.</p>
Formato	<p>El formato largo contiene Nombre, Ubicación, Contacto, dirección IP, número de serie del dispositivo, fecha y hora, código de suceso y descripción del suceso. El formato corto proporciona sólo la descripción del suceso.</p>
Nombre de usuario Contraseña Confirmar contraseña	<p>Si su servidor de correo requiere autenticación, escriba su nombre de usuario y contraseña aquí. Esto realiza una autenticación simple, no SSI.</p>

Prueba del correo electrónico.

Ruta: Administración > Notificación > Correo electrónico > prueba

Envíe un mensaje de prueba a un destinatario configurado.

Capturas de SNMP

Receptores de capturas.

Ruta: Administración > Notificación > Capturas de SNMP > receptores de capturas

Permite ver los receptores de capturas por Nombre de host/IP NMS. Se puede configurar hasta seis receptores de capturas.

- Para configurar un nuevo receptor de capturas, haga clic en **Agregar receptor de capturas**.
- Para modificar o eliminar un receptor de capturas, primero haga clic en su dirección IP o nombre de host para acceder a su configuración. (Si se elimina un receptor de capturas, todos los parámetros de notificación configurados bajo acciones de sucesos para el receptor de capturas eliminado se ponen en sus valores predeterminados.)
- Para especificar el tipo de captura para un receptor de capturas, seleccione el botón de radio SNMPv1 o SNMPv3. Para que un NMS reciba ambos tipos de capturas, se deben configurar dos receptores de capturas para ese NMS, uno para cada tipo de capturas.

Ítem	Definición
Generación de capturas	Permite activar (el valor predeterminado) o desactivar la generación de capturas para este receptor de capturas.
Nombre de host/IP NMS	La dirección IPv4/ IPv6 o nombre de host de este receptor de capturas. El valor predeterminado, 0.0.0.0, deja el receptor de capturas sin definir.

Opción SNMPv1.

Elemento	Definición
Nombre de comunidad	El nombre (<code>public</code> de manera predeterminada) que se usa como identificador cuando se envían capturas SNMPv1 a este receptor de capturas.
Capturas de autenticación	Cuando esta opción está activada (el valor predeterminado), el NMS identificado por el valor de Nombre de host/IP NMS recibirá capturas de autenticación (capturas generadas por intentos no válidos de iniciar una sesión en este dispositivo). Para desactivar esa capacidad, quite la marca de la casilla de verificación.

Opción SNMPv3. Permite seleccionar el identificador del perfil de usuario para este receptor de capturas. (Para ver la configuración de los perfiles de usuario identificados por los nombres de usuario seleccionables aquí, elija **Red** en la barra de menú superior y **perfiles de usuario** bajo **SNMPv3** en el menú de navegación izquierdo.)



Véase **SNMPv3** para obtener información sobre la creación de perfiles de usuario y la selección de métodos de autenticación y cifrado.

Prueba de capturas SNMP

Ruta: Administración > Notificación > Capturas de SNMP > prueba

Resultado de la última prueba. El resultado de la prueba de capturas SNMP más reciente. Una prueba de capturas SNMP con éxito sólo verifica que se ha enviado una captura; no verifica que la captura haya sido recibida por el receptor de capturas seleccionado. Una prueba de capturas tiene éxito si se cumplen las siguientes condiciones:

- La versión de SNMP (SNMPv1 o SNMPv3) configurada para el receptor de capturas seleccionado está activada en este dispositivo.
- El receptor de capturas está activado.
- Si se ha seleccionado un nombre de host para la dirección de **Destinatario**, ese nombre de host se puede asignar a una dirección IP válida.

Hasta. Seleccione la dirección IP o nombre de host al cual se enviará una captura SNMP de prueba. Si no está configurado ningún receptor de capturas, se muestra un vínculo a la página de configuración de **Receptor de capturas**.

Syslog

Ruta: Registros > Syslog > opciones

La PDU de Rack puede enviar mensajes a hasta cuatro servidores Syslog cuando tiene lugar un suceso. Los servidores Syslog registran los sucesos que tienen lugar en los dispositivos de red en un registro que proporciona un registro centralizado de los sucesos.



Esta guía del usuario no describe en detalle Syslog ni sus valores de configuración. Véase **RFC3164** para obtener más información acerca de Syslog.

Identificación de los servidores Syslog.

Ruta: Registros > Syslog > servidores

Parámetro	Definición
Servidor Syslog	Utiliza direcciones IPv4/ IPv6 o nombres de host para identificar de uno a cuatro servidores para recibir los mensajes Syslog enviados por la PDU de Rack.
Puerto	El puerto del protocolo de datagrama de usuario (UDP) que utilizará la PDU de Rack para enviar los mensajes de Syslog. El valor predeterminado es 514 , el puerto UDP asignado a Syslog.
Protocolo	Permite elegir el idioma de los mensajes Syslog.

Configuración de Syslog.

Ruta: Registros > Syslog > configuración

Parámetro	Definición
Generación de mensajes	Activa (de manera predeterminada) o desactiva la función Syslog.
Código de instalación	Selecciona el código de instalación asignado a los mensajes de Syslog de la PDU de Rack (el valor predeterminado es Usuario). NOTA: Usuario es el valor que mejor define los mensajes Syslog enviados por la PDU de Rack. No cambie esta selección a menos que se lo aconseje el administrador de red o sistema Syslog.
Asignación de gravedad	Asigna cada nivel de gravedad de los sucesos de PDU de Rack o de entorno a prioridades Syslog disponibles. No debería necesitar cambiar las asignaciones. Las siguientes definiciones proceden de RFC3164: <ul style="list-style-type: none">• Emergencia: El sistema está inutilizable.• Alerta: Debe efectuarse una acción de forma inmediata.• Crítica: Condiciones críticas• Error: Condiciones de error• Advertencia: Condiciones de advertencia• Aviso: Condiciones normales pero significativas• Información: Mensajes informativos• Depuración: Mensajes de nivel de depuración A continuación se muestran los valores predeterminados de los parámetros de Prioridad local : <ul style="list-style-type: none">• Crítico se asigna a Crítico• Advertencia se asigna a Advertencia• Informativa se asigna a Información NOTA: Para desactivar los mensajes Syslog, véase Configuración de las acciones de sucesos .

Prueba de Syslog y ejemplo de formato.

Ruta: Registros > Syslog > prueba

Envía un mensaje de prueba a los servidores Syslog configurados mediante la opción **servidores**.

1. Seleccione una gravedad para asignarla al mensaje de prueba.
2. Defina el mensaje de prueba, de acuerdo con los campos de mensaje requeridos.
 - La prioridad (PRI): la prioridad Syslog asignada al suceso del mensaje, y el código de instalación de los mensajes enviados por la PDU de Rack.
 - La cabecera: un registro de hora y la dirección IP de la PDU de Rack.
 - La parte del mensaje (MSG):
 - El campo TAG, seguido de dos puntos y un espacio, identifica el tipo de suceso.
 - El campo CONTENT es el texto del suceso, seguido (opcionalmente) de un espacio y el código del suceso.

Por ejemplo, **Dell: Test Syslog** es válido.

Administración: Funciones de red

The screenshot displays the Dell Managed Rack PDU web interface. The top navigation bar includes 'Home', 'Device Manager', 'Environment', 'Logs', and 'Administration'. The 'Administration' tab is active, and the 'Network' sub-tab is selected. A 'No Alarms' indicator is visible in the top right corner. The left sidebar contains a tree view with categories: TCP/IP (ipv4 settings, ipv6 settings), Ping Response, Port Speed, DNS (configuration, test), Web (access, ssl certificate), Console (access, ssh host key), SNMPv1 (access, access control), SNMPv3 (access, user profiles, access control), and FTP server. The main content area is titled 'Web Access' and features three radio buttons for 'Access': 'Disable', 'Enable HTTP' (which is selected), and 'Enable HTTPS'. Below these are input fields for 'HTTP Port' (set to 80) and 'HTTPS Port' (set to 443), each with a range of values in brackets. 'Apply' and 'Cancel' buttons are located at the bottom of the configuration area. A note states: 'Note: Some configuration settings will require a reboot to activate.' The footer of the interface shows 'Link 1 | Link 2 | Link 3' on the left, 'Managed Rack PDU' in the center, and the 'DELL' logo on the right.

Configuración de TCP/IP y de la comunicación

Configuración de TCP/IP

Ruta: **Administración > Red > TCP/IP**

La opción **TCP/IP** del menú de navegación izquierdo, seleccionada de manera predeterminada cuando se elige **Red** en la barra de menú superior, muestra la dirección IPv4, máscara de subred, puerta de enlace predeterminada, dirección MAC y modo de inicio actuales de la PDU de Rack.



Para obtener información sobre las opciones de DHCP y DHCP, véase **RFC2131** y **RFC2132**.

Parámetro	Descripción
Activar	Active o desactive IPv4 con esta casilla de verificación.
Manual	Permite configurar IPv4 manualmente introduciendo la dirección IP, la máscara de subred y la puerta de enlace predeterminada.
<p>1. Generalmente no es necesario cambiar los valores predeterminados de estos tres parámetros en las páginas de configuración:</p> <ul style="list-style-type: none">•Clase de distribuidor: DELL•ID cliente: La dirección MAC de la PDU de Rack, que la identifica de manera única en la red de área local (LAN)•Clase de usuario: El nombre del módulo de firmware de aplicación	



Parámetro	Descripción
BOOTP	<p>Un servidor BOOTP proporciona los valores de TCP/IP. A intervalos de 32 segundos, la PDU de Rack solicita asignación de red a cualquier servidor BOOTP:</p> <ul style="list-style-type: none"> • Si la PDU de Rack recibe una respuesta válida, inicia los servicios de red. • Si la PDU de Rack encuentra un servidor BOOTP, pero la solicitud a ese servidor falla o excede el tiempo de espera, la PDU de Rack deja de solicitar valores de red hasta que se reinicia. • De manera predeterminada, si existe una configuración anterior de los parámetros de red, y la PDU de Rack no recibe ninguna respuesta válida a cinco solicitudes (la original y cuatro reintentos), utiliza la configuración anterior de los parámetros para permanecer accesible. <p>Haga clic en Siguiente>> para acceder a la página Configuración BOOTP para cambiar el número de reintentos o la acción que se debe realizar si fallan todos los reintentos¹:</p> <ul style="list-style-type: none"> • Nº máx. de reintentos: Introduzca el número de reintentos que tendrán lugar cuando no se reciba ninguna respuesta válida, o cero (0) para un número ilimitado de reintentos. • Si los reintentos fallan: Seleccione Utilizar configuración anterior (el valor predeterminado) o Detener solicitud BOOTP.
<p>1. Generalmente no es necesario cambiar los valores predeterminados de estos tres parámetros en las páginas de configuración:</p> <ul style="list-style-type: none"> • Clase de distribuidor: DELL • ID cliente: La dirección MAC de la PDU de Rack, que la identifica de manera única en la red de área local (LAN) • Clase de usuario: El nombre del módulo de firmware de aplicación 	

Parámetro	Descripción
DHCP	<p>El valor predeterminado. A intervalos de 32 segundos, la PDU de Rack solicita asignación de red a cualquier servidor DHCP:</p> <ul style="list-style-type: none">• Si la PDU de Rack recibe una respuesta válida, no necesita la cookie de distribuidor del servidor DHCP para aceptar el arrendamiento e iniciar los servicios de red.• Si la PDU de Rack encuentra un servidor DHCP, pero la solicitud a ese servidor falla o excede el tiempo de espera, deja de solicitar valores de red hasta que se reinicia¹.• Requerir cookie específica del distribuidor para aceptar la dirección de DHCP: Seleccionando esta casilla de verificación, se puede exigir que el servidor DHCP proporcione una cookie que suministra información a la PDU de Rack.
<p>1. Generalmente no es necesario cambiar los valores predeterminados de estos tres parámetros en las páginas de configuración:</p> <ul style="list-style-type: none">• Clase de distribuidor: DELL• ID cliente: La dirección MAC de la PDU de Rack, que la identifica de manera única en la red de área local (LAN)• Clase de usuario: El nombre del módulo de firmware de aplicación	

Opciones de respuesta de DHCP

Cada respuesta DHCP válida contiene opciones que proporcionan los valores de TCP/IP que necesita la PDU de Rack para funcionar en una red, y otra información que afecta al funcionamiento de la PDU de Rack.

Vendor Specific Information (opción 43). La PDU de Rack utiliza esta opción en una respuesta DHCP para determinar si la respuesta DHCP es válida. Esta opción contiene una opción específica en formato TAG/LEN/DATA, denominada la Cookie del distribuidor. Ésta está desactivada de manera predeterminada.

- **Cookie del distribuidor. Tag 1, Len 4, Data “1APC”**

La opción 43 comunica a la PDU de Rack que se ha configurado un servidor DHCP para las PDU de Rack Dell.

A continuación, en formato hexadecimal, se muestra un ejemplo de una opción “Vendor Specific Information” que contiene la cookie del distribuidor:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

Opciones de TCP/IP. La PDU de Rack utiliza las siguientes opciones en una respuesta DHCP válida para definir la configuración de TCP/IP. Todas estas opciones excepto la primera se describen en **RFC2132**.

- **IP Address** (del campo **yiaddr** de la respuesta DHCP, descrita en **RFC2131**): La dirección IP que el servidor DHCP arrienda a la PDU de Rack.
- **Subnet Mask** (opción 1): El valor de máscara de subred que necesita la PDU de Rack para funcionar en la red.
- **Router**, es decir, Default Gateway (opción 3): La dirección de la puerta de enlace predeterminada que necesita la PDU de Rack para funcionar en la red.
- **IP Address Lease Time** (opción 51): La duración del arrendamiento de la dirección IP a la PDU de Rack.
- **Renewal Time, T1** (opción 58): El tiempo que debe esperar la PDU de Rack después de que le sea asignado el arrendamiento de una dirección IP antes de que pueda solicitar una renovación de ese arrendamiento.

- **Rebinding Time, T2** (opción 59): El tiempo que debe esperar PDU de Rack después de que le sea asignado el arrendamiento de una dirección IP antes de que pueda intentar revincular ese arrendamiento.

Otras opciones. La PDU de Rack también usa estas opciones en una respuesta DHCP válida. Todas estas opciones excepto la última se describen en **RFC2132**.

- **Network Time Protocol Servers** (opción 42): Hasta dos servidores NTP (primario y secundario) que puede utilizar la PDU de Rack.
- **Time Offset** (opción 2): La desviación, en segundos, de la subred de la PDU de Rack de la Hora universal coordinada (UTC).
- **Domain Name Server** (opción 6): Hasta dos servidores DNS (primario y secundario) que puede utilizar la PDU de Rack.
- **Host Name** (opción 12): El nombre de host que utilizará la PDU de Rack (longitud máxima de 32 caracteres).
- **Domain Name** (opción 15): El nombre de dominio que utilizará la PDU de Rack (longitud máxima de 64 caracteres).
- **Boot File Name** (del campo **file** de la respuesta DHCP, descrita en **RFC2131**): La ruta de directorios completa a un archivo de configuración de usuario (.ini file) para descargarlo. El campo **siaddr** de la respuesta DHCP especifica la dirección IP del servidor del cual la PDU de Rack descargará el archivo .ini. Después de la descarga, la PDU de Rack utiliza el archivo .ini como un archivo de inicio para reconfigurar sus parámetros.

Ruta: Administración > Red > TCP/IP > configuración de IPv6

Parámetro	Descripción
Activar	Active o desactive IPv6 con esta casilla de verificación.
Manual	Permite configurar IPv6 manualmente introduciendo la dirección IP y la puerta de enlace predeterminada.
Configuración automática	Cuando la casilla de verificación Configuración automática está seleccionada, el sistema obtiene los prefijos de direccionamiento del router (si está disponible). Utiliza esos prefijos para configurar automáticamente las direcciones IPv6.



Parámetro	Descripción
Modo DHCPv6	<p>Controlado por router: La selección de esta opción significa que DHCPv6 es controlado por los indicadores Managed (M) y Other (O) recibidos en los anuncios de router IPv6. Cuando se recibe un anuncio de router, la Tarjeta de administración de red comprueba si están configurados los indicadores M y O. La Tarjeta de administración de red interpreta el estado de los “bits” M (Managed Address Configuration Flag) y O (Other Stateful Configuration Flag) en los siguientes casos:</p> <ul style="list-style-type: none"> • <i>Ninguno de los dos está configurado:</i> Indica que la red local no tiene infraestructura DHCPv6. La Tarjeta de administración de red utiliza los anuncios de router y la configuración manual para obtener las direcciones que no son de enlace local y otros valores. • <i>M, o M y O están configurados:</i> En esta situación, se produce una configuración de direcciones DHCPv6 completa. DHCPv6 se utiliza para obtener las direcciones Y otros valores de configuración. Esto se conoce como DHCPv6 stateful. Una vez que se ha recibido el indicador M, la configuración de direcciones DHCPv6 permanece en vigor hasta que se cierra la interfaz en cuestión. Eso ocurre aunque se reciban paquetes de anuncio de router subsiguientes en los que el indicador M no esté configurado. Si se recibe un indicador O primero y luego se recibe un indicador M posteriormente, la Tarjeta de administración de red realiza una configuración de direcciones completa a la recepción del indicador M • <i>Sólo O está configurado:</i> En esta situación, la Tarjeta de administración de red envía un paquete de solicitud de información DHCPv6. DHCPv6 se utilizará para configurar “otros” parámetros (como la ubicación de los servidores DNS), pero NO para proporcionar direcciones. Esto se conoce como DHCPv6 stateless. <p>Dirección y otros datos: Con este botón de radio seleccionado, DHCPv6 se utiliza para obtener direcciones Y otros valores de configuración. Esto se conoce como DHCPv6 stateful.</p> <p>Sólo información que no sea de dirección: Con este botón de radio seleccionado, DHCPv6 se utilizará para configurar “otros” parámetros (como la ubicación de los servidores DNS), pero NO para proporcionar direcciones. Esto se conoce como DHCPv6 stateless.</p> <p>Nunca: Seleccione esto para desactivar DHCPv6.</p>

Ping de respuesta

Ruta: Administración > Red > Ping de respuesta

Seleccione la casilla de verificación **Activar** para que **IPv4 Ping Response** permita que la Tarjeta de administración de red responda a los ping de red. Quite la marca de la casilla de verificación para desactivar una respuesta de la Tarjeta de administración de red. Eso no es aplicable a IPv6.

Velocidad de puerto

Ruta: Administración > Red > Velocidad de puerto

El parámetro **Velocidad de puerto** define la velocidad de comunicación del puerto TCP/IP.

- Con **Negociación automática** (el valor predeterminado), los dispositivos Ethernet negocian la transmisión a la velocidad más alta posible, pero si las velocidades admitidas de dos dispositivos no coinciden, se usa la velocidad más lenta.
- También tiene la posibilidad de elegir 10 Mbps o 100 Mbps, cada uno de ellos con la opción de half-duplex (comunicación en sólo una dirección a la vez) o full-duplex (comunicación en ambas direcciones simultáneamente en el mismo canal).

DNS

Ruta: Administración > Red > DNS > opciones

Utilice las opciones que se encuentran debajo de **DNS** para configurar y probar el sistema de nombres de dominio (DNS):

- Seleccione **Servidor DNS principal** o **Servidor DNS secundario** para especificar las direcciones IPv4 o IPv6 del servidor DNS primario y el secundario opcional. Para que la PDU de Rack pueda enviar correo electrónico, se debe definir por lo menos la dirección IP del servidor DNS primario.
 - La PDU de Rack espera hasta 15 segundos a una respuesta del servidor DNS primario o el servidor DNS secundario (si está especificado un servidor DNS secundario). Si la PDU de Rack no recibe una respuesta durante ese tiempo, no se puede enviar correo electrónico. Por lo tanto, utilice servidores DNS que estén en el mismo segmento que la PDU de Rack o en un segmento próximo (pero no en una red de área amplia [WAN]).
 - Después de definir las direcciones IP de los servidores DNS, verifique que el DNS funciona correctamente introduciendo el nombre DNS de un ordenador de su red para buscar la dirección IP de ese ordenador.
- **Nombre de host:** Después de configurar un nombre de host aquí y un nombre de dominio en el campo **Nombre de dominio**, los usuarios pueden introducir un nombre de host en cualquier campo de la interfaz de la PDU de Rack (excepto las direcciones de correo electrónico) que acepte un nombre de dominio.
- **Nombre de dominio (IPv4):** El nombre de dominio se configura aquí sólo. En todos los demás campos de la interfaz de la PDU de Rack (excepto las direcciones de correo electrónico) que aceptan nombres de dominio, la PDU de Rack añade este nombre de dominio cuando se introduce sólo un nombre de host.
 - Para anular todos los casos de la expansión de un nombre de host especificado mediante la adición del nombre de dominio, ponga el campo de nombre de dominio en su valor predeterminado, `somedomain.com`, o en `0.0.0.0`.

- Para anular la expansión de una entrada de nombre de host específica (por ejemplo, cuando se define un receptor de capturas), incluya un punto al final. La PDU de Rack reconoce un nombre de host con un punto al final (como por ejemplo, *mySnmpServer.*) como si fuera un nombre de dominio completo y no añade el nombre de dominio.
- **Nombre de dominio (IPv6):** Especifique el nombre de dominio IPv6 aquí.
- Seleccione **prueba** para enviar una consulta DNS que pruebe la configuración de sus servidores DNS:
 - Como **Tipo de consulta**, seleccione el método que se va a utilizar en la consulta DNS:
 - **por host:** El nombre URL del servidor
 - **por FQDN:** el nombre de dominio completo
 - **por IP:** La dirección IP del servidor
 - **por MX:** El agente de intercambio de correo utilizado por el servidor
 - Como **Pregunta de consulta**, identifique el valor que se va a utilizar para el tipo de consulta seleccionado:

Tipo de consulta seleccionado	Pregunta de consulta que se va a utilizar
por Host	El URL
por FQDN	El nombre de dominio completo, <i>mi_servidor.mi_dominio.</i>
por IP	La dirección IP
por MX	La dirección del agente de intercambio de correo

- Vea el resultado de la solicitud DNS de prueba en el campo **Última respuesta de consulta**.

Web

Ruta: Administración > Red > Web > *opciones*

Opción	Descripción
acceso	<p>Para activar los cambios en cualquiera de estas selecciones, cierre la sesión en la PDU de Rack:</p> <ul style="list-style-type: none">• Desactivar: Desactiva el acceso a la interfaz Web. (Para volver a activar el acceso, inicie una sesión en la interfaz de línea de comandos y a continuación escriba el comando <code>http -S enable</code>. Para un acceso HTTPS, escriba <code>https -S enable</code>.)• Activar HTTP (el valor predeterminado): Activa Hypertext Transfer Protocol (HTTP), que proporciona acceso Web por medio de nombre de usuario y contraseña, pero no cifra los nombre de usuario, las contraseñas ni los datos durante la transmisión.• Activar HTTPS: Activa Hypertext Transfer Protocol (HTTPS) sobre Secure Sockets Layer (SSL). SSL cifra los nombres de usuario, las contraseñas y los datos durante la transmisión, y autentica la PDU de Rack por medio de certificado digital. Cuando HTTPS está activado, el explorador muestra un pequeño icono de un candado. <p>Véase “Creación e instalación de certificados digitales” en el Apéndice B: Manual de seguridad para elegir entre los varios métodos para utilizar certificados digitales.</p> <p>Puerto HTTP: El puerto TCP/IP (el 80 de manera predeterminada) utilizado para comunicarse por HTTP con la PDU de Rack.</p> <p>Puerto HTTPS: El puerto TCP/IP (el 443 de manera predeterminada) utilizado para comunicarse por HTTPS con la PDU de Rack.</p> <p>En uno y otro de estos dos puertos, se puede cambiar el valor del puerto a cualquier puerto no utilizado del 5000 al 32768 para obtener seguridad adicional. Entonces los usuarios deben utilizar dos puntos (:) en el campo de dirección del explorador para especificar el número de puerto. Por ejemplo, para un número de puerto de 5000 y una dirección IP de 152.214.12.114:</p> <pre>http://152.214.12.114:5000 https://152.214.12.114:5000</pre>

Opción	Descripción
certificado ssl	<p>Agregar, reemplazar o quitar un certificado de seguridad.</p> <p>Status (Estado):</p> <ul style="list-style-type: none"> • Sin instalar: No está instalado un certificado, o ha sido instalado por FTP o SCP en una ubicación incorrecta. Al utilizar Agregar o reemplazar archivo de certificado se instala el certificado en la ubicación correcta, <code>/ssl</code> en la PDU de Rack. • Generando: La PDU de Rack está generando un certificado porque no se ha encontrado ningún certificado válido. • Cargando: Se está activando un certificado en la PDU de Rack. • Certificado válido: Un certificado válido ha sido instalado o ha sido generado por la PDU de Rack. Haga clic en este vínculo para ver el contenido del certificado. <p>Si instala un certificado no válido, o si no se carga ningún certificado válido cuando se activa SSL, la PDU de Rack genera un certificado predeterminado, proceso que retrasa el acceso a la interfaz durante hasta un minuto. Se puede utilizar el certificado predeterminado para una seguridad básica basada en cifrado, pero se muestra un mensaje de alerta de seguridad cada vez que se inicia una sesión.</p> <p>Agregar o reemplazar archivo de certificad: Permite introducir o buscar el archivo de certificado creado con el Security Wizard (Asistente para la seguridad).</p> <p>Véase “Creación e instalación de certificados digitales” en el Apéndice B: Manual de seguridad para elegir un método para utilizar certificados digitales creados por el Asistente para la seguridad o generados por la PDU de Rack.</p> <p>Quitar: Elimina el certificado actual.</p>

Consola

Ruta: Administración > Red > Consola > *opciones*

Opción	Descripción
acceso	<p>Elija una de las siguientes opciones para un acceso por Telnet o Secure Shell (SSH):</p> <ul style="list-style-type: none">• Desactivar: Desactiva todo acceso a la interfaz de línea de comandos.• Telnet activado (el valor predeterminado): Telnet transmite los nombres de usuario, las contraseñas y los datos sin cifrado.• Activar SSH: SSH transmite los nombres de usuario, las contraseñas y los datos en forma cifrada, proporcionando protección contra los intentos de interceptar, falsificar o alterar los datos durante la transmisión. <p>Configure los puertos que van a ser utilizados por estos protocolos:</p> <ul style="list-style-type: none">• Puerto Telnet: El puerto Telnet utilizado para comunicarse con la PDU de Rack (el 23 de manera predeterminada). Se puede cambiar el valor del puerto a cualquier puerto no utilizado del 5000 al 32768 para obtener seguridad adicional. Entonces los usuarios deben utilizar dos puntos (:) o un espacio, según lo requiera su programa cliente Telnet, para especificar el puerto no predeterminado. Por ejemplo, para el puerto 5000 y una dirección IP de 152.214.12.114, el cliente Telnet requiere uno de los siguientes comandos: <pre>telnet 152.214.12.114:5000 telnet 152.214.12.114 5000</pre>• Puerto SSH: El puerto SSH utilizado para comunicarse con la PDU de Rack (el 22 de manera predeterminada). Se puede cambiar el valor del puerto a cualquier puerto no utilizado del 5000 al 32768 para obtener seguridad adicional. Véase en la documentación del cliente SSH el formato de línea de comando que se requiere para especificar un puerto no predeterminado.

Opción	Descripción
clave de host ssh	<p>Estado indica el estado de la clave de host (clave privada):</p> <ul style="list-style-type: none"> • SSH desactivado: Ninguna clave de host en uso: Cuando está desactivado, SSH no puede usar una clave de host. • Generando: La PDU de Rack está creando una clave de host porque no se ha encontrado ninguna clave de host válida. • Cargando: Se está activando una clave de host en la PDU de Rack. • Válida: En el directorio <code>/ssh</code> (la ubicación que se requiere en la PDU de Rack está una de las siguientes claves de host válidas): <ul style="list-style-type: none"> • Una clave de host de 1024 bits o 2048 bits creada por el Asistente para la seguridad • Una clave de host RSA de 2048 bits generada por la PDU de Rack <p>Agregar o reemplazar: Permite buscar y cargar un archivo de clave de host creado por el Asistente para la seguridad.</p> <p>Para usar el Asistente para la seguridad, consulte el Apéndice B: Manual de seguridad.</p> <p>NOTA: Para reducir el tiempo que se necesita para activar SSH, cree y cargue una clave de host por adelantado. Si activa SSH sin una clave de host cargada, la PDU de Rack tarda hasta un minuto en crear una, y el servidor SSH no está accesible durante ese tiempo.</p> <p>Quitar: Quita la clave de host actual.</p>



Para usar SSH, debe tener instalado un cliente SSH. La mayoría de las plataformas Linux y UNIX incluyen un cliente SSH, pero los sistemas operativos Windows de Microsoft no. Hay disponibles clientes de diversos vendedores.

SNMP

Todos los nombres de usuario, contraseñas y nombres de comunidad para SNMP se transfieren por la red como texto sin formato. Si su red necesita la alta seguridad del cifrado, desactive el acceso SNMP o ponga el acceso para cada comunidad en Lectura. (Una comunidad con acceso de Lectura puede recibir información de estado y utilizar capturas SNMP.)



Para obtener información detallada sobre la forma de mejorar y administrar la seguridad del sistema, véase [Apéndice B: Manual de seguridad](#).

SNMPv1

Ruta: Administración > Red > SNMPv1 > opciones

Opción	Descripción
acceso	Activar acceso a SNMPv1: Activa SNMP versión 1 como método de comunicación con este dispositivo.
control de acceso	<p>Se puede configurar hasta cuatro entradas de control de acceso para especificar los Sistemas de administración de red (NMS) que tienen acceso a este dispositivo. La página inicial de control de acceso, de manera predeterminada, asigna una entrada a cada una de las cuatro comunidades SNMPv1 disponibles, pero se puede modificar esa configuración para aplicar más de una entrada a cualquier comunidad para conceder acceso por varias direcciones IPv4 e IPv6, nombres de host o máscaras de dirección IP específicos. Para editar la configuración de control de acceso de una comunidad, haga clic en su nombre de comunidad.</p> <ul style="list-style-type: none">• Si se deja sin cambiar la entrada de control de acceso predeterminada de una comunidad, esa comunidad tiene acceso a este dispositivo desde cualquier ubicación de la red.• Si se configuran múltiples entradas de control de acceso para un nombre de comunidad, el límite de cuatro entradas obliga a que una o más de las otras comunidades no deban tener ninguna entrada de control de acceso. Si no se lista ninguna entrada de control de acceso para una comunidad, esa comunidad no tiene acceso a este dispositivo. <p>Nombre de comunidad: El nombre que debe utilizar un NMS para acceder a la comunidad. La longitud máxima es de 15 caracteres ASCII, y los nombres de comunidad predeterminados para las cuatro comunidades son public, private, public2 y private2.</p> <p>Nombre de host/IP NMS: La dirección IPv4 o IPv6, máscara de dirección IP o nombre de host que controla el acceso por los NMS. Un nombre de host o una dirección IP específica (como por ejemplo, 149.225.12.1) permite el acceso únicamente por el NMS que se encuentra en esa ubicación. Las direcciones IP que contienen 255 restringen el acceso de la manera siguiente:</p> <ul style="list-style-type: none">• 149.225.12.255: Acceso únicamente por un NMS en el segmento 149.225.12.• 149.225.255.255: Acceso únicamente por un NMS en el segmento 149,225.• 149.255.255.255: Acceso únicamente por un NMS en el segmento 149.• 0.0.0.0 (el valor predeterminado) que también se puede expresar como 255.255.255.255: Acceso por cualquier NMS en cualquier segmento. <p>Tipo de acceso: Las acciones que puede realizar un NMS a través de la comunidad.</p> <ul style="list-style-type: none">• Lectura: Sólo operaciones GET, en cualquier momento• Escritura: Operaciones GET en cualquier momento, y SET cuando no está ningún usuario en una sesión en la interfaz Web o la interfaz de línea de comandos.• Escritura+: Operaciones GET y SET en cualquier momento.• Desactivar: Ninguna operación GET ni SET en ningún momento.



SNMPv3

Ruta: Administración > Red > SNMPv3 > opciones

Para las operaciones GET y SET y receptores de capturas SNMP, SNMPv3 utiliza un sistema de perfiles de usuario para identificar a los usuarios. Un usuario SNMPv3 debe contar con un perfil de usuario asignado en el programa de software de MIB para poder realizar operaciones GET y SET, buscar en la MIB y recibir capturas.



Para utilizar SNMPv3, debe tener un programa MIB que sea compatible con SNMPv3.

La PDU de Rack admite autenticación SHA o MD5 y cifrado AES o DES.

Opción	Descripción
acceso	Acceso a SNMPv3: Activa SNMPv3 como método de comunicación con este dispositivo.

Opción	Descripción
perfiles de usuario	<p>De manera predeterminada, lista las configuraciones de cuatro perfiles de usuario, configurados con los nombres de usuario dell snmp profile1 a dell snmp profile4, y sin autenticación ni privacidad (sin cifrado). Para modificar los parámetros siguientes de un perfil de usuario, haga clic en un nombre de usuario de la lista.</p> <p>Nombre de usuario: El identificador del perfil de usuario. SNMP versión 3 asigna operaciones GET, SET y capturas a un perfil de usuario haciendo que se corresponda el nombre de usuario del perfil con el nombre de usuario del paquete de datos que se está transmitiendo. Un nombre de usuario puede tener hasta 32 caracteres ASCII.</p> <p>Clave de autenticación: Una frase de 15 a 32 caracteres ASCII (dell auth passphrase, de manera predeterminada) que verifica que el NMS que se comunica con este dispositivo a través de SNMPv3 es el NMS que dice que es, que el mensaje no se ha cambiado durante la transmisión, y que el mensaje se ha comunicado en el momento correcto, indicando que no se ha retrasado y que no se ha copiado y enviado de nuevo después en un momento incorrecto.</p> <p>Clave de privacidad: Una frase de 15 a 32 caracteres ASCII (dell crypt passphrase, de manera predeterminada) que asegura la privacidad de los datos (por medio de cifrado) que un NMS envía a este dispositivo o recibe de este dispositivo a través de SNMPv3.</p> <p>Protocolo de autenticación: La implementación de SNMPv3 de Dell admite autenticación SHA y MD5. No tendrá lugar autenticación a menos que se seleccione un protocolo de autenticación.</p> <p>Protocolo de privacidad: La implementación de SNMPv3 de Dell admite AES y DES como protocolos para el cifrado y descifrado de datos. La privacidad de los datos transmitidos requiere que esté seleccionado un protocolo de privacidad y que se proporcione una clave de privacidad en la solicitud del NMS. Cuando está activado un protocolo de privacidad pero el NMS no proporciona una clave de privacidad, la solicitud SNMP no se cifra.</p> <p>Nota: No se puede seleccionar el protocolo de privacidad si no está seleccionado un protocolo de autenticación.</p>

Opción	Descripción
control de acceso	<p>Se pueden configurar hasta cuatro entradas de control de acceso para especificar los NMS que tienen acceso a este dispositivo. La página inicial de control de acceso, de manera predeterminada, asigna una entrada a cada uno de los cuatro perfiles de usuario, pero se puede modificar esa configuración para aplicar más de una entrada a cualquier perfil de usuario para conceder acceso por varias direcciones IP, nombres de host o máscaras de dirección IP específicas.</p> <ul style="list-style-type: none"> • Si se deja sin cambiar la entrada de control de acceso predeterminada de un perfil de usuario, todos los NMS que usan ese perfil tienen acceso a este dispositivo. • Si se configuran múltiples entradas de acceso para un perfil de usuario, el límite de cuatro entradas obliga a que uno o más de los otros perfiles de usuario no deban tener ninguna entrada de control de acceso. Si no se lista ninguna entrada de control de acceso para un perfil de usuario, no tiene acceso a este dispositivo ningún NMS que use ese perfil. <p>Para editar la configuración de control de acceso de un perfil de usuario, haga clic en su nombre de usuario.</p> <p>Acceso: Marque la casilla de verificación Activar para activar el control de acceso especificado por los parámetros de esta entrada de control de acceso.</p> <p>Nombre de usuario: En la lista desplegable, seleccione el perfil de usuario al que se aplicará esta entrada de control de acceso. Las elecciones disponibles son los cuatro nombres de usuario que se configuran por medio de la opción perfiles de usuario del menú de navegación izquierdo.</p> <p>Nombre de host/IP NMS: La dirección IP, máscara de dirección IP o nombre de host que controla el acceso por el NMS. Un nombre de host o una dirección IP específica (como por ejemplo, 149.225.12.1) permite el acceso únicamente por el NMS que se encuentra en esa ubicación. Una máscara de dirección IP que contiene 255 restringe el acceso de la manera siguiente:</p> <ul style="list-style-type: none"> • 149.225.12.255: Acceso únicamente por un NMS en el segmento 149.225.12. • 149.225.255.255: Acceso únicamente por un NMS en el segmento 149.225. • 149.255.255.255: Acceso únicamente por un NMS en el segmento 149. • 0.0.0.0 (el valor predeterminado) que también se puede expresar como 255.255.255.255: Acceso por cualquier NMS en cualquier segmento.

Servidor FTP

Ruta: Administración > Red > Servidor FTP

Los valores de configuración de **Servidor FTP** activan (de manera predeterminada) o desactivan el acceso al servidor FTP y especifican el puerto TCP/IP (el 21 de manera predeterminada) que usa el servidor FTP para comunicarse con la PDU de Rack. El servidor FTP utiliza el puerto especificado y el puerto un número menor que el puerto especificado.

Se puede cambiar el valor del **Puerto** al número de cualquier puerto sin usar del 5001 al 32768 para obtener seguridad adicional. Entonces los usuarios deben usar dos puntos (:) para especificar el número de puerto no predeterminado. Por ejemplo, para el puerto 5001 y la dirección IP 152.214.12.114, el comando sería `ftp 152.214.12.114:5001`.



FTP transfiere los archivos sin cifrado. Para mayor seguridad, desactive el servidor FTP y transfiera los archivos con SCP. Al seleccionar y configurar Secure Shell (SSH), se activa SCP automáticamente.



Para obtener información detallada sobre la forma de mejorar y administrar la seguridad del sistema, véase [Apéndice B: Manual de seguridad](#).

Administración: Opciones generales

The screenshot displays the administration interface for a Dell Managed Rack PDU. The top navigation bar includes tabs for Home, Device Manager, Environment, Logs, and Administration. The Administration tab is active, and the General sub-tab is selected. A 'No Alarms' indicator is visible in the top right corner. The left sidebar contains a menu with the following items: Identification (selected), Date/Time (with sub-items: mode, daylight saving, date format), User Config File, Preferences, Reset/Reboot, Quick Links, and About. The main content area is titled 'Identification' and contains three input fields: Name (John Doe), Contact (Unknown), and Location (Unknown). Below these fields are 'Apply' and 'Cancel' buttons. The footer of the interface shows 'Link 1 | Link 2 | Link 3' on the left, 'Managed Rack PDU' in the center, and the Dell logo on the right.

Field	Value
Name:	John Doe
Contact:	Unknown
Location:	Unknown

Identificación

Ruta: Administración > General > Identificación

Permite definir el **Nombre** (el nombre del dispositivo), la **Ubicación** (la ubicación física), y el **Contacto** (la persona responsable del dispositivo) utilizados por el agente SNMP de la Rack PDU. Estos valores son los valores utilizados para los Identificadores de objeto (OID) MIB-II **sysName**, **sysContact** y **sysLocation**.



Para obtener más información acerca de los OID MIB-II, véase la Dell Management Information Base (MIB).

Poner la fecha y la hora

Método

Ruta: Administración > General > Fecha/hora > modo

Permite poner la fecha y la hora utilizadas por la Rack PDU. Se pueden cambiar los valores actuales manualmente o por medio de un servidor NTP (Network Time Protocol):

- **Modo manual:** Siga uno de estos métodos:
 - Introduzca la fecha y la hora para la Rack PDU.
 - Marque la casilla de verificación **Aplicar la hora del ordenador local** para que sea igual a los valores de fecha y hora del ordenador que está usando.
- **Sincronizar con el servidor NTP:** Hacer que un servidor NTP defina la fecha y la hora para la Rack PDU.

Parámetro	Definición
Servidor NTP principal	Introduzca la dirección IP o el nombre de dominio del servidor NTP principal.
Servidor NTP secundario	Introduzca la dirección IP o el nombre de dominio del servidor NTP secundario, cuando hay disponible un servidor secundario.
Zona horaria	Seleccione una zona horaria. El número de horas que precede a cada zona horaria en la lista es la desviación de la Hora universal coordinada (UTC), anteriormente Hora media de Greenwich.
Intervalo de actualización	Permite definir la frecuencia, en horas, con la que la Rack PDU accede al servidor NTP para una actualización. <i>Mínimo:</i> 1; <i>Máximo:</i> 8760 (1 año).
Actualizar con NTP ahora	Permite iniciar una actualización inmediata de la fecha y hora por el servidor NTP.

Horario de verano

Ruta: Administración > General > Fecha/hora > horario de verano

Permite activar el horario de verano convencional de EE.UU., o activar y configurar un horario de verano personalizado que se corresponda con el horario de verano que se implementa en su zona local. DST está desactivado de manera predeterminada.

Al personalizar el horario de verano:

- Si el horario de verano local empieza o termina siempre la cuarta vez que ocurre un día concreto de la semana en un mes (p. ej., el cuarto domingo), elija **Cuarto/último**. Si ocurre un quinto domingo en ese mes otro año, el ajuste de la hora sigue cambiando el cuarto domingo.
- Si el horario de verano local empieza o termina siempre la última vez que ocurre un día concreto de la semana en un mes, tanto si es la cuarta o la quinta vez, elija **Quinto/último**.

Formato

Ruta: Administración > General > Fecha/hora > formato de fecha

Permite seleccionar el formato numérico en el que se muestran todas las fechas en esta interfaz de usuario. En las selecciones, cada letra m (mes), d (día) e y (año) representa un dígito. Los días y los meses de un sólo dígito se muestran con un cero inicial.

Uso de un archivo .ini

Ruta: Administración > General > Archivo de configuración de usuario

Permite usar la configuración de una Rack PDU para configurar otra. Recupere el archivo config.ini de la Rack PDU configurada, personalice ese archivo (p.ej., para cambiar la dirección IP) y cargue el archivo personalizado en la nueva Rack PDU. El nombre del archivo puede tener hasta 64 caracteres, y debe tener el sufijo .ini.

Estado	Informa del progreso de la carga. La carga se lleva a cabo con éxito aunque el archivo contenga errores, pero un suceso de sistema informa de los errores en el registro de sucesos.
Carga	Busque el archivo personalizado y cárguelo para que la Rack PDU actual pueda utilizarlo para establecer su propia configuración.



Para recuperar y personalizar el archivo de una Rack PDU configurada, véase [Cómo exportar los valores de configuración](#).

En vez de cargar el archivo en una Rack PDU, se puede exportar a múltiples Rack PDU utilizando un script FTP o SCP.

Registro de sucesos y Unidades de temperatura

Ruta: Administración > General > Preferencias

Códigos de colores del registro de sucesos

Esta opción está desactivada de manera predeterminada. Marque la casilla **Códigos de colores del registro de sucesos** para activar la codificación por colores del texto de alarma registrado en el registro de sucesos. Las entradas de suceso del sistema y las entradas de cambio de la configuración no cambian de color.

Color del texto	Gravedad de la alarma
Rojo	Crítica: Existe una alarma crítica, que requiere acción inmediata.
Naranja	Advertencia: Existe una condición de alarma que requiere atención y que podría poner en peligro los datos o el equipo si no se aborda su causa.
Verde	Alarma retirada: Las condiciones que han causado la alarma han mejorado.
Negro	Normal: No hay ninguna alarma. La Rack PDU y todos los dispositivos conectados funcionan con normalidad.

Cambio de la escala predeterminada de temperatura

Seleccione la escala de temperatura (Fahrenheit o Celsius) en la cual se muestran todas las mediciones de temperatura en esta interfaz de usuario.

Restablecimiento de la PDU de rack

Ruta: Administración > General > Restablece...

Acción	Definición
Reiniciar interfaz de administración	Reinicia la interfaz de la Rack PDU.
Restablecer todo ¹	Quite la marca de la casilla de verificación Excluir TCP/IP para restablecer todos los valores de configuración; marque la casilla de verificación Excluir TCP/IP para restablecer todos los valores excepto los valores TCP/IP.
Restablecer sólo ¹	TCP/IP: Pone la Configuración TCP/IP en DHCP y BOOTP , su valor predeterminado, obligando a que la Rack PDU reciba su configuración TCP/IP de un servidor DHCP o BOOTP. Consulte Configuración de TCP/IP y de la comunicación .
	Configuración de sucesos: Restablece todos los cambios en la configuración de sucesos, por suceso y por grupo, a sus valores predeterminados.
	RPDU en configuración predeterminada: Restablece sólo la configuración de la PDU de rack, no la configuración de red, a sus valores predeterminados.

1. El restablecimiento puede llevar hasta un minuto.



Configuración de los vínculos

Ruta: Administración > General > Vínculos rápidos

Seleccione la ficha **Administración**, **General** en la barra de menú superior, y **Vínculos rápidos** en el menú de navegación izquierdo para ver y cambiar los vínculos a URL que se muestran en la parte inferior izquierda de cada página de la interfaz.

De manera predeterminada, estos vínculos ofrecen acceso a las siguientes páginas Web:

- **Link 1:** dell.com
- **Link 2:** dell.com/home
- **Link 3:** dell.com/business

Para reconfigurar cualquiera de los parámetros siguientes, haga clic en el nombre del vínculo en la columna **Mostrar**:

- **Mostrar:** El nombre corto del vínculo que se muestra en cada página de la interfaz
- **Nombre:** Un nombre que identifica plenamente el objetivo o finalidad del vínculo
- **Dirección:** Cualquier URL—por ejemplo, el URL de otro dispositivo o servidor

Acerca de la Rack PDU

Ruta: Administración > General > Acerca de

La información del hardware es útil para la resolución de problemas con la Rack PDU. El número de serie y la dirección MAC también están disponibles en la Rack PDU misma.

La información de firmware del Módulo de aplicación, del SO de Dell (AOS) y del Monitor de inicio indica el nombre, la versión de firmware y la fecha y hora en que se ha creado cada módulo de firmware. Esta información también es útil para la resolución de problemas.

Administración de tiempo de actividad es la cantidad de tiempo que ha estado funcionando la interfaz de manera continua.

Cómo exportar los valores de configuración

Recuperación y exportación del archivo .ini

Resumen del procedimiento

Un administrador puede recuperar el archivo .ini de una PDU de rack y exportarlo a otra PDU de rack o a múltiples PDU de rack.

1. Configurar una PDU de rack para que tenga los valores que se desea exportar.
2. Recuperar el archivo .ini de esa PDU de rack.
3. Personalizar el archivo para cambiar por lo menos los valores TCP/IP.
4. Utilizar un protocolo de transferencia de archivos admitido por la PDU de rack para transferir una copia a una o más PDU de rack. Para una transferencia a múltiples PDU de rack, utilizar un script FTP o SCP.

Cada PDU de rack receptora utiliza el archivo para reconfigurar sus propios parámetros y a continuación lo elimina.

Contenido del archivo .ini

El archivo config.ini que se recupera de una PDU de rack contiene lo siguiente:

- *encabezamientos de sección y palabras clave* (sólo los admitidos por el dispositivo del cual se recupera el archivo): Los encabezamientos de sección son nombres de categoría encerrados entre corchetes ([]). Las palabras clave, debajo de cada encabezamiento de sección, son etiquetas que describen parámetros de la PDU de rack específicos. Cada palabra clave va seguida de un signo igual y un valor (el predeterminado o un valor configurado).

- La palabra clave **Override**: Con su valor predeterminado, esta palabra clave impide la exportación de una o más palabras clave y sus valores específicos del dispositivo. Por ejemplo, en la sección [**NetworkTCP/IP**], el valor predeterminado de **Override** (la dirección MAC de la PDU de rack) bloquea la exportación de los valores de **SystemIP**, **SubnetMask**, **DefaultGateway** y **BootMode**.

Procedimientos detallados

Recuperación. Para configurar y recuperar un archivo .ini para exportar:

1. Si es posible, utilice la interfaz de una PDU de rack para configurarla con los valores para exportar. Al editar directamente el archivo .ini se corre el riesgo de introducir errores.
2. Para utilizar FTP para recuperar config.ini de la PDU de rack configurada:
 - a. Abra una conexión con la PDU de rack, utilizando su dirección IP:

```
ftp> open dirección_ip
```

- b. Inicie una sesión utilizando un nombre de usuario y contraseña de Administrador.

- c. Recupere el archivo config.ini que contiene la configuración de la PDU de rack:

```
ftp> get config.ini
```

El archivo se escribe en la carpeta desde la que se ha iniciado FTP.

Personalización. Debe personalizar el archivo antes de exportarlo.

1. Utilice un editor de texto para personalizar el archivo.
 - Los encabezamientos de sección, las palabras clave y los valores predefinidos no son sensibles a mayúsculas y minúsculas, pero los valores de cadena que se definen sí lo son.
 - Utilice comillas adyacentes para no indicar ningún valor. Por ejemplo, `LinkURL1=""` indica que el URL no está definido a propósito.
 - Encierre entre comillas todos los valores que contengan espacios iniciales o finales o que ya estén encerrados entre comillas.
 - Para exportar sucesos programados, configure los valores directamente en el archivo `.ini`.
 - Para exportar una hora de sistema con la mayor exactitud, si las PDU de rack receptoras pueden acceder a un servidor NTP (Network Time Protocol), configure `enabled` (activado) para `NTPEnable`:
`NTPEnable=enabled`
También puede reducir el tiempo de transmisión exportando la sección `[SystemDate/Time]` como un archivo `.ini` por separado.
 - Para añadir comentarios, inicie cada línea de comentario con un punto y coma (;).
2. Copie el archivo personalizado en otro nombre de archivo en la misma carpeta:
 - El nombre del archivo puede tener hasta 64 caracteres y debe tener el sufijo `.ini`.
 - Conserve el archivo personalizado original para un uso futuro. **El archivo que se conserva es el único registro de sus comentarios.**

Transferencia del archivo a una sola PDU de rack. Para transferir el archivo .ini a otra PDU de rack, realice cualquiera de las dos acciones siguientes:

- Desde la interfaz Web de la PDU de rack receptora, seleccione la ficha **Administración, General** en la barra de menú superior, y **Archivo de configuración de usuario** en el menú de navegación izquierdo. Introduzca la ruta completa del archivo, o utilice **Browse** (Buscar).
- Utilice cualquier protocolo de transferencia de archivos admitido por las PDU de rack, es decir, FTP, FTP Client, SCP o TFTP. El ejemplo siguiente utiliza FTP:

- a. Desde la carpeta que contiene la copia del archivo .ini personalizado, utilice FTP para iniciar una sesión en la PDU de rack a la cual va a exportar el archivo .ini:

```
ftp> open dirección_ip
```

- b. Exporte la copia del archivo .ini personalizado al directorio raíz de la PDU de rack receptora:

```
ftp> put nombredearchivo.ini
```

Exportación del archivo a múltiples PDU de rack. Para exportar el archivo .ini a múltiples PDU de rack, Utilice FTP o SCP, pero escriba un script que incorpore y repita los pasos utilizados para exportar el archivo a una sola PDU de rack.

El suceso de carga y los mensajes de error

El suceso y sus mensajes de error

Tiene lugar el siguiente suceso cuando la PDU de rack receptora termina de utilizar el archivo .ini para actualizar sus valores de configuración.

Carga completa de archivo de configuración, con *número* valores válidos

Si una palabra clave, nombre de sección o valor no es válido, la carga por la PDU de rack receptora tiene éxito, y un texto adicional del suceso indica el error.

Texto del suceso	Descripción
Advertencia de archivo de configuración: Palabra clave no válida en línea <i>número</i> . Advertencia de archivo de configuración: Valor no válido en línea <i>número</i> .	Una línea con una palabra clave o un valor no válido se ignora.
Advertencia de archivo de configuración: Sección no válida en línea <i>número</i> .	Si un nombre de sección no es válido, todos los pares palabra clave-valor de esa sección se ignoran.
Advertencia de archivo de configuración: Palabra clave detectada fuera de una sección en línea <i>número</i> .	Una palabra clave introducida al principio del archivo (es decir, antes de cualquier encabezamiento de sección) se ignora.
Advertencia de archivo de configuración: El archivo de configuración supera el tamaño máximo.	Si el archivo es demasiado grande, se produce una carga incompleta. Reduzca el tamaño del archivo, o divídalo en dos archivos, e intente cargarlo de nuevo.

Mensajes de config.ini

Una PDU de rack desde la cual se descargue el archivo config.ini debe ser descubierta correctamente para que se incluya su configuración. Si la PDU de rack no está presente o no se detecta, el archivo config.ini contiene un mensaje bajo el nombre de sección correspondiente, en vez de palabras clave y valores. Por ejemplo:

```
PDU de rack no descubierta
```

Si no pensaba exportar la configuración de la PDU de rack como parte de la importación del archivo .ini, ignore esos mensajes.

Errores generados por valores anulados

La palabra clave **Override** y su valor generará mensajes de error en el registro de sucesos cuando bloquee la exportación de valores.



Véase [Contenido del archivo .ini](#) para obtener información acerca de los valores que se anulan.

Como los valores anulados son específicos del dispositivo y no son adecuados para exportar a otras PDU de rack, ignore esos mensajes de error. Para evitar esos mensajes de error, elimine las líneas que contengan la palabra clave **Override** y las líneas que contienen los valores que anulan. No elimine ni cambie la línea que contiene el encabezamiento de sección.

Transferencias de archivos

Cómo actualizar el firmware

Ventajas de actualizar el firmware

Cuando se actualiza el firmware de la PDU de rack:

- Se obtienen las últimas correcciones de errores y mejoras en el rendimiento.
- Nuevas funciones pasan a estar disponibles para su uso inmediato.

Mantener la concordancia de las versiones del firmware en toda la red asegura que todas las PDU de rack acepten las mismas funciones de la misma manera.

Archivos de firmware

Una versión del firmware consta de tres módulos: Un módulo de sistema operativo (AOS), un módulo de aplicación y un módulo de monitor de inicio (bootmon). Cada módulo contiene uno o más CRC (Cyclical Redundancy Check) para proteger sus datos de la corrupción durante la transferencia.

Los archivos de los módulos de sistema operativo (AOS), de aplicación y de monitor de inicio utilizados con la PDU de rack comparten el mismo formato básico:

`dell_versión-dehardware_tipo_versión-defirmware.bin`

- **dell**: Indica que se trata de un archivo de Dell.
- **versión-dehardware**: `hw0x` identifica la versión del hardware en el que se puede usar este archivo binario.
- **tipo**: Identifica si el archivo es el módulo de sistema operativo (AOS), el módulo de aplicación o el módulo de monitor de inicio para PDU de rack.
- **versión**: El número de versión del archivo.
- **bin**: Indica que se trata de un archivo binario.



Véase [Acerca de la Rack PDU](#) para comprobar el número de versión de cada módulo de firmware de una PDU de rack.

Métodos de transferencia de archivos de firmware

Para actualizar el firmware de una PDU de rack, use uno de estos métodos:

- Desde un ordenador en red que esté usando cualquier sistema operativo admitido, utilice FTP o SCP para transferir los módulos de firmware de AOS y de aplicación individuales.
- Para una PDU de rack que no esté en su red, utilice XMODEM a través de una conexión serie para transferir los módulos de firmware individuales de su ordenador a la PDU de rack.



Cuando se transfieren módulos de firmware individuales, **se debe** transferir el módulo de sistema operativo (AOS) a la PDU de rack antes de transferir el módulo de aplicación.

Utilice FTP o SCP para actualizar una PDU de rack

FTP. Para utilizar FTP para actualizar una PDU de rack por la red:

- La PDU de rack debe estar conectada a la red, y deben estar configurados su IP de sistema, su máscara de subred y su puerta de enlace predeterminada.
- El servidor FTP debe estar activado en la PDU de rack.
- Debe haberse descargado los archivos de firmware de Dell.com.

Para transferir los archivos:

1. En un ordenador de la red, abra una ventana de indicador de comando. Vaya al directorio que contiene los archivos de firmware y liste los archivos:

```
C:\>cd\dell  
C:\dell>dir
```

En los archivos listados, `xxx` representa el número de versión del firmware:

- `dell_hw05_aos_xxx.bin`
- `dell_hw05_application_xxx.bin`

2. Abra una sesión de cliente FTP:

```
C:\dell>ftp
```

3. Escriba **open** y la dirección IP de la PDU de rack, y pulse INTRO. Si el valor de **puerto** para el servidor FTP ha cambiado respecto a su valor predeterminado de **21**, debe utilizar el valor no predeterminado en el comando FTP.

- En los clientes FTP Windows, separe un número de puerto no predeterminado de la dirección IP mediante un espacio. Por ejemplo:

```
ftp> open 150.250.6.10 21000
```

- Algunos clientes FTP en vez de eso requieren dos puntos antes del número de puerto.

4. Inicie una sesión como Administrador; **admin** es el nombre de usuario y contraseña predeterminados.

5. Actualice el AOS. (En el ejemplo, **xxx** es el número de versión del firmware):

```
ftp> bin
```

```
ftp> put dell_hw05_aos_xxx.bin
```

6. Cuando FTP confirme la transferencia, escriba **quit** (salir) para cerrar la sesión.

7. Después de 20 segundos, repita los pasos 2 al 5. En el paso 5, use el nombre de archivo del módulo de aplicación.

SCP. Para utilizar Secure CoPy (SCP) para actualizar el firmware de la PDU de rack:

1. Identifique y localice los módulos de firmware que se describen en las instrucciones anteriores para FTP.

2. Utilice una línea de comando SCP para transferir el módulo de firmware de AOS a la PDU de rack. El ejemplo siguiente utiliza **xxx** para representar el número de versión del módulo de AOS:

```
scp dell_hw05_aos_xxx.bin
```

```
dell@158.205.6.185:dell_hw05_aos_xxx.bin
```

3. Utilice una línea de comando SCP similar, con el nombre del módulo de aplicación, para transferir el módulo de firmware de aplicación a la PDU de rack.

Cómo actualizar múltiples PDU de rack

Utilice FTP o SCP para actualizar múltiples PDU de rack. Para actualizar múltiples PDU de rack utilizando un cliente FTP o utilizando SCP, escriba un script que realice automáticamente el procedimiento.

Uso de XMODEM para actualizar una PDU de rack

Para utilizar XMODEM para actualizar una PDU de rack que no esté en la red, primero se deben descargar los archivos de firmware de Dell.com.

Para transferir los archivos:

1. Seleccione un puerto serie del ordenador local y desactive cualquier servicio que utilice el puerto.
2. Conecte el cable de configuración serie suministrado en el puerto seleccionado y en el puerto serie de la PDU de rack.
3. Ejecute un programa emulador de terminal, como por ejemplo, HyperTerminal, y configure el puerto seleccionado con los siguientes valores 57600 bps, 8 bits de datos, sin paridad, 1 bit de parada y sin control de flujo.
4. Pulse el botón RESET (Restablecer) de la PDU de rack, e inmediatamente después pulse la tecla INTRO dos veces, o hasta que aparezca el indicador del Monitor de inicio: **BM>**
5. Escriba **XMODEM**, y a continuación pulse INTRO.
6. En el menú del programa de terminal, seleccione XMODEM, y a continuación seleccione el archivo binario del firmware de AOS para transferir utilizando XMODEM. Una vez completada la transferencia XMODEM, aparece de nuevo el indicador del Monitor de inicio.
7. Para instalar el módulo de aplicación, repita el paso 5 y el paso 6. En el paso 6, utilice el nombre de archivo del módulo de aplicación.
8. Escriba **reset** (restablecer) o pulse el botón Reset para reiniciar la PDU de rack.



Para obtener información sobre el formato utilizado para los módulos de firmware, consulte [Archivos de firmware](#).

Verificación de las actualizaciones

Verificación del éxito o fracaso de la transferencia

Para verificar si una actualización de firmware se ha realizado con éxito, utilice el comando `xferStatus` en la interfaz de línea de comandos para ver el resultado de la última transferencia, o utilice un SNMP GET para el OID `mfiletransferStatusLastTransferResult`.

Códigos de resultado de la última transferencia

Código	Descripción
Successful (Éxito)	La transferencia de archivos ha concluido satisfactoriamente.
Result not available (Resultado no disponible)	No se han registrado transferencias de archivos.
Failure unknown (Fallo desconocido)	La última transferencia de archivos ha fallado por razones desconocidas.
Server inaccessible (Servidor inaccesible)	No se ha podido encontrar el servidor TFTP o FTP en la red.
Server access denied (Acceso a servidor denegado)	El servidor TFTP o FTP ha denegado el acceso.
File not found (Archivo no encontrado)	El servidor TFTP o FTP no ha podido localizar el archivo solicitado.
File type unknown (Tipo de archivo desconocido)	El archivo se ha descargado pero no se ha reconocido su contenido.
File corrupt (Archivo corrupto)	El archivo se ha descargado pero ha fallado por lo menos una comprobación de redundancia cíclica (CRC).

Verificación de los números de versión del firmware instalado.

Utilice la interfaz Web para verificar las versiones de los módulos de firmware actualizados seleccionando la ficha **Administración, General** en la barra de menú superior, y **Acerca de** en el menú de navegación izquierdo, o utilice un SNMP GET para el OID MIB II **sysDescr**. En la interfaz de línea de comandos, utilice el comando **about**.

Resolución de problemas

PDU de Rack Problemas de acceso

Problema	Solución
No se puede hacer ping a la PDU de Rack	<p>Si el LED de estado de la PDU de Rack está en verde, intente hacer ping a otro nodo del mismo segmento de red que la PDU de Rack. Si eso falla, no es un problema de la PDU de Rack. Si el LED de estado no está en verde, o si se realiza con éxito la prueba de ping, efectúe las siguientes comprobaciones:</p> <ul style="list-style-type: none">• Verifique todas las conexiones de red.• Verifique la dirección IP de la PDU de Rack y del NMS.• Si el NMS está en una red (o subred) física diferente que la PDU de Rack, verifique la dirección IP de la puerta de enlace (o router) predeterminada.• Verifique el número de bits de subred de la máscara de subred de la PDU de Rack.
No se puede asignar el puerto de comunicaciones mediante un programa de terminal	<p>Antes de que se pueda utilizar un programa de terminal para configurar la PDU de Rack, se debe cerrar cualquier aplicación, servicio o programa que esté usando el puerto de comunicaciones.</p>
No se puede acceder a la interfaz de línea de comandos por medio de una conexión serie	<p>Asegúrese de que no ha cambiado la velocidad en baudios. Pruebe 2400, 9600, 19200 o 38400.</p>
No se puede acceder a la interfaz de línea de comandos de manera remota	<ul style="list-style-type: none">• Asegúrese de que está utilizando el método de acceso correcto: Telnet o Secure Shell (SSH). Un Administrador puede activar estos métodos de acceso. De manera predeterminada, Telnet está activado. La activación de SSH desactiva Telnet automáticamente.• Con SSH, la PDU de Rack puede estar creando una clave de host. La PDU de Rack puede tardar hasta un minuto en crear la clave de host, y SSH está inaccesible durante ese tiempo.

Problema	Solución
No se puede acceder a la interfaz Web	<ul style="list-style-type: none">• Verifique que el acceso HTTP o HTTPS está activado.• Asegúrese de que especifica el URL correcto: uno que esté en consonancia con el sistema de seguridad utilizado por la PDU de Rack. SSL requiere https, no http, al principio del URL.• Verifique que puede hacer ping a la PDU de Rack.• Verifique que está utilizando un explorador Web admitido para la PDU de Rack. Consulte Exploradores Web aceptados.• Si la PDU de Rack acaba de reiniciarse y se está configurando la seguridad SSL, la PDU de Rack puede estar generando un certificado de servidor. La PDU de Rack puede tardar hasta un minuto en crear este certificado, y el servidor SSL no está disponible durante ese tiempo.

Apéndice A: Lista de comandos aceptados

Descripción de los comandos de la Tarjeta de administración de red

```
?
about
alarmcount
  [-p [all | warning | critical]]
boot
  [-b <dhcpBootp | dhcp | bootp | manual>]
  [-a <remainDhcpBootp | gotoDhcpOrBootp>]
  [-o <stop | prevSettings>]
  [-f <retry then fail #>]
  [-c <dhcp cookie> [enable | disable]]
  [-s <retry then stop #>]
  [-v <clase de distribuidor>]
  [-i <ID cliente>]
  [-u <clase de usuario>]
cd
console
  [-S<disable | telnet | ssh>]
  [-pt <telnet n de puerto>]
  [-ps <SSH n de puerto>]
  [-b <2400 | 9600 | 19200 | 38400>]
date
  [-d <"cadenadefecha">]
  [-t <00:00:00>]
  [-f [mm/dd/aa | dd.mm.aaaa | mmm-dd-aa | dd-mmm-aa | aaaa-mm-dd]]
delete
dir
dns
  [-OM <enable | disable>]
  [-p <servidor DNS primario>]
  [-s <servidor DNS secundario>]
  [-d <nombre de dominio>]
  [-n <nombre de dominio IPv6>]
  [-h <nombre de host>]
eventlog
exit
format
```

```
ftp
  [-p <número de puerto>]
  [-S <enable | disable>]
help
netstat
ntp
  [-OM <enable | disable>]
  [-p <servidor NTP primario>]
  [-s <servidor NTP secundario>]
ping
  [<dirección IP o nombre DNS>]
portspeed
  [-s [auto | 10H | 10F | 100H | 100F]]
prompt
  [-s [long | short]]
quit
radius
  [-a <access> [local | radiusLocal | radius]]
  [-p# <IP de servidor>]
  [-s# <secreto de servidor>]
  [-t# <tiempo de espera de servidor>]
reboot
resetToDef
  [-p <all | keepip>] (todo o mantener ip)
snmp, snmpv3
  [-S <enable | disable>]
system
  [-n <nombre del sistema>]
  [-c <contacto del sistema>]
  [-l <ubicación del sistema>]
tcpip
  [-i <dirección IP>]
  [-s <máscara de subred>]
  [-g <puerta de enlace>]
  [-d <nombre de dominio>]
  [-h <nombre de host>]
tcpip6
  [-S <enable | disable>]
  [-man <enable | disable>]
  [-auto <enable | disable>]
  [-i <dirección IPv6>]
  [-g <puerta de enlace IPv6>]
  [-d6 <router | stateful | stateless | never>]
```

user
[-an <nombre de Administrador>]
[-dn <nombre de Usuario de dispositivo>]
[-rn <nombre de Usuario de sólo lectura>]
[-ap <contraseña de Administrador>]
[-dp <contraseña de Usuario de dispositivo>]
[-rp <contraseña de Usuario de sólo lectura>]
[-t <tiempo de espera por inactividad en minutos>]

web
[-S <disable | http | https>]
[-ph <nº. de puerto http>]
[-ps <nº. de puerto https>]

xferINI
xferStatus

Descripción de los comandos de dispositivo

devLowLoad
[<potencia>]

devNearOver
[<potencia>]

devOverLoad
[<potencia>]

devReading
[<"potencia" | "energía">]

devStartDly

humLow
[<humedad>]

humMin
[<humedad>]

humReading

inNormal

inReading

olAssignUsr
[<"all" | nombre de toma de corriente | nº. de toma de corriente > <usuario>]

olCancelCmd
[<"all" | nombre de toma de corriente | nº. de toma de corriente>]

olDlyOff
[<"all" | nombre de toma de corriente | nº. de toma de corriente>]

olDlyOn
[<"all" | nombre de toma de corriente | nº. de toma de corriente>]

olDlyReboot
[<"all" | nombre de toma de corriente | nº. de toma de corriente>]

olGroups

oLowLoad
[<"all" | nombre de toma de corriente | nº. de toma de corriente> <potencia>]

oName
[<"all" | nº. de toma de corriente > <nuevo nombre>]

oNearOver
[<"all" | nombre de toma de corriente | nº. de toma de corriente> <potencia>]

oOff
[<"all" | nombre de toma de corriente | nº. de toma de corriente>]

oOffDelay
[<"all" | nombre de toma de corriente | nº. de toma de corriente> <tiempo>]

oOn
[<"all" | nombre de toma de corriente | nº. de toma de corriente>]

oOnDelay
[<"all" | nombre de toma de corriente | nº. de toma de corriente> <tiempo>]

oOverLoad
[<"all" | nombre de toma de corriente | nº. de toma de corriente> <potencia>]

oRebootTime
[<"all" | nombre de toma de corriente | nº. de toma de corriente> <tiempo>]

oReading
[<"all" | nombre de toma de corriente | nº. de toma de corriente > <current | power | energy>]

oReboot
[<"all" | nombre de toma de corriente | nº. de toma de corriente>]

oStatus
[<"all" | nombre de toma de corriente | nº. de toma de corriente>]

oUnasgnUsr
[<"all" | nombre de toma de corriente | nº. de toma de corriente > <usuario>]

phLowLoad
[<"all" | nº. de fase> <corriente>]

phNearOver
[<"all" | nº. de fase> <corriente>]

phOverLoad
[<"all" | nº. de fase> <corriente>]

phReading
[<"all" | nº. de fase> <"corriente" | "voltaje" | "potencia">]

phRestrictn
[<"all" | nº. de fase> <none | near | over>]

prodInfo

tempHigh
[<"F" | "C"> <temperatura>]

tempMax
[<"F" | "C"> <temperatura>]

tempReading
[<"F" | "C">]

```
userAdd  
    [<nuevo usuario>]  
userDelete  
    [<usuario>]  
userList  
userPasswd  
    [<usuario> <nueva contraseña> <nueva contraseña>]  
whoami
```

Apéndice B: Manual de seguridad

Contenido y finalidad de este Apéndice

Este apéndice documenta funciones de seguridad del firmware version 5.x.x para PDU de rack Dell® que hacen posible que las PDU de rack funcionen de manera remota por la red.

Este apéndice documenta los siguientes protocolos y funciones, cómo seleccionar los que son adecuados para su situación y cómo configurarlos y usarlos dentro de un sistema de seguridad general:

- Telnet y Secure Shell (SSH)
- Secure Sockets Layer (SSL)
- RADIUS
- SNMPv1 y SNMPv3

Además, este apéndice documenta cómo utilizar el Rack PDU Security Wizard (Asistente para la seguridad de la PDU de rack) para crear los componentes que se requieren para la alta seguridad disponible a través de SSL y SSH.

Funciones de seguridad

Protección de contraseñas

No se almacena ninguna contraseña en la PDU de rack en texto sencillo.

- Las contraseñas se codifican utilizando un algoritmo hash unidireccional.
- Las contraseñas, que se utilizan para la autenticación y cifrado, se cifran antes de ser almacenadas en la PDU de rack.

Resumen de los métodos de acceso

Acceso remoto a la interfaz de línea de comandos.

Acceso de seguridad	Descripción
Acceso mediante nombre de usuario y contraseña	Siempre activado

Acceso remoto a la interfaz de línea de comandos.

Acceso de seguridad	Descripción
Métodos disponibles: <ul style="list-style-type: none">• Nombre de usuario y contraseña• Puerto de servidor seleccionable• Protocolos de acceso que pueden activarse y desactivarse• Secure Shell (SSH)	Para una alta seguridad, utilice SSH. <ul style="list-style-type: none">• Con Telnet, el nombre de usuario y la contraseña se transmiten como texto sencillo.• La activación de SSH desactiva Telnet y proporciona acceso cifrado a la interfaz de línea de comandos para proporcionar protección adicional contra los intentos de interceptación, falsificación o alteración de los datos durante la transmisión.

SNMPv1 y SNMPv3.

Acceso de seguridad	Descripción
<p>Métodos disponibles (SNMPv1):</p> <ul style="list-style-type: none">• Nombre de comunidad• Nombre de host• Filtros de IPs de NMS• Agentes que pueden activarse y desactivarse• Cuatro comunidades de acceso con capacidad de lectura/escritura/desactivación	<p>Tanto para SNMPv1 como para SNMPv3, el nombre de host restringe el acceso al Network Management System (NMS) en esa ubicación sólo, y los filtros de IPs de NMS permiten el acceso únicamente a los NMS especificados mediante uno de los formatos de dirección IP de los siguientes ejemplos:</p> <ul style="list-style-type: none">• 159.215.12.1: Sólo el NMS en la dirección IP 159.215.12.1.• 159.215.12.255: Cualquier NMS en el segmento 159.215.12.• 159.215.255.255: Cualquier NMS en el segmento 159.215.• 159.255.255.255: Cualquier NMS en el segmento 159.• 0.0.0.0 o 255.255.255.255: Cualquier NMS. <p>SNMPv3 tiene funciones de seguridad adicionales que incluyen lo siguiente:</p> <ul style="list-style-type: none">• Una contraseña de autenticación para asegurarse de que un NMS que intente acceder a la PDU de rack sea el NMS que dice ser.• Cifrado de los datos durante la transmisión, con una contraseña de privacidad necesaria para el cifrado y desciframiento.
<p>Métodos disponibles (SNMPv3):</p> <ul style="list-style-type: none">• Cuatro perfiles de usuario• Autenticación mediante una contraseña de autenticación• Cifrado mediante una contraseña de privacidad• Autenticación SHA o MD5• Algoritmo de cifrado AES o DES• Filtros de IPs de NMS	

Protocolos de transferencia de archivos.

Acceso de seguridad	Descripción
<p>Métodos disponibles:</p> <ul style="list-style-type: none">• Nombre de usuario y contraseña• Puerto de servidor seleccionable• Servidor FTP y protocolos de acceso que pueden activarse y desactivarse• Secure CoPy (SCP)	<p>Con FTP, el nombre de usuario y la contraseña se transmiten como texto sencillo, y los archivos se transfieren sin cifrado.</p> <p>Utilice SCP para cifrar el nombre de usuario y la contraseña y los archivos que se transfieran, como por ejemplo las actualizaciones de firmware, los archivos de configuración, los archivos de registro, los certificados Secure Sockets Layer (SSL) y las claves de host Secure Shell (SSH). Si elige SCP como protocolo de transferencia de archivos, active SSH y desactive FTP.</p>

Servidor Web.

Acceso de seguridad	Descripción
<p>Métodos disponibles:</p> <ul style="list-style-type: none">• Nombre de usuario y contraseña• Puerto de servidor seleccionable• Acceso a interfaz Web que pueden activarse y desactivarse• Secure Sockets Layer (SSL)	<p>En el modo de autenticación HTTP básico, el nombre de usuario y la contraseña se transmiten codificados en base 64 (sin cifrado).</p> <p>SSL está disponible en los exploradores Web aceptados por la Tarjeta de administración o dispositivo habilitado para red y en la mayoría de los servidores Web. El protocolo Web HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) cifra y descifra las solicitudes de página al servidor Web y las páginas devueltas por el servidor Web al usuario.</p>

RADIUS.

Acceso de seguridad	Descripción
<p>Métodos disponibles:</p> <ul style="list-style-type: none">• Autenticación centralizada de los derechos de acceso• Un secreto de servidor compartido entre el servidor RADIUS y la PDU de rack o dispositivo	<p>RADIUS (Remote Authentication Dial-In User Service) es un servicio de autenticación, autorización y contabilidad que se usa para administrar centralmente el acceso remoto de cada PDU de rack. (La PDU de rack admite las funciones de autenticación y autorización.)</p>

Prioridades de acceso

La prioridad de acceso, empezando por la prioridad más alta, será del modo siguiente:

- Acceso local a la interfaz de línea de comandos desde un ordenador con una conexión serie directa a la PDU de rack
- Acceso Telnet o Secure Shell (SSH) a la interfaz de línea de comandos desde un ordenador remoto
- Acceso Web

Cambiar inmediatamente los nombres de usuario y contraseñas predeterminadas

Después de la instalación y la configuración inicial de la PDU de rack, cambie inmediatamente los nombres de usuario y contraseñas predeterminados por nombres de usuario y contraseñas únicos para establecer una seguridad básica.

Asignaciones de puertos

Si Telnet, el servidor FTP, SSH/SCP o el servidor Web utiliza un puerto no estándar, un usuario debe especificar el puerto en la línea de comando o dirección Web utilizada para acceder a la PDU de rack. Un número de puerto no estándar proporciona un nivel adicional de seguridad. Los puertos se establecen inicialmente en los “puertos bien conocidos” para los protocolos. Para aumentar la seguridad, ponga los puertos en cualquier número de puerto no utilizado entre el 5001 y el 32768 para el servidor FTP y entre el 5000 y el 32768 para los demás protocolos y servidores. (El servidor FTP utiliza el puerto especificado y el puerto un número menor que el puerto especificado.)

Nombres de usuario, contraseñas y nombres de comunidad con SNMPv1

Todos los nombres de usuario, contraseñas y nombres de comunidad para SNMPv1 se transfieren por la red como texto sencillo. Un usuario capaz de supervisar el tráfico de red puede determinar los nombres de usuario y contraseñas necesarios para iniciar una sesión en las cuentas de la interfaz de línea de comandos o la interfaz Web de la PDU de rack. Si su red necesita la mayor seguridad de las opciones basadas en cifrado disponibles para la interfaz de línea de comandos y la interfaz Web, desactive el acceso SNMPv1 o ponga su acceso en **Lectura**. (El acceso de **Lectura** le permite recibir información de estado y utilizar capturas SNMPv1.)

Para desactivar el acceso SNMPv1, en la ficha **Administración**, seleccione **Red** en la barra de menú superior y **acceso** bajo el encabezamiento **SNMPv1** en el menú de navegación izquierdo. Quite la marca de la casilla de verificación **Activar acceso a SNMPv1** y haga clic en **Aplicar**.

Para poner el acceso SNMPv1 en **Lectura**, en la ficha **Administración**, seleccione **Red** en la barra de menú superior y **control de acceso** bajo el encabezamiento **SNMPv1** en el menú de navegación izquierdo. Luego, para cada Network Management System (NMS) configurado, haga clic en los nombres de comunidad y ponga el tipo de acceso en **Lectura**.

Autenticación

Se pueden elegir funciones de seguridad para la PDU de rack que controlan el acceso proporcionando una autenticación básica por medio de nombres de usuario, contraseñas y direcciones IP, sin utilizar cifrado. Estas funciones de seguridad básicas son suficiente para la mayoría de los entornos en los que no se transfieren datos confidenciales.

Comandos SNMP GET, SNMP SET y Capturas SNMP

Para una mejor autenticación cuando se usa SNMP para supervisar o configurar la PDU de rack, elija SNMPv3. La contraseña de autenticación que se usa con los perfiles de usuario SNMPv3 asegura que un Network Management System (NMS) que intente comunicarse con la PDU de rack sea el NMS que dice ser, que el mensaje no se haya cambiado durante la transmisión, y que el mensaje no se haya retrasado, copiado ni enviado de nuevo posteriormente en un momento incorrecto. SNMPv3 está desactivado de manera predeterminada.

La implementación de Dell de SNMPv3 permite el uso del protocolo SHA-1 o MD5 para la autenticación.

Interfaz Web e interfaz de línea de comandos

Para asegurarse de que los datos y la comunicación entre la PDU de rack y las interfaces de cliente (la interfaz de línea de comandos y la interfaz Web) no puedan ser interceptadas, se puede proporcionar un mayor nivel de seguridad utilizando uno o más de los siguientes métodos basados en cifrado:

- Para la interfaz Web, utilice el protocolo Secure Sockets Layer (SSL)
- Para cifrar los nombres de usuario y las contraseñas para el acceso a la interfaz de línea de comandos, utilice el protocolo Secure Shell (SSH)
- Para cifrar los nombres de usuario, las contraseñas y los datos para la transferencia segura de archivos, utilice el protocolo Secure CoPy (SCP)



Para más información sobre la seguridad basada en cifrado, véase [Cifrado](#).

Cifrado

Comandos SNMP GET, SNMP SET y Capturas SNMP

Para una comunicación cifrada cuando se usa SNMP para supervisar o configurar la PDU de rack, elija SNMPv3. La contraseña de privacidad que se utiliza con los perfiles de usuario SNMPv3 asegura la privacidad de los datos (por medio de cifrado, utilizando el algoritmo de cifrado AES o DES) que un NMS envía a o recibe de la PDU de rack.

Secure Shell (SSH) y Secure CoPy (SCP) para la interfaz de línea de comandos

El protocolo Secure Shell. SSH proporciona un mecanismo seguro para acceder a consolas de ordenador o a *shells*, de manera remota. El protocolo autentica el servidor (en este caso, la PDU de rack) y cifra todas las transmisiones entre el cliente SSH y el servidor.

- SSH es una alternativa de alta seguridad a Telnet. Telnet no proporciona cifrado.
- SSH protege el nombre de usuario y la contraseña, que son las credenciales para la autenticación, de ser utilizados por cualquiera que intercepte el tráfico de red.
- Para autenticar el servidor SSH (la PDU de rack) para el cliente SSH, SSH utiliza una clave de host exclusiva del servidor SSH. La clave de host es una identificación que no se puede falsificar, y que impide que un servidor no válido de la red obtenga un nombre de usuario y contraseña presentándose como un servidor válido.



Para obtener información sobre aplicaciones cliente SSH aceptadas, véase [Telnet y Secure Shell \(SSH\)](#). Para crear una clave de host, véase [Creación de una clave de host SSH](#).

- La PDU de rack acepta SSH version 2, que proporciona protección contra los intentos de interceptar, falsificar o cambiar los datos durante la transmisión.
- Cuando se activa SSH, Telnet se desactiva automáticamente.

- La interfaz, cuentas de usuario y derechos de acceso de usuario son los mismos tanto si se accede a la interfaz de línea de comandos a través de SSH como si se accede a través de Telnet.

Secure CoPy. SCP es una aplicación de transferencia segura de archivos que se puede utilizar en lugar de FTP. SCP utiliza el protocolo SSH como protocolo de transporte subyacente para el cifrado de los nombres de usuario, contraseñas y archivos.

- Cuando se activa y configura SSH, se activa y configura automáticamente SCP. No se necesita una configuración adicional de SCP.
- Se debe desactivar FTP explícitamente. No se desactiva al activar SSH. Para desactivar FTP, en la ficha **Administración**, seleccione **Red** en la barra de menú superior y **Servidor FTP** en el menú de navegación izquierdo. Quite la marca de la casilla de verificación **Activar** y haga clic en **Aplicar**.

Secure Sockets Layer (SSL) para la interfaz Web

Para una comunicación Web segura, active Secure Sockets Layer (SSL) seleccionando HTTPS como modalidad de protocolo que utilizar para el acceso a la interfaz Web de la PDU de rack. HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) es un protocolo Web que cifra y descifra las solicitudes de página del usuario y las páginas que son devueltas por el servidor Web al usuario.

La PDU de rack acepta SSL version 3.0 y el protocolo asociado Transport Layer Security (TLS) version 1.0. La mayoría de los exploradores le permiten seleccionar la versión SSL para activar.

Cuando SSL está activado, el explorador muestra un pequeño icono de un candado.



SSL utiliza un certificado digital para posibilitar que el explorador autentique el servidor (en este caso, la PDU de rack). El explorador verifica lo siguiente:

- El formato del certificado de servidor es correcto
- La fecha y hora de expiración del certificado de servidor no ha pasado
- El nombre DNS o la dirección IP especificado cuando un usuario inicia una sesión coincide con el nombre común en el certificado de servidor
- El certificado de servidor está firmado por una autoridad de certificación de confianza

Los fabricantes de los exploradores importantes distribuyen certificados raíz CA de las Autoridades de Certificación comerciales en el almacén (cache) de certificados de su explorador para que pueda comparar la firma del certificado de servidor con la firma de un certificado raíz CA.

Se puede utilizar el Rack PDU Security Wizard (Asistente para la seguridad de la PDU de rack) para crear una solicitud de firma de certificado a una Autoridad de certificación externa, o si no se desea utilizar una Autoridad de certificación existente, se puede crear un certificado raíz Dell para cargarlo en el almacén (cache) de certificados del explorador. También se puede utilizar el Asistente para crear un certificado de servidor para cargarlo en la PDU de rack.



Véase [Creación e instalación de certificados digitales](#) para obtener un resumen de cómo se usan estos certificados.

Para crear certificados y solicitudes de certificado, véase [Creación de un certificado raíz y de certificados de servidor](#) y [Creación de un certificado de servidor y una solicitud de firma](#).

SSL también usa diversos algoritmos y cifrados para autenticar el servidor, cifrar datos y asegurar la integridad de los datos, es decir, que no hayan sido interceptados y enviados por otro servidor.



Los páginas Web a las que se ha accedido recientemente se guardan en la cache del explorador Web y le permiten volver a esas páginas sin tener que reintroducir su nombre de usuario y contraseña. Cierre siempre la sesión del explorador antes de dejar su ordenador desatendido.

Creación e instalación de certificados digitales

Finalidad

Para la comunicación en red que requiere un nivel más elevado de seguridad que el cifrado de contraseñas, la interfaz Web de la PDU de rack acepta el uso de certificados digitales con el protocolo Secure Sockets Layer (SSL). Los certificados digitales pueden autenticar la PDU de rack (el servidor) para el explorador Web (el cliente SSL).



Se puede generar una clave de 1024 bits, o una clave de 2048 bits, que proporciona un cifrado complejo y un nivel más elevado de seguridad.

Las secciones que siguen resumen los tres métodos de creación, implementación y uso de certificados digitales para ayudarle a determinar el método más adecuado para su sistema.

- **Método 1:** Usar el certificado predeterminado generado automáticamente por la PDU de rack.
- **Método 2:** Usar el Rack PDU Security Wizard para crear un certificado CA y un certificado de servidor.
- **Método 3:** Utilizar el Rack PDU Security Wizard para crear una solicitud de firma de certificado para que sea firmada por el certificado raíz de una Autoridad de certificación externa y para crear un certificado de servidor.



También puede utilizar el Método 3 si su empresa o agencia opera su propia Autoridad de certificación. Utilice el Rack PDU Security Wizard de la misma forma, pero use su propia Autoridad de certificación en vez de una Autoridad de certificación comercial.

Elección de un método para su sistema

Utilizando el protocolo Secure Sockets Layer (SSL), se puede elegir cualquiera de los siguientes métodos para el uso de certificados digitales.

Método 1: Usar el certificado predeterminado generado automáticamente por la PDU de rack. Cuando se activa SSL, se debe reiniciar la PDU de rack. Durante el reinicio, si no existe ningún certificado de servidor, la PDU de rack genera un certificado de servidor predeterminado que está autofirmado pero que no se puede configurar.

El Método 1 tiene las siguientes ventajas y desventajas.

- **Ventajas:**

- Antes de ser transmitidos, el nombre de usuario y contraseña y todos los datos a y desde la PDU de rack son cifrados.
- Puede utilizar este certificado de servidor predeterminado para proporcionar seguridad basada en cifrado mientras instala cualquiera de las otras dos opciones de certificado digital, o puede continuar utilizándolo por los beneficios de cifrado que SSL proporciona.

- **Desventajas:**

- La PDU de rack tarda hasta 1 minuto en crear este certificado, y la interfaz Web no está disponible durante ese tiempo. (Este retraso se produce la primera que se inicia una sesión después de activar SSL.)
- Este método no incluye la autenticación proporcionada por un certificado CA (un certificado firmado por una Autoridad de certificación) que proporcionan los métodos 2 y 3. No hay ningún certificado CA almacenado en el explorador. Por lo tanto, cuando se inicia una sesión en la PDU de rack, el explorador genera una alerta de seguridad, indicando que no está disponible un certificado firmado por una autoridad de confianza, y pregunta si se desea proseguir. Para evitar este mensaje, se debe instalar el certificado de servidor predeterminado en el almacén (cache) de certificados del explorador de cada usuario que necesite acceso a la PDU de rack, y cada usuario debe utilizar siempre el nombre de dominio completo del servidor al iniciar una sesión en la PDU de rack.

- El certificado de servidor predeterminado tiene el número de serie de la PDU de rack en lugar de un *nombre común* válido (el nombre DNS o la dirección IP de la PDU de rack). Por lo tanto, aunque la PDU de rack puede controlar el acceso a su interfaz Web por nombre de usuario, contraseña y tipo de cuenta (p. ej., **Administrador, Usuario de sólo dispositivo o Usuario de sólo lectura**), el explorador no puede autenticar qué PDU de rack está enviando o recibiendo los datos.
- La longitud de la *clave pública* (clave RSA) que se usa para el cifrado al establecer una sesión SSL es de 2048 bits, de manera predeterminada.

Método 2: Usar el Rack PDU Security Wizard para crear un certificado CA y un certificado de servidor. Utilice el Rack PDU Security Wizard para crear dos certificados digitales:

- Un *certificado raíz CA* (certificado raíz de Autoridad de certificación) que el Rack PDU Security Wizard utiliza para firmar todos los certificados de servidor y que luego se instalan en el almacén (cache) de certificados del explorador de cada usuario que necesite acceso a la PDU de rack.
- Un *certificado de servidor* que se carga en la PDU de rack. Cuando el Rack PDU Security Wizard crea un certificado de servidor, utiliza el certificado raíz CA para firmar el certificado de servidor.

El explorador Web autentica la PDU de rack que está enviando o solicitando datos:

- Para identificar la PDU de rack, el explorador utiliza el *nombre común* (dirección IP o nombre DNS de la PDU de rack) que se ha especificado en el *nombre distinguido* del certificado de servidor cuando se creó el certificado.
- Para confirmar que el certificado de servidor está firmado por una autoridad de firma “de confianza”, el explorador compara la firma del certificado de servidor con la firma del certificado raíz almacenado en el explorador. Una fecha de expiración confirma si el certificado de servidor es vigente.

El Método 2 tiene las siguientes ventajas y desventajas.

- **Ventajas:**

- Antes de ser transmitidos, el nombre de usuario y contraseña y todos los datos a y desde la PDU de rack son cifrados.
- Usted elige la longitud de la *clave pública* (clave RSA) que se utiliza para el cifrado cuando se establece una sesión SSL (se puede utilizar 1024 bits, que es el valor predeterminado, o 2048 bits para proporcionar un cifrado complejo y un nivel elevado de seguridad).
- El certificado de servidor que se carga en la PDU de rack posibilita que SSL autentique que los datos se están recibiendo de o enviando a la PDU de rack correcta. Esto proporciona un nivel adicional de seguridad que va más allá del cifrado del nombre de usuario, la contraseña y los datos transmitidos.
- El certificado raíz que se instala en el explorador posibilita que el explorador autentique el certificado de servidor de la PDU de rack para proporcionar protección adicional contra el acceso no autorizado.

- **Desventaja:**

Como los certificados no tienen la firma digital de una Autoridad de certificación comercial, se debe cargar un certificado raíz individualmente en el almacén (cache) de certificados del explorador de cada usuario. (Los fabricantes de exploradores ya proporcionan certificados raíz para Autoridades de certificación comerciales en el almacén de certificados del explorador, tal como se describe en Método 3.)

Método 3: Utilizar el Rack PDU Security Wizard para crear una solicitud de firma de certificado para que sea firmada por el certificado raíz de una Autoridad de certificación externa y para crear un certificado de servidor.

Utilice el Rack PDU Security Wizard para crear una solicitud (un archivo **.csr**) para enviarla a una Autoridad de certificación. La Autoridad de certificación devuelve un certificado firmado (un archivo **.crt**) basado en la información que se ha enviado en la solicitud. Utilice entonces el Rack PDU Security Wizard para crear un certificado de servidor (un archivo **.p15**) que incluye la firma del certificado raíz devuelto por la Autoridad de certificación. Cargue el certificado de servidor en la PDU de rack.



También puede utilizar el Método 3 si su empresa o agencia opera su propia Autoridad de certificación. Utilice el Rack PDU Security Wizard de la misma forma, pero use su propia Autoridad de certificación en vez de una Autoridad de certificación comercial.

El Método 3 tiene las siguientes ventajas y desventajas.

- **Ventajas:**

- Antes de ser transmitidos, el nombre de usuario y contraseña y todos los datos a y desde la PDU de rack son cifrados.
- Tiene el beneficio de una autenticación por una Autoridad de certificación que ya tiene un certificado raíz firmado en el cache de certificados del explorador. (Los certificados CA de Autoridades de certificación comerciales se distribuyen como parte del software del explorador, y es probable que una Autoridad de certificación de su propia empresa o agencia haya cargado ya su certificado CA en el almacén de certificados del explorador de cada usuario.) Por lo tanto, no es necesario cargar un certificado raíz en el explorador de cada usuario que necesite acceso a la PDU de rack.
- Usted elige la longitud de la *clave pública* (clave RSA) que se utiliza para establecer una sesión SSL (se puede utilizar 1024 bits, que es el valor predeterminado, o 2048 bits para proporcionar un cifrado complejo y un nivel elevado de seguridad).
- El certificado de servidor que se carga en la PDU de rack posibilita que SSL autentique que los datos se están recibiendo de o enviando a la PDU de rack correcta. Esto proporciona un nivel adicional de seguridad que va más allá del cifrado del nombre de usuario, la contraseña y los datos transmitidos.
- El explorador coteja la firma digital del certificado de servidor que se ha cargado en la PDU de rack con la firma del certificado raíz CA que ya está en el cache de certificados del explorador para proporcionar protección adicional contra el acceso no autorizado.

- **Desventajas:**

- Su instalación requiere el paso adicional de solicitar un certificado raíz firmado a una Autoridad de certificación.
- Una Autoridad de certificación externa puede cobrar una cantidad por el suministro de certificados firmados.

Cortafuegos

Aunque algunos métodos de autenticación proporcionan un mayor nivel de seguridad que otros, la protección completa frente a las infracciones de seguridad es casi imposible de conseguir. Los - cortafuegos correctamente configurados constituyen un elemento fundamental en el esquema de seguridad global.

Uso del Rack PDU Security Wizard (Asistente para la seguridad de la PDU de rack)

El Rack PDU Security Wizard crea los componentes necesarios para obtener una alta seguridad para una PDU de rack en la red cuando se usa Secure Sockets Layer (SSL) y los protocolos y rutinas de cifrado relacionados.

Autenticación mediante certificados y claves de host

La *Autenticación* verifica la identidad de un usuario o un dispositivo en red (como, por ejemplo, una PDU de rack). Las contraseñas normalmente identifican a los usuarios de ordenador. Sin embargo, para las transacciones o comunicaciones que requieren métodos de seguridad más estrictos en Internet, la PDU de rack acepta métodos de autenticación más seguros.

- Secure Sockets Layer (SSL), que se usa para un acceso Web seguro, utiliza certificados digitales para la autenticación. Se emite un certificado *raíz* CA digital por una Autoridad de certificación (CA) como parte de una infraestructura de clave pública, y su firma digital debe coincidir con la firma digital de un certificado de servidor en la PDU de rack.
- Secure Shell (SSH), que se usa para el acceso de terminal remoto a la interfaz de línea de comandos de la PDU de rack, utiliza una *clave de host* pública para la autenticación.

Cómo se usan los certificados. La mayoría de los exploradores Web, incluidos todos los exploradores aceptados por las PDU de rack, contienen un conjunto de certificados raíz CA de todas las Autoridades de certificación comerciales.

Tiene lugar una autenticación del servidor (en este caso, la PDU de rack) cada vez que se realiza una conexión del explorador con el servidor. El explorador realiza comprobaciones para estar seguro de que el certificado del servidor está firmado por una Autoridad de certificación conocida para el explorador.

Para que tenga lugar una autenticación:

- Cada servidor (PDU de rack) con SSL activado debe tener un certificado de servidor en el servidor mismo.
- Cualquier explorador que se use para acceder a la interfaz Web de la PDU de rack debe contener el certificado raíz CA que firmó el certificado de servidor.

Si la autenticación falla, un mensaje del explorador le pregunta si desea continuar aunque no pueda autenticar el servidor.

Si su red no requiere la autenticación proporcionada por los certificados digitales, puede utilizar el certificado predeterminado que la PDU de rack genera automáticamente. La firma digital del certificado predeterminado no será reconocida por los exploradores, pero un certificado predeterminado le permite utilizar SSL para el cifrado de los nombres de usuario, contraseñas y datos transmitidos. (Si utiliza el certificado predeterminado, el explorador le pregunta si acepta un acceso no autenticado antes de iniciarle una sesión en la interfaz Web de la PDU de rack.)

Cómo se usan las claves de host SSH. Una *clave de host* SSH autentica la identidad del servidor (la PDU de rack) cada vez que un cliente SSH contacta con ese servidor. Cada servidor con SSH activado debe tener una clave de host SSH en el servidor mismo.

Archivos que se crean para obtener seguridad SSL y SSH

Utilice el Rack PDU Security Wizard para crear estos componentes de un sistema de seguridad SSL y SSH:

- El certificado de servidor para la PDU de rack, si desea los beneficios de autenticación que proporciona un certificado como éste. Se puede crear cualquiera de los dos tipos de certificado de servidor siguientes:
 - Un certificado de servidor firmado por un certificado raíz CA personalizado también creado con el Rack PDU Security Wizard. Use este método si su empresa o agencia no tiene su propia Autoridad de certificación y no desea utilizar una Autoridad de certificación externa para firmar el certificado de servidor.
 - Un certificado de servidor firmado por una Autoridad de certificación externa. Esta Autoridad de certificación puede ser una que sea gestionada por su propia empresa o agencia o una de las Autoridades de certificación comerciales cuyos certificados raíz CA se distribuyen como parte del software de un explorador.
- Una solicitud de firma de certificado que contenga toda la información que se requiere para un certificado de servidor excepto la firma digital. Se necesita esta solicitud si se utiliza una Autoridad de certificación externa.
- Un certificado raíz CA.
- Una clave de host SSH que su programa cliente SSH utiliza para autenticar la PDU de rack cuando se inicia una sesión en la interfaz de línea de comandos.



Usted define si las claves públicas para los certificados SSL y las claves de host para SSH que se crean con el Rack PDU Security Wizard son claves RSA de 1024 bits (el valor predeterminado), o claves RSA de 2048 bits, que proporcionan un cifrado complejo y un nivel más elevado de seguridad.



Si no se crean y utilizan certificados de servidor SSL y claves de host SSH con el Rack PDU Security Wizard, la PDU de rack genera claves RSA de 2048 bits.

Sólo los productos Dell PDU de rack pueden utilizar certificados de servidor, claves de host y certificados raíz CA creados por el Rack PDU Security Wizard. Esos archivos no funcionan con productos tales como OpenSSL® y Microsoft® Internet Information Services (IIS).

Creación de un certificado raíz y de certificados de servidor

Resumen

Use este procedimiento si su empresa o agencia no tiene su propia Autoridad de certificación y no desea utilizar una Autoridad de certificación comercial para firmar los certificados de servidor.



Defina el tamaño de la clave RSA pública que forma parte del certificado generado por el Rack PDU Security Wizard. Se puede generar una clave de 1024 bits, o una clave de 2048 bits, que proporciona un cifrado complejo y un nivel más elevado de seguridad. (La clave predeterminada generada por la PDU de rack, si no utiliza el Asistente, es de 2048 bits.)

- Crear un certificado raíz CA que firme todos los certificados de servidor que se vayan a utilizar con la PDU de rack. Durante esa tarea, se crean dos archivos:
 - El archivo con el sufijo **.p15** es un archivo cifrado que contiene la clave privada y el certificado raíz público de la Autoridad de certificación. Este archivo firma los certificados de servidor.
 - El archivo con el sufijo **.crt** contiene sólo el certificado raíz público de la Autoridad de certificación. Cargue este archivo en cada explorador Web que se vaya a usar para acceder a la PDU de rack para que el explorador pueda validar el certificado de servidor de esa PDU de rack.
- Crear un certificado de servidor, que se almacena en un archivo con un sufijo **.p15**. Durante esa tarea, se le solicita el certificado raíz CA que firma el certificado de servidor.
- Cargar el certificado de servidor en la PDU de rack.
- Para cada PDU de rack que necesite un certificado de servidor, repita las tareas que crean y cargan el certificado de servidor.

El procedimiento

Crear el certificado raíz CA.

1. Si el Rack PDU Security Wizard no está instalado ya en su ordenador, obtenga y ejecute el programa de instalación (**Rack PDU Security Wizard.exe**).
2. En el menú **Inicio** de Windows, seleccione **Programas** y a continuación **Rack PDU Security Wizard**.
3. En la pantalla con el rótulo **Step 1** (Paso 1), seleccione **CA Root Certificate** (Certificado raíz CA) como tipo de archivo para crear, y luego seleccione la longitud de la clave que generar (use 1024 bits, que es el valor predeterminado, o 2048 bits para proporcionar un cifrado complejo y un nivel elevado de seguridad).
4. Introduzca un nombre para este archivo, que contendrá el certificado raíz público y la clave privada de la Autoridad de certificación. El archivo debe tener un sufijo **.p15** y, de manera predeterminada, se creará en la carpeta de instalación **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. En la pantalla con el rótulo **Step 2** (Paso 2), proporcione la información para configurar el certificado raíz CA. Los campos **Country** (País) y **Common Name** (Nombre común) son los únicos campos que se requieren. Para el campo **Common Name**, introduzca un nombre identificador de su empresa o agencia. Use únicamente caracteres alfanuméricos, sin espacios.



De manera predeterminada, un certificado raíz CA es válido durante 10 años a partir de la fecha y hora actual, pero se pueden modificar los campos **Validity Period Start** (Inicio del periodo de validez) y **Validity Period End** (Fin del periodo de validez).

6. En la pantalla siguiente, revise el resumen del certificado. Desplace la pantalla hacia abajo para ver el número de serie y huellas digitales únicos del certificado. Para realizar cualquier cambio en la información que ha suministrado, haga click en **Back** (Atrás). Revise la información.



La información del tema del certificado y la información del emisor del certificado deben ser idénticas.

7. La última pantalla verifica que se ha creado el certificado y muestra información que se necesita para las próximas tareas:
 - La ubicación y el nombre del archivo **.p15** que se va a utilizar para firmar los certificados de servidor.
 - La ubicación y el nombre del archivo **.crt** , que es el certificado raíz CA para cargar en el explorador de cada usuario que necesite acceder a la PDU de rack.

Cargar el certificado raíz CA en su explorador. Cargue el archivo **.crt** en el explorador de cada usuario que necesite acceder a la PDU de rack.



Consulte el sistema de ayuda del explorador para obtener información sobre cómo cargar el archivo **.crt** en el almacén (cache) de certificados del explorador. A continuación se expone un resumen del procedimiento para Microsoft Internet Explorer.

1. Seleccione **Herramientas** y a continuación **Opciones de Internet** en la barra de menú.
2. En el cuadro de diálogo, en la ficha **Contenido** haga clic en **Certificados** y luego en **Importar**.
3. El Asistente para importación de certificados le guía hasta el final del procedimiento. El tipo de archivo que hay que seleccionar es X.509, y el Certificado raíz público CA es el archivo **.crt** creado en el procedimiento **Creación de un certificado raíz y de certificados de servidor**.

Crear un certificado de usuario de servidor SSL.

1. En el menú **Inicio** de Windows, seleccione **Programas** y a continuación **Rack PDU Security Wizard**.
2. En la pantalla con el rótulo **Step 1** (Paso 1), seleccione **SSL Server Certificate** (Certificado de servidor SSL) como tipo de archivo, y luego seleccione la longitud de la clave que generar (use 1024 bits, que es el valor predeterminado, o 2048 bits para proporcionar un cifrado complejo y un nivel elevado de seguridad).
3. Introduzca un nombre para este archivo, que contendrá el certificado de servidor y la clave privada. El archivo debe tener un sufijo **.p15** y, de manera predeterminada, se creará en la carpeta **C:\Program Files\Dell\Rack PDU Security Wizard**.
4. Haga clic en **Buscar**, y seleccione el certificado raíz CA creado en el procedimiento [Creación de un certificado raíz y de certificados de servidor](#). El certificado raíz CA se usa para firmar el Certificado de usuario de servidor que se está generando.

5. En la pantalla con el rótulo **Step 2** (Paso 2), proporcione la información para configurar el certificado de servidor. **Country** (País) y **Common Name** (Nombre común) son los únicos campos que se requieren. Para el campo **Common Name**, introduzca la dirección IP o el nombre DNS del servidor (la PDU de rack). De manera predeterminada, un certificado de servidor es válido durante 10 años, pero se pueden modificar los campos **Validity Period Start** (Inicio del periodo de validez) y **Validity Period End** (Fin del periodo de validez).



Como la información de configuración forma parte de la firma, la información de cada certificado debe ser única. La configuración de un certificado de servidor no puede ser la misma que la configuración del certificado raíz CA. (La fecha de expiración no se considera como parte de la configuración única. Alguna otra información de configuración también debe diferir.)

6. En la pantalla siguiente, revise el resumen del certificado. Desplace la pantalla hacia abajo para ver el número de serie y huellas digitales únicos del certificado. Para realizar cualquier cambio en la información que ha suministrado, haga click en **Back** (Atrás). Revise la información.
7. La última pantalla verifica que se ha creado el certificado y le indica que cargue el certificado de servidor en la PDU de rack. Muestra la ubicación y el nombre del Certificado de servidor, que tiene un sufijo de archivo **.p15** y contiene la clave privada y el certificado raíz público de la PDU de rack.

Cargue el certificado de servidor en la PDU de rack.

1. En la ficha **Administración**, seleccione **Red** en la barra de menú superior y **certificado ssl** bajo el encabezamiento **Web** en el menú de navegación izquierdo.

2. Seleccione **Agregar o reemplazar Archivo de certificado**, y busque el certificado de servidor, el archivo **.p15** que se ha creado en el procedimiento **Creación de un certificado raíz y de certificados de servidor**. (La ubicación predeterminada es **C:\Program Files\Dell\Rack PDU Security Wizard**.)



Se puede utilizar FTP o Secure CoPy (SCP) en su lugar para transferir el certificado de servidor. Con SCP, el comando para transferir un certificado de nombre **cert.p15** a una PDU de rack con una dirección IP de 156.205.6.185 sería:

```
scp cert.p15 dell@156.205.6.185
```

Creación de un certificado de servidor y una solicitud de firma

Resumen

Use este procedimiento si su empresa o agencia tiene su propia Autoridad de certificación o si piensa utilizar una Autoridad de certificación comercial para firmar los certificados de servidor.

- Crear una Solicitud de firma de certificado (CSR). La CSR contiene toda la información de un certificado de servidor excepto la firma digital. Este proceso crea dos archivos de salida:
 - El archivo con el sufijo **.p15** contiene la clave privada de la PDU de rack.
 - El archivo con el sufijo **.csr** contiene la solicitud de firma de certificado, que se envía a una Autoridad de certificación externa.
- Cuando reciba el certificado firmado de la Autoridad de certificación, importe ese certificado. La importación del certificado combina el archivo **.p15** que contiene la clave privada y el archivo que contiene el certificado firmado de la Autoridad de certificación externa. El archivo de salida es un nuevo archivo de certificado de servidor cifrado con un sufijo **.p15**.
- Cargar el certificado de servidor en la PDU de rack.
- Para cada PDU de rack que necesite un certificado de servidor, repita las tareas que crean y cargan el certificado de servidor.

El procedimiento

Crear la Solicitud de firma de certificado (CSR).

1. Si el Rack PDU Security Wizard no está instalado ya en su ordenador, obtenga y ejecute el programa de instalación (**Rack PDU Security Wizard.exe**).
2. En el menú **Inicio** de Windows, seleccione **Programas** y a continuación **Rack PDU Security Wizard**.

3. En la pantalla con el rótulo **Step 1** (Paso 1), seleccione **Certificate Request** (Solicitud de certificado) como tipo de archivo para crear, y luego seleccione la longitud de la clave que generar (use 1024 bits, que es el valor predeterminado, o 2048 bits para proporcionar un cifrado complejo y un nivel elevado de seguridad).
4. Introduzca un nombre para este archivo, que contendrá la clave privada de la PDU de rack. El archivo debe tener un sufijo **.p15** y, de manera predeterminada, se creará en la carpeta de instalación **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. En la pantalla con el rótulo **Step 2** (Paso 2), proporcione la información para configurar la solicitud de firma de certificado (CSR), es decir, la información que desea que contenga el certificado de servidor firmado. Los campos **Country** (País) y **Common Name** (Nombre común) son necesarios. Los demás campos son opcionales. Para el campo **Common Name**, introduzca la dirección IP o el nombre DNS de la PDU de rack.



De manera predeterminada, un certificado de servidor es válido durante 10 años a partir de la fecha y hora actual, pero se pueden modificar los campos **Validity Period Start** (Inicio del periodo de validez) y **Validity Period End** (Fin del periodo de validez).

6. En la pantalla siguiente, revise el resumen del certificado. Desplace la pantalla hacia abajo para ver el número de serie y huellas digitales únicos del certificado. Para realizar cualquier cambio en la información que ha suministrado, haga click en **Back** (Atrás). Revise la información.



La información del tema del certificado y la información del emisor del certificado deben ser idénticas.

7. La última pantalla verifica que se ha creado la solicitud de firma de certificado y muestra la ubicación y el nombre del archivo, que tiene una extensión **.csr**.

- Envíe la solicitud de firma de certificado a una Autoridad de certificación externa, bien sea una Autoridad de certificación comercial o, si procede, una Autoridad de certificación gestionada por su propia empresa o agencia.



Consulte las instrucciones proporcionadas por la Autoridad de certificación respecto a la firma y emisión de certificados de servidor.

Importar el certificado firmado. Cuando la Autoridad de certificación externa devuelva el certificado firmado, importe el certificado. Este procedimiento combina el certificado firmado y la clave privada en un certificado de servidor SSL que entonces se carga en la PDU de rack.

- En el menú **Inicio** de Windows, seleccione **Programas** y a continuación **Rack PDU Security Wizard**.
- En la pantalla con el rótulo **Step 1** (Paso 1), seleccione **Import Signed Certificate** (Importar certificado firmado).
- Busque y seleccione el certificado de servidor firmado que ha recibido de la Autoridad de certificación externa. El archivo tiene un sufijo **.cer** o **.crt**.
- Busque y seleccione el archivo que ha creado en el **paso 4** de la tarea **Crear la Solicitud de firma de certificado (CSR)**. Este archivo tiene una extensión **.p15**, contiene la clave privada de la PDU de rack, y, de manera predeterminada, está en la carpeta de instalación **C:\Program Files\Dell\Rack PDU Security Wizard**.
- Especifique un nombre para el archivo de salida que va a ser el certificado de servidor firmado que se carga en la PDU de rack. El archivo debe tener un sufijo **.p15**.
- Haga clic en **Next** (Siguiendo) para generar el certificado de servidor. La **Issuer Information** (Información del emisor) en la pantalla resumen confirma que la Autoridad de certificación externa ha firmado el certificado.
- La última pantalla verifica que se ha creado el certificado y le indica que cargue el certificado de servidor en la PDU de rack. Muestra la ubicación y el nombre del certificado de servidor, que tiene una extensión de archivo **.p15** y contiene la clave privada de la PDU de rack y la clave pública obtenida del archivo **.cer** o **.crt**.

Cargue el certificado de servidor en la PDU de rack.

1. En la ficha **Administración**, seleccione **Red** en la barra de menú superior y **certificado ssl** bajo el encabezamiento **Web** en el menú de navegación izquierdo.
2. Seleccione **Agregar o reemplazar Archivo de certificado**, y busque el certificado de servidor, el archivo **.p15** que se ha creado en el procedimiento **Creación de un certificado raíz y de certificados de servidor**. (La ubicación predeterminada es **C:\Program Files\Dell\Rack PDU Security Wizard**.)



También se puede utilizar FTP o Secure CoPy (SCP) para transferir el certificado de servidor a la PDU de rack. Con SCP, el comando para transferir un certificado de nombre **cert.p15** a una PDU de rack con una dirección IP de 156.205.6.185 sería:

```
scp cert.p15 dell@156.205.6.185
```

Creación de una clave de host SSH

Resumen

Este procedimiento es opcional. Si selecciona cifrado SSH, pero no crea una clave de host, la PDU de rack genera una clave RSA de 2048 bits cuando se reinicia. Usted define si las claves de host para SSH que se crean con el Rack PDU Security Wizard son claves RSA de 1024 bits o de 2048 bits.



Se puede generar una clave de 1024 bits, o una clave de 2048 bits, que proporciona un cifrado complejo y un nivel mayor de seguridad.

- Utilizar el Rack PDU Security Wizard para crear una clave de host, que se cifra y se guarda en un archivo con el sufijo **.p15**.
- Cargar la clave de host en la PDU de rack.

El procedimiento

Crear la clave de host.

1. Si el Rack PDU Security Wizard no está instalado ya en su ordenador, obtenga y ejecute el programa de instalación (**Rack PDU Security Wizard.exe**).
2. En el menú **Inicio** de Windows, seleccione **Programas** y a continuación **Rack PDU Security Wizard**.
3. En la pantalla con el rótulo **Step 1** (Paso 1), seleccione **SSH Server Host Key** (Clave de host de servidor SSH) como tipo de archivo para crear, y luego seleccione la longitud de la clave que generar (use 1024 bits, que es el valor predeterminado, o 2048 bits para proporcionar un cifrado complejo y un nivel elevado de seguridad) .
4. Introduzca un nombre para este archivo, que contendrá la clave de host. El archivo debe tener un sufijo **.p15**. De manera predeterminada, el archivo se creará en la carpeta de instalación **C:\Program Files\Dell\Rack PDU Security Wizard**.
5. Haga clic en **Next** (Siguiente) para generar la clave de host.
6. La pantalla resumen muestra las huellas digitales SSH version 2, que son únicas para cada clave de host e identifican a la clave de host. Después de cargar la clave de host en la PDU de rack, se puede verificar que se ha cargado la clave de host correcta verificando que las huellas digitales mostradas aquí coinciden con las huellas digitales SSH de la PDU de rack, según se muestran por el programa cliente SSH.
7. La última pantalla verifica que se ha creado la clave de host, le indica que cargue la clave de host en la PDU de rack, y muestra la ubicación y el nombre de la clave de host, que tiene un sufijo de archivo **.p15**.

Cargar la clave de host en la PDU de rack.

1. En la ficha **Administración**, seleccione **Red** en la barra de menú superior y **clave de host ssh** bajo el encabezamiento **Consola** en el menú de navegación izquierdo.
2. Seleccione **Agregar o reemplazar Clave de host**, y busque (Browse) la clave de host, el archivo **.p15** que se ha creado en el procedimiento **Crear la clave de host**. (La ubicación predeterminada es **C:\Program Files\Dell\Rack PDU Security Wizard**.)
3. En la parte inferior de la página **User Host Key** (Clave de host de usuario), observe la huella digital SSH. Inicie una sesión en la PDU de rack a través del programa cliente SSH, y verifique que se ha cargado la clave de host correcta verificando que estas huellas digitales coinciden con las huellas digitales que muestra el programa cliente.



También se puede utilizar FTP o Secure CoPy (SCP) para transferir la clave de host a la PDU de rack. Con SCP, el siguiente comando transferiría una clave de host de nombre **hostkey.p15** a una PDU de rack con una dirección IP de 156.205.6.185:

```
scp hostkey.p15 dell@156.205.6.185
```

Acceso a la interfaz de línea de comandos y seguridad

Los usuarios con cuenta de Administrador o de Usuario de dispositivo pueden acceder a la interfaz de línea de comandos mediante Telnet o Secure Shell (SSH), dependiendo del método de acceso que esté activado. (Un administrador puede activar estos métodos de acceso seleccionando la ficha **Administración**, luego **Red** en la barra de menú superior y **acceso** bajo el encabezamiento **Consola** en el menú de navegación izquierdo.) De manera predeterminada, Telnet está activado. La activación de SSH desactiva Telnet automáticamente.

Telnet para un acceso básico. Telnet proporciona la seguridad básica de la autenticación por nombre de usuario y contraseña, pero no la elevada seguridad que ofrece el cifrado.

SSH para un acceso de alta seguridad. Si utiliza el acceso de alta seguridad de SSL para la interfaz Web, use Secure Shell (SSH) para acceder a la interfaz de línea de comandos. SSH cifra los nombres de usuario, las contraseñas y los datos transmitidos.

La interfaz, las cuentas de usuario y los derechos de acceso de usuario son los mismos, tanto si accede a la interfaz de línea de comandos mediante SSH como si lo hace a través de Telnet; sin embargo, para utilizar SSH, primero debe configurar SSH y tener instalado un programa cliente SSH en su ordenador.

Telnet y Secure Shell (SSH)

Mientras SSH está activado, no se puede utilizar Telnet para acceder a la interfaz de línea de comandos. La activación de SSH activa SCP automáticamente.



Cuando SSH está activado y su puerto está configurado, no se requiere ninguna configuración más para utilizar Secure CoPy (SCP). SCP usa la misma configuración que SSH.



Para usar SSH, debe tener instalado un cliente SSH. La mayoría de las plataformas Linux y UNIX[®] incluyen un cliente SSH, pero los sistemas operativos Windows de Microsoft no. Hay disponibles clientes SSH de diversos vendedores.

Para configurar las opciones de Telnet y Secure Shell (SSH):

1. En la ficha **Administración** de la interfaz Web, seleccione **Red** en la barra de menú superior, y a continuación la opción **acceso** bajo el encabezamiento **Consola** en el menú de navegación izquierdo.
2. Configure los parámetros de puerto para Telnet y SSH.



Para obtener información sobre la seguridad adicional que proporciona un puerto no estándar, véase [Asignaciones de puertos](#).

3. Bajo **Consola** en el menú de navegación izquierdo, seleccione **clave de host ssh**, especifique un archivo de clave de host creado anteriormente con el Rack PDU Security Wizard, y cárguelo en la PDU de rack.

Si no se especifica un archivo de clave de host aquí, si instala una clave de host no válida, o si activa SSH sin ninguna clave de host instalada, la PDU de rack genera una clave de host RSA de 2048 bits. Para que la PDU de rack cree una clave de host, debe reiniciarse. **La PDU de rack puede tardar hasta 1 minuto en crear esta clave de host, y SSH no está accesible durante ese tiempo.**



También, desde una interfaz de línea de comandos como, por ejemplo, el indicador de comando de un sistema operativo Windows, se puede utilizar FTP o Secure CoPy (SCP) para transferir el archivo de clave de host.

4. Muestre la *huella digital* de la clave de host SSH para SSH version 2. La mayoría de los clientes SSH muestran la huella digital al inicio de una sesión. Compare la huella digital mostrada por el cliente con la huella digital que se ha registrado desde la interfaz Web o la interfaz de línea de comandos de la PDU de rack.

Acceso a la interfaz Web y seguridad: HTTP y HTTPS (con SSL)

HyperText Transfer Protocol (HTTP) proporciona acceso por medio de nombre de usuario y contraseña, pero no cifra los nombre de usuario, las contraseñas ni los datos durante la transmisión. HyperText Transfer Protocol over Secure Sockets Layer (HTTPS) cifra los nombre de usuario, las contraseñas y los datos durante la transmisión, y proporciona autenticación de la PDU de rack por medio de certificados digitales.



Consulte [Creación e instalación de certificados digitales](#) para elegir entre los varios métodos para utilizar certificados digitales.

Para configurar HTTP y HTTPS:

1. En la ficha **Administración**, seleccione **Red** en la barra de menú superior y **acceso** bajo **Web** en el menú de navegación izquierdo.

2. Active HTTP o HTTPS y configure los puertos que va a utilizar cada uno de los dos protocolos. Los cambios surten efecto la próxima vez que se inicia una sesión. Cuando SSL está activado, el explorador muestra un pequeño icono de un candado.



Para obtener información sobre la seguridad adicional que proporciona un puerto no estándar, véase [Asignaciones de puertos](#).

3. Seleccione **certificado ssl** bajo **Web** en el menú de navegación izquierdo para determinar si está instalado un certificado de servidor en la PDU de rack. Si se ha creado un certificado con el Rack PDU Security Wizard pero no está instalado:
- En la interfaz Web, busque el archivo de certificado y cárguelo en la PDU de rack.
 - También, como alternativa, puede utilizar el protocolo Secure CoPy (SCP) o FTP para cargar el archivo de certificado en la PDU de rack.



Crear y cargar un certificado de servidor por adelantado reduce el tiempo que se requiere para activar HTTPS. Si se activa HTTPS sin ningún certificado de servidor cargado, la PDU de rack crea uno cuando se reinicia. **La PDU de rack puede tardar hasta 1 minuto en crear el certificado, y el servidor SSH no está disponible durante ese tiempo.**



Un certificado generado por la PDU de rack tiene algunas limitaciones. Consulte [Método 1: Usar el certificado predeterminado generado automáticamente por la PDU de rack](#).

4. Si está cargado un certificado de servidor digital, el campo **Status** muestra el enlace. **Certificado válido**. Haga clic en el enlace para mostrar los parámetros del certificado.

Parámetro	Descripción
Emitido para:	<p>Nombre común (CN): La dirección IP o el nombre DNS de la PDU de rack. Este campo controla cómo se debe iniciar una sesión en la interfaz Web.</p> <ul style="list-style-type: none"> • Si se especificó una dirección IP para este campo cuando se creó el certificado, utilice una dirección IP para iniciar una sesión. • Si se especificó el nombre DNS para este campo cuando se creó el certificado, utilice el nombre DNS para iniciar una sesión. <p>Si no se usa la dirección IP o el nombre DNS que se ha especificado para el certificado, la autenticación falla, y se recibe un mensaje de error preguntando si se desea continuar.</p> <p>Para un certificado de servidor generado de manera predeterminada por la PDU de rack, este campo muestra en su lugar el número de serie de la PDU de rack.</p> <p>Organización (O), Unidad organizativa (OU), y Localidad, País: El nombre, unidad organizativa y ubicación de la organización que está utilizando el certificado de servidor. Para un certificado de servidor generado de manera predeterminada por la PDU de rack, el campo Unidad organizativa (OU) muestra “Internally Generated Certificate” (Certificado generado internamente).</p> <p>Número de serie: El número de serie del certificado de servidor.</p>
Emitido por:	<p>Nombre común (CN): El Nombre común que se especifica en el certificado raíz CA. Para un certificado de servidor generado de manera predeterminada por la PDU de rack, este campo muestra en su lugar el número de serie de la PDU de rack.</p> <p>Organización (O) y Unidad organizativa (OU): El nombre y la unidad organizativa de la organización que ha emitido el certificado de servidor. Si el certificado de servidor ha sido generado de manera predeterminada por la PDU de rack o dispositivo, este campo muestra “Internally Generated Certificate” (Certificado generado internamente).</p>
Validez:	<p>Emitido el: La fecha y hora en que se ha emitido el certificado.</p> <p>Caduca el: La fecha y hora en que expira el certificado.</p>



Parámetro	Descripción
Huellas digitales	<p>Cada una de las dos huellas digitales es una cadena larga de caracteres alfanuméricos, puntuada mediante signos de dos puntos. Una huella digital es un identificador único para autenticar adicionalmente el servidor. Registre las huellas digitales para compararlas con las huellas digitales que contiene el certificado, según se muestran en el explorador.</p> <p>Huella digital SHA1: Una huella digital creada por un algoritmo Secure Hash Algorithm (SHA-1).</p> <p>Huella digital MD5: Una huella digital creada por un algoritmo Message Digest 5 (MD5).</p>

Funciones y servidores RADIUS aceptados

Funciones aceptadas

Funciones de autenticación y autorización aceptadas: Remote Authentication Dial-In User Service (RADIUS). Utilice RADIUS para administrar centralmente el acceso remoto para cada PDU de rack. Cuando un usuario accede a la PDU de rack, se envía una solicitud de autenticación al servidor RADIUS para determinar el nivel de permiso del usuario.



Para más información sobre los niveles de permiso, véase [Tipos de cuentas de usuario](#).

Servidores RADIUS aceptados

Servidores RADIUS aceptados: FreeRADIUS y Microsoft IAS 2003. Otras aplicaciones RADIUS comúnmente disponibles pueden funcionar pero no han sido probadas totalmente.

Configuración de la PDU de rack

Autenticación



Los nombres de usuario RADIUS que se utilizan con la PDU de rack están limitados a 32 caracteres.

En la ficha **Administración**, seleccione **Seguridad** en la barra de menú superior. A continuación, bajo **Usuarios remotos** en el menú de navegación izquierdo, seleccione **autenticación** para definir un método de autenticación:

- **Sólo autenticación local:** RADIUS se desactiva. La autenticación local se activa.
- **RADIUS, después autenticación local:** Se activa tanto la autenticación RADIUS como la local. La autenticación se solicita primero al servidor RADIUS; la autenticación local se utiliza sólo si el servidor RADIUS no responde.
- **RADIUS sólo:** RADIUS se activa. La autenticación local se desactiva.



Si está seleccionado **RADIUS sólo**, y el servidor RADIUS no está disponible, está identificado incorrectamente o está configurado incorrectamente, el acceso remoto no está disponible para ningún usuario. Debe utilizar una conexión serie con la interfaz de línea de comandos y cambiar el valor de acceso RADIUS a `local` o a `radiusLocal` para volver a conseguir acceso. Por ejemplo, el comando para cambiar el valor de acceso a `local` sería:

```
radius -a local
```

RADIUS

Para configurar RADIUS, en la ficha **Administración**, seleccione **Seguridad** en la barra de menú superior. A continuación, bajo **Usuarios remotos** en el menú de navegación izquierdo, seleccione **RADIUS**.

Parámetro	Definición
Servidor RADIUS	El nombre de servidor o la dirección IP del servidor RADIUS. NOTA: Los servidores RADIUS utilizan el puerto 1812 de manera predeterminada para autenticar a los usuarios. Para utilizar un puerto diferente, añada dos puntos seguido del número del nuevo puerto al final del nombre o dirección IP del servidor RADIUS.
Secreto	El secreto compartido entre el servidor RADIUS y la PDU de rack.
Tiempo de espera para respuesta	El tiempo en segundos que la PDU de rack espera a una respuesta del servidor RADIUS.
Probar configuración	Introduzca el nombre de usuario y la contraseña de Administrador para probar la ruta del servidor RADIUS que ha configurado.
Omitir prueba y aplicar	No probar la ruta del servidor RADIUS.

Si se listan dos servidores configurados y **RADIUS**, después autenticación local o **RADIUS sólo** es el método de autenticación activado, se puede cambiar el servidor RADIUS que autenticará a los usuarios haciendo clic en el botón **Cambiar prioridad de servidor**.

Configuración del servidor RADIUS

Debe configurar su servidor RADIUS para que funcione con la PDU de rack. Los ejemplos de esta sección pueden diferir algo del contenido o formato requerido de su servidor RADIUS concreto. En los ejemplos, cualquier referencia a tomas de corriente sólo es aplicable a dispositivos PDU de rack que admitan usuarios de toma de corriente.

1. Añada la dirección IP de la PDU de rack a la lista (archivo) de clientes de servidor RADIUS.
2. Los usuarios deben configurarse con atributos de tipo de servicio a menos que se definan atributos específicos del distribuidor en su lugar. Si no se configuran atributos de tipo de servicio, el usuario tiene acceso de sólo lectura (a la interfaz Web sólo). Los dos valores aceptables para Tipo de servicio son Administrative-User (6), que da al usuario permisos de Administrador, y Login-User (1), que da al usuario permisos de Dispositivo.



Consulte la documentación del servidor RADIUS para obtener información acerca del archivo de usuarios RADIUS.

Ejemplo utilizando atributos de tipo de servicio

En el siguiente ejemplo de un archivo de usuarios RADIUS:

- RPDUAdmin corresponde a **Service-Type** (Tipo de servicio): **Administrative-User**, (6)
- RPDUDevice corresponde a **Service-Type**: **Login-User**, (1)
- RPDUReadOnly corresponde a **Service-Type**: **null** (nulo)

```
RPDUAdmin      Auth-Type = Local, Password = "admin"  
                Service-Type = Administrative-User
```

```
RPDUDevice     Auth-Type = Local, Password = "device"  
                Service-Type = Login-User
```

```
RPDUReadOnly   Auth-Type = Local, Password = "readonly"
```

Ejemplos utilizando Atributos específicos del distribuidor

Se pueden utilizar Atributos específicos del distribuidor (VSAs) en vez de los atributos de Tipo de servicio proporcionados por el servidor RADIUS. Este método requiere una entrada en el diccionario y un archivo de usuarios RADIUS. En el archivo de diccionario, se pueden definir los nombres para las palabras clave ATTRIBUTE y VALUE, pero no los valores numéricos. Si se cambian los valores numéricos, la autenticación y autorización RADIUS no funcionará correctamente. Los VSA tienen prioridad sobre los atributos RADIUS estándar.

Archivo de diccionario. A continuación se muestra un ejemplo de un archivo de diccionario RADIUS (dictionary.dell):

```
#
# dictionary.dell
#
#
VENDOR    DELL 318
#
# Atributos
#
ATTRIBUTE DELL-Service-Type 1 integer DELL
ATTRIBUTE DELL-Outlets      2 string  DELL

VALUE DELL-Service-Type Admin      1
VALUE DELL-Service-Type Device     2
VALUE DELL-Service-Type ReadOnly   3
#
# Para dispositivos con usuarios de toma de corriente sólo
#
VALUE DELL-Service-Type Outlet     4
```

Archivo de usuarios RADIUS con VSAs. A continuación se muestra un ejemplo de un archivo de usuarios RADIUS con VSAs:

```
VSAdmin      Auth-Type = Local, Password = "admin"  
             DELL-Service-Type = Admin  
  
VSADevice    Auth-Type = Local, Password = "device"  
             DELL-Service-Type = Device  
  
VSAReadOnly  Auth-Type = Local, Password = "readonly"  
             DELL-Service-Type = ReadOnly  
  
# Dar al usuario acceso a las tomas de corriente (outlets)  
# de dispositivo 1, 2 y 3.  
VSAOutlet    Auth-Type = Local, Password = "outlet"  
             DELL-Service-Type = Outlet,  
             DELL-Outlets = "1,2,3"
```



Véase los siguientes temas relacionados:

- [Tipos de cuentas de usuario](#) para obtener información sobre los tres niveles de permiso de usuario básicos (Administrador, Usuario de dispositivo y Usuario de sólo lectura).
- [Servidores RADIUS aceptados](#) para obtener información sobre los servidores RADIUS probados y aceptados.

Ejemplo con contraseñas shadow UNIX. Si se usan archivos de contraseñas shadow UNIX (**/etc/passwd**) con los archivos de diccionario RADIUS, se pueden utilizar los dos métodos siguientes para autenticar a los usuarios:

- Si todos los usuarios UNIX tienen privilegios administrativos, añada lo siguiente al archivo de “usuarios” RADIUS. Para permitir sólo Usuarios de dispositivo, cambie Dell-Service-Type a **Device**.

```
DEFAULT    Auth-Type = System
           DELL-Service-Type = Admin
```

- Añada nombres de usuario y atributos al archivo de “usuarios” RADIUS, y verifique la contraseña frente a **/etc/passwd**. El ejemplo siguiente es para los usuarios **bconners** y **thawk**:

```
bconners   Auth-Type = System
           DELL-Service-Type = Admin

thawk      Auth-Type = System
           DELL-Service-Type = Outlet
           DELL-Outlets = "1,2,3"
```

Índice

A

Acceso

- a la interfaz de línea de comandos de manera remota 15
- activación o desactivación de métodos de acceso
 - a la interfaz de línea de comandos 169
 - a la interfaz Web 167
- prioridades 2
- resolución de problemas 199

Acceso de usuario, tipos de cuentas 3

Acceso del usuario

- identificación en la interfaz de la consola de control 19

Acciones de sucesos 144

- configuración por grupo 146
- configuración por suceso 145

Activar

- búsqueda inversa 128
- correo electrónico para un destinatario 150
- reenvío de correo electrónico a servidores SMTP externos 151
- Telnet 169
- versiones de SSH 169

Actualizar con NTP ahora, configuración de fecha y hora 179

Actualizar el firmware 191

Administración

- Menú Notificación 143
- Menú Red 157
- Menú Seguridad 135

Aplicar la hora del ordenador local 179

archivo event.txt

- contenido 132
- importar a una hoja de cálculo 132

Archivos de configuración de usuario

- anulación de valores específicos del dispositivo 186
- contenido 185
- exportación de la hora del sistema por separado 187
- mensajes por dispositivos no descubiertos 190
- personalización 187
- recuperación y exportación 185
- suceso de carga y mensajes de error 189
- uso de protocolos de transferencia de archivos para transferir 188
- uso del archivo como archivo de inicio con DHCP 162

archivos ini, Véase Archivos de configuración de usuario

Asignación de gravedad (parámetro Syslog) 155

Asistente para la seguridad

- certificados
 - para usarlos con una Autoridad de certificación 230
 - creación de certificados sin una Autoridad de certificación 224
 - creación de claves de host SSH 233
 - creación de solicitudes de firma 230

Autenticación

- con RADIUS 243
- con SNMPv3 211
- con SSL 214
- para la interfaz Web y la interfaz de línea de comandos 211

Autenticación de los usuarios por medio de RADIUS 137



B

BOOTP

Comunicación de la PDU de rack con el servidor BOOTP 6

LED de estado que indica solicitudes BOOTP 13

Botón Function (Función) 12

Búsqueda inversa 128

C

Campos de identificación en la pantalla principal 19

Capturas

receptores de capturas 152

Carga pico 96

restablecer, kWh
restablecer 99

Certificados

creación e instalación para SSL 215

elección del método a utilizar 215

métodos

Rack PDU Security Wizard crea todos los certificados 217

Usar el certificado predeterminado 216

Usar una Autoridad de certificación (CA) 218

Certificados de servidor

creación sin una Autoridad de certificación 224

para usarlos con una Autoridad de certificación 230

Certificados raíz, creación 224

Certificados, cómo crear, ver o quitar 168

Cierre de sesión automático por inactividad 142

Cifrado

con SNMPv3 212

con SSH y SCP para la interfaz de línea de comandos 212

con SSL para la interfaz Web 238

Cipher suites (Conjuntos de cifrado)

finalidad de los algoritmos y cifrados 214

Claves de host

agregar o reemplazar 170

creación con el Asistente para la seguridad 233

estado 170

transferencia a la PDU de rack 238

Código de instalación (parámetro Syslog) 155

Códigos de resultado de la última transferencia 196

Conector 10/100 base-T, panel frontal 12

Configuración

Autenticación RADIUS 139

SSH 237

SSL 238

Configuración de fecha y hora 179

Configuración de la hora 179

Configuración TCP/IP 5, 8

Contactos secos

configuración 124

entradas del panel frontal 11

Contraseñas

cambiar inmediatamente para mayor seguridad 209

definir para cada tipo de cuenta 136

para el depósito del registro de datos 131
recuperación 9

uso de puertos no estándar para obtener seguridad adicional 209

valor predeterminado para todos los tipos de cuenta 86

Correo electrónico
configuración de destinatarios 150
configuración de los parámetros de
notificación 148
mensaje de prueba 151
usar para enviar mensajes a un
buscapersonas 150

D

Desactivar
búsqueda inversa 128
correo electrónico para un destinatario 150
Telnet 169
uso de un servidor proxy 86

DHCP

Comunicación de la PDU de rack con el
servidor DHCP 7
cookie de distribuidor 161

Dirección de destinatario, destinatarios de
correo electrónico 150

Dirección de remitente (parámetro
SMTP) 149

DNS

especificación de servidores DNS por la
dirección IP 165
tipos de consulta 166

Duración del reinicio (Reboot Duration) 113

E

Encabezamientos de sección, archivo de
configuración de usuario
185

Envío de mensajes a buscapersonas
utilizando correo electrónico 150

Estado

en la pantalla principal de la consola de
control 20

Estado de alarma, contactos de entrada 124

Estado de la carga 96

Exploradores

Certificados CA en almacén (cache) del
explorador 214
icono de un candado cuando SSL está
instalado 213
mensajes de error 88
peligro de dejar el explorador abierto 214
tipos y versiones aceptados 85

F

Fecha y hora de inicio de sesión
consola de control 19

Ficha Device Manager (Administrador del
dispositivo) 96

Ficha Entorno 122

Ficha Inicio 92

Firmware

actualización de múltiples PDU de Rack 195
métodos de transferencia de archivos
FTP o SCP 193
XMODEM 195
ventajas de actualizar 191

Formato de fecha, configuración 180

Formatos de las direcciones URL 87

FTP

configuración de servidor 176
desactivar FTP si se usa SSH y SCP 213
para la transferencia de certificados de
servidor 229, 239
para la transferencia de claves de host 238
transferencia de archivos de firmware 193
uso de puertos no estándar para obtener
seguridad radical 209
utilizar para recuperar el registro de sucesos
o de datos 132

G

- Generación de capturas, para receptores de capturas 152
- Generación de mensajes (parámetro Syslog) 155
- Grupos de tomas de corriente
 - configuraciones típicas 107
 - creación de grupos locales 104
 - editar 105
 - eliminar 105
 - finalidad y ventajas 100
 - globales 99
 - habilitar 103
 - iniciadores 99
 - locales 99
 - reglas para la configuración 102
 - requisitos del sistema 101
 - seguidores 99
- Grupos de tomas de corriente globales 99
 - crear 105
 - verificación de la instalación y la configuración 109
- Grupos de tomas de corriente iniciadores 99
- Grupos de tomas de corriente locales 99
 - crear 104
- grupos de tomas de corriente seguidores 99

H

- Histéresis 123
- Horario de verano 180
- Huellas digitales, mostrar y comparar 238

I

- Identificación (Nombre, Ubicación y Contacto)
 - en la interfaz Web 178

- Identificación de contacto (con quién ponerse en contacto) 178
- Inicio de sesión
 - Interfaz Web 86
 - localmente (a través de un puerto serie) en la consola de control 17
 - prioridades de acceso 2
- Inicio del registro en una nueva ventana, necesidad de JavaScript. 126
- Interfaz de línea de comandos 15
 - acceso remoto 15
 - códigos de respuesta 24
 - configuración de los parámetros de TCP/IP 8
 - configuración del acceso 169
 - descripción de comandos 25
 - ? 25
 - about 25
 - alarmcount 26
 - boot 27
 - cd 28
 - console 29
 - date 30
 - date (fecha) 35
 - delete 31
 - devLowLoad 47
 - devNearOver 47
 - devOverLoad 48
 - devReading 49
 - devStartDly 50
 - dir 31
 - dns 32
 - eventlog 33
 - exit (salir) 33
 - format (formatear) 33
 - FTP 34
 - help 34
 - humLow 51
 - humMin 52
 - humReading 52
 - inNormal 53
 - inReading 53
 - netstat 35
 - olAssignUsr 54



- oICancelCmd 55
- oIDlyOff 56
- oIDlyOn 57
- oIDlyReboot 58
- oIGroups 59
- oILowLoad 60
- oIName 61
- oINearOver 62
- oIOff 63
- oIOffDelay 64
- oIOn 65
- oIOnDelay 66
- oIOverLoad 67
- oIRboot 70
- oIRbootTime 68
- oIReading 69
- oIStatus 71
- oIUnasgnUsr 72
- phLowLoad 73
- phNearOver 74
- phOverLoad 75
- phReading 76
- phRestrictn 77
- ping 36
- portSpeed 36
- prodInfo 78
- prompt 37
- quit (salir) 37
- radius 38
- reboot 39
- resetToDef 40
- sensorName 79
- system 41
- tcpip 42, 43
- tempHigh 80
- tempMax 81
- tempReading 82
- user 44
- userAdd 82
- userDelete 82
- userList 83
- userPasswd 83
- web 45
- whoami 84
- xferINI 46

- xferStatus 46

- inicio de sesión 15

- pantalla principal 18

- sintaxis de un comando 22

Interfaz Web 89

- configuración del acceso 167

- Formatos de las direcciones URL 87

- inicio de sesión 86

- resolución de problemas de acceso 199

Intervalo de actualización, configuración de fecha y hora 179

J

JavaScript, se requiere para iniciar el registro en una nueva ventana 126

L

LED 10/100, panel frontal 12, 14

LED de estado de la red, panel frontal 12, 13

LEDs de fase, panel frontal 11

Link (como parámetro de toma de corriente) 113

M

Mensajes de error

- explorador 88

- por valores anulados en archivo .ini 190

Menú Notificación 144

Menú Red 157

Menú Seguridad

- Parámetros RADIUS 244

- usuarios remotos, autenticación 243

Menús
Notificación 144
Red 157
Registros 125
Seguridad 135

N

Network Time Protocol (NTP) 179
Nombre de comunidad
 para receptores de capturas 153
Nombre de host de receptores de capturas 152
Nombre de host/IP NMS para receptores de capturas 152
Nombre de usuario
 valor predeterminado según el tipo de cuenta 86
Nombre de usuario, cambiar inmediatamente para mayor seguridad 209
Nombre del sistema 178
Nombres de usuario
 definir para cada tipo de cuenta. 136
 máximo número de caracteres para RADIUS 137
Notificación, retardo o repetición 145

O

Opciones de Acerca de
 para obtener información acerca de la PDU de rack 184

P

Palabra clave Override, archivo de configuración de usuario 186

Palabras clave de archivo de configuración de usuario 185
pantalla de LEDs, panel frontal 12
Pantalla principal
 estado 20
 fecha y hora de inicio de sesión 19
 Identificación del acceso del usuario 19
 Up Time (Tiempo de actividad) 19
 valores de firmware mostrados 19
 visualización de la identificación 19
Parámetro capturas de autenticación 153
Parámetro Servidor RADIUS 244
Parámetro Tiempo de espera para RADIUS 139, 244
Parámetros de toma de corriente configurar 113
 control de las tomas de corriente 110
PDU de Rack
 configuración del nombre y la ubicación 98
PDU de rack
 inicio 4
 panel frontal 11
 resolución de problemas de acceso 198
Preferencia de unidad 182
Probar
 ruta de servidor RADIUS 139
Prueba
 configuración de destinatario de correo electrónico 151
 Consulta DNS 166
 receptor de capturas 153
Puerto de sensor de temp/humedad, panel frontal 12
Puerto serie RJ-45, panel frontal 12
Puertos
 HTTP y HTTPS 167
 Servidor FTP 34, 176
 Servidor RADIUS 39, 139
 Telnet y SSH 169
Puertos, asignación 209

R

Rack PDU

Características del producto 1

RADIUS

configuración 139

configuración de servidor 140

servidores RADIUS admitidos 141

Registro de datos

importar a una hoja de cálculo 132

Parámetro Intervalo de registro 130

rotación (archivo) 131

uso de FTP o SCP para recuperarlo 132

Registro de sucesos

errores por valores anulados en archivo
.ini 190

presentación y uso 126

uso de FTP o SCP para recuperar 132

Reiniciar

tomas de corriente 111, 116

Reiniciar interfaz de administración 183

Requisitos del sistema, grupos de tomas de corriente 101

Resolución de problemas

lista de comprobaciones 198

problemas de acceso a la tarjeta de
administración 198

Valor RADIUS sólo cuando RADIUS no está
disponible 138

Restablecer sólo 183

Restablecer todo 183

Retardo de apagado (Power Off Delay) 113

Retardo de encendido (Power On Delay) 113

Retardo de inicio en frío (Coldstart Delay) 98

S

SCP

activado y configurado con SSH 213, 237
para la transferencia cifrada de archivos 212

para la transferencia de certificados de
servidor 229, 233

para la transferencia de claves de host 235

para una transferencia de archivos de alta
seguridad 176

transferencia de archivos de firmware 193

uso de un puerto no estándar 209

utilizar para recuperar el registro de sucesos
o de datos 132

Secure CoPy. Véase SCP.

Secure SHell. Consulte SSH.

Secure Sockets Layer. Véase SSL

Seguridad

autenticación

con SSH y SCP 212

por medio de certificados digitales con
SSL 214

por medio de RADIUS 243

cambiar inmediatamente el nombre de
usuario y la contraseña 209

cifrado con SSH y SCP 212

clientes SSH aceptados 237

cómo se usan las claves de host SSH 222

cómo se usan los certificados 222

desactivación de interfaces menos
seguras 212

desactivación de interfaces menos
seguras 213

resumen de los métodos de acceso 206

SCP como alternativa a FTP 213

solicitudes de firma de certificado 214

SSL

algoritmos y cifrados de cipher suites
(conjuntos de cifrado) 214

elección de un método para utilizar
certificados 215

uso de puertos no estándar para obtener
seguridad adicional 209

Sensor de humedad

configuración de umbrales 122

- Sensor de temperatura
 - configuración de umbrales 122
 - Servidor NTP principal 179
 - Servidor NTP secundario 179
 - Servidor SMTP
 - parámetros 149
 - seleccionar para destinatarios de correo electrónico 151
 - Servidor SMTP de destinatario 151
 - Servidor SMTP local
 - definir por dirección IP o nombre DNS 149
 - opción recomendada para enrutar el correo electrónico 151
 - Servidores proxy
 - configuración para no establecer un proxy para la PDU 86
 - desactivar el uso de 86
 - Sincronizar con el servidor NTP (Fecha y hora) 179
 - SNMP
 - acceso y control de acceso
 - SNMPv1 172
 - SNMPv3 173
 - capturas de autenticación 153
 - desactivar SNMPv1 para sistemas de alta seguridad 171
 - v1
 - Acceso de LECTURA 210
 - desactivar 210
 - v3
 - autenticación 211
 - cifrado 212
 - Solicitudes de firma 230
 - SSH 16
 - activar 237
 - cifrado 212
 - clave de host
 - como identificador que no se puede falsificar 212
 - creación con el Asistente para la seguridad 233
 - transferencia a la PDU de rack 238
 - claves de host 170
 - configuración 237
 - huellas digitales, mostrar y comparar 238
 - obtención de un cliente SSH 237
 - SSL
 - autenticación por medio de certificados digitales 214
 - cómo crear, ver o quitar certificados 168
 - solicitudes de firma de certificado 214
 - Suceso de carga 189
 - Sucesos de toma de corriente
 - descripción 111, 116
 - Sucesos recientes
 - Sucesos del dispositivo en la página Inicio 93
 - Syslog
 - asignación de gravedad de sucesos a prioridades Syslog 155
 - identificación del servidor y el puerto Syslog 154
- ## T
- Telnet 16
 - Tiempo de actividad en la interfaz Web 184
 - Tiempo de espera por inactividad 142
 - Tomas de corriente globales 99
 - Tomas de corriente globales 99
- ## U
- Ubicación (valor del sistema) 178
 - Umbrales de carga 97
 - Unidades de temperatura (Fahrenheit o Celsius) 182

- Up Time (Tiempo de actividad)
 - pantalla principal de la consola de control 19
- Usuarios locales, configuración del acceso de usuario 136
- Usuarios remotos
 - autenticación 137
 - configuración del acceso de usuario 137
- Utilidad Ping para resolución de problemas de acceso 198

V

- Velocidad de puerto Ethernet 164
- Velocidad de puerto, configuración para Ethernet 164
- Versiones de firmware mostradas en la pantalla principal 19
- Vínculos rápidos, configuración 184
- Vínculos, configuración 184
- Vínculos, rápidos 91

X

- XMODEM para transferir archivos de firmware 195

Z

- Zona horaria, para sincronizar con servidor NTP 179

**La información en este documento está sujeta a cambios sin previo aviso.
© 2010 Dell Inc. Todos los derechos reservados.**

La reproducción de estos materiales de cualquier manera sea la que sea sin el permiso por escrito de Dell Inc. está estrictamente prohibida.

Marcas comerciales utilizadas en este texto: *Dell* y el logotipo *DELL* son marcas comerciales de Dell Inc.

En este documento se pueden utilizar otras marcas y nombres comerciales para referirse a las entidades que reivindican las marcas y nombres o sus productos. Dell Inc. renuncia a todo interés propietario en marcas y nombres comerciales que no sean los propios.

11/2010 Número de pieza 990-3926-009

www.dell.com | support.dell.com