

Dell EMC Integrated Data Protection Appliance

Versión 2.2

Introducción

302-004-953

A01

Copyright © 2018 Dell Inc. o sus filiales. Todos los derechos reservados.

Publicado en Junio de 2018

Dell considera que la información de este documento es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA "TAL CUAL". DELL NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y, ESPECÍFICAMENTE, RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO. EL USO, LA COPIA Y LA DISTRIBUCIÓN DE CUALQUIER SOFTWARE DE DELL DESCRITO EN ESTA PUBLICACIÓN REQUIEREN LA LICENCIA DE SOFTWARE CORRESPONDIENTE.

Dell, EMC y otras marcas comerciales pertenecen a Dell Inc. o sus filiales. Las demás marcas comerciales pueden ser propiedad de sus respectivos dueños. Publicado en México.

Dirección local de EMC

EMC Argentina (Cono Sur) Tel. +54-11-4021-3622 <http://www.emc.com/es-ar/index.htm>

EMC México Tel. +52-55-5080-3700 <http://www.emc.com/es-mx/index.htm>

EMC Venezuela (Norte de Latinoamérica) Tel. +58-212-206-6911 <http://www.emc.com/es-ve/index.htm>

CONTENIDO

Capítulo 1	Introducción	5
	Alcance del documento y público de destino.....	6
	Características del producto.....	6
	Protección automática del sistema.....	7
	Descripción general de la conectividad de red.....	8
Capítulo 2	Configuración de DP4400	9
	Preparación del ambiente de red.....	10
	Hoja de trabajo de configuración.....	11
	Soporte en línea.....	11
	Conexión a ACM.....	11
	Asistente de configuración de redes.....	13
	Appliance Configuration Manager.....	15
	Bienvenido.....	15
	Licencia.....	15
	Ajustes generales.....	15
	Información del cliente.....	15
	Configuración manual de direcciones IP del componente.....	16
	Resumen.....	16
	Progreso de la configuración.....	16
	Configuración de Secure Remote Services para los componentes	16
	Próximos pasos.....	17
	Solución de problemas.....	17
Capítulo 3	Acerca del tablero	19
	Pestaña Home del tablero ACM.....	20
	Panel IDPA System Manager.....	21
	Panel Backup Server.....	22
	Panel Protection Storage.....	22
	Panel Reporting and Analytics.....	23
	Panel Search.....	23
	Panel Cloud Disaster Recovery.....	24
	Panel Virtualization.....	25
	Paneles Customer Support y General Settings.....	25
	Cuentas de usuario para los componentes.....	26
	Cambio de contraseñas y sincronización de los componentes.....	27
Capítulo 4	Ejecución de un respaldo de VM	29
	Descripción general de respaldos de VM.....	30
	Definición de los clientes de vCenter y VMware.....	30
	Implementación del proxy de Avamar.....	35
	Instalación del hot fix del proxy de Avamar.....	36
	Creación y ejecución de la política de respaldo.....	37
Capítulo 5	Restauración de un respaldo de VM	39
	Restauración de una máquina virtual	40

	Restauración mediante acceso instantáneo.....	43
	Restauración de archivos específicos.....	45
Capítulo 6	Generación de informes	47
	Creación de un informe.....	48

CAPÍTULO 1

Introducción

Esta sección contiene los siguientes temas:

- [Alcance del documento y público de destino.....](#) 6
- [Características del producto.....](#) 6
- [Protección automática del sistema.....](#) 7
- [Descripción general de la conectividad de red.....](#) 8

Alcance del documento y público de destino

En este documento, se describe IDPA y se explica cómo realizar la configuración inicial de software después de configurar el hardware del dispositivo. Además, se describe un número de procedimientos que puede usar para que IDPA esté en funcionamiento en un tiempo relativamente corto.

El público objetivo de este documento incluye personal de campo, partners y clientes responsables de la administración y la operación de IDPA.

Características del producto

IDPA proporciona una configuración simplificada y la integración de componentes de protección de datos en una solución consolidada.

Implementación y configuración simplificadas

IDPA modelo DP4400 es un sistema de 2U hiperconvergente que un usuario puede instalar y configurar en el sitio.

El software del sistema para cada componente se instala y se configura en la mayor medida posible antes de enviar el dispositivo. El dispositivo trae incorporado lo siguiente: aplicación de respaldo, almacenamiento de destino, creación de informes y analítica, búsqueda y Appliance Configuration Manager (ACM).

Esta versión incluye el IDPA System Manager y agrega la recuperación ante desastres en la nube (CDRA) opcional a la pila de software.

Administración centralizada

ACM proporciona una interfaz gráfica basada en Web para configurar, monitorear y actualizar el dispositivo. IDPA System Manager proporciona funcionalidades avanzadas de administración y monitoreo de IDPA desde un solo panel e incluye las siguientes características:

- Tableros integrales que incluyen la siguiente información del sistema de Avamar y IDPA:
 - Actividades de respaldo
 - Actividades de replicación
 - Capacidad
 - Estado
 - Alertas
- El monitoreo de múltiples funcionalidades incluye el estado del sistema y las actividades.
- Funcionalidades de administración para la aplicación de respaldo.
- Operaciones avanzadas de búsqueda y recuperación mediante la integración con Search.
- Funcionalidades de creación de informes.

Administración de respaldo

IDPA protege los clientes virtuales y físicos, los distintos tipos de sistemas de archivos, las aplicaciones y las bases de datos

Monitoreo y analítica

La función de monitoreo y analítica ofrece una sólida funcionalidad de creación de informes con secciones específicas para diversas funciones. Los informes lo ayudan a

recuperar información acerca del ambiente para que pueda revisar y analizar las actividades en el ambiente. Con estos informes, puede identificar interrupciones en el ambiente, diagnosticar problemas, planificar tareas para disminuir los riesgos y pronosticar tendencias futuras. Según los requisitos empresariales, puede ejecutar plantillas personalizadas de informes y de tableros según demanda o programadas en intervalos definidos.

El tablero de ACM muestra un resumen de la configuración de los componentes individuales y permite al administrador monitorear el dispositivo, cambiar los detalles de configuración o actualizar el sistema y sus componentes. El tablero también muestra información sobre las alertas de estado del dispositivo para el servidor y los componentes de VMware.

Search

La función Search proporciona una manera eficaz para buscar datos de respaldo dentro de IDPA y, a continuación, restaurar el respaldo o descargar los resultados de búsqueda. Las actividades de recopilación programadas se usan para recopilar e indexar los metadatos, que luego se almacenan dentro de IDPA.

Recuperación ante desastres

DD Cloud DR es una solución opcional que facilita la recuperación de máquinas virtuales en las instalaciones, ya que proporciona la capacidad de recuperar esas máquinas virtuales en la nube. DD Cloud DR se integra con la aplicación de respaldo dentro de IDPA para copiar los respaldos de datos de máquinas virtuales a la nube pública. A continuación, puede realizar pruebas de DR o conmutación por error de los ambientes de producción mediante la organización de una conversión completa de la máquina virtual a una instancia de Elastic Compute Cloud (EC2) de Amazon Web Services y mediante la ejecución de esta instancia en la nube.

CDRA es una aplicación incorporada que administra la implementación de la infraestructura necesaria para la nube y la copia de los respaldos de máquinas virtuales a la nube, y organiza la compresión, el cifrado y la copia de los datos respaldados de VM a la nube.

Nota

CDRA es opcional.

Escalabilidad

IDPA está diseñado para ser escalable, de modo que puede crecer con las necesidades cambiantes. La configuración básica de DP4400 incluye 24 TB de espacio de almacenamiento, que se puede expandir con licencia de capacidad adicional en incrementos de 12 TB hasta un máximo de 96 TB.

Soporte unificado

El mismo equipo de Servicio al cliente es compatible con el hardware y el software utilizados en el dispositivo.

Nota

IDPA es compatible con redes activadas para IPv4 y no se admite en un ambiente IPv6 puro o en redes de doble pila.

Protección automática del sistema

IDPA está configurado para protegerse contra la pérdida de datos con las aplicaciones de almacenamiento y respaldo incluidas en el sistema. El sistema está protegido con

trabajos de respaldo definidos e iniciados automáticamente, que se programan a diario y tienen un período de retención de 30 días. Los metadatos del sistema se protegen mediante respaldo de punto de control para el almacenamiento de destino interno.

Descripción general de la conectividad de red

Cuando se utiliza un rango de direcciones IP durante la configuración de IDPA, se asignan las direcciones IP en un orden estándar. Utilice la tabla a continuación para determinar qué dirección IP se asigna a un componente.

La primera columna de cada tabla, Asignación de rango de IP, es el valor que se debe agregar a la primera dirección IP en el rango.

Tabla 1 Asignaciones de rango de direcciones IP para DP4400

Asignación de rango de IP	Ejemplo	Componente	Campo asignado
+0	192.0.2.1	vCenter	Máquina virtual de VMware vCenter Server
+1	192.0.2.2	Almacenamiento de destino	IP de datos 1
+2	192.0.2.3	Almacenamiento de destino	IP de datos 2
+3	192.0.2.4	Almacenamiento de destino	IP de datos 3
+4	192.0.2.5	Aplicación de respaldo	IP del servidor
+5	192.0.2.6	Aplicación de respaldo	VM de proxy Avamar
+6	192.0.2.7	IDPA System Manager	VM de IDPA System Manager
+7	192.0.2.8	Analítica y creación de informes	Máquina virtual del host del servidor de aplicaciones
+8	192.0.2.9	Analítica y creación de informes	Máquina virtual del host del servidor de almacenamiento de datos
+9	192.0.2.10	Search	Máquina virtual del host del nodo de índice maestro
+10	192.0.2.11	DD Cloud DRCDRA (opcional)	Dispositivo virtual Data Domain Cloud Disaster Recovery (DD Cloud DR) Complemento de Cloud DR (CDRA)

CAPÍTULO 2

Configuración de DP4400

- [Preparación del ambiente de red](#)..... 10
- [Hoja de trabajo de configuración](#)..... 11
- [Appliance Configuration Manager](#)..... 15
- [Solución de problemas](#)..... 17

Preparación del ambiente de red

Antes de comenzar

Debe tener una computadora en la ubicación de instalación con lo siguiente:

- Un adaptador de alimentación, de C13 a NEMA 5-15 (para Norteamérica), o un cable de alimentación para el adaptador de alimentación de la laptop con un conector C13, que permite encender la laptop desde una PDU de rack
- Un puerto Ethernet
- Google Chrome 64.0.3282.140 o versiones posteriores, o Mozilla Firefox 47.2 o versiones posteriores

Nota

DP4400 es compatible con solo una red. No se admiten configuraciones de red independientes de administración, respaldo o replicación (por ejemplo, etiquetado de VLAN).

Se deben realizar los siguientes pasos antes de comenzar la configuración inicial con Appliance Configuration Manager:

Procedimiento

1. Identifique 14 direcciones IP sin asignar para los componentes de IDPA. Para simplificar la configuración, seleccione 14 direcciones contiguas.

Tenga en cuenta que todos los componentes deben ejecutarse en una única VLAN o subred, con la excepción de la interfaz de iDRAC, que puede estar en una VLAN o subred independiente. Para obtener más información acerca de las direcciones IP, consulte la [Descripción general de la conectividad de red](#) en la página 8.
2. Registre las 14 direcciones IP en el DNS con entradas de búsqueda directa e inversa para cada dirección. Asegúrese de que se puede realizar una operación de ping en el enrutador para las 14 direcciones IP.
3. Descargue los archivos de licencia para Data Domain Virtual Edition (DDVE), Avamar Virtual Edition (AVE) y Data Protection Advisor (DP Advisor) desde el sistema de administración de licencia electrónica (ELMS).

La persona de contacto en su orden de compra debería haber recibido un correo electrónico que explica cómo iniciar sesión en el servidor de ELMS y cómo descargar los archivos de licencia.

Hoja de trabajo de configuración

Sírvase de esta hoja de trabajo para recopilar y registrar la información a la hora de empezar a configurar el dispositivo mediante lo siguiente:

- Soporte en línea
- Asistente de configuración de redes
- *Appliance Configuration Manager* ACM

Soporte en línea

Registre la siguiente información relacionada con su cuenta de Soporte en línea:

Credenciales del servicio de soporte en línea

Se requiere su nombre de usuario y su contraseña para la configuración de Secure Remote Services (anteriormente conocido como ESRS). Para crear una cuenta de Soporte en línea, visite support.emc.com.

ID de sitio

Se crea un ID de sitio en los sistemas de soporte para cada ubicación de su organización donde se han instalado productos de Dell EMC. Se requiere su ID de sitio durante la configuración inicial. Verifique su número de ID de sitio en Soporte en línea:

1. Inicie sesión en Soporte en línea con sus credenciales.
2. Seleccione **Centro de servicios**.
3. En la sección **Administración** de la página Centro de servicios, haga clic en **Ver y administrar la información de la empresa**.
4. Haga clic en **Ver sitios** y asegúrese de que el sitio donde se instaló IDPA aparezca en el área Mis sitios.

Nota

También puede buscar un sitio y agregarlo a la lista Mis sitios. Si no está disponible un ID de sitio o si el ID de sitio correcto no aparece en la lista, debe notificar al representante de campo local para solicitar uno.

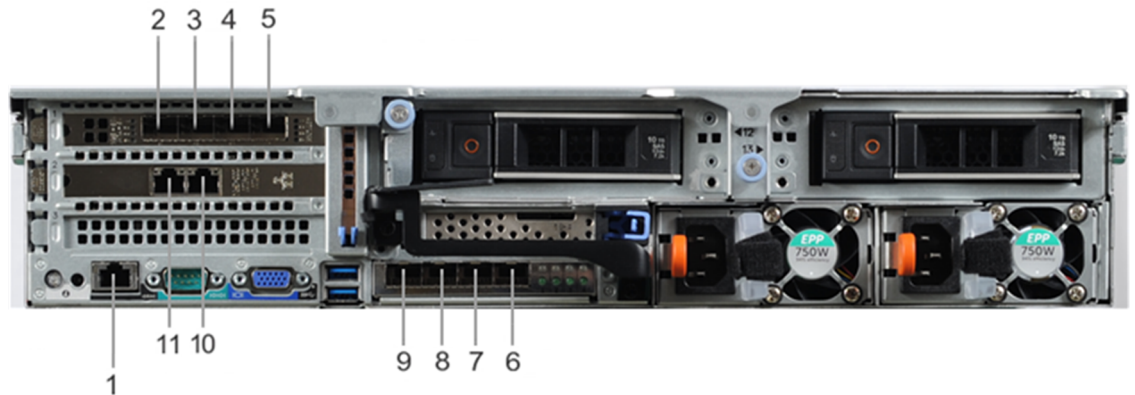
Conexión a ACM

Conéctese a la interfaz del usuario de ACM y comience el proceso de configuración. Para obtener una experiencia sin inconvenientes, habilite las conexiones de red pública y privada en su computadora de servicio.

Antes de comenzar

- Después de encender el dispositivo, espere cinco minutos para que finalice el arranque.
- Verifique que la computadora de servicio esté conectada al puerto GbE identificado como (10) en [Figura 1](#) en la página 12.
- En la computadora de servicio, registre la configuración de la dirección IP para la interfaz de Ethernet que está conectada a DP4400.

Figura 1 Conexiones de red de DP4400 y de iDRAC



Procedimiento

1. En la computadora de servicio, asigne la dirección IP estática 192.168.100.98 y la máscara de subred 255.255.255.0 para la interfaz de Ethernet que está conectada a DP4400.

La puerta de enlace predeterminada no es obligatoria.

2. Verifique que ACM responda a un ping en la dirección IP predeterminada de ACM, 192.168.100.100.
3. Para conectarse a la interfaz del usuario de ACM, escriba `https://192.168.100.100:8543/` en una ventana del navegador.
4. Inicie sesión en ACM con el nombre de usuario y la contraseña predeterminados de la cuenta del sistema:

- **Nombre de usuario:** root
- **Contraseña:** Idpa_1234

5. Proporcione una contraseña nueva cuando se le indique.

Nota

Esta contraseña se asignará a todos los componentes del dispositivo. Debe contener entre 9 y 20 caracteres e incluir al menos un carácter compatible de cada tipo. Los siguientes tipos de caracteres son compatibles:

- Letras en mayúscula (A-Z)
- Letras en minúscula (a-z)
- Números (0-9)
- Caracteres especiales: punto (.), guion (-) y guion bajo (_)

La contraseña no debe incluir nombres comunes o nombres de usuario como `root` o `admin`.

El sistema cierra la sesión después de cambiar la contraseña. Debe volver a iniciar sesión con la nueva contraseña.

6. En la pantalla **End User License Agreement**, acepte el EULA.

Resultados

Aparece la pantalla **Network Configuration**.

Asistente de configuración de redes

Después de aceptar el EULA, establezca la conectividad inicial con los componentes de DP4400.

La información que se necesita para esta sección está registrada en el *Cuestionario previo a la contratación de Integrated Data Protection Appliance*.

Nota

IDPA es compatible con redes activadas para IPv4 y no se admite en un ambiente IPv6 puro o en redes de doble pila.

Procedimiento

1. Proporcione la siguiente información para la configuración de redes básica:

Subnet mask

Máscara de dirección IP que identifica el rango de direcciones IP en la subred donde se conecta el dispositivo.

Nota

El DP4400 es compatible con solo una red. No son compatibles las configuraciones de red independientes de administración, respaldo o replicación (por ejemplo, el etiquetado de VLAN).

Gateway

Dirección IP de la puerta de enlace predeterminada del dispositivo.

Primary DNS server

Servidor DNS principal para el ambiente de red.

Secondary DNS server

Servidor DNS secundario para el ambiente de red.

Domain name

Nombre de dominio para el ambiente de red.

Appliance Configuration Manager IP

Dirección IP para asignar a ACM.

ESXi IP

Dirección IP para asignar al servidor ESXi.

2. Haga clic en **Submit**.

Requisitos posteriores

- Después de configurar las redes básicas, el navegador web enviará automáticamente a ACM la dirección IP asignada durante la configuración de redes.

Nota

Para que el envío automático funcione correctamente, la computadora que utilice para completar la configuración debe estar conectada a la misma red que la dirección IP configurada de ACM.

- Si no puede tener conexiones a redes públicas y privadas al mismo tiempo, desconéctese de la red de configuración de dispositivos privados y, luego, conéctese a la red en la que se encuentra la dirección IP de ACM para completar el resto de la configuración.
- Una vez que se complete la configuración de red, restablezca la configuración de la dirección IP del adaptador de red en la computadora de servicio a su estado anterior.

Appliance Configuration Manager

ACM lo guía a través de la configuración inicial de IDPA y prepara el dispositivo para su uso. Sírvese de la lista siguiente de pantallas y acciones relacionadas como guía durante el proceso de configuración inicial.

Para acceder a la interfaz del usuario de ACM, escriba la dirección IP que asignó a ACM en un navegador de la siguiente manera:

`https://<configured ACM IP address>:8543/dataprotection`

Bienvenido

Lea la información de requisitos previos y seleccione la casilla de verificación para aceptar.

(Opcional) Seleccione **Cloud Disaster Recovery**.

Nota

Si decide configurar **Cloud Disaster Recovery**, no puede quitarla de IDPA más tarde.

Licencia

Cargue los archivos de licencia Data Domain, Avamar y Data Protection Advisor que obtuvo de Soporte en línea.

Ajustes generales

Seleccione su zona horaria y escriba las direcciones IP del servidor NTP, SNMP y SMTP.

Nota

La IP del servidor SNMP es la dirección de un trap host externo. A pesar de que este es un valor obligatorio, puede ingresar la dirección IP de cualquier servidor al que pueda acceder si no hay un servidor SNMP disponible.

Seleccione **IP address range (11)** y, en el campo asociado, escriba la primera dirección IP en el rango secuencial de 11 direcciones IP para que IDPA la use. ACM asigna una dirección IP en el rango a cada máquina virtual de la configuración.

Nota

Se recomienda especificar un rango de IP. Los rangos de IP no son obligatorios, pero reducen la cantidad de direcciones IP que tienen que escribirse manualmente durante los pasos del asistente más tarde.

(Opcional) Para especificar las direcciones IP no secuenciales para cada máquina virtual en la configuración, no seleccione **IP address range**.

Información del cliente

Introduzca la información de contacto del cliente, incluidos el nombre, la dirección de correo electrónico y el número de contacto del administrador, y también el nombre de

la ubicación, el nombre de la empresa y el ID del sitio. El servicio al cliente usará esta información para ponerse en contacto con usted cuando sea necesario.

Configuración manual de direcciones IP del componente

Si seleccionó **IP address range** en la pantalla **General Settings**, vaya a [Resumen](#) en la página 16.

(Configuración manual) Si no seleccionó **IP address range** en la pantalla **General Settings**, escriba una dirección IP en cada campo en las siguientes pantallas:

- **vCenter**
- **Protection Storage**
- **Backup Server**
- **IDPA System Manager**
- **Reporting and Analytics**
- **Search**
- **Cloud Disaster Recovery** (si está seleccionada en la pantalla **Welcome**)

Resumen

Repase el resumen de configuración. Para realizar cambios, regrese a las pantallas anteriores.

Cuando la configuración sea correcta, haga clic en **Submit**. El proceso continúa automáticamente.

Nota

El proceso de configuración tarda varias horas en completarse y continúa por sí solo si se desconecta de DP4400. Si la sesión se interrumpe durante la configuración, verifique que esté conectado a la red y escriba la dirección IP de ACM en el navegador de la siguiente manera:

`https://<configured ACM IP address>:8543/dataprotection`

Si se le indica, inicie sesión con las credenciales de ACM para ver el estado actual del progreso de la configuración.

Progreso de la configuración

Una vez completado el proceso de configuración, puede descargar la información de configuración como un archivo PDF o XML.

Al finalizar, haga clic en **Finish**.

Configuración de Secure Remote Services para los componentes

(Opcional) Introduzca la dirección IP de la puerta de enlace de Secure Remote Services y sus credenciales de Soporte en línea para enviar la información del sistema de componentes al servicio al cliente y acelerar la resolución de problemas.

Nota

Este paso se repite para cada componente que se pueda registrar en Secure Remote Services.

Próximos pasos

Resultados

Aparece la pestaña **Home** del tablero de ACM. En la pestaña **Home** del tablero, puede ver los detalles del producto y la configuración de red; administrar la contraseña, la zona horaria y la configuración de NTP, SNMP y SMTP; y modificar la información de soporte del cliente.

Consulte [Acerca del tablero](#) en la página 19 para obtener más información sobre el uso del tablero de ACM para monitorear y administrar los componentes de IDPA.

Solución de problemas

Creación y descarga de un paquete de registro

Puede crear y descargar un paquete de registro que se puede analizar o enviar al servicio al cliente.

1. En ACM, haga clic en el icono del paquete de registro en la esquina superior derecha y seleccione **Create log bundle**.
2. En el cuadro de diálogo Create log bundle, seleccione los componentes que desee incluir en el paquete de registro y haga clic en OK.
3. Cuando se cree el paquete de registro, vuelva a seleccionar el icono del paquete de registro y seleccione **Download log bundle**. A continuación, especifique la ubicación de descarga y haga clic en OK.

Acceso a vCenter

Si necesita iniciar sesión en vCenter para solucionar un problema encontrado durante la instalación, utilice el usuario *idpauser@localos* y la contraseña común para IDPA. Esta cuenta de usuario tiene privilegios limitados, pero tiene acceso a información que puede ayudar a identificar y solucionar problemas.

CAPÍTULO 3

Acerca del tablero

El tablero de ACM le permite administrar la configuración para el dispositivo y los componentes individuales, actualizar información de soporte del cliente y actualizar el software para el dispositivo y sus componentes.

Para acceder al tablero, escriba `https://<ACM IP address>:8543/` en un navegador web e inicie sesión. El tablero requiere Google Chrome 64.0.3282.140 o versiones posteriores, o Mozilla Firefox 47.2 o versiones posteriores.

Nota

El tablero se activa solamente después de configurar IDPA.

En la vista inicial, se visualiza la página **Home** y las pestañas **Health** y **Upgrade**.

- [Pestaña Home del tablero ACM](#)..... 20
- [Panel IDPA System Manager](#)..... 21
- [Panel Backup Server](#)..... 22
- [Panel Protection Storage](#)..... 22
- [Panel Reporting and Analytics](#)..... 23
- [Panel Search](#)..... 23
- [Panel Cloud Disaster Recovery](#)..... 24
- [Panel Virtualization](#)..... 25
- [Paneles Customer Support y General Settings](#)..... 25
- [Cuentas de usuario para los componentes](#)..... 26
- [Cambio de contraseñas y sincronización de los componentes](#)..... 27

Pestaña Home del tablero ACM

La pestaña **Home** proporciona una descripción general del estado y la configuración para IDPA y cada componente.

En la pestaña **Home** del tablero, puede ver los detalles del producto y la configuración de red; administrar la contraseña, la zona horaria y la configuración de NTP, SNMP y SMTP; y modificar la información de soporte del cliente.

También puede configurar LDAP, crear y descargar paquetes de registros, actualizar la contraseña común en todos los componentes, registrar componentes con Secure Remote Services (anteriormente conocido como ESRS) e instalar los componentes opcionales (CDRA).

Nota

El vínculo de configuración de Secure Remote Services está presente en el menú del icono de engranaje. Mueva el cursor del mouse sobre el icono de engranaje para ver la lista de todas las opciones de menú.

Si falla DPS o DPA durante la configuración, ACM no detiene toda la configuración. El proceso de configuración sigue funcionando hasta completarse. Cuando finaliza el proceso de configuración, el tablero de ACM proporciona una opción para configurar el componente fallido (DPS o DPA).

Descarga de los detalles de configuración

Para descargar un archivo PDF con los detalles actuales de la configuración de IDPA, haga clic en el icono de Adobe PDF.

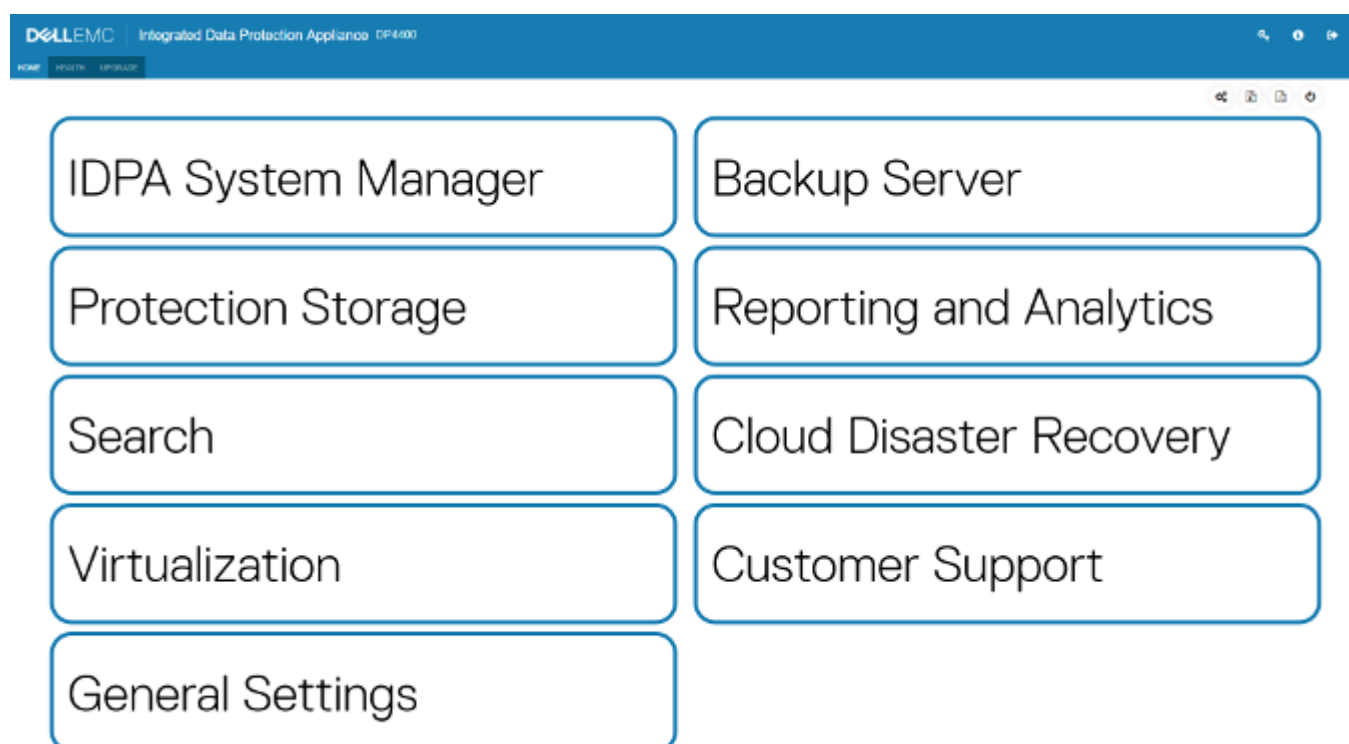
Administración de los componentes del sistema

La pestaña **Home** contiene los paneles para cada una de las siguientes funciones:

- **IDPA System Manager**
- **Backup Server**
- **Protection Storage**
- **Reporting and Analytics**
- **Search**
- **Cloud Disaster Recovery**
- **Virtualization**
- **Servicio al cliente**
- **General Settings**

Nota

Si hay un componente al que no se puede acceder en la red o que tiene una credencial almacenada incorrecta, el panel correspondiente le indica al usuario que resuelva el problema.

Figura 2 Diseño del inicio del tablero de ACM sin los detalles individuales del panel

Nota

Cuando ACM se reinicia, intenta iniciar cada componente. Esto puede afectar la velocidad de funcionamiento de la interfaz del usuario de ACM.

Panel IDPA System Manager

En el panel **IDPA System Manager**, se muestra la versión de IDPA System Manager y la dirección IP del componente. Para iniciar **IDPA System Manager Web UI**, haga clic en el botón e inicie sesión.

Nota

Si no se configuró LDAP externo, utilice `idpauser` como nombre de usuario. Si se configuró LDAP externo, utilice el nombre de usuario de LDAP.

Mueva el cursor a **Services** para ver información de estado de los servicios de IDPA System Manager.

Figura 3 Panel **IDPA System Manager** en la página **Home** de ACM



Para obtener más información sobre los flujos de trabajo y las funcionalidades de IDPA System Manager, consulte la *IDPA System Manager Guía de administración*.

Panel Backup Server

En el panel **Backup Server**, se muestra la dirección IP del componente, la versión de Avamar, el almacenamiento de metadatos de respaldo total y disponible, el estado de la licencia del nodo del servidor de respaldo y si la instalación de agentes está en curso. Haga clic en el vínculo **Download Agents** que aparece después de que finaliza la instalación del agente para cargar la GUI de restauración web de Avamar, desde la que se pueden cargar los agentes de Avamar.

Figura 4 Panel **Backup Server** en la página **Home** de ACM



Para obtener más información acerca de la función de los agentes de respaldo y cómo instalarlos, consulte la *Avamar Guía de administración*. Mueva el cursor a **Services** para ver información de estado de los servicios de Avamar.

Panel Protection Storage

En el panel **Protection Storage**, se visualiza la versión de DD OS, la dirección IP del componente, el almacenamiento de respaldo total y disponible, el sistema de archivos y el estado de licencia del nodo de almacenamiento con protección, y todas las alertas que requieren acción por parte del usuario. Para acceder a una funcionalidad adicional del componente, haga clic en el vínculo **Protection Storage System Manager**.

Figura 5 Panel **Protection Storage** en la página **Home** de ACM

Protection Storage 



IP Address	10.241.189.134	Version	Data Domain OS 6.1.1.10-590811
Total backup storage	48.407 TB	Available backup storage	48.240 TB
File system status		License status	
Cloud Storage	192.000 TB		

[Protection Storage system manager](#)

Panel Reporting and Analytics

En el panel **Reporting and Analytics**, se muestran la versión de DP Advisor, las direcciones IP de Application Server y Datastore Server, el estado de la licencia del nodo de informes y análisis, y cualquier alerta que requiera una acción por parte del usuario. Para cargar la consola Reporting and Analytics, haga clic en el vínculo **Reporting and Analytics Web UI**. Mueva el cursor a **Services** para ver información de estado de los servicios de DP Advisor.

Figura 6 Panel **Reporting and Analytics** en la página **Home** de ACM

Reporting and Analytics 



Version	6.5.0.103022	License status	
Application Server IP	10.241.189.140	Datastore Server IP	10.241.189.141

Reporting and Analytics Web UI

Services 

Si DP Advisor no se configuró durante el proceso de configuración inicial, en el panel se muestra un mensaje que indica que la opción Reporting and Analytics no está configurada. Para configurar el nodo de informes y análisis, haga clic en el mensaje. Aparece la pantalla Reporting and Analytics Configuration. En la pantalla **Reporting and Analytics Configuration**, proporcione las direcciones IP y la información de licencia requerida y, a continuación, haga clic en **Configure**.

Panel Search

En el panel **Search**, se muestra la versión de Search, para el nodo de índice maestro y cualquier alerta que requiera la acción por parte del usuario. Para cargar la consola Search, haga clic en el vínculo **Search**. Mueva el cursor a **Services** para ver información de estado de los servicios de Search.

Figura 7 Panel **Search** en la página **Home** de ACM

Si Search no se configuró durante el proceso de configuración inicial, el panel muestra un mensaje que indica que la búsqueda no está configurada. Para configurar el nodo de búsqueda, haga clic en el mensaje. Aparece la pantalla Search Configuration. En la pantalla **Search Configuration**, proporcione la dirección IP requerida y haga clic en **Configure**.

Panel Cloud Disaster Recovery

El panel **Cloud Disaster Recovery** muestra la versión de CDRA y todas las alertas que requieren acción por parte del usuario. Para cargar la consola Cloud Disaster Recovery, haga clic en el vínculo **Cloud Disaster Recovery Web UI**.

Figura 8 Panel **Cloud Disaster Recovery** en la página **Home** de ACM.

Si CDRA no se configuró durante el proceso de configuración inicial, el panel muestra **Click here to configure Cloud Disaster Recovery**, lo cual indica que la recuperación ante desastres en la nube no está configurada. Para configurar el nodo de recuperación ante desastres en la nube, haga clic en el mensaje. Aparece la pantalla Cloud Disaster Recovery Configuration. En la pantalla **Cloud Disaster Recovery Configuration**, escriba la dirección IP y haga clic en **Configure**.

Nota

- No cambie la contraseña de usuario raíz de Avamar antes de configurar CDRA desde el tablero.
- No cambie la contraseña de usuario de DD Boost antes de configurar CDRA desde el tablero.
- Si la dirección de correo electrónico y la cuenta en la nube no están configuradas en CDRA, la página de inicio de sesión de CDRA no funciona. El usuario debe configurar manualmente la dirección de correo electrónico y la cuenta en la nube en CDRA.

Panel Virtualization

En el panel **Virtualization**, se muestra información sobre el ambiente virtual interno en el dispositivo, como la dirección IP y la versión de vCenter Server y host ESXi.

Figura 9 Panel **Virtualization** en la página **Home** de ACM

Virtualization



vCenter IP Address	10.241.189.133	vCenter Version	6.5.0.8024368
ESXi IP Address	10.241.189.22	ESXi Version	VMware ESXi 6.5.0 build-7388607

[vCenter Web UI](#)

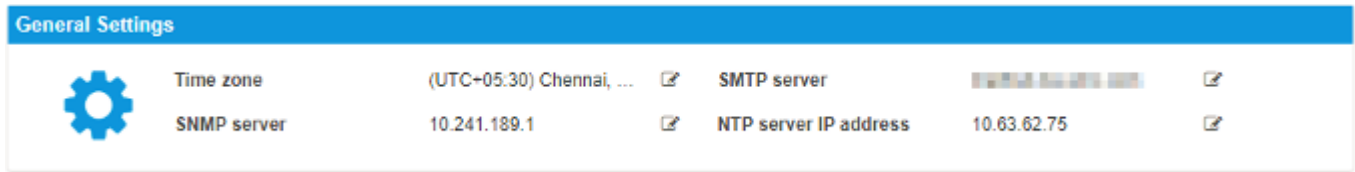
Paneles Customer Support y General Settings

En el panel **Customer Support**, se muestra la información de contacto del sitio y el contacto del administrador. Para ver el valor completo de un elemento, pase el cursor sobre él.

Figura 10 Panel **Customer Support** en la página **Home** de ACM.

Customer Support					
	Admin name			Admin contact number	 
	Admin email			Company name	 
	Location			Site ID	 

En el panel **General Settings**, se muestra la configuración básica, por ejemplo, la configuración de redes y el tiempo. Para ver el valor completo de un elemento, pase el cursor sobre él.

Figura 11 Panel **General Settings** en la página **Home** de ACM


Cuentas de usuario para los componentes

La configuración de IDPA utiliza las cuentas de usuario en [Tabla 2](#) en la página 26. De forma predeterminada, estas cuentas utilizan la contraseña común de IDPA . Para obtener información sobre cómo cambiar las contraseñas de componente, consulte [Cambio de contraseñas y sincronización de los componentes](#) en la página 27.

Tabla 2 Componente y asignación de la cuenta de usuario

Componente	Uso de SSO	Nombre de usuario	Contraseña
ACM	No	root	Contraseña común proporcionada durante la configuración de DP4400.
IDPA System Manager (si no está configurado el LDAP externo)	No	idpauser	Contraseña común proporcionada durante la configuración de DP4400.
IDPA System Manager (si está configurado el LDAP externo)	No	Credenciales de LDAP correspondientes	Contraseña de LDAP externo, según corresponda.
Avamar	Sí	N/C	SSO se encargará de este registro automáticamente.
Data Domain	No	sysadmin	Contraseña común proporcionada durante la configuración de DP4400.
Data Protection Advisor	No	administrator	Contraseña común proporcionada durante la configuración de DP4400.
Search	Sí	N/C	SSO se encargará de este registro automáticamente.
CDRA	No	admin	Contraseña común proporcionada durante la configuración de DP4400.
CDRS	No	admin o monitor	Contraseña configurada durante la implementación de CDR.
vCenter	No	idpauser	Contraseña común proporcionada durante la configuración de DP4400.

Tabla 2 Componente y asignación de la cuenta de usuario (continuación)

Componente	Uso de SSO	Nombre de usuario	Contraseña
ESXi	No	idpauser	Contraseña común proporcionada durante la configuración de DP4400.

Cambio de contraseñas y sincronización de los componentes

El cambio de contraseña de usuario con un solo clic es una de las nuevas funciones presentadas en DP4400. Se recomienda que use la función para cambiar la contraseña, ya que cambia las contraseñas para todos los componentes de IDPA.

Nota

No se recomienda cambiar las contraseñas de los componentes individuales. Debido a cualquier circunstancia imprevista, si tiene que cambiar las contraseñas de los componentes individuales, consulte la siguiente sección.

Cambio de contraseñas para los componentes individuales

Algunos cambios para la configuración y las contraseñas de un componente requieren la actualización de la configuración de otros componentes.

Cambiar una contraseña para un componente hace que la interfaz del usuario de ACM muestre el mensaje de error `password out of sync`. Para permitir que ACM recopile información del estado de los componentes, debe actualizar la contraseña almacenada en la interfaz del usuario de ACM para que coincida. Para actualizar una contraseña no sincronizada, haga clic en el texto del error.

CAPÍTULO 4

Ejecución de un respaldo de VM

Esta sección contiene los siguientes temas:

• Descripción general de respaldos de VM	30
• Definición de los clientes de vCenter y VMware	30
• Implementación del proxy de Avamar	35
• Instalación del hot fix del proxy de Avamar	36
• Creación y ejecución de la política de respaldo	37

Descripción general de respaldos de VM

Tan pronto como su ambiente esté en funcionamiento, puede seguir los pasos de esta sección para respaldar un cliente de VMware.

Si es la primera vez que utiliza Avamar, en la sección se incluyen tareas de preparación, como la definición de clientes de vCenter y VMware, y la implementación de un proxy de Avamar.

Todo el proceso está organizado en los siguientes procedimientos:

- [Definición de los clientes de vCenter y VMware.](#)
- [Implementación del proxy de Avamar.](#)
- [Instalación del hot fix del proxy de Avamar.](#)
- [Creación y ejecución de la política de respaldo](#)

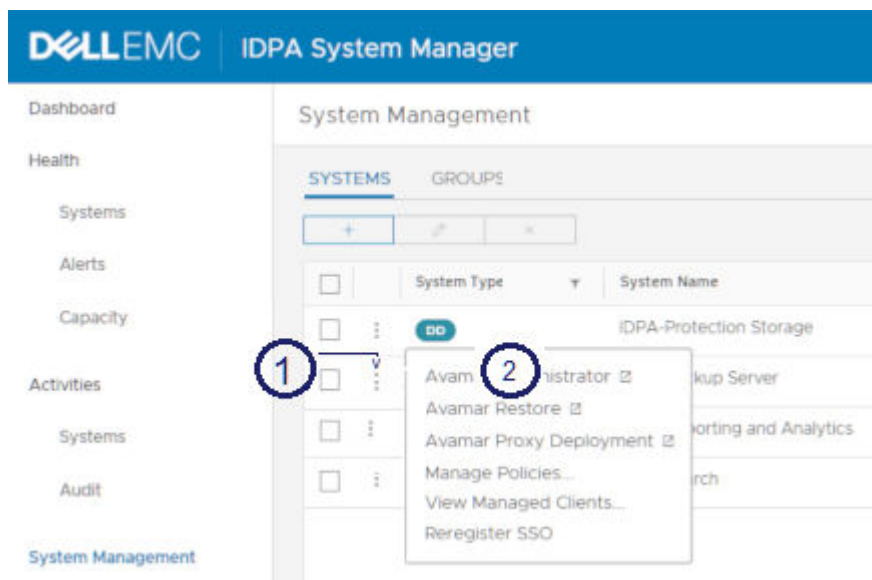
Para obtener más información acerca de los respaldos de Avamar, se encuentra disponible la documentación de Avamar, incluida la *Guía de administración de Avamar* y la *Guía de usuario de los clientes de respaldo de Avamar*.

Definición de los clientes de vCenter y VMware

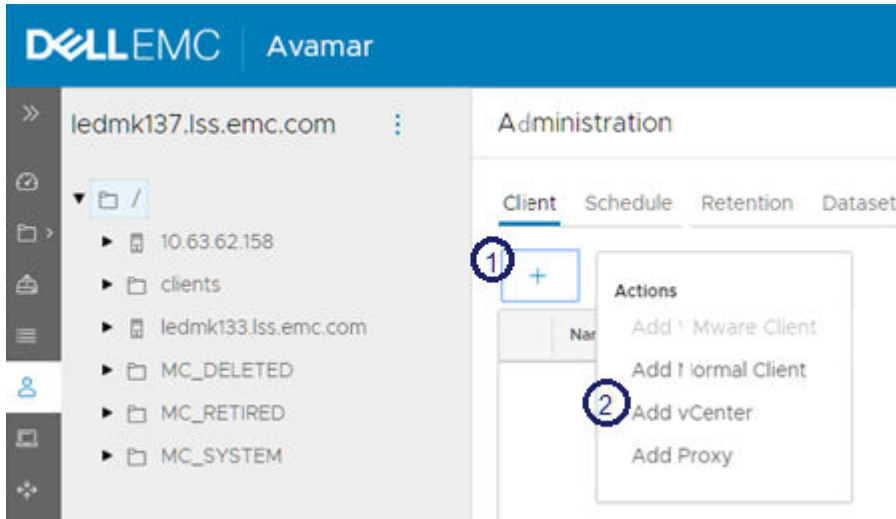
Este procedimiento muestra cómo crear los clientes de vCenter y VM y agregar un conjunto de datos al cliente de VM.

Procedimiento

1. Mediante un navegador, inicie sesión en el tablero de ACM en *https://<ACM IP address>:8543*.
2. Haga clic en **IDPA System Manager Web UI** e inicie sesión en System Manager.
3. Haga clic en **System Management** en el panel de navegación para que aparezca el panel **System Management**.
4. Haga clic en los puntos suspensivos verticales para el servidor de respaldo de IDPA y seleccione **Avamar Restore** para iniciar la interfaz del usuario de Avamar.



1. Haga clic en los puntos suspensivos verticales.
 2. Seleccione **Avamar Restore**.
5. En el panel de navegación de Avamar, haga clic en **Administration**.
 6. Para agregar el cliente de vCenter:
 - a. Haga clic en el signo más (+) y seleccione **Add vCenter** para iniciar el asistente.



1. Haga clic en el signo más.
2. Seleccione **Add vCenter**

- b. Utilice la siguiente tabla para completar los campos en cada página. Haga clic en **Next** para avanzar a la próxima página.

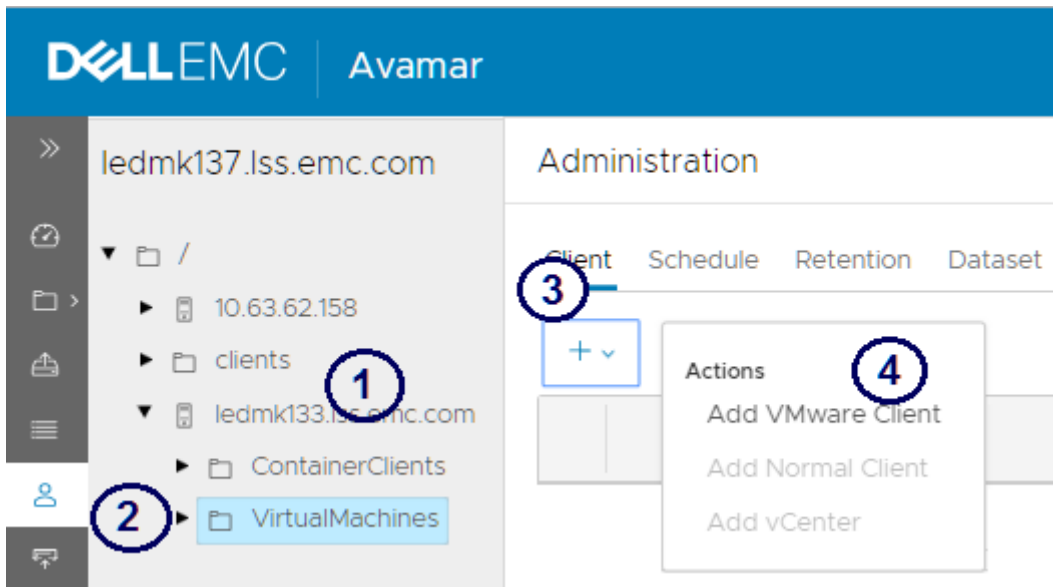
Tabla 3 Incorporación de clientes de vCenter

Página	Campo	Descripción
Client Information	Client Type	Seleccione VMware vCenter.
	New Client Name or IP	Nombre del cliente o dirección IP.
	Client Domain	Nombre del dominio.
vCenter Information	User Name	El nombre de usuario del administrador de vCenter Server.
	Password	La contraseña del administrador.
	Port	El número de puerto HTTPS de vCenter.
Advanced	Todos los campos son opcionales para esta tarea.	
Optional Information	Todos los campos son opcionales para esta tarea.	

- c. Haga clic en **ADD** para completar el asistente. Luego, actualice la pantalla para verificar el nuevo cliente de vCenter.

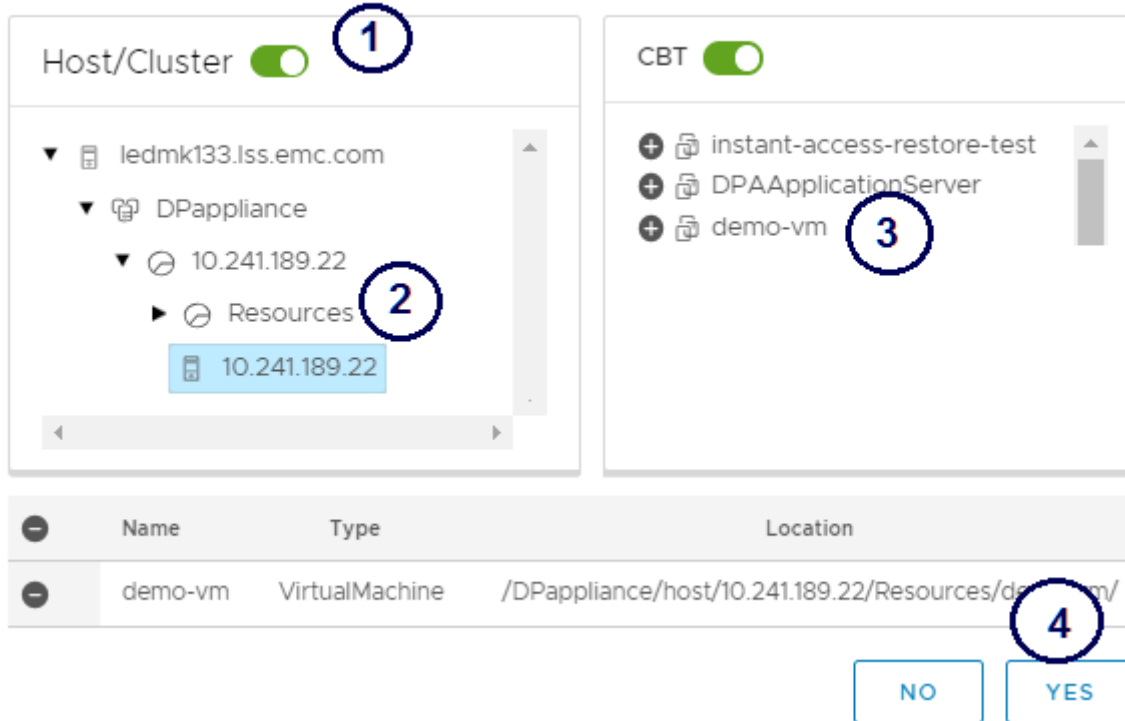
7. Para agregar el cliente de VMware:

- a. En el panel central, expanda el nuevo cliente de vCenter y haga clic en **VirtualMachines**.
- b. En el panel derecho, haga clic en el signo más (+) y seleccione **Add VMware Client**.



1. Expanda vCenter.
 2. Haga clic en **VirtualMachines**.
 3. Haga clic en el signo más.
 4. Seleccione **Add VMware Client**.
- c. En la ventana **Select VMware Entity**, active el botón **Host/Cluster**. A continuación, expanda el árbol de Host/Cluster y seleccione el clúster que aloja la máquina virtual que desea respaldar.
- Las máquinas virtuales asignadas al clúster se muestran en el panel derecho.
- d. En el panel derecho, seleccione la máquina virtual que desea respaldar y haga clic en **YES**.

Select VMware Entity



Host/Cluster ☒ 1

ledmk133.lss.emc.com

DPappliance

10.241.189.22

Resources 2

10.241.189.22

CBT ☒

instant-access-restore-test

DPAApplicationServer

demo-vm 3

Name	Type	Location
demo-vm	VirtualMachine	/DPappliance/host/10.241.189.22/Resources/demo-vm/

NO YES 4

1. Active el botón **Host/Cluster**.
2. Seleccione el clúster.
3. Seleccione la máquina virtual.
4. Haga clic en **YES**.

8. Para agregar el conjunto de datos:

- a. Haga clic en **Administration** en el panel de navegación de Avamar y seleccione la carpeta del dominio raíz en el panel central.
- b. Seleccione **Dataset** en el panel derecho y, a continuación, haga clic en el signo más (+) para visualizar la ventana **Create DataSet**.
- c. En el campo Dataset Name, escriba un nombre para el conjunto de datos.
- d. Haga clic en **Windows VMware Image** en la lista **Plugins** para visualizar la página **Windows VMware Image**.
- e. Seleccione la casilla de verificación **Index VMware Image Backups** y haga clic en **Submit**.

NOTA: La indexación se utiliza para la restauración de archivos específicos y es opcional para el respaldo de máquinas virtuales completas. Si la selecciona aquí, le permitirá restaurar archivos específicos, como se describe en [Restauración de archivos específicos](#).

Create DataSet

DataSet Name: vm_dataset

The screenshot shows the 'Create DataSet' configuration window. It has two tabs: 'Option' (selected) and 'Source Data'. On the left, under the 'Plugins' section, a list of backup plugins is shown. The 'Windows VMware Image' plugin is selected and highlighted in blue. On the right, under the 'Option' tab, there are three checked options: 'Use Changed Block Tracking (CBT) to increase performance', 'set annotation tag LastBackupStatus and LastSuccessfulBackup', and 'Index VMware Image Backups'. At the bottom right, there are two buttons: 'CLOSE' and 'SUBMIT'.

1. DataSet Name: vm_dataset

2. Windows VMware Image

3. Index VMware Image Backups

4. SUBMIT

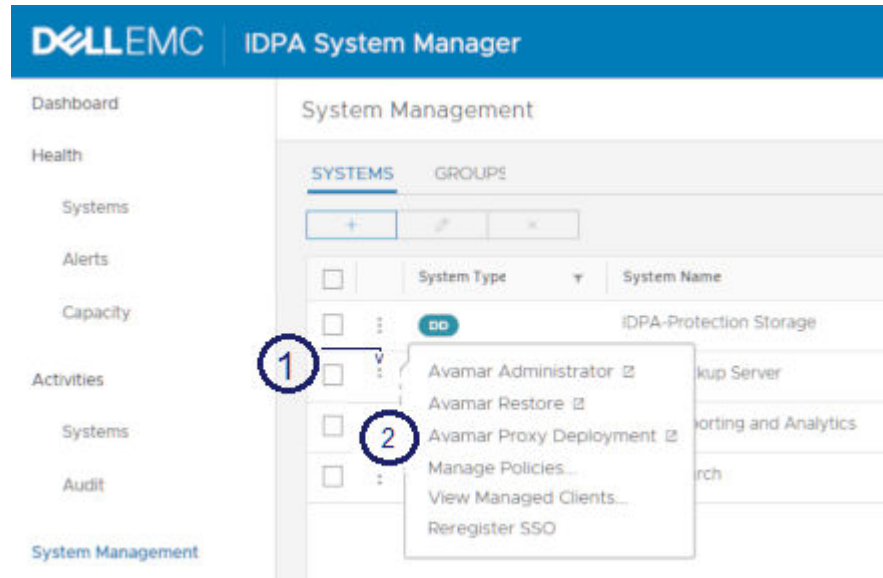
1. Introduzca el nombre del conjunto de datos.
2. Seleccione **Windows VMware Image**.
3. Seleccione **Index VMware Image Backups**.
4. Haga clic en **Submit**.

Implementación del proxy de Avamar

Implemente el proxy de Avamar en cada vCenter que desee proteger.

Procedimiento

1. Inicie **IDPA System Manager Web UI** y haga clic en **System Manager** en el panel de navegación.
2. En el panel derecho, haga clic en los puntos suspensivos verticales frente al servidor de respaldo de IDPA y seleccione **Avamar Proxy Deployment**.



1. Haga clic en los puntos suspensivos verticales.
2. Seleccione **Avamar Proxy Deployment**.
3. En la ventana **Config**, especifique **vCenter**, **Data Change Rate** y **Backup Window**. A continuación, seleccione la casilla de verificación **Protect Virtual Machines on Local Storage**.
4. Haga clic en **CREATE RECOMMENDATION**.
En el panel **Recommendations**, se muestran los nuevos proxies propuestos debajo de cada host ESXi.
5. Expanda los listados en el panel **Recommendations** y seleccione **New proxy** en el host del servidor ESXi.
6. Haga clic en  para visualizar el cuadro de diálogo **New Proxy**.
 - a. Escriba el nombre de host del proxy en el campo **Name**.
 - b. En **Domain**, seleccione el dominio del servidor Avamar donde residirá el proxy.
 - c. Escriba la dirección IP en el campo **IP**.
 - d. Seleccione un área de almacenamiento de datos en la lista **Datastore**.
 - e. Seleccione **VM Network** de la lista **Network**.
 - f. Escriba el nombre completo del servidor totalmente calificado o la dirección IP en el campo **DNS**.

- g. Escriba la dirección IP del gateway de red en el campo **Gateway**.
 - h. Escriba la máscara de red en el campo **Netmask**.
 - i. Haga clic en **Save**.
7. Haga clic en  para implementar el proxy.

La implementación del proxy se muestra en el panel inferior.

Instalación del hot fix del proxy de Avamar

Para usar la indexación de la máquina virtual en el momento del respaldo de imagen, debe instalar Avamar Hotfix 298624 en todos los proxies de Avamar. Si no aplica el hot fix de Avamar, los proxies pueden quedarse sin espacio de almacenamiento debido a que se está activando de manera predeterminada el registro de depuración.

Antes de comenzar

Descargue Avamar Hotfix 298624 desde la siguiente ubicación:

ftp://avamar_ftp:anonymous@ftp.avamar.com/software/hotfixes/298624/SLES12SP1_64/AvamarVMwareCombined-linux-sles12sp1-x86_64-7.5.101-101.rpm

Repita este procedimiento para cada proxy Avamar. Se requieren las siguientes credenciales predeterminadas para la autenticación o la conexión a un proxy de Avamar:

Nombre de usuario: `root`

Contraseña: `avam@r`

Procedimiento

1. Con el comando `scp` o WinSCP, copie el archivo de hot fix en `/space/avamar/var` en el proxy.
2. Conéctese con el protocolo SSH al proxy con las credenciales predeterminadas.
3. Escriba el comando `rm -f /tmp/*.SQL`
4. Vaya al directorio en el que se encuentra ubicado el archivo hot fix.
`cd /space/avamar/var`
5. Instale el hot fix:

```
rpm -Uvh AvamarVMwareCombined-linux-sles12sp1-x86_64-7.5.101.101.rpm --force
```

Resultados

Para verificar la correcta instalación de RPM, compruebe la versión con el siguiente comando:

```
avtar --version
```

Si el RPM está instalado, el resultado es el siguiente:

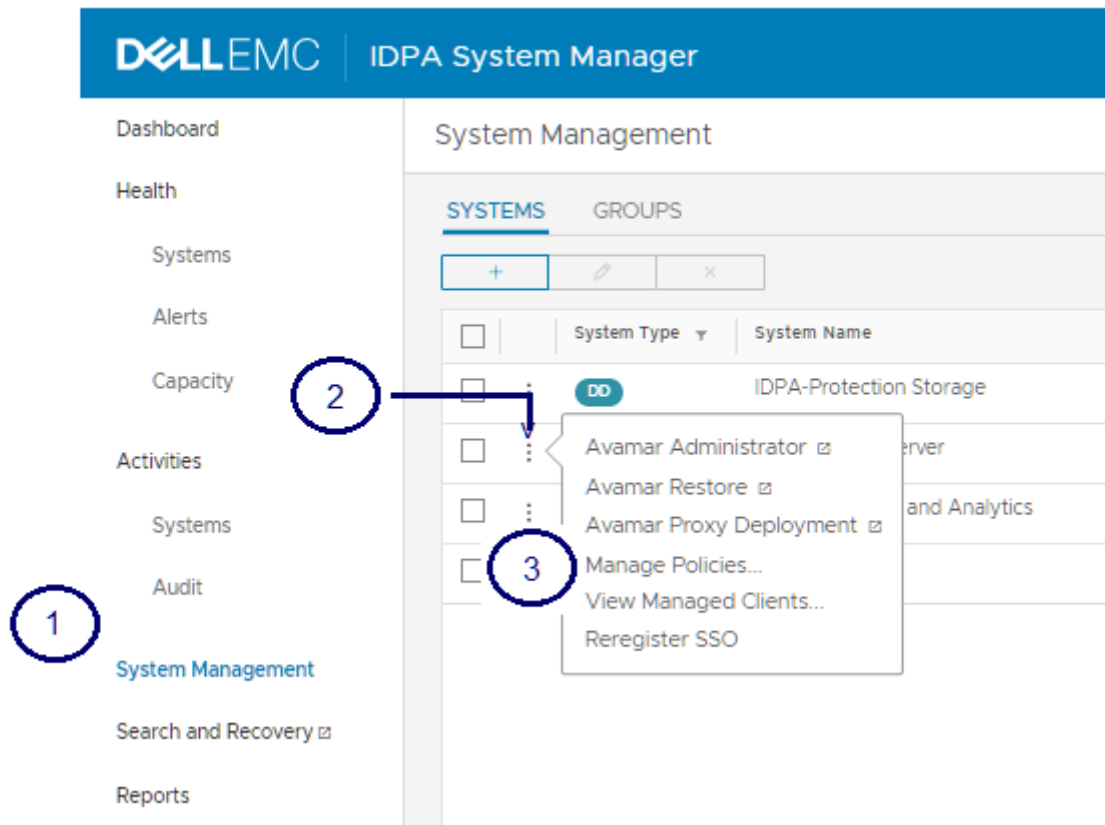
```
version: 7.5.101-101_HF298624
```

Creación y ejecución de la política de respaldo

En estos pasos, se muestra cómo crear la política para proteger al cliente de VMware y, a continuación, ejecutar la política.

Procedimiento

1. En IDPA System Manager, haga clic en **System Management** en el panel de navegación.
2. En el panel derecho, haga clic en los puntos suspensivos verticales para el servidor de respaldo de IDPA y seleccione **Manage Policies**.



1. Haga clic en **System Management**.
2. Haga clic en los puntos suspensivos verticales.
3. Seleccione **Manage Policies**.

Aparece el panel **Manage Policies**.

3. En el panel **Manage Policies**, haga clic en el signo más (+) para iniciar el asistente **Add Policy**.
4. Utilice la siguiente tabla para completar las páginas del asistente. Haga clic en **Next** para avanzar a la próxima página.

Tabla 4 Incorporación de políticas

Página	Campo	Descripción
Information	Name	El nombre de la política.
	Domain	Acepte la entrada predeterminada.
	Enable	Haga clic para habilitar la política.
	Dataset	Seleccione VMware Image Dataset .
	Schedule	Seleccione Daily Schedule .
	Retention	Seleccione Default Retention .
Clients	Available Clients	Seleccione el cliente de máquina virtual definido anteriormente en esta guía.
Proxies (Optional)	Available Proxies	Seleccione el proxy definido anteriormente en esta guía.

5. Haga clic en **Finish**.

La nueva política se muestra en la lista de políticas.

6. Para ejecutar la política, selecciónela en la lista de políticas y haga clic en **BACKUP NOW**.

The screenshot shows the Dell EMC IDPA System Manager interface. The sidebar on the left contains navigation links: Dashboard, Health, Systems, Alerts, Capacity, Activities, and System Management. The main panel is titled 'System Management > Manage Policies'. It shows the 'POLICIES' tab selected, with a table of policies. The 'VMware_Image' policy is selected, indicated by a blue circle and the number '1'. The 'BACKUP NOW' button is highlighted with a blue circle and the number '2'.

Domain	Name	Enabled
/	Default Group	false
/	Default Proxy Group	false
/	VMware_Image	true
/	test	true

1. Seleccione la política.

2. Haga clic en **BACKUP NOW**.

7. Monitoree la política de ejecución. Para ello, haga clic en **Systems** debajo de **Activities** en el panel de navegación.

CAPÍTULO 5

Restauración de un respaldo de VM

En esta sección, se describen tres métodos diferentes para restaurar el respaldo de VM que se creó en el capítulo anterior:

- [Restauración de una máquina virtual](#) 40
- [Restauración mediante acceso instantáneo](#)..... 43
- [Restauración de archivos específicos](#)..... 45

Restauración de una máquina virtual

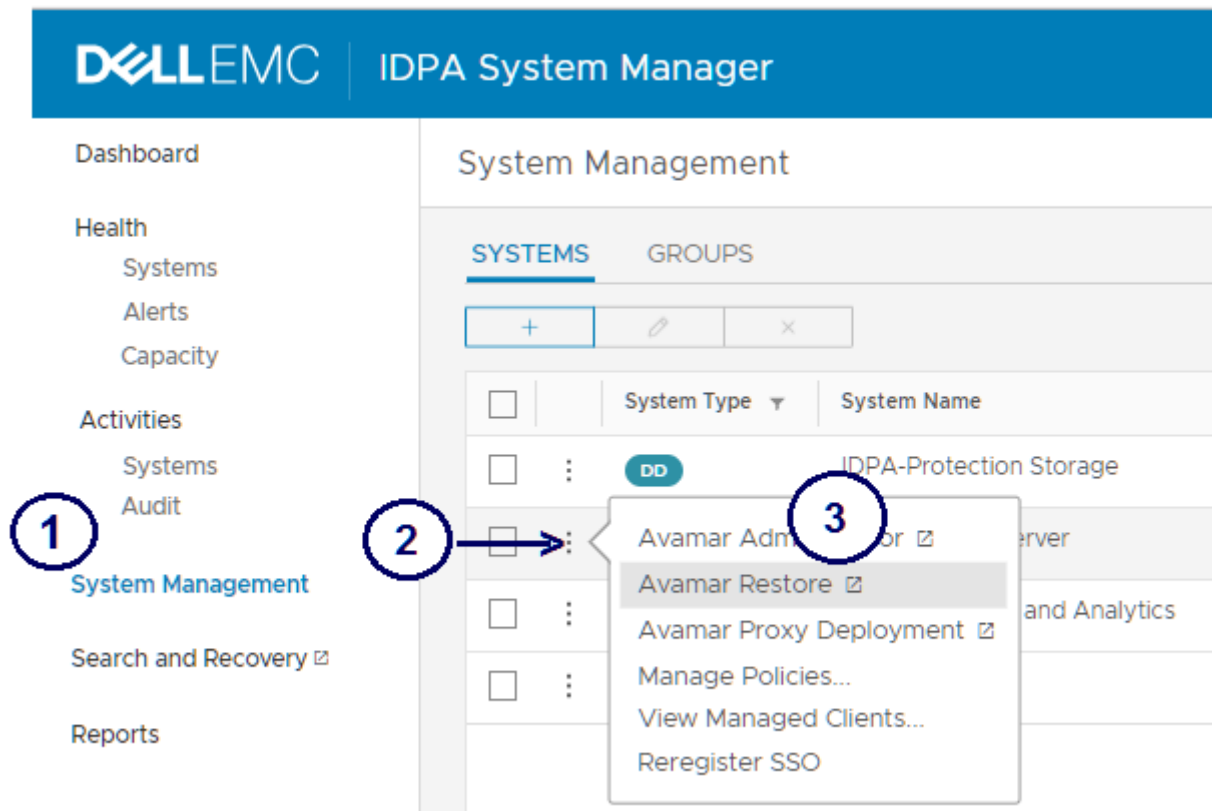
En estos pasos se ilustra el procedimiento básico de restauración de VM.

Antes de comenzar

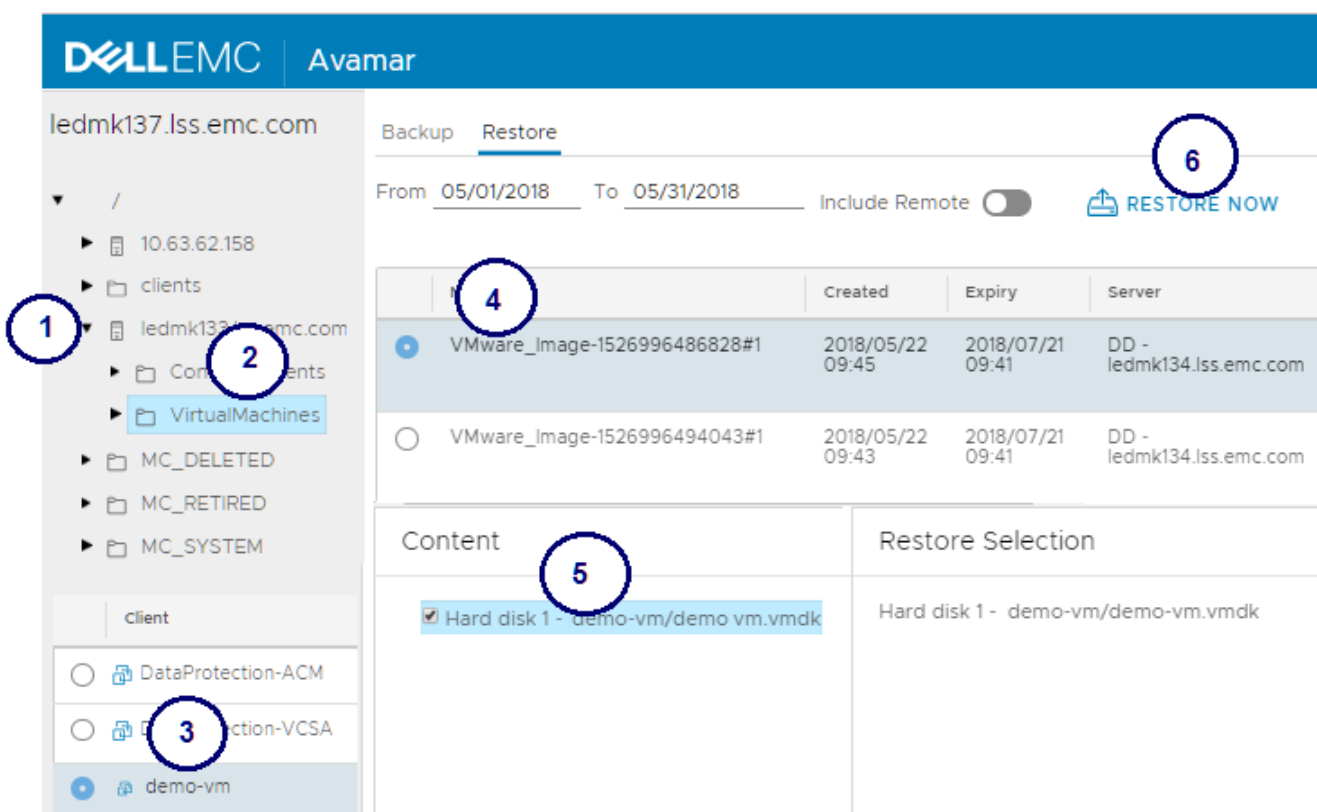
Debe existir un respaldo de la máquina virtual a fin de realizar una restauración.

Procedimiento

1. Acceda a IDPA System Manager y haga clic en **System Management** en el panel de navegación.
2. En el panel derecho, haga clic en los puntos suspensivos verticales a la izquierda del servidor de respaldo de IDPA y seleccione **Avamar Restore**.



1. Seleccione **System Management**.
2. Haga clic en los puntos suspensivos verticales.
3. Seleccione **Avamar Restore**.
3. Expanda el vCenter en el panel central y seleccione **VirtualMachines** para visualizar los clientes de VM que pertenecen a ese vCenter.
4. En la lista de clientes, seleccione al cliente de VM que desee restaurar.
5. En el panel derecho, seleccione el respaldo que desee restaurar y, a continuación, seleccione el contenido de la restauración en el área **Content**.
6. Para iniciar el asistente de restauración, seleccione el contenido que desee restaurar y haga clic en **RESTORE NOW**.



1. Expanda vCenter.
2. Haga clic en **VirtualMachines**.
3. Seleccione el cliente.
4. Seleccione el respaldo más reciente.
5. Seleccione el contenido.
6. Haga clic en **Restore Now**.
7. Utilice la siguiente tabla para completar cada página del asistente. Haga clic en **NEXT** para avanzar a la próxima página.

Tabla 5 Restauración desde una máquina virtual

Página del asistente	Campo	Descripción
Basic Config	Destination	Seleccione Restore to new Virtual Machine .
	Post Restore Options	Seleccione Do not power on VM after restore .
	Proxy	Seleccione Automatic .
Advanced Config	vCenter	Seleccione la dirección IP de vCenter para administrar la VM restaurada.
	VM Name	Introduzca un nombre para la VM restaurada.
Location		Expanda el árbol y seleccione la VM donde desee ejecutar la restauración.
Host/Cluster		Expanda el árbol y seleccione el host/clúster de ESXi.
Resource Pool		Expanda el árbol y seleccione el pool de recursos.

Tabla 5 Restauración desde una máquina virtual (continuación)

Página del asistente	Campo	Descripción
Datastore		Seleccione el almacén de datos ESX de destino.

8. En la página **Summary**, revise sus entradas y haga clic en **FINISH** para ejecutar la restauración.
9. Para monitorear los resultados, seleccione **Activity** en el árbol de navegación de Avamar y visualice los resultados del procesamiento en el panel derecho.

Restauración mediante acceso instantáneo

Puede usar la función de acceso instantáneo para realizar la recuperación de una VM prácticamente en tiempo real. Monta una imagen de copia de seguridad de VM en un recurso compartido NFS en su ambiente de respaldo y activa la máquina virtual para que pueda administrarse en vCenter.

Después de completar estos pasos, debe mover la máquina virtual de su ambiente de respaldo al sistema de producción.

Procedimiento

1. Inicie el IDPA System Manager y haga clic en **System Management** en el panel de navegación.
2. En el panel derecho, haga clic en los puntos suspensivos verticales a la izquierda del servidor de respaldo de IDPA y seleccione **Avamar Restore**.
3. Expanda el árbol de vCenter y seleccione **VirtualMachines** para visualizar la lista **Client**.
4. Seleccione el cliente en la lista **Client** para visualizar los respaldos recientes de ese cliente en el panel derecho.
5. Seleccione el respaldo que desee restaurar. A continuación, seleccione el contenido en el área **Content** y haga clic en **Restore Now** en la esquina superior derecha para iniciar el asistente Restore.

The screenshot shows the Dell EMC Avamar Restore interface. The top navigation bar includes the Dell EMC logo and the word "Avamar". The main interface is divided into several sections:

- Left Panel (Navigation):** Shows a tree view of the system. The "VirtualMachines" folder is selected, indicated by a blue circle with the number 1.
- Top Bar:** Includes tabs for "Backup" and "Restore". The "Restore" tab is active. Below the tabs, there are date filters "From 05/01/2018 To 05/31/2018", a toggle for "Include Remote", and a "RESTORE NOW" button with a blue circle and the number 5.
- Client List Table:** A table with columns: Name, Label, Created, Plugin, and Size. The first row is selected, indicated by a blue circle with the number 3.

Name	Label	Created	Plugin	Size
MOD-1526564097797#1	6	2018/05/17 09:39	Windows VMware I	80 GB
MOD-1525888167605#1	5	2018/05/09 13:52	Windows VMware I	80 GB
MOD-1525888160592#1	4	2018/05/09 13:50	Windows VMware I	80 GB
MOD-1525871082323#1	3	2018/05/09 09:05	Windows VMware I	80 GB
MOD-1525869725749#1	2	2018/05/09 08:45	Windows VMware I	80 GB
- Client Selection:** Below the table, a list of clients is shown. The "demo-vm" client is selected, indicated by a blue circle with the number 2.
- Content Selection:** A section labeled "Content" with a blue circle and the number 4. It shows a list of backup files, with "demo-vm/demo-vm.vmdk" selected.
- Restore Selection:** A section labeled "Restore Selection" showing the selected file "demo-vm/demo-vm.vmdk".

1. Seleccione **VirtualMachines**.
2. Seleccione el cliente.

3. Seleccione el respaldo más reciente.
4. Seleccione el contenido.
5. Haga clic en **Restore Now**.
6. Utilice la siguiente tabla para completar cada página del asistente. Haga clic en **NEXT** para avanzar a la próxima página.

Tabla 6 Restauración mediante acceso instantáneo

Página del asistente	Campo	Descripción
Basic Config	Destination	Seleccione Instant Access .
	Post Restore Options	Seleccione una opción de restauración.
	Proxy	Seleccione Automatic .
Advanced Config	vCenter	Seleccione la dirección IP de vCenter para administrar la VM restaurada.
	VM Name	Introduzca un nombre para la VM restaurada.
Location		Expanda el árbol y seleccione la VM donde desee ejecutar la restauración.
Host/Cluster		Expanda el árbol y seleccione el host/clúster de ESXi.
Resource Pool		Expanda el árbol y seleccione el pool de recursos.

7. En la página **Summary**, revise sus entradas y haga clic en **FINISH** para ejecutar la restauración.
8. Para monitorear los resultados, seleccione **Activity** en el árbol de navegación de Avamar y visualice los resultados del procesamiento en el panel derecho.

Restauración de archivos específicos

Puede restaurar archivos específicos directamente desde los resultados de búsqueda.

Antes de comenzar

Asegúrese de que Avamar indexe sus imágenes de VM respaldadas. Para obtener instrucciones, consulte la *Guía del administrador de búsqueda de Dell EMC*.

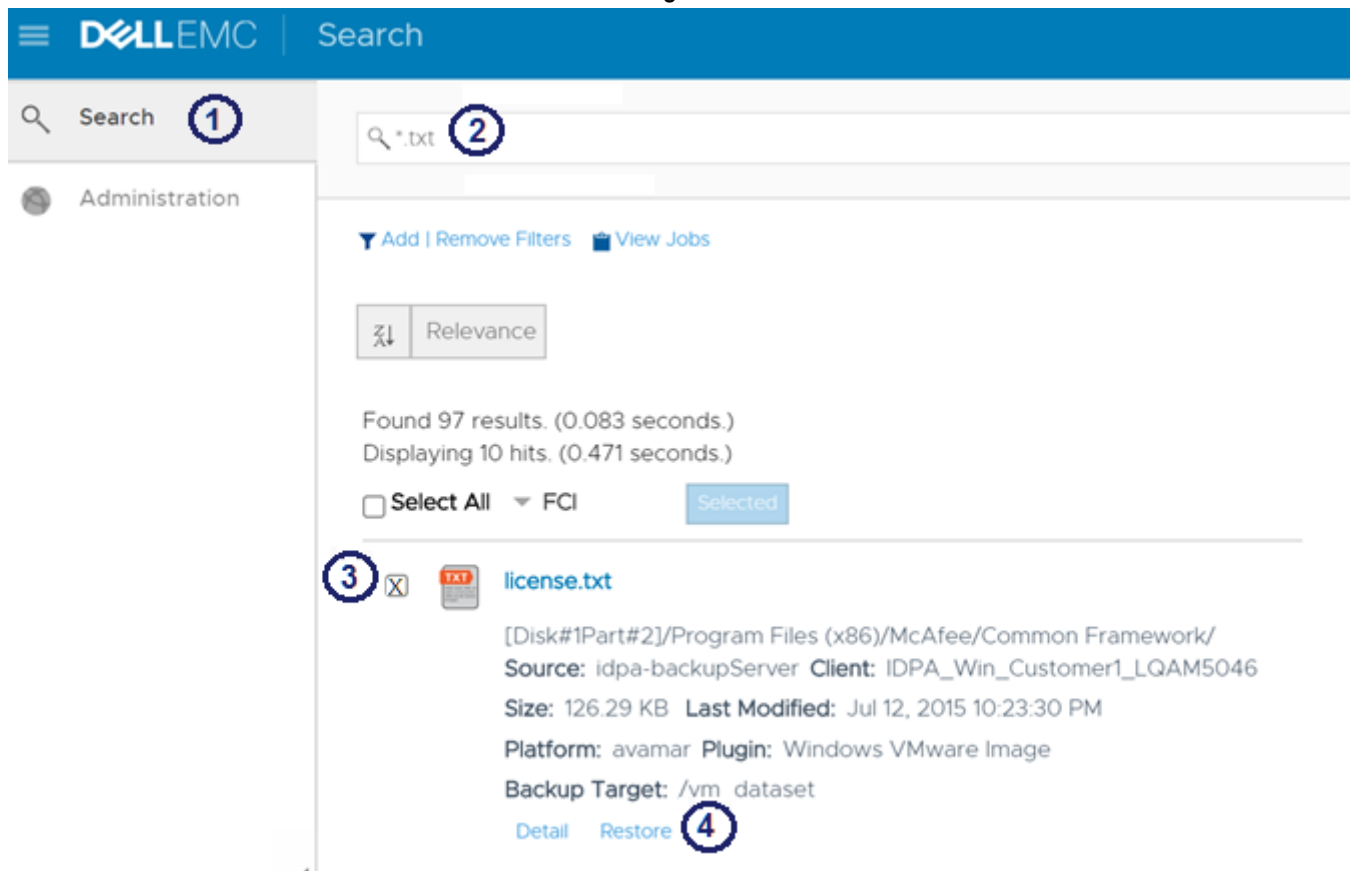
En este procedimiento, se utiliza la aplicación Search para buscar y restaurar archivos específicos en un respaldo de VM.

Procedimiento

1. Acceda a IDPA System Manager y seleccione **Search and Recovery** en el panel de navegación.
2. Inicie sesión en la aplicación Search.
3. En el campo **Search**, introduzca una consulta para recuperar archivos específicos y haga clic en **Search**. (También puede usar las opciones de filtro para refinar los resultados de búsqueda).

Se visualizan los archivos recuperados.

4. Seleccione los archivos que desee restaurar y haga clic en **Restore** para visualizar el cuadro de diálogo **Restore**.



1. Haga clic en **Search**.
2. Introduzca la consulta de búsqueda.
3. Seleccione uno o más archivos.

4. Haga clic en **Restore**.

5. Use la siguiente tabla para completar el cuadro de diálogo **Restore**.

Tabla 7 Restauración de archivos específicos

Campo	Descripción
Original path / Destination path	Selección de la ubicación de la restauración. Cuando corresponda, haga clic en Overwrite y seleccione Restore Access Control List para proteger el archivo con la misma configuración de lista de control de acceso.
Client	Cuando esté seleccionada la opción Destination Path , seleccione el cliente donde desee guardar el archivo.
Restore to	Especifique la ruta donde desee guardar el archivo.
Username / Password	Especifique el nombre de usuario de VM y la contraseña.

6. Haga clic en **Restore** para iniciar el proceso de restauración.
7. Para monitorear los resultados, haga clic en **View Jobs** debajo del campo **Search** y actualice la pantalla para ver las acciones en curso.

CAPÍTULO 6

Generación de informes

Esta sección contiene los siguientes temas:

- [Creación de un informe](#)..... 48

Creación de un informe

De manera inmediata, puede ejecutar 11 informes previamente diseñados para los sistemas Avamar y Data Domain.

Para obtener más información acerca de estos informes, consulte la *Guía del producto de Dell EMC Data Protection Advisor*.

Si desea generar sus propios informes, consulte la *Guía de creación de informes personalizada de Dell EMC Data Protection*.

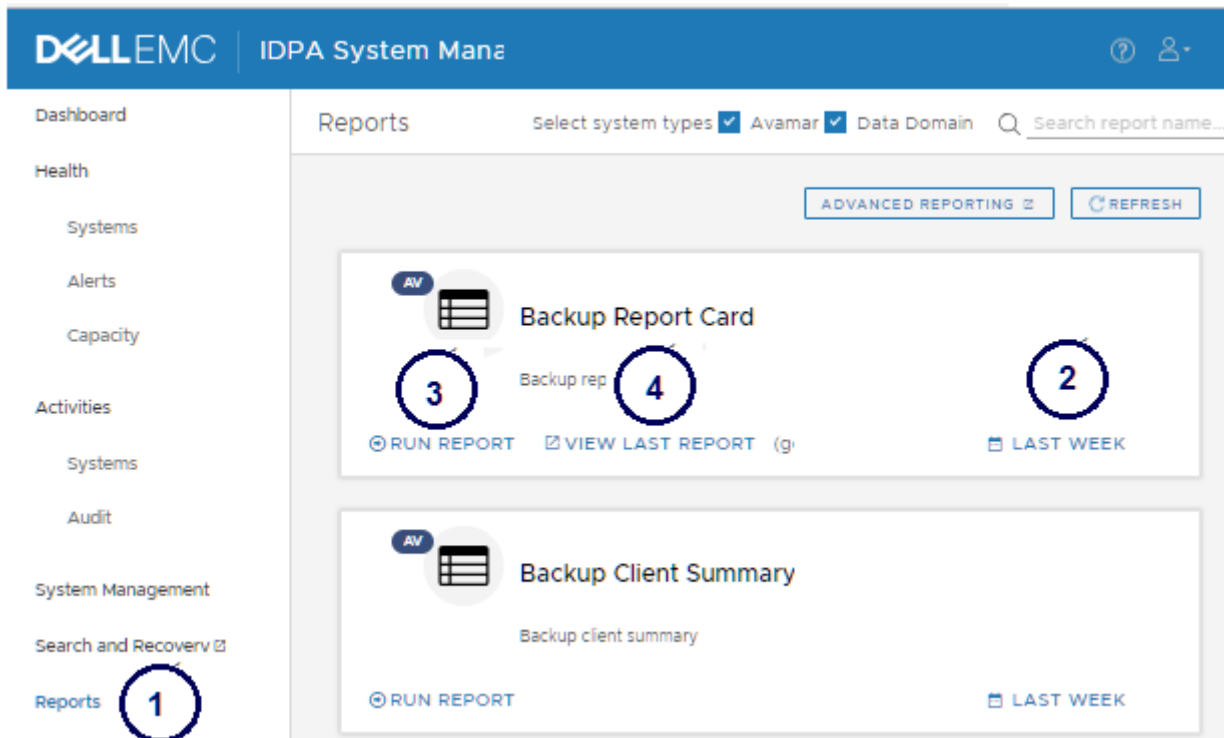
Procedimiento

1. Acceda a *IDPA System Manager* y seleccione **Reports** en el panel de navegación.

En el panel derecho, cada tipo de informe se muestra en una tarjeta independiente. El panel muestra informes de Avamar y Data Domain, pero puede utilizar las casillas de verificación en la esquina superior derecha para filtrar los informes que se muestran.

El período para cada informe se muestra en la esquina inferior derecha. El período de informe predeterminado es la semana anterior, pero puede cambiarlo; para ello, haga clic en **Last Week** y seleccione otro período.

2. Para generar un informe, haga clic en **Run Report** debajo del nombre del informe.



1. Seleccione **Reports**.
2. (Opcional) Cambie el período de tiempo.
3. Haga clic en **RUN REPORT**.
4. Haga clic en **VIEW LAST REPORT**.

IDPA genera el informe y muestra **View Last Report** cuando está listo para la visualización.

3. Haga clic en **View Last Report** para visualizar el informe en una nueva ventana.

