Dell EMC OpenManage Integration versión 1.1.1 con Microsoft Windows Admin Center

Guía del usuario

February 2021
Rev. A01

Notas, precauciones y advertencias

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

© 2019 - 2021 Dell Inc. o sus subsidiarias. Todos los derechos reservados. Dell, EMC y otras marcas comerciales son marcas comerciales de Dell Inc. o sus filiales. Es posible que otras marcas comerciales sean marcas comerciales de sus respectivos propietarios.

Tabla de contenido

Capítulo 1: Descripción general de OpenManage Integration with Microsoft Windows Admin Center..... 5
Historial de revisión....5
Novedades de esta versión....6
Recursos adicionales....7

Capítulo 2: Introducción a OpenManage Integration with Microsoft Windows Admin Center....8

Capítulo 3: Puertos requeridos por Dell EMC OpenManage Integration with Microsoft Windows Admin Center....9

Capítulo 4: Administración de servidores Dell EMC PowerEdge....10
Estado de la condición: componentes de nodos de destino compatibles....11
Inventario de hardware: componentes compatibles del nodo objetivo....11

Capítulo 5: Administrar clústeres de conmutación por error y Azure Stack HCI....13
Estado de mantenimiento: componentes compatibles del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI....14
Inventario de hardware: componentes compatibles del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI....14

Capítulo 6: Cómo ver detalles de la iDRAC de los servidores de PowerEdge y los nodos de los clústeres HCI y de conmutación por error....16

Capítulo 7: Actualizar los servidores PowerEdge y los nodos de los clústeres HCI y de conmutación por error....17
Configuración de las herramientas de cumplimiento de normas de la actualización....18
Configurar ajustes de proxy....18
Actualizar nodos objetivo....19
Paso 1: Generación del informe de cumplimiento: componentes del nodo de destino....19
Paso 2: Visualización del informe de cumplimiento y selección de componentes: componentes del nodo de destino....20
Paso 3: Actualización: componentes del nodo de destino....22
Actualizar los nodos de HCI y los clústeres de conmutación por error....22
Paso 1: generación del informe de cumplimiento. Componentes del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI....23
Paso 2: Visualización del informe de cumplimiento y selección de componentes: componentes de nodos de destino en clústeres de conmutación por error y Azure Stack HCI....24
Paso 3: actualización. Componentes del nodo objetivo en los clústeres de conmutación por error y Azure Stack HCI....26

Capítulo 8: Solución de problemas....27
Disponibilidad de los registros de la extensión OMIMSWAC....27
Disponibilidad de los registros de la operación de actualización....27
No se pueden copiar los archivos necesarios en el nodo de destino para obtener la información de inventario....28
No se puede obtener el inventario de estado y hardware desde la iDRAC....28

No se pueden completar ni seleccionar los discos para las operaciones de destellar o dejar de destellar....28
El estado de la licencia es Desconocido o Sin licencia....29
El trabajo falló al descargar los componentes necesarios para las operaciones de actualización del servidor y compatible en clústeres....29
CredSSP falló durante la actualización....29
El trabajo falló al generar el informe de cumplimiento....30
El trabajo falló al actualizar los componentes seleccionados....30
Componente que muestra no cumplimiento después de la actualización....31
Acceso denegado a OpenManage Integration....31
Fallas de Dell Update Package (DUP)....31
Falla del clúster de prueba con errores de comunicación de red....32
La red de la NIC USB se muestra como red de clúster particionada....32

Capítulo 9: Identificación de la generación del servidor Dell EMC PowerEdge....33

Capítulo 10: Cómo ponerse en contacto con Dell EMC....34

Apéndice A: Glosario....35

Apéndice B: Apéndice....37

1

Descripción general de OpenManage Integration with Microsoft Windows Admin Center

Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) permite a los administradores de TI gestionar servidores PowerEdge como hosts, clústeres de conmutación por error Microsoft creados con servidores PowerEdge e infraestructura hiperconvergente (HCI) creada utilizando las soluciones Dell EMC para Microsoft Azure Stack HCI (nodos Storage Space Direct Ready o nodos AX). OMIMSWAC simplifica las tareas de los administradores de TI mediante la gestión remota de los servidores PowerEdge y los clústeres durante todo su ciclo de vida. Para obtener más información sobre las características y los beneficios de OMIMSWAC, consulte la documentación en Dell.com/OpenManageManuals.

Características clave de OMIMSWAC

- OMIMSWAC cuenta con una solución simplificada para que los administradores de TI administren eficazmente lo siguiente:
  - Los servidores Dell EMC PowerEdge que se ejecutan en los sistemas operativos Windows compatibles.
  - Los clústeres Azure Stack HCI basados en nodos AX o Storage Spaces Direct Ready desde Dell EMC.
  - Clústeres de conmutación por error de Microsoft creados con servidores Dell EMC PowerEdge.
- Ver el estado general, el inventario de hardware y el inventario de iDRAC de nodos, incluida la información de nivel de componentes de todas las plataformas Dell EMC compatibles.
- Proporciona informes de cumplimiento de actualización en relación con catálogos de actualización verificados de Dell EMC y notificaciones para versiones de catálogo nuevas.
- Compatibilidad con diferentes configuraciones básicas en OMIMSWAC cuando está conectado a Internet:
  - Catálogo de Dell EMC Enterprise para servidores PowerEdge y clústeres que contengan servidores PowerEdge.
  - Catálogo de soluciones Dell EMC Azure Stack HCI para soluciones Dell EMC para Microsoft Azure Stack HCI.
  - Catálogo de soluciones Dell EMC MX para PowerEdge MX Modular.
- Compatibilidad con configuraciones básicas locales creadas mediante Dell EMC Repository Manager (DRM).
- Actualizar servidores PowerEdge con respecto a la configuración básica: BIOS, controlador, firmware o aplicaciones de administración de sistemas.
- Actualización compatible en clústeres en función de la configuración básica validada (BIOS, controlador, firmware o aplicaciones de administración de sistemas) para clúster de conmutación por error basado en el servidor PowerEdge y soluciones Dell EMC para Microsoft Azure Stack HCI.
- Puede ver información de iDRAC de servidores PowerEdge. Para la administración fuera de banda, puede iniciar directamente la consola de iDRAC desde Windows Admin Center.
- Disponibilidad de la extensión y documentación de OMIMSWAC localizada en inglés, francés, alemán, español, chino simplificado y japonés.

Temas:

- Historial de revisión
- Novedades de esta versión
- Recursos adicionales

Historial de revisión

Fecha	Revisión del documento	Descripción de cambios
Agosto de 2020	A00	Versión inicial de OMIMSWAC 1.1.1
Enero de 2021	A01	• Se agregó compatibilidad para Windows Admin Center 2009 GA.

Fecha	Revisión del documento	Descripción de cambios
		• Los nodos objetivo que ejecutan el SO Windows Server Core no son compatibles.

Novedades de esta versión

Versión 1.1.1

- Compatibilidad para Microsoft Windows Admin Center versión 2007 GA y 2009 GA.
- Compatibilidad con servidor Edge PowerEdge XE2420 con firmware de iDRAC 4.00.129.00 o posterior.
- Reparaciones y mejoras:
  - Puede acceder a OMIMSWAC desde la consola de Windows Admin Center (WAC) después de iniciar sesión en WAC usando las credenciales de usuario de gateway sin privilegios de administrador.

    En la versión anterior, se denegó el acceso a OMIMSWAC desde la consola de WAC si inició sesión en el WAC con las credenciales de usuario de gateway sin privilegios de administrador.
  - Permite a OMIMSWAC recuperar la información de inventario para los clústeres conectados mediante Single Sign On.

    En la versión anterior, la recuperación de la información de inventario fallaba cuando un clúster estaba conectado mediante la autenticación Single Sign On y WAC dejaba de responder.
  - Permite generar el informe de cumplimiento para los nodos o los clústeres de destino conectados mediante una contraseña que contiene determinados caracteres especiales.

    En la versión anterior, la generación de cumplimiento fallaba cuando un servidor o clúster se conectaba mediante una contraseña que contenía caracteres especiales, como comillas dobles ("), acento grave (') y punto y coma (;).
- Restablecimiento del parámetro `CauClusterRole` para permitir la funcionalidad de actualización automática del clúster especificado después de que se completa la operación de actualización compatible en clústeres (CAU).

Versión 1.1.0

- Se agregó compatibilidad para catálogos en línea Dell EMC:
  - Catálogo de Dell EMC Enterprise para servidores PowerEdge y clústeres que contengan servidores PowerEdge.
  - Catálogo de soluciones Dell EMC Azure Stack HCI para soluciones Dell EMC para Microsoft Azure Stack HCI.
  - Catálogo de soluciones Dell EMC MX para PowerEdge MX Modular.
- Capacidad para realizar una actualización de servidor, incluidas actualizaciones selectivas de componentes.
- Posibilidad de realizar una actualización compatible con clústeres en función de la configuración básica validada (BIOS, controlador, firmware y aplicaciones de administración del sistema) en los siguientes elementos.
  - Clúster de conmutación por error basado en servidor PowerEdge
  - Soluciones Dell EMC para Microsoft Azure Stack HCI

    NOTA: Para la función de actualización compatible con clústeres, se debe instalar una licencia Premium en cada uno de los nodos de un clúster.

- Para localizar discos físicos o identificar discos físicos fallidos, se proporciona aprovisionamiento para hacer que los emisores de luz (LED) de los discos físicos parpadeen y dejen de parpadear.
- Compatibilidad para plataformas más nuevas:
  - Plataformas basadas en nodos AX: soluciones Dell EMC para nodos Microsoft Azure Stack HCI: AX-640, AX-6515 y AX-740xd.
  - Plataformas basadas en los nodos Storage Spaces Direct Ready de Dell EMC: Soluciones Dell EMC para Microsoft Azure Stack HCI: R440, R640, R740xd y R740xd2.
- Compatibilidad para Microsoft Windows Admin Center versión 1910.2.
- Capacidad de monitorear el estado y el inventario de aceleradores (GPU) con los servidores PowerEdge más recientes basados en iDRAC9.
- Mejoras de interfaz del usuario para el inventario y la supervisión del estado de la memoria persistente Intel.
- Mejoras en el rendimiento de Update Compliance.
- Correlación entre controladoras de almacenamiento y discos físicos para ver los discos asociados.
- Capacidad para actualizar la información de estado, inventario y iDRAC de los nodos de destino administrados, a fin de garantizar que la información de inventario que se muestra sea la más reciente.
- Mejora de capacidad de uso mediante la descarga automática de DSU e IC, necesarios para la actualización de componentes.

- Capacidad para descargar las utilidades del catálogo, la DSU y el IC desde Internet mediante la configuración de proxy para generar el informe de cumplimiento.
- Muestra el distintivo de soluciones Dell EMC con **certificación para Azure Stack HCI** para las soluciones Dell EMC para clústeres Microsoft Azure Stack HCI consistentes en nodos AX o nodos Storage Spaces Direct Ready.

Recursos adicionales

Tabla 1. Recursos adicionales

Documento	Descripción	Disponibilidad
Guía de instalación de Dell EMC OpenManage Integration with Microsoft Windows Admin Center	Proporciona información sobre la instalación y configuración de OpenManage Integration with Microsoft Windows Admin Center.	1. Vaya a Dell.com/OpenManageManuals. 2. Seleccione **OpenManage Integration with Microsoft Windows Admin Center**. 3. Haga clic en **DOCUMENTACIÓN** > **MANUALES Y DOCUMENTOS** para tener acceso a estos documentos.
Notas de la versión de Dell EMC OpenManage Integration with Microsoft Windows Admin Center	Sirven para informar acerca de nuevas características, problemas conocidos y soluciones alternativas en OpenManage Integration with Microsoft Windows Admin Center.	
Informe de cumplimiento de infraestructura de Dell EMC para servidores PowerEdge y los clústeres Azure Stack HCI mediante OMIMSWAC	En este informe técnico, se describe el proceso para generar un informe de cumplimiento de actualización para servidores PowerEdge, clústeres Microsoft Azure Stack HCI y clústeres de conmutación por error basados en Hyper-V mediante OMIMSWAC.	
Documentación de Microsoft Windows Admin Center	Es una fuente para obtener más información acerca del uso de Microsoft Windows Admin Center.	https://www.microsoft.com/en-us/cloud-platform/windows-admin-center

2

Introducción a OpenManage Integration with Microsoft Windows Admin Center

Antes de iniciar la extensión Dell EMC OpenManage Integration en Windows Admin Center, asegúrese de lo siguiente:

- Haber iniciado sesión en Windows Admin Center como administrador de puerta de enlace.

Después de instalar OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC), realice las siguientes acciones para iniciar la extensión:

1. En la esquina superior izquierda de Windows Admin Center, seleccione:
   - Para Windows Admin Center versión 1910.2 GA, 2007 GA o 2009 GA: **Administrador de servidores** o **Administrador de clústeres** en el menú desplegable.
2. En la lista, seleccione una conexión de servidor o clúster y, a continuación, haga clic en **Conectar**.
3. Ingrese las credenciales del servidor o clúster.

   NOTA: Si no se le pide ingresar las credenciales, asegúrese de seleccionar "Administrar como" e ingrese las cuentas correspondientes de administrador del servidor o administrador de clústeres.

   NOTA: OMIMSWAC no es compatible con los métodos de autenticación de Single Sign On y tarjeta inteligente.
4. En el panel izquierdo de Microsoft Windows Admin Center, en **EXTENSIONES**, haga clic en **Dell EMC OpenManage Integration**.

Cuando inicia OpenManage Integration por primera vez, se muestra un aviso al cliente para indicar las operaciones que ejecuta OpenManage Integration, como habilitar NIC USB y crear un usuario de iDRAC en el nodo objetivo. Haga clic en **Aceptar** para seguir administrando servidores PowerEdge mediante OpenManage Integration.

NOTA: Una vez que se recopila la información de los nodos administrados, OMIMSWAC elimina el usuario iDRAC creado anteriormente.

Para garantizar el funcionamiento correcto de OpenManage Integration with Microsoft Windows Admin Center, asegúrese de lo siguiente:

- El firewall en su entorno empresarial permite la comunicación a través del puerto SMB 445.
- El servicio Redfish está habilitado en el nodo de destino.
- Existe un espacio para usuario de iDRAC disponible en el nodo de destino.
- Asegúrese de que el nodo de destino no se inicie en Lifecycle Controller.
- El nodo de destino no se encuentra en el estado de reinicio o está apagado.
- El adaptador de la NIC USB no está deshabilitado en el SO del nodo de destino.
- El modo de bloqueo está deshabilitado en el nodo de destino.
- La política de ejecución de PowerShell se establece en RemoteSigned en el sistema con Windows Admin Center instalado y en el sistema operativo del nodo de destino. Para obtener más información, consulte https://www.dell.com/support/article/sln318718/dell-emc-openmanage-integration-with-microsoft-windows-admin-center-omimswac-fails-to-query-host-information.

NOTA: Para la administración de servidores PowerEdge, OMIMSWAC utiliza un SO interno para la interfaz de paso de iDRAC. De manera predeterminada, se podrá acceder a la iDRAC mediante la dirección IP 169.254.0.1/<Subnet> o 169.254.1.1/<Subnet>. Sin embargo, si el host tiene otra interfaz de red en la misma subred (por ejemplo, cuando se instala una herramienta como VMFleet), es posible que OMIMSWAC no pueda comunicarse con la iDRAC desde el SO host. Para resolver el conflicto, inicie sesión en iDRAC y cambie la dirección IP de la NIC USB en la sección de paso de SO a iDRAC. Para obtener más información acerca de la asignación de esta dirección IP, consulte la documentación de la iDRAC en el sitio de soporte de Dell EMC.

Para administrar:

- Servidores PowerEdge, consulte Administración de servidores Dell EMC PowerEdge en la página 10.
- En el caso de los clústeres Microsoft de conmutación por error creados con servidores PowerEdge o Azure Stack HCI, creados con nodos AX o Microsoft Storage Spaces Direct Ready de Dell EMC, consulte Administrar clústeres de conmutación por error y Azure Stack HCI en la página 13.

3

Puertos requeridos por Dell EMC OpenManage Integration with Microsoft Windows Admin Center

Tabla 2. Puertos requeridos por Dell EMC OpenManage Integration with Microsoft Windows Admin Center

Funcionalidad de OpenManage Integration with Windows Admin Center	Sistema con Windows Admin Center instalado	Nodo objetivo/nodo de clúster	Sistema en el que esté disponible el catálogo DRM	Sistema en el que estén disponibles las utilidades DSU e IC	iDRAC del nodo objetivo/ nodo de clúster
Instalación	ND	ND	ND	ND	ND
Desinstalación	ND	ND	ND	ND	ND
Estado, hardware e inventario del iDRAC	445: salida	445: entrada	ND	ND	443 (puerto predeterminado)
Configuración de herramientas de actualización: conexión de prueba	445: salida	ND	ND	445: entrada	ND
Cumplimiento de normas de la actualización	ND	445: entrada	445: salida	445: salida	ND
Notificaciones del cumplimiento de normas de la actualización	445: salida	ND	445: entrada	ND	ND
Actualización del nodo objetivo y actualización compatible con clústeres	ND	Puertos WinRM predeterminados proporcionados por Microsoft	445: salida	445: salida	443 (puerto predeterminado)

Para obtener más información sobre el puerto SMB 445, consulte https://go.microsoft.com/fwlink/?linkid=2101556.

Para obtener más información sobre los puertos WinRM, consulte https://docs.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management.

4

Administración de servidores Dell EMC PowerEdge

Requisitos previos:

- Debe tener una sesión abierta en Microsoft Windows Admin Center como administrador de la gateway.
- Debe tener instalada la extensión Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC). Para obtener más información acerca del procedimiento de instalación, consulte la *Guía de instalación de Dell EMC OpenManage Integration with Microsoft Windows Admin Center*.
- Las conexiones del servidor se agregan en Microsoft Windows Admin Center. Si desea obtener más información sobre cómo agregar conexiones del servidor, consulte https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center.

Para administrar servidores PowerEdge:

1. En la esquina superior izquierda de Windows Admin Center, seleccione **Administrador del servidor** en el menú desplegable.
2. En la lista, seleccione una conexión de servidor y, a continuación, haga clic en **Conectar**.

   NOTA: Si no ingresó las credenciales del servidor cuando agregó la conexión, debe ingresarlas cuando se conecte al servidor con la opción "Administrar como".

3. En el panel izquierdo de Microsoft Windows Admin Center, en **EXTENSIONES**, haga clic en **Dell EMC OpenManage Integration**.
4. Seleccione:
   - **Condición**: para ver el estado de los componentes del nodo objetivo. Un icono de estado representa el estado de condición general del nodo objetivo. Consulte Estado de la condición: componentes de nodos de destino compatibles en la página 11.
   - **Inventario**: para ver la información detallada del inventario de hardware de los componentes del nodo objetivo. Consulte Inventario de hardware: componentes compatibles del nodo objetivo en la página 11.
   - **Actualizar**: para ver el informe de cumplimiento y para actualizar los componentes a la versión de configuración básica. Consulte Actualizar los servidores PowerEdge y los nodos de los clústeres HCI y de conmutación por error en la página 17.
   - **iDRAC**: para ver los detalles del iDRAC de los nodos objetivo. Puede iniciar directamente la consola de iDRAC desde Windows Admin Center mediante OpenManage Integration. Consulte Cómo ver detalles de la iDRAC de los servidores de PowerEdge y los nodos de los clústeres HCI y de conmutación por error en la página 16.

NOTA: Los detalles del estado, el inventario de hardware y el iDRAC se almacenan en la memoria caché y no se cargan cada vez que se carga la extensión. Para ver los detalles del iDRAC y el estado de la condición y del inventario más recientes, haga clic en **Actualizar** en la esquina superior derecha del Estado de la condición.

NOTA: Para los servidores modulares (servidores PowerEdge modelos YX2X, YX3X, YX4X, YX5X y superiores), no se muestra la siguiente información relacionada con ventiladores y fuentes de alimentación:

- Estado de la condición
- Valores de atributos en la tabla de inventario de hardware

NOTA: En el caso de los servidores PowerEdge modelos YX2X e YX3X con una versión de firmware anterior a la 2.60.60.60, no se muestra información acerca de los siguientes componentes:

- Estado de condición: aceleradores, memoria, controladoras de almacenamiento, gabinetes de almacenamiento y discos físicos.
- Inventario de hardware: aceleradores, memoria, controladoras de almacenamiento, gabinetes de almacenamiento, discos físicos, dispositivos de red y firmware.

Temas:

- Estado de la condición: componentes de nodos de destino compatibles
- Inventario de hardware: componentes compatibles del nodo objetivo

Estado de la condición: componentes de nodos de destino compatibles

Se muestra el estado de los siguientes componentes del nodo de destino:

- CPU
- Aceleradores
- Memoria
- Controladoras de almacenamiento
- Gabinetes de almacenamiento
- Discos físicos
- iDRAC
- Sistemas de alimentación
- Ventiladores
- Voltajes
- Temperaturas

NOTA: La información sobre el estado está disponible para los aceleradores en los modelos YX4X de los servidores PowerEdge y versiones superiores con iDRAC versión 4.00.00.00 o superior.

NOTA: La memoria Intel **DIMM** se identifica como **IntelPersistent** con un icono.

Los estados de condición se representan mediante un gráfico de anillos. Puede seleccionar distintas secciones del gráfico de anillos para filtrar el estado de los componentes. Por ejemplo, cuando selecciona la sección roja, solo se muestran los componentes con estado crítico.

Para ver el estado de la condición más reciente, en la esquina superior derecha de la pestaña **Estado** haga clic en **Actualizar**.

NOTA: En las controladoras de almacenamiento de software y los discos físicos conectados a la controladora SATA integrada, el estado de condición del inventario siempre se muestra como “Desconocido”.

Inventario de hardware: componentes compatibles del nodo objetivo

Se muestran los inventarios de hardware de los siguientes componentes del nodo objetivo:

- Sistema
- Firmware
- CPU
- Aceleradores
- Memoria
- Controladoras de almacenamiento

  Para ver los discos físicos de una controladora de almacenamiento, haga clic en el enlace **Ver discos** en **Discos relacionados**. Los discos físicos se muestran en la pestaña **Discos físicos**.

- Gabinetes de almacenamiento
- Dispositivos de red
- Discos físicos

  Para ver las propiedades adicionales de un disco, seleccione el disco y, a continuación, haga clic en **Propiedades avanzadas**. Para ver la controladora de almacenamiento asociada, haga clic en el enlace de la controladora de almacenamiento en **Propiedades avanzadas**. La controladora de almacenamiento asociada aparece en la pestaña **Controladoras de almacenamiento**. Si los discos físicos están conectados a la CPU, el enlace de la controladora de almacenamiento no está disponible en **Propiedades avanzadas**.

  Hacer destellar y dejar de hacer destellar los discos físicos

  Seleccione un disco físico y haga clic en **Hacer destellar** para activar el destello de los LED en el disco físico. Los LED representan el estado de los discos físicos. Que los discos físicos estén destellando, ayuda a localizar y además, a identificar los discos físicos defectuosos del centro de datos. Para deshabilitar el destello de los discos físicos, seleccione un disco y haga clic en **Dejar de hacer destellar**.

NOTA: Puede que las funciones para hacer destellar y dejar de hacer destellar no estén disponibles para:

- Discos asociados a las tarjetas del Subsistema de almacenamiento optimizado de arranque (BOSS).
- Dispositivos con una versión de firmware del iDRAC inferior a 3.30.30.30. Actualice el firmware del iDRAC a la versión más reciente para activar las operaciones para hacer destellar y dejar de hacer destellar.

NOTA:

- Cuando se ejecuta la operación para hacer destellar o dejar de hacer destellar, el botón **Actualizar** para cargar la información más reciente del inventario de estado y hardware está deshabilitado. Además, cuando el inventario de estado y hardware se está cargando en OMIMSWAC, las operaciones para hacer destellar y dejar de hacer destellar se deshabilitan.
- La operación para hacer destellar o dejar de hacer destellar falla en los discos físicos que están conectados a una controladora SATA integrada con un error `Hacer destellar/Dejar de hacer destellar puede no ser compatible con <nombre_disco>.`

- Sistemas de alimentación
- Ventiladores

Para ver la información más reciente sobre el inventario de hardware, en la esquina superior derecha de la pestaña **Inventario**, haga clic en **Actualizar**.

Para ver los detalles de la iDRAC del nodo objetivo, consulte Cómo ver detalles de la iDRAC de los servidores de PowerEdge y los nodos de los clústeres HCI y de conmutación por error en la página 16.

NOTA: En **Inventario**, los valores de los atributos de algunos componentes del nodo objetivo se muestran en blanco, ya que es posible que el valor no esté disponible en el nodo objetivo.

NOTA: En Inventario de firmware, para algunos dispositivos de red con varios puertos, ya que la versión de firmware correspondiente es igual para todos los puertos, solo se mostrará un solo puerto con la versión de firmware.

NOTA: Es posible que la información de algunos de los atributos de los gabinetes de almacenamiento, el inventario de firmware y el componente de memoria no esté disponible para:

- servidores PowerEdge modelos YX2X e YX3X.
- servidores PowerEdge modelo YX4X con una versión de iDRAC anterior a la 3.30.30.30.

NOTA: Para el backplane de SSD de PCIe de los gabinetes de almacenamiento, es posible que algunos valores de los atributos no estén disponibles.

NOTA: La información sobre el estado está disponible para los aceleradores en los modelos YX4X de los servidores PowerEdge y versiones superiores con iDRAC versión 4.00.00.00 o superior.

NOTA: La memoria Intel **DIMM** se identifica como **IntelPersistent** con un icono.

5

Administrar clústeres de conmutación por error y Azure Stack HCI

Requisitos previos:

- Tener una sesión abierta en Microsoft Windows Admin Center como administrador de puerta de enlace.
- Debe tener instalada la extensión Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC). Para obtener más información acerca del procedimiento de instalación, consulte la *Guía de instalación de Dell EMC OpenManage Integration with Microsoft Windows Admin Center*.
- Tiene conexiones agregadas de clúster de conmutación por error o hiperconvergentes en Microsoft Windows Admin Center. Para obtener más información acerca de cómo agregar conexiones de clúster de conmutación por error o hiperconvergentes, consulte https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/understand/windows-admin-center.
- Asegúrese de que pueda acceder a todos los nodos de clúster mediante la dirección IP, el nombre de host o el Nombre de dominio completamente calificado (FQDN) antes de administrar el clúster con OMIMSWAC.

Para administrar los clústeres Microsoft de conmutación por error creados con servidores PowerEdge y Azure Stack HCI creados con nodos AX o nodos Storage Spaces Direct Ready de Dell EMC:

1. En la esquina superior izquierda de Windows Admin Center, seleccione:
   - Para Windows Admin Center versión 1910.2 GA, 2007 GA o 2009 GA: **Administrador de clústeres** del menú desplegable.
2. En la lista, seleccione una conexión de clúster de conmutación por error o hiperconvergente y, luego, haga clic en **Conectar**.
3. En el panel izquierdo de Microsoft Windows Admin Center, en **EXTENSIONES**, haga clic en **Dell EMC OpenManage Integration**.
4. Para administrar un clúster hiperconvergente o de conmutación por error, seleccione:
   - **Estado**: para ver el estado de mantenimiento de los componentes del servidor de los nodos individuales en el clúster.
     - En la sección **Estado de mantenimiento general**, se muestra el estado general del clúster. Seleccione diferentes secciones del gráfico de anillos para filtrar el estado de los componentes de los nodos del clúster.

       NOTA: Es posible que el estado general del clúster se muestre como crítico o como una advertencia, a pesar de que los componentes de los nodos que se muestran en Windows Admin Center están en buen estado. Para obtener más detalles sobre los componentes en estado crítico, acceda a la consola de la iDRAC correspondiente.

     Consulte Estado de mantenimiento: componentes compatibles del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI en la página 14.
   - **Inventario**: para ver la información detallada del inventario de hardware del componente. En la página **Descripción general**, se enumeran los detalles básicos de los nodos del clúster de conmutación por error o hiperconvergente. Seleccione el nodo que desea para ver el inventario de hardware detallado de los componentes del servidor. Consulte Inventario de hardware: componentes compatibles del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI en la página 14.
   - **Actualizar**: para ver y actualizar los gráficos de cumplimiento de los nodos y los componentes. Expanda el nodo requerido para ver un informe de cumplimiento de normas detallado de los componentes. Consulte Actualizar los servidores PowerEdge y los nodos de los clústeres HCI y de conmutación por error en la página 17.
   - **iDRAC**: para ver los detalles del iDRAC de los nodos individuales. Puede iniciar directamente la consola de iDRAC desde Windows Admin Center mediante OpenManage Integration. Consulte Cómo ver detalles de la iDRAC de los servidores de PowerEdge y los nodos de los clústeres HCI y de conmutación por error en la página 16.

NOTA: Los detalles del estado, el inventario de hardware y el iDRAC se almacenan en la memoria caché y no se cargan cada vez que se carga la extensión. Para ver los detalles del iDRAC y el estado de la condición y del inventario más recientes, haga clic en **Actualizar** en la esquina superior derecha del Estado de la condición.

Temas:

- Estado de mantenimiento: componentes compatibles del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI
- Inventario de hardware: componentes compatibles del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI

Estado de mantenimiento: componentes compatibles del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI

En la página **Clúster: Azure Stack HCI**, seleccione la pestaña **Estado** para ver el estado general del clúster de conmutación por error o HCI y el estado de mantenimiento de los siguientes componentes de los nodos objetivo en los nodos del clúster de conmutación por error o Azure Stack HCI. La selección de una sección crítica o de advertencia en el gráfico de anillos de estado general muestra los nodos correspondientes y los componentes en el estado crítico o de advertencia, respectivamente.

- CPU
- Aceleradores
- Memoria
- Controladoras de almacenamiento
- Gabinetes de almacenamiento
- Discos físicos
- iDRAC
- Sistemas de alimentación
- Ventiladores
- Voltajes
- Temperaturas

NOTA: La información sobre el estado está disponible para los aceleradores en los modelos YX4X de los servidores PowerEdge y versiones superiores con iDRAC versión 4.00.00.00 o superior.

NOTA: La memoria Intel **DIMM** se identifica como **IntelPersistent** con un icono.

Los estados de condición se representan mediante un gráfico de anillos. Puede seleccionar distintas secciones del gráfico de anillos para filtrar el estado de los componentes. Por ejemplo, cuando selecciona la sección roja, solo se muestran los componentes con estado crítico.

En un clúster de conmutación por error o HCI, si se seleccionan diferentes secciones del gráfico de anillos para los componentes individuales, se enumeran los nodos respectivos con el estado del componente. Expanda los nodos para ver los componentes en un estado específico.

Para ver el estado de la condición más reciente, en la esquina superior derecha de la pestaña **Estado** haga clic en **Actualizar**.

NOTA: Para las controladoras de almacenamiento de software y los discos físicos conectados a la controladora SATA integrada, el estado del inventario siempre se mostrará como "Desconocido".

Inventario de hardware: componentes compatibles del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI

Se muestra el inventario de hardware de los siguientes componentes del nodo objetivo de los nodos en un clúster de conmutación por error o Azure Stack HCI:

- Sistema
- Firmware
- CPU
- Aceleradores
- Memoria
- Controladoras de almacenamiento

  Para ver los discos físicos de una controladora de almacenamiento, haga clic en el enlace **Ver discos** en **Discos relacionados**. Los discos físicos se muestran en la pestaña **Discos físicos**.

  Gabinetes de almacenamiento
- Dispositivos de red

- Discos físicos

  Para ver las propiedades adicionales de un disco, seleccione el disco y, a continuación, haga clic en **Propiedades avanzadas**. Para ver la controladora de almacenamiento asociada, haga clic en el enlace de la controladora de almacenamiento en **Propiedades avanzadas**. La controladora de almacenamiento asociada aparece en la pestaña **Controladoras de almacenamiento**. Si los discos físicos están conectados a la CPU, el enlace de la controladora de almacenamiento no está disponible en **Propiedades avanzadas**.

  Hacer destellar y dejar de hacer destellar los discos físicos

  Seleccione un nodo y, luego, seleccione un disco físico; haga clic en **Hacer destellar** para activar el destello de los LED en el disco físico. Los LED representan el estado de los discos físicos. Que los discos físicos estén destellando, ayuda a localizar y además, a identificar los discos físicos defectuosos del centro de datos. Para deshabilitar el destello de los discos físicos, seleccione un disco y haga clic en **Dejar de hacer destellar**. En un clúster, la operación para hacer destellar o dejar de hacer destellar de un nodo seleccionado se debe completar antes de utilizar la operación para hacer destellar o dejar de hacer destellar en un nodo diferente.

  NOTA: Puede que las funciones para hacer destellar y dejar de hacer destellar no estén disponibles para:
  - Discos asociados a las tarjetas del Subsistema de almacenamiento optimizado de arranque (BOSS).
  - Dispositivos con una versión de firmware del iDRAC inferior a 3.30.30.30. Actualice el firmware del iDRAC a la versión más reciente para activar las operaciones para hacer destellar y dejar de hacer destellar.
    - Si las operaciones para hacer destellar y dejar de hacer destellar no están disponibles para los discos admitidos seleccionados, incluso con iDRAC versión de firmware 3.30.30.30 y superior, actualice el firmware del iDRAC a la versión más reciente para activar las operaciones para hacer destellar y dejar de hacer destellar.

  NOTA:
  - Cuando se ejecuta la operación para hacer destellar o dejar de hacer destellar, el botón **Actualizar** para cargar la información más reciente del inventario de estado y hardware está deshabilitado. Y, cuando el inventario de estado y hardware se carga en OMIMSWAC, las operaciones para hacer destellar y dejar de hacer destellar se deshabilitan.
  - La operación para hacer destellar o dejar de hacer destellar falla en los discos físicos que están conectados a una controladora SATA integrada con un error `Hacer destellar/Dejar de hacer destellar puede no ser compatible con <nombre_disco>.`
- Sistemas de alimentación
- Ventiladores

Para ver la información más reciente sobre el inventario de hardware, en la esquina superior derecha de la pestaña **Inventario**, haga clic en **Actualizar**.

Para ver los detalles de la iDRAC del nodo objetivo, consulte Cómo ver detalles de la iDRAC de los servidores de PowerEdge y los nodos de los clústeres HCI y de conmutación por error en la página 16.

NOTA: En **Inventario**, los valores de los atributos de algunos componentes del nodo objetivo se muestran en blanco, ya que es posible que el valor no esté disponible en el nodo objetivo.

NOTA: En Inventario de firmware, para algunos dispositivos de red con varios puertos, ya que la versión de firmware correspondiente es igual para todos los puertos, solo se mostrará un solo puerto con la versión de firmware.

NOTA: Es posible que la información de algunos de los atributos de los gabinetes de almacenamiento, el inventario de firmware y el componente de memoria no esté disponible para:
- servidores PowerEdge modelos YX2X e YX3X.
- servidores PowerEdge modelo YX4X con una versión de iDRAC anterior a la 3.30.30.30.

NOTA: Para el backplane de SSD de PCIe de los gabinetes de almacenamiento, es posible que algunos valores de los atributos no estén disponibles.

NOTA: La información sobre el estado está disponible para los aceleradores en los modelos YX4X de los servidores PowerEdge y versiones superiores con iDRAC versión 4.00.00.00 o superior.

NOTA: La memoria Intel **DIMM** se identifica como **IntelPersistent** con un icono.

6

Cómo ver detalles de la iDRAC de los servidores de PowerEdge y los nodos de los clústeres HCI y de conmutación por error

Para ver los siguientes detalles de iDRAC del nodo objetivo, seleccione **Administrador del servidor** o **Administrador de clústeres** en la esquina superior izquierda de Microsoft Windows Admin Center y, luego, seleccione un servidor o una conexión de clústeres en la lista. En el panel izquierdo, en EXTENSIONES, haga clic en **Dell EMC OpenManage Integration** y vaya a la pestaña **iDRAC**.

NOTA: Para los clústeres hiperconvergentes y de conmutación por error, expanda los nodos para ver los siguientes detalles.

- Dirección IP de la iDRAC. Puede iniciar la consola de iDRAC directamente desde Microsoft Windows Admin Center.
- Versión de IPMI.
- Versión del firmware de la iDRAC.

7

Actualizar los servidores PowerEdge y los nodos de los clústeres HCI y de conmutación por error

OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) permite generar detalles de cumplimiento y actualizar componentes, como BIOS, controladores, firmware o aplicaciones de administración del sistema de los nodos de destino, y los nodos en clústeres HCI y de conmutación por error. Puede utilizar un catálogo en línea u offline para generar los detalles de cumplimiento y actualizar los componentes.

En OMIMSWAC, haga clic en **Actualizar**. Aparece la ventana de actualización.

En esta página, puede generar un informe de cumplimiento de normas y actualizar los componentes de la siguiente manera:

1. Generar informe de cumplimiento: seleccione el catálogo de la fuente de actualización (catálogo en línea u offline) para obtener los detalles de la actualización de cada dispositivo y generar un informe de cumplimiento.
2. Verificar el informe de cumplimiento y confirmar la selección de componentes: verifique el informe de cumplimiento generado. De forma predeterminada, se seleccionan todos los componentes de no cumplimiento (excepto los componentes que se pueden degradar). Seleccione o borre los componentes que desea actualizar y, a continuación, confirme la selección de componentes.
3. Actualizar: actualice el nodo o el clúster de destino.

Para generar un informe de cumplimiento y actualizar un nodo de destino, consulte Actualizar el nodo de destino. Para generar el informe de cumplimiento y actualizar los nodos de clústeres HCI y de conmutación por error, consulte Actualizar nodos de clústeres HCI y de conmutación por error.

OpenManage Integration utiliza el catálogo en línea u offline para crear bases. El catálogo contiene las versiones más recientes del BIOS, el controlador, el firmware o las aplicaciones de administración del sistema. Es posible que la aplicación de administración del sistema incluya IC, el paquete de controladores, iSM, OMSA etc. OpenManage Integration también utiliza las herramientas Dell EMC System Update Utility (DSU) y Dell EMC Inventory Collector (IC) para obtener los detalles de actualización de cada dispositivo. Las herramientas DSU e IC ayudan a generar el informe de cumplimiento y corregir los dispositivos de no cumplimiento mediante su actualización.

Cuando selecciona un catálogo offline o en línea, OMIMSWAC recolecta las herramientas DSU e IC configuradas en **Configuración** > **Herramientas de actualización**. Para configurar las herramientas de actualización, consulte Configuración de las herramientas de cumplimiento de la actualización. Si no se han ajustado las herramientas DSU e IC en la configuración, OMIMSWAC con acceso a Internet las descarga de `www.downloads.dell.com`.

En la sección **Notificaciones** de Windows Admin center, recibe una notificación cuando esté disponible un nuevo archivo de catálogo en línea u offline. Para generar el informe de cumplimiento más reciente, en la pestaña **Actualizar**, ejecute el informe de cumplimiento de actualización.

NOTA: La función de actualización compatible con clústeres (CAU) es compatible con la siguiente plataforma con licencias válidas:

- Modelos YX4X de servidor Dell EMC PowerEdge y superior con iDRAC firmware 4.00.00.00 o posterior.
- Soluciones Dell EMC para Microsoft Azure Stack HCI con iDRAC firmware 4.00.00.00 o posterior.

Para obtener más información acerca de las licencias, consulte *Licenciamiento de OpenManage Integration with Windows Admin Center* en la Guía de instalación de OMIMSWAC.

Temas:

- Configuración de las herramientas de cumplimiento de normas de la actualización
- Actualizar nodos objetivo
- Actualizar los nodos de HCI y los clústeres de conmutación por error

Configuración de las herramientas de cumplimiento de normas de la actualización

Para generar el informe de cumplimiento de la actualización más reciente y los detalles de los componentes del dispositivo, OpenManage Integration sin acceso a Internet requiere que configure los ajustes para las herramientas de cumplimiento de actualizaciones. Las versiones compatibles de las utilidades Dell System Update (DSU) y Dell Inventory Collector (IC) para lOpenManage Integration versión 1.1.1 son:

- Versión de DSU: 1.8.1. Descargue la DSU de https://downloads.dell.com/OMIMSWAC/DSU/.
- Versión IC: Descargue el IC desde https://downloads.dell.com/OMIMSWAC/IC/.

La siguiente configuración es necesaria cuando OMIMSWAC no está conectado a Internet y se utiliza el catálogo de Dell EMC Repository Manager (DRM) sin conexión para generar el informe de cumplimiento y actualizar los componentes.

1. En la pestaña **Configuración**, ingrese la ubicación del recurso compartido donde se ubica la utilidad DSU.

   La DSU se utiliza para implementar los paquetes de actualización de Dell en los nodos objetivo.
2. Ingrese la ubicación del recurso compartido donde se ubica la utilidad IC.

   La utilidad IC se utiliza para recopilar la información del inventario de hardware de los nodos objetivo.
3. Ingrese la información de identificación para acceder a la ubicación del recurso compartido.

   NOTA: Cuando OMIMSWAC se desinstala, los datos que se encuentran en la página de Configuración no se eliminan. Si vuelve a instalar OMIMSWAC posteriormente, los datos configurados con anterioridad en la página de Configuración aún estarán disponibles. Sin embargo, la contraseña no estará disponible.
4. Para confirmar si se puede acceder a las utilidades, haga clic en **Probar conexión**.
5. Haga clic en **Guardar** para guardar la configuración de las herramientas de actualización.

   Las contraseñas de la configuración de la herramienta de actualización se conservan solo para la sesión actual del navegador. Asegúrese de volver a introducir la contraseña después de abrir una nueva sesión del navegador para que la función de Cumplimiento de la actualización de OpenManage Integration with Microsoft Windows Admin Center funcione correctamente.

   Para generar el informe de cumplimiento de actualización más reciente, consulte Generación de informe de cumplimiento: nodo objetivo y Generación de informe de cumplimiento: componentes del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI.

Configurar ajustes de proxy

OMIMSWAC proporciona una opción para descargar las utilidades de los catálogos, las DSU y los IC desde Internet mediante la configuración de proxy para generar el informe de cumplimiento. Sin embargo, OMIMSWAC, que está conectado a Internet por proxy, no admite la actualización de los nodos objetivo o clústeres que utilizan catálogos en línea. En este caso, se admite el cumplimiento y las actualizaciones que utilizan el catálogo offline.

Puede configurar los ajustes de proxy para conectarse a un servidor proxy que actúe como intermediario entre el sistema de gateway e Internet. Si la configuración de la herramienta de cumplimiento de actualización de OMIMSWAC no está configurada y el sistema de gateway no está conectado a Internet, esta comprueba la conexión a Internet mediante la configuración de proxy.

Para conectarse a un servidor proxy:

1. Ingrese la dirección IP del servidor proxy en el siguiente formato:

   `https://<Dirección IP>` o **`http://<Dirección IP>`**
2. Ingrese el número de puerto del servidor proxy en el siguiente formato y haga clic en **Guardar**.

   `<número de puerto> (https)` o **`<número de puerto> (http)`**

   Por ejemplo: 443 (https) u 80 (http)

   Para generar el informe de cumplimiento de actualización más reciente, consulte Generación de informe de cumplimiento: nodo objetivo y Generación de informe de cumplimiento: componentes del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI.

Actualizar nodos objetivo

Mediante el uso de OpenManage Integration with Windows Admin Center, puede ver el informe de cumplimiento (BIOS, controlador, firmware o aplicación de administración de sistemas) y actualizar los componentes de los nodos objetivo.

Requisitos previos de cumplimiento y actualización

Antes de generar un informe de cumplimiento y actualizar los componentes, asegúrese de lo siguiente:

- Se cumplen los requisitos de hardware y software que se detallan en la *matriz de compatibilidad* de la Guía de instalación.
- Para administrar un nodo objetivo, conéctese al nodo objetivo mediante la opción **Administrar como** y proporcione las credenciales correspondientes de administrador del nodo objetivo. Asegúrese de que el usuario forme parte del grupo de usuarios locales de los administradores de la gateway. Para obtener más información acerca de la selección de "Administrar como", consulte la sección "Introducción a Windows Admin Center" en la documentación del Microsoft.
- Tenga cuidado con la carga de trabajo antes de actualizar el nodo objetivo.
- Asegúrese de que se haya recuperado la información del inventario para el nodo objetivo.
- Asegúrese de que el modo de bloqueo del iDRAC esté deshabilitado. Para deshabilitar el modo de bloqueo del sistema iDRAC, consulte los documentos del iDRAC.
- Para SAS RAID_Driver, asegúrese de lo siguiente:
  - Establezca la controladora SATA en el modo RAID.
  - Establezca las NVMe PCIe SSDs en el modo RAID.

  Para obtener más información sobre la configuración del modo RAID, consulte Apéndice
- Asegúrese de que el WAC no esté instalado en el nodo objetivo que desea actualizar.
- Asegúrese de que se pueda acceder al nodo objetivo mediante la dirección IP, el nombre de host y el nombre de dominio completamente calificado (FQDN) del nodo objetivo.

  NOTA: Si no se puede acceder al nodo objetivo y se ejecuta la actualización del nodo objetivo, es posible que el estado de la actualización muestre una falla. En este caso, si reinicia el nodo objetivo inmediatamente después de actualizar y volver a ejecutar el cumplimiento, es posible que el estado de los componentes del nodo objetivo muestre cumplimiento, mientras que el estado general de la actualización del nodo objetivo puede seguir mostrando una falla.

NOTA: No se recomienda actualizar un nodo objetivo en el que está instalado el WAC. Para admitir esta situación, instale el WAC en otro nodo objetivo (no relacionado con el WAC) y complete la actualización.

NOTA: Mientras el cumplimiento o la actualización están en curso, no está permitido ejecutar ninguna otra tarea de cumplimiento o actualización para el mismo nodo objetivo que incluye las solicitudes de actualización de las herramientas de actualización MS WAC.

Paso 1: Generación del informe de cumplimiento: componentes del nodo de destino

Para generar un informe de cumplimiento de un nodo de destino, seleccione **Actualizar > Fuente de actualización** y elija cualquiera de las opciones disponibles de catálogo en línea u offline de la siguiente manera:

Generación del informe de cumplimiento mediante el catálogo en línea

Para usar el catálogo en línea, OMIMSWAC debe estar conectado a Internet con o sin configuración de proxy. OMIMSWAC con acceso a Internet le permite usar la opción de catálogo en línea de la lista desplegable **Fuente de actualización** para descargar automáticamente el catálogo.

Para ver los detalles del cumplimiento, debe realizar la siguiente acción:

1. En **Actualizar > Fuente de actualización**, seleccione cualquiera de las opciones disponibles del catálogo en línea.

   El catálogo en línea correspondiente se selecciona de forma predeterminada según el nodo de destino.

   Los catálogos en línea disponibles varían según el nodo o el clúster de destino al que está conectado, como se indica a continuación:
   - Para los servidores PowerEdge y los clústeres que contienen servidores PowerEdge: el catálogo de Dell EMC Enterprise que contiene las versiones validadas de los componentes de los servidores PowerEdge.
   - En los servidores MX: el catálogo de soluciones de Dell EMC MX que contiene las versiones validadas de los componentes de PowerEdge MX Modular.

- En los nodos de clúster Azure Stack HCI: el catálogo de soluciones de Dell EMC Azure Stack HCI que contiene las versiones validadas de los componentes de los nodos de AX y Storage Spaces Direct Ready Nodes.

Para obtener más información acerca de los catálogos disponibles, consulte el Apéndice.

2. Seleccione **Siguiente: detalles de cumplimiento:** para generar el informe de cumplimiento.

OMIMSWAC descarga el catálogo, recolecta las herramientas DSU e IC configuradas en la pestaña **Configuración**, y genera un informe de cumplimiento. Si no se han configurado las herramientas DSU e IC en **Configuración**, entonces OMIMSWAC las descarga de `www.downloads.Dell.com` para generar el informe de cumplimiento.

Los detalles del cumplimiento se procesan y el informe se encuentra disponible en **Actualizar** > **Detalles de cumplimiento**. Para obtener más detalles sobre el informe de cumplimiento, consulte Ver informe de cumplimiento.

Generación del informe de cumplimiento mediante el catálogo offline

OMIMSWAC con o sin acceso a Internet le permite seleccionar el catálogo Dell EMC Repository Manager offline para generar un informe de cumplimiento.

Antes de generar el informe de cumplimiento más reciente de los componentes del nodo de destino, asegúrese de los siguientes aspectos: Se necesitan los siguientes requisitos previos cuando OMIMSWAC no está conectado a Internet, y el catálogo offline de Dell EMC Repository Manager (DRM) se utiliza para generar un informe de cumplimiento y actualizar los componentes.

- Configure los detalles de la ubicación compartida donde se ubican las aplicaciones DSU e IC. Consulte Configuración de las herramientas de cumplimiento de la actualización.
- Genere los archivos de catálogo más recientes mediante la aplicación Dell EMC Repository Manager (DRM). Puede descargar la versión compatible de DRM desde Dell EMC Repository Manager.

Para ver los detalles del cumplimiento, debe realizar las siguientes acciones:

1. En **Actualizar** > **Fuente de actualización**, seleccione **Offline - Catálogo Dell EMC Repository Manager** en la lista desplegable. El catálogo en línea se selecciona de manera predeterminada.

   Offline - Catálogo Dell EMC Repository Manager: cuando los repositorios DRM están disponibles en una ubicación compartida y se aplican a todos los nodos administrados por OMIMSWAC en centros de datos sin conexión a Internet.

2. Ingrese la ruta del recurso compartido CIFS donde se colocan los archivos de catálogo y las credenciales de usuario para acceder esta ruta; a continuación, seleccione **Siguiente: detalles de cumplimiento:**.

   Los archivos de catálogo se pueden generar mediante la aplicación Dell EMC Repository Manager (DRM). Asegúrese de que en el repositorio del catálogo compartido todos los Dell Update Packages (DUP) requeridos estén disponibles para el nodo objetivo.

   Si se proporciona una nueva ruta de catálogo, la ruta anterior utilizada para procesar el cumplimiento de la actualización ya no está disponible.

OMIMSWAC recolecta el catálogo desde la ruta compartida, recolecta las herramientas DSU e IC configuradas en la pestaña **Configuración**, y genera un informe de cumplimiento. Si no se han configurado las herramientas DSU e IC en la **Configuración**, OMIMSWAC con acceso a Internet las descarga de `www.downloads.dell.com` para generar el informe de cumplimiento.

NOTA: Debe proporcionar archivos de catálogo individuales con la información de identificación del usuario al administrador del servidor y al administrador de clústeres, respectivamente.

Los detalles del cumplimiento se procesan y el informe se encuentra disponible en **Actualizar** > **Detalles de cumplimiento**. Para obtener más detalles sobre el informe de cumplimiento, consulte Ver informe de cumplimiento.

Paso 2: Visualización del informe de cumplimiento y selección de componentes: componentes del nodo de destino

Se procesan los detalles de cumplimiento de actualización y se muestra el informe de cumplimiento. El gráfico de anillos representa con códigos de colores la cantidad de componentes en los estados de cumplimiento, urgentes, recomendados y opcionales. El informe de cumplimiento representa una vista detallada de todos los componentes; contiene el nombre del componente, la versión actual, el tipo, la versión de base, el estado de cumplimiento, la gravedad y el tipo de cumplimiento.

Nombres de los atributos	Descripción
Nombre del componente	Especifica el nombre del componente.

	Por ejemplo: `Serial-ATA_Firmware_6FGD4_WN64_E012_A00`
Cumplimiento	Especifica el tipo de cumplimiento, ya sea cumplimiento o no cumplimiento. • `Cumplimiento`: los nodos de destino en esta categoría tienen las mismas versiones del BIOS, los controladores, el firmware y la aplicación de administración del sistema que el catálogo importado. • `No cumplimiento`: los nodos de destino en esta categoría necesitan actualizaciones del BIOS, los controladores, el firmware o la aplicación de administración del sistema.
Gravedad	Especifica si el cumplimiento es urgente, recomendado u opcional. • `Urgente`: la actualización contiene cambios para mejorar la fiabilidad y la disponibilidad del sistema Dell EMC o el componente relacionado. Por lo tanto, aplique esta actualización inmediatamente. • `Recomendado`: la actualización contiene mejoras o cambios que mantendrán actualizados el software del sistema y la compatibilidad con otros módulos del sistema (firmware, BIOS, controladores y aplicación de administración del sistema). • `Opcional`: la actualización contiene cambios que solo afectan determinadas configuraciones, o bien proporciona nuevas funciones que es posible que se apliquen o no al entorno. Revise las especificaciones de la actualización para determinar si esta se puede aplicar al sistema.
Versión actual	Especifica la versión actual del componente. Por ejemplo: `E012`
Versión de base	Especifica que la versión pertenece al catálogo importado. Por ejemplo: `E013`
Tipo	Especifica el tipo de componente. Por ejemplo: `firmware`, `BIOS`, `controlador`, `aplicación`
Tipo de cumplimiento	Especifica si el componente es actualizable, degradable o es igual. • `Actualizable`: el componente se puede actualizar desde la versión actual. • `Degradable`: el componente se puede degradar de la versión actual. • `Igual`: la versión actual del componente es igual a la versión de base.

1. De forma predeterminada, se seleccionan todos los componentes actualizables que no tienen cumplimiento.

   Borre los componentes seleccionados o seleccione los componentes degradables que no tienen cumplimiento que desea actualizar. Sin embargo, si desea cambiar cualquiera de las selecciones predeterminadas, asegúrese de que se cumplan las dependencias entre el firmware y los controladores del componente respectivo.

2. Una vez que se hayan seleccionado para actualización los componentes, en **Detalles de cumplimiento**, haga clic en **Siguiente: resumen** a fin de avanzar a la página de resumen del informe para confirmar.

   NOTA: Cuando los componentes se seleccionan y se confirman, si el modo de bloqueo está habilitado en la iDRAC en el nodo de destino, se produce un error y no se puede continuar con la actualización. Deshabilite el modo de bloqueo en el nodo de destino que se está administrando mediante OMIMSWAC antes de actualizar el nodo de destino. Para deshabilitar el modo de bloqueo del sistema iDRAC, consulte los documentos del iDRAC.

   - Para cambiar la selección de componentes durante la operación de actualización, en la pestaña **Resumen**, haga clic en **Atrás** para ir a la pestaña **Detalles de cumplimiento**, y seleccione o borre la selección de componentes.
   - Si desea cambiar la fuente de actualización y volver a ejecutar el cumplimiento, haga clic en **Salir** para acceder a la **Fuente de actualización**.

NOTA: Si un catálogo no contiene actualizaciones para un componente, este componente no se muestra en el informe de cumplimiento que se genera a través de la integración de OpenManage Integration with Microsoft Windows Admin Center.

Paso 3: Actualización: componentes del nodo de destino

Después de generar el informe de cumplimiento en la pestaña **Detalles de cumplimiento** y confirmar la selección de componentes en la pestaña **Resumen**, puede continuar con la actualización de los componentes del nodo de destino de la siguiente manera:

1. Para actualizar el BIOS, el controlador, el firmware o la aplicación de administración del sistema del servidor de PowerEdge a la versión más reciente, en **Resumen**, haga clic en **Siguiente: actualizar**. Será dirigido a la ventana **Estado de actualización**.
   NOTA: Mientras la actualización está en curso, no se recomienda salir ni cerrar el navegador. Si cierra o sale del navegador, la actualización del nodo de destino puede fallar.
2. Una vez que haya finalizado el trabajo de actualización recibe una notificación de OMIMSWAC.
   - Una vez que la actualización se haya realizado correctamente, el informe de cumplimiento (basado en las selecciones anteriores) se vuelve a procesar automáticamente y se muestra en la pestaña **Actualizar**.
   - Si la operación de actualización falla, revise los archivos de registro almacenados en la siguiente ruta para obtener más detalles.
     - Sistema de gateway: `<Directorio de Windows>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
     - Sistema de gateway de Windows 10: `<Unidad instalada de Windows>\Usuarios\<user_name>\AppData\Local\Temp\generated\logs`
   - Para volver a ejecutar el informe de cumplimiento, haga clic en **Volver a ejecutar cumplimiento** e ingrese los detalles de configuración de cumplimiento.

Actualizar los nodos de HCI y los clústeres de conmutación por error

La función de actualización compatible con clústeres (CAU) en OpenManage Integration with Windows Admin Center (OMIMSWAC) le permite ver el informe de cumplimiento (BIOS, controlador, firmware o aplicación de administración de sistemas) y actualizar los componentes de los nodos de HCI y de los clústeres de conmutación por error sin afectar las cargas de trabajo.

NOTA: La función CAU es compatible con las siguientes plataformas con licencias válidas:

- Modelos YX4X de servidor Dell EMC PowerEdge y superior con iDRAC firmware 4.00.00.00 o posterior.
- Soluciones Dell EMC para Microsoft Azure Stack HCI con iDRAC firmware 4.00.00.00 o posterior.

Requisitos previos de cumplimiento y actualización

Antes de generar un informe de cumplimiento y actualizar los componentes, asegúrese de lo siguiente:

- Se cumplen los requisitos de hardware y software que se detallan en la *matriz de compatibilidad* de la Guía de instalación.
- Asegúrese de que el servicio de clúster esté activo antes de ejecutar el cumplimiento de la actualización. Cuando el servicio de clúster está inactivo, es posible que no se genere un informe de cumplimiento de la actualización para un nodo objetivo.
- Para administrar un clúster, conéctese con el clúster mediante la opción **Administrar como** y proporcione las credenciales de administrador de clúster adecuadas. Asegúrese de que el usuario forme parte del grupo de usuarios locales de los administradores de la gateway. Para obtener más información acerca de la selección de “Administrar como”, consulte la sección “Introducción a Windows Admin Center” en la documentación del Microsoft.
- Asegúrese de que las herramientas de administración de clústeres de conmutación por error (RSAT-Clustering-Mgmt) estén instaladas en los nodos objetivo.
- Asegúrese de que se haya recuperado la información del inventario para el nodo objetivo.
- Asegúrese de que los discos físicos y virtuales estén en buen estado antes de activar la CAU.
- Asegúrese de que el modo de bloqueo del iDRAC esté deshabilitado. Para deshabilitar el modo de bloqueo del sistema iDRAC, consulte los documentos del iDRAC.
- Para SAS RAID_Driver, asegúrese de lo siguiente:
  - Establezca la controladora SATA en el modo RAID.
  - Establezca las NVMe PCIe SSDs en el modo RAID.

  Para obtener más información sobre la configuración del modo RAID, consulte Apéndice
- Asegúrese de que se pueda acceder al nodo objetivo mediante la dirección IP, el nombre de host y el nombre de dominio completamente calificado (FQDN) del nodo objetivo.

NOTA: Si no se puede acceder al nodo objetivo y se ejecuta la actualización del nodo objetivo, es posible que el estado de la actualización muestre una falla. En este caso, si reinicia el nodo objetivo inmediatamente después de actualizar y vuelve a ejecutar el cumplimiento, es posible que el estado de los componentes del nodo objetivo indique cumplimiento, mientras que el estado general de la actualización del servidor puede continuar mostrando una falla.

- Asegúrese de que las licencias Premium de OMIMSWAC estén instaladas en todos los nodos del clúster para usar la función CAU. Para verificar la licencia, puede generar un informe de cumplimiento para ver la licencia instalada en cada nodo.

NOTA: Se recomienda validar el clúster antes de activar la CAU. Para obtener más información acerca de la validación de un clúster, consulte los documentos de Microsoft sobre cómo Validar hardware para un clúster.

NOTA: No se recomienda actualizar un clúster en el que esté instalado el WAC en un nodo del clúster. Para admitir esta situación, instale el WAC en otro sistema que no forme parte del clúster y complete la actualización.

NOTA: Mientras el proceso de cumplimiento o la actualización están en curso, no está permitido ejecutar ninguna otra tarea de cumplimiento o actualización para el mismo clúster que incluya las solicitudes de actualización de las herramientas de actualización de MS WAC.

NOTA: La función CAU no es compatible con los modelos YX2X y YX3X de los servidores Dell EMC PowerEdge.

Paso 1: generación del informe de cumplimiento. Componentes del nodo objetivo en clústeres de conmutación por error y Azure Stack HCI

Para generar un informe de cumplimiento de los componentes del nodo objetivo en los clústeres de conmutación por error y Azure Stack HCI, seleccione **Actualizar > Fuente de actualización** y elija cualquiera de las opciones disponibles de catálogo offline o en línea de la siguiente manera:

Generación del informe de cumplimiento mediante el catálogo en línea

Para usar el catálogo en línea, OMIMSWAC debe estar conectado a Internet. OMIMSWAC con acceso a Internet le permite usar la opción de catálogo en línea de la lista desplegable **Fuente de actualización** para descargar automáticamente el catálogo.

Para ver los detalles del cumplimiento, debe realizar la siguiente acción:

1. En **Actualizar > Fuente de actualización**, seleccione cualquiera de las opciones disponibles del catálogo en línea. El catálogo en línea correspondiente se selecciona de manera predeterminada en función del clúster.

   Los catálogos en línea disponibles varían según el nodo de clúster o nodo objetivo al que está conectado como se indica a continuación:
   - Para los servidores PowerEdge y los clústeres que contienen servidores PowerEdge: el catálogo de Dell EMC Enterprise que contiene las versiones validadas de los componentes de los servidores PowerEdge.
   - En los servidores MX: el catálogo de soluciones de Dell EMC MX que contiene las versiones validadas de los componentes de PowerEdge MX Modular.
   - En los nodos de clúster Azure Stack HCI: el catálogo de soluciones de Dell EMC Azure Stack HCI que contiene las versiones validadas de los componentes de los nodos de AX y Storage Spaces Direct Ready Nodes.

   Para obtener más información acerca de los catálogos disponibles, consulte el Apéndice.

2. Seleccione **Siguiente: detalles de cumplimiento:** para generar el informe de cumplimiento.

OMIMSWAC descarga el catálogo, recolecta las herramientas DSU e IC configuradas en la pestaña **Configuración**, y genera un informe de cumplimiento. Si no se han configurado las herramientas DSU e IC en **Configuración**, entonces OMIMSWAC las descarga de `www.downloads.Dell.com` para generar el informe de cumplimiento.

Será dirigido al informe de cumplimiento generado en la ventana **Detalles de cumplimiento**. Para obtener más detalles sobre el informe de cumplimiento, consulte Ver informe de cumplimiento.

Generación del informe de cumplimiento mediante el catálogo offline

OMIMSWAC con o sin acceso a Internet le permite seleccionar el catálogo Dell EMC Repository Manager offline para generar un informe de cumplimiento.

Antes de generar el informe de cumplimiento más reciente de un clúster, asegúrese de lo siguiente: Se necesitan los siguientes requisitos previos cuando OMIMSWAC no está conectado a Internet, y el catálogo offline de Dell EMC Repository Manager (DRM) se utiliza para generar un informe de cumplimiento y actualizar los componentes.

- Configure los detalles de la ubicación compartida donde se ubican las aplicaciones DSU e IC. Consulte Configuración de las herramientas de cumplimiento de la actualización.
- Genere los archivos de catálogo más recientes mediante la aplicación Dell EMC Repository Manager (DRM). Puede descargar la versión compatible de DRM desde Dell EMC Repository Manager.

Para ver los detalles del cumplimiento, debe realizar las siguientes acciones:

1. En **Actualizar** > **Fuente de actualización**, seleccione **Offline - Catálogo Dell EMC Repository Manager** en la lista desplegable. El catálogo en línea se selecciona de manera predeterminada.

   Catálogo Dell EMC Repository Manager offline: cuando los repositorios de DRM están disponibles en una ubicación compartida y se aplica a todos los dispositivos administrados por OMIMSWAC en centros de datos sin conexión a Internet.

   NOTA: Se recomienda usar los archivos del catálogo Azure Stack HCI para generar un informe de cumplimiento de Azure Stack HCI.
2. Ingrese la ruta de acceso del recurso compartido CIFS donde se colocan los archivos del catálogo y la información de identificación para acceder a la ruta de acceso del recurso compartido CIFS y, a continuación, seleccione **Siguiente: detalles de cumplimiento:** para generar el informe de cumplimiento.

   Los archivos de catálogo se pueden generar mediante la aplicación Dell EMC Repository Manager (DRM). Asegúrese de que en el repositorio del catálogo compartido todos los Dell Update Packages (DUP) requeridos estén disponibles para el nodo objetivo.

   Si se proporciona una nueva ruta de catálogo, la ruta anterior utilizada para procesar el cumplimiento de la actualización ya no está disponible.

OMIMSWAC recolecta el catálogo desde la ruta compartida, recolecta las herramientas DSU e IC configuradas en la pestaña **Configuración**, y genera un informe de cumplimiento. Si no se han configurado las herramientas DSU e IC en la **Configuración**, OMIMSWAC con acceso a Internet las descarga de `www.downloads.dell.com` para generar el informe de cumplimiento.

NOTA: Debe proporcionar archivos de catálogo individuales con la información de identificación del usuario al administrador del servidor y al administrador de clústeres, respectivamente.

Será dirigido al informe de cumplimiento generado en la ventana **Detalles de cumplimiento**. Para obtener más detalles sobre el informe de cumplimiento, consulte Ver informe de cumplimiento.

Paso 2: Visualización del informe de cumplimiento y selección de componentes: componentes de nodos de destino en clústeres de conmutación por error y Azure Stack HCI

Se procesan los detalles de cumplimiento de actualización y se muestra el informe de cumplimiento. El gráfico de anillos representa con códigos de colores la cantidad de componentes en los estados de cumplimiento, urgentes, recomendados y opcionales. El informe de cumplimiento representa una vista detallada de todos los componentes; contiene el nombre del componente, la versión actual, el tipo, la versión de base, el estado de cumplimiento, la gravedad y el tipo de cumplimiento.

En el caso de los clústeres HCI y de conmutación por error, el cumplimiento de la actualización de los nodos de destino y los componentes individuales se representa mediante dos gráficos de anillos: Resumen de nodos y Resumen de componentes. Si desea realizar un análisis mayor, revise los nodos individuales en el informe de cumplimiento para conocer la versión actual, las versiones de base y el tipo de cumplimiento de los componentes, y para ver todos los nodos y los componentes en los estados de no cumplimiento, urgentes, recomendados y opcionales, respectivamente.

Junto con la información de cumplimiento, también se muestra el estado de la licencia (licencia Premium de OMIMSWAC) de cada nodo. Todos los nodos de destino que participan en el clúster deben tener licencias válidas; de lo contrario, no podrá continuar con la actualización del clúster. Para obtener más información acerca del licenciamiento de OMIMSWAC, consulte la Guía de instalación de OMIMSWAC.

Nombres de los atributos	Descripción
Nombre del componente	Especifica el nombre del componente. Por ejemplo: `Serial-ATA_Firmware_6FGD4_WN64_E012_A00`

Cumplimiento	Especifica el tipo de cumplimiento, ya sea cumplimiento o no cumplimiento. • `Compliant` - Los nodos de destino en esta categoría tienen las mismas versiones del BIOS, los controladores, el firmware y la aplicación de administración del sistema que el catálogo importado. • `Non-Compliant` - Los nodos de destino en esta categoría necesitan actualizaciones del BIOS, los controladores, el firmware o la aplicación de administración del sistema.
Gravedad	Especifica si el cumplimiento es urgente, recomendado u opcional. • `Urgent` - La actualización contiene cambios para mejorar la confiabilidad y la disponibilidad del sistema Dell EMC o el componente relacionado. Por lo tanto, aplique esta actualización inmediatamente. • `Recommended` - La actualización cuenta con mejoras o cambios que mantendrán actualizados el software del sistema y la compatibilidad con otros módulos del sistema (BIOS, controladores, firmware y aplicación de administración del sistema). • `Optional` - La actualización contiene cambios que solo afectan determinadas configuraciones o proporcionan nuevas funciones que se podrían aplicar o no en el entorno. Revise las especificaciones de la actualización para determinar si esta se puede aplicar al sistema.
Versión actual	Especifica la versión actual del componente. Por ejemplo: `E012`
Versión de base	Especifica que la versión pertenece al catálogo importado. Por ejemplo: `E013`
Tipo	Especifica el tipo de componente. Por ejemplo: `Firmware`, `BIOS`, `Driver`. `Application`
Tipo de cumplimiento	Especifica si el componente es actualizable, degradable o es igual. • `Upgradable`: el componente se puede actualizar desde la versión actual. • `Downgradable`: el componente puede cambiar a una versión anterior desde la actual. • `Same`: la versión actual del componente es la misma que la versión base.

1. De forma predeterminada, se seleccionan para la actualización todos los componentes actualizables que no tienen cumplimiento.

   Borre los componentes seleccionados o seleccione los componentes degradables que no tienen cumplimiento que desea actualizar. Sin embargo, si desea cambiar cualquiera de las selecciones predeterminadas, asegúrese de que se cumplan las dependencias entre el firmware y los controladores del componente respectivo.

2. Una vez que haya seleccionado los componentes, en **Detalles de cumplimiento**, haga clic en **Siguiente: resumen** a fin de avanzar a la página de resumen del informe para confirmar.

   NOTA: Cuando los componentes se seleccionan y se confirman, si el modo de bloqueo está habilitado en la iDRAC en un nodo de destino, se produce un error y no se puede continuar con la actualización. Deshabilite el modo de bloqueo en el nodo de destino que se está administrando mediante OMIMSWAC antes de actualizar el clúster. Para deshabilitar el modo de bloqueo del sistema iDRAC, consulte los documentos del iDRAC.

   - Para cambiar la selección de componentes durante la operación de actualización, en la pestaña **Resumen**, haga clic en **Atrás** para ir a la pestaña **Detalles de cumplimiento**, y seleccione o borre la selección de componentes.
   - Si desea cambiar la fuente de actualización y volver a ejecutar el cumplimiento, haga clic en **Salir** para acceder a la **Fuente de actualización**.

NOTA: Si un catálogo no contiene actualizaciones para un componente, este componente no se muestra en el informe de cumplimiento que se genera a través de la integración de OpenManage Integration with Microsoft Windows Admin Center.

Paso 3: actualización. Componentes del nodo objetivo en los clústeres de conmutación por error y Azure Stack HCI

Después de generar el informe de cumplimiento en la pestaña **Detalles de cumplimiento** y confirmar la selección de componentes en la pestaña **Resumen**, continúe con la actualización de los componentes del nodo objetivo en los clústeres de conmutación por error y Azure Stack HCI como se indica a continuación:

1. Para actualizar el BIOS, el controlador, el firmware o la aplicación de administración de sistemas de los componentes del nodo objetivo en Azure Stack HCI y el clúster de conmutación por error a la versión más reciente, en **Resumen**, haga clic en **Siguiente: actualización compatible con clústeres**.

   Se solicita un mensaje para habilitar el CredSSP.

2. Haga clic en **Sí** para habilitar el CredSSP y continuar actualizando los componentes seleccionados. Será dirigido a la ventana **Estado de actualización**.

   Para mejorar la seguridad, deshabilite el CredSSP después de que se complete la operación de actualización.

   NOTA: Mientras la actualización está en curso en la ventana **Estado de actualización**, no se recomienda salir ni cerrar el navegador. Si cierra o sale del navegador, la actualización del clúster puede fallar.

   El trabajo de actualización continúa en segundo plano independientemente de si la sesión de la UI está activa o no. Si la sesión de la UI está activa, se muestra el estado de progreso del nivel de nodo. Una vez que haya finalizado el trabajo de actualización recibe una notificación de OMIMSWAC.

   - Una vez que la actualización se haya realizado correctamente, el informe de cumplimiento (basado en las selecciones anteriores) se vuelve a procesar automáticamente y se muestra en la pestaña **Actualizar**.
   - Si la operación de actualización falla, revise los archivos de registro que se almacenan en la siguiente ruta para la solución de problemas.
     - Sistema de gateway: `<Directorio de Windows>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
     - Sistema de gateway de Windows 10: `<Unidad instalada de Windows>\Usuarios\<user_name>\AppData\Local\Temp\generated\logs`
   - Para volver a ejecutar el informe de cumplimiento, haga clic en **Volver a ejecutar cumplimiento** e ingrese los detalles de configuración de cumplimiento.

NOTA: Si falla un trabajo de actualización, los componentes actualizados no se revertirán a la versión anterior. Debido a esto, en ocasiones, el BIOS, el firmware o la versión del controlador entre los nodos del clúster no estarán en el mismo nivel. En este caso, excluya el componente actualizado para volver a ejecutar la actualización.

8

Solución de problemas

Temas:

- Disponibilidad de los registros de la extensión OMIMSWAC
- Disponibilidad de los registros de la operación de actualización
- No se pueden copiar los archivos necesarios en el nodo de destino para obtener la información de inventario.
- No se puede obtener el inventario de estado y hardware desde la iDRAC.
- No se pueden completar ni seleccionar los discos para las operaciones de destellar o dejar de destellar.
- El estado de la licencia es Desconocido o Sin licencia
- El trabajo falló al descargar los componentes necesarios para las operaciones de actualización del servidor y compatible en clústeres.
- CredSSP falló durante la actualización
- El trabajo falló al generar el informe de cumplimiento
- El trabajo falló al actualizar los componentes seleccionados.

Disponibilidad de los registros de la extensión OMIMSWAC

Los registros de los nodos de destino y de clúster de la extensión OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) están disponibles en `<Windows Directory>\Temp\OMIMSWAC`. Los registros capturan información cuando se ejecutan las funcionalidades de OMIMSWAC y también proporcionan información de depuración sobre cualquier error que se produzca durante la ejecución de cualquier operación de OMIMSWAC. Se puede acceder fácilmente a los registros de diversas funcionalidades de OMIMSWAC con la ayuda de la siguiente convención de nomenclatura:

- Para el inventario de hardware y estado: `Inventory<ID*>`
- Para el cumplimiento de normas de la actualización: `FirmwareCompliance<ID*>`
- Para las notificaciones de actualización: `Notification<ID*>`

Disponibilidad de los registros de la operación de actualización

Los registros de aplicaciones de la función de cumplimiento de la actualización están disponibles en la siguiente ruta:

- Sistema de gateway: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs`
- Sistema de gateway de Windows 10: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs`

El estado de descarga de los catálogos en línea se captura en los registros de aplicaciones y los puede consultar para la solución de problemas de errores de descarga en los catálogos en línea.

Cuando selecciona la fuente del catálogo en línea, y si DSU e IC no se ajustan antes en la configuración, OMIMSWAC descarga las utilidades de catálogo, DSU e IC en la siguiente ruta:

- Sistema de gateway: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\Share\temp\<server/cluster_name>`
- Sistema de gateway de Windows 10: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\Share\temp\<server/cluster_name>`

Asegúrese de que el archivo del catálogo descargado, DSU e IC no se modificó durante la generación del cumplimiento y la actualización. El archivo del catálogo, las utilidades DSU e IC se eliminan automáticamente después de que se genera y actualiza el informe de cumplimiento.

Los registros del script previos a la actualización que se ejecuta en los clústeres HCI para poner el almacenamiento en modo de mantenimiento están disponibles en `<Directorio de Windows>\Temp\precau.log`, en cada nodo. Los registros del script posterior a la actualización que se ejecuta en los clústeres HCI para restaurar el almacenamiento desde el modo de mantenimiento están disponibles en `<Directorio de Windows>\Temp\postcau.log`, en cada nodo.

No se pueden copiar los archivos necesarios en el nodo de destino para obtener la información de inventario.

Asegúrese de que:

- El nodo de destino no se encuentra en el estado de reinicio y está encendido.
- El firewall no bloquea la comunicación a través del puerto SMB 445. Para obtener más información, consulte Preparar el ambiente para Windows Admin Center.

No se puede obtener el inventario de estado y hardware desde la iDRAC.

Para obtener información sobre el inventario de estado y hardware desde la iDRAC, asegúrese de que se cumplan los siguientes requisitos:

- En la administración de servidores PowerEdge, OMIMSWAC utiliza un sistema operativo interno para la interfaz de paso de la iDRAC. De manera predeterminada, podrá acceder a la iDRAC con la dirección IP 169.254.0.1/*<Subred>* o 169.254.1.1/*<Subred>*. Sin embargo, si el host tiene otra interfaz de red en la misma subred (por ejemplo, cuando se instala una herramienta como VMFleet), es posible que OMIMSWAC no pueda comunicarse con la iDRAC desde el sistema operativo del host.

  Para resolver el conflicto, inicie sesión en la iDRAC y cambie la dirección IP de la NIC USB en la sección de paso de sistema operativo a iDRAC. Para obtener más información acerca de la asignación de esta dirección IP, consulte la documentación de la iDRAC en el sitio de soporte.

- En la administración de clústeres, antes de administrarlos con OMIMSWAC, se puede acceder a todos los nodos de clúster mediante la dirección IP, el nombre de host y el nombre de dominio completamente calificado (FQDN).
- Si el servicio Redfish está deshabilitado, habilítelo a través de la interfaz de usuario de la iDRAC. Para obtener más información, consulte la documentación de la iDRAC que se encuentra en el sitio de soporte de Dell EMC.
- Hay ranuras de usuario disponibles en la iDRAC para crear nuevos usuarios.

No se pueden completar ni seleccionar los discos para las operaciones de destellar o dejar de destellar.

- **Causa**: el servicio Redfish no está habilitado.

  Resolución: habilite el servicio Redfish a través de la interfaz de usuario de la iDRAC. Para obtener más información, consulte la documentación de la iDRAC que se encuentra en el sitio de soporte de Dell EMC.

- **Causa**: después de que se haya cargado el inventario de hardware en OMIMSWAC, si se elimina el disco físico, las operaciones de destellar y dejar de destellar fallan con el error: `Blink may not be supported with <Disk_Name>.`

  Resolución: inserte el disco físico y haga clic en **Actualizar** para volver a cargar la información del inventario en OMIMSWAC; posteriormente, vuelva a ejecutar las operaciones de destellar y dejar de destellar.

- **Causa**: si la versión de firmware de la iDRAC es anterior a 3.30.30.30, los discos físicos no se pueden seleccionar para hacer destellar ni dejar de destellar.

  Resolución: actualice el firmware de la iDRAC a la versión más reciente, y vuelva a intentar las operaciones de destellar y dejar de destellar.

- Las operaciones de destellar y dejar de destellar fallan si un disco físico está conectado a una controladora de SATA integrada y el estado de la condición es `Desconocido`, lo que indicaría que el disco no es compatible con las operaciones de destellar o dejar de destellar.

El estado de la licencia es Desconocido o Sin licencia

Si el estado de la licencia es `Desconocido` o `Sin licencia`, asegúrese de los siguientes aspectos:

- La licencia no está vencida.
- Las licencias están presentes en cada nodo de destino.
- El nodo de destino no se encuentra en el estado de reinicio y está encendido.
- Redfish está habilitado.
- Las licencias de Azure Stack HCI o del servidor PowerEdge se importaron al hardware correspondiente. No se admite la importación de una licencia de Azure Stack HCI a un servidor PowerEdge ni de una licencia de servidor PowerEdge a un servidor de Azure Stack HCI.

Si el problema persiste:

1. Vaya a la iDRAC.
2. Asegúrese de que Redfish esté habilitado.
3. Deshabilite el paso de sistema operativo a iDRAC y, a continuación, habilítelo.

   Para obtener más información acerca de cómo habilitar o deshabilitar el paso de sistema operativo a iDRAC, consulte la guía del usuario de la iDRAC.

Disponibilidad de los registros de licencias

Los registros relacionados con la licencia están disponibles en la siguiente ruta y se pueden encontrar si busca *DellLicenseCollection* en el archivo *Limpieza*.

- Sistema de gateway: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\CleanupXXXXXXXXXXXXXX.log`
- Sistema de gateway de Windows 10: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\CleanupXXXXXXXXXXXXXX.log`

El trabajo falló al descargar los componentes necesarios para las operaciones de actualización del servidor y compatible en clústeres.

Causa: durante la exportación del repositorio mediante Dell EMC Repository Manager (DRM), el trabajo de exportación puede completarse con el estado “Parcialmente correcto”. En este caso, es posible que falte uno o varios DUP del repositorio.

Resolución: vuelva a intentar exportar el repositorio en DRM y asegúrese de que el trabajo se ha completado correctamente.

Causa: es posible que uno o varios componentes no se hayan descargado cuando la fuente de actualización se ha seleccionado como una fuente en línea.

Resolución: asegúrese de que haya conexión a Internet y vuelva a intentar descargar el catálogo desde la fuente en línea. Para obtener más información, consulte la guía del usuario de Dell EMC Repository Manager.

CredSSP falló durante la actualización

- **Causa**: durante la actualización de un clúster, la delegación de credenciales mediante CredSSP puede tener errores.

  Resolución: vuelva a conectar el clúster a través del nombre de dominio completamente calificado y haga clic en la casilla de verificación **Utilizar esta credencial para todos los servidores**.

  Por ejemplo, si el nombre de dominio es test.dev.com, use **`test.dev.com\administrator`** como el nombre de dominio y, a continuación, haga clic en la casilla de verificación **Utilizar esta credencial para todos los servidores**.

- **Causa**: si se utiliza la autenticación de CredSSP para ejecutar scripts en una máquina remota, el trabajo de actualización puede fallar con un error.

  El problema se debe a que CredSSP se deshabilitó en la máquina del gateway.

  Resolución: para resolver el problema, siga los pasos que se indican a continuación:

  1. En la ventana de PowerShell, ejecute `gpedit`

2. En la ventana Editor de políticas de grupo, **Configuraciones de la computadora** > **Plantillas administrativas** > **Sistema** > **Delegación de credenciales**
3. Seleccione **Permitir la delegación de credenciales nuevas con autenticación de servidor de solo NTLM** y habilítela.
4. Ejecute `gpupdate/force` en PowerShell.

El trabajo falló al generar el informe de cumplimiento

Causa: cuando se conecta a un nodo o clúster de destino mediante Inicio de sesión único en vez de "Administrar como" y genera un informe de cumplimiento a través de OMIMSWAC, la generación de cumplimiento puede fallar.

Resolución: antes de conectarse al nodo o clúster de destino, asegúrese de seleccionar "Administrar como" y proporcionar las cuentas del administrador de servidores o administrador de clústeres correspondientes.

Causa: cuando se genera un informe de cumplimiento, este proceso puede fallar con el siguiente error en el registro:

```
Starting a command on the remote server failed with the following error message : The
WinRM client sent a request to the remote WS-Management service and was notified that the
request size exceeded the configured MaxEnvelopeSize quota. For more information, see the
about_Remote_Troubleshooting Help topic.
```

Resolución: asegúrese de que:

- La conectividad de red entre el sistema de gateway y el nodo de destino está intacta.
- La copia de archivos funciona entre el sistema de gateway y el nodo de destino. Para comprobarlo:
  1. Cree una sesión basada en la credencial del nodo de destino mediante la ejecución del siguiente comando de PowerShell:

     ```
     $SecurePassword = convertto-securestring <password> -asplaintext -force

     $credential = New-Object System.Management.Automation.PSCredential -ArgumentList <userid>,
     $SecurePassword

     $session = New-PSSession -ComputerName <MN FQDN> -Credential $credential -ErrorAction
     SilentlyContinue
     ```

  2. Copie un archivo de prueba en el nodo de destino fallido suponiendo que "Test.txt" se encuentra en la unidad C:\

     ```
     Copy-Item -Path "C:\Test.txt" -Destination "C:\" -Recurse -Force -ToSession $session
     ```

- Si el problema persiste después de realizar las acciones anteriores, intente reiniciar el servicio Windows Remote Management (WS-Management) en el nodo de destino (la copia de archivo presenta fallas) y, a continuación, vuelva a ejecutar el cumplimiento.

Causa: cuando se genera un informe de cumplimiento de un clúster, es posible que este proceso falle en los nodos del clúster.

Resolución: asegúrese de que:

- El servicio de clúster se debe estar ejecutando en el nodo del clúster mediante el comando de PowerShell `Get-ClusterService`.
- El nodo de clúster no debe estar apagado ni reiniciándose.
- Cuando agregue un clúster a Windows Admin Center, asegúrese de utilizar el nombre de clúster en formato FQDN.

Causa: cuando se genera un informe de cumplimiento mediante el navegador Microsoft Edge de Windows 10, este proceso puede fallar con el siguiente error: `Unable to generate compliance report. The Manage As credentials have not been set or are not in domain\user format.`

Resolución: realice cualquiera de las siguientes acciones:

- Conecte el nodo de destino con las credenciales utilizando el nombre de dominio completamente calificado (por ejemplo, **`dominio.lab\nombre de usuario`**) o el dominio de nivel superior (por ejemplo, **`dominio\nombre de usuario`**).
- Borre la memoria caché del navegador y vuelva a ejecutar el cumplimiento.
- Asegúrese de que la DNS esté configurada correctamente en el sistema instalado de WAC para conectarse al nodo de destino con las credenciales adecuadas.

El trabajo falló al actualizar los componentes seleccionados.

En ocasiones, la actualización CAU o de los nodos de destino puede fallar. Las causas y las soluciones se indican a continuación:

- En el caso de CAU, valide el clúster antes de activar la actualización compatible con clústeres. Para obtener más información acerca de la validación de un clúster, consulte el documento de Microsoft Validar el hardware de un clúster.
- **Causa**: el archivo de inventario de cumplimiento no está disponible para algunos nodos, o bien no se pueden copiar archivos del nodo al gateway después de haber generado el cumplimiento.

  Resolución: vuelva a ejecutar el cumplimiento.

- **Causa**: debido a un problema de conexión a Internet, pueden fallar los siguientes elementos:
  - Verificación de firma de DSU o IC
  - Descarga del catálogo en línea
  - Descarga de DUP

  Si alguno de los elementos anteriores falla, la actualización CAU o del servidor también fallará.

  Resolución: asegúrese de tener conexión a Internet, y vuelva a ejecutar el cumplimiento y la actualización.

- **Causa**: el instalador de DSU no se borra de un nodo, ya que, en ocasiones, el proceso de Windows Admin Center (sme.exe) bloquea el archivo del instalador.

  Solución: reinicie el servicio Windows Admin Center desde las consolas de los servicios de Windows.

- **Causa**: la CAU falla si alguno de los discos no está en buen estado.

  Resolución: asegúrese de que los discos físicos y virtuales estén en buen estado antes de activar la CAU. Si algún disco se encuentra en un estado no óptimo, consulte el documento de Microsoft para dejarlo en un estado correcto.

- **Causa**: la CAU falla si cualquiera de los nodos de clúster está en pausa.

  Resolución: reanude los nodos del clúster (funciones de conmutación por error) antes de activar la CAU.

Componente que muestra no cumplimiento después de la actualización

Después de la actualización, es posible que algunos componentes muestren que no cumplen.

Resolución: en este caso, compruebe los registros de limpieza; haga que los registros de DSU verifiquen si el componente tiene algún ERROR. Si el componente necesita algún requisito previo antes de la actualización, cumpla ese requisito y, a continuación, vuelva a ejecutar la actualización.

Acceso denegado a OpenManage Integration

Causa: cuando inicia sesión en Windows Admin Center (WAC) con las credenciales de usuario del gateway sin privilegios de administrador, e intenta iniciar OpenManage Integration desde la consola de WAC, puede aparecer un error de acceso denegado.

Resolución: antes de iniciar la extensión Dell EMC OpenManage Integration en Windows Admin Center, debe iniciar sesión en WAC como administrador del gateway.

Fallas de Dell Update Package (DUP)

Es posible que Dell EMC Update Package (DUP) no pueda actualizar los componentes después de haber activado una actualización. Hay varias razones por las que falla el DUP durante la actualización. Observe las siguientes soluciones posibles para resolver el problema:

- En la máquina instalada de Windows Admin Center (WAC), revise los archivos de registro para obtener más información sobre la falla de descarga del DUP y la asignación de componentes. La asignación de componentes se proporciona con el propósito de identificar el componente (seleccionado para actualizar) en el catálogo de DUP. Los archivos de registro se encuentran en la siguiente ruta.

  Sistema de gateway:

  - Actualización de servidor: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\<PrepareUpdate XXXX>`
  - CAU: `<Windows Directory>\ServiceProfiles\NetworkService\AppData\Local\Temp\generated\logs\Update XXXX`

  Sistema de gateway de Windows 10:

- Actualización de servidor: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\<PrepareUpdate XXXX>`
- CAU: `<Windows installed drive>\Users\<user_name>\AppData\Local\Temp\generated\logs\Update XXXX`

- A continuación, se muestran mensajes de registro de ejemplo:
  - Registro de error de falla descarga del DUP

    ```
    28-Apr-2020 12:19:18 AM::: Error >>> Message : DUPs for some of the selected components are not present in DRM repository.
    ```

  - Archivo de registro de asignación de componentes

    ```
    ## Format: :>> Component Name -> Package Name

    :>> [0001] Broadcom NetXtreme Gigabit Ethernet -> Network_Firmware_RG25N_WN64_21.60.2_01.EXE
    ```

- En el nodo de destino, consulte la asignación de componentes y busque el archivo de registro de DUP relacionado con los componentes; a continuación, compruebe el código de retorno especificado en `<Directorio de Windows>\Dell\UpdatePackage\log\<Package Name>`. Consulte la guía del usuario de Dell EMC Update Package para obtener la causa y la posible resolución.

  A continuación, se muestra un ejemplo de código de retorno de una situación de falla de DUP:

  ```
  Exit code = 1 (Failure)

  2020-04-21 23:48:27

  Update Package finished. Exit code = 1
  ```

- El DUP puede fallar cuando se intenta degradar un componente del controlador a una versión inferior. En este caso, desinstale el controlador del sistema operativo y, a continuación, vuelva a ejecutar la actualización del componente desde OMIMSWAC. Para obtener más información acerca de cómo desinstalar controladores, consulte el documento de Microsoft.

Como alternativa, también puede intentar las siguientes acciones:

- Restablezca y actualice la iDRAC a la versión 4.20.20.20 o superior y, a continuación, vuelva a ejecutar la actualización. Para obtener más información sobre cómo restablecer o actualizar la iDRAC, consulte la documentación de la iDRAC.
- Ejecute la actualización manualmente en el nodo de destino, mediante la descarga desde la ruta especificada en `<Directorio de Windows>\Dell\UpdatePackage\log\<Package Name>` en el registro de DUP. Un ejemplo de firmware de red es https://downloads.dell.com/FOLDER06091050M/1/Network_Firmware_TWFF6_WN64_16.26.60.00.EXE.
- Asegúrese de que el DUP seleccionado sea compatible con el sistema operativo y la plataforma seleccionados, para lo cual debe buscar el nombre del componente en el sitio de soporte de Dell. URL del sitio de soporte de Dell: https://www.dell.com/support/home/in/en/inbsd1/?app=products.

Falla del clúster de prueba con errores de comunicación de red

Causa: cuando tiene la NIC USB habilitada en la iDRAC, si ejecuta el comando Probar clúster para verificar la preparación de la creación del clúster o el estado del clúster, es posible que vea un error en el informe de validación. El error indica que las direcciones IPv4 asignadas a la NIC USB del sistema operativo del host no se pueden usar para comunicarse con las otras redes de clúster. Este error se puede ignorar de forma segura.

Resolución: deshabilite la NIC USB (etiquetada como Ethernet de forma predeterminada) antes de ejecutar el comando Probar clúster.

La red de la NIC USB se muestra como red de clúster particionada

Causa: cuando la NIC USB está habilitada en la iDRAC, las redes de clúster en el administrador de clústeres de conmutación por error muestran aquellas que están asociadas con la NIC USB como particionadas. Este problema se produce debido a que la comunicación del clúster está habilitada de forma predeterminada en todos los adaptadores de red y las direcciones IPv4 de NIC USB no se pueden utilizar para comunicarse externamente, por lo tanto, interrumpen la comunicación del clúster en esas NIC. Este error se puede ignorar de forma segura.

Resolución: deshabilite la comunicación del clúster con las redes asociadas con las NIC USB desde el administrador de clústeres.

9

Identificación de la generación del servidor Dell EMC PowerEdge

Para cubrir una variedad de modelos de servidores, ahora se hace referencia a los servidores PowerEdge mediante la convención de nomenclatura genérica y no mediante su generación.

En este tema se explica cómo identificar la generación de un servidor PowerEdge al que se hace referencia utilizando la convención de nomenclatura genérica.

Ejemplo:

El modelo del servidor R740 es un sistema de rack que cuenta con dos procesadores de la 14.ª generación de servidores con procesadores Intel. En la documentación de, para referirse a R740, se utiliza el servidor **YX4X** con la convención de nomenclatura genérica y estas siglas hacen referencia a lo siguiente:

- La letra **Y** (alfabeto) indica el tipo (factor de forma: nube [C], flexible [F], modular [M o MX], rack [R], torre [T]) del servidor.
- La letra **X** (dígito) señala la clase (número de procesadores) del servidor.
- El dígito **4** indica la generación del servidor.
- La letra **X** (dígito) señala la marca del procesador.

Tabla 3. Convención de nomenclatura de servidores PowerEdge junto con ejemplos

Servidores YX5X	Servidores YX4X	Servidores YX3X
PowerEdge R7515	PowerEdge M640	PowerEdge M630
PowerEdge R6515	PowerEdge R440	PowerEdge M830
	PowerEdge R540	PowerEdge T130

10

Cómo ponerse en contacto con Dell EMC

Dell EMC proporciona varias opciones de servicio y asistencia en línea y por teléfono. La disponibilidad varía según el país y el producto y es posible que algunos de los servicios no estén disponibles en su área.

NOTA: Si no dispone de una conexión a Internet activa, puede encontrar información de contacto en la factura de compra, en el albarán o en el catálogo de productos de Dell EMC.

Si desea ponerse en contacto con Dell EMC para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio de atención al cliente:

1. Vaya a Dell.com/support.
2. Seleccione su país o región de preferencia en la lista que se encuentra en la parte inferior derecha de la página.
3. Haga clic en **Comuníquese con nosotros** y seleccione el enlace de soporte correspondiente.

A

Glosario

En la siguiente tabla se definen o identifican abreviaturas y siglas que se utilizan en esta guía.

Tabla 4. Glosario

Abreviaturas/Siglas	Definición
OMIMSWAC: OpenManage Integration with Microsoft Windows Admin Center	Dell EMC OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) permite a los administradores de TI gestionar servidores PowerEdge como hosts, clústeres de conmutación por error Microsoft creados con servidores PowerEdge e infraestructura hiperconvergente (HCI) creada utilizando las soluciones Dell EMC para Microsoft Azure Stack HCI. OMIMSWAC simplifica las tareas de los administradores de TI mediante la gestión remota de los servidores PowerEdge y los clústeres durante todo su ciclo de vida.
BIOS	Sistema básico de entrada y salida. El BIOS es un firmware que está incorporado en un chip de memoria pequeño en la tarjeta madre o la placa base de la computadora. Funciona como una interfaz entre el hardware y el sistema operativo del equipo. El BIOS también contiene las instrucciones que la computadora utiliza para realizar instrucciones básicas, como si se debe iniciar desde la unidad de disco duro o de la red
Consola	La aplicación de administración que utiliza un usuario para realizar tareas de administración remota de la plataforma.
DRM: Dell EMC Repository Manager	Dell EMC Repository Manager (DRM) es una aplicación dentro de la cartera de Dell OpenManage que les permite a los administradores de TI administrar fácilmente las actualizaciones del sistema. Dell Repository Manager ofrece una interfaz de búsqueda que se utiliza para crear recopilaciones de software personalizadas conocidas como agrupaciones y repositorios de Dell Update Packages (DUP).
DSU: utilidad Dell EMC System Update	Dell EMC System Update (DSU) es una herramienta de implementación de actualizaciones optimizada para script que permite aplicar Dell Update Packages (DUP) a los nodos de destino de Dell EMC.
FQDN	Nombre de dominio completamente calificado.
Administradores de gateway	Los administradores de gateway pueden configurar quién obtiene acceso y también la forma en que los usuarios se autentican en el gateway. Solo los administradores de gateway pueden ver y ajustar la configuración de acceso en Windows Admin Center. Los administradores locales de la máquina del gateway son siempre administradores del servicio de gateway de Windows Admin Center.
Sistema de gateway	Windows Admin Center instalado como un gateway en un servidor de Windows.
Usuario del gateway	Los usuarios de gateway pueden conectarse al servicio de gateway de Windows Admin Center para administrar servidores a través de ese gateway, pero no pueden cambiar los permisos de acceso ni el mecanismo de autenticación que se utiliza para autenticarse en el gateway.
Sistema de gateway de Windows 10	Windows Admin Center instalado como un gateway en un SO Windows 10.
HCI	Infraestructura hiperconvergente.
IC: Dell EMC Inventory Collector	Inventory Collector se utiliza para realizar un inventario del sistema objetivo, comparar los resultados con un repositorio o catálogo, e implementar únicamente las actualizaciones que se requieran.
iDRAC	Dell Remote Access Controller integrado.
IPMI	Interfaz de administración de plataforma inteligente

Tabla 4. Glosario (continuación)

Abreviaturas/Siglas	Definición
LED	Diodo emisor de luz
NIC	Tarjeta de interfaz de red, también conocida como controladora de interfaz de red
Offline: Catálogo de Dell EMC Repository Manager	Se recomienda cuando los repositorios DRM están disponibles en una ubicación compartida y se aplican a todos los dispositivos administrados por OMIMSWAC en centros de datos sin conexión a Internet.
En línea (HTTPS): catálogo de soluciones de Dell EMC Azure Stack HCI	Los catálogos de actualización de firmware y controladores de las soluciones Dell EMC para Azure Stack HCI conforman un catálogo de todas las versiones validadas de los componentes de Ready Node y AHCI. Recomendado para clústeres de Azure Stack HCI (creados con Dell EMC Microsoft Storage Spaces Direct Ready Nodes y Dell EMC Appliance para Azure Stack HCI) y los servidores de Azure Stack HCI.
En línea (HTTPS): catálogo de Dell EMC Enterprise	Recomendado para servidores PowerEdge.
En línea (HTTPS): catálogo de soluciones de Dell EMC MX	Se recomienda para los modelos MX de los servidores PowerEdge.
SATA	Interfaz de conexión en serie de tecnología avanzada que está destinada a reemplazar la anticuada tecnología **PATA**.
USB	Bus universal en serie
UI	Interfaz de usuario
<Directorio de Windows>	C:\Windows

B

Apéndice

SAS-RAID_Driver

Mientras se realiza la operación de cumplimiento de la actualización para SAS RAID_Driver, asegúrese de que la *controladora SATA* y los *SSD PCIe NVMe* estén configurados en modo RAID. Para configurar el Modo RAID:

1. Cuando aparezca la ventana **Prueba automática de encendido (POST) de Dell**, presione F2.

   Se muestra la ventana **Configuración del sistema Dell PowerEdge**.

   - En **Configuración del BIOS del sistema**, configure el modo RAID en **Configuración SATA** > **SATA incorporada**.
   - En **Configuración del BIOS del sistema**, configure el modo RAID en **Configuración NVMe** > **Modo NVMe**.

Catálogo recomendado para los nodos o clústeres de destino

En la siguiente tabla, se muestra el catálogo recomendado para un nodo o clúster de destino en “Fuente de actualización”.

Clústeres o nodos de destino	Catálogo recomendado
Servidor PowerEdge (rack, modular y torre)	En línea (HTTPS): catálogo de Dell EMC Enterprise (para servidores PowerEdge)
Servidor MX	En línea (HTTPS): catálogo de soluciones de Dell EMC MX (para servidores PowerEdge)
Nodos Ready para clúster AHCI (dispositivo S2D o AX)	En línea (HTTPS): catálogo de soluciones de Dell EMC Azure Stack HCI
Clúster que contiene MX y servidor PowerEdge	En línea (HTTPS): catálogo de Dell EMC Enterprise (para servidores PowerEdge)
Clúster que contiene nodos Ready de AHCI y servidor PowerEdge	En línea (HTTPS): catálogo de Dell EMC Enterprise (para servidores PowerEdge)
Clúster que contiene PowerEdge, MX y servidor AHCI con nodos Ready	En línea (HTTPS): catálogo de Dell EMC Enterprise (para servidores PowerEdge)
Servidor o clúster Edge PowerEdge XE2420	En línea (HTTPS): catálogo de Dell EMC Enterprise (para servidores PowerEdge)