Acronis

PRODUCTO #7 ADVANCED MANAGEMENT

Acceso a vulnerabilidades y gestión de parches

La **evaluación de vulnerabilidades** es un proceso que consiste en identificar, cuantificar y priorizar las vulnerabilidades encontradas en el sistema. Con el módulo de evaluación de vulnerabilidades, podrá analizar los equipos en busca de vulnerabilidades y asegurarse de que todos los sistemas operativos y las aplicaciones instaladas estén actualizados y funcionen correctamente.

El análisis de evaluación de vulnerabilidades es compatible con equipos con los siguientes sistemas operativos:

- Windows. Para obtener más información, consulte "Productos de Microsoft y de terceros compatibles" (p. 1065).
- macOS. Para obtener más información, consulte "Productos de Apple y de terceros compatibles" (p. 1066).
- Equipos Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Para obtener más información, consulte "Productos de Linux compatibles" (p. 1067).

Utilice la función de **gestión de parches** para gestionar los parches (actualizaciones) de las aplicaciones y los sistemas operativos instalados en sus equipos y mantener actualizados sus sistemas. Con el módulo de gestión de parches, podrá aprobar manual o automáticamente la instalación de actualizaciones en sus equipos.

La gestión de parches es compatible con equipos con sistemas operativos Windows. Para obtener más información, consulte "Productos de Microsoft y de terceros compatibles" (p. 1065).

Evaluación de vulnerabilidades

El proceso de evaluación de vulnerabilidades está formado por los siguientes pasos:

1. Cree un plan de protección con el módulo de evaluación de vulnerabilidades habilitado, especifique los ajustes de la evaluación de vulnerabilidades y asigne el plan a los equipos.
2. El sistema, si está planificado o se le pide, envía un comando para que se ejecute la evaluación de vulnerabilidades en los agentes de protección instalados en los equipos.
3. Los agentes reciben el comando, empiezan analizar equipos en busca de vulnerabilidades y generan la actividad de análisis.
4. Cuando haya terminado la evaluación de vulnerabilidades, los agentes generan los resultados y los envían al servicio de supervisión.
5. El servicio de supervisión procesa los datos de los agentes y muestra los resultados en los widgets de evaluación de vulnerabilidades y en la lista de vulnerabilidades encontradas.
6. Cuando tenga una lista de vulnerabilidades encontradas, podrá procesarla y decidir cuáles se deben solucionar.

Puede comprobar los resultados del análisis de la evaluación de vulnerabilidades en los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

Productos de Microsoft y de terceros compatibles

Los siguientes productos de Microsoft y de terceros para sistemas operativos Windows son compatibles con la evaluación de vulnerabilidades y la administración de parches:

Productos de Microsoft compatibles

Sistema operativo Windows

- Windows 7 (Enterprise, Professional y Ultimate)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Sistema operativo Windows Server

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office y componentes relacionados

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Componentes relacionados con el sistema operativo Windows

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio y aplicaciones
- Componentes del sistema operativo

Aplicaciones del servidor

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

Productos de terceros compatibles con Windows

El trabajo remoto se extiende cada vez más por el mundo, por lo que es importante que los clientes VPN y las herramientas de colaboración y comunicación estén siempre actualizados, así como que se analicen en busca de posibles vulnerabilidades. El servicio Cyber Protection permite realizar evaluación de vulnerabilidades y gestión de parches para tales aplicaciones.

Herramientas de colaboración y comunicación, clientes VPN

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

Para obtener más información sobre los productos de terceros compatibles para Windows, consulte Lista de productos de terceros compatibles con gestión de parches (62853).

Productos de Apple y de terceros compatibles

Los siguientes productos de Apple y de terceros para macOS son compatibles con la evaluación de vulnerabilidades:

Productos de Apple compatibles

macOS

- macOS 10.13.x y posterior

Aplicaciones integradas de macOS

- Safari, iTunes y otros.

Productos de terceros compatibles para macOS

- Microsoft Office (Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC media player

Productos de Linux compatibles

Distribuciones Linux y versiones de este sistema operativo que son compatibles con la evaluación de vulnerabilidades:

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

Configuración de la evaluación de vulnerabilidades

Para obtener más información sobre cómo crear un plan de protección con el módulo de evaluación de vulnerabilidades, consulte "Creación de un plan de protección". El análisis de la evaluación de vulnerabilidades se puede llevar a cabo cuando esté planificado o cuando se desee (mediante la acción **Ejecutar ahora** de un plan de protección).

Puede especificar los ajustes siguientes en el módulo de evaluación de vulnerabilidades.

Qué analizar

Seleccione los productos de software que quiera analizar para detectar vulnerabilidades:

- Equipos Windows:
  - **Productos de Microsoft**
  - **Productos de terceros compatibles con Windows**: para obtener más información sobre los productos de terceros compatibles para Windows, consulte Lista de productos de terceros compatibles con gestión de parches (62853).

- Equipos macOS:
  - **Productos de Apple**
  - **Productos de terceros para macOS**
- Equipos Linux:
  - **Analizar paquetes de Linux**

Planificación

Defina la planificación que se deberá seguir para llevar a cabo el análisis de la evaluación de vulnerabilidades en los equipos seleccionados:

Campo	Descripción
Planificar la ejecución de tareas con los siguientes eventos	Esta configuración define cuándo se ejecutará la tarea. Los valores disponibles son los siguientes: • **Planificar por hora**: esta es la configuración predeterminada. La tarea se ejecutará según la hora especificada. • **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario inicie sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. • **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, la tarea se iniciará cuando cualquier usuario cierre sesión. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. **Nota** La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación. • **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.
Tipo de planificación	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Los valores disponibles son los siguientes: • **Mensual**: seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea. • **Diariamente**: esta es la configuración predeterminada. Seleccione los días de la semana en los que se ejecutará la tarea. • **Cada hora**: seleccione los días de la semana, el número de

Campo	Descripción
	repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.
Iniciar a las	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora** Seleccione la hora exacta a la que se ejecutará la tarea.
Ejecutar dentro de un intervalo de fechas	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Establezca un rango en el que la planificación configurada sea efectiva.
Especifique una cuenta de usuario cuyo inicio de sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario inicia sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario inicie sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico inicie sesión.
Especifique una cuenta de usuario que al cerrar sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario cierra sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario cierre sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico cierre sesión.
Condiciones de inicio	Defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea. Las condiciones de inicio para el análisis antimalware son similares a las de inicio del **Módulo de copia de seguridad** que se describen en "Condiciones de inicio". Puede definir las siguientes condiciones de inicio adicionales: • **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00. • **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo**

Campo	Descripción
	• **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows. • **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio. **Nota** En Linux, las condiciones de inicio no están admitidas.

Evaluación de vulnerabilidades para equipos Windows

Puede analizar equipos Windows y productos de terceros para Windows para buscar vulnerabilidades.

Pasos para configurar la evaluación de vulnerabilidades para equipos Windows

1. En la consola de Cyber Protect, cree un plan de protección y habilite el módulo **Evaluación de vulnerabilidades**.
2. Especifique la configuración de la evaluación de vulnerabilidades:
   - **Qué analizar**: seleccione **Productos de Microsoft**, **productos de terceros para Windows** o ambos.
   - **Planificación** : define la planificación para ejecutar la evaluación de vulnerabilidades.

   Para obtener más información sobre las opciones de **Planificación**, consulte "Configuración de la evaluación de vulnerabilidades" (p. 1067).
3. Asigne el plan a los equipos Windows.

Después de un análisis de evaluación de vulnerabilidades, verá una lista de vulnerabilidades halladas. Puede procesar la información y decidir cuáles de las vulnerabilidades halladas deben arreglarse.

Para comprobar los resultados de la evaluación de vulnerabilidades, consulte los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

Evaluación de vulnerabilidades para equipos Linux

Puede escanear equipos Linux en busca de vulnerabilidades a nivel de aplicación y núcleo.

Para configurar la evaluación de vulnerabilidades en equipos Linux

1. En la consola de Cyber Protect, cree un plan de protección y habilite el módulo **Evaluación de vulnerabilidades**.
2. Especifique la configuración de la evaluación de vulnerabilidades:

- **Qué analizar**: seleccione **Analizar paquetes de Linux**.
- **Planificación** : define la planificación para ejecutar la evaluación de vulnerabilidades.

  Para obtener más información sobre las opciones de **Planificación**, consulte "Configuración de la evaluación de vulnerabilidades" (p. 1067).

3. Asigne el plan a los equipos de Linux.

Después de un análisis de evaluación de vulnerabilidades, verá una lista de vulnerabilidades halladas. Puede procesar la información y decidir cuáles de las vulnerabilidades halladas deben arreglarse.

Para comprobar los resultados de la evaluación de vulnerabilidades, consulte los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

Evaluación de vulnerabilidades para dispositivos macOS

Puede analizar los dispositivos macOS para buscar vulnerabilidades a nivel del sistema operativo y de las aplicaciones.

Pasos para configurar la evaluación de vulnerabilidades para dispositivos macOS

1. En la consola de Cyber Protect, cree un plan de protección y habilite el módulo **Evaluación de vulnerabilidades**.
2. Especifique la configuración de la evaluación de vulnerabilidades:
   - **Qué analizar**: seleccione **Productos de Apple**, **productos de terceros para macOS** o ambos.
   - **Planificación** : define la planificación para ejecutar la evaluación de vulnerabilidades.

     Para obtener más información sobre las opciones de **Planificación**, consulte "Configuración de la evaluación de vulnerabilidades" (p. 1067).
3. Asigne el plan a los dispositivos de macOS.

Después de un análisis de evaluación de vulnerabilidades, verá una lista de vulnerabilidades halladas. Puede procesar la información y decidir cuáles de las vulnerabilidades halladas deben arreglarse.

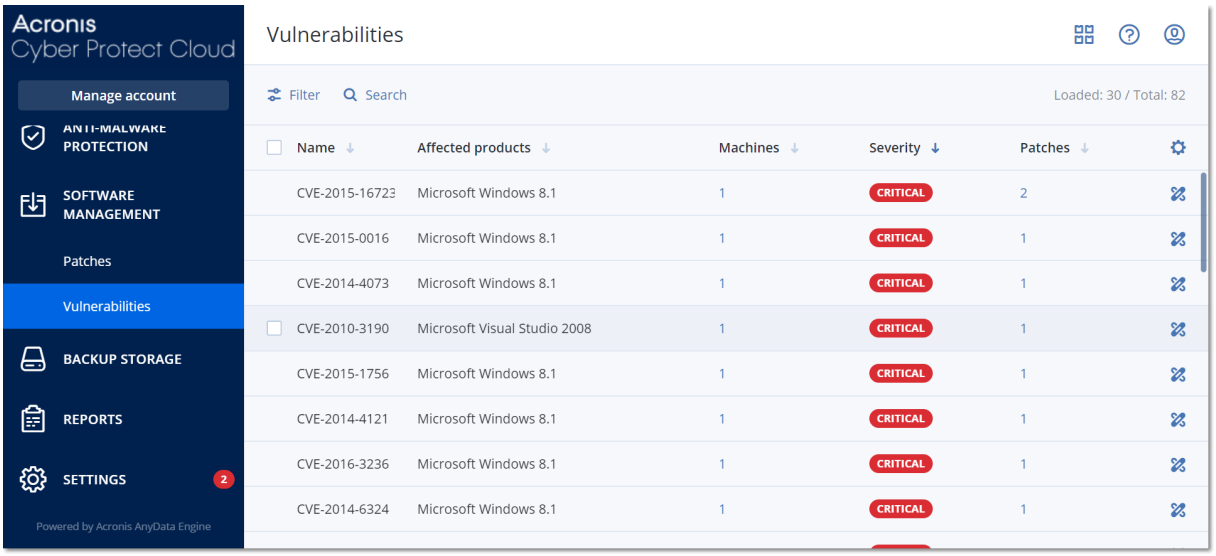
Para comprobar los resultados de la evaluación de vulnerabilidades, consulte los widgets de **Supervisión** > **Información general** > **Vulnerabilidades/Vulnerabilidades existentes**.

Gestión de vulnerabilidades encontradas

Si la evaluación de vulnerabilidades se ha llevado a cabo al menos una vez y se detecta alguna vulnerabilidad, las podrá encontrar en **Gestión del software** > **Vulnerabilidades**. En la lista de vulnerabilidades se muestran tanto aquellas en las que hay que instalar parches como para las que no hay ningún parche sugerido. Puede usar el filtro para mostrar únicamente las vulnerabilidades con parches.

Nombre	Descripción
Nombre	Nombre de la vulnerabilidad.
Productos afectados	Productos de software en los que se han encontrado vulnerabilidades.
Equipos	Número de equipos afectados.
Gravedad	La gravedad de la vulnerabilidad encontrada. Se pueden asignar los siguientes niveles según el sistema Common Vulnerability Scoring System (CVSS): • **Crítico**: 9-10 CVSS • **Alto**: 7-9 CVSS • **Medio**: 3-7 CVSS • **Bajo**: 0-3 CVSS • **Ninguno**
Parches	Número de parches adecuado.
Fecha de publicación	La fecha y la hora en las que se publicó la vulnerabilidad en Vulnerabilidades y exposiciones comunes (CVE).
Fecha de la detección	Fecha en la que se detectó por primera vez una vulnerabilidad existente en equipos.

Si hace clic en su nombre en la lista, encontrará la descripción de las vulnerabilidades encontradas.



Pasos para iniciar el proceso de resolución de vulnerabilidades

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Vulnerabilidades**.
2. Seleccione la vulnerabilidad en la lista y, a continuación, haga clic en **Instalar parches**. Se abrirá el asistente de solución de vulnerabilidades.
3. Seleccione los parches que se van a instalar en los equipos seleccionados y haga clic en **Siguiente**.

4. Seleccione los equipos en los cuales desea instalar los parches.
5. Seleccione las opciones de reinicio.
   a. Seleccione si quiere que el equipo se reinicie después de instalar los parches.

Opción	Descripción
No	Los equipos no se reiniciarán automáticamente después de instalar los parches.
Si es necesario	Los equipos se reiniciarán únicamente si es necesario para aplicar los parches.
Sí	Los equipos se reiniciarán automáticamente después de instalar los parches. También puede especificar cuándo tendrá lugar el reinicio.

   b. [Opcional] Si quiere programar el reinicio del equipo mientras se está realizando una copia de seguridad del equipo, seleccione **No reiniciar hasta que finalice la copia de seguridad**.
6. Haga clic en **Instalar parches**.

Como resultado, los parches seleccionados se instalan en los equipos indicados.

Gestión de parches

Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Para obtener más información sobre los productos de terceros compatibles para Windows, consulte Lista de productos de terceros compatibles con gestión de parches (62853).

Utilice la funcionalidad de gestión de parches para:

- instalar actualizaciones a nivel de aplicación y sistema operativo
- aprobar la instalación manual o automática de parches
- instalar parches cuando se desee o según una planificación
- definir de forma precisa qué parches instalar según distintos criterios: gravedad, categoría y estado de aprobación
- llevar a cabo copias de seguridad previas a las actualizaciones por si no se realizan correctamente
- definir la acción de reinicio después de la instalación de parches

Nota
Para trabajar con actualizaciones de Windows, la función de gestión de parches requiere que las actualizaciones de Windows estén habilitadas en la carga de trabajo.

Cyber Protection presenta tecnología de par a par con el fin de minimizar el tráfico del ancho de banda de red. Puede elegir uno o varios agentes dedicados que descargarán actualizaciones de Internet y las distribuirán ente otros agentes en la red. Además, todos los agentes compartirán actualizaciones con el resto como agentes del mismo nivel.

El flujo de trabajo de gestión de parches

El flujo de trabajo de gestión de parches incluye pasos para configurar y aplicar un plan de protección, ejecutar un análisis de evaluación de vulnerabilidades, configurar los ajustes de parches, aprobar parches y, por último, instalar los parches que se hayan aprobado. Los pasos exactos del flujo de trabajo son los siguientes.

1. Configure un plan de protección que tenga los módulos **Evaluación de vulnerabilidades** y **Gestión de parches** habilitados.
2. Configure los ajustes de la evaluación de vulnerabilidades. Para obtener más información sobre esta configuración, consulte "Configuración de la evaluación de vulnerabilidades" (p. 1067).
3. Configure los ajustes de la gestión de parches. Para obtener más información sobre esta configuración, consulte "Configuración de gestión de parches en el plan de protección" (p. 1074)
4. Aplique el plan de protección a uno o más equipos.
5. Espere a que se complete el análisis de evaluación de vulnerabilidades. El análisis comenzará automáticamente según la planificación configurada en el plan de protección. También puede iniciar el análisis bajo demanda manualmente haciendo clic en el icono **Ejecutar ahora** en el módulo **Evaluación de vulnerabilidades** del plan de protección.
6. Apruebe los parches. Puede definir la configuración de la aprobación automática de parches, que incluye la instalación automática de los parches en equipos de prueba. Para obtener más información, consulte "Aprobación automática de parches" (p. 1082). También puede aprobar los parches manualmente cambiando su estado de aprobación a **Aprobado**. Para obtener más información, consulte "Aprobar parches manualmente" (p. 1087).
7. Instale los parches. Los parches aprobados se pueden instalar automáticamente según la planificación configurada en el plan de protección. También puede instalar parches bajo demanda manualmente. Para obtener más información, consulte "Instalar parches bajo demanda" (p. 1087).

Puede revisar los resultados de la instalación de parches en el widget **Supervisión** > **Información general** > **Historial de instalación de parches**.

Configuración de gestión de parches en el plan de protección

En el módulo **Gestión de parches** del plan de protección, puede configurar los siguientes ajustes de gestión de parches:

- Qué actualizaciones se deben instalar para productos de Microsoft y terceros en sistemas operativos de Windows.

- Cuándo ejecutar la instalación automática de parches.
- Si se debe ejecutar una copia de seguridad antes de la actualización.

Para obtener más información sobre cómo crear un plan de protección y habilitar el módulo **Gestión de parches**, consulte "Creación de un plan de protección" (p. 230).

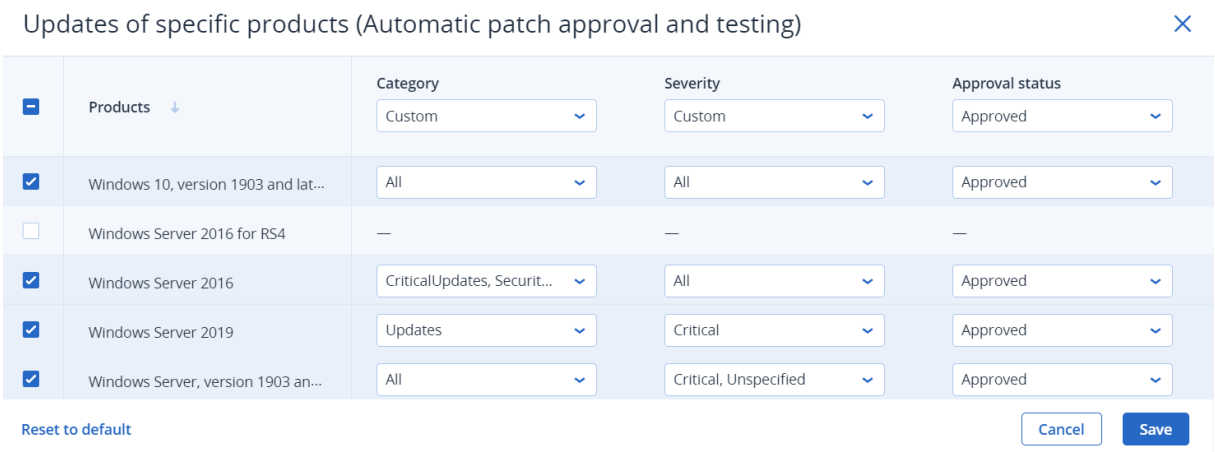
Nota
La disponibilidad de esta característica depende de las cuotas de servicio habilitadas para su cuenta.

Productos de Microsoft

Para instalar las actualizaciones de Microsoft en los equipos seleccionados, habilite la opción **Actualizar productos de Microsoft**.

Seleccione la opción de instalación:

Opción	Descripción
Todas las actualizaciones	Utilice esta opción si desea instalar todas las actualizaciones aprobadas.
Solo actualizaciones de seguridad y críticas	Utilice esta opción si desea instalar todas las actualizaciones críticas y de seguridad aprobadas.
Actualizaciones de productos específicos (aprobación y comprobación automática de parches)	Utilice esta opción si desea definir ajustes personalizados para diferentes productos. Si desea actualizar productos específicos, para cada producto puede definir qué actualizaciones instalar por categoría, gravedad o estado de aprobación. Seleccione esta opción si desea configurar las pruebas y la aprobación automática de pruebas de los parches.



En el caso de los productos de Microsoft, la distribución de parches usar el servicio de la API de Windows. Los parches y las actualizaciones no se descargan ni se almacenan internamente ni en

agentes de distribución. Se descargan de Microsoft CDN. Por lo tanto, el agente no puede descargar ni distribuir parches aunque tenga asignado el rol de actualizador.

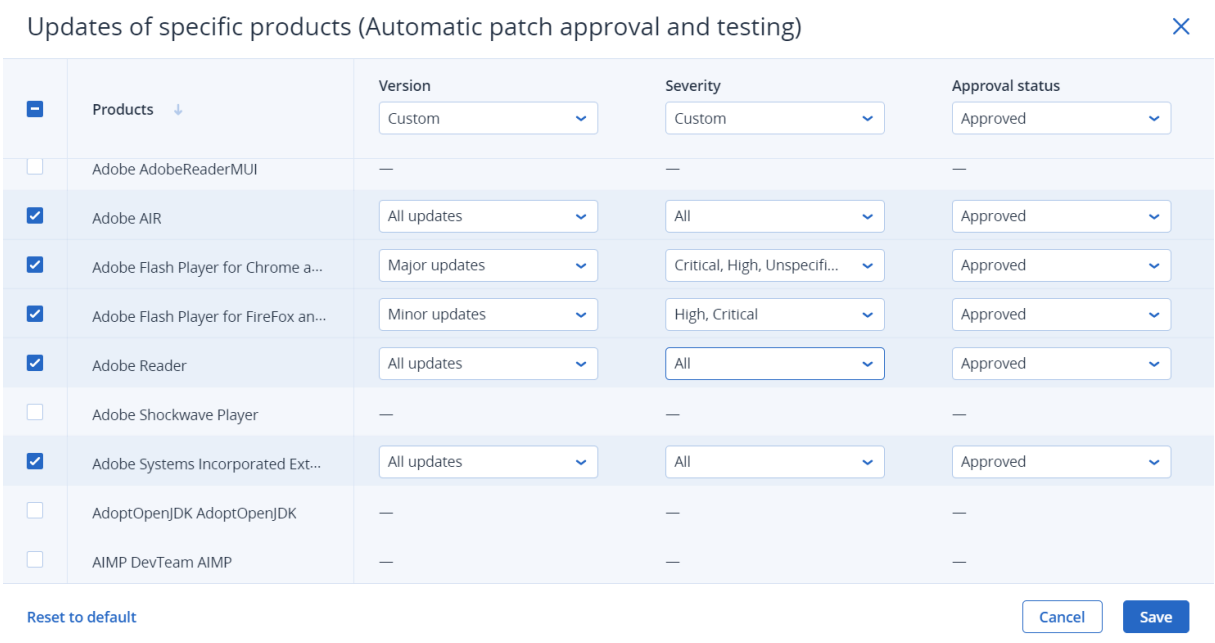
Productos de terceros a Windows

Para instalar las actualizaciones de terceros para Windows en los equipos seleccionados, habilite la opción **Productos de terceros para Windows**.

Seleccione las opciones de instalación:

Opción	Descripción
Todas las actualizaciones	Utilice esta opción si desea instalar todas las actualizaciones aprobadas. *
Solo actualizaciones importantes	Utilice esta opción si desea instalar todas las actualizaciones importantes aprobadas.
Solo actualizaciones menores	Utilice esta opción si desea instalar actualizaciones menores aprobadas.
Actualizaciones de productos específicos (aprobación y comprobación automática de parches)	Utilice esta opción si desea definir ajustes personalizados para diferentes productos. Si desea actualizar productos específicos, para cada producto puede definir qué actualizaciones instalar por categoría, gravedad o estado de aprobación. Seleccione esta opción si desea configurar las pruebas y la aprobación automática de pruebas de los parches.
Instale las últimas versiones solo para las aplicaciones con vulnerabilidades detectadas	Seleccione esta casilla de verificación si desea instalar las últimas actualizaciones solo para las aplicaciones en las que se hayan detectado vulnerabilidades. *

* Esta opción requiere la versión 23.11.36772 del agente Cyber Protect o posterior.



En el caso de los productos Windows de terceros, los parches de distribuyen directamente a las cargas de trabajo gestionadas desde una base de datos interna de Acronis. Si se asigna el rol de actualizador a un agente, este se utilizará para descargar y distribuir los parches.

Planificación

Defina la planificación y las condiciones que se seguirán para instalar las actualizaciones en los equipos seleccionados.

Campo	Descripción
Planificar la ejecución de tareas con los siguientes eventos	Esta configuración define cuándo se ejecutará la tarea. Los valores disponibles son los siguientes: • **Planificar por hora**: esta es la configuración predeterminada. La tarea se ejecutará según la hora especificada. • **Cuando el usuario inicia sesión en el sistema**: de forma predeterminada, el inicio de sesión de cualquier usuario iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. • **Cuando el usuario cierra sesión en el sistema**: de forma predeterminada, cuando cualquier usuario cierre sesión se iniciará la tarea. Puede modificar esta configuración para que únicamente una cuenta de usuario concreta pueda activar la tarea. **Nota** La tarea no se ejecutará al apagarse el sistema. Apagar y cerrar sesión son dos acciones diferentes de la configuración de la programación.

Campo	Descripción
	• **Al iniciarse el sistema**: la tarea se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la tarea se ejecutará cuando el sistema operativo se apague.
Tipo de planificación	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Los valores disponibles son los siguientes: • **Mensual**: seleccione los meses y las semanas o días del mes en los que se ejecutará la tarea. • **Diariamente**: esta es la configuración predeterminada. Seleccione los días de la semana en los que se ejecutará la tarea. • **Cada hora**: seleccione los días de la semana, el número de repeticiones y el intervalo de tiempo en los que se ejecutará la tarea.
Iniciar a las	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora** Seleccione la hora exacta a la que se ejecutará la tarea.
Configurar el periodo de mantenimiento para parches	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Seleccione esta configuración si desea que la instalación de parches se ejecute solo durante el intervalo de tiempo que especifique. Si no se completa el proceso de instalación de parches antes de la hora de finalización definida en el periodo de mantenimiento para parches, se detendrá automáticamente.
Ejecutar dentro de un intervalo de fechas	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Planificar por hora**. Establezca un rango en el que la planificación configurada sea efectiva.
Especifique una cuenta de usuario cuyo inicio de sesión en el sistema operativo iniciará una tarea	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario inicia sesión en el sistema**. Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario inicie sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico inicie sesión.
Especifique una cuenta de usuario que al cerrar sesión en el	El campo se muestra si, en **Planificar la ejecución de tareas con los siguientes eventos**, ha seleccionado **Cuando el usuario cierra sesión en el sistema**.

Campo	Descripción
sistema operativo iniciará una tarea	Los valores disponibles son los siguientes: • **Cualquier usuario**: utilice esta opción si quiere que se inicie la tarea cuando cualquier usuario cierre sesión. • **El siguiente usuario**: utilice esta opción si quiere que se inicie la tarea solo cuando un usuario específico cierre sesión.
Condiciones de inicio	Defina todas las condiciones que se deben cumplir de forma simultánea para que se ejecute la tarea. Las condiciones de inicio para el análisis antimalware son similares a las de inicio del **Módulo de copia de seguridad** que se describen en "Condiciones de inicio". Puede definir las siguientes condiciones de inicio adicionales: • **Distribuir las horas de inicio de la tarea en un período de tiempo**: esta opción le permite establecer el plazo de tiempo de la tarea para evitar cuellos de botella en la red. Puede especificar el retraso en horas o minutos. Por ejemplo, si la hora de inicio predeterminada son las 10:00 y el retraso es de 60 minutos, la tarea empezará entre las 10:00 y las 11:00. • **Si el equipo está apagado, ejecutar las tareas perdidas al iniciar el equipo** • **Evitar el modo de suspensión o hibernación durante la ejecución de una tarea**: esta opción solo se aplica en equipos que ejecuten Windows. • **Si no se cumplen las condiciones de inicio, ejecutar la tarea de todos modos después de**: especifique el periodo tras el que se ejecutará la tarea, sin importar el resto de las condiciones de inicio. **Nota** En Linux, las condiciones de inicio no están admitidas.
Reiniciar después de la actualización	Defina si reiniciar automáticamente el equipo una vez que se complete la instalación de las actualizaciones. Los valores disponibles son los siguientes: • **Nunca**: los equipos no se reiniciarán nunca después de las actualizaciones. • **Si es necesario**: el reinicio tendrá lugar únicamente si es necesario para aplicar las actualizaciones. • **Siempre**: siempre se reiniciará el equipo tras las actualizaciones. Puede especificar cuándo tendrá lugar el reinicio.
No reiniciar hasta que la copia de seguridad haya	Si selecciona esta opción, se retrasará el reinicio del equipo hasta que finalice la copia de seguridad en caso de que se esté ejecutando un proceso de copia de seguridad.

Campo	Descripción
finalizado	

Copia de seguridad anterior a la actualización

Realizar una copia de seguridad antes de instalar actualizaciones de software: el sistema creará una copia de seguridad incremental del equipo antes de instalar cualquier actualización en él. Si anteriormente no se había creado ninguna copia de seguridad, se creará una copia de seguridad completa del equipo. Con esta opción podrá evitar situaciones en las que la instalación de actualizaciones no se realice correctamente y tenga que volver al estado anterior. Para que la opción **Copia de seguridad anterior a la actualización** funcione, los equipos correspondientes deben tener el módulo de copias de seguridad y el de gestión de parches habilitados en un plan de protección, y contar con los elementos que se van a incluir en la copia de seguridad, ya sea todo el equipo o los volúmenes de inicio del sistema de arranque. Si selecciona elementos inapropiados para la copia de seguridad, el sistema no le permitirá habilitar la opción **Copia de seguridad anterior a la actualización**.

Ver la lista de parches disponibles

Cuando se completa una evaluación de vulnerabilidades, puede ver información sobre los parches disponibles en **Gestión del software** > **Parches**.

Para ver los detalles de un parche de específico, haga clic en él en la lista de parches.

En la siguiente tabla se describe la información del parche que puede ver en la pantalla.

Campo	Descripción
Estado de aprobación	El estado de aprobación se necesita principalmente para aquellas situaciones en las que las aprobaciones se realizan automáticamente. Puede para definir uno de los siguientes estados para un parche: • **Aprobado**: el parche se ha instalado al menos en un equipo y se ha validado correctamente. • **Rechazado**: el parche no es seguro y puede dañar el sistema de un equipo. • **Aprobación pendiente**: el estado del parche no está claro y hay que validarlo
Acuerdo de licencia	• Acepto • No acepto. Si no acepta el acuerdo de licencia, el estado del parche pasa a ser **Rechazado** y no se instalará.
Gravedad	Nivel de gravedad del parche: • **Crítico** • **Alto** • **Medio** • **Bajo**

	• **Ninguno**
Proveedor	Proveedor del parche.
Producto afectado	Producto en el que se puede aplicar el parche.
Versiones instaladas	Versiones del producto que ya están instaladas.
Versión	Versión del parche.
Categoría	Categoría a la que pertenece el parche: • **Actualización crítica**: correcciones de amplia distribución para tratar problemas específicos asociados a errores críticos no relacionados con aspectos de seguridad. • **Actualización de la seguridad**: revisiones de amplia distribución para tratar problemas específicos asociados a errores de seguridad. • **Actualización de la definición**: actualizaciones aplicadas a virus u otros archivos de definiciones. • **Paquete acumulativo de actualizaciones**: conjuntos acumulativos de revisiones, actualizaciones de seguridad, actualizaciones críticas y actualizaciones que se recopilan para facilitar su implementación. Un paquete acumulativo está orientado normalmente a un área específica, como la seguridad, o a un componente de un producto, como Servicios de Internet Information Server (IIS). • **Paquete de servicio**: conjuntos acumulativos de todas las revisiones, actualizaciones de seguridad, actualizaciones críticas y actualizaciones creadas desde el lanzamiento del producto. Los paquetes de servicios también pueden contener un número limitado de funciones o cambios de diseño solicitados por el cliente. • **Herramienta**: utilidades o funciones que ayudan a llevar a cabo una tarea o un conjunto de tareas. • **Paquete de funciones**: lanzamientos de nuevas funciones que se suelen incluir en la última versión de los productos. • **Actualización**: correcciones que se emplean muchísimo para tratar problemas específicos asociados a errores que no son críticos ni están relacionados con aspectos de seguridad. • **Aplicación**: parches para una aplicación.
Fecha de publicación	Fecha en la que se publicó el parche.
Notificado por última vez	La fecha de la última vez que se notificó el parche
Instalado por primera vez	La fecha de la primera instalación correcta del parche en un equipo
KB de Microsoft	Si el parche es para un producto de Microsoft, el campo muestra el ID del artículo

	de la Base de conocimientos
Equipos	Número de equipos afectados.
Vulnerabilidades	Número de vulnerabilidades. Si hace clic en esta opción, se le redirigirá a la lista de vulnerabilidades.
Tamaño	Tamaño medio del parche.
Idioma	Idioma que admite el parche.
Sitio del proveedor	Sitio oficial del proveedor.

Configurar el tiempo de los parches en la lista

Para mantener la lista de parches actualizada, configure el tiempo que permanece cada parche en la lista desde la pantalla **Parches**. Esta configuración define el tiempo durante el cual el parche disponible detectado se conservará en la lista de parches. Se eliminará el parche de la lista una vez que se haya instalado correctamente en todos los equipos en los que faltaba o cuando transcurra el tiempo en la lista indicado.

Pasos para configurar el tiempo de los parches en la lista

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Haga clic en **Configuración**.
3. En **Tiempo en la lista**, seleccione la opción adecuada.

Opción	Descripción
Siempre	El parche se mantiene siempre en la lista.
7 días	El parche se eliminará de la lista siete días después de su primera instalación. Por ejemplo, supongamos que tiene dos equipos en los que se deben instalar parches. Uno de ellos está en línea y el otro fuera de línea. El parche se ha instalado en el primer equipo. Cuando pasen siete días, el parche se eliminará, aunque no esté instalado en el segundo equipo porque estaba fuera de línea.
30 días	El parche se eliminará de la lista treinta días después de su primera instalación.

Aprobación automática de parches

Con la aprobación automática de parches, el proceso de instalación de actualizaciones en los equipos le resultará más sencillo. Esta función evita que la instalación de parches se retrase debido al proceso manual de aprobación de parches. Las actualizaciones y correcciones importantes se instalan con mayor rapidez, lo que aumenta la fiabilidad del sistema.

Puede usar la aprobación automática de parches en situaciones de prueba para instalar los parches automáticamente. Si los parches se instalan correctamente en los equipos de prueba, también lo

harán automáticamente en los equipos de producción. Para obtener más información sobre esta situación, consulte "Caso de uso de prueba y aprobación automática de parches" (p. 1083).

También puede usar la aprobación automática de parches para instalar los parches automáticamente en el entorno de producción y saltarse la fase de prueba. Para obtener más información sobre esta situación, consulte "Caso de uso de aprobación automática de parches sin prueba" (p. 1086).

Configuración de la aprobación automática de parches

Puede configurar la aprobación automática de parches para evitar que la instalación de parches se retrase debido al proceso manual de aprobación de parches.

Pasos para configurar la aprobación automática de parches

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Haga clic en **Configuración**.
3. Habilite la **Aprobación automática de parches**.
4. Establezca los ajustes de la aprobación automática de parches.
   a. Seleccione la opción de aprobación automática de parches.

Opción	Descripción
Prueba y aprobación automática de parches	El estado de aprobación del parche cambiará a **Aprobado** cuando transcurra el número especificado de días desde la instalación correcta del parche. Le recomendamos que utilice esta configuración si quiere instalar primero los parches en un equipo de prueba para asegurarse de que todo funciona correctamente y, a continuación, instalarlos en su entorno de producción.
Aprobación automática de parches sin prueba	El estado de aprobación del parche cambiará a **Aprobado** cuando transcurra el número especificado de días desde que se encontró el parche.

   b. Seleccione el número de días que deben transcurrir desde que se cumpla la condición de la opción de aprobación automática de parches. Después de este periodo, el estado de aprobación de los parches cambiará automáticamente de **Aprobación pendiente** a **Aprobado**.
5. Seleccione **Aceptar automáticamente los acuerdos de licencia**.
6. Haga clic en **Aplicar**.

Caso de uso de prueba y aprobación automática de parches

Si quiere probar los nuevos parches en un equipo de prueba antes de instalarlos en sus equipos de producción, puede configurar dos planes de protección, uno para la instalación de parches de prueba y otro para la instalación de parches ya probados en equipos de producción. De ese modo,

se asegurará de que los parches que instale en el entorno de producción sean seguros y de que los equipos de producción funcionen correctamente después de la instalación del parche.

El caso de uso consiste en los pasos siguientes:

1. Establezca los ajustes de la aprobación automática de parches. Seleccione la opción **Prueba y aprobación automática de parches**. Para obtener más información, consulte "Configuración de la aprobación automática de parches" (p. 1083).
2. Configure un plan de protección para pruebas (por ejemplo, "Instalación de parches en entornos de prueba") con el módulo **Gestión de parches** habilitado y aplíquelo a los equipos del entorno de prueba. Especifique la siguiente condición con respecto a la instalación de parches: el estado de aprobación del parche debe ser **Aprobación pendiente**. Este paso es necesario para validar los parches y comprobar si los equipos funcionan correctamente después de su instalación. Para obtener más información, consulte "Configurar el plan de protección Instalación de parches en entornos de prueba" (p. 1084).
3. Configure un plan de protección para el entorno de producción (por ejemplo, "Instalación de parches en entornos de producción") con el módulo **Gestión de parches** habilitado y aplíquelo a los equipos del entorno de producción. Especifique la siguiente condición con respecto a la instalación de parches: el estado del parche debe ser **Aprobado**. Para obtener más información, consulte "Configurar el plan de protección Instalación de parches en entornos de producción" (p. 1085).
4. Ejecute el plan Instalación de parches en entornos de prueba y compruebe los resultados. Deje el estado de aprobación de los equipos que no tienen ningún problema como **Aprobación pendiente** y cambie el de aquellos que no funcionan correctamente a **Rechazado**. Una vez transcurrido el número de días establecido en **Aprobación automática de parches**, el estado de aprobación de los parches cambiará automáticamente de **Aprobación pendiente** a **Aprobado**. Cuando ejecute el plan Instalación de parches en entornos de producción, solo se instalarán los parches con el estado **Aprobado** en los equipos de producción. Para obtener más información, consulte "Ejecutar el plan de protección Instalación de parches de prueba y rechazar parches no seguros" (p. 1086).
5. Ejecute el plan Instalación de parches en entornos de producción.

Configurar el plan de protección Instalación de parches en entornos de prueba

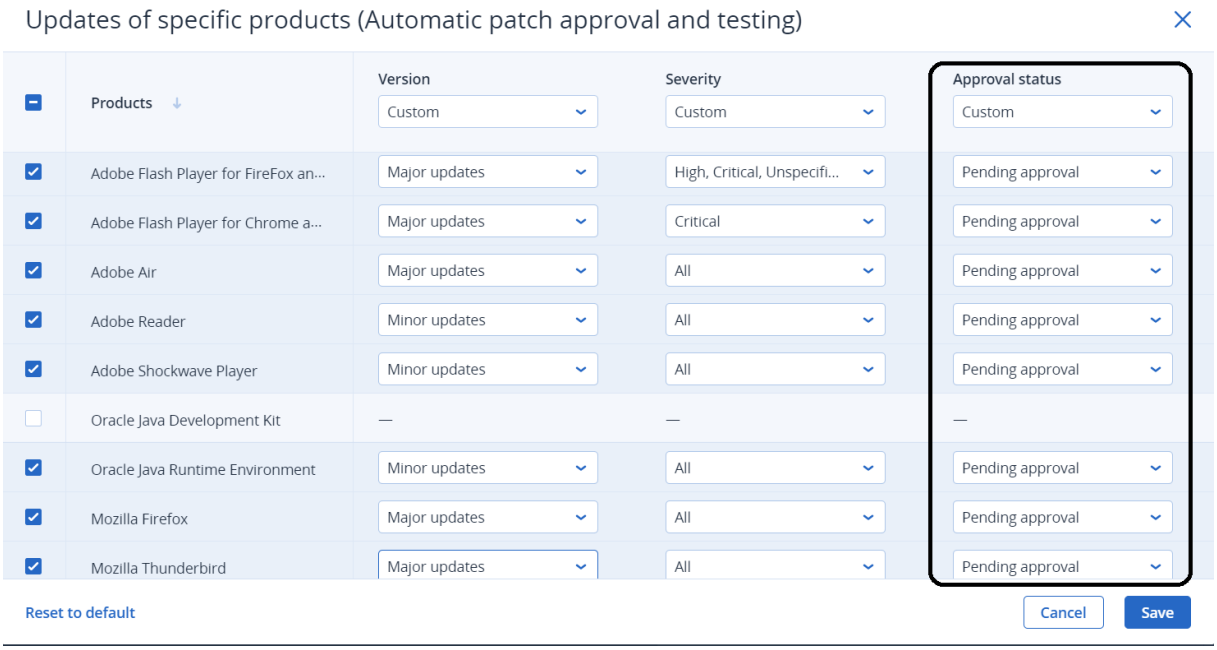
Puede configurar un plan de protección con ajustes de instalación de parches para sus equipos en el entorno de prueba.

Pasos para configurar el plan de protección Instalación de parches en entornos de prueba

1. En la consola de Cyber Protect, vaya a **Administración** > **Planes de protección**.
2. Haga clic en **Crear plan**.
3. Habilite el módulo **Gestión de parches**.
4. Defina qué actualizaciones desea instalar para productos de Microsoft y terceros, establezca una planificación y realice una copia de seguridad previa a la actualización. Para obtener más información sobre esta configuración, consulte "Configuración de gestión de parches en el plan

de protección" (p. 1074).

Importante
Seleccione el estado de aprobación **Aprobación pendiente** para todos aquellos productos que se vayan a actualizar. De ese modo, el agente instalará únicamente los parches cuyo estado sea **Aprobación pendiente** en los equipos seleccionados del entorno de prueba.



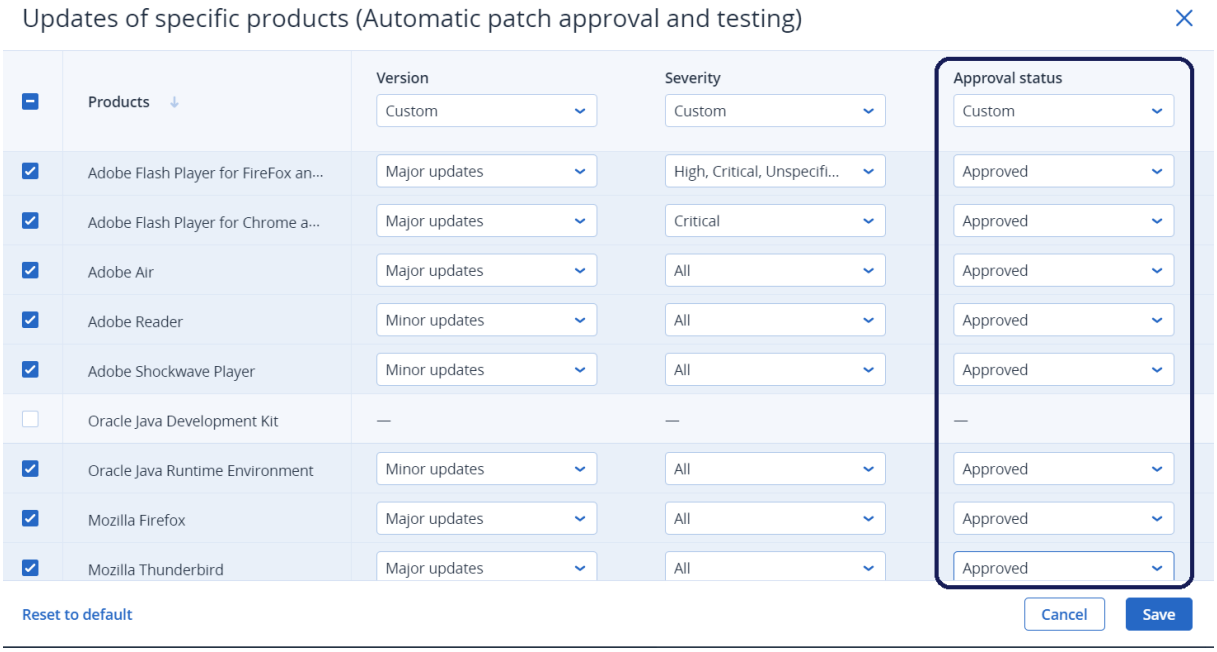
Configurar el plan de protección Instalación de parches en entornos de producción

Puede configurar un plan de protección con ajustes de instalación de parches para sus equipos en el entorno de producción.

Pasos para configurar el plan de protección Instalación de parches en entornos de producción

1. En la consola de Cyber Protect, vaya a **Administración** > **Planes de protección**.
2. Haga clic en **Crear plan**.
3. Habilite el módulo **Gestión de parches**.
4. Defina qué actualizaciones desea instalar para productos de Microsoft y terceros, establezca una planificación y realice una copia de seguridad previa a la actualización. Para obtener más información sobre esta configuración, consulte "Configuración de gestión de parches en el plan de protección" (p. 1074).

Importante
Defina la opción **Estado de aprobación** como **Aprobado** para todos aquellos productos que se vayan a actualizar. De ese modo, el agente instalará únicamente los parches cuyo estado sea **Aprobado** en los equipos seleccionados del entorno de producción.



Ejecutar el plan de protección Instalación de parches de prueba y rechazar parches no seguros

Una vez que se hayan instalado los parches en los equipos del entorno de prueba, puede comprobar si todo funciona correctamente. Puede dejar el estado de aprobación de los equipos que no tienen ningún problema como **Aprobación pendiente** y cambiar el de aquellos que no funcionan correctamente a **Rechazado**.

Pasos para ejecutar el plan de protección Instalación de parches de prueba y rechazar parches no seguros

1. Ejecute el plan de protección Instalación de parches en entornos de prueba (según la planificación o manualmente).
2. Según el resultado, podrá ver cuáles de los parches instalados son seguros.
3. Vaya a **Gestión del software** > **Parches** y establezca el **Estado de aprobación** como **Rechazado** para aquellos parches que no sean seguros.

Caso de uso de aprobación automática de parches sin prueba

Si quiere instalar automáticamente los nuevos parches en los equipos de producción lo antes posible, sin instalarlos primero en los equipos de prueba, puede configurar solo un plan de protección.

El caso de uso consiste en los pasos siguientes:

1. Establezca los ajustes de la aprobación automática de parches. Selecciona la opción **Aprobación automática de parches sin prueba**. Para obtener más información, consulte "Configuración de la aprobación automática de parches" (p. 1083).

2. Configure un plan de protección para el entorno de producción (por ejemplo, "Instalación de parches en entornos de producción") con el módulo **Gestión de parches** habilitado y aplíquelo a los equipos del entorno de producción. Especifique la siguiente condición con respecto a la instalación de parches: el estado del parche debe ser **Aprobado**. Para obtener más información, consulte "Configurar el plan de protección Instalación de parches en entornos de producción" (p. 1085).
3. Ejecute el plan Instalación de parches en entornos de producción.

Aprobar parches manualmente

Puede aprobar un parche manualmente para acelerar su instalación al omitir la fase de prueba.

Requisitos previos

- Debe aplicarse un plan de protección con el módulo **Gestión de parches** habilitado a al menos un equipo de Windows.
- Debe haber parches aún sin instalar en el equipo o los equipos en los que se ha aplicado el plan de protección.

Pasos para probar parches manualmente

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Seleccione los parches que quiera instalar y acepte los acuerdos de licencia.
3. Establezca el **Estado de aprobación** de los parches en **Aprobado**.
   El estado de aprobación de los parches se establecerá en **Aprobado**. Los parches se instalarán automáticamente en los equipos según la planificación definida en el plan de protección. Si quiere instalar los parches de forma inmediata, siga el procedimiento que se describe en "Instalar parches bajo demanda" (p. 1087).

Instalar parches bajo demanda

Puede instalar parches bajo demanda manualmente si no quiere esperar a que llegue la hora de instalación planificada.

Puede iniciar la instalación manual del parche desde tres pantallas: **Parches**, **Vulnerabilidades** y **Todos los dispositivos**.

Pasos para instalar un parche manualmente

Desde Parches

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Parches**.
2. Acepte los acuerdos de licencia para los parches que quiera instalar.
3. En el asistente **Instalar parches**, seleccione los parches que quiera instalar y haga clic en **Instalar**.
4. Seleccione los equipos en los cuales desea instalar los parches.

5. Seleccione las opciones de reinicio.
   a. Seleccione si quiere que el equipo se reinicie después de instalar los parches.

Opción	Descripción
No	Los equipos no se reiniciarán automáticamente después de instalar los parches.
Si es necesario	Los equipos se reiniciarán únicamente si es necesario para aplicar los parches.
Sí	Los equipos se reiniciarán automáticamente después de instalar los parches. También puede especificar cuándo tendrá lugar el reinicio.

   b. [Opcional] Si quiere programar el reinicio del equipo mientras se está realizando una copia de seguridad del equipo, seleccione **No reiniciar hasta que finalice la copia de seguridad**.
6. Haga clic en **Instalar parches**.

Desde Vulnerabilidades

1. En la consola de Cyber Protect, vaya a **Gestión del software** > **Vulnerabilidades**.
2. Lleva a cabo el proceso de solución tal y como se describe en "Gestión de vulnerabilidades encontradas" (p. 1071).

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione el equipo en el que desea instalar los parches.
3. Haga clic en **Parche**.
4. Seleccione los parches que quiera instalar y haga clic en **Siguiente**.
5. Seleccione las opciones de reinicio.
   a. Seleccione si quiere que el equipo se reinicie después de instalar los parches.

Opción	Descripción
No	Los equipos no se reiniciarán automáticamente después de instalar los parches.
Si es necesario	Los equipos se reiniciarán únicamente si es necesario para aplicar los parches.
Sí	Los equipos se reiniciarán automáticamente después de instalar los parches. También puede especificar cuándo tendrá lugar el reinicio.

   b. [Opcional] Si quiere programar el reinicio del equipo mientras se está realizando una copia de seguridad del equipo, seleccione **No reiniciar hasta que finalice la copia de seguridad**.
6. Haga clic en **Instalar parches**.

Gestión del inventario de software y hardware

Inventario de software

La función de inventario de software está disponible para los dispositivos que tengan el paquete Advanced habilitado o que cuenten con una licencia de Cyber Protect (heredada). La función le permite visualizar todas las aplicaciones de software instaladas en los dispositivos Windows y macOS.

Para obtener datos del inventario de software, puede ejecutar análisis automáticos o manuales en los dispositivos.

Puede utilizar los datos del inventario de software para:

- buscar y comparar información acerca de todas las aplicaciones instaladas en los dispositivos de la empresa
- determinar si es necesario actualizar una aplicación
- determinar si es necesario eliminar una aplicación sin usar
- comprobar que la versión de software de varios dispositivos de la compañía sea la misma
- supervisar los cambios en el estado del software entre análisis consecutivos.

Habilitar el análisis de inventario de software

Cuando se habilita el análisis de inventario de software en los dispositivos, el sistema recopila automáticamente los datos de software cada 12 horas.

La función de análisis de inventario de software viene habilitada de forma predeterminada para todos los dispositivos que tienen la licencia necesaria, pero puede modificar la configuración siempre que lo desee.

Nota
Solo los inquilinos de cliente pueden habilitar o deshabilitar el análisis de inventario de software. Los inquilinos unidad pueden ver los ajustes del análisis de inventario de software, pero no pueden modificarlos.

Pasos para habilitar el análisis de inventario de software

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Protección**.
3. Haga clic en **Escaneo de inventario**.
4. Haga clic en el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo **Análisis del inventario de software**.

Pasos para deshabilitar el análisis de inventario de software

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Protección**.
3. Haga clic en **Escaneo de inventario**.
4. Haga clic en el interruptor que se encuentra junto al nombre del módulo para deshabilitar el módulo **Análisis del inventario de software**.

Ejecución manual de un análisis de inventario de software

Puede ejecutar manualmente un análisis de inventario de software desde la pantalla **Inventario de software**, o bien desde la pestaña **Software** de la pantalla **Inventario**.

Requisitos previos

- El dispositivo debe tener un sistema operativo Windows o macOS.
- El dispositivo tiene la licencia de Cyber Protect (heredada) necesaria o tiene un paquete Advanced Management activado.

Pasos para ejecutar un análisis de inventario de software desde la pantalla Inventario de software

1. En la consola de Cyber Protect, vaya a **Gestión del software**.
2. Haga clic en **Inventario de software**.
3. En el campo desplegable **Agrupar por:**, seleccione **Dispositivos**.
4. Busque el dispositivo que desee analizar y haga clic en **Analizar ahora**.

Pasos para ejecutar un análisis de inventario de software desde la pestaña Software de la pantalla Inventario

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Haga clic en el dispositivo que desee analizar, y haga clic en **Inventario**.
3. En la pestaña **Software**, haga clic en **Analizar ahora**.

Búsqueda en el inventario de software

Puede visualizar y buscar los datos de todas las aplicaciones de software que están disponibles en todos los dispositivos de la empresa.

Requisitos previos

- Los dispositivos deben tener un sistema operativo Windows o macOS.
- Los dispositivos tienen la licencia de Cyber Protect (heredada) necesaria o tienen un paquete Advanced Management activado.
- El análisis de inventario de software de los dispositivos se ha realizado correctamente.

Pasos para visualizar todas las aplicaciones de software disponibles en los dispositivos con Windows y macOS de la empresa

1. En la consola de Cyber Protect, vaya a **Gestión del software**.
2. Haga clic en **Inventario de software**.

   De forma predeterminada, los datos se agrupan por dispositivo. En la siguiente tabla se describen los datos que aparecen en la pantalla **Inventario de software**.

Columna	Descripción
Nombre	Nombre de la aplicación.
Versión	Versión de la aplicación.
Estado	Estado de la aplicación. • **Nueva**. • **Actualización realizada**. • **Eliminada**. • **No hay cambios**.
Proveedor	Proveedor de la aplicación.
Fecha de instalación	La fecha y la hora en las que se instaló la aplicación.
Última ejecución	Solo para dispositivos con macOS. La fecha y la hora en las que la aplicación estuvo activa por última vez.
Ubicación	Directorio en el que se ha instalado la aplicación.
Usuario	Usuario que ha instalado la aplicación.
Tipo de sistema	Solo para dispositivos con Windows. Tipo de bits de la aplicación. • **X86** para aplicaciones de 32 bits. • **X64** para aplicaciones de 64 bits.

3. Para agrupar los datos por aplicación, en el campo desplegable **Agrupar por:** seleccione **Aplicaciones**.
4. Para disminuir la cantidad de información que aparece en la pantalla, utilice un filtro o una combinación de filtros.
   a. Haga clic en **Filtrar**.
   b. Seleccione un filtro o una combinación de varios filtros.

      En la siguiente tabla se describen los datos de la pantalla **Inventario de software**.

Filtro	Descripción
Nombre de dispositivo	Nombre de dispositivo. Es posible seleccionar varias opciones. Use este filtro si desea comparar el software de dispositivos específicos.

Filtro	Descripción
Aplicación	Nombre de la aplicación. Es posible seleccionar varias opciones. Con este filtro, puede comparar los datos de una aplicación concreta de dispositivos específicos o de todos los dispositivos.
Proveedor	Proveedor de la aplicación. Es posible seleccionar varias opciones. Use este filtro si desea ver todas las aplicaciones de un proveedor concreto de dispositivos específicos o de todos los dispositivos.
Estado	Estado de la aplicación. Es posible seleccionar varias opciones. Use este filtro si desea ver todas las aplicaciones con el estado seleccionado de dispositivos específicos o de todos los dispositivos.
Fecha de instalación	Fecha en la que se ha instalado la aplicación. Use este filtro si desea ver todas las aplicaciones instaladas en una fecha específica de dispositivos específicos o de todos los dispositivos.
Fecha del análisis	Fecha del análisis de inventario de software. Use este filtro si desea ver la información acerca del software de dispositivos específicos o de todos los dispositivos analizados en esa fecha.

c. Haga clic en **Aplicar**.

5. Para buscar en toda la lista de inventario de software, use la paginación que aparece en la parte inferior izquierda de la pantalla.

- Haga clic en el número de la página que desea abrir.
- En el campo desplegable, seleccione el número de la página que desea abrir.

Visualización del inventario de software de un solo dispositivo

Puede ver una lista de todas las aplicaciones de software instaladas en un solo dispositivo, así como información detallada acerca de las aplicaciones, como el estado, la versión, proveedor, fecha de instalación, última ejecución y ubicación.

Requisitos previos

- El dispositivo debe tener un sistema operativo Windows o macOS.
- El dispositivo tiene la licencia de Cyber Protect (heredada) necesaria o tiene un paquete Advanced Management activado.
- El análisis de inventario de software del dispositivo se ha realizado correctamente.

Pasos para visualizar el inventario de software de un solo dispositivo desde la pantalla Inventario de software

1. En la consola de Cyber Protect, vaya a **Gestión del software**.
2. Haga clic en **Inventario de software**.
3. En el campo desplegable **Agrupar por:**, seleccione **Dispositivos**.
4. Busque el dispositivo que desee inspeccionar mediante una de las opciones siguientes.
   - Buscar el dispositivo mediante la opción **Filtrar**:
     a. Haga clic en **Filtrar**.
     b. En el campo **Nombre de dispositivo**, seleccione el nombre del dispositivo que desea ver.
     c. Haga clic en **Aplicar**.
   - Buscar el dispositivo mediante la opción de **Buscar** dinámicamente:
     a. Haga clic en **Buscar**.
     b. Escriba el nombre completo del dispositivo o parte del mismo.

Pasos para visualizar el inventario de software de un solo dispositivo desde la pantalla Dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Haga clic en el dispositivo que desee ver, y haga clic en **Inventario**.
3. Haga clic en la pestaña **Software**.

Inventario de hardware

La función de inventario de hardware le permite visualizar todos los componentes de hardware disponibles en:

- los dispositivos físicos Windows y macOS con una licencia compatible con la característica del inventario de hardware.
- las máquinas virtuales Windows y macOS que funcionen en las siguientes plataformas de virtualización: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo y Virtuozzo Hybrid Infrastructure. Para obtener más información sobre las versiones compatibles de las plataformas de virtualización, consulte "Plataformas de virtualización compatibles" (p. 32).

Nota
La característica del inventario de hardware para las máquinas virtuales no es compatible con las ediciones heredadas de Cyber Protect.

La característica del inventario de hardware es compatible solo con los dispositivos en los que está instalado un agente de protección.

Para obtener datos del inventario de hardware, puede ejecutar análisis automáticos o manuales en los dispositivos.

Puede utilizar los datos del inventario de hardware para:

- descubrir todos los activos de hardware de la organización
- buscar en el inventario de hardware de todos los dispositivos de su organización
- comparar los componentes de hardware de los diversos dispositivos de la empresa
- ver información detallada acerca de un componente de hardware.

Habilitar el análisis de inventario de hardware

Cuando se habilita el análisis de inventario de hardware en dispositivos físicos y máquinas virtuales, el sistema recopila automáticamente los datos de hardware cada 12 horas.

La función de análisis de inventario de hardware viene habilitada de forma predeterminada, pero puede modificar la configuración cuando sea necesario.

Nota
Solo los inquilinos de cliente pueden habilitar o deshabilitar el análisis de inventario de hardware. Los inquilinos unidad pueden ver los ajustes del análisis de inventario de hardware, pero no pueden modificarlos.

Pasos para habilitar el análisis de inventario de hardware

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Protección**.
3. Haga clic en **Escaneo de inventario**.
4. Haga clic en el interruptor que se encuentra junto al nombre del módulo para habilitar el módulo **Análisis del inventario de hardware**.

Pasos para deshabilitar el análisis de inventario de hardware

1. En la consola de Cyber Protect, vaya a **Configuración**.
2. Haga clic en **Protección**.
3. Haga clic en **Escaneo de inventario**.
4. Haga clic en el interruptor que se encuentra junto al nombre del módulo para deshabilitar el módulo **Análisis del inventario de hardware**.

Ejecución manual de un análisis de inventario de hardware

Puede ejecutar manualmente un análisis de inventario de hardware para un solo dispositivo, así como visualizar los datos actuales de los componentes de hardware del dispositivo.

Nota
El análisis del inventario de hardware de las máquinas virtuales solo es compatible cuando la fecha y la hora actual de la máquina virtual corresponde a la fecha y la hora actual en UTC. Para asegurarse de que la máquina virtual utiliza la configuración de hora correcta, desactive la opción **Sincronización de hora** de la máquina virtual, establezca la fecha, la hora y la zona horaria actuales y reinicie **Acronis Agent Core Service** y **Acronis Managed Machine Service**.

Requisitos previos

- (Para todos los dispositivos) El dispositivo tiene un sistema operativo Windows o macOS.
- (Para todos los dispositivos) Los dispositivos tienen una licencia que admite la función de inventario de hardware. Tenga en cuenta que la función de inventario de hardware para las máquinas virtuales no es compatible con las ediciones de Cyber Protect (heredadas).
- (Para todos los dispositivos) Un agente de protección está instalado en el dispositivo.
- (Para máquinas virtuales) La máquina se ejecuta en una de las plataformas de virtualización compatibles. Para obtener más información, consulte "Inventario de hardware" (p. 1093).

Pasos para ejecutar un análisis de inventario de hardware en un solo dispositivo

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. Haga clic en el dispositivo que desee analizar, y haga clic en **Inventario**.
3. En la pestaña **Hardware**, haga clic en **Analizar ahora**.

Búsqueda en el inventario de hardware

Puede visualizar y buscar los datos de todos los componentes de hardware que están disponibles en todos los dispositivos de la empresa.

Requisitos previos

- (Para todos los dispositivos) Los dispositivos deben tener un sistema operativo Windows o macOS.
- (Para todos los dispositivos) Los dispositivos deben tener una licencia compatible con la característica del inventario de hardware. Tenga en cuenta que la característica del inventario de hardware para las máquinas virtuales no es compatible con las ediciones heredadas de Cyber Protect.
- (Para todos los dispositivos) Un agente de protección está instalado en el dispositivo.
- (Para todos los dispositivos) El análisis de inventario de hardware de los dispositivos se ha realizado correctamente.
- (Para máquinas virtuales) La máquina se ejecuta en una de las plataformas de virtualización compatibles. Para obtener más información, consulte "Inventario de hardware" (p. 1093).

Pasos para visualizar todos los componentes de hardware disponibles en los dispositivos con Windows y macOS de la empresa

1. En la consola de Cyber Protect, vaya a **Dispositivos**.
2. En el campo desplegable **Vista:**, seleccione **Hardware**.

Nota
La vista es un conjunto de columnas que determina los datos que se ven en la pantalla. Las vistas predefinidas son **Estándar** y **Hardware**. Puede crear y guardar vistas personalizadas que incluyan distintos conjuntos de columnas, y que resulten más prácticas para sus necesidades.

En la siguiente tabla se describen los datos que aparecen en la vista **Hardware**.

Columna	Descripción
Nombre	Nombre de dispositivo.
Estado del análisis de hardware	Estado del análisis de hardware. • **Completado**. • **Sin iniciar**. • El estado **No compatible** se muestra para aquellas cargas de trabajo que no son compatibles con la funcionalidad de inventario de hardware, como equipos virtuales, dispositivos móviles o dispositivos con Linux. • **Actualizar agente** se muestra cuando el dispositivo tiene instalada una versión desactualizada del agente. Al hacer clic en esta acción, se le redirigirá a la página Configuración > Agentes, donde el administrador puede actualizar el agente. • **Actualizar cuota**. Al hacer clic aquí, se abrirá un cuadro de diálogo donde el administrador puede cambiar la licencia actual por otra disponible para licencias de inquilino.
Procesador	Modelos de todos los procesadores del dispositivo.
Núcleos de procesador	Número de núcleos de todos los procesadores del dispositivo.
Almacenamiento en disco	El almacenamiento utilizado y el almacenamiento total de todos los discos del dispositivo.
Memoria	La capacidad de RAM del dispositivo.
Fecha del análisis	La fecha y la hora del último análisis de inventario de hardware.
Placa base	La placa base del dispositivo.

Columna	Descripción
Número de serie de la placa base	El número de serie de la placa base.
Versión del BIOS	La versión del BIOS del sistema.
Organización	Organización a la que pertenece el dispositivo.
Propietario	Propietario del dispositivo.
Dominio	Dominio del dispositivo.
Sistema operativo	Sistema operativo del dispositivo.
Compilación del sistema operativo	Compilación del sistema operativo del dispositivo.

3. Para añadir columnas a la tabla, haga clic en el icono de opciones de la columna y seleccione aquellas columnas que desee incluir en la tabla.
4. Para disminuir la cantidad de información que aparece en la pantalla, utilice uno o más filtros.
   a. Haga clic en **Buscar**.
   b. Haga clic en la flecha y, a continuación, haga clic en **Hardware**.
   c. Seleccione un filtro o una combinación de varios filtros.
      En la siguiente tabla se describen los filtros de **Hardware**.

Filtro	Descripción
Modelo de procesador	Es posible seleccionar varias opciones. Use este filtro si desea ver los datos de hardware de los dispositivos que cuentan con el modelo de procesador especificado.
Núcleos de procesador	Use este filtro si desea ver los datos de hardware de los dispositivos que cuentan con el número de núcleos de procesador especificado.
Tamaño total del disco	Use este filtro si desea ver los datos de hardware de los dispositivos que cuentan con el tamaño total de disco especificado.
Capacidad de memoria	Use este filtro si desea ver los datos de hardware de los dispositivos que cuentan con la capacidad de memoria especificada.

   d. Haga clic en **Aplicar**.
5. Para ordenar los datos de forma ascendente, haga clic en el nombre de una columna.

Visualización del hardware de un solo dispositivo

Puede ver información detallada acerca de la placa base, procesadores, memoria, gráficos, unidades de almacenamiento, redes y sistema de un dispositivo específico.

Requisitos previos

- (Para todos los dispositivos) El dispositivo tiene un sistema operativo Windows o macOS.
- (Para todos los dispositivos) Los dispositivos deben tener una licencia compatible con la característica del inventario de hardware. Tenga en cuenta que la característica del inventario de hardware para las máquinas virtuales no es compatible con las ediciones heredadas de Cyber Protect.
- (Para todos los dispositivos) Un agente de protección está instalado en el dispositivo.
- (Para todos los dispositivos) El análisis de inventario de hardware del dispositivo se ha realizado correctamente.
- (Para máquinas virtuales) La máquina se ejecuta en una de las plataformas de virtualización compatibles. Para obtener más información, consulte "Inventario de hardware" (p. 1093).

Pasos para ver información detallada acerca del hardware de un dispositivo específico

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. En el campo desplegable **Vista:**, seleccione **Hardware**.
3. Busque el dispositivo que desee inspeccionar empleando uno de los métodos que se describen a continuación.
   - Buscar el dispositivo mediante la opción **Filtrar**:
     a. Haga clic en **Filtrar**.
     b. Seleccione un filtro o una combinación de varios parámetros de filtro para buscar el dispositivo.
     c. Haga clic en **Aplicar**.
   - Buscar el dispositivo mediante la opción **Buscar**:
     a. Haga clic en **Buscar**.
     b. Escriba el nombre completo del dispositivo o parte del mismo y haga clic en **Introducir**.
4. Haga clic en la fila donde aparece el dispositivo, y haga clic en **Inventario**.
5. Haga clic en la pestaña **Hardware**.
   Se muestran los datos de hardware siguientes.

Componente de hardware	Información que se muestra
Placa base	Nombre, fabricante, modelo y número de serie de la placa base del dispositivo.
Procesadores	Fabricante, modelo, velocidad máxima del reloj y número de núcleos de cada procesador del dispositivo.
Memoria	Capacidad, fabricante y número de serie de la memoria del dispositivo.

Componente de hardware	Información que se muestra
Gráficos	Fabricante y modelo de las GPU del dispositivo.
Unidades de almacenamiento	Modelo, tipo de medio, espacio disponible y tamaño de las unidades de almacenamiento del dispositivo.
Red	Dirección MAC, dirección IP y tipo de adaptadores de red del dispositivo.
Sistema	ID del producto, fecha de instalación original, tiempo de arranque del sistema, fabricante del sistema, modelo del sistema, versión del BIOS, dispositivo de arranque, configuración regional del sistema y zona horaria del sistema.

Conexión a cargas de trabajo para asistencia o escritorio remotos

La funcionalidad de escritorio remoto y asistencia remota es una forma cómoda de conectarse a las cargas de trabajo de su organización para controlarlas o recibir asistencia de forma remota. A partir de diciembre de 2022, la funcionalidad es compatible con los protocolos NEAR, RDP y el uso compartido de pantalla de Apple. Para obtener más información, consulte "Protocolos de conexión remota" (p. 1105).

Puede utilizar la funcionalidad de escritorio remoto para ejecutar las siguientes tareas:

- Conectarse a cargas de trabajo remotas de Windows, macOS y Linux con NEAR en el modo de solo visualización.
- Conectarse a cargas de trabajo remotas de Windows con RDP.
- Conectarse a cargas de trabajo remotas de macOS mediante el uso compartido de pantalla de Apple en modo de solo visualización o en modo cortina.
- Conectarse a cargas de trabajo administradas y controlarlas de forma remota con conexiones remotas de la nube.
- Conectarse a cargas de trabajo no administradas y controlarlas de forma remota con conexiones remotas directas.
- Conectarse a cargas de trabajo remotas no administradas con Acronis Asistencia rápida.
- Conectarse a cargas de trabajo remotas con métodos de autenticación diferentes: con credenciales de carga de trabajo remotas, solicitando permiso para observar y controlar o con un código de acceso (para Asistencia rápida).
- Observar varios monitores al mismo tiempo en la vista múltiple.
- Grabar sesiones remotas (al estar conectado a través de NEAR).
- Ver el informe de historial de sesiones.

Para obtener más información acerca de las características que forman parte de los paquetes de Standard y Advanced Management, consulte "Funciones de asistencia y escritorio remotos" (p. 1102).

Puede utilizar la funcionalidad de asistencia remota para ejecutar las siguientes tareas:

- Conectarse a cargas de trabajo remotas de Windows, macOS y Linux con NEAR en el modo de control.
- Conectarse a cargas de trabajo remotas de macOS mediante el uso compartido de pantalla de Apple en modo de control.
- Proporcionar asistencia remota para las cargas de trabajo con conexiones remotas de la nube.
- Transferir archivos entre las cargas de trabajo locales y remotas.
- Realizar acciones de administración básicas en la carga de trabajo remota: reiniciar, apagar,

pausar, vaciar papelera de reciclaje y cerrar la sesión del usuario remoto.

- Supervisar la carga de trabajo remota con capturas de pantalla periódicas del escritorio.

Para obtener más información acerca de las características que forman parte de la protección estándar y Advanced Management, consulte "Funciones de asistencia y escritorio remotos" (p. 1102).

Importante

Para activar la funcionalidad completa de escritorio y asistencia remotos en una carga de trabajo administrada, debe configurar y aplicar un plan de administración remota a la carga de trabajo. Aunque puede aplicar solo un plan de administración remota a una carga de trabajo, según sus necesidades, puede configurar planes de administración remota diferentes y aplicarlos a diferentes cargas de trabajo.

Por ejemplo, puede crear un plan de administración remota que solo tenga habilitado el protocolo RDP y aplicarlo a varias cargas de trabajo. De esa forma, podrá conectarse de forma remota a esas cargas de trabajo sin activar la licencia de Advanced Management por carga de trabajo y sin pagar costes adicionales.

Por otro lado, puede crear otro plan de administración remota que tenga activados los protocolos NEAR y el uso compartido de pantalla de Apple. En este caso, se activará la licencia de Advanced Management por carga de trabajo y se le cobrará por cada carga de trabajo a la que se aplique este plan de administración remota.

Para obtener más información acerca de los planes de administración remota y trabajar con ellos, consulte "Planes de administración remota" (p. 1109).

Nota

La funcionalidad de asistencia y escritorio remotos requiere:

- una sola instalación de Cliente de Connect en la carga de trabajo (host) gestionada. El sistema le sugerirá que descargue el cliente cuando intente ejecutar una acción remota (control remoto o asistencia remota) en una carga de trabajo de destino por primera vez. De forma alternativa, puede descargar Cliente de Connect desde la ventana **Descargas** en la consola de Protección. Para obtener más información acerca de los ajustes que puede configurar, consulte "Configuración de los ajustes de Cliente de Connect" (p. 1142).
- instalación del Agente de Connect en las cargas de trabajo gestionadas. El Agente de Connect es un módulo que forma parte del agente de Protección, a partir de la versión 15.0.31266.
- para las cargas de trabajo remotas de macOS, se deben conceder los permisos de sistema necesarios para el Agente de Connect. Para obtener más información, consulte "Instalación de agentes de protección en macOS" (p. 88).
- ejecución de la aplicación Acronis Asistencia rápida en las cargas de trabajo sin gestionar. Puede descargar Acronis Asistencia rápida desde el sitio web.

Para obtener más información sobre las plataformas compatibles con cada componente de asistencia y escritorio remotos, consulte "Plataformas compatibles" (p. 1104).

Funciones de asistencia y escritorio remotos

La siguiente tabla le ofrece más información acerca de los cambios de las funciones compatibles de asistencia y escritorio remotos que se incorporaron en diciembre de 2022.

Característica	Protección estándar antes de diciembre de 2022	Advanced Management antes de diciembre de 2022	Protección estándar después de diciembre de 2022	Advanced Management después de diciembre de 2022
Asistencia remota a través de RDP para Windows	Sí	No	No	No
Compartir una conexión remota con usuarios	No	Sí	No	No
Conexiones remotas				
Acciones remotas	No	No	Sí	Sí
Selección de una sesión para conectarse a Windows, macOS o Linux	No	No	No	Sí
Conexión directa mediante RDP y el uso compartido de pantalla de Apple	No	No	No	Sí
Control de varias ventanas	No	No	No	Sí
Modos de conexión: control, solo visualización y cortina	No	No	No	Sí
Compatibilidad con credenciales comunes para conexiones remotas	No	No	Sí	Sí
Conexiones simultáneas por técnico				
a través de RDP	Sí	Sí	Sí	Sí
a través de NEAR	No	No	No	Sí
Transferencia y uso compartido de archivos				
de Windows a Windows,	No	No	No	Sí

Característica	Protección estándar antes de diciembre de 2022	Advanced Management antes de diciembre de 2022	Protección estándar después de diciembre de 2022	Advanced Management después de diciembre de 2022
macOS o Linux				
de macOS a Windows, macOS o Linux	No	No	No	Sí
de Linux a Windows, macOS o Linux	No	No	No	Sí
Conexión mediante la aplicación Asistencia rápida				
de Windows a Windows, macOS o Linux	No	No	No	Sí
de macOS a Windows, macOS o Linux	No	No	No	Sí
de Linux a Windows, macOS o Linux	No	No	No	Sí
Conexiones remotas mediante protocolos				
Conexión remota a través de NEAR				
de Windows a Windows, macOS o Linux	No	No	No	Sí
de macOS a Windows, macOS o Linux	No	No	No	Sí
de Linux a Windows, macOS o Linux	No	No	No	Sí
Conexión remota a través de RDP (cliente de escritorio)				
de Windows a Windows	Sí	Sí	Sí	Sí
de macOS a Windows	Sí	Sí	Sí	Sí
de Linux a Windows	No	No	Sí	Sí
Conexión remota a través de RDP (cliente web)				
de Windows a Windows	Sí	Sí	Sí	Sí
de macOS a Windows	Sí	Sí	Sí	Sí
de Linux a Windows	No	No	Sí	Sí

Característica	Protección estándar antes de diciembre de 2022	Advanced Management antes de diciembre de 2022	Protección estándar después de diciembre de 2022	Advanced Management después de diciembre de 2022
Conexión remota a través del uso compartido de pantalla de Apple				
de Windows, macOS o Linux a macOS	No	No	No	Sí
Administración de sesiones				
Grabación de sesiones	No	No	No	Sí
Informes y supervisión				
Historial de sesiones y búsqueda	No	No	No	Sí
Transmisión de captura de pantalla	No	No	No	Sí

Plataformas compatibles

La siguiente tabla enumera los sistemas operativos compatibles para cada componente de la funcionalidad de asistencia y escritorio remotos.

Componente del escritorio remoto	Plataformas compatibles
Cliente de Connect	• Windows 7 o posterior • macOS 10.13 o posterior • Linux: openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Agente de Connect	• Windows 7 o posterior • Windows Server 2008 R2 o posterior • macOS 10.13 o posterior • Linux: Red Hat Enterprise Linux 8 y 8.1

Componente del escritorio remoto	Plataformas compatibles
	Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis Asistencia rápida	• Windows 7 o posterior • Windows Server 2008 R2 o posterior • macOS 10.13 o posterior • Linux: Red Hat Enterprise Linux 8 y 8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

Protocolos de conexión remota

La funcionalidad de escritorio remoto utiliza los siguientes protocolos para las conexiones remotas.

NEAR

NEAR es un protocolo altamente seguro desarrollado por Acronis que tiene las siguientes características:

- ### H.264

  NEAR implementa tres modos de calidad: **Suave**, **Equilibrado** y **Nítido**. En el modo **Suave**, NEAR utiliza la codificación H.264 de hardware en macOS y Windows para codificar la imagen de escritorio y recurrir al codificador de software si el codificador de hardware no está disponible. El tamaño de la imagen actualmente está limitado a la resolución Full HD (1920x1080).

- ### Códec adaptable

  En los modos de calidad **Equilibrado** y **Nítido**, NEAR utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264.

  En el modo **Equilibrado**, la calidad de la imagen se ajusta automáticamente según sus condiciones de red actuales y mantiene la velocidad de frotogramas actual.

En el modo **Nítido**, la imagen tiene la máxima calidad, pero podría tener una velocidad de fotogramas reducida si su red, procesador o tarjeta de vídeo se sobrecargan.

El códec adaptable utiliza OpenCL en Windows y macOS cuando está disponible en sus controladores gráficos.

- ### Transferencia de sonido

  NEAR es capaz de capturar el sonido del equipo remoto y transferirlo al host. Para obtener más información acerca de habilitar el redireccionamiento del sonido remoto en Windows, macOS y Linux, consulte "Redireccionamiento de sonido remoto" (p. 1106).

- ### Diferentes opciones de inicio de sesión

  Puede utilizar los siguientes métodos para iniciar sesión en la carga de trabajo remota.

  Código de acceso: el usuario que ha iniciado sesión en la carga de trabajo remota ejecuta Asistencia rápida y le dice el código de acceso. Con este método, siempre se conecta a la sesión del usuario conectado en ese momento.

  Credenciales de la carga de trabajo: inicie sesión en la carga de trabajo remota con las credenciales del administrador que están registradas en la carga de trabajo.

  Solicitar permiso para observar o controlar: el usuario que ha iniciado sesión en la carga de trabajo remota le pedirá que permita o deniegue la conexión.

- ### Seguridad

  Sus datos siempre están cifrados de dos formas con cifrado AES en NEAR.

RDP

El protocolo de escritorio remoto (RDP) es un protocolo propio desarrollado por Microsoft que permite la conexión con el ordenador de Windows sobre una conexión de red.

Uso compartido de pantalla de Apple

El uso compartido de pantalla de Apple es un cliente VNC de Apple incluido como parte de macOS versión 10.5 y posteriores.

Redireccionamiento de sonido remoto

Cliente de Connect es compatible con la transmisión de audio a través del protocolo de conexión NEAR. Para obtener más información sobre NEAR, consulte "Protocolos de conexión remota" (p. 1105).

Redireccionamiento del sonido desde una carga de trabajo remota de Windows

Para las cargas de trabajo de Windows, el sonido remoto debería transmitirse automáticamente. Asegúrese de que hay dispositivos de salida de sonido (altavoces o auriculares) conectados a la carga de trabajo remota.

Redireccionamiento del sonido desde una carga de trabajo remota de macOS

Para habilitar el redireccionamiento de sonido desde una carga de trabajo macOS, asegúrese de que:

- La carga de trabajo tiene instalado el agente de Protección.
- La carga de trabajo tiene instalado un controlador de captura del sonido.
- La carga de trabajo utiliza el protocolo NEAR para las conexiones remotas.

Nota
En macOS 10.15 Catalina, se debe otorgar el permiso de micrófono al Agente de Connect. Para obtener más información sobre el permiso de micrófono al Agente de Connect, consulte "Conceder los permisos de sistema necesarios para el Agente de Connect" (p. 82).

El agente funciona con los siguientes controladores de captura de sonido: Soundflower o Blackhole.

El proceso de instalación en las versiones más recientes se describe en la página de wikis de Blackhole: https://github.com/ExistentialAudio/BlackHole/wiki/Installation.

Nota
actualmente, Cliente de Connect es compatible solo con la versión de dos canales de Blackhole.

De manera alternativa, si Homebrew está instalado en la carga de trabajo, puede instalar Blackhole mediante la ejecución de este comando:

```
brew install --cask blackhole-2ch
```

Nota
Si bien el sonido de una carga de trabajo remota de macOS se redirecciona, el usuario que ha iniciado sesión en la carga de trabajo remota no escuchará el sonido.

Redireccionamiento del sonido desde una carga de trabajo remota de Linux

El redireccionamiento de sonido remoto debería funcionar automáticamente con la mayoría de las distribuciones de Linux. Si el redireccionamiento de sonido remoto no funciona de forma predeterminada, instale el controlador PulseAudio mediante la ejecución del siguiente comando:

```
sudo apt-get install pulseaudio
```

Conexiones a cargas de trabajo remotas para asistencia o escritorio remotos

La funcionalidad de asistencia y escritorio remotos ofrece diversas formas de establecer conexiones directas remotas o en la nube con sus cargas de trabajo.

Las conexiones directas se establecen a través de TCP/IP en la red del área local (LAN) entre Cliente de Connect y la carga de trabajo remota que no tiene un agente instalado. No requiere acceso a Internet.

Las conexiones de la nube se establecen entre Cliente de Connect y el agente o Asistencia rápida en la carga de trabajo a través de Acronis Cloud.

La siguiente tabla proporciona más información sobre las opciones de conexión de la nube.

Conexión en la nube	Opción de conexión en la nube	Modo Ver	Acción remota compatible	Disponible para
a través de NEAR	de Cliente de Connect a Agente de Connect de Cliente de Connect a Asistencia rápida	Control Solo visualización	Escritorio remoto Asistencia remota	cargas de trabajo administradas
a través de RDP	de Cliente de Connect a Agente de Connect desde el cliente web a Agente de Connect	Control	Escritorio remoto	cargas de trabajo administradas
a través del uso compartido de pantalla de Apple	de Cliente de Connect a Agente de Connect	Control Solo visualización Cortina	Escritorio remoto Asistencia remota	cargas de trabajo administradas

La siguiente tabla proporciona más información sobre las opciones de conexión directa.

Conexión directa	Opción de conexión directa	Acción remota compatible	Disponible para
a través de RDP	desde Cliente de Connect al servidor RDP	Escritorio remoto	cargas de trabajo no

Conexión directa	Opción de conexión directa	Acción remota compatible	Disponible para
			administradas
a través del uso compartido de pantalla de Apple	de Cliente de Connect al servidor del uso compartido de pantalla de Apple	Escritorio remoto Asistencia remota	cargas de trabajo no administradas

Planes de administración remota

Los planes de administración remota son planes que aplica al agente de Protección para habilitar y configurar la funcionalidad de escritorio y asistencia remotos en sus cargas de trabajo administradas.

Si no se aplica ningún plan de administración remota a una carga de trabajo, la funcionalidad de escritorio y asistencia remotos se limitará a las acciones remotas (reiniciar, apagar, pausar, vaciar papelera de reciclaje y cerrar la sesión del usuario remoto).

Nota
La disponibilidad de la configuración que puede configurar en el plan de administración remota depende del paquete de servicios que se aplica al inquilino. Para acceder a toda la configuración, active el paquete de Advanced Management. Para obtener más información acerca de las características que forman parte de los paquetes de Standard y Advanced Management, consulte "Funciones de asistencia y escritorio remotos" (p. 1102).

Creación de un plan de administración remota

Puede crear un plan de administración remota y asignarlo a una carga de trabajo para configurar la funcionalidad de asistencia y escritorio remotos en la carga de trabajo administrada.

Nota
La disponibilidad de la configuración del plan de administración remota depende de la cuota de servicio que está asignada al inquilino. Si usa la funcionalidad estándar, solo puede configurar conexiones a través de RDP.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para crear un plan de administración remota

Desde planes de administración remota

1. En la consola de Cyber Protect, vaya a **Administración** > **Planes de administración remota**.
2. Cree un plan de administración remota mediante una de estas dos opciones:
   - Si no hay planes de administración remota en la lista, haga clic en **Crear**.
   - Si hay planes de administración remota en la lista, haga clic en **Crear plan**.
3. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Continuar**.
4. Haga clic en **Protocolos de conexión** y active los protocolos que desee que estén disponibles en este plan de administración remota para las conexiones remotas: NEAR, RDP o el uso compartido de pantalla de Apple.
5. [Opcional] Para el protocolo NEAR, en la sección **Configuración de seguridad**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción	Disponible para
Bloquee la carga de trabajo cuando el usuario desconecte de la sesión de la consola	Si selecciona este ajuste, la carga de trabajo se bloqueará cuando se desconecte de la sesión de la consola.	Windows y macOS
Permitir que solo un usuario a la vez se conecte con NEAR o transfiera archivos	Si selecciona esta configuración, las conexiones que utilizan NEAR y la transferencia de archivos no serán posibles mientras haya una conexión remota activa a la carga de trabajo.	Windows, macOS y Linux
Permitir que el administrador de la carga de trabajo se conecte a cualquier sesión de usuario que no sea administrador	Si selecciona esta configuración, el administrador podrá conectarse a cualquier sesión de usuario estándar en la carga de trabajo. Si **Permitir que el administrador de la carga de trabajo se conecte a cualquier sesión de usuario que no sea administrador** y **Permitir creación de sesión del sistema** están desactivadas, solo podrá conectarse a sesiones de administrador	Windows y macOS

Configuración	Descripción	Disponible para
	activas en las cargas de trabajo remotas de macOS.	
Permitir la creación de sesiones del sistema	Si selecciona esta configuración, cuando establezca conexiones remotas, el administrador se conectará en una sesión nueva y no en una de las sesiones activas existentes.	macOS
Permitir la sincronización del portapapeles	Si selecciona esta configuración, podrá transferir datos entre su portapapeles y el portapapeles de la carga de trabajo remota. Por ejemplo, podrá copiar texto de un archivo en la carga de trabajo remota y pegarlo en un archivo de su carga de trabajo, y viceversa.	Windows, macOS y Linux

6. Haga clic en **Configuración de seguridad**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción
Mostrar si la carga de trabajo se controla de forma remota	Si selecciona esta configuración, se mostrará una notificación en el escritorio de la carga de trabajo remota cuando haya una conexión de escritorio remoto activa con la carga de trabajo.
Pedir permiso al usuario para realizar capturas de pantalla de la carga de trabajo	Si selecciona esta configuración, el usuario de la carga de trabajo remota será notificado cuando el administrador solicite la transmisión de capturas de pantalla desde la carga de trabajo.

7. Haga clic en **Gestión de cargas de trabajo**, seleccione las funciones que desee que estén disponibles en las cargas de trabajo remotas y, a continuación, haga clic en **Listo**.

Configuración	Descripción	Disponible el
Transferencia de archivos	Permite la transferencia de archivos entre cargas de	Windows, macOS y Linux

Configuración	Descripción	Disponible el
	trabajo locales y remotas.	
Transmisión de captura de pantalla	Habilite la transmisión de capturas de pantalla del escritorio de la carga de trabajo remota para la consola de Cyber Protect.	Windows, macOS y Linux

8. Haga clic en **Configuración de pantalla**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Nota
La **Configuración de pantalla** solo está disponible para las conexiones a través de NEAR.

Configuración	Descripción	Disponible el
Use la deduplicación del escritorio para capturarlo	La duplicación del escritorio es uno de los métodos de captura de pantalla de Windows. En algunos entornos, puede ser inestable. Si no utiliza la deduplicación del escritorio, utilizará el método básico (BitBlt) en su lugar. Es mucho más lento, pero más estable.	Windows
Use la aceleración de OpenCL	La aceleración de OpenCL puede acelerar el códec adaptable, que se encarga del modo de calidad **Equilibrado**, mediante la ejecución de algunos cálculos en la unidad de procesamiento gráfico (GPU). Para ello, es necesario instalar el controlador de OpenCL en el Linux remoto. El códec adaptable utiliza OpenCL en macOS y Windows cuando está disponible en sus controladores gráficos.	Linux
Use la codificación H.264 de hardware	NEAR es compatible con tres	Windows y macOS

Configuración	Descripción	Disponible el
	modos de calidad: **Suave**, **Equilibrado** y **Nítido**. El modo **Suave** utiliza la codificación H.264 para codificar la imagen del escritorio. El modo **Equilibrado** utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264. La calidad de la imagen se ajusta automáticamente según sus condiciones de red actuales y mantiene la velocidad de fotogramas actual. El modo **Nítido** utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264. La imagen siempre tiene la máxima calidad, pero podría tener una velocidad de fotogramas reducida por segundos si su red, procesador o tarjeta de vídeo se sobrecargan.	

9. Si desea que la información sobre los usuarios que iniciaron sesión por última vez en las cargas de trabajo esté disponible en la información de la carga de trabajo, haga clic en **Caja de herramientas**, seleccione **Mostrar últimos usuarios que iniciaron sesión** y, a continuación, haga clic en **Listo**.

   Para obtener más información sobre los usuarios que iniciaron sesión por última vez, consulte "Buscar el último usuario que ha iniciado sesión" (p. 398).
10. [Opcional] Pasos para añadir cargas de trabajo al plan:
    a. Haga clic en **Añadir cargas de trabajo**.
    b. Seleccione las cargas de trabajo y haga clic en **Añadir**.
    c. Si hay problemas de compatibilidad que desea resolver, siga el procedimiento descrito en "Resolución de problemas de compatibilidad con planes de administración remota" (p. 1122).

11. Haga clic en **Crear**.

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que quiera aplicar un plan de administración remota.
3. Haga clic en **Proteger** y, a continuación, en **Agregar plan**.
4. Haga clic en **Crear plan** y seleccione **Administración remota**.
5. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Continuar**.
6. Haga clic en **Protocolos de conexión** y active los protocolos que desee que estén disponibles en este plan de administración remota para las conexiones remotas: NEAR, RDP o el uso compartido de pantalla de Apple.
7. [Opcional] Para el protocolo NEAR, en la sección **Configuración de seguridad**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción	Disponible para
Bloquee la carga de trabajo cuando el usuario desconecte de la sesión de la consola	Si selecciona este ajuste, la carga de trabajo se bloqueará cuando se desconecte de la sesión de la consola.	Windows y macOS
Permitir que solo un usuario a la vez se conecte con NEAR o transfiera archivos	Si selecciona esta configuración, las conexiones que utilizan NEAR y la transferencia de archivos no serán posibles mientras haya una conexión remota activa a la carga de trabajo.	Windows, macOS y Linux
Permitir que el administrador de la carga de trabajo se conecte a cualquier sesión de usuario que no sea administrador	Si selecciona esta configuración, el administrador podrá conectarse a cualquier sesión de usuario estándar en la carga de trabajo. Si **Permitir que el administrador de la carga de trabajo se conecte a cualquier sesión de usuario que no sea administrador** y **Permitir creación de sesión del**	Windows y macOS

Configuración	Descripción	Disponible para
	sistema están desactivadas, solo podrá conectarse a sesiones de administrador activas en las cargas de trabajo remotas de macOS.	
Permitir la creación de sesiones del sistema	Si selecciona esta configuración, cuando establezca conexiones remotas, el administrador se conectará en una sesión nueva y no en una de las sesiones activas existentes.	macOS
Permitir la sincronización del portapapeles	Si selecciona esta configuración, podrá transferir datos entre su portapapeles y el portapapeles de la carga de trabajo remota. Por ejemplo, podrá copiar texto de un archivo en la carga de trabajo remota y pegarlo en un archivo de su carga de trabajo, y viceversa.	Windows, macOS y Linux

8. Haga clic en **Configuración de seguridad**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Configuración	Descripción
Mostrar si la carga de trabajo se controla de forma remota	Si selecciona esta configuración, se mostrará una notificación en el escritorio de la carga de trabajo remota cuando haya una conexión de escritorio remoto activa con la carga de trabajo.
Pedir permiso al usuario para realizar capturas de pantalla de la carga de trabajo	Si selecciona esta configuración, el usuario de la carga de trabajo remota será notificado cuando el administrador solicite la transmisión de capturas de pantalla desde la carga de trabajo.

9. Haga clic en **Gestión de cargas de trabajo**, seleccione las funciones que desee que estén disponibles en las cargas de trabajo remotas y, a continuación, haga clic en **Listo**.

Configuración	Descripción	Disponible el
Transferencia de archivos	Permite la transferencia de archivos entre cargas de trabajo locales y remotas.	Windows, macOS y Linux
Transmisión de captura de pantalla	Habilite la transmisión de capturas de pantalla del escritorio de la carga de trabajo remota para la consola de Cyber Protect.	Windows, macOS y Linux

10. Haga clic en **Configuración de pantalla**, marque o desmarque las casillas de verificación para habilitar o deshabilitar la configuración correspondiente y haga clic en **Listo**.

Nota
La **Configuración de pantalla** solo está disponible para las conexiones a través de NEAR.

Configuración	Descripción	Disponible el
Use la deduplicación del escritorio para capturarlo	La duplicación del escritorio es uno de los métodos de captura de pantalla de Windows. En algunos entornos, puede ser inestable. Si no utiliza la deduplicación del escritorio, utilizará el método básico (BitBlt) en su lugar. Es mucho más lento, pero más estable.	Windows
Use la aceleración de OpenCL	La aceleración de OpenCL puede acelerar el códec adaptable, que se encarga del modo de calidad **Equilibrado**, mediante la ejecución de algunos cálculos en la unidad de procesamiento gráfico (GPU). Para ello, es necesario instalar el controlador de OpenCL en el Linux remoto. El códec adaptable utiliza OpenCL en macOS y Windows cuando está disponible en sus controladores gráficos.	Linux

Configuración	Descripción	Disponible el
Use la codificación H.264 de hardware	NEAR es compatible con tres modos de calidad: **Suave**, **Equilibrado** y **Nítido**. El modo **Suave** utiliza la codificación H.264 para codificar la imagen del escritorio. El modo **Equilibrado** utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264. La calidad de la imagen se ajusta automáticamente según sus condiciones de red actuales y mantiene la velocidad de fotogramas actual. El modo **Nítido** utiliza el códec adaptable, que ofrece una calidad de imagen completa de 32 bits, en comparación con el modo de "vídeo" utilizado por H.264. La imagen siempre tiene la máxima calidad, pero podría tener una velocidad de fotogramas reducida por segundos si su red, procesador o tarjeta de vídeo se sobrecargan.	Windows y macOS

11. Si desea que la información sobre los usuarios que iniciaron sesión por última vez en las cargas de trabajo esté disponible en la información de la carga de trabajo, haga clic en **Caja de herramientas**, seleccione **Mostrar últimos usuarios que iniciaron sesión** y, a continuación, haga clic en **Listo**.

    Para obtener más información sobre los usuarios que iniciaron sesión por última vez, consulte "Buscar el último usuario que ha iniciado sesión" (p. 398).
12. Haga clic en **Crear**.

Adición de una carga de trabajo a un plan de administración remota

Según sus necesidades, puede añadir cargas de trabajo a un plan de administración remota después de crearlo.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para añadir una carga de trabajo a un plan de administración remota

Desde planes de administración remota

1. En la consola de Cyber Protect, vaya a **Administración** > **Planes de administración remota**.
2. Haga clic en el plan de administración remota.
3. Según si el plan ya se ha aplicado a una carga de trabajo, haga lo siguiente:
   - Haga clic en **Añadir cargas de trabajo**, si el plan todavía no se ha aplicado a ninguna carga de trabajo.
   - Haga clic en **Gestionar cargas de trabajo**, si el plan se ha aplicado a alguna carga de trabajo.
4. Seleccione una carga de trabajo de la lista y haga clic en **Agregar**.
5. Haga clic en **Guardar**.
6. Haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Desde Todos los dispositivos

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que quiera aplicar un plan de administración remota.
3. Haga clic en **Proteger** y, a continuación, en **Agregar plan**.
4. En **Seleccione un plan de la lista que figura a continuación**, seleccione **Administración remota** para ver solo los planes de administración remota.
5. Haga clic en **Aplicar**.
6. Haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Eliminación de cargas de trabajo de un plan de administración remota

Según sus necesidades, puede eliminar cargas de trabajo de un plan de administración remota.

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para eliminar cargas de trabajo de un plan de administración remota

1. En la consola de Cyber Protect, vaya a **Administración** > **Planes de administración remota**.
2. Haga clic en el plan de administración remota.
3. Haga clic en **Gestionar cargas de trabajo**.
4. Seleccione una o varias cargas de trabajo que quiera eliminar del plan de administración remota y haga clic en **Eliminar**.
5. Haga clic en **Listo**.
6. Haga clic en **Guardar**.

Acciones adicionales con planes de administración remota existentes

Desde la pantalla **Planes de administración remota**, puede realizar las siguientes acciones adicionales con los planes de administración remota: ver detalles, editar, ver las actividades, ver las alertas, renombrar, habilitar, deshabilitar, clonar, exportar, establecer como favorito, establecer como predeterminado y eliminar.

Ver detalles

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para ver los detalles de un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Ver detalles**.

Editar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para editar un plan

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Editar**.

Actividades

Pasos para ver las actividades relacionadas con un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.

2. Haga clic en **Actividades**.
3. Haga clic en una actividad para ver más información sobre ella.

Alertas

Pasos para ver las alertas

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Alertas**.

Cambiar nombre

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para cambiar el nombre de un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Cambiar nombre**.
3. Escriba el nuevo nombre del plan y haga clic en **Continuar**.

Habilitar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para habilitar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Habilitar**.

Deshabilitar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para deshabilitar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Deshabilitar**.

Clonar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para clonar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Clonar**.
3. Haga clic en **Crear**.

Exportar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para exportar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Exportar**.
   La configuración del plan se exporta en un formato JSON al equipo local.

Establecer como predeterminado

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para establecer un plan de administración remota como predeterminado

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Establecer como predeterminado**.
3. En la ventana de confirmación, haga clic en **Establecer**.
   En la pantalla **Planes de administración remota**, la etiqueta **Predeterminado** aparece junto al nombre del plan.

Establecer como favorito

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para establecer un plan de administración remota como favorito

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Añadir a favoritos**.

En la pantalla de **Planes de administración remota**, aparece un icono de estrella junto al nombre del plan.

Eliminar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para eliminar un plan de administración remota

1. En la pantalla **Planes de administración remota**, haga clic en el icono de **Más acciones** del plan de administración remota.
2. Haga clic en **Eliminar**.
3. Seleccione **Confirmo** y, a continuación, haga clic en **Eliminar**.

Problemas de compatibilidad con planes de administración remota

En algunos casos, aplicar un plan de administración remota en una carga de trabajo podría causar problemas de compatibilidad. Es posible que observe los siguientes problemas de compatibilidad:

- Planes en conflicto: este problema aparece cuando otro plan de administración remota ya se ha aplicado a la carga de trabajo, ya que solo se puede aplicar un plan de administración remota a una carga de trabajo.
- El sistema operativo es incompatible: este problema aparece cuando el sistema operativo de la carga de trabajo no es compatible.
- Agente no compatible: este problema aparece cuando la versión del agente de protección de la carga de trabajo está obsoleta y no es compatible con la funcionalidad de escritorio remoto.
- Cuota insuficiente: este problema aparece cuando no hay una cuota de servicio suficiente en el inquilino para asignarla a las cargas de trabajo seleccionadas.

Si se aplica el plan de administración remota a un máximo de 150 cargas de trabajo seleccionadas de forma individual, se le pedirá que resuelva los conflictos existentes antes de guardar el plan. Para resolver un conflicto, elimine la causa raíz o las cargas de trabajo afectadas desde el plan. Para obtener más información, consulte "Resolución de problemas de compatibilidad con planes de administración remota" (p. 1122). Si guarda el plan sin resolver los conflictos, se deshabilitará automáticamente para las cargas de trabajo no compatibles y se mostrarán alertas.

Si se aplica el plan de administración remota a más de 150 cargas de trabajo o grupos de dispositivos, primero se guardará y, después, se comprobará la compatibilidad. El plan se deshabilitará automáticamente para las cargas de trabajo incompatibles y se mostrarán las alertas.

Resolución de problemas de compatibilidad con planes de administración remota

Según la causa de los problemas de compatibilidad, puede ejecutar diferentes acciones para resolverlos como parte del proceso de creación de un nuevo plan de administración remota.

Nota
Al resolver un problema de compatibilidad mediante la eliminación de cargas de trabajo de un plan, no puede eliminar las cargas de trabajo que son parte de un grupo de dispositivos.

Pasos para resolver problemas de compatibilidad

1. Haga clic en **Revise los problemas**.
2. [Pasos para resolver problemas de compatibilidad con los planes de administración remota existentes mediante la eliminación de cargas de trabajo desde el nuevo plan]
   a. En la pestaña **Planes en conflicto**, seleccione las cargas de trabajo que desee eliminar.
   b. Haga clic en **Eliminar cargas de trabajo del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
3. [Pasos para resolver problemas de compatibilidad con los planes de administración remota mediante la deshabilitación de los planes que ya se han aplicado a las cargas de trabajo]
   a. Haga clic en **Deshabilitar los planes aplicados**.
   b. Haga clic en **Deshabilitar** y, a continuación, haga clic en **Cerrar**.
4. [Para resolver problemas de compatibilidad con sistemas operativos no compatibles]
   a. En la pestaña **Sistema operativo no compatible**, seleccione las cargas de trabajo que desee eliminar.
   b. Haga clic en **Eliminar cargas de trabajo del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
5. [Para resolver problemas de compatibilidad con agentes no compatibles mediante la eliminación de cargas de trabajo desde el plan]
   a. En la pestaña **Agentes no compatibles**, seleccione las cargas de trabajo que desee eliminar.
   b. Haga clic en **Eliminar cargas de trabajo del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
6. [Para resolver problemas de compatibilidad con agentes no compatibles mediante la actualización de la versión del agente] Haga clic en **Ir a la lista de agentes**.

   Nota
   Esta opción solamente está disponible para los administradores de clientes.

7. [Para resolver problemas de compatibilidad con una cuota insuficiente mediante la eliminación de cargas de trabajo desde el plan]
   a. En la pestaña **Cuota insuficiente**, seleccione las cargas de trabajo que desee eliminar.
   b. Haga clic en **Eliminar cargas de trabajo del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
8. [Para resolver problemas de compatibilidad con una cuota insuficiente mediante el aumento de la cuota del cliente]

Nota
Esta opción solamente está disponible para los administradores de partner.

a. En la pestaña **Cuota insuficiente**, haga clic en **Ir al portal de administración**.

b. Aumentar la cuota de servicio para el cliente.

Credenciales de la carga de trabajo

Puede añadir credenciales de administrador o que no sean de administrador de las cargas de trabajo remotas (nombre de usuario y contraseña o contraseña de VNC), guardarlas en el almacén de credenciales de la nube y utilizarlas para la autenticación automática cuando se conecte a las cargas de trabajo que administra. De este modo, en lugar de introducir esas credenciales de forma manual cada vez durante el paso de autenticación de la conexión, puede guardarlas en el almacén de credenciales una vez y asignarlas a varias cargas de trabajo, y Cliente de Connect utilizará esas credenciales cada vez que usted quiera conectarse a las cargas de trabajo de forma remota.

Nota
Las credenciales que se almacenan en el almacén de credenciales no se comparten entre los distintos niveles de inquilino. Se comparten solo en el mismo nivel de inquilino y para el mismo inquilino cliente o inquilino partner.

Esto significa que si un inquilino cliente tiene varios administradores, verán y compartirán las credenciales del almacén de credenciales. Sin embargo, los administradores de partners o de clientes de otros inquilinos no podrán ver o utilizar esas credenciales.

Agregar credenciales

Puede agregar credenciales y utilizarlas para las conexiones remotas a varias cargas de trabajo.

Pasos para agregar credenciales a una carga de trabajo y guardarlas en el Almacén de credenciales

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo para la que desee agregar credenciales.
3. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
4. Haga clic en **Agregar credenciales**.
5. En el **Almacén de credenciales**, haga clic en **Agregar credenciales**.

6. Introduzca las credenciales.

Campo	Descripción
Nombre de las credenciales	Identificador de las credenciales que se mostrarán en el almacén de credenciales.
Nombre de usuario	Nombre de usuario que se utilizará para las conexiones remotas a la carga de trabajo de destino.
Contraseña	La contraseña se utilizará para las conexiones remotas a la carga de trabajo de destino.
Contraseña de VNC	Este campo solo está disponible para el uso compartido de pantalla de Apple.

7. Haga clic en **Guardar**.

Asignación de credenciales a una carga de trabajo

Después de agregar credenciales, puede utilizarlas para autenticarse automáticamente cuando se conecte a una carga de trabajo que gestione.

Pasos para asignar las credenciales guardadas a una carga de trabajo para la autenticación automática

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
3. En la pestaña del protocolo soportado (NEAR, RDP o el uso compartido de pantalla de Apple), haga clic en **Añadir credenciales**.
4. En el **Almacén de credenciales**, seleccione las credenciales de la lista y haga clic en **Seleccionar credenciales**.

Eliminar credenciales

Puede eliminar credenciales que ya no se necesiten.

Pasos para eliminar credenciales de el almacén de credenciales

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
3. En la pestaña del protocolo admitido (NEAR, RDP o el uso compartido de pantalla de Apple),

haga clic en **Eliminar**.

4. Haga clic en **Eliminar** en la ventana de confirmación.

Anular la asignación de credenciales de una carga de trabajo

Puede anular la asignación de credenciales de una carga de trabajo, pero conservarlas en el almacén de credenciales.

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
3. En la pestaña del protocolo admitido (NEAR, RDP o el uso compartido de pantalla de Apple), haga clic en **Anular asignación**.
4. Haga clic en **Anular asignación** en la ventana de confirmación.

Trabajar con cargas de trabajo gestionadas

Las cargas de trabajo gestionadas son cargas de trabajo en las que se ha instalado el agente de Protección.

Puede realizar las siguientes acciones en las cargas de trabajo remotas gestionadas:

- conectarse a la asistencia remota o al escritorio remoto mediante NEAR en modo de control o solo visualización
- conectarse al escritorio remoto con RDP en el modo de control
- conectarse a la asistencia remota o al escritorio remoto mediante uso compartido de pantalla de Apple en modo control, solo visualización o en modo cortina
- conectarse al escritorio remoto a través del cliente web
- reiniciar, apagar, pausar, vaciar papelera de reciclaje y cierre la sesión del usuario remoto de las cargas de trabajo remotas
- transferir archivos entre su carga de trabajo y las cargas de trabajo remotas
- supervisarlos con capturas de pantalla

Nota
Las conexiones del escritorio remoto a cargas de trabajo gestionadas requieren la instalación de un agente de Protección y la aplicación de un plan de administración remota en la carga de trabajo.

Ajuste de la configuración de RDP

Puede configurar los ajustes que se aplicarán automáticamente para las conexiones RDP de control remoto a la carga de trabajo administrada.

Pasos para configurar los ajustes RDP de una carga de trabajo

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Acceda al menú **Configuración** de una de las siguientes maneras:
   - Haga clic en **Escritorio remoto** y luego en **Configuración**.
   - Haga clic en **Administrar** y luego en **Configuración**.
3. Configure los ajustes en la pestaña **RDP**.

Configuración	Descripción
Reproducción de audio	Estos ajustes habilitan o deshabilitan el redireccionamiento del sonido de la carga de trabajo remota en tu carga de trabajo local.
Grabación de audio	Estos ajustes determinan si la grabación de audio (cuando se hable al micrófono) se transferirá a la carga de trabajo remota.
Redirigir impresoras	Si selecciona este ajuste, las impresoras de su carga de trabajo estarán disponibles en la carga de trabajo remota.
Redirigir archivos	Estos ajustes definen si los archivos de la carga de trabajo local se compartirán a la carga de trabajo remota.
Profundidad del color	Estos ajustes determinan el número de colores en la imagen que transferirá RDP. Un valor más alto requiere más ancho de banda. **Color intenso**: 16 bits **Color real**: • 24 bits para conexiones RDP a través del cliente web • 32 bits para conexiones RDP a través de Cliente de Connect

4. Haga clic en el botón Cerrar.

Conexión a cargas de trabajo administradas para asistencia o escritorio remotos

Nota
La disponibilidad de los protocolos de conexión que puede utilizar para las conexiones remotas depende de la configuración del plan de administración remota y del sistema operativo de la carga de trabajo remota.

Requisitos previos

- Un plan de administración remota con el protocolo de conexión correspondiente habilitado se aplica a la carga de trabajo gestionada.
- La cuota de servicio requerida se asigna a la carga de trabajo. (La cuota de servicio se adquiere automáticamente cuando aplica un plan de administración remota a la carga de trabajo).
- [Para conexiones a través del uso compartido de pantalla de Apple] El uso compartido de pantalla de Apple está activado en la carga de trabajo de macOS.

- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para conectarse de forma remota a una carga de trabajo administrada para asistencia o escritorio remotos

1. En la consola Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo a la que desee conectarse.
3. Haga clic en **Escritorio remoto**.
   Por defecto, NEAR se selecciona como protocolo de conexión.
4. [Opcional] En la lista desplegable **Protocolo de conexión**, seleccione el protocolo de conexión que desee utilizar.
5. Haga clic en el modo de vista que quiera usar.

Protocolo	Conexiones remotas a	Modo Ver	Acción remota compatible
NEAR	Windows Linux macOS	**Controlar**: En este modo, podrá observar y ejecutar operaciones en la carga de trabajo remota. **Solo visualización**: en este modo, solo podrá observar la carga de trabajo remota.	Escritorio remoto Asistencia remota
RDP	Windows	**Controlar**: En este modo, podrá ver y ejecutar operaciones en la carga de trabajo remota. **Nota** Si RDP está desactivado en la configuración del sistema operativo de la carga de trabajo, aparecerá una ventana emergente. Utilice esta ventana para habilitar RDP para la carga de trabajo para la sesión actual o en general: • Si desea habilitar RDP para esta carga de trabajo solo para la sesión actual, seleccione **Deshabilitarlo una vez finalizada la sesión** y, a continuación, haga clic en **Permitir**. • Si desea habilitar RDP para esta carga de trabajo, haga clic en **Permitir**.	Escritorio remoto
Uso compartido de pantalla	macOS	**Controlar**: En este modo, podrá observar y ejecutar operaciones en la carga de trabajo remota.	Escritorio remoto Asistencia

Protocolo	Conexiones remotas a	Modo Ver	Acción remota compatible
de Apple		**Solo visualización**: en este modo, solo podrá observar la carga de trabajo remota. **Cortina**: disponible solo para cargas de trabajo de macOS. Si se conecta a la carga de trabajo remota en el modo cortina, la pantalla de la carga de trabajo remota se atenuará, y el usuario remoto no podrá ver sus acciones en la carga de trabajo.	remota

6. En función de si Cliente de Connect está instalado en su carga de trabajo, lleve a cabo una de las siguientes acciones:
   - Si Cliente de Connect no está instalado, descárguelo, instálelo y, a continuación, en la ventana emergente de confirmación que aparece, seleccione **Permitir**.
   - Si Cliente de Connect ya está instalado, en la ventana emergente de confirmación que aparece, haga clic en **Abrir Cliente de Connect**.
7. En la ventana **Autenticación**, seleccione una opción de autenticación y facilite las credenciales necesarias.

Nota
Si tiene credenciales asignadas a la carga de trabajo, la autenticación se llevará a cabo automáticamente y se omitirá este paso. Para obtener más información, consulte "Asignación de credenciales a una carga de trabajo" (p. 1125).

Opción de autenticación	Descripción
Con las credenciales de la carga de trabajo remota	Se le permitirá establecer la conexión remota después de proporcionar el nombre de usuario y la contraseña de un usuario administrador de la carga de trabajo remota. Esta opción está disponible para NEAR, RDP y el uso compartido de pantalla de Apple. Puede utilizar esta opción para autenticar la asistencia y el escritorio remotos.
Solicitar permiso para observar	Se le permitirá establecer la conexión remota en el modo de observación después de que el usuario que ha iniciado sesión en la carga de trabajo remota lo permita. Esta opción está disponible para NEAR y el uso compartido de pantalla de Apple.

Opción de autenticación	Descripción
	Puede utilizar esta opción para autenticar la asistencia remota.
Solicitar permiso para controlar	Se le permitirá establecer la conexión remota en el modo de control después de que el usuario que ha iniciado sesión en la carga de trabajo remota lo permita. Esta opción está disponible para NEAR y el uso compartido de pantalla de Apple. Puede utilizar esta opción para autenticar la asistencia remota.

8. Haga clic en **Conectar** y luego en la sesión que mostrar (si hay más de una sesión de usuario disponible en la carga de trabajo).
   Cliente de Connect abrirá una ventana del visor nueva en la que podrá ver el escritorio de la carga de trabajo remota. El visor tiene una barra de herramientas con acciones adicionales que puede ejecutar en la carga de trabajo remota después de establecer la conexión remota. Para obtener más información, consulte "Uso de la barra de herramientas en la ventana del Visor" (p. 1139).

Conectar a una carga de trabajo gestionada a través del cliente web

Puede establecer una conexión a escritorio remoto para una carga de trabajo administrada a través del cliente web.

Requisitos previos

- La cuota de servicio estándar se asigna a la carga de trabajo.
- Un plan de administración remota con RDP habilitado se aplica a la carga de trabajo administrada.
- Se ha habilitado RDP en la carga de trabajo administrada.
- Su buscador es compatible con HTML5.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para conectar a una carga de trabajo de forma remota a través de un cliente web

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que desee conectarse de forma remota y, a continuación, haga clic en **Escritorio remoto**>**Conectarse a través del cliente web**.
3. Introduzca el nombre de usuario y la contraseña para acceder a la carga de trabajo y haga clic en **Conectar**.

Nota
Si tiene credenciales asignadas a la carga de trabajo, la autenticación se llevará a cabo automáticamente y se omitirá este paso. Para obtener más información, consulte "Asignación de credenciales a una carga de trabajo" (p. 1125).

Transferir archivos

Puede transferir fácilmente archivos entre la carga de trabajo local y una carga de trabajo gestionada.

Requisitos previos

- Un plan de administración remota con el protocolo NEAR y la transferencia de archivos habilitados se aplica a la carga de trabajo.
- La cuota de Advanced Management se aplica a la carga de trabajo.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para transferir archivos entre la carga de trabajo local y una carga de trabajo gestionada

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo con la que desee transferir archivos.
3. Haga clic en **Administrar** y luego en **Transferir archivos**.
4. En función de si Cliente de Connect está instalado en su carga de trabajo, lleve a cabo una de las siguientes acciones:
   - Si Cliente de Connect no está instalado, descárguelo, instálelo y, a continuación, en la ventana emergente de confirmación que aparece, haga clic en **Permitir**.
   - Si Cliente de Connect ya está instalado, en la ventana emergente de confirmación que aparece, haga clic en **Abrir Cliente de Connect**.
5. En la ventana **Autenticación**, seleccione una opción de autenticación y facilite las credenciales necesarias.

Opción de autenticación	Descripción
Con las credenciales de la carga de trabajo remota	Se le permitirá establecer la conexión remota después de proporcionar el nombre de usuario y la contraseña de un usuario administrador de la carga de trabajo remota.
Solicitar permiso para transferir archivos	Se le permitirá transferir archivos después de que el usuario que ha iniciado sesión en la carga de trabajo remota lo permita.

6. En la ventana **Transferencia de archivos**, examine los archivos, arrástrelos y suéltelos en el destino que desee.

   Nota
   Los archivos de la carga de trabajo local aparecen en el panel de la izquierda, y los archivos de la carga de trabajo remota aparecen en el panel de la derecha.
   Cuando comienza una transferencia de archivos, aparece en el panel de **Tareas**.

7. [Opcional] Si desea eliminar las tareas completadas del panel de **Tareas**, haga clic en **Borrar completadas**.
8. Cuando se completen todas las transferencias, cierre la ventana.

Llevar a cabo acciones de control en cargas de trabajo gestionadas

Puede gestionar una carga de trabajo remota mediante acciones de control básico sobre ella: vaciar papelera de reciclaje, suspender, reiniciar, apagar y cierre la sesión del usuario remoto.

Requisitos previos

- La cuota de servicio estándar se aplica a la carga de trabajo.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Vaciar papelera de reciclaje

Pasos para vaciar la papelera de reciclaje en la carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Vaciar papelera de reciclaje**.
4. Seleccione la sesión de usuario para la que desee llevar a cabo la acción y haga clic en **Vaciar papelera de reciclaje**.

Suspender

Pasos para suspender una carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Suspender**.

Reiniciar

Pasos para reiniciar una carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.

3. Haga clic en **Gestionar** y, a continuación, haga clic en **Reiniciar**.
   - Para cargas de trabajo de Windows, seleccione si desea permitir que el usuario que tenga la sesión iniciada localmente en la carga de trabajo guarde los cambios antes de que se reinicie dicha carga de trabajo y, a continuación, seleccione al usuario y haga clic en **Reiniciar** de nuevo.
   - Para cargas de trabajo de macOS, seleccione si desea permitir que el usuario que tenga la sesión iniciada localmente en la carga de trabajo guarde los cambios antes de que se reinicie la carga de trabajo y, a continuación, haga clic en **Reiniciar** de nuevo.
   - Para las cargas de trabajo de Linux, haga clic en **Reiniciar**.

Apagar

Pasos para apagar una carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Apagar**.
   - Para cargas de trabajo de Windows, seleccione si desea permitir que el usuario que tenga la sesión iniciada localmente en la carga de trabajo guarde los cambios antes de que se apague la carga de trabajo, y, a continuación, seleccione al usuario y haga clic en **Apagar** de nuevo.
   - Para cargas de trabajo de macOS, seleccione si desea permitir que el usuario que tenga la sesión iniciada localmente en la carga de trabajo guarde los cambios antes de que se apague la carga de trabajo y, a continuación, haga clic en **Apagar** de nuevo.
   - Para las cargas de trabajo de Linux, haga clic en **Apagar** de nuevo.

Cierre la sesión del usuario remoto

Pasos para cerrar la sesión de usuario de una carga de trabajo remota

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo en la que desee llevar a cabo esta acción.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Cierre la sesión del usuario remoto**.
4. Seleccione el usuario del que desea cerrar sesión y, a continuación, haga clic en **Cerrar sesión**.

Supervisión de cargas de trabajo mediante la transmisión de captura de pantalla

Puede supervisar el estado de una carga de trabajo con la función de transmisión de captura de pantalla.

Requisitos previos

- Un plan de administración remota con la función de transmisión de captura de pantalla habilitada se aplica a la carga de trabajo.

- La versión del agente de protección está actualizada y es compatible con la función de transmisión de capturas de pantalla.
- La cuota de servicio de Advanced Management se aplica a la carga de trabajo.
- La carga de trabajo está en línea.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Supervisión de una carga de trabajo mediante la transmisión de captura de pantalla

Pasos para supervisar una carga de trabajo mediante la transmisión de captura de pantalla

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Transmisión de captura de pantalla**.
2. Haga clic en la carga de trabajo que quiera supervisar.
3. Seleccione la sesión de usuario.
4. Seleccione la pantalla.
5. Seleccione la tasa de actualización para hacer una nueva captura de pantalla del escritorio.
6. Seleccione la calidad de la imagen.
7. Para descargar la captura de pantalla, haga clic en el icono de descarga.

Captura de pantalla de una carga de trabajo

Pasos para hacer una captura de pantalla de una carga de trabajo gestionada

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Equipos con agentes**.
2. Haga clic en la carga de trabajo de la que desee hacer una captura de pantalla.
3. Haga clic en **Gestionar** y, a continuación, haga clic en **Hacer captura del escritorio**.
   La pantalla **Transmisión de captura de pantalla** se abrirá con la carga de trabajo preseleccionada. Según la configuración del plan de administración remota que se aplica a la carga de trabajo, verá la captura de pantalla o la verá después de que el usuario de la carga de trabajo remota apruebe la solicitud.

Observar varias cargas de trabajo gestionadas de manera simultánea

Puede observar los escritorios de varias cargas de trabajo remotas de manera simultánea en una sola ventana.

Nota
El número de escritorios que puede ver de manera simultánea en la ventana depende del tamaño de su monitor.

Requisitos previos

- NEAR o el Uso compartido de la pantalla están habilitados en los planes de administración remota que se aplican a las cargas de trabajo.
- La cuota de servicio de Advanced Management se aplica a la carga de trabajo.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para observar varias cargas de trabajo de manera simultánea

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Seleccione las cargas de trabajo que desea observar.
3. Haga clic en **Vista múltiple**.
4. En función de si Cliente de Connect está instalado en su carga de trabajo, lleve a cabo una de las siguientes acciones:
   - Si Cliente de Connect no está instalado, descárguelo, instálelo y, a continuación, en la ventana emergente de confirmación que aparece, seleccione **Permitir**.
   - Si Cliente de Connect ya está instalado, en la ventana emergente de confirmación que aparece, haga clic en **Abrir Cliente de Connect**.
5. En la ventana **Autenticación**, seleccione una opción de autenticación y facilite las credenciales necesarias.

Opción de autenticación	Descripción
Con las credenciales de la carga de trabajo remota	Se le permitirá establecer la conexión remota después de proporcionar el nombre de usuario y la contraseña de un usuario administrador en la carga de trabajo remota.
Solicitar permiso para observar	Se le permitirá establecer la conexión remota en el modo de observación después de que el usuario que ha iniciado sesión en la carga de trabajo remota lo permita.

6. Si desea utilizar el mismo método de autenticación y las credenciales cuando se conecte a todas las cargas de trabajo remotas que ha seleccionado en el paso 2, seleccione **Usar en otros equipos**.
7. Haga clic en **Conectar**.

   En la barra de herramientas de la ventana de vista múltiple, puede seleccionar un modo de visualización en el que conectarse a una carga de trabajo. Esta acción abrirá una ventana del Visor independiente para esa carga de trabajo.

Nota
Si alguna de las cargas de trabajo seleccionadas está fuera de línea o tiene una versión obsoleta del agente instalada, no se mostrará en la ventana de vista múltiple.
Todas las conexiones de vista múltiple a cargas de trabajo remotas están en el modo **Solo visualización**.

Trabajar con cargas de trabajo sin gestionar

Las cargas de trabajo sin gestionar son cargas de trabajo en las que no se ha instalado el agente de Protección.

Puede realizar las siguientes acciones en las cargas de trabajo remotas sin gestionar:

- conectarse a la asistencia remota mediante Acronis Asistencia rápida
- conectarse a la asistencia o el escritorio remotos mediante una dirección IP
- transferir archivos entre su carga de trabajo y la carga de trabajo remota mediante Asistencia rápida

Nota
Para conectarse de forma remota a cargas de trabajo no administradas con Asistencia rápida, asegúrese de que:

- El paquete de Advanced Management está activado para su inquilino de cliente.
- La aplicación Asistencia rápida se ejecuta en la carga de trabajo remota a la que desee conectarse.

Conectar a cargas de trabajo no administradas a través de Acronis Asistencia rápida

Puede utilizar la función Asistencia rápida para conectarse de forma remota bajo demanda a las cargas de trabajo no gestionadas y proporcionar ayuda a tiempo.

Requisitos previos

- El paquete de Advanced Management se asigna a su inquilino de cliente.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.
- El usuario remoto ha facilitado el ID de la carga de trabajo y el código de acceso de Asistencia rápida.
- El usuario remoto ha descargado y ejecutado Acronis Asistencia rápida.

Pasos para conectarse a una carga de trabajo para asistencia remota mediante Asistencia rápida

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Asistencia rápida**.
3. En la ventana **Asistencia rápida**, introduzca el ID de carga de trabajo que le proporcionó el usuario final y, a continuación, seleccione **Conectar**.
4. Haga clic en **Conectar**.
5. En función de si Cliente de Connect está instalado en su carga de trabajo, lleve a cabo una de las siguientes acciones:
   - Si Cliente de Connect no está instalado, descárguelo, instálelo y, a continuación, en la ventana emergente de confirmación que aparece, seleccione **Permitir**.
   - Si Cliente de Connect ya está instalado, en la ventana emergente de confirmación que aparece, haga clic en **Abrir Cliente de Connect**.
6. En la ventana **Autenticación**, introduzca el código de acceso.
7. Cliente de Connect abrirá una ventana del visor nueva en la que podrá ver el escritorio de la carga de trabajo remota. El visor tiene una barra de herramientas con acciones adicionales que puede ejecutar en la carga de trabajo remota después de establecer la conexión remota. Para obtener más información, consulte "Uso de la barra de herramientas en la ventana del Visor" (p. 1139).

Conectar a cargas de trabajo gestionadas mediante una dirección IP

Si hay una carga de trabajo no administrada en su LAN, puede conectarse a ella para obtener asistencia o control remotos mediante su dirección IP. Esta conexión no requiere acceso a Internet.

Requisitos previos

- El paquete de Advanced Management se asigna a su inquilino de cliente.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.

Pasos para conectarse a una carga de trabajo para asistencia o escritorio remotos mediante su dirección IP

1. En la consola de Cyber Protect, vaya a **Todos los dispositivos**.
2. Haga clic en **Asistencia rápida**.
3. Haga clic en la pestaña **Vía dirección IP**.
4. Introduzca la dirección IP y el puerto de la carga de trabajo.
5. Seleccione un protocolo de conexión RDP (cargas de trabajo de Windows) o el uso compartido de pantalla de Apple (para cargas de trabajo de macOS), según el sistema operativo de la carga de trabajo remota.

Nota
Las conexiones a través de RDP admiten la acción de escritorio remoto, y las conexiones a través del uso compartido de pantalla de Apple admiten tanto la acción de escritorio remoto como la de asistencia remota.

6. Haga clic en **Conectar**.
7. En la ventana **Autenticación**, facilite las credenciales necesarias.

Para las conexiones a través del uso compartido de pantalla de Apple, Cliente de Connect abrirá una nueva ventana de visualización en la que podrá ver el escritorio de la carga de trabajo remota. El visor tiene una barra de herramientas con acciones adicionales que podrá realizar en la carga de trabajo remota una vez se establezca la conexión remota. Para obtener más información, consulte "Uso de la barra de herramientas en la ventana del Visor" (p. 1139).

Transferir archivos mediante Acronis Asistencia rápida

Puede utilizar la función Asistencia rápida para transferir archivos entre su carga de trabajo y las cargas de trabajo sin gestionar.

Requisitos previos

- El paquete de Advanced Management se asigna a su inquilino de cliente.
- La autenticación de doble factor está habilitada en su cuenta de usuario en Acronis Cyber Protect Cloud.
- El usuario remoto ha descargado y ejecutado Acronis Asistencia rápida.
- El usuario remoto ha facilitado el ID del equipo de todo el contenido del equipo y el código de acceso de Asistencia rápida.

Pasos para transferir archivos a una carga de trabajo con Asistencia rápida

1. En la consola de Cyber Protect, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en **Asistencia rápida**.
3. En la ventana **Asistencia rápida**, introduzca el ID de la carga de trabajo que el usuario final le proporcionó y seleccione **Transferencia de archivos**.
4. Haga clic en **Conectar**.
5. En función de si Cliente de Connect está instalado en su carga de trabajo, lleve a cabo una de las siguientes acciones:
   - Si Cliente de Connect no está instalado, descárguelo, instálelo y, a continuación, en la ventana emergente de confirmación que aparece, seleccione **Permitir**.
   - Si Cliente de Connect ya está instalado, en la ventana emergente de confirmación que aparece, haga clic en **Abrir Cliente de Connect**.
6. En la ventana **Autenticación**, introduzca el código de acceso.

7. En la ventana **Transferencia de archivos**, examine los archivos, arrástrelos y suéltelos en el destino que desee.

   Nota
   Los archivos de la carga de trabajo local aparecen en el panel de la izquierda, y los archivos de la carga de trabajo remota aparecen en el panel de la derecha.
   Cuando comienza una transferencia de archivos, aparece en el panel de **Tareas**.

8. [Opcional] Si desea eliminar las tareas completadas del panel de **Tareas**, haga clic en **Borrar completadas**.
9. Cuando se completen todas las transferencias, cierre la ventana.

Uso de la barra de herramientas en la ventana del Visor

Después de conectarse a una carga de trabajo remota, puede utilizar la barra de herramientas de la ventana del visor para ejecutar rápidamente las distintas acciones.

Icono	Descripción
	**Tamaño real** Adapta el escritorio de la carga de trabajo remota para que un píxel del escritorio remoto se corresponda con un píxel de la ventana del visor.
	**Zoom para ajustar** Adapta el escritorio de la carga de trabajo remota para ajustarlo a la ventana del visor.
	**Bloquear** y **Desbloquear pantalla** Muestra un marcador de posición en la pantalla de la carga de trabajo remota para que el usuario remoto no vea sus acciones.
	**Hacer captura** Guarde la imagen de escritorio del servidor remoto en un archivo local.
	**Seleccione la pantalla** Seleccione la pantalla de la carga de trabajo remota que quiera ver y la resolución deseada. Disponible para conexiones a través del uso compartido de pantalla de Apple con macOS y conexiones NEAR con cualquier sistema operativo.
	**Calidad de la imagen** Ajusta la calidad de la imagen de la pantalla remota desde el blanco y

Icono	Descripción
	negro a la mejor posible en las conexiones a través del uso compartido de pantalla de Apple.
	**Calidad de la imagen NEAR** Ajusta la calidad o la proporción de rendimiento de las conexiones NEAR. El lado izquierdo del control deslizante (Suave) da prioridad al rendimiento sobre la calidad de imagen, el derecho (Nítido) supone la mejor calidad de la pantalla del escritorio remoto, pero probablemente peor rendimiento.
	**Enviar Ctrl+Alt+Supr** Envía una secuencia Ctrl + Alt + Suprimir a la carga de trabajo remota. Disponible para cargas de trabajo de Windows y Linux.
	**Transferencia de archivos** Abre la ventana del administrador de archivos para intercambiar archivos entre la carga de trabajo remota y la local. Disponible para conexiones NEAR.
	**Anclar la barra de herramientas** Desactiva la ocultación automática de la barra de herramientas del visor. Disponible para cargas de trabajo de Windows.
	**Pantalla completa** Cambia al modo de pantalla completa y adapta la carga de trabajo remota para que llene la pantalla local por completo. Disponible para cargas de trabajo de Windows.
	**Cerrar** Cierra la ventana del Visor y finaliza la sesión del control remoto. Disponible para cargas de trabajo de Windows.

Según el tipo de conexión, puede que hayan opciones adicionales disponibles cuando haga clic en el icono **Otros**.

Opción	Descripción
Iniciar grabación/Detener la grabación	Grabe la sesión de escritorio remoto actual. Las grabaciones de la sesión se guardan como archivos .crec en la carga de trabajo local. Puede abrir archivos .crec con Acronis Cliente de Connect.

Opción	Descripción
	Disponible para conexiones NEAR
Sincronización automática del portapapeles	Cuando esta opción esté activada, el cliente sincronizará automáticamente su portapapeles local y el portapapeles del equipo remoto. Disponible para conexiones NEAR y a través del uso compartido de pantalla de Apple
Enviar portapapeles **Obtener portapapeles**	**Enviar portapapeles** reemplaza el contenido del portapapeles del equipo remoto con el contenido del portapapeles local. **Obtener portapapeles** transfiere el contenido del portapapeles del equipo remoto al portapapeles local.
Teclado inteligente/Teclas Raw/Teclas Raw con todos los accesos directos	Cambia el modo de entrada del teclado para la conexión actual. **Teclado inteligente**: el cliente transmite los códigos Unicode de los símbolos tecleados a nivel local al equipo remoto **Teclas Raw**: el cliente utiliza los códigos raw de los botones del teclado que presiona. **Teclas Raw con todos los accesos directos**: el cliente deshabilita los accesos directos del sistema local para que se transmitan también al sistema operativo remoto.
Enfoque del teclado al mantener el ratón	Cuando se habilita, el cliente solo captura la entrada del teclado mientras el cursor del ratón local se sitúa encima de la ventana del Visor. Cuando se deshabilita, el cliente captura su teclado siempre que la ventana esté activa.
Mostrar información de conexión/Ocultar la información de conexión	Cuando se seleccione **Mostrar información de conexión**, aparecerá un pequeño panel de información sobre la pantalla del escritorio remoto, que mostrará la información más esencial sobre la conexión actual.
Sonido remoto	Permite que el cliente redirija el sonido desde el equipo remoto al local. Disponible para conexiones NEAR
Preferencias	Configure los ajustes de Cliente de Connect. Para obtener más información, consulte "Configuración de los ajustes de Cliente de Connect" (p. 1142).

Grabar y reproducir sesiones remotas

Puede grabar una sesión remota a través de NEAR en Acronis Cliente de Connect.

Para grabar una sesión remota

1. En la barra de herramientas del Visor en Cliente de Connect, haga clic en **Otro** y seleccione **Iniciar Grabación**.
2. Seleccione un nombre y una ubicación para el registro.

   Por defecto, se asignará un nombre al archivo con la fecha y hora actuales y se ubicará en la carpeta **Documentos** en el directorio principal del usuario actual. Mientras la grabación esté activa, en la barra de herramientas del **Visor** verá un círculo rojo parpadeante en la esquina superior derecha de la pantalla remota y el temporizador de grabación.
3. Para detener la grabación, haga clic en **Otro** y luego en **Detener la grabación**. En un Mac, también puede hacer clic en **Detener** en la barra de herramientas.

   Todos los archivos .crec creados por Acronis Cliente de Connect se abrirán por defecto con Acronis Cliente de Connect.

Para reproducir una grabación

1. Localice un archivo de grabación.
2. Ábralo.

   El reproductor de grabaciones de Acronis Cliente de Connect se abre. Tenga en cuenta que no es posible desplazarse por la grabación. Para encontrar un momento determinado de la grabación, espere hasta que el reproductor lo alcance.
3. [Opcional] Para ajustar la velocidad de reproducción, utilice los iconos **<<** y **>>** en la sección de controles de reproducción.

   La grabación se almacena como una secuencia de eventos transmitidos desde y hacia el servidor remoto durante una conexión. Esto asegura la mejor calidad posible de la grabación con un tamaño de archivo mínimo. Sin embargo, esto también significa que no es posible navegar por la grabación. En este momento tampoco es posible convertir las grabaciones a un formato de vídeo.

Configuración de los ajustes de Cliente de Connect

Después de instalar Cliente de Connect en su carga de trabajo, puede configurar los ajustes según sus preferencias.

Pasos para configurar los ajustes de Cliente de Connect

1. En el menú de inicio, busque **Cliente de Connect** e inícielo.
2. Configure los ajustes en la pestaña **General**.

Opción	Descripción
Escribir registros detallados	Seleccione esta opción para permitir a Cliente de Connect escribir registros detallados. Si está deshabilitado, el cliente solo escribirá información general en el archivo de registro.
Configuración del proxy	Seleccione si desea utilizar el proxy del sistema predeterminado o configurar un proxy SOCKSS personalizado.

3. Configure los ajustes en la pestaña **Visor**.

Opción	Descripción
Solicitar confirmación al cerrar un visor	Seleccione esta opción si desea que Cliente de Connect muestre un mensaje de confirmación cuando intente cerrar la ventana del Visor para evitar el cierre accidental.
Al minimizar	Seleccione si desea suspender la actividad del Visor al minimizar para reducir la carga de la CPU.
Al maximizar	Seleccione si desea habilitar el modo de pantalla completa al maximizar.
Transferencia de portapapeles	Habilite la visualización del indicador de transferencia del Portapapeles en la ventana del Visor cada vez que copie o pegue texto e imágenes.
Modo teclado	Habilite la visualización del indicador de modo de Entrada en el título de la ventana del Visor cuando los eventos del ratón y el teclado se envíen al equipo remoto.
Portapapeles	Seleccione **Sincronizar automáticamente el portapapeles** para habilitar la sincronización automática del portapapeles cuando esté disponible.
Enviar eventos de teclado	Escoja si desea utilizar la entrada de su teclado local siempre que la ventana del Cliente de Connect esté activa o solo cuando el puntero del ratón local esté sobre ella.
Color en segundo plano del Visor	Cambie el color en segundo plano de la ventana del Visor.
Volver a conectar automáticamente	Seleccione **Habilitar para volver a conectar automáticamente** si desea que Cliente de Connect vuelva a establecer la conexión automáticamente si se ha interrumpido.
H.264	Puede deshabilitar los decodificadores de hardware.
Cerrar cuando esté inactiva	Seleccione el intervalo de tiempo de inactividad después del cual cerrar la ventana del Visor.

4. Configure los ajustes en la pestaña **Teclado**.

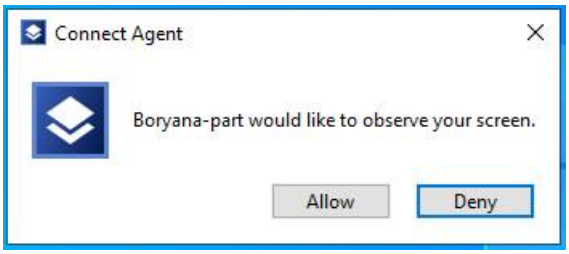
Opción	Descripción
Asignaciones de modificadores	Cambie el comportamiento de las claves del modificador con un menú emergente. Estos ajustes se almacenan de forma independiente para las conexiones NEAR, RDP y el uso compartido de pantalla de Apple.
Modo de entrada	Para cada tipo de conexión (seleccionada en el encabezado del panel), seleccione el modo de entrada predeterminado del teclado.

5. Haga clic en **Aceptar**.

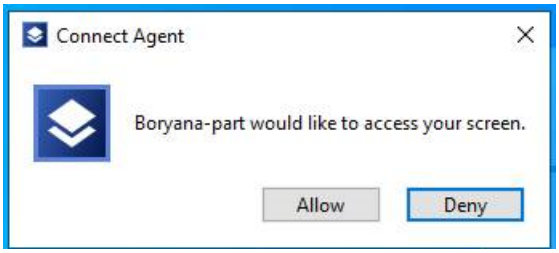
Los notificadores del escritorio remoto

El Agente de Connect muestra cuadros de diálogo de acción (notificadores) en el escritorio de la carga de trabajo remota en los siguientes casos:

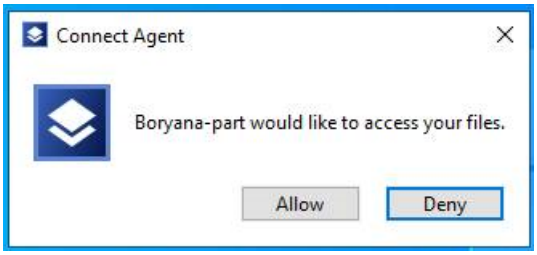
- cuando intenta conectarse a la carga de trabajo de forma remota pidiendo permiso para observar. El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede permitir o denegar la solicitud.



- cuando intenta conectarse a la carga de trabajo de forma remota pidiendo permiso para controlar. El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede permitir o denegar la solicitud.



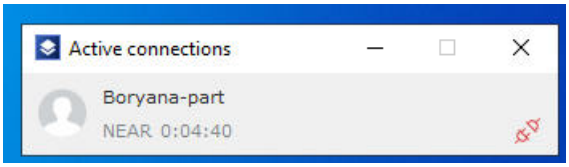
- cuando intenta intercambiar archivos entre su carga de trabajo y la carga de trabajo remota mediante la solicitud de permiso para transferir archivos. El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede permitir o denegar la solicitud.



Cuando establece una conexión a escritorio remoto con una carga de trabajo, el usuario que ha iniciado sesión en la carga de trabajo verá un notificador de conexión diferente que contiene la siguiente información:

- nombre del usuario que está conectado de forma remota
- protocolo de conexión que se utiliza para establecer la conexión remota
- duración de la conexión remota

El usuario que ha iniciado sesión en la carga de trabajo remota de forma local puede terminar la conexión en cualquier momento haciendo clic en el icono **Desconectar** o el icono **Cerrar**.



Supervisión del estado y el rendimiento de las cargas de trabajo

Puede supervisar los parámetros del sistema y el estado de las cargas de trabajo de su organización. Si un parámetro está fuera de la normal, se le notificará inmediatamente y podrá resolver el problema rápidamente. También puede configurar alertas personalizadas y acciones de respuesta automáticas. Estas acciones se ejecutarán de forma automática para resolver anomalías en el comportamiento de las cargas de trabajo.

Nota
La funcionalidad de supervisión requiere la instalación de la versión 15.0.35324 o posterior del agente de Protección en las cargas de trabajo.

Planes de supervisión

Para iniciar la supervisión de los parámetros de rendimiento, hardware, software, sistema y seguridad de sus cargas de trabajo gestionadas, aplique un plan de supervisión en estas. Los planes de supervisión consisten en diferentes monitores que puede habilitar y configurar. Algunos monitores admiten el tipo de supervisión basado en anomalías. Para obtener más información acerca de los planes de supervisión, consulte "Planes de supervisión" (p. 1181). Para obtener más información acerca de los monitores disponibles que puede configurar en los planes de supervisión, consulte "Monitores configurables" (p. 1147).

Si el agente no puede recopilar datos de una carga de trabajo por algún motivo, el sistema generará una alerta.

Tipos de supervisión

Debe configurar el tipo de supervisión para cada monitor que habilite en el plan. El tipo de supervisión determina el algoritmo que el monitor utilizará para estimar el comportamiento normal y las desviación de la carga de trabajo. Hay dos tipos de supervisión: basada en umbrales y basada en anomalías. Algunos monitores admiten solo el tipo de supervisión basado en umbrales.

La supervisión basada en umbrales hace un seguimiento de los valores de los parámetros para ver si están por encima o por debajo del valor del umbral que configura. Con este tipo de supervisión, usted debe definir los valores de umbral correctos para las cargas de trabajo. El sistema determina el comportamiento normal según estos valores de umbral estáticos y sin tener en cuenta otras condiciones específicas que pueden causar el comportamiento. Por este motivo, la supervisión basada en umbrales podría ser menos precisa que la basada en anomalías.

La supervisión basada en anomalías utiliza modelos de aprendizaje automático para crear el patrón de comportamiento normal para una carga de trabajo y detectar comportamientos anormales. Para obtener más información, consulte "Supervisión basada en anomalías" (p. 1147).

Supervisión basada en anomalías

La supervisión basada en anomalías utiliza modelos de aprendizaje automático para crear el patrón de comportamiento normal para una carga de trabajo y detectar anomalías (picos inesperados en los datos de series temporales) en el comportamiento de la carga de trabajo. Cuando se activa este tipo de supervisión, el sistema crea un modelo y empieza a formarse a sí mismo y a ajustar el modelo a la carga de trabajo específica según los datos que recopila de la carga de trabajo. Esto significa que, al principio del periodo de formación, posiblemente los datos no sean completamente precisos. Para crear un modelo de confianza se necesitan al menos tres semanas de formación del modelo. A medida que el sistema recopile más datos y analice los conjuntos de datos históricos, perfeccionará el modelo progresivamente y creará los umbrales dinámicos superior e inferior para cada métrica de la carga de trabajo. Este tipo de supervisión es más flexible en comparación a la basada en umbrales, ya que el sistema supervisa los valores de los parámetros y su contexto. Por ejemplo, puede ser normal que una carga de trabajo específica tenga una carga mayor a determinadas horas del día. Un tipo de supervisión basada en umbrales lo interpretaría erróneamente como un comportamiento anómalo y activaría una alerta.

Puede restablecer los modelos de aprendizaje automático de una carga de trabajo. En este caso, el sistema eliminará todos los datos y modelos de los monitores aplicados a la carga de trabajo. Para obtener más información, consulte "Restablecimiento de los modelos de aprendizaje automático" (p. 1193).

Plataformas compatibles con la supervisión

La función de supervisión es compatible con los siguientes sistemas operativos.

Versiones de Windows compatibles	Versiones de macOS compatibles
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura)

Monitores configurables

La funcionalidad de supervisión es compatible con los siguientes monitores, divididos en seis categorías: hardware, rendimiento, software, sistema, seguridad y personalizado.

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
Hardware					
Espacio de disco	Supervisa el espacio libre en una unidad específica de la carga de trabajo.	Windows macOS	1 minuto	Sí	Protección estándar
Temperatura de CPU	Supervisa la temperatura de la CPU.	Windows macOS	30 seg	Sí	Advanced Management
Temperatura de GPU	Supervisa la temperatura de la GPU.	Windows macOS	30 seg	Sí	Advanced Management
Cambios del hardware	Supervisa los cambios de hardware, como añadir, eliminar o sustituir hardware en una carga de trabajo	Windows macOS	24 horas	No	Protección estándar
Rendimiento					
Uso de la CPU	Supervisa el uso total de la CPU (por todas las CPU de la carga de trabajo).	Windows macOS	30 seg	Sí	Advanced Management
Uso de la memoria	Supervisa el uso de la memoria total (por todas las ranuras de memoria de la carga de	Windows macOS	30 seg	Sí	Advanced Management

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
	trabajo).				
Velocidad de transferencia del disco	Supervisa la velocidad de lectura y escritura de cada disco físico de la carga de trabajo.	Windows macOS	30 seg	Sí	Advanced Management
Uso de la red	Supervisa el tráfico de entrada y salida para cada adaptador de red de la carga de trabajo.	Windows macOS	30 seg	Sí	Advanced Management
Uso de la CPU por proceso	Supervisa el uso que hace determinado proceso de la CPU.	Windows macOS	30 seg	No	Advanced Management
Uso de la memoria por proceso	Supervisa el uso de la memoria del proceso seleccionado.	Windows macOS	30 seg	No	Advanced Management
Velocidad de transferencia del disco por proceso	Supervisa la velocidad de lectura y escritura del proceso seleccionado.	Windows macOS	30 seg	No	Advanced Management
Uso de la red por proceso	Supervisa el tráfico de entrada y salida del proceso	Windows macOS	30 seg	No	Advanced Management

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
	seleccionado.				
Software					
Estado del servicio de Windows	Supervisa el estado del servicio de Windows seleccionado (En ejecución o detenido).	Windows	30 seg	No	Advanced Management
Estado del proceso	Supervisa el estado del proceso seleccionado (En ejecución o detenido).	Windows macOS	30 seg	No	Advanced Management
Software instalado	Supervisa la instalación, actualización o eliminación de aplicaciones de software.	Windows macOS	24 horas	No	Advanced Management
Sistema					
Último reinicio del sistema	Supervisa cuándo se ha reiniciado la carga de trabajo.	Windows macOS	1 hora	No	Protección estándar
Registro de eventos de Windows	Supervisa los eventos específicos de datos esenciales para el negocio en los registros de eventos de Windows.	Windows	10 min	No	Advanced Management

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
Tamaño de archivos y carpetas	Supervisa el tamaño total de los archivos o carpetas seleccionados.	Windows macOS	10 min	No	Protección estándar
Seguridad					
Estado de Windows Update	Supervisa el estado de actualización de Windows de la carga de trabajo y si se han instalado las actualizaciones más recientes.	Windows	15 min	No	Advanced Management
Estado del firewall	Supervisa el estado del cortafuegos integrado o de terceros que está instalado en la carga de trabajo.	Windows macOS	5 min	No	Advanced Management
Estado de software antimalware	Supervisa el estado del software antimalware integrado o de terceros que está instalado en la carga de trabajo.	Windows macOS	5 min	No	Advanced Management
Error al iniciar sesión	Supervisa los intentos de inicio de sesión sin éxito de la	Windows	1 hora	No	Advanced Management

Monitor	Descripción	Sistemas operativos compatibles	Frecuencia de la recopilación de datos	Soporte para la supervisión basada en anomalías	Disponibilidad en la protección estándar o en Advanced Management
	carga de trabajo.				
Estado de AutoRun	Supervisa si la función AutoRun está activada en el soporte de almacenamiento extraíble.	Windows	1 hora	No	Advanced Management
Personalizado					
Personalizado	Supervisa los objetos personalizados mediante la ejecución de secuencias de comandos.	Windows macOS	personalizado	No	Advanced Management

Configuración del monitor de espacio en disco

Espacio en disco supervisa el espacio libre en una unidad específica de la carga de trabajo.

Nota
A la hora de calcular el espacio, el monitor utiliza bytes binarios (1024 bytes por KB, 1024 KB por MB y 1024 MB por GB) para las cargas de trabajo de Windows y macOS.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Dispositivo	La unidad que quiere supervisar. Los valores disponibles son los siguientes: • **Unidad del sistema**: Este es el valor predeterminado. • **Cualquier unidad**
Operador	El operador es una función condicional que define cómo definir el

Configuración	Descripción
	rendimiento del parámetro. Los valores disponibles son los siguientes: • **Menos de**: Este es el valor predeterminado. • **Menor o igual que**
Umbral de espacio libre en disco	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-100 (%). El valor predeterminado es 20.
Incluir unidades extraíbles	Este parámetro está disponible si el valor **Dispositivo** es **Cualquier unidad**. Seleccione este parámetro si desea añadir unidades extraíbles, como unidades flash USB, para la supervisión. De manera predeterminada, se deshabilita la configuración.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 30.
Supervisión basada en anomalías	
Dispositivo	La unidad que quiere supervisar. Los valores disponibles son los siguientes: • **Unidad del sistema**: Este es el valor predeterminado. • **Cualquier unidad**
Modelo de periodo de formación	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos.

Configuración	Descripción
	De manera predeterminada, se selecciona la configuración.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. El valor predeterminado es 30 minutos.

Configuración de la supervisión de temperatura de la CPU

La temperatura de la CPU supervisa la temperatura de la CPU de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Se ha excedido la temperatura de la CPU (°C)	El valor máximo del parámetro supervisado. Si se supera el valor, el sistema genera una alerta. Escriba un valor entero (°C). El valor predeterminado es 80.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Modelo de periodo de formación	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia.

Configuración	Descripción
	2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 15.

Configuración de la supervisión de temperatura de la GPU

La temperatura de la GPU supervisa la temperatura de la GPU de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Se ha excedido la temperatura de la GPU	El valor máximo del parámetro supervisado. Si se supera el valor, el sistema detecta una anomalía. Escriba un valor entero (°C). El valor predeterminado es 80.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Modelo de periodo de	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y

Configuración	Descripción
formación	creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado.

Configuración	Descripción
	Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 15.

Configuración del monitor de cambios de hardware

Los cambios de hardware supervisan los cambios de hardware, como añadir, eliminar o sustituir hardware en una carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Componentes del hardware	Seleccione uno o varios componentes de hardware en los que desee supervisar los cambios. Los valores disponibles son los siguientes: • **Todos**: Este es el valor predeterminado. • **Placa base** • **CPU** • **RAM** • **Disco** • **GPU** • **Adaptador de red**
Qué supervisar	Especifique los cambios para los que desee supervisar los componentes de hardware seleccionados. Puede seleccionar varios elementos de la lista. Los valores disponibles son los siguientes: • **Cualquier cambio**: Este es el valor predeterminado. • **Componentes recién añadidos** • **Componentes remplazados** • **Componentes eliminados**

Configuración de la supervisión del uso de la CPU

El **Uso de la CPU** supervisa el uso total de la CPU (uso del procesador) de la carga de trabajo. Si la carga de trabajo tiene varias CPU, el uso total de la CPU será la suma del uso de la CPU para cada CPU.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Operador	El operador es una función condicional que define cómo definir el

Configuración	Descripción
	rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de uso de la CPU	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-100 (%). El valor predeterminado es 90.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Modelo de periodo de formación	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la

Configuración	Descripción
	formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 15.

Configuración de la supervisión del uso de la memoria

Uso de memoria supervisa el uso de la memoria total de todos los módulos de memoria de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro.

Configuración	Descripción
	Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de uso de la memoria	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-100 (%). El valor predeterminado es 90.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Modelo de periodo de formación	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de

Configuración	Descripción
	formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 30 minutos.

Configuración de la supervisión de la velocidad de transferencia del disco

Velocidad de transferencia de disco supervisa la velocidad de lectura y escritura de cada disco físico de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Qué supervisar	Seleccione la velocidad que quiere supervisar. Los valores disponibles son los siguientes:

Configuración	Descripción
	• **Velocidad de lectura y velocidad de escritura**. Este es el valor predeterminado. • **Velocidad de lectura** • **Velocidad de escritura**
Operador de velocidad de lectura	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de velocidad de lectura	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo de velocidad de lectura	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Operador de velocidad de escritura	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de velocidad de escritura	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo de velocidad de escritura	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

Configuración	Descripción
Supervisión basada en anomalías	
Modelo de periodo de formación	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Qué supervisar	Seleccione la velocidad que quiere supervisar. Los valores disponibles son los siguientes: • **Velocidad de lectura y velocidad de escritura**. Este es el valor predeterminado. • **Velocidad de lectura** • **Velocidad de escritura**
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia.

Configuración	Descripción
	2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar. • **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía (velocidad de lectura)	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 25.
Duración de la anomalía (velocidad de escritura)	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 25.

Configuración del monitor de uso de red

El **uso de red** supervisa el tráfico de entrada y salida para cada adaptador de red de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Supervisión basada en umbrales	
Dirección del tráfico	La dirección del tráfico que quiere supervisar. Los valores disponibles son los siguientes: • **Tráfico entrante y saliente**. Este es el valor predeterminado. • **Tráfico de entrada** • **Tráfico de salida**
Operador de tráfico de entrada	El operador es una función condicional que define cómo definir el rendimiento del parámetro.

Configuración	Descripción
	Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de tráfico de entrada	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo del tráfico de entrada	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Operador del tráfico de salida	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de tráfico de salida	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo del tráfico de salida	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Supervisión basada en anomalías	
Modelo de periodo de formación	El periodo durante el cual el sistema formará a los modelos de aprendizaje automático según los datos que recopilen los agentes y creará patrones de comportamiento normales de la carga de trabajo. Cuanto mayor sea el periodo de formación del modelo, más preciso será el patrón de comportamiento a largo plazo que cree el sistema. Se recomienda que el periodo mínimo de formación del modelo sea de

Configuración	Descripción
	veintiún días. Escriba un valor entero (días). El valor predeterminado es 21.
Reciba alertas de anomalías durante el periodo de formación	Si selecciona este parámetro, recibirá alertas sobre anomalías durante el periodo de formación del modelo. Estas alertas pueden ser falsas, ya que los modelos siguen formándose y podrían no ser lo suficientemente precisos. De manera predeterminada, se selecciona la configuración.
Dirección del tráfico	• **Tráfico entrante y saliente**. Este es el valor predeterminado. • **Tráfico de entrada** • **Tráfico de salida**
Nivel de confidencialidad	El nivel de sensibilidad actúa como filtro preliminar de anomalías si los valores se encuentran en un intervalo específico. Este filtro opera de forma independiente desde el algoritmo de detección de anomalías. Su objetivo es que el algoritmo de detección de anomalías deje de procesar las anomalías que están dentro de un intervalo especificado. Durante el periodo de formación: 1. El algoritmo se forma mediante los datos recopilados durante la formación. 2. El algoritmo lleva a cabo la detección de anomalías en los datos de formación. 3. Se aplica un proceso de filtrado basado en la desviación media y estándar. 4. Se filtran las anomalías que existen en un intervalo especificado. 5. A partir de los puntos de datos anómalos restantes, se selecciona la anomalía de menor nivel. Este nivel (un número decimal entre 0 y 1) se registra en el modelo. Durante la predicción: 1. El algoritmo predice anomalías en los datos de inferencia. 2. Las anomalías previstas se filtran según la desviación media y estándar y el nivel de confidencialidad. 3. Las anomalías restantes también se filtran según este principio: los valores por encima del nivel del umbral se consideran una anomalía, mientras que los valores por debajo del nivel del umbral se consideran comportamiento normal. Los valores disponibles son los siguientes: • **Bajo**: el nivel bajo equivale al valor medio y al valor de desviación estándar. • **Normal**: es el valor predeterminado. El nivel normal equivale al valor medio y a dos veces el valor de desviación estándar.

Configuración	Descripción
	• **Alto**: equivale al valor medio y a tres veces el valor de desviación estándar.
Duración de la anomalía (de entrada)	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 25.
Duración de la anomalía (de salida)	El sistema solo generará una alerta cuando detecte una anomalía si el comportamiento anómalo persiste en el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 25.

Configuración del uso de la CPU por supervisión del proceso

El **uso de la CPU por proceso** supervisa el uso de la CPU del proceso seleccionado. Si hay varias instancias del mismo proceso, el sistema supervisará el uso total por todas las instancias del proceso y generará una alerta cuando se cumplan las condiciones.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	Nombre del proceso que quiere supervisar. Introduzca el nombre del proceso sin la extensión.
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero en el intervalo 1-100 (%). El valor predeterminado es 90.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

Configuración del uso de la memoria por supervisión del proceso

El **uso de la memoria por proceso** supervisa el uso de la memoria del proceso seleccionado. Si hay varias instancias del mismo proceso, el sistema supervisará el uso total por todas las instancias del proceso y generará una alerta cuando se cumplan las condiciones.

Nota
Los agentes utilizan todo el conjunto de trabajo del proceso (privado y compartido) para calcular el tamaño del uso de memoria por proceso. Por este motivo, el tamaño del uso de memoria que indica el widget puede diferir del que se muestra en el Administrador de tareas de Windows (conjunto de trabajo privado).

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	Nombre del proceso que quiere supervisar. Introduzca el nombre del proceso sin la extensión.
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb). El valor predeterminado es 1.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

Configuración de la supervisión de la velocidad de transferencia del disco por proceso

Velocidad de transferencia de disco por proceso supervisa la velocidad de lectura y escritura del proceso seleccionado. Si hay varias instancias del mismo proceso, el sistema supervisará el uso total por todas las instancias del proceso y generará una alerta cuando se cumplan las condiciones.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	El nombre del proceso que quiere supervisar. Introduzca el nombre del proceso sin la extensión.
Qué supervisar	La velocidad que quiere supervisar. Los valores disponibles son los siguientes: • **Velocidad de lectura y velocidad de escritura**. Este es el valor predeterminado. • **Velocidad de lectura** • **Velocidad de escritura**
Operador de velocidad de lectura	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de velocidad de lectura	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo de velocidad de lectura	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Operador de velocidad de escritura	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de velocidad de escritura	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo de	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado.

Configuración	Descripción
velocidad de escritura	Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

Configuración del uso de la red por supervisión del proceso

Uso de la red por proceso supervisa el tráfico de entrada y salida del proceso seleccionado. Si hay varias instancias del mismo proceso, el sistema supervisará el uso total por todas las instancias del proceso y generará una alerta cuando se cumplan las condiciones en todas las instancias.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	Nombre del proceso que quiere supervisar. Introduzca el nombre del proceso sin la extensión.
Dirección del tráfico	La dirección del tráfico que quiere supervisar. Los valores disponibles son los siguientes: • **Tráfico entrante y saliente**. Este es el valor predeterminado. • **Tráfico de entrada** • **Tráfico de salida**
Operador de tráfico de entrada	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de tráfico de entrada	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo del tráfico de entrada	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.
Operador del tráfico de salida	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes:

Configuración	Descripción
	• **Más de**: Este es el valor predeterminado. • **Mayor o igual que** • **Menos de** • **Menor o igual que**
Umbral de tráfico de salida	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (kb/s). El valor predeterminado es 0 kb/s.
Periodo de tiempo del tráfico de salida	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 5.

Configuración de la supervisión del estado del servicio de Windows

Estado del servicio de Windows supervisa si el servicio de evento de Windows seleccionado se está ejecutando o está detenido.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del servicio	El nombre del servicio de Windows que quiere supervisar. Puede seleccionar un nombre de servicio de la lista de servicios de Windows. La lista se rellena con todos los agentes del inquilino después de que se complete correctamente el análisis de inventario de software en las cargas de trabajo. También puede añadir un nombre de servicio que no figure en la lista. Esta es la única opción disponible si no se realiza el análisis de inventario de software en las cargas de trabajo.
Estado del servicio	Si el servicio se encuentra en el estado seleccionado, el sistema generará un evento. Los valores disponibles son los siguientes: • **En ejecución** • **Detenido**: Este es el valor predeterminado.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 1.

Configuración del monitor de estado del proceso

El **estado del proceso** supervisa si el proceso seleccionado se está ejecutando o está detenido. Si hay varias instancias del mismo proceso, el sistema supervisará cada instancia del proceso y generará la alerta cuando se cumplan las condiciones en todas las instancias del proceso.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del proceso	El nombre del proceso que quiere supervisar. Especifique el nombre de un archivo ejecutable sin la extensión.
Estado del proceso	Si el proceso está en el estado seleccionado, el sistema generará un evento. Los valores disponibles son los siguientes: • **En ejecución** • **Detenido**: Este es el valor predeterminado.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 1-60 (min). El valor predeterminado es 1.

Configuración del monitor de Software instalado

El monitor **Software instalado** supervisa la instalación, actualización o eliminación de aplicaciones de software en la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Qué software supervisar	Especifique el software que quiere supervisar. Los valores disponibles son los siguientes: • **Cualquier software**: Este es el valor predeterminado. • **Software específico**
Nombres del software	Este parámetro está disponible si selecciona el valor **Software específico** para **Qué software supervisar**. Escriba el nombre de una o varias aplicaciones de software. Puede seleccionar un nombre de aplicación de software de la lista de servicios de Windows. La lista se rellena con todos los agentes del inquilino después de que se complete correctamente el análisis de inventario de software en las cargas de trabajo. También puede añadir un nombre de aplicación de software que no figure en la lista. Esta es la única opción

Configuración	Descripción
	disponible si no se realiza el análisis de inventario de software en las cargas de trabajo.
Estado de instalación	Especifique si desea supervisar software instalado, no instalado o actualizado. Los valores disponibles son los siguientes: • **Instalado**: Este es el valor predeterminado. Si selecciona este valor, el monitor generará una alerta cuando se instale una nueva aplicación de software en la carga de trabajo. • **Actualizado**: Si selecciona este valor, el monitor generará una alerta cuando se actualice una aplicación de software. • **No instalado**: si selecciona este valor, el monitor generará una alerta cuando se desinstale una aplicación de software o no esté disponible en la carga de trabajo.

Configuración de la supervisión del último reinicio del sistema

Último reinicio del sistema supervisa cuando la carga de trabajo se ha reiniciado por última vez.

Puede configurar el siguiente parámetro para el monitor:

Configuración	Descripción
La carga de trabajo no se ha reiniciado durante	El periodo (número de días) desde el último reinicio de la carga de trabajo. Si la carga de trabajo no se ha reiniciado durante un periodo superior al que ha especificado, el sistema generará una alerta. Escriba un valor entero entre 1 y 180 (días). El valor predeterminado es 30.

Configuración de la supervisión del registro de eventos de Windows

Registro de eventos de Windows supervisa los eventos específicos de datos esenciales para el negocio en los registros de eventos de Windows.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Nombre del registro de eventos	Seleccione un registro de eventos específico en una lista de registros de eventos de Windows que estén disponibles en el Visor de eventos de Windows. Los valores disponibles son los siguientes: • **Cualquiera** —Este es el valor predeterminado. • **Aplicación** • **Seguridad**

Configuración	Descripción
	• **Sistema**
Origen del evento	Nombre del origen del evento Puede seleccionar el valor de una lista de orígenes del evento que se recopilan de todos los agentes del inquilino o introducir un nuevo nombre de origen manualmente. Si el análisis de inventario de software está deshabilitado en el inquilino, la lista de orígenes del evento estará vacía.
Modo de coincidencia	En este campo, puede especificar si quiere conectar los ajustes de **ID de los eventos**, **Tipo de evento** y **Descripción del evento** utilizando el operador **Cualquiera** o **Todos**. Los valores disponibles son los siguientes: • **Cualquiera**:Este es el valor predeterminado. Se generará una alerta solo si coincide alguno de los criterios seleccionados. • **Todos**: se generará una alerta si coinciden todos los criterios seleccionados.
ID de los eventos	Escriba uno o varios ID de eventos, separados por una coma Si el sistema encuentra en el registro de eventos alguno de los códigos de evento que ha introducido en este campo, se generará una alerta.
Tipo de evento	Seleccione uno o más tipos de evento que desee supervisar. Los valores disponibles son los siguientes: • **Cualquiera** —Este es el valor predeterminado. • **Error** • **Advertencia** • **Información** • **Auditoría correcta** • **Fallo de auditoría**
Descripción del evento	Frases o palabras clave específicas de la descripción del evento que quiera buscar. Cada frase o palabra clave que escriba debe estar entre comillas y separadas por una coma. Si el sistema encuentra alguna de las frases o palabras clave que ha introducido, se generará una alerta.
Número de ocurrencias	El número mínimo de ocurrencias en el registro que debe tener un evento durante el periodo de tiempo especificado para que el sistema genere una alerta. Escriba un valor entero entre 1 y 1000.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado.

Configuración	Descripción
	Escriba un valor entero y seleccione la unidad: minutos o horas. El valor predeterminado es 60 minutos.

Configuración de la supervisión del tamaño de archivos y carpetas

Tamaño de archivos y carpetas supervisa el tamaño total de los archivos o carpetas seleccionados.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Archivos o carpetas para supervisar	Las rutas de los archivos o las carpetas que quiere supervisar. También puede especificar los archivos o las carpetas que quiere excluir de la supervisión. Puede utilizar los siguientes caracteres comodín: • `*`: para cero o más caracteres en un nombre de archivo o carpeta • `?`: para exactamente un carácter en un nombre de archivo o carpeta Para las cargas de trabajo de Windows: • La ruta completa debe empezar por la letra de la unidad seguida del separador `:\`. • Puede utilizar la barra diagonal o inversa como un carácter separador de ruta. • El nombre del archivo o la carpeta no debe acabar en un espacio o un punto. Para las cargas de trabajo de macOS: • La ruta completa debe empezar por el directorio raíz. • Puede utilizar la barra diagonal como un carácter separador de ruta. • El nombre del archivo o la carpeta no debe acabar en un espacio o un punto. No es obligatorio especificar una ubicación concreta para los filtros de exclusión. Los archivos introducidos sin una ubicación específica se excluirán en las carpetas supervisadas.
Operador	El operador es una función condicional que define cómo definir el rendimiento del parámetro. Los valores disponibles son los siguientes: • **Más de**: Este es el valor predeterminado. • **Menos de**
Valor del umbral	El valor del umbral y el valor **Operador** determinan el rendimiento normal del parámetro supervisado. Cuando el valor del parámetro supervisado

Configuración	Descripción
	esté fuera de la norma, el sistema generará una alerta. Escriba un valor entero (MB).
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero en el intervalo 10-60 (min). El valor predeterminado es 10.

Configuración de la supervisión del estado de actualización de Windows

Estado de actualización de Windows supervisa el estado de actualización de Windows de la carga de trabajo y si se han instalado las actualizaciones más recientes.

Si habilita esta supervisión, el sistema generará una alerta en los siguientes casos.

- La actualización de Windows está deshabilitada en la carga de trabajo.
- La actualización de Windows está habilitada en la carga de trabajo, pero no se han instalado las actualizaciones más recientes.

Configuración de la supervisión del estado del firewall

El estado del cortafuegos supervisa el firewall integrado o de terceros que está instalado en la carga de trabajo.

Si habilita esta supervisión, el sistema generará una alerta en los siguientes casos.

- El firewall integrado en el SO (firewall de Windows Defender o firewall de macOS) está deshabilitado y no se ejecuta ningún firewall de terceros.
- El firewall de Windows Defender está deshabilitado para las redes públicas.
- El firewall de Windows Defender está deshabilitado para las redes privadas.
- El firewall de Windows Defender está deshabilitado para las redes de dominio.

Configuración del monitor de inicios de sesión fallidos

Inicios de sesión fallidos supervisa los intentos de inicio de sesión sin éxito de la carga de trabajo.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Umbral de intentos de inicio de sesión fallidos	El valor del umbral determina los límites del rendimiento normal del parámetro supervisado. Cuando se supera el valor del umbral, el valor está fuera de la norma.

Configuración	Descripción
	Escriba un valor entero. El valor predeterminado es 60.
Periodo de tiempo	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado. Escriba un valor entero entre 1 y 24 y seleccione una unidad: horas o días. El valor predeterminado es 12.

Configuración de la supervisión del estado del software antimalware

El **estado del software antimalware** supervisa el software antimalware integrado o de terceros que está instalado en la carga de trabajo.

Si habilita esta supervisión, el sistema generará una alerta cuando identifique una de las siguientes condiciones.

- El software antimalware no está instalado en la carga de trabajo.
- El software antimalware está instalado, pero no se está ejecutando.
- El software antimalware está instalado y se está ejecutando, pero las definiciones de malware no están actualizadas.

Nota
Esta condición se comprueba para los sistemas operativos de Windows y Windows Server.

Sistema operativo	Software antimalware admitido
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton antivirus • SentinelOne • Endpoint Security de Trend Micro con Apex One • Worry-Free Business de Trend Micro • McAfee Endpoint Security • McAfee Endpoint Protection para SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus

Sistema operativo	Software antimalware admitido
	• Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **Nota** Puede que el monitor funcione con otras aplicaciones antimalware, pero no se lo podemos asegurar.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus para Mac • Sophos Home • Sophos Endpoint Protection • Avast Security para Mac • AVG AntiVirus para Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus para Mac • Comodo Antivirus para Mac • K7 Antivirus para Mac • Vipre Advanced Security • Total AV para Mac **Nota** Puede que el monitor funcione con otras aplicaciones antimalware, pero no se lo podemos asegurar.

Configuración de la supervisión del estado de la función AutoRun

El **estado de la función AutoRun** supervisa si la función AutoRun está activada para el soporte extraíble.

Por motivos de seguridad, recomendamos deshabilitar la función AutoRun para el dispositivo extraíble en la carga de trabajo. Si la función está habilitada, el sistema generará una alerta.

Configuración del monitor personalizado

Los monitores **personalizados** personalizan los objetos mediante la ejecución de una secuencia de comandos.

Puede configurar los siguientes parámetros para el monitor:

Configuración	Descripción
Secuencia de comandos que ejecutar	Lista de secuencias de comandos predefinidas desde el repositorio de secuencias de comandos.
Planificación	La hora a la que se ejecuta la secuencia de comandos y, de forma opcional, otras condiciones que deberían cumplirse para ejecutar la secuencia de comandos. Los valores disponibles son los siguientes: • **Planificar por hora**: la secuencia de comandos se ejecutará a la hora, el día, la semana o el mes que especifique. Este es el valor predeterminado. **Tipo de planificación**: **Cada hora**, **Diaria** o **Mensual** **Ejecutar dentro de un intervalo de fechas**: un intervalo de tiempo en el que ejecutar la secuencia de comandos. • **Cuando el usuario inicia sesión en el sistema**: la secuencia de comandos se ejecutará cuando un usuario inicie sesión en la carga de trabajo. • **Cuando el usuario cierra sesión en el sistema**: la secuencia de comandos se ejecutará cuando un usuario cierre sesión en la carga de trabajo. • **Al iniciarse el sistema**: la secuencia de comandos se ejecutará cuando el sistema operativo se inicie. • **Al apagarse el sistema**: la secuencia de comandos se ejecutará se apague el sistema. • **Cuando el sistema esté en línea**: la secuencia de comandos se ejecutará cuando la carga de trabajo esté disponible en línea. **Condiciones de inicio**: la tarea se ejecutará en un momento o evento específico solo si se cumple la condición. Cuando se seleccionan varias

Configuración	Descripción
	condiciones, deben cumplirse todas simultáneamente para que se inicie la tarea. De forma predeterminada, se selecciona la condición **Evitar el modo de suspensión o hibernación para iniciar una tarea programada**. **Si no se cumplen las condiciones de inicio, ejecute la tarea de todos modos después de**: esta condición está activada de forma predeterminada. El valor predeterminado es 1 hora.
Cuenta para ejecutar la secuencia de comandos	La cuenta en la que se ejecutará la secuencia de comandos. Los valores disponibles son los siguientes: • **Cuenta de sistema**: Este es el valor predeterminado. • **Cuenta con sesión iniciada actualmente**
Duración máxima	El periodo máximo durante el cual se puede ejecutar la secuencia de comandos en la carga de trabajo. Si la secuencia de comandos no se completa durante este periodo, la operación fallará. Escriba un valor entero entre 1 y 1440 (minutos). El valor predeterminado es 3 minutos.
Directiva de ejecución de PowerShell	La directiva de ejecución de PowerShell. Los valores disponibles son los siguientes: • **Sin definir** • **AllSigned** • **Bypass**: Este es el valor predeterminado. • **RemoteSigned** • **Restringido** • **Sin restringir** Para obtener más información sobre estos valores, consulte la documentación de Microsoft.

Planes de supervisión

Los planes de supervisión son planes que aplica en sus cargas de trabajo gestionadas para habilitar y configurar la funcionalidad de supervisión.

Si no se aplica ningún plan de supervisión a una carga de trabajo, las características de supervisión no estarán disponibles para la carga de trabajo.

Nota
La disponibilidad de la configuración que puede configurar en el plan de supervisión depende del paquete de servicios que se aplica al inquilino. Para acceder a toda la configuración, active el paquete de Advanced Management.

Crear un plan de supervisión

Puede crear un plan de supervisión y asignarle cargas de trabajo para configurar la funcionalidad de supervisión en las cargas de trabajo gestionadas.

Requisitos previos

La versión del agente que está instalada en la carga de trabajo es compatible con la funcionalidad de supervisión.

Pasos para crear un plan de supervisión

Desde Planes de supervisión

1. En la consola de Protección, vaya a **Administración** > **Planes de supervisión**.
2. Cree un plan de supervisión mediante una de estas dos opciones:
   - Si no hay planes de supervisión en la lista, haga clic en **Crear**.
   - Si no hay planes de supervisión en la lista, haga clic en **Crear plan**.
3. En la ventana **Crear plan de supervisión**, según si el paquete de Advanced Management está activado para su inquilino, haga lo siguiente:
   - Si su inquilino utiliza la protección estándar, los siguientes cuatro monitores se añadirán automáticamente al plan de supervisión: Espacio del disco, cambios de hardware, último reinicio del sistema y tamaño de archivos y carpetas.
   - Si el paquete de Advanced Management está habilitado para su cliente, seleccione una de las opciones de plantilla y haga clic en **Siguiente**.

Opción	Descripción
Recomendada	Seleccione esta opción para crear un plan de supervisión con la configuración de supervisión predeterminada.
Personalizado	Utilice esta opción para crear un plan de supervisión desde cero.

4. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Aceptar**.
5. [Opcional] Para añadir un monitor al plan, haga clic en **Añadir monitor**, en el monitor de la lista y en **Añadir**.

Nota
La configuración del monitor se rellenará automáticamente con los valores predeterminados. Puede añadir hasta tres monitores del mismo tipo y hasta 30 monitores en total a un plan de supervisión.

6. [Opcional] En la pantalla de parámetros de supervisión, cambie la configuración predeterminada del monitor y las alertas y haga clic en **Listo**.

Nota
Puede configurar diferentes parámetros para cada monitor. Para obtener más información, consulte "Monitores configurables" (p. 1147) y "Configuración de alertas de supervisión" (p. 1193).

7. [Opcional] Para eliminar un monitor, haga clic en el icono de la papelera y en **Eliminar**.
8. [Opcional] Pasos para añadir cargas de trabajo al plan:
   a. Haga clic en **Añadir cargas de trabajo**.
   b. Seleccione las cargas de trabajo y haga clic en **Añadir**.
   c. Si hay problemas de compatibilidad que desea resolver, siga el procedimiento descrito en "Resolución de problemas de compatibilidad con planes de supervisión" (p. 1191).
9. Haga clic en **Crear**.

Desde Todos los dispositivos

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que desee aplicar un plan de supervisión.
3. Haga clic en **Proteger**.
4. Según si el plan de supervisión se aplica a la carga de trabajo, haga lo siguiente:
   - Si un plan de supervisión ya se aplica a la carga de trabajo, haga clic en **Crear plan** y seleccione **Supervisión**.
   - Si no se aplica ningún plan de supervisión a la carga de trabajo, haga clic en **Agregar plan** y luego en **Crear plan** y seleccione **Supervisión**.
5. En la ventana **Crear plan de supervisión**, seleccione una de las opciones de plantilla y haga clic en **Siguiente**.

Opción	Descripción
Recomendada	Seleccione esta opción para crear un plan de supervisión con la configuración de supervisión predeterminada.
Personalizado	Utilice esta opción para crear un plan de supervisión desde cero.

6. [Opcional] Para cambiar el nombre predeterminado del plan, haga clic en el icono del lápiz, escriba el nombre del plan y haga clic en **Aceptar**.

7. [Opcional] Si desea cambiar la configuración predeterminada del monitor y las alertas, configure los nuevos valores y haga clic en **Listo**.

   Nota
   Puede añadir hasta tres monitores del mismo tipo y hasta 30 monitores en total a un plan de supervisión.

8. [Opcional] En la pantalla de parámetros de supervisión, cambie la configuración predeterminada del monitor y las alertas y haga clic en **Listo**.

   Nota
   Puede configurar diferentes parámetros para cada monitor. Para obtener más información, consulte "Monitores configurables" (p. 1147) y "Configuración de alertas de supervisión" (p. 1193).

9. [Opcional] Para eliminar un monitor, haga clic en el icono de la papelera y en **Eliminar**.
10. Haga clic en **Crear**.

Añadir cargas de trabajo a los planes de supervisión

Según sus necesidades, puede añadir cargas de trabajo a un plan de supervisión después de crearlo.

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- La versión del agente que está instalada en la carga de trabajo es compatible con la funcionalidad de supervisión.
- Al menos un plan de supervisión está disponible.

Pasos para añadir una carga de trabajo a un plan de supervisión

Desde Planes de supervisión

1. En la consola de Protección, vaya a **Administración** > **Planes de supervisión**.
2. Haga clic en el plan de supervisión.
3. Según si el plan ya se ha aplicado a una carga de trabajo, haga lo siguiente:
   - Haga clic en **Añadir cargas de trabajo**, si el plan todavía no se ha aplicado a ninguna carga de trabajo.
   - Haga clic en **Gestionar cargas de trabajo**, si el plan se ha aplicado a alguna carga de trabajo.
4. Seleccione una carga de trabajo de la lista y haga clic en **Agregar**.
5. Haga clic en **Guardar**.
6. Si es necesario, haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Desde Todos los dispositivos

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo a la que desee aplicar un plan de supervisión.
3. Haga clic en **Proteger**.
4. Busque el plan de supervisión al que desee añadir la carga de trabajo y haga clic en **Aplicar**.
5. Si es necesario, haga clic en **Confirmar** para aplicar la cuota de servicio necesaria a la carga de trabajo.

Revocación de planes de supervisión

Puede revocar un plan de supervisión desde una carga de trabajo donde se aplique el plan.

Requisitos previos

Al menos un plan de supervisión se aplica a la carga de trabajo.

Pasos para revocar el plan de supervisión

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en la carga de trabajo y en **Proteger**.
3. Haga clic en el icono **Más acciones** del plan de supervisión que desea revocar y, a continuación, en **Revocar**.

Configuración de las acciones de respuesta automática

Las medidas de respuesta automática en los eventos de alertas son medidas o acciones predefinidas que se activan automáticamente en respuesta a los incidentes o eventos detectados. El propósito de estas acciones es mitigar las posibles amenazas y reducir el daño.

Puede configurar una o varias medidas de respuesta automática en los eventos de alertas. El número máximo de medidas de respuesta automática por monitor son 20.

Pasos para configurar medidas de respuesta automática

1. En la consola de Protección, vaya a **Administración** > **Planes de supervisión**.
2. Seleccione el plan de supervisión en el que quiere configurar las medidas de respuesta automática.
3. Seleccione el monitor en el que quiere configurar las medidas de respuesta automática, o, si aún no ha añadido ningún monitor, haga clic en **Añadir monitor**, haga clic en el monitor de la lista, haga clic en **Añadir** y, por último, seleccione el monitor.
4. Haga clic en el enlace junto a **Acciones de respuesta automática**.
5. En la ventana **Acciones de respuesta automática**, añada una o varias acciones de respuesta que se ejecutarán automáticamente cuando se active una alerta.

6. Configure cada una de las medidas de respuesta. Por ejemplo, si ha añadido la medida de respuesta **Iniciar un servicio de Windows**, haga lo siguiente:
   a. Junto a **Servicio de Windows**, haga clic en **Especificar**.
   b. En el campo **Servicio**, seleccione un servicio para iniciar una medida de respuesta.
   c. Haga clic en **Listo**.
7. En la lista con todas las medidas de respuesta añadidas, utilice las flechas hacia arriba y abajo o arrastre y suelte para establecer la secuencia de las medidas de respuesta.
8. Configure cómo gestionar las medidas de respuesta siguientes si falla la anterior. Seleccione una de las siguientes opciones:
   a. **Continuar con la medida de respuesta siguiente**.
   b. **No continuar con la medida de respuesta siguiente**.
9. Haga clic en **Listo**.

   Verá el número de medidas configuradas junto a la opción de **Acciones de respuesta automática** en el plan de supervisión. Puede modificar o eliminar estas medidas, así como añadir nuevas en cualquier momento.

La siguiente tabla enumera y describe todas las acciones de respuesta automática disponibles en la configuración del monitor.

Acción de respuesta automática	Descripción	SO compatibles
Ejecutar una secuencia de comandos	Si añade esta medida, puede: 1. Seleccionar una determinada secuencia de comandos para ejecutar en la carga de trabajo. 2. Especifique la cuenta con la que quiere ejecutar la secuencia de comandos. 3. Especifique la duración máxima de la operación. 4. Especifique la directiva de ejecución de PowerShell. 5. Ejecutar una secuencia de comandos. Para llevar a cabo esta medida, necesita una licencia del paquete de Advanced Management para la carga de trabajo (si todavía no está asignada). El sistema ejecutará la secuencia de comandos remota seleccionada con los parámetros especificados cuando se cumplan las condiciones.	Windows y macOS
Reiniciar la carga de trabajo	Si añade esta medida el sistema reiniciará la	Windows y

Acción de respuesta automática	Descripción	SO compatibles
	carga de trabajo de forma remota cuando se cumplan las condiciones.	macOS
Detener el proceso	Si añade esta medida, puede especificar que se detenga el proceso cuando se introduzca manualmente el nombre del proceso. El sistema detendrá el proceso cuando se cumplan las condiciones.	Windows y macOS
Iniciar el servicio de Windows	Si añade esta medida, puede seleccionar qué servicio de Windows se debe iniciar en la lista dinámica de servicios que rellenan los agentes. El sistema iniciará el servicio cuando se cumplan las condiciones.	Windows
Detener el servicio de Windows	Si añade esta medida, puede seleccionar qué servicio de Windows se debe detener en la lista dinámica de servicios que rellenan los agentes. El sistema detendrá el servicio cuando se cumplan las condiciones.	Windows
Habilitar la actualización de Windows	Si añade esta medida, el sistema habilitará la actualización de Windows cuando se cumplan las condiciones. Esta acción solo está disponible en la supervisión del estado de la actualización de Windows.	Windows
Deshabilitar AutoRun en las unidades extraíbles	Si añade esta medida, el sistema deshabilitará la función AutoRun en los soportes de almacenamiento extraíbles para la carga de trabajo cuando se cumplan las condiciones. Esta acción solo está disponible en la supervisión del estado de la función Autorun.	Windows

Acciones adicionales con planes de supervisión

Desde la pantalla **Planes de supervisión**, puede realizar las siguientes acciones adicionales con los planes de supervisión: ver detalles, editar, ver las actividades, ver las alertas, renombrar, habilitar,

deshabilitar, clonar, exportar, establecer como favorito, establecer como predeterminado y eliminar.

Ver detalles

Pasos para consultar los detalles de un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Ver detalles**.
3. [Opcional] Si desea consultar los detalles de un monitor habilitado en el plan, haga clic en el nombre del monitor.

Editar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para editar un plan

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Editar**.
3. [Opcional] Para eliminar un monitor del plan, haga clic en el icono de papelera de reciclaje situado a la derecha del nombre del monitor.
4. [Opcional] Para habilitar o deshabilitar un monitor del plan, utilice el conmutador que se encuentra junto al nombre del monitor.
5. [Opcional] Para editar los parámetros del monitor, siga los pasos siguientes:
   a. Haga clic en el nombre del monitor.
   b. Haga clic en la información general de los parámetros del monitor.
   c. En la pantalla **Parámetros del monitor**, configure los parámetros y haga clic en **Listo**.

      Nota
      Puede configurar diferentes parámetros para cada monitor. Para obtener más información, consulte "Monitores configurables" (p. 1147) y "Configuración de alertas de supervisión" (p. 1193).

   d. Cierre la pantalla y confirme los cambios.
6. [Opcional] Para añadir un monitor, haga clic en **Añadir monitor** y, a continuación, si es necesario, edite los parámetros según se indica en el paso anterior.
7. Haga clic en **Guardar**.

Actividades

Pasos para ver las actividades relacionadas con un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Actividades**.
3. Haga clic en una actividad para ver más información sobre ella.

Alertas

Pasos para ver las alertas

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Alertas**.

Cambiar nombre

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para cambiar el nombre de un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Cambiar nombre**.
3. Escriba el nuevo nombre del plan y haga clic en **Aceptar**.

Habilitar

Requisitos previos

- La autenticación de doble factor está habilitada en su cuenta de usuario.
- El plan de supervisión se aplica al menos a una carga de trabajo.

Pasos para habilitar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Habilitar**.

Deshabilitar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para deshabilitar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Deshabilitar**.

Clonar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para clonar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Clonar**.
3. Haga clic en **Crear**.

Exportar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para exportar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Exportar**.
   La configuración del plan se exporta en formato JSON al equipo local.

Eliminar

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Pasos para eliminar un plan de supervisión

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Eliminar**.
3. Seleccione **Confirmo** y, a continuación, haga clic en **Eliminar**.

Establecer como predeterminado

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para establecer un plan de supervisión como predeterminado

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Establecer como predeterminado**.

3. En la ventana de confirmación, haga clic en **Establecer**.
   En la pantalla de **Planes de supervisión**, la etiqueta **Predeterminado** aparece junto al nombre del plan.

Agregar a favoritos

Requisitos previos

La autenticación de doble factor está habilitada en su cuenta de usuario.

Para marcar un plan de supervisión como favorito

1. En la pantalla de **Planes de supervisión**, haga clic en el icono de **Más acciones** del plan de supervisión.
2. Haga clic en **Añadir a favoritos**.
   En la pantalla de **Planes de supervisión**, aparece un icono de estrella junto al nombre del plan.

Problemas de compatibilidad con planes de supervisión

En algunos casos, aplicar un plan de supervisión en una carga de trabajo podría causar problemas de compatibilidad. Es posible que observe los siguientes problemas de compatibilidad:

- El sistema operativo es incompatible: este problema aparece cuando el sistema operativo de la carga de trabajo no es compatible.
- Agente no compatible: este problema aparece cuando la versión del agente de protección de la carga de trabajo está obsoleta y no es compatible con la funcionalidad de supervisión.
- Cuota insuficiente: este problema aparece cuando no hay una cuota de servicio suficiente en el inquilino para asignarla a las cargas de trabajo seleccionadas.

Si se aplica el plan de supervisión a un máximo de 150 cargas de trabajo seleccionadas de forma individual, se le pedirá que resuelva los conflictos existentes antes de guardar el plan. Para resolver un conflicto, elimine la causa raíz o las cargas de trabajo afectadas desde el plan. Para obtener más información, consulte "Resolución de problemas de compatibilidad con planes de supervisión" (p. 1191). Si guarda el plan sin resolver los conflictos, se deshabilitará automáticamente para las cargas de trabajo no compatibles y se mostrarán alertas.

Si se aplica el plan de supervisión a más de 150 cargas de trabajo o grupos de dispositivos, primero se guardará y, después, se comprobará la compatibilidad. El plan se deshabilitará automáticamente para las cargas de trabajo incompatibles y se mostrarán las alertas.

Resolución de problemas de compatibilidad con planes de supervisión

Según la causa de los problemas de compatibilidad, puede ejecutar diferentes acciones para resolverlos como parte del proceso de creación de un nuevo plan de supervisión.

Pasos para resolver problemas de compatibilidad

1. Haga clic en **Revise los problemas**.
2. [Opcional] Para resolver problemas de compatibilidad con sistemas operativos mediante la eliminación de cargas de trabajo desde el plan:
   a. En la pestaña **Sistema operativo no compatible**, seleccione las cargas de trabajo que desee eliminar.
   b. Haga clic en **Eliminar cargas de trabajo del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
3. [Opcional] Para resolver problemas de compatibilidad con sistemas operativos mediante la deshabilitación de un monitor del plan:
   a. En la pestaña **Sistema operativo no compatible**, seleccione los monitores que desee eliminar.
   b. Haga clic en **Deshabilitar monitor**.
   c. Haga clic en **Deshabilitar** y, a continuación, haga clic en **Cerrar**.
4. [Opcional] Para resolver problemas de compatibilidad con agentes no compatibles mediante la eliminación de cargas de trabajo desde el plan:
   a. En la pestaña **Agentes no compatibles**, seleccione las cargas de trabajo que desee eliminar.
   b. Haga clic en **Eliminar cargas de trabajo del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
5. [Opcional] Para resolver problemas de compatibilidad con agentes no compatibles mediante la actualización de la versión del agente, haga clic en **Ir a la lista de agentes**.

   Nota
   Esta opción solamente está disponible para los administradores de clientes.

6. [Opcional] Para resolver problemas de compatibilidad con una cuota insuficiente mediante la eliminación de cargas de trabajo desde el plan:
   a. En la pestaña **Cuota insuficiente**, seleccione las cargas de trabajo que desee eliminar.
   b. Haga clic en **Eliminar cargas de trabajo del plan**.
   c. Haga clic en **Eliminar** y, a continuación, haga clic en **Cerrar**.
7. [Opcional] Para resolver problemas de compatibilidad con una cuota insuficiente mediante el aumento de la cuota del cliente:
   a. En la pestaña **Cuota insuficiente**, haga clic en **Ir al portal de administración**.
   b. Aumentar la cuota de servicio para el cliente.

      Nota
      Esta opción solamente está disponible para los administradores de partner.

Restablecimiento de los modelos de aprendizaje automático

Puede restablecer los modelos de una carga de trabajo cuando se vuelven obsoletos o dejan de ser válidos por algún motivo. Esta acción eliminará los modelos creados y los datos de la carga de trabajo que hayan recopilado los monitores con el tipo de supervisión basada en anomalías y, a continuación, iniciará la formación de los modelos de aprendizaje automático para la carga de trabajo desde cero.

Para restablecer los modelos de aprendizaje automático para una carga de trabajo

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en una carga de trabajo de la lista y, a continuación, en la pestaña **Detalles**.
3. En la sección **Restablecer los modelos de aprendizaje automático**, haga clic en **Restablecer**.
4. Vuelva a hacer clic en **Restablecer** en la ventana de confirmación.

Supervisión de alertas

Las alertas de supervisión se muestran en la consola de Protección y se envían por correo electrónico cuando el comportamiento supervisado de las cargas de trabajo está fuera de lo normal. Las alertas aseguran que se informe a los interesados lo antes posible cuando haya algún problema en el entorno de TI de la organización.

Nota
Para habilitar las alertas de supervisión a través del correo electrónico, debe configurar al menos una directiva de notificaciones por correo electrónico para el tipo de alerta correspondiente. Para obtener más información, consulte "Configurar directivas de notificaciones por correo electrónico" (p. 1201).

Configuración de alertas de supervisión

Puede configurar los parámetros de la alerta del monitor al añadir un monitor a un plan de supervisión o al editar un monitor que ya esté disponible en un plan de supervisión.

Pasos para configurar alertas de supervisión

1. En la ventana **Parámetros del monitor**, vaya a la sección **Generar alertas**.
2. En **Gravedad de la alerta**, seleccione la gravedad que corresponde a la prioridad de la alerta.

Opción	Descripción
Crítico	Estas alertas tienen la máxima prioridad y están relacionadas con problemas que son críticos para el funcionamiento de la carga de trabajo. Resuelva estos problemas lo antes posible.
Error	Una alerta de error es menos grave e indica que algo va mal o no se

Opción	Descripción
	comporta de forma normal. Resuelva los problemas a tiempo para evitar que den lugar a problemas más graves.
Advertencia	Una alerta de advertencia indica que existe una situación de la que debe ser consciente, pero es posible que aún no esté causando ningún problema. Resuelva estos problemas después de resolver los que están causando alertas críticas y de error. Este es el valor predeterminado.
Informativo	Estas alertas son las de menor prioridad. La gravedad informativa no indica un problema. Dichas alertas ofrecen información sobre las acciones relacionadas con un objeto supervisado.

3. En **Frecuencia de alertas**, seleccione con qué frecuencia el sistema debería generar una alerta cuando se cumpla la condición.

Opción	Descripción
Una vez hasta pasar la comprobación	El sistema generará una alerta una vez hasta que la comprobación se complete correctamente. Este es el valor predeterminado.
Después de X fallos consecutivos	El sistema generará una alerta después de X comprobaciones consecutivas fallidas, donde X es un valor entero.

4. En **Mensaje de alerta**, haga clic en el icono de lápiz para editar el mensaje de alerta predeterminado que se utilizará cuando el sistema genere una alerta. Puede especificar un mensaje de alerta personalizado que incluya variables. Para obtener más información acerca de las variables que puede utilizar, consulte "Variables de alertas de supervisión" (p. 1194).

   Nota
   Puede configurar más de un mensaje de alerta para algunos de los monitores.

5. Habilite la **Resolución automática de alertas** si desea que el sistema resuelva automáticamente la alerta cuando el parámetro supervisado vuelva al estado normal y el comportamiento vuelva a ser normal. De manera predeterminada, se habilita la configuración.

Variables de alertas de supervisión

Puede configurar diferentes variables de alertas para diferentes monitores. Para utilizar una variable, debe estar adjunta en {{}}.

La siguiente tabla proporciona más información sobre las variables disponibles.

Variable	Descripción	Disponible para supervisión
plan_name	El nombre de la directiva	Todos los monitores
monitor_name	El nombre de la subdirectiva del plan de supervisión	Todos los monitores
workload_ name	El nombre de la carga de trabajo	Todos los monitores
threshold_ value	Condiciones de supervisión específicas o umbrales para generar una alerta	Todos los monitores que admiten la supervisión basada en umbrales.
threshold_unit	La unidad que está asociada al valor del umbral. Por ejemplo, %, MB o mb/s.	Todos los monitores que admiten la supervisión basada en umbrales.
time_period	El sistema solo generará una alerta cuando detecte un problema si el valor del parámetro está fuera de la norma durante el periodo especificado.	Todos los monitores que admiten la supervisión basada en umbrales.
time_unit	La unidad que estará asociada al periodo de tiempo (seg./min./horas/día).	Todos los monitores que admiten la supervisión basada en umbrales.
anomaly_value	El valor de la anomalía	Todos los monitores que admiten la supervisión basada en anomalías.
anomaly_unit	La unidad que estará asociada al valor de anomalía	Todos los monitores que admiten la supervisión basada en anomalías.
deviation_value	El valor de desviación	Todos los monitores que admiten la supervisión basada en anomalías.
deviation_unit	La unidad que estará asociada al valor de desviación	Todos los monitores que admiten la supervisión basada en anomalías.

Variable	Descripción	Disponible para supervisión
drive_name	La unidad de Windows o la partición de macOS	Espacio de disco,
CPU_model	El modelo de la CPU supervisada	Temperatura de CPU
GPU_model	El modelo de la GPU supervisada	Temperatura de GPU
hardware_model	El modelo del componente supervisado	Cambios del hardware
hardware_component	El tipo de hardware supervisado	Cambios del hardware
hardware_model_old	El modelo del componente supervisado que se ha reemplazado	Cambios del hardware
hardware_model_new	El modelo del nuevo componente supervisado que se ha añadido	Cambios del hardware
disk_model	El modelo del disco	Velocidad de transferencia del disco
network_adapter_model	El modelo del adaptador de red	Uso de la red
process_name	El nombre del proceso	Uso de la CPU por proceso Uso de la memoria por proceso Velocidad de transferencia del disco por proceso Uso de la red por proceso Estado del proceso
service_name	El nombre del servicio	Estado del servicio de Windows
software_name	El de la aplicación de software	Software instalado
software_version	La versión de la aplicación de software	Software instalado
software_version_old	La versión de la aplicación de software antes de la actualización	Software instalado

Variable	Descripción	Disponible para supervisión
software_ version_new	La versión de la nueva aplicación de software actualizada	Software instalado
number_of_ occurrences	El número de veces que aparece un evento en el registro	Registro de eventos de Windows
event_types	El tipo de evento	Registro de eventos de Windows
event_source	El origen del evento	Registro de eventos de Windows
event_log_ name	El nombre del evento	Registro de eventos de Windows
firewall_ software_name	El nombre del software del firewall	Estado del cortafuegos
antimalware_ software_name	El nombre del software antimalware	Estado de software antimalware
user_name	El nombre del usuario	Estado de la función AutoRun
script_name	El nombre de la secuencia de comandos	Personalizado

Medidas de respuesta manuales

Cuando vea una alerta, puede seleccionar una medida de respuesta que desee ejecutar sobre los eventos con alertas.

Pasos para ejecutar una medida de respuesta manual

1. En la consola de Protección, vaya a **Alertas**.
2. Abra la alerta que quiera ver.
3. Haga clic en **Medida de respuesta** y seleccione una medida de respuesta de la lista desplegable:

La lista de medidas de respuesta disponible para una alerta específica depende del tipo de alerta, de la disponibilidad de las funciones para un inquilino concreto y del sistema operativo de la carga de trabajo.

La siguiente tabla enumera y describe todas las medias de respuesta manuales para que pueda consultarlas.

Medida de respuesta manual	Descripción	SO compatibles
Examinar la tendencia de	Abre una ventana con el gráfico **Uso del**	Windows y

Medida de respuesta manual	Descripción	SO compatibles
uso del espacio de disco	**espacio de disco**, en la que puede: • Examinar cómo ha cambiado el uso del espacio de disco con el tiempo (para el último día, los últimos siete días o el último mes). • Examinar el delta para el uso del espacio de disco en el valor relativo (%) para el periodo seleccionado.	macOS
Examinar la tendencia de crecimiento del tamaño de los archivos	Abre una ventana con el gráfico **Crecimiento del tamaño de los archivos**, en la que puede: • Examinar cómo ha cambiado el tamaño total de los archivos y carpetas supervisados con el tiempo (para el último día, los últimos siete días o el último mes). • Examinar el delta para el tamaño total de los archivos en el valor relativo (%) para el periodo seleccionado.	Windows y macOS
Ejecutar una secuencia de comandos	Abre una ventana en la que puede: 1. Seleccionar una determinada secuencia de comandos para ejecutar en la carga de trabajo. 2. Especifique la cuenta con la que quiere ejecutar la secuencia de comandos. 3. Especifique la duración máxima de la operación. 4. Especifique la directiva de ejecución de PowerShell. 5. Ejecutar una secuencia de comandos. Para llevar a cabo esta acción, necesita una licencia del paquete de Advanced Management para la carga de trabajo (si todavía no está asignada).	Windows y macOS
Conectar a través de NEAR	Acronis Cliente de Connect establece una conexión remota.	Windows y macOS
Conectar a través de RDP	Acronis Cliente de Connect establece una conexión remota.	Windows

Medida de respuesta manual	Descripción	SO compatibles
Abrir inventario de hardware	Se le redirigirá a la pestaña **Inventario de hardware** para la carga de trabajo actual.	Windows y macOS
Examinar los 10 principales procesos que han cargado la CPU	Abre una ventana con los 10 principales procesos que han cargado la CPU y pueden haber causado que se sobrecaliente (La instantánea del sistema en el momento de la generación de la alerta).	Windows y macOS
Examinar los 10 principales procesos que han cargado la GPU	Abre una ventana con los 10 principales procesos que han cargado la GPU y pueden haber causado que se sobrecaliente (La instantánea del sistema en el momento de la generación de la alerta).	Windows y macOS
Examinar los 10 principales procesos que han cargado la memoria	Abre una ventana con los 10 principales procesos que han cargado la memoria (La instantánea del sistema en el momento de la generación de la alerta).	Windows y macOS
Examinar los 10 principales procesos que han cargado el disco	Abre una ventana con los 10 principales procesos que han cargado el disco (La instantánea del sistema en el momento de la generación de la alerta).	Windows y macOS
Examinar los 10 principales procesos que han cargado la red	Abre una ventana con los 10 principales procesos que han cargado el adaptador de interfaz de red (La instantánea del sistema en el momento de la generación de la alerta).	Windows y macOS
Examinar el uso de recursos por proceso	Abre una ventana con información detallada acerca del uso de recursos de hardware por proceso relacionado: Uso de la CPU, uso de la memoria, disco E/S, uso de red.	Windows y macOS
Reiniciar carga de trabajo	Abre una ventana de confirmación. Reinicia la carga de trabajo después de la confirmación.	Windows y macOS
Iniciar el servicio de Windows	Abre una ventana de confirmación. Inicia el servicio de Windows después de la confirmación.	Windows
Detener el servicio de Windows	Abre una ventana de confirmación. Detiene el servicio de Windows después de la confirmación.	Windows

Medida de respuesta manual	Descripción	SO compatibles
Detener proceso	Abre una ventana de confirmación. Detiene el proceso al cual se refiere la alerta después de la confirmación.	Windows y macOS
Habilitar la actualización de Windows	Abre una ventana de confirmación. Habilita la actualización de Windows después de la confirmación.	Windows
Deshabilitar la función AutoRun en las unidades extraíbles	Abre una ventana de confirmación. Deshabilita la función AutoRun a nivel del sistema de la carga de trabajo después de la confirmación.	Windows

Importante
Por motivos de seguridad, se requiere la Autenticación de doble factor para ejecutar las siguientes medidas de respuesta manuales:

- Ejecutar una secuencia de comandos
- Conectar a través de NEAR
- Conectar a través de RDP
- Reiniciar carga de trabajo
- Iniciar el servicio de Windows
- Detener el servicio de Windows
- Detener proceso
- Habilitar la actualización de Windows
- Deshabilitar la función AutoRun en las unidades extraíbles

Consultar las alertas de supervisión para una carga de trabajo

En la pestaña de **Alertas**, puede ver las alertas de supervisión de una carga de trabajo específica y realizar diferentes acciones de alerta.

Para ver las alertas de supervisión para una carga de trabajo

1. En la consola de Protección, vaya a **Todos los dispositivos**.
2. Haga clic en una carga de trabajo, y luego seleccione la pestaña **Alertas**.
3. [Opcional] En el panel de alerta de supervisión, realice una de las siguientes acciones:
   - Para borrar la alerta, haga clic en **Borrar**.
   - Para tomar una acción de respuesta, haga clic en **Medida de respuesta** y luego en la acción.

- Para contactar con el equipo de Soporte, haga clic en **Obtener soporte**.

4. [Opcional] Para borrar todas las alertas de supervisión para la carga de trabajo, haga clic en **Borrar todo**.

Visualización del registro de alertas de supervisión

Puede ver todos los eventos relacionados con una alerta de supervisión en orden cronológico: las acciones de respuesta (tanto automáticas como manuales) que se ejecutaron y las notificaciones por correo electrónico que se enviaron.

Pasos para ver el registro de auditoría de una alerta de supervisión

1. En la consola de Protección, vaya a **Alertas**.
2. Abra la **Vista de tabla**.
3. En la lista de alertas, haga clic en la alerta de supervisión que desea ver.
4. Haga clic en **Detalles** y, a continuación, en **Registro de alertas**.

Configurar directivas de notificaciones por correo electrónico

Las directivas de notificaciones por correo electrónico especifican qué usuarios recibirán notificaciones por correo electrónico de diferentes monitores.

Desde la pantalla **Notificaciones por correo electrónico**, puede realizar las acciones siguientes con las directivas de notificaciones por correo electrónico: añadir, editar, habilitar, deshabilitar y eliminar.

Añadir

Pasos para añadir una nueva directiva de notificación por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. Haga clic en **Añadir directiva**.
3. Haga clic en **Seleccionar destinatarios**.
4. En la pantalla **Seleccionar destinatarios**, seleccione los usuarios que desea que reciban alertas por correo electrónico y haga clic en **Seleccionar**.
5. En **Tipos de alerta**, seleccione los monitores para los que desea que el sistema envíe alertas por correo electrónico.
6. Haga clic en **Agregar**.

Editar

Para editar una directiva de notificaciones por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. Haga clic en el icono de puntos suspensivos de la directiva de notificaciones y, luego, en **Editar**.
3. [Opcional] Para cambiar los destinatarios, haga clic en **Editar destinatarios**, añada o elimine usuarios de la lista y haga clic en **Seleccionar**.
4. [Opcional] En **Tipos de alerta**, seleccione los tipos de alerta de supervisión que desea que se envíen a los destinatarios seleccionados.
5. Haga clic en **Guardar**.

Habilitar

Para habilitar una directiva de notificaciones por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. En la pantalla **Notificaciones por correo electrónico**, haga clic en el icono de **...** de la directiva de notificaciones por correo electrónico.
3. Haga clic en **Habilitar**.

Deshabilitar

Para deshabilitar una directiva de notificaciones por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. En la pantalla **Notificaciones por correo electrónico**, haga clic en el icono de **...** de la directiva de notificaciones por correo electrónico.
3. Haga clic en **Deshabilitar**.

Eliminar

Para eliminar una directiva de notificaciones por correo electrónico

1. En la consola de Protección, vaya a **Configuración** > **Notificaciones por correo electrónico**.
2. En la pantalla **Notificaciones por correo electrónico**, haga clic en el icono de **...** de la directiva de notificaciones por correo electrónico.
3. Haga clic en **Eliminar** y, luego, en **Confirmar**.

Ver datos de supervisión

Para cada carga de trabajo, puede ver la lista de monitores aplicados, el estado actual de los monitores y los detalles históricos del rendimiento en una vista gráfica. Puede usar esta información para analizar el estado del recurso informático y cómo ha cambiado el estado con el tiempo.

Requisitos previos

- El plan de supervisión se aplica a la carga de trabajo.
- La carga de trabajo está en línea y tiene datos para el monitor correspondiente.

- La versión del agente que está instalada en la carga de trabajo es compatible con los planes de supervisión.

Pasos para ver los monitores aplicados a una carga de trabajo y los datos del monitor

1. En la consola de Protección, vaya a **Dispositivos** > **Todos los dispositivos**.
2. Haga clic en una carga de trabajo y luego en la pestaña **Supervisión**.
   La pestaña **Supervisión** muestra un widget para cada monitor que está habilitado para la carga de trabajo. Cada widget muestra la siguiente información:

Información mostrada	Descripción
Nombre del monitor	El nombre del monitor
Último resultado	El valor más reciente del parámetro supervisado o el estado más reciente del evento
Última comprobación	La fecha y la hora en las que el monitor recopiló los últimos datos
Alertas	El número de alertas que ha generado el monitor y aún no se han resuelto. Si hay al menos una alerta sin resolver generada por este monitor, al hacer clic en el número se abrirá la pestaña **Alertas**. Las alertas se filtrarán y solo se mostrarán las de este monitor.

   Nota
   Los widgets se verán en la pestaña 15 minutos (o la frecuencia de supervisión mínima establecida para el monitor) después de aplicar un plan de supervisión a la carga de trabajo.

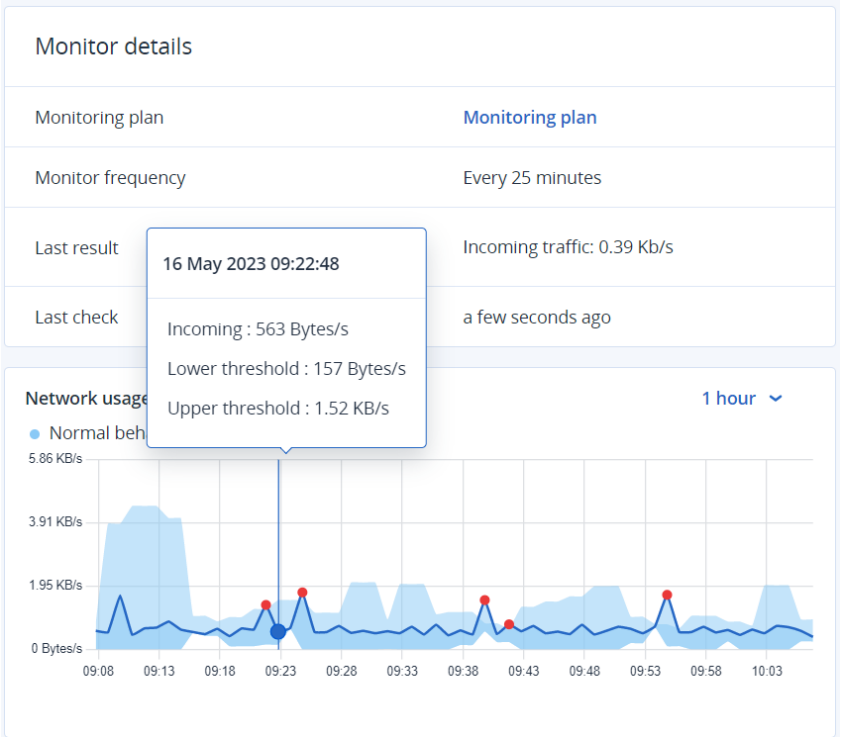
3. [Opcional] Para ver más información sobre el monitor, y si aplica, los datos históricos recopilados para el parámetro supervisado, en el widget del monitor, haga clic en el icono de puntos suspensivos y, a continuación, en **Detalles**.
   Para obtener más información acerca de los detalles de monitor que puede ver en los widgets, consulte "Widgets de supervisión" (p. 1203).

Widgets de supervisión

En el widget de supervisión, puede ver la siguiente información acerca de la supervisión.

Detalle	Descripción
Plan de supervisión	El nombre del plan de supervisión que incluye la supervisión. El nombre del plan de supervisión es un enlace que abre el plan de supervisión en el modo de vista.
Frecuencia del	El intervalo de tiempo durante el cual el monitor recopila datos de la carga

Detalle	Descripción
monitor	de trabajo
Último resultado	El valor más reciente del parámetro supervisado o el estado más reciente del evento
Última comprobación	La fecha y la hora en las que el monitor recopiló los últimos datos
Última alerta	La fecha y la hora en las que se generó la última alerta. El campo se muestra solo si se ha generado al menos una alerta para el monitor.
Gráfico histórico	Para los monitores que recogen datos de series temporales, el widget muestra datos históricos para un período seleccionado (1 hora, 6 horas, 12 horas, 1 día, 1 semana o 1 mes) en una vista gráfica. El gráfico muestra los valores reales de los parámetros durante el período que seleccione. Si por alguna razón el agente no ha enviado los datos recopilados a la nube, los valores faltantes se muestran como una línea punteada que conecta los puntos de datos con valores reales que preceden y siguen al valor faltante. Para los monitores que utilizan la supervisión **Basada en anomalías**, el gráfico muestra el área de líneas base, una línea que muestra los valores reales de la métrica y las anomalías. Las anomalías son los picos o los valores que están fuera de las líneas de base y se muestran como puntos rojos en el gráfico. Si pasa el ratón por encima de la gráfica, podrá ver el valor real y los valores del umbral para un momento específico.

Detalle	Descripción
	 **Nota** Los datos de los gráficos se muestran en la zona horario del sistema local. Se trata de la zona horaria del navegador de la carga de trabajo por la que accede a la consola de Protección.