Acronis

acronis.com

Acronis Cyber Appliance

Guía de inicio rápido

REVISIÓN: 03/08/2021

Contenido

1 Acerca de Acronis Cyber Appliance ... 3

1.1 Acronis Cyber Appliance exterior ... 3

2 Instrucciones de seguridad ... 5

3 Instalación de Acronis Cyber Appliance ... 6

3.1 Extraer Acronis Cyber Appliance ... 6

3.2 Montaje de Acronis Cyber Appliance en el bastidor ... 6

3.3 Conectar cables a Acronis Cyber Appliance ... 9

3.4 Configurar Acronis Cyber Appliance ... 11

3.4.1 Crear un clúster nuevo ... 11

3.4.2 Unirse al clúster existente ... 14

3.4.3 Configurar el clúster a través del panel de administración ... 17

4 Gestión de licencias ... 18

4.1 Instalación de claves de licencia ... 19

4.2 Instalación de licencias SPLA ... 20

5 Gestión de actualizaciones ... 21

6 Configuración de Acronis Cyber Infrastructure y Acronis Cyber Protect ... 24

6.1 Implementar el clúster de procesamiento ... 24

6.2 Implementar la máquina virtual del dispositivo todo en uno de Acronis Cyber Protect ... 24

6.2.1 Descargar la máquina virtual del dispositivo todo en uno de Acronis Cyber Protect ... 24

6.2.2 Implementar el dispositivo todo en uno de Acronis Cyber Protect ... 25

6.3 Creación del almacenamiento de copias de seguridad ... 27

6.4 Realizar operaciones de copias de seguridad ... 28

6.4.1 Añadir los equipos de los que se va a hacer una copia de seguridad ... 28

6.4.2 Configuración de un plan de protección ... 28

7 Obtener soporte técnico ... 31

8 Anexo: Especificaciones ... 32

8.1 Especificaciones técnicas ... 32

8.1.1 Especificaciones del suministro de alimentación ... 32

8.2 Especificaciones medioambientales ... 33

8.2.1 Requisitos de calidad del aire ... 34

1 Acerca de Acronis Cyber Appliance

Acronis Cyber Appliance ofrece un clúster de 5 nodos Acronis Cyber Infrastructure en tres chasis de servidor montados en bastidor de 19 pulgadas. Acronis Cyber Appliance se implementa en una solución de infraestructura definida por un software universal y fácil de usar que combina virtualización y almacenamiento. Gracias a Acronis Cyber Infrastructure, puede crear y administrar máquinas virtuales y disponer de almacenamiento de archivos, bloques y objetos, incluido un repositorio local para copias de seguridad en la nube. También puede implementar Acronis Cyber Protect en el clúster de procesamiento de Acronis Cyber Infrastructure y que tanto el almacenamiento como la copia de seguridad del servidor se ejecuten en Acronis Cyber Appliance.

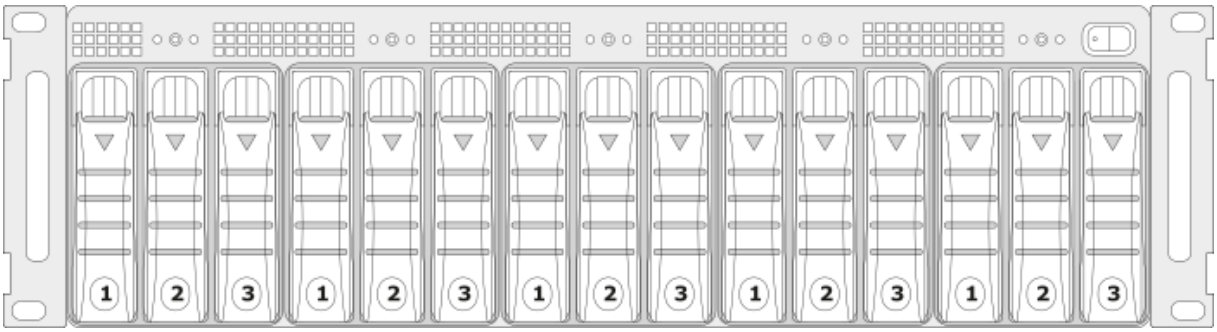
Existen varios modelos de Acronis Cyber Appliance según su capacidad de almacenamiento:

Modelo	Almacenamiento sin formato, TB	Almacenamiento utilizable[1], TB	
		Capacidad	Rendimiento
15031	60	31	18
15062	120	62	36
15078	150	78	45
15093	180	93	54
15108	210	108	60
15124	240	124	69

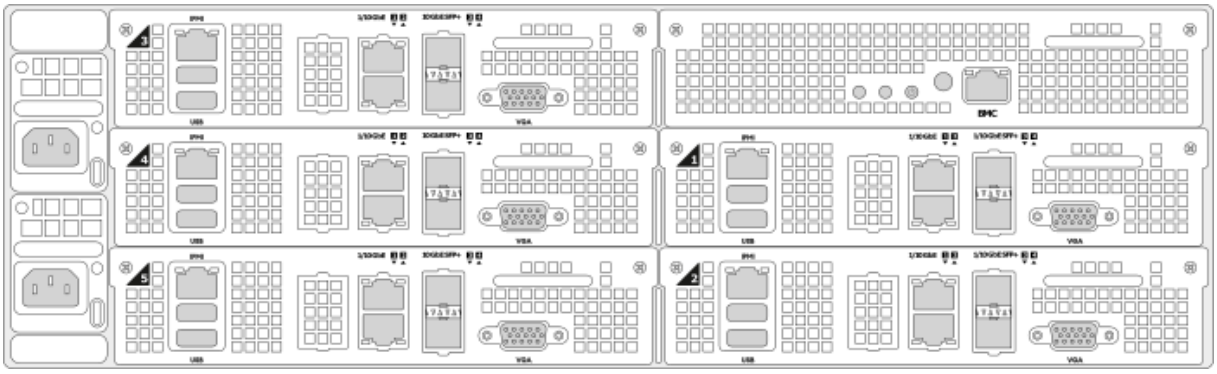
[1]Con el esquema de redundancia recomendado. Se recomienda la codificación de borrado 3+2 para la capacidad y la replicación=3 para el rendimiento.

1.1 Acronis Cyber Appliance exterior

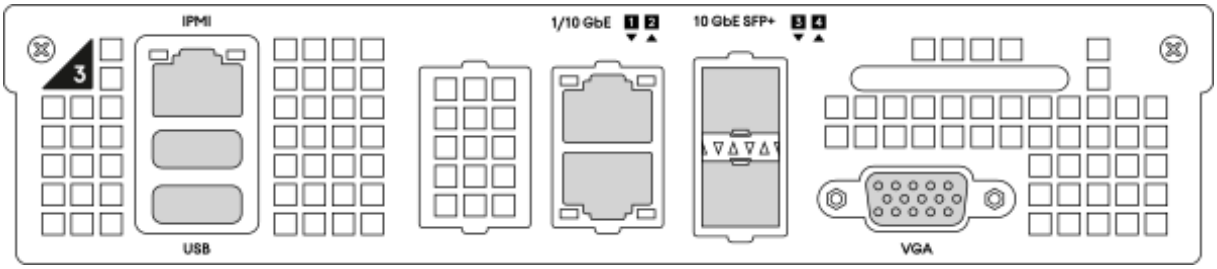
Acronis Cyber Appliance cuenta con cinco nodos idénticos. En la parte frontal del dispositivo, bajo el bisel frontal, se encuentran los botones de encendido y apagado y restablecer, un LED de encendido para cada nodo y el conmutador de energía principal. El panel frontal también ofrece acceso a los discos de cada nodo: tres por nodo, ordenados de izquierda a derecha. Por ejemplo, los tres discos a la izquierda son del primer nodo, los tres siguientes son del segundo, y así sucesivamente.



En la parte posterior de Acronis Cyber Appliance hay dos tomas de corriente y una serie de opciones de conectividad.



Cada nodo tiene sus propios puertos de red, IPMI, USB y VGA.



Los puertos IPMI, USB y VGA solo son necesarios para diagnósticos avanzados. IPMI permite acceder a los nodos mediante la red para su gestión fuera de banda con una consola remota. La contraseña IPMI predeterminada para acceder al nodo de administración mediante SSH es **Acronis!Infra%30** (cambia a una contraseña especificada por el usuario cuando se está implementando). Los puertos USB y VGA permiten conectar un teclado y monitor a un nodo si la red no está disponible.

La administración diaria de Acronis Cyber Appliance se realiza mediante la red con el panel de administración, como se describe posteriormente en esta guía.

2 Instrucciones de seguridad

Advertencia.
Solo un técnico de servicio certificado puede reparar Acronis Cyber Appliance. Solo puede realizar las operaciones de resolución de problemas que autorice el equipo de soporte técnico. La garantía no cubre los daños causados por reparaciones no autorizadas.

Si necesita restablecer un nodo a la configuración predeterminada de fábrica, póngase en contacto con el equipo de soporte técnico, como se describe en "Obtener soporte técnico" (p. 31).

3 Instalación de Acronis Cyber Appliance

Antes de instalar Acronis Cyber Appliance, asegúrese de que cuenta con:

- 3 espacios de bastidor del servidor en un gabinete estándar de 19 pulgadas
- Al menos cinco puertos de entre 1 y 10 GbE libres en un conmutador de red (se recomiendan 10 GbE)
- Al menos cinco cables de remiendo RJ45 a RJ45 para conectar el dispositivo al conmutador
- Dos tomas de corriente

Si quiere configurar el enlace a la red, también necesitará (a) cinco puertos de entre 1 y 10 GbE libres en un conmutador de red (se recomiendan 10 GbE) y (b) cinco cables de remiendo RJ45 a RJ45 para conectar el dispositivo al conmutador.

Si desea obtener acceso a los nodos desde una consola remota para realizar administración fuera de banda, también necesitará (a) seis puertos de 1 GbE libres en un conmutador de red y (b) seis cables de remiendo RJ45 a RJ45 para conectar el dispositivo al conmutador.

Siga los siguientes pasos para instalar Acronis Cyber Appliance:

1. Extraiga Acronis Cyber Appliance.
2. Monte el dispositivo en un bastidor.
3. Conecte los cables al dispositivo.
4. Configure Acronis Cyber Appliance con el asistente.
5. Inicie sesión en el panel de administración e instale una licencia.
6. Configure las cargas de trabajo deseadas en el panel de administración.

En las siguientes secciones se describen del primer al quinto paso. Para obtener más información sobre el sexto paso, consulte la Guía del administrador.

3.1 Extraer Acronis Cyber Appliance

Antes de montar el dispositivo y conectarlo, examine el contenido del embalaje para asegurarse de que no presenta daños.

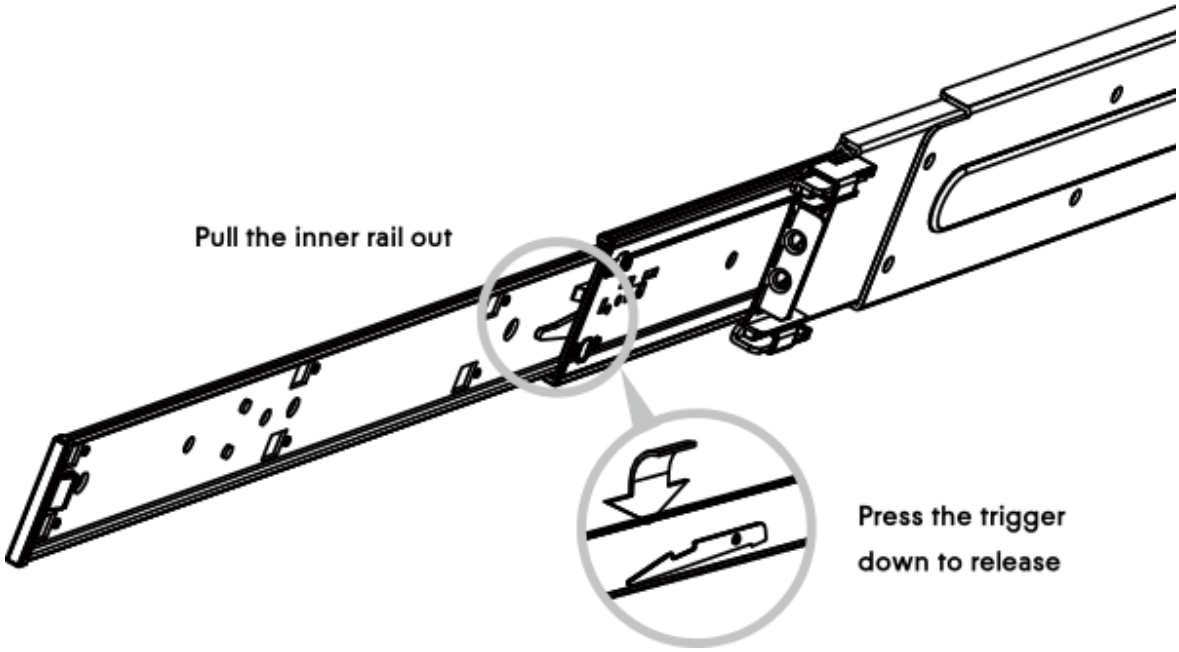
Antes de continuar, asegúrese de que los siguientes contenidos se encuentren en el embalaje: el chasis del dispositivo, los raíles de montaje, dos cables de alimentación y esta guía de inicio rápido.

3.2 Montaje de Acronis Cyber Appliance en el bastidor

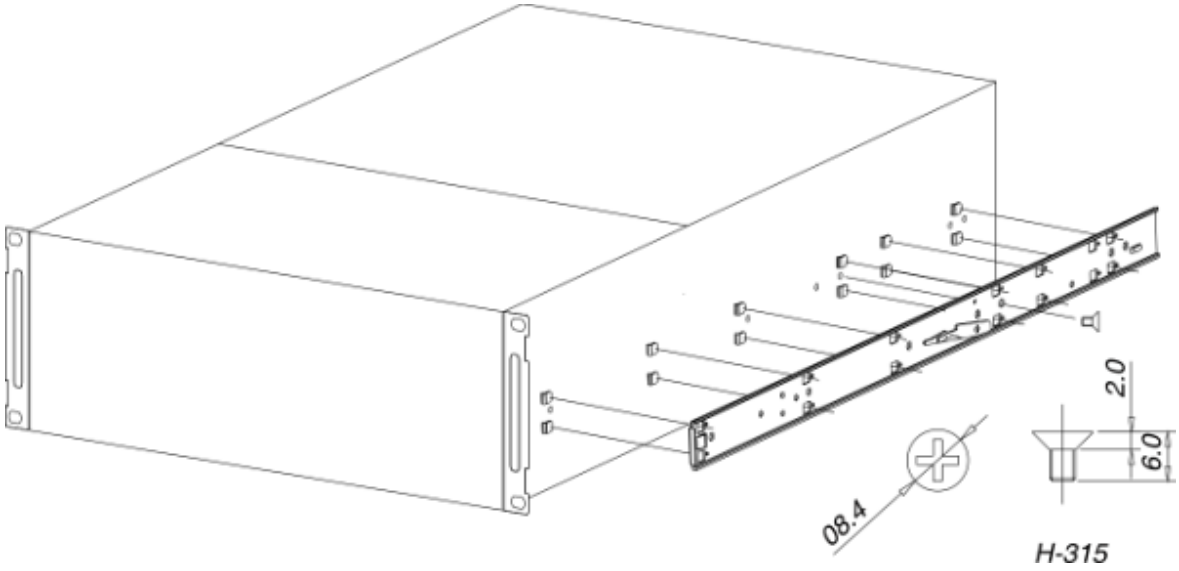
El dispositivo incluye un conjunto de rieles de servidor. Siga los siguientes pasos para instalar el riel y montar Acronis Cyber Appliance en el bastidor.

1. Separe los raíles internos y externos.

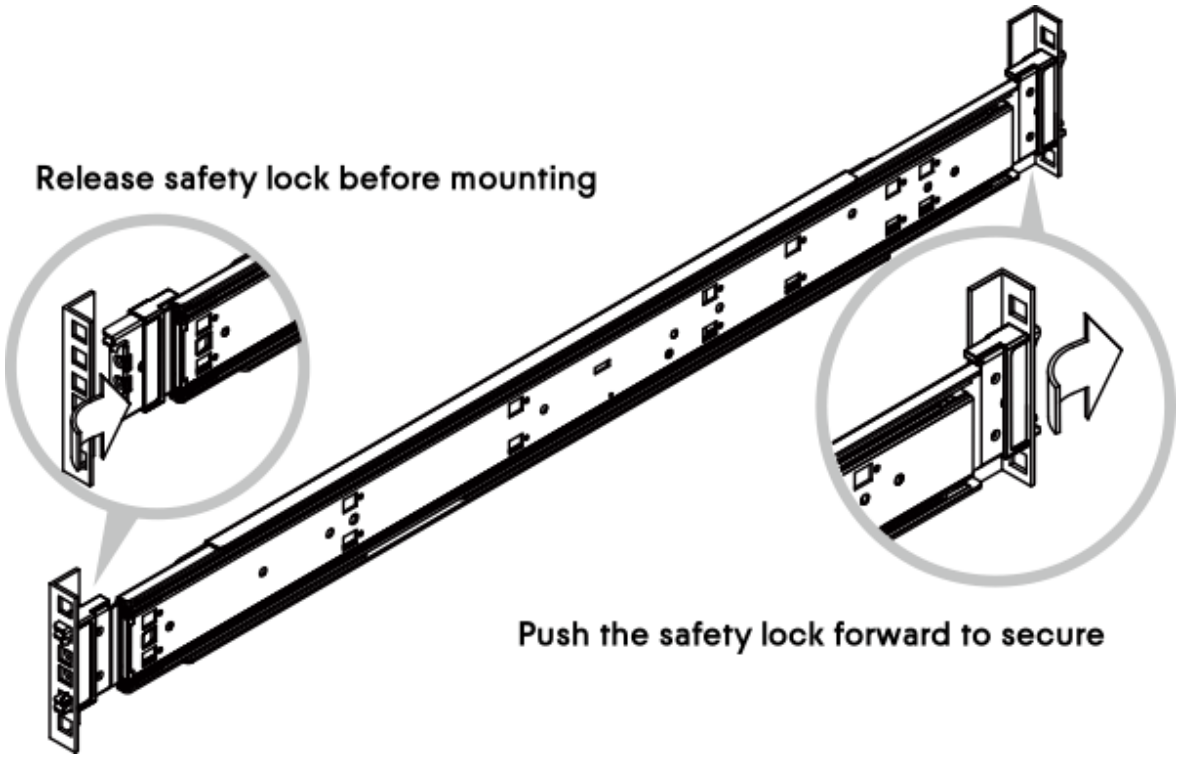
   Separe el raíl interno del externo deslizándolo hacia delante hasta que se pueda ver la pestaña de bloqueo, según se muestra en la siguiente ilustración. Apriete la pestaña y separe el raíl interno del externo deslizándolos.



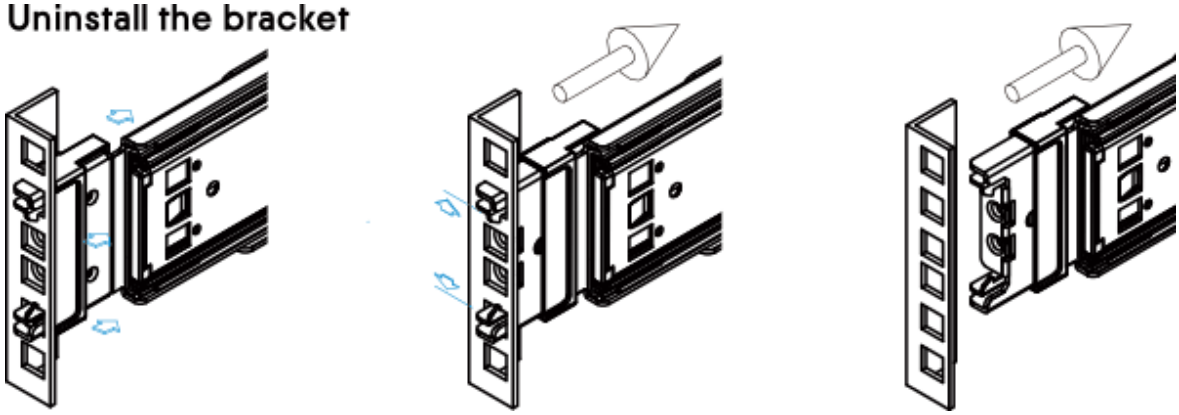
2. Acople el raíl interno al dispositivo.
   Nivele las líneas rectangulares del raíl interno a las bayonetas premoldeadas en el lateral del chasis. Fije el raíl interno con un conjunto de tornillos después de que las bayonetas hayan atravesado las líneas y se hayan acoplado correctamente.



3. Instale el raíl externo en el bastidor.
   Al seleccionar la ubicación, fíjese en que los raíles estén en el centro del dispositivo. Asegúrese de instalar los raíles externos dejando un espacio libre por encima y por debajo.
   Asegúrese de que el cierre de seguridad esté desbloqueado cuando vaya a montar los soportes.
   Inserte los pasadores de sujeción en los agujeros cuadrados superiores e inferiores del raíl, desde la parte posterior. Empuje hacia delante el cierre de seguridad para fijar el soporte.



Uninstall the bracket

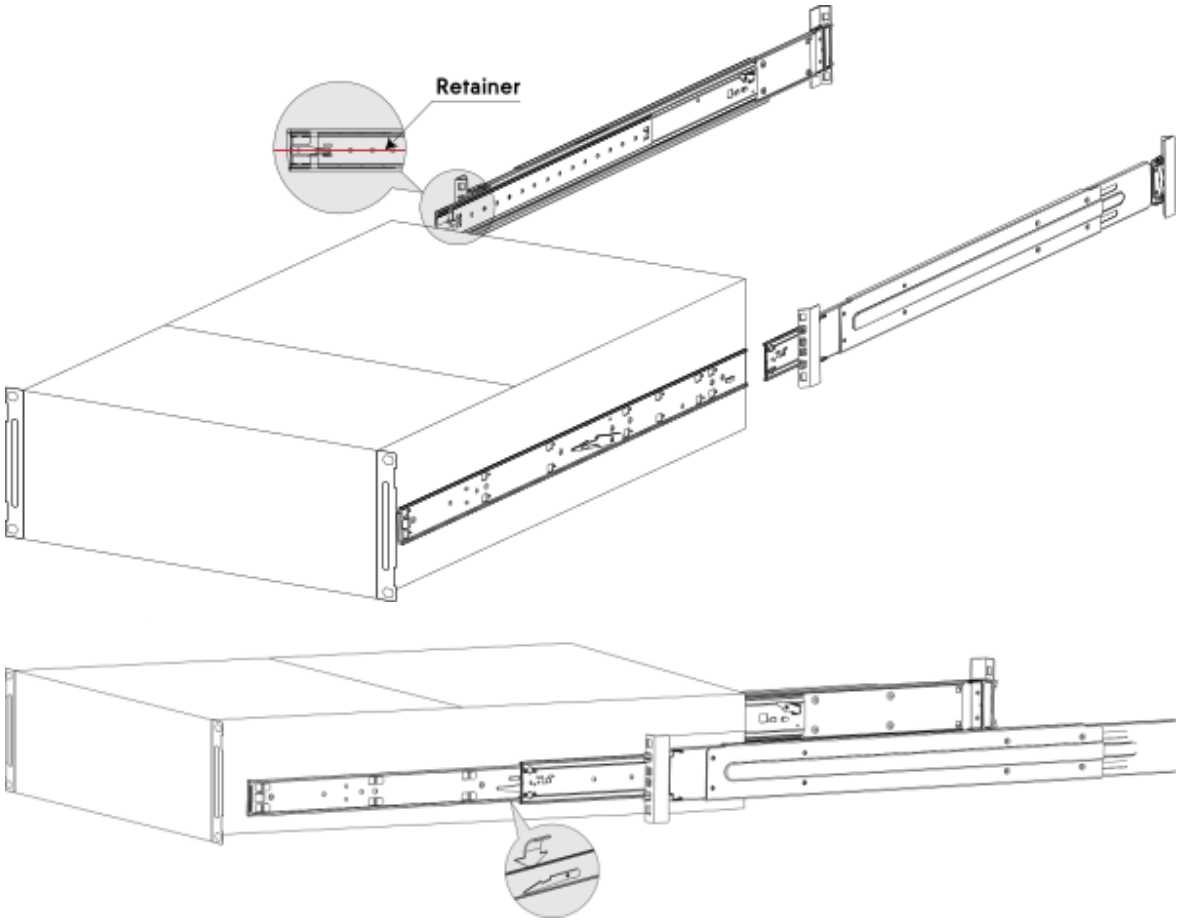


4. Monte el chasis en el bastidor.

Importante
Es necesario que este paso lo realicen dos personas.

Inserte el raíl interno en el externo, como se muestra en la figura.

Importante
Asegúrese de que el gancho de bolas esté totalmente abierto antes de instalar el chasis. De lo contrario, se podría dañar el chasis.

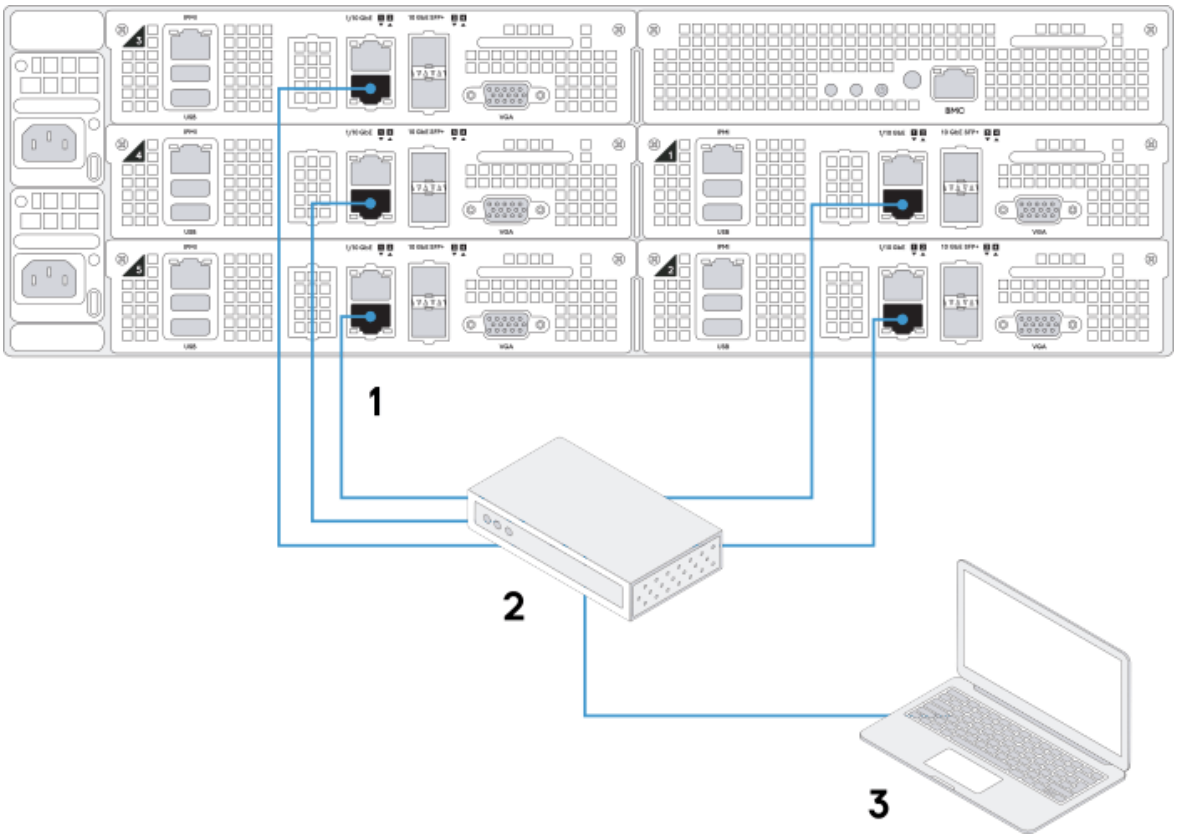


3.3 Conectar cables a Acronis Cyber Appliance

Nota
Para obtener más información sobre la configuración de la infraestructura de red, consulte la Guía del administrador.

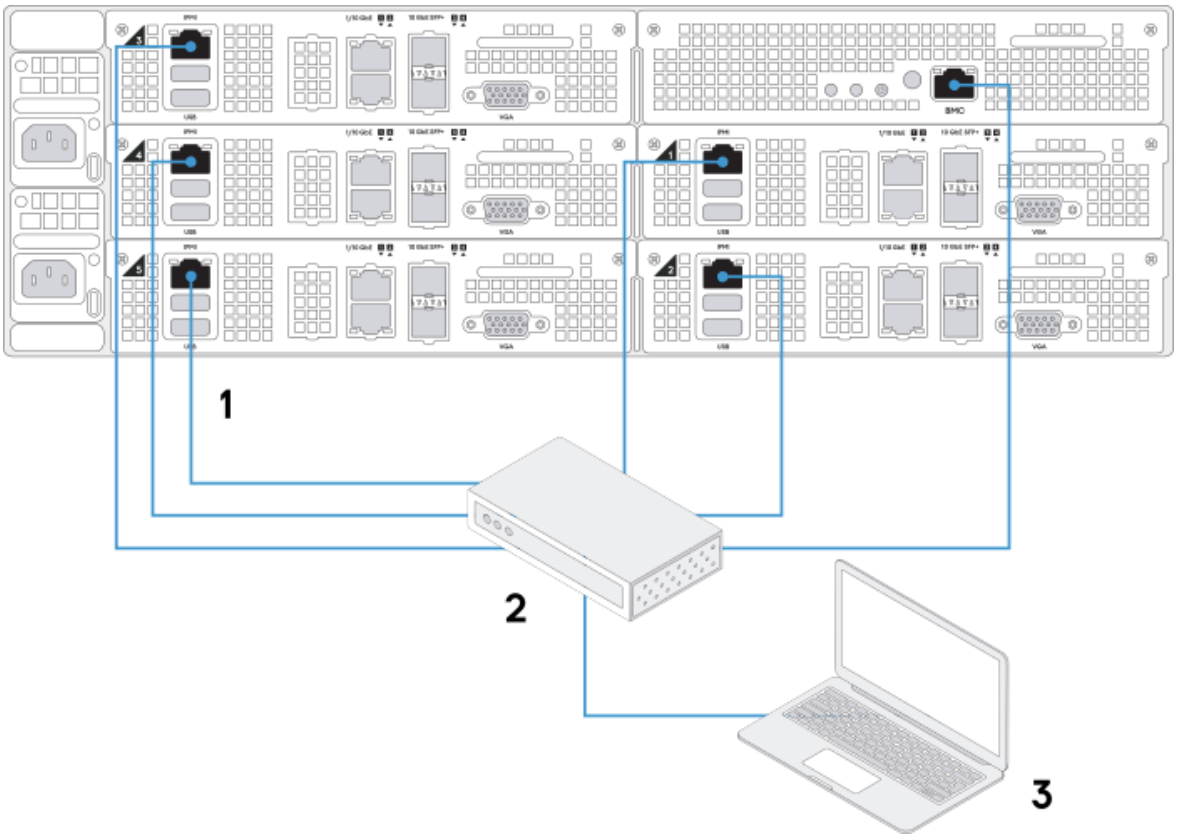
Para preparar Acronis Cyber Appliance para configurarlo, haga lo siguiente:

1. Conecte el dispositivo a las tomas de corriente con los cables de alimentación suministrados.
2. Conecte los puertos SFP+ o RJ45 de todos los nodos (**1** en el diagrama) a un conmutador (**2** en el diagrama) con acceso a una subred dedicada a su infraestructura. Después, conecte el portátil de administración (**3** en el diagrama) al mismo conmutador. El siguiente diagrama presenta un ejemplo de la conexión por cable.



Importante
Los nodos tienen direcciones IP preconfiguradas: de 10.20.20.11 a 10.20.20.15.

3. (Opcional) Conecte las interfaces de red de administración fuera de banda de cada nodo y (**1** en el diagrama) a un conmutador con acceso a una subred IPMI de su dispositivo (**2** en el diagrama). Los nodos tienen direcciones IP IPMI preconfiguradas: de 10.20.30.11 a 10.20.30.15. El chasis tiene la dirección IP IPMI 10.20.30.10. Conecte el portátil de administración (**3** en el diagrama) al mismo conmutador.



3.4 Configurar Acronis Cyber Appliance

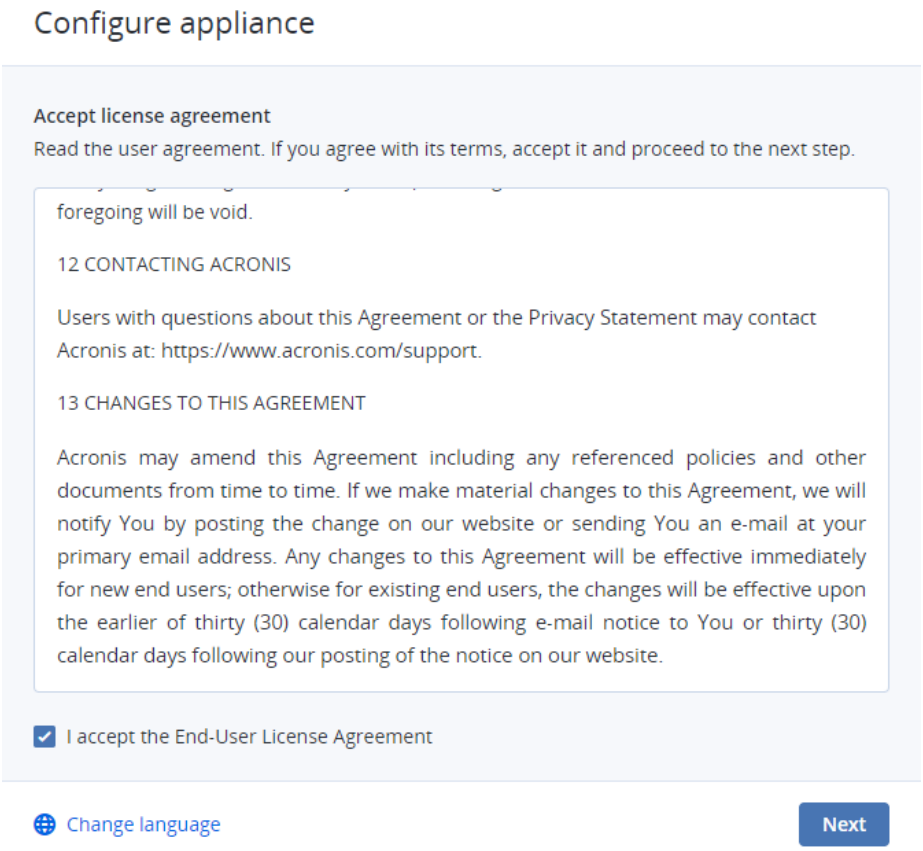
Siga los siguientes pasos para configurar Acronis Cyber Appliance:

1. Encienda el dispositivo al (a) mantener pulsado el conmutador principal durante cinco segundos o (b) pulsar los botones de encendido de cada nodo.
2. Conecte a la red un portátil de administración desde el que va a configurar Acronis Cyber Appliance. Asígnele una IP estática de la misma subred en la que se encuentren los nodos, como 10.20.20.100. Como ya se ha mencionado, los nodos tienen direcciones IP preconfiguradas: de 10.20.20.11 a 10.20.20.15.
3. En este equipo, abra un navegador web y visite la dirección IP predeterminada del nodo principal, 10.20.20.11. Se ha probado el asistente de configuración y funciona con las versiones más recientes de los navegadores web Firefox, Chrome y Safari.

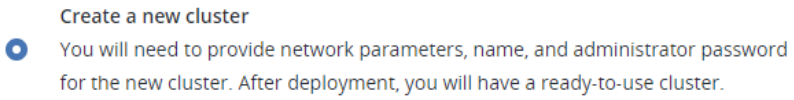
En el asistente, puede crear un clúster nuevo o conectar el dispositivo a un clúster que ya se haya creado con Acronis Cyber Infrastructure.

3.4.1 Crear un clúster nuevo

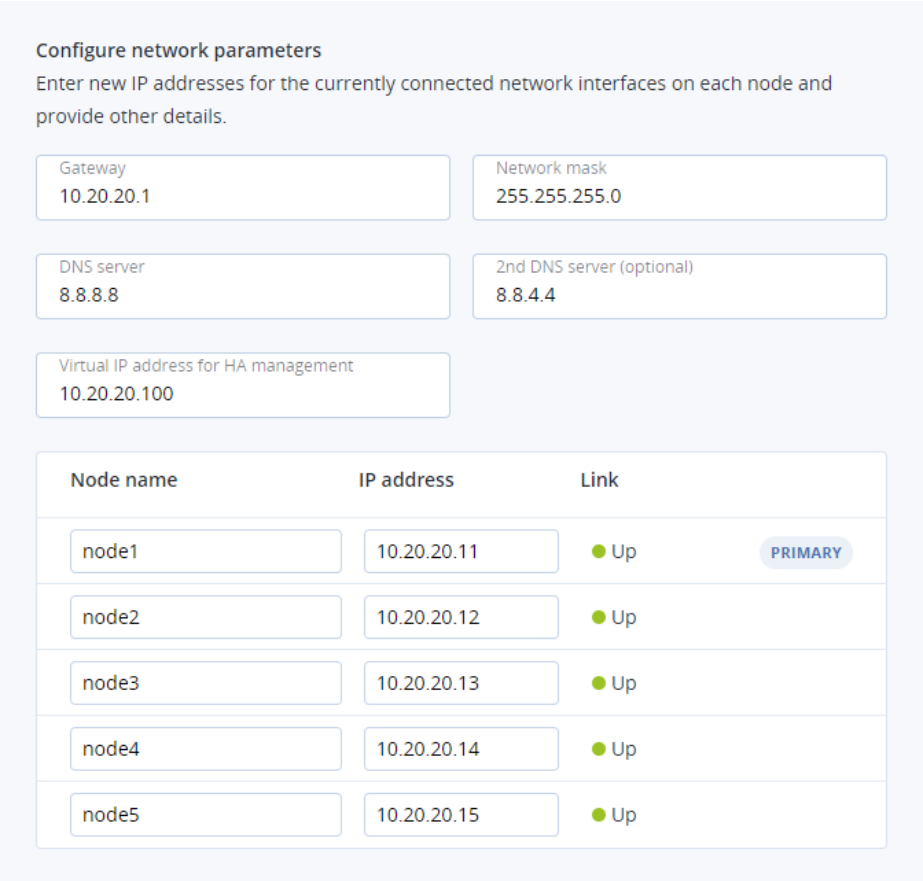
1. Cuando aparezca el asistente de configuración, haga clic en **Configurar**. No desconecte el dispositivo hasta que termine la configuración.
2. Lea y acepte el acuerdo de licencia. Después, haga clic en **Siguiente**.



3. En el siguiente paso, seleccione **Crear un clúster nuevo**.



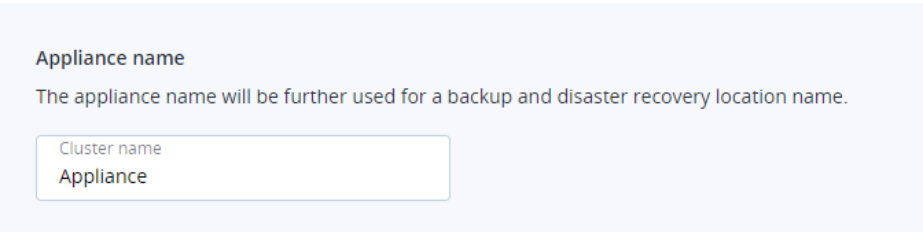
4. En **Configurar parámetros de red**, introduzca lo siguiente:
   - Una puerta de enlace. Consulte con su administrador de red para escoger dirección de puerta de enlace adecuada.
   - Una máscara de red. Consulte con su administrador de red para escoger la máscara de red o subred adecuada.
   - Al menos un servidor DNS local.
   - Una dirección IP virtual en la cual accederá al panel de administración. Puede obtener más información sobre su alta disponibilidad en «Habilitar alta disponibilidad del nodo de administración» de la Guía del administrador.
   - Nuevos nombres de servidor para los nodos (o bien mantenga los nombres predeterminados). Cada nodo debe tener únicamente un nombre. De lo contrario, la instalación se interrumpirá. Puede cambiar los nombres de los nodos para que cumplan las directivas de nombres de su organización.
   - Nuevas direcciones IP estáticas para las interfaces de red conectadas a todos los nodos. Si deja vacíos los campos, se usarán las direcciones predeterminadas de 10.20.20.11 a 10.20.20.15.



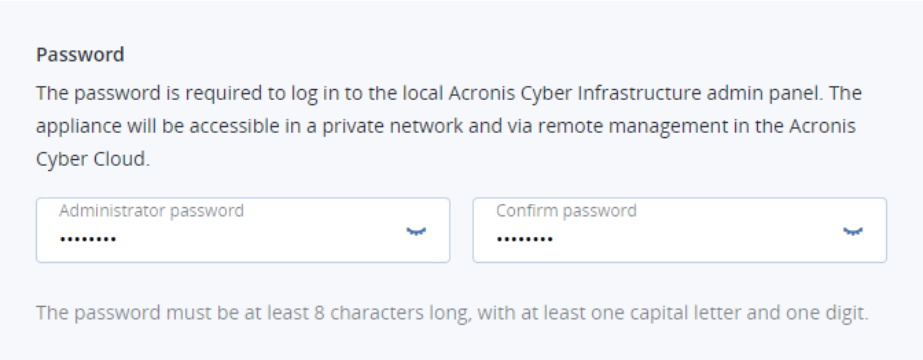
Si no es posible alcanzar uno o más nodos desde el principal, se marcarán como fuera de línea. En este caso, asegúrese de que los nodos están encendidos y conectados a la red correspondiente. Se bloqueará la implementación hasta que todos los nodos muestren una luz verde (que significa que el modo principal puede acceder a ellos y configurarlos).

Nota
Después podrá configurar enlaces y LAN virtuales en el panel de administración.

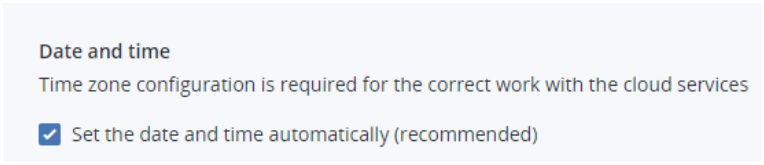
5. En **Nombre del dispositivo**, introduzca el nombre del clúster. No podrá cambiarlo.



6. En **Contraseña**, indique una contraseña para acceder al panel de administración local de Acronis Cyber Infrastructure.



7. En **Fecha y hora**, se recomienda seleccionar la casilla de verificación **Establecer fecha y hora automáticamente**. Puede borrarla y seleccionar una zona horaria y una hora personalizadas. Tenga en cuenta que los nodos se comunican unos con otros. Por ello, deben encontrarse en la misma zona horaria y tener configurada la misma hora para garantizar su correcta sincronización.

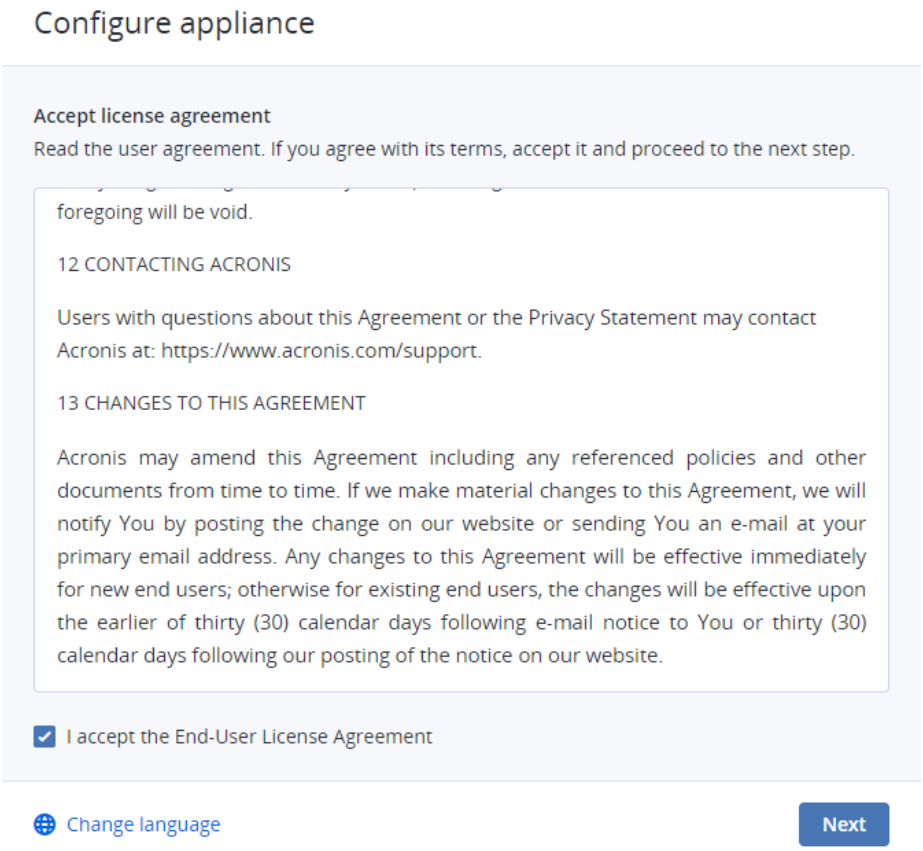


8. Haga clic en **Enviar**. Comenzará la configuración, tal y como se indicará en la barra de progreso.
9. Espere a que la barra de progreso avance hasta el final. Si ha cambiado las direcciones IP predeterminadas de los nodos, asigne una dirección IP estática a la nueva subred de los nodos y al portátil de administración desde el que acceda a Acronis Cyber Appliance.

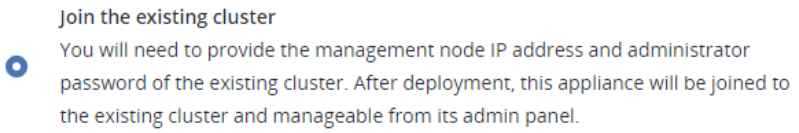
3.4.2 Unirse al clúster existente

Puede conectar el dispositivo al clúster de Acronis Cyber Infrastructure existente. Para ello, necesitará la dirección IP privada del nodo de administración y las credenciales de administrador del clúster existente. Una vez configurado el dispositivo, se añadirán los cinco nodos y se administrarán desde el panel de administración del clúster existente.

1. Cuando aparezca el asistente de configuración, haga clic en **Configurar**. No desconecte el dispositivo hasta que termine la configuración.
2. Lea y acepte el acuerdo de licencia. Después, haga clic en **Siguiente**.



3. En el siguiente paso, seleccione **Unirse al clúster existente**.



4. En **Configurar parámetros de red**, introduzca lo siguiente:
   - Una máscara de red. Consulte con su administrador de red para escoger la máscara de red o subred adecuada.
   - Nuevos nombres de servidor para los nodos (o bien mantenga los nombres predeterminados). Puede cambiar los nombres de los nodos para que cumplan las directivas de nombres de su organización.

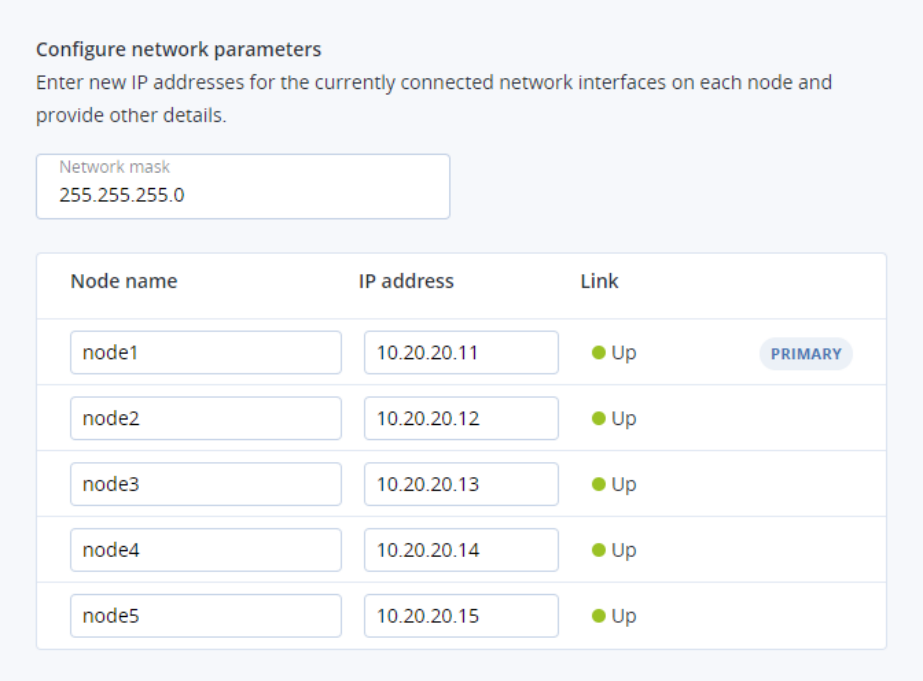
     Nota
     Cada nodo del clúster existente y del dispositivo debe tener únicamente un nombre. Si al menos dos nodos tienen el mismo nombre, la instalación se detendrá.

   - Nuevas direcciones IP estáticas para las interfaces de red conectadas a todos los nodos.

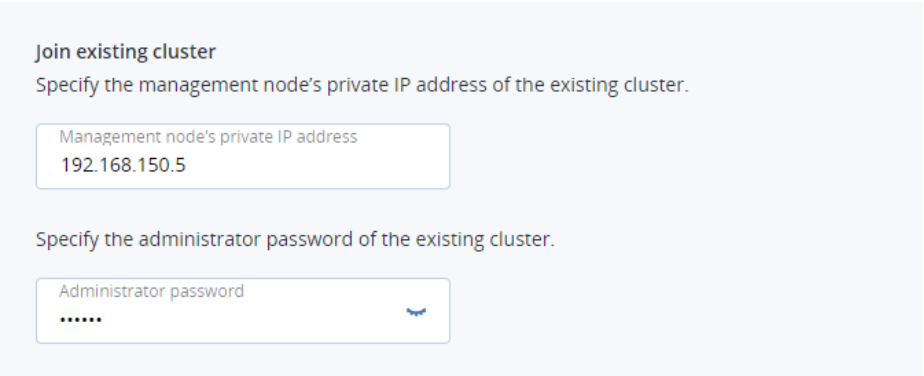
Nota
Utilice las direcciones IP de la red/subred del clúster existente. La instalación se bloqueará hasta que se asignen direcciones IP de la misma subred/red a los cinco nodos como en el clúster existente.

Si no es posible alcanzar uno o más nodos desde el principal, se marcarán como fuera de línea. En este caso, asegúrese de que los nodos están encendidos y conectados a la red correspondiente. Se bloqueará la implementación hasta que todos los nodos muestren una luz verde (que significa que el modo principal puede acceder a ellos y configurarlos).

Nota
Después podrá configurar enlaces y LAN virtuales en el panel de administración.



5. En **Unirse al clúster existente**, introduzca la dirección IP privada del nodo de administración y la contraseña de administrador del clúster existente.



6. Durante la implementación, se comparan las versiones Acronis Cyber Infrastructure del clúster existente y del dispositivo. Si hay discrepancias importantes, se le pedirá que especifique una

configuración de red para acceder a Internet. Después, se descargarán las actualizaciones necesarias y el dispositivo se mejorará o se revertirá para ajustarse a la versión del clúster existente.

3.4.3 Configurar el clúster a través del panel de administración

1. En cuanto se complete la configuración, verá un enlace al panel de administración del clúster. Inicie sesión con el nombre de usuario y la contraseña del clúster.
2. Si debe realizar cambios adicionales en la configuración de red, por ejemplo, crear enlaces y LAN virtuales, conecte los cables a los otros puertos de red y siga las instrucciones de «Creación de acoplamientos de red» y «Creación de interfaces VLAN» en la Guía del administrador.
3. Si ha creado un clúster nuevo, actualice el producto a la última versión antes de implementarlo (consulte "Gestión de actualizaciones" (p. 21)). Acceda a **Configuración** > **Licencias** y actualice la licencia de prueba predeterminada mediante clave o SPLA (para obtener más información, consulte "Gestión de licencias" (p. 18)). Si no tiene licencia, contacte con su representante de ventas.
4. Después, podrá configurar el clúster para utilizar Acronis Cyber Protect (consulte "Configuración de Acronis Cyber Infrastructure y Acronis Cyber Protect" (p. 24)) o la carga de trabajo que necesite tal y como se describe en la Guía del administrador.

4 Gestión de licencias

Acronis Cyber Appliance tiene licencia para dos tipos de implementaciones:

- Nube híbrida. Incluye una garantía de hardware de 3 años y requiere una suscripción a Acronis Cyber Protect Cloud. Al cabo de 3 años, la garantía del hardware debe renovarse por otro período de 1 o 3 años.

  Este tipo de implementación requiere la instalación de una licencia SPLA, tal y como se describe en "Instalación de licencias SPLA" (p. 20).
- Nube privada. Incluye una licencia de 3 años para Acronis Cyber Infrastructure y garantía de hardware. Al cabo de 3 años, tanto la licencia como la garantía deben renovarse por otro período de 1 o 3 años.

  Este tipo de implementación requiere la instalación de una clave de licencia, tal y como se describe en "Instalación de claves de licencia" (p. 19).

Para obtener más información sobre las opciones de licencia, consulte https://kb.acronis.com/content/62324.

Acronis Cyber Infrastructure admite los siguientes modelos de licencias para los entornos de producción:

- Clave de licencia. Si se implementa el modelo de aprovisionamiento, las claves son de tiempo limitado (suscripción) o perpetuas y conceden una determinada capacidad de almacenamiento. Si ya existe una licencia comercial instalada, la clave aumenta la fecha de caducidad o el límite de almacenamiento.
- Acuerdo de licencia del proveedor de servicios (SPLA). El SPLA implementa un modelo de pago por uso: concede una capacidad de almacenamiento ilimitada y se cobra a los clientes por su uso real de estos recursos. Con un SPLA, Acronis Cyber Infrastructure envía automáticamente informes a Acronis Cyber Cloud cada cuatro horas. La licencia se muestra con una fecha de caducidad de dos semanas, que dura desde el último informe enviado hasta después de cada informe. Si no se reciben informes durante dos semanas, la licencia caduca. Para que los informes lleguen a su destino, el clúster debe ser capaz de acceder al centro de datos de Acronis que se ha utilizado para habilitar el SPLA. Asegúrese de que el puerto TCP 443 está abierto.

  Nota
  Una licencia SPLA es válida para Cloud Partners. Si hay un SPLA habilitado, solo puede conectar Backup Gateway con Acronis Cyber Protect Cloud, pero no con Acronis Cyber Protect. Para conectar Backup Gateway a estos productos, deberá utilizar claves de licencia. Además, el uso de Acronis Backup Gateway no se incluye en el SPLA en Acronis Cyber Infrastructure. El SPLA únicamente incluye el uso universal que no está relacionado con la copia de seguridad. El uso de copia de seguridad se muestra en la sección Acronis Cyber Protect Cloud de Acronis Cyber Cloud.

Puede cambiar el modelo de licencia en cualquier momento:

- Si cambia el modo de concesión de licencias (por ejemplo, de una clave de licencia a un SPLA o de una suscripción a una licencia perpetua), se cancela la clave utilizada previamente aunque todavía

no haya caducado. Las claves canceladas ya no se podrán volver a usar.

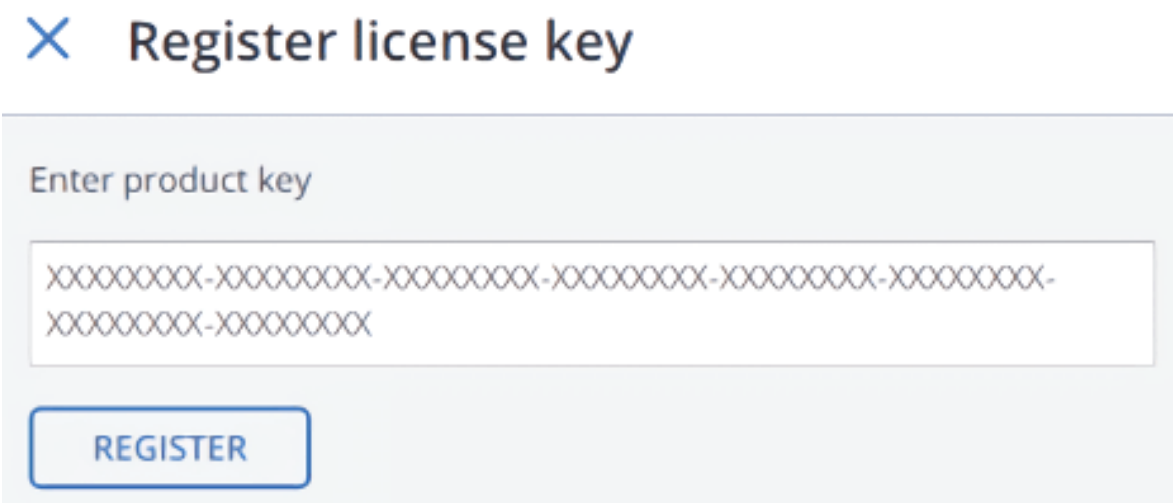
- Si cambia de un SPLA a una clave de licencia, se cambia el modelo de licencia a suscripción o perpetua. Cuando lo haya hecho, pídale a su proveedor de servicios que deshabilite la aplicación de Acronis Cyber Infrastructure de su cuenta o que elimine la cuenta para cancelar su SPLA.

Importante
Si caduca una licencia, todas las operaciones de escritura al clúster de almacenamiento se detienen hasta que se instale una licencia válida.

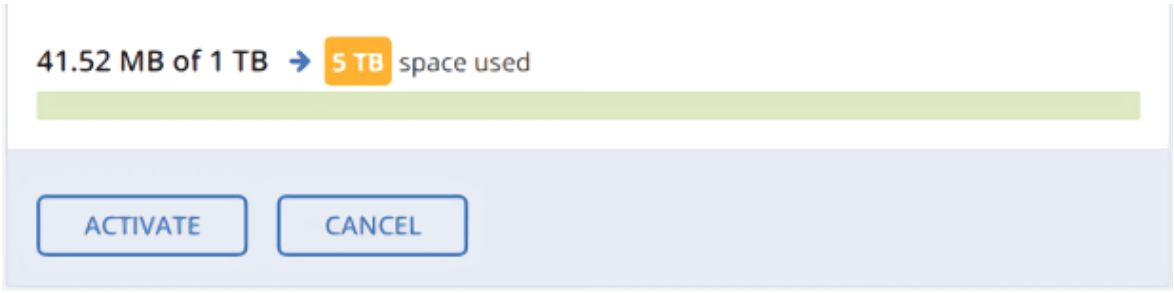
4.1 Instalación de claves de licencia

Para instalar una clave de licencia, haga lo siguiente:

1. Si cambia de un SPLA, solicite a su proveedor de servicios que cancele el acuerdo mediante la deshabilitación de la aplicación Acronis Cyber Infrastructure de su cuenta o la eliminación de la cuenta.
2. En la pantalla **Configuración** > **Licencias**,haga clic en **Mejorar** y luegoen **Registrar clave**.

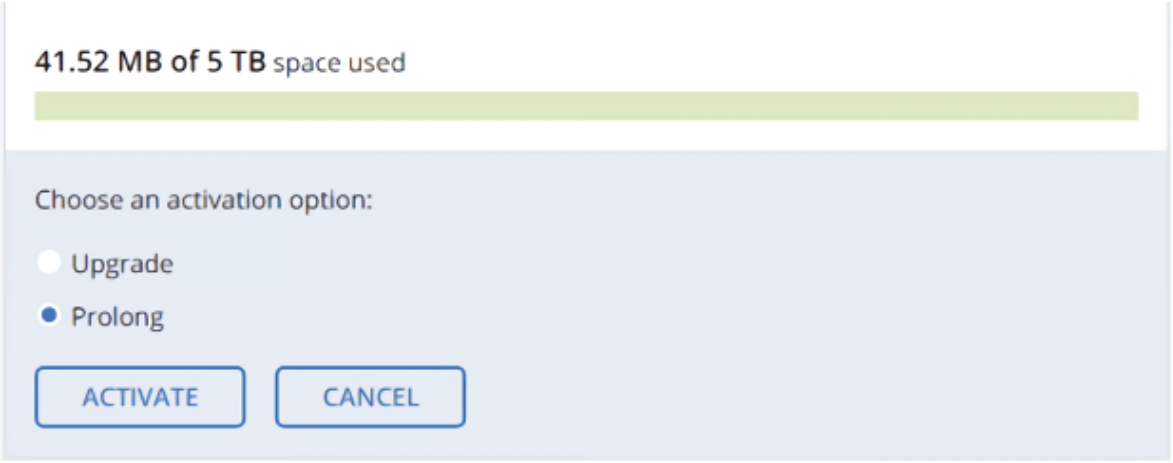


3. En la ventana **Registrar clave licencia**, pegue la clave de licencia y luego haga clic en **Registro**.



4. De vuelta a la pantalla **Licencias**, haga clic en **Activar** si activa a partir de una versión de prueba, o seleccione una de las opciones siguientes:
   - **Actualizar**, para añadir capacidad de almacenamiento a la licencia activa.
   - **Prolongar**, para prolongar la licencia que está a punto de caducar.

Luego haga clic en **Activar**.



La fecha de caducidad o la capacidad de almacenamiento cambiará según lo que otorgue la licencia.

4.2 Instalación de licencias SPLA

Para instalar una licencia SPLA, siga los siguientes pasos:

1. En la pantalla **Configuración** > **Licencias**, haga clic en **Actualizar** y luego haga clic en **Utilizar SPLA**.
2. En la ventana **Utilizar SPLA**, seleccione una región de la lista desplegable. Si su centro de datos no aparece enumerado aquí, introduzca directamente su URL en el campo desplegable, por ejemplo: **https://eu-cloud.acronis.com**. Luego haga clic en **Activar**. Se le redirigirá a la página de inicio de sesión de Acronis Cyber Cloud.

   Nota
   Para obtener más información sobre los centros de datos, consulte https://kb.acronis.com/servicesbydc.

3. Inicie sesión en Acronis Cyber Cloud.
4. En la ventana **Registrar clúster**, acepte el acuerdo de licencia.
5. En la ventana de confirmación del registro, haga clic en **Listo**.

El clúster registrado aparecerá en Acronis Cyber Cloud. Podrá supervisar el uso de los recursos y descargar informes.

5 Gestión de actualizaciones

Acronis Cyber Appliance admite las actualizaciones acumulativas no disruptivas. Los nodos se actualizan uno por uno y la disponibilidad de los datos no se ve afectada. Durante una actualización, un nodo que necesita reiniciarse puede entrar en el modo de mantenimiento. En este caso, las cargas de trabajo y las máquinas virtuales alojadas en este nodo se migran en vivo a otros nodos. Después de la actualización, el nodo vuelve a estar en funcionamiento y las cargas de trabajo y máquinas virtuales migradas vuelven al nodo.

Para obtener más información sobre el modo de mantenimiento, consulte «Realización del mantenimiento de los nodos» en la Guía del administrador.

Puede actualizar diferentes componentes del clúster juntos o de forma independiente. En cualquier caso, los componentes se actualizan en el siguiente orden:

1. Los nodos de clúster se actualizan primero.
2. Los nodos de administración se actualizan solo cuando todos los nodos de clúster están actualizados. El nodo de administración primario es el último en actualizarse.
3. El servicio de procesamiento se actualiza en los nodos de procesamiento y solo cuando todos los nodos, tanto de clúster como de procesamiento, están actualizados.

Para actualizar el kernel con ReadyKernel, consulte «Actualizar el kernel con ReadyKernel» de la Guía de línea de comandos del administrador.

Tenga en cuenta lo siguiente antes de empezar a actualizar nodos:

- Los nodos se deben actualizar únicamente en el panel de administración o mediante la herramienta `vinfra` (consulte «Gestión de actualizaciones» de la Guía de línea de comandos del administrador). No utilice `yum update`.
- Deshabilite los repositorios de terceros.
- Para comprobar si existen actualizaciones y descargarlas, el clúster debe estar en buen estado y cada nodo de la infraestructura debe ser capaz de abrir una conexión de Internet saliente. Esto significa que los nodos no deben estar sin conexión y que el DNS del clúster debe estar configurado y señalar a un DNS capaz de resolver los nombres de los servidores externos. Para obtener más información, consulte «Adición de servidores DNS externos» en la Guía del administrador.
- Los nodos sin asignar no se pueden actualizar.
- Las actualizaciones se aplican a un nodo cada vez.
- Solo puede actualizar los nodos de administración en grupo, junto a los nodos de procesamiento y tras actualizar todos los nodos de clúster.
- Solo puede actualizar el clúster de procesamiento junto a los nodos de administración.

Para actualizar el clúster de almacenamiento del panel de administración, haga lo siguiente:

1. Abra la pantalla **Configuración** > **Actualizaciones**. La fecha de la última comprobación se muestra en la esquina superior derecha. Haga clic en la flecha circular para comprobar si hay nuevas actualizaciones. Si hay actualizaciones disponibles para un componente de clúster, su

estado de actualización cambia a **Disponible**. Si hay que reiniciar un nodo, aparecerá **Es necesario reiniciar** junto a la versión disponible.

2. Haga clic en **Descargar** en la esquina superior derecha para obtener las actualizaciones. Espere hasta que se descarguen las actualizaciones y su estado de actualización cambie a **Listo para instalar**.
3. [Opcional] Haga clic en **Notas de la versión** para leer las notas de la versión.
4. Seleccione los nodos que desee actualizar:
   - Para actualizar los nodos de clúster, seleccione los nodos de clúster deseados.
   - Para actualizar los nodos de administración y el clúster de procesamiento, seleccione todos los nodos de administración, el clúster de procesamiento y los nodos de clúster que necesiten actualizarse.
5. Haga clic en **Actualizar** para continuar.
6. Si ha seleccionado nodos que requieren reiniciar, realice lo siguiente:
   a. Decida si estos nodos entrarán en el nodo de mantenimiento. Seleccione **Modo de mantenimiento** si desea poner los nodos en modo de mantenimiento.
   b. Si ha seleccionado nodos en el servicio de procesamiento, seleccione cómo migrar las máquinas virtuales que se ejecutan en dichos nodos:
      - Con la opción **Ignorar máquinas virtuales que no se pueden migrar en vivo**, las máquinas virtuales de un nodo que entren en el modo de almacenamiento se migrarán en vivo a otros nodos de procesamiento. Se ignorarán las máquinas virtuales que no se pueden migrar en vivo. Esto se aplica a las máquinas virtuales que tengan GPU virtuales o dispositivos PCI conectados o si otros nodos de procesamiento tienen recursos de CPU virtual o RAM insuficientes. Las máquinas virtuales ignoradas seguirán ejecutándose hasta que reinicie o apague el nodo. En este caso, se detendrán y se producirá un tiempo de inactividad. Se iniciarán automáticamente cuando el nodo vuelva a encenderse.
      - Con la opción **Ignorar máquinas virtuales que no se pueden migrar en vivo o que han generado errores al hacerlo**, las máquinas virtuales de un nodo que entren en el modo de almacenamiento se migrarán en vivo a otros nodos de procesamiento. Se ignorarán las máquinas virtuales que no se pueden migrar en vivo. Esto se aplica a las máquinas virtuales que tengan GPU virtuales o dispositivos PCI conectados o si otros nodos de procesamiento tienen recursos de CPU virtual o RAM insuficientes. Aquellas máquinas virtuales ignoradas o que hayan generado errores durante la migración en vivo continuarán ejecutándose hasta que reinicie o apague el nodo. En este caso, se detendrán y se producirá un tiempo de inactividad. Se iniciarán automáticamente cuando el nodo vuelva a encenderse.
      - Con la opción **Migrar en vivo todas las máquinas virtuales**, todas las máquinas virtuales de un nodo que entren en el modo de almacenamiento se migrarán en vivo a otros nodos de procesamiento.
   c. [Opcional] Seleccione **Interrumpir la actualización si el nodo no puede entrar en modo de mantenimiento** para detener la actualización si se produce un error al entrar en mantenimiento.
7. Revise los componentes seleccionados y haga clic en **Instalar**.

Mientras se instalan las actualizaciones, puede poner en pausa o cancelar el proceso. Una vez completada la actualización, el estado de los componentes cambiará a **Actualizado**.

Si la actualización falla, haga clic en **Detalles** para ver los detalles del problema y decidir cómo proceder. Puede cancelar la actualización, resolver los problemas e intentar de nuevo la actualización, sin tiempo de inactividad. De manera alternativa, puede forzar la actualización sin poner los nodos en mantenimiento. Los nodos se reiniciarán, lo que puede provocar un tiempo de inactividad de las cargas de trabajo que se ejecutan en ellos.

6 Configuración de Acronis Cyber Infrastructure y Acronis Cyber Protect

Esta sección describe cómo implementar y configurar Acronis Cyber Protect como equipo virtual de dispositivo todo en uno en Acronis Cyber Infrastructure. Puede conectar su clúster de Acronis Cyber Appliance a Acronis Cyber Protect como back-end de almacenamiento. Como resultado, el almacenamiento y el servidor de la copia de seguridad se ejecutarán en Acronis Cyber Appliance.

6.1 Implementar el clúster de procesamiento

Antes de crear un clúster de procesamiento, asegúrese de que la red esté configurada de acuerdo con las recomendaciones que aparecen en «Configuración de redes para el clúster de procesamiento» de la Guía del administrador. Los requisitos básicos son: (a) que los tipos de tráfico **máquina virtual privada**, **máquina virtual pública**, **API de procesamiento** y **copias de seguridad de máquinas virtuales** se asignen a redes; (b) que los nodos que se van a añadir al clúster de procesamiento se conecten a estas redes y a la misma red que el tipo de tráfico **máquina virtual pública**.

Cuando haya configurado las redes, puede crear el clúster de procesamiento:

1. En la pantalla **Procesamiento**, haga clic en **Crear clúster de procesamiento**.
2. En la sección **Nodos**, seleccione los nodos que desea añadir al clúster de procesamiento y asegúrese de que el estado de red de cada nodo seleccionado es **Configurado**. Después, haga clic en **Siguiente**.

   Si las interfaces de red del nodo no están configuradas, haga clic en el icono de la rueda dentada, seleccione redes según sea necesario y luego haga clic en **Aplicar**.
3. En la sección **Red física**, deshabilite la gestión de la dirección IP si desea que un servidor DHCP externo asigne la dirección IP de la máquina virtual de Acronis Cyber Protect. Si no, puede habilitarla. Para obtener más información, consulte «Creación del clúster de procesamiento" de la Guía del administrador.
4. En el paso **Resumen**, revise la configuración y luego haga clic en **Crear clúster**.

Puede supervisar la implementación del clúster de procesamiento en la pantalla **Procesamiento**.

6.2 Implementar la máquina virtual del dispositivo todo en uno de Acronis Cyber Protect

6.2.1 Descargar la máquina virtual del dispositivo todo en uno de Acronis Cyber Protect

1. Vaya a https://account.acronis.com/ e inicie sesión en su cuenta. Si no la tiene, deberá crear una. Consulte https://kb.acronis.com/regacc.

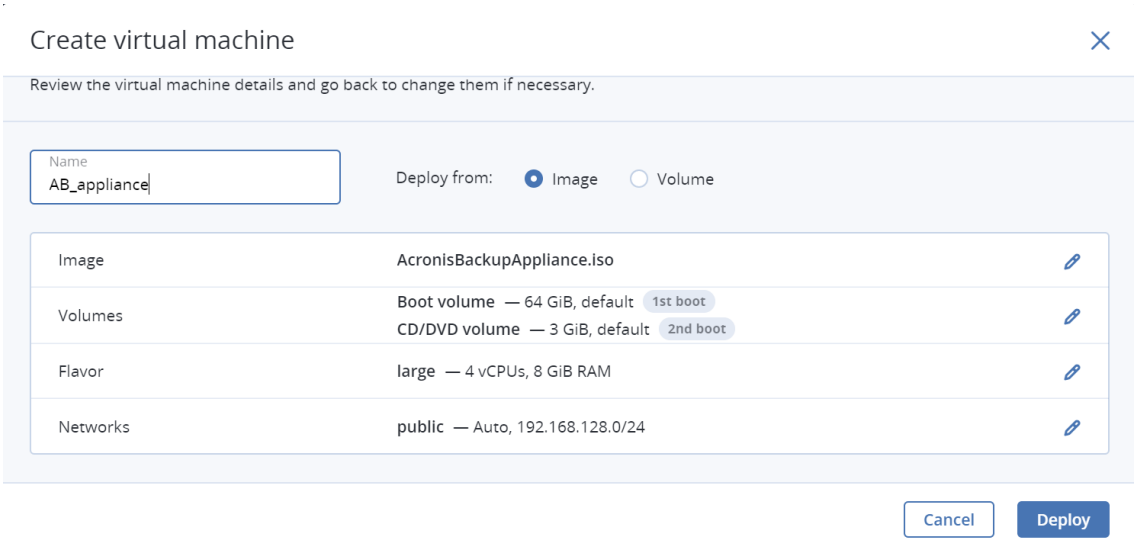
2. Registre sus productos de Acronis si todavía no lo ha hecho. Para obtener más información, consulte https://kb.acronis.com/productwebreg.
3. En la sección **Productos**, localice los enlaces de descarga de Acronis Cyber Protect. Para obtener más información, consulte https://kb.acronis.com/latest.
4. Descargue AcronisCyberProtect_All-in-One_Appliance.zip.
5. Extraiga AcronisBackupAppliance.iso.
6. Añada esta imagen al clúster de procesamiento de Acronis Cyber Infrastructure tal y como se describe a continuación:
   a. En la pestaña **Procesamiento** > **Máquinas virtuales** > **Imágenes**, haga clic en **Añadir imagen**.
   b. En la ventana **Añadir imagen**, haga clic en **Examinar** y seleccione el archivo ISO.
   c. Especifique el nombre de la imagen y seleccione el SO **Linux genérico**. Haga clic en **Agregar**.

   Para obtener más información, consulte «Carga de imágenes para máquinas virtuales» de la Guía del administrador.

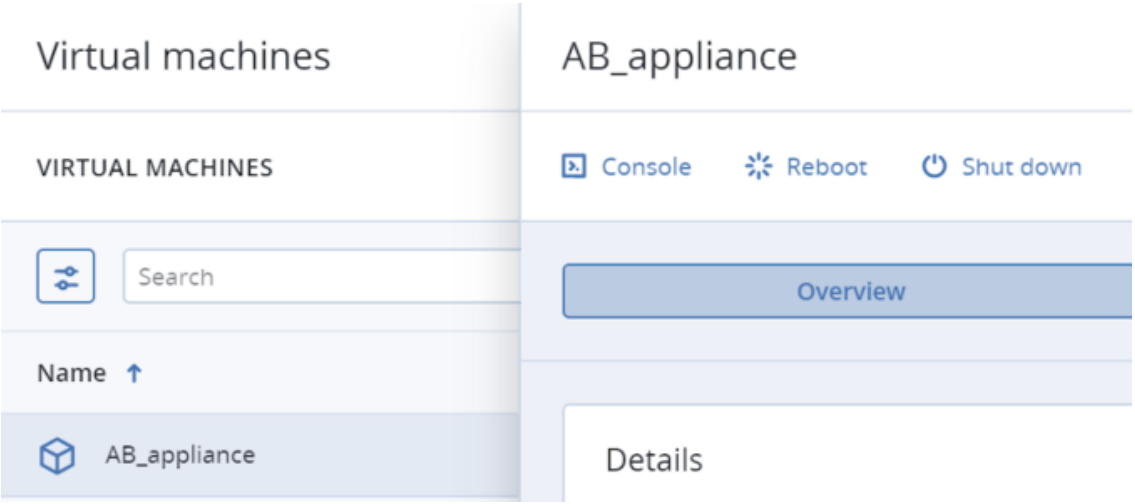
6.2.2 Implementar el dispositivo todo en uno de Acronis Cyber Protect

El dispositivo todo en uno de Acronis Cyber Protect es una máquina virtual preconfigurada que implementa en Acronis Cyber Infrastructure. Para obtener más información sobre el dispositivo, consulte el dispositivo de Acronis Cyber Protect.

a. En la pestaña **Procesamiento** > **Máquinas virtuales** > **Máquinas virtuales**, haga clic en **Crear máquina virtual**. Se abrirá una ventana en la que deberá especificar los parámetros de la máquina virtual.
b. Especifique un nombre para la nueva máquina virtual.
c. En **Implementar desde**, seleccione **Imagen**.
d. En la ventana **Imágenes**, seleccione **AcronisBackupAppliance.iso** y luego haga clic en **Listo**.
e. No es necesario añadir volúmenes en la ventana **Volúmenes**. Para instalar Acronis Cyber Protect, es suficiente con el volumen añadido automáticamente para el disco del sistema.
f. En la ventana **Variante**, seleccione la variante **grande** y luego haga clic en **Listo**. Esta variante le proporcionará 4 vCPU y 8 GB de RAM al dispositivo virtual de Acronis Cyber Protect.
g. En la ventana de red, haga clic en **Añadir**, seleccione una interfaz de red virtual pública y luego haga clic en **Añadir**. Aparecerá en la lista de **Interfaces de red**. Para obtener más información sobre las interfaces, consulte «Creación de máquinas virtuales» de la Guía del administrador.
h. De vuelta a la ventana **Crear máquina virtual**, haga clic en **Implementar** para crear y arrancar la máquina virtual.



i. En la pestaña **Procesamiento** > **Máquinas virtuales** > **Máquinas virtuales**, seleccione la máquina virtual creada. Después, haga clic en **Consola** e instale el SO de Acronis Cyber Protect mediante la consola VNC integrada.

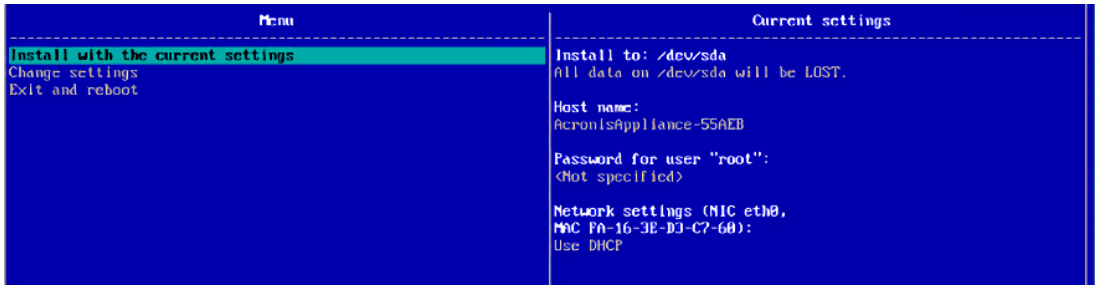


i. En la pantalla de instalación inicial, seleccione **Instalar o actualizar Acronis Cyber Protect** y pulse la tecla **Entrar**.

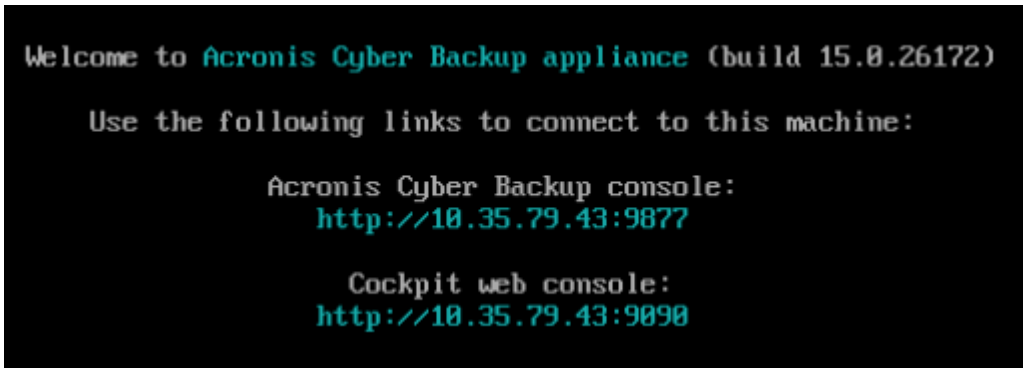
Nota
El programa de instalación inicial expira después de 15 segundos y el sistema intentará iniciarse mediante el nuevo volumen virtual. Si ve el mensaje "Iniciando desde el disco local... No se encuentra el dispositivo de arranque", reinicie la máquina virtual haciendo clic en **Enviar claves** > **Ctrl** + **Alt** + **Del**.

ii. Cambie la configuración de la instalación: especifique un nombre de servidor (opcional) y

una contraseña para el usuario raíz y, a continuación, configure los ajustes de red.



Cuando se complete la instalación, aparecerá la información de la pantalla de acceso de la consola de Acronis Cyber Protect. Utilice la consola de Acronis Cyber Protect para configurar y gestionar las operaciones de copia de seguridad.



Nota
Para instalar la licencia completa de Acronis Cyber Protect, consulte https://kb.acronis.com/content/65662.

6.3 Creación del almacenamiento de copias de seguridad

1. En el panel de administración de Acronis Cyber Infrastructure, vaya a la pantalla **Infraestructura** > **Redes**. Asegúrese de que se han añadido los tipos de tráfico **Copia de seguridad (ABGW) privada** y **Copia de seguridad (ABGW) pública** a las redes que vaya a utilizar.
2. Abra la pantalla **Servicios de almacenamiento** > **Almacenamiento de la copia de seguridad** y haga clic en **Crear almacenamiento de copias de seguridad**.
3. En el paso **Destino de copias de seguridad**, seleccione **clúster Acronis Cyber Infrastructure**.
4. En el paso **Nodos**, seleccione los nodos que desee añadir al almacenamiento de copia de seguridad y haga clic en **Siguiente**.
5. En el paso **Política de almacenamiento**, seleccione el modo de redundancia con la **codificación 3+2** y, a continuación, haga clic en **Siguiente**.
6. En el paso **DNS**, especifique el nombre del DNS que se asociará al clúster seleccionado y con el que haya registrado dicho clúster en Acronis Cyber Protect (por ejemplo, copiadeseguridad.ejemplo.es). El nuevo nombre del DNS está asociado a la dirección IP de cada

nodo del clúster seleccionado. El agente de copia de seguridad selecciona de manera automática un nodo específico para la operación de copia de seguridad. Haga clic en **Siguiente**.

7. En el paso **Cuenta de Acronis**, especifique la URL con la dirección IP o el nombre del servidor de la máquina utilizada para acceder a la consola de Acronis Cyber Protect (por ejemplo: http://192.168.128.212:9877). Si utiliza https, asegúrese de que el certificado SSL es de confianza. Facilite las credenciales del administrador del servidor de gestión local (por ejemplo, «raíz»). Haga clic en **Siguiente**.
8. En el paso **Resumen**, revise la configuración y haga clic en **Crear**.

6.4 Realizar operaciones de copias de seguridad

6.4.1 Añadir los equipos de los que se va a hacer una copia de seguridad

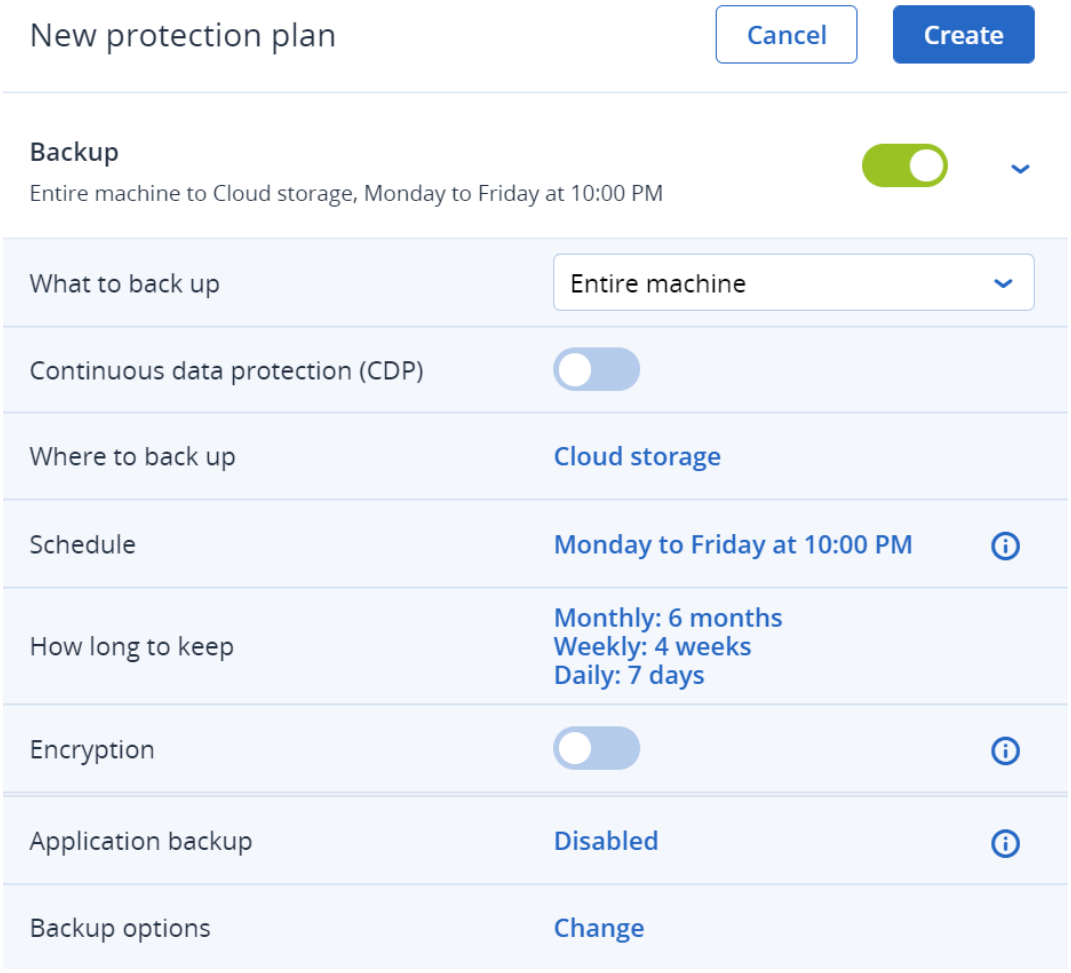
Antes de realizar la copia de seguridad de una máquina, debe instalar un agente de ciberprotección. Los agentes son aplicaciones que realizan copias de seguridad, recuperación y otras operaciones con los datos de los equipos gestionados por Acronis Cyber Protect. Elija un agente teniendo en cuenta los elementos que va a incluir en la copia de seguridad. Para obtener más información, consulte la lista completa de los sistemas operativos y entornos compatibles.

1. Abra la consola de Acronis Cyber Protect en su navegador e inicie sesión.
2. Para añadir una máquina al servidor de gestión, vaya a **Dispositivos** > **Todos los dispositivos** y, a continuación, haga clic en **Añadir**. Se le pedirá que seleccione el agente de ciberprotección según el tipo de máquina que desee añadir.
3. Una vez que el agente de ciberprotección se haya descargado, ejecútelo localmente en esa máquina.

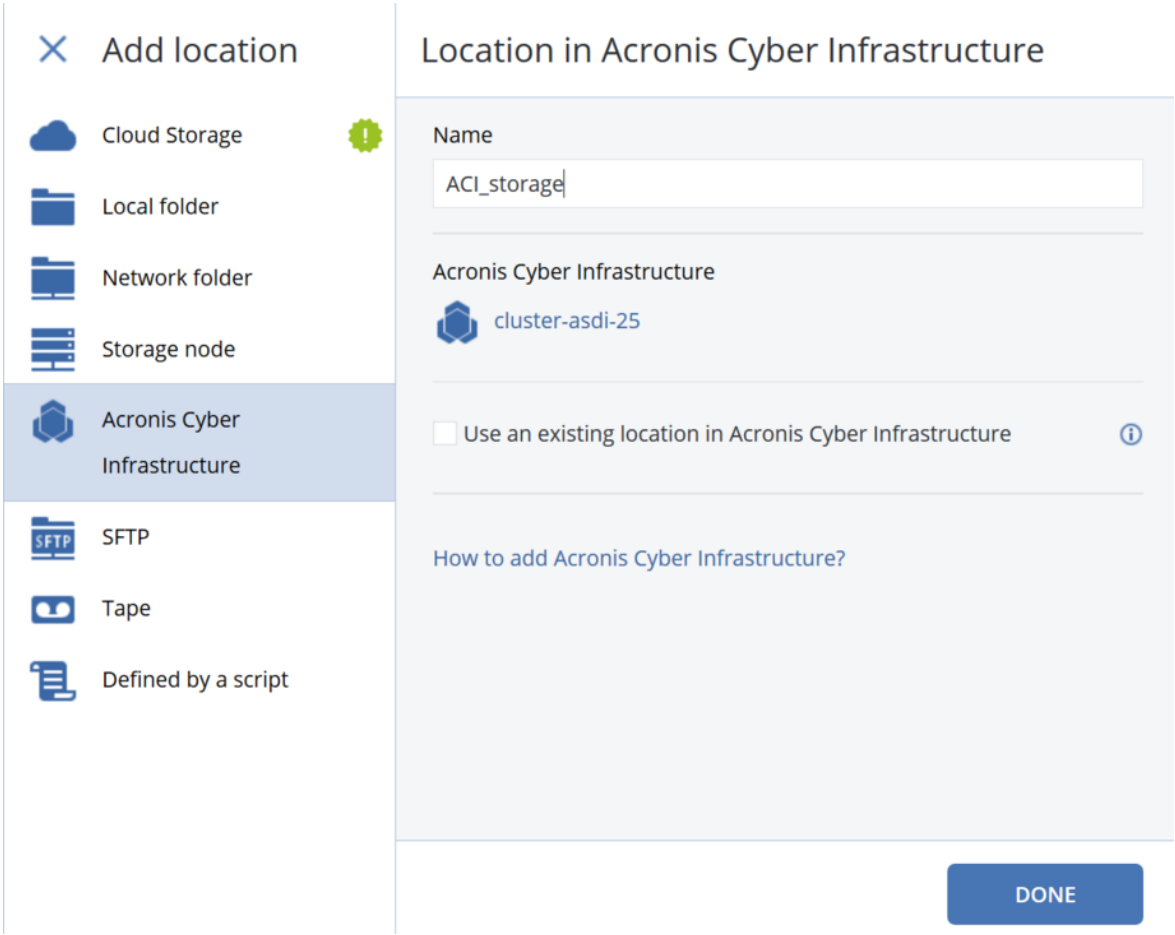
6.4.2 Configuración de un plan de protección

Un plan de protección es una serie de reglas que especifican cómo se protegerán los datos en una máquina determinada. Para crear un plan de protección, siga estos pasos:

1. Seleccione los equipos que quiera proteger.
2. Haga clic en **Proteger** y, a continuación, en **Crear plan**. Se abrirá una plantilla nueva de plan de protección.



3. Haga clic en **Dónde realizar copias de seguridad**.
4. Haga clic en **Añadir ubicación** y seleccione **Acronis Cyber Infrastructure**.



5. Haga clic en **Realizado**.
6. Haga clic en **Crear** para crear un plan nuevo. Para ejecutar un plan de protección existente, haga clic en **Ejecutar ahora**.

Para obtener información detallada acerca de cómo configurar y utilizar Acronis Cyber Protect, consulte la documentación del producto.

7 Obtener soporte técnico

Si necesita soporte técnico, contacte con Acronis de la siguiente manera:

1. Visite la página de soporte técnico https://www.acronis.com/en-us/support/contact-us/.
2. Inicie sesión en su cuenta.
3. Seleccione el producto que está usando.
4. Escoja si desea contactar con el equipo de soporte técnico por correo electrónico o por teléfono.

Recuerde que debe proporcionar acceso remoto a su Acronis Cyber Appliance a los ingenieros de soporte técnico, como se indica en el Acuerdo de nivel de servicio. Para garantizar la seguridad, se recomienda que cree una lista de direcciones IP de confianza específicas que usarán los ingenieros de soporte técnico para comunicarse con usted, y que bloquee el acceso externo desde cualquier otra dirección. Para obtener más información, consulte la Base de conocimientos en https://kb.acronis.com/sdiremote.

También puede utilizar los siguientes recursos de autoservicio:

- La base de conocimientos en https://kb.acronis.com/, un repositorio de preguntas frecuentes, instrucciones paso a paso y artículos sobre problemas conocidos. Visite las siguientes secciones de la base de conocimientos para obtener información acerca de Acronis Cyber Appliance y soluciones de software relacionadas:
  - Acronis Cyber Appliance, https://kb.acronis.com/acronis-appliance
  - Acronis Cyber Infrastructure, https://kb.acronis.com/acronis-cyber-infrastructure
  - Acronis Cyber Protect Cloud, https://kb.acronis.com/es/acronis-cyber-protect-cloud
  - Acronis Cyber Protect 12.5, https://kb.acronis.com/acronis-cyber-protect-15
- Encontrará documentación para usuarios y manuales que describen cómo usar Acronis Cyber Appliance y el software de Acronis https://www.acronis.com/support/documentation

Para obtener información acerca de la garantía de Acronis Cyber Appliance, consulte la sección de Soporte técnico en https://www.acronis.com/en-us/support/hwappliancesupport

8 Anexo: Especificaciones

Este capítulo detalla las especificaciones técnicas y medioambientales de Acronis Cyber Appliance.

8.1 Especificaciones técnicas

En la siguiente tabla se enumeran las piezas de hardware de Acronis Cyber Appliance.

Chasis	3 unidades de 435 x 130 x 600 mm (anchura x altura x profundidad) y 34,5 kg
CPU	Intel Atom C3958 a 2 GHz de 16 núcleos con TDP de 31 W, compatible con VT-d, sin Hyper-Threading
RAM	2 DDR4-2400 ECC de Samsung de 16 GB, con 32 GB (hasta 256 GB)
Unidad de sistema operativo	1 SSD Intel S4600 de 2,5" y 240 GB
Unidades de caché	1 SSD Intel S4600 de 2,5" y 240 GB
Unidades de almacenamiento	3 discos duros Enterprise SATA de 4, 8, 10 o 12 TB por nodo, 15 en total
Red	2 RJ45 de entre 1 y 10 GbE y 2 SPF+ de 10 GbE
Fuente de alimentación	1+1 de 750 W, la corriente compartida y redundancia en frío dependerán de las cargas de energía (consulte también la siguiente tabla)
Puertos de E/S	Parte posterior: 2 USB 2.0, 1 VGA, 2 RJ45 de entre 1 y 10 GbE, 2 SPF+ de 10 GbE y 1 RJ45 de administración
Software	Acronis Cyber Infrastructure
Protección de datos	Codificación de borrado y replicación mediante políticas de almacenamiento
Redundancia	Unidades de disco de datos intercambiables en caliente 2 fuentes de alimentación intercambiables en caliente Sin único punto de error Actualizaciones de software en línea sin interrupciones
Supervisión, administración	CLI, GUI, API, IPMI

8.1.1 Especificaciones del suministro de alimentación

En la siguiente tabla se enumeran las especificaciones del suministro de alimentación del dispositivo.

Voltaje, frecuencia	De 100 a 240 V, de 50 a 60 Hz

Consumo energético en W	750			
Disipación del calor máxima (BTU/h)	2300			
Irrupción máxima en A	40			
Corriente de entrada	Entrada de CA		Corriente máxima	
	100–127 VCA, 8,8 A		200–240 VCA, 4,3 A	
Eficiencia del suministro de alimentación (Clase Platinum)	10 % de carga	20 % de carga	50 % de carga	100 % de carga
	80 %	90 %	94 %	91 %
Corrección del factor de potencia de entrada[1]	Potencia de salida	20 % de carga	50 % de carga	100 % de carga
	Factor de potencia	>0,80	>0,95	>0,95

[1]Probada a 230 VCA y 50 Hz y a 115 VCA y 60 Hz. El factor de potencia de entrada es mayor que los valores en la tabla a la capacidad nominal del suministro de alimentación, y cumple los requisitos de Energy Star®.

8.2 Especificaciones medioambientales

En las siguientes tablas se detallan las especificaciones medioambientales de Acronis Cyber Appliance.

Temperatura de almacenamiento	-40 °C a 85 °C (-40 °F a 185 °F)
Gradiente de temperatura de almacenamiento	20 °C (68 °F) por hora
Temperatura de funcionamiento	10 °C a 35 °C (50 °F a -95 °F)
Gradiente de temperatura de funcionamiento	20 °C (68 °F) por hora
Intervalo de porcentaje de humedad relativa de almacenamiento	Entre 10 % y 95 % (sin condensación)
Intervalo de porcentaje de humedad relativa de funcionamiento	Entre 10 % y 85 % (sin condensación)
Vibración de almacenamiento	1,87 Grms (De 10 a 500 Hz)
Vibración de funcionamiento	0,26 Grms (De 5 a 350 Hz)
Impacto de almacenamiento	65 G por 2 ms
Impacto de funcionamiento	5 G
Altura de almacenamiento	12.000 m (39.370 ft)
Altura de funcionamiento	3048 m (10.000 ft)

8.2.1 Requisitos de calidad del aire

El aire debe estar libre de:

- Polvo y agentes contaminantes corrosivos
- Polvo y partículas conductivos (como limaduras de zinc)

El polvo residual aéreo debe tener un punto de delicuescencia menor que una humedad relativa del 60 %. El punto de delicuescencia es la humedad relativa a la que los materiales cristalinos comienzan a absorber grandes cantidades de agua de la atmósfera.

Nivel de corrosión gaseosa en ángstroms de acuerdo con el estándar ISA:

- La reactividad del cobre debe ser menor de 300 A/mes, clase G1 (ANSI/ISA 71.04-1985).
- La reactividad de la plata debe ser menor de 200 A/mes (AHSRAE TC9.9).