

# Acronis

## Acronis Cyber Infrastructure 3.5

Guía de inicio rápido de Backup  
Gateway de para VMware vSphere

31 de julio de 2020

## Declaración de copyright

Copyright ©Acronis International GmbH, 2003-2020. Todos los derechos reservados.

"Acronis", "Acronis Compute with Confidence", "Acronis Recovery Manager", "Acronis Secure Zone", "Acronis True Image", "Acronis Try&Decide" y el logo de Acronis son marcas comerciales de Acronis International GmbH.

Linux es una marca registrada de Linus Torvalds.

VMware y VMware Ready son marcas comerciales o marcas registradas de VMware, Inc. en Estados Unidos o en otras jurisdicciones.

Windows y MS-DOS son marcas registradas de Microsoft Corporation.

Todas las otras marcas comerciales y derechos de autor mencionados son propiedad de sus respectivos propietarios.

La distribución de las versiones sustancialmente modificadas del presente documento está prohibida sin el permiso explícito del titular del derecho de autor.

La distribución de este trabajo o trabajo derivado en cualquier forma de libroestándar (papel) para fines comerciales está prohibida excepto que se obtenga permiso previo del titular del derecho de autor.

LA DOCUMENTACIÓN SE PROPORCIONA «TAL COMO SE ENCUENTRA» Y SE EXCLUYEN TODAS LAS CONDICIONES EXPLÍCITAS O IMPLÍCITAS, DECLARACIONES Y GARANTÍAS, INCLUIDA CUALQUIER GARANTÍA IMPLÍCITA DE COMERCIABILIDAD, IDONEIDAD CON UN PROPÓSITO ESPECÍFICO O NO VIOLACIÓN DE DERECHOS DE TERCEROS, SALVO EN LA MEDIDA EN QUE DICHAS EXCLUSIONES TENGAN VALIDEZ LEGAL.

Es posible que se suministre código de terceros junto con el software o servicio. Los términos de la licencia de terceros se detallan en el archivo license.txt ubicado en el directorio raíz de instalación. La última lista actualizada del código de terceros y los términos de la licencia asociada que se utiliza con el software y/o servicio está siempre disponible en <http://kb.acronis.com/content/7696>.

## Tecnologías patentadas de Acronis

Las tecnologías utilizadas en este producto están cubiertas y protegidas por uno o más de los siguientes números de patentes estadounidenses:

7.047.380; 7.275.139; 7.281.104; 7.318.135; 7.353.355; 7.366.859; 7.475.282; 7.603.533; 7.636.824; 7.650.473; 7.721.138; 7.779.221; 7.831.789; 7.886.120; 7.895.403; 7.934.064; 7.937.612; 7.949.635; 7.953.948; 7.979.690; 8.005.797; 8.051.044; 8.069.320; 8.073.815; 8.074.035; 8.145.607; 8.180.984; 8.225.133; 8.261.035; 8.296.264; 8.312.259; 8.347.137; 8.484.427; 8.645.748; 8.732.121 y aplicaciones pendientes de patente.

# Índice general

<b>1. Acerca de esta guía</b> . . . . .	<b>1</b>
1.1 Requisitos . . . . .	1
<b>2. Configuración de redes</b> . . . . .	<b>3</b>
<b>3. Creación de equipos virtuales</b> . . . . .	<b>6</b>
<b>4. Implementación de Acronis Cyber Infrastructure en equipos virtuales</b> . . . . .	<b>12</b>
4.1 Implementación del nodo de gestión . . . . .	13
4.2 Implementación de nodos secundarios . . . . .	15
<b>5. Añadir espacio a Acronis Cyber Infrastructure</b> . . . . .	<b>17</b>
<b>6. Conexión del software Acronis Backup a los back-end de almacenamiento mediante Backup Gateway</b> . . . . .	<b>19</b>
6.1 Conexión al clúster de almacenamiento local mediante Backup Gateway . . . . .	20
6.2 Conexión a recursos compartidos de NFS externos mediante Backup Gateway . . . . .	23
6.3 Conexión al sistema de almacenamiento público en el cloud a través de Backup Gateway . . . . .	26
6.3.1 Requisitos y restricciones importantes . . . . .	27
6.3.2 Configuración de Backup Gateway . . . . .	28

## CAPÍTULO 1

# Acerca de esta guía

Esta guía explica cómo implementar Acronis Cyber Infrastructure y configurar Backup Gateway en VMware vSphere 6.5 y versiones posteriores.

En resumen, deberá hacer lo siguiente:

1. Configure las redes.
2. Crear equipos virtuales para Acronis Cyber Infrastructure.
3. Implemente Acronis Cyber Infrastructure en los equipos virtuales.

Todos estos pasos se describen de forma detallada en los siguientes capítulos.

Después de implementar Acronis Cyber Infrastructure, deberá configurarlo para su situación particular. En *Conexión del software Acronis Backup a los back-end de almacenamiento mediante Backup Gateway* (página 19) se indican los pasos para configurar Backup Gateway. Hay disponibles otras instrucciones en el Manual del administrador <admins\_guide:index>.

## 1.1 Requisitos

- En el caso de Backup Gateway, Acronis Cyber Infrastructure puede implementarse en un único equipo virtual. Sin embargo, para una implementación de uso general, se recomienda crear tres o cinco equipos virtuales para habilitar el equilibrado de carga y la alta disponibilidad.
- Asegúrese de que el almacén de datos vSphere tiene suficiente espacio de almacenamiento libre. Cada equipo virtual ocupa al menos 425 GB (dos discos de almacenamiento de 200 GB y un disco del sistema de 25 GB). La plantilla de Acronis Cyber Infrastructure también ocupa unos 35 GB.

- Asegúrese de que el servidor tiene memoria suficiente. 4 GB de RAM es el mínimo requerido para la configuración de un nodo. Por lo demás, se requieren al menos 8 GB de RAM para el nodo de gestión, mientras que cada nodo secundario ocupa al menos 4 GB de RAM.
- Utilice un contenedor de objetos para cada clúster de Backup Gateway.

---

**Nota:** Todos los requisitos de hardware para esta situación de Backup Gateway se describen en Hardware Requirements.

---

## CAPÍTULO 2

# Configuración de redes

Acronis Cyber Infrastructure requiere normalmente dos redes: una pública para la conectividad exterior y otra privada para el intercambio de datos entre equipos virtuales. Aunque la red pública puede estar ya configurada, se recomienda crear una red privada dedicada aunque ya exista una. Para crear una red privada, necesita un conmutador virtual con parámetros de seguridad personalizados y un grupo de puertos.

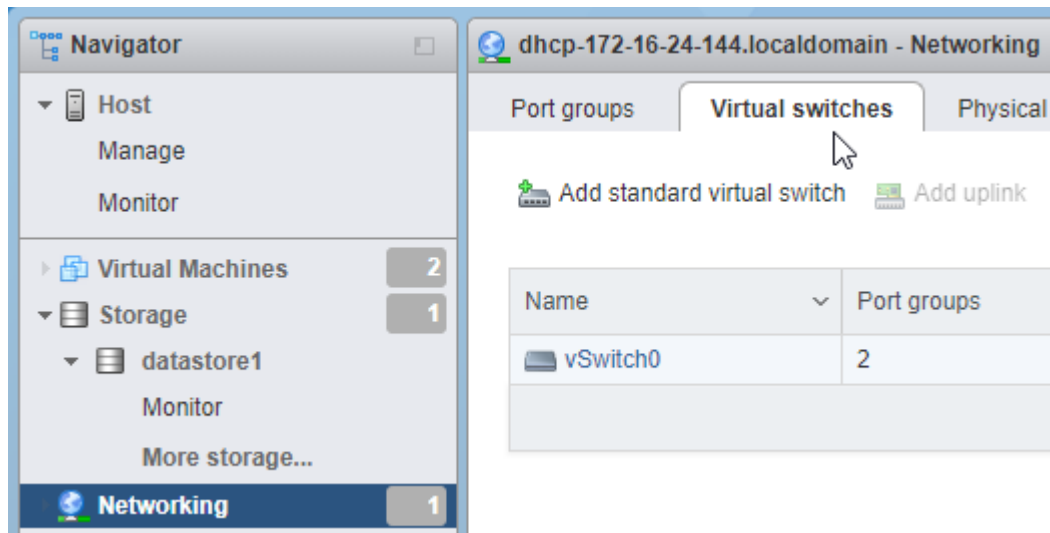
---

**Nota:** Todos los requisitos de red se describen en Planning Network.

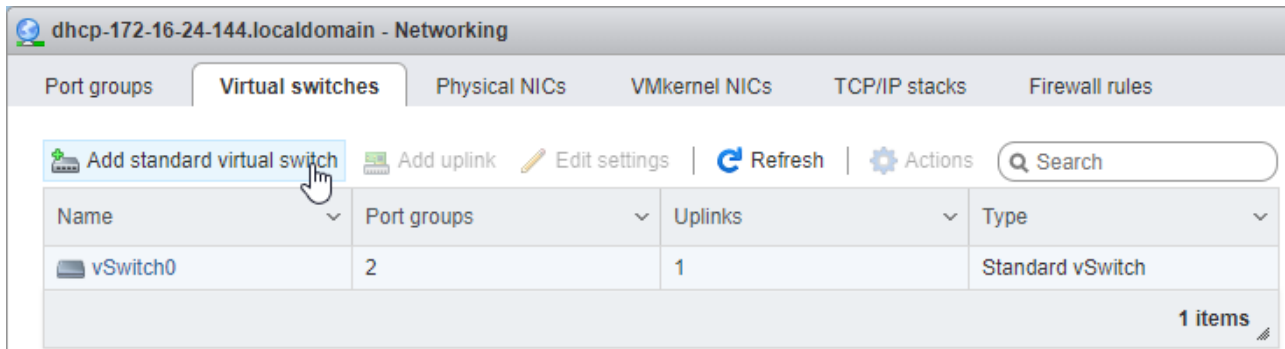
---

Para crear un conmutador virtual, siga estos pasos:

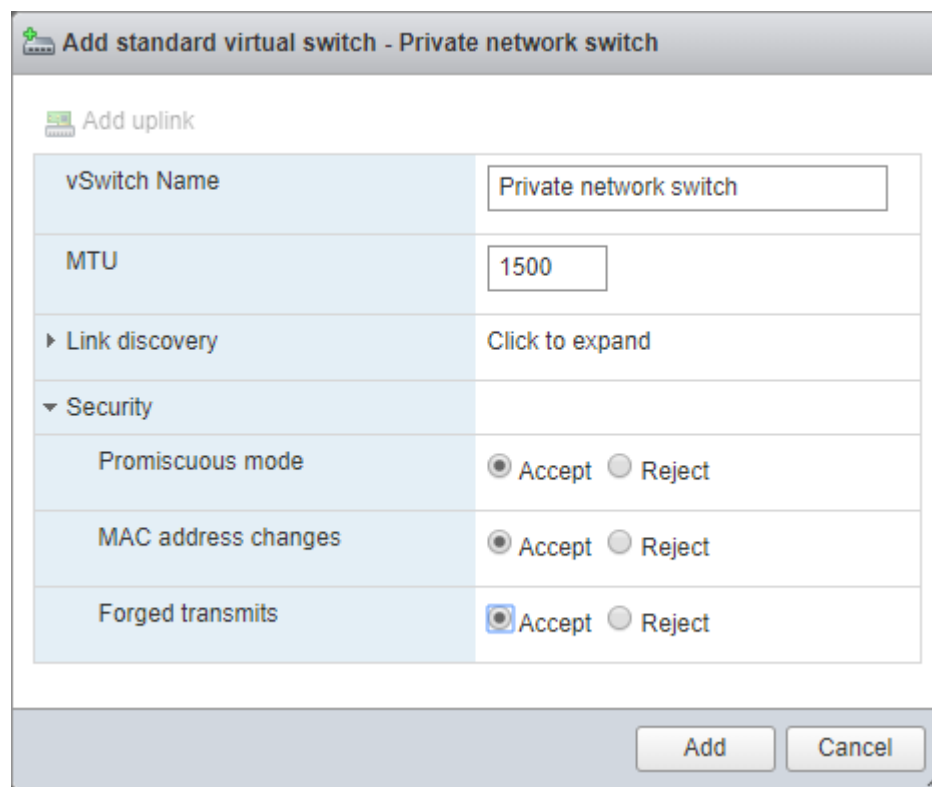
1. En Host Client, haga clic en **Conexión de Redes** en el menú izquierdo. Abra la pestaña **Conmutadores virtuales**.



2. Haga clic en **Añadir conmutador virtual estándar** en la barra de herramientas.

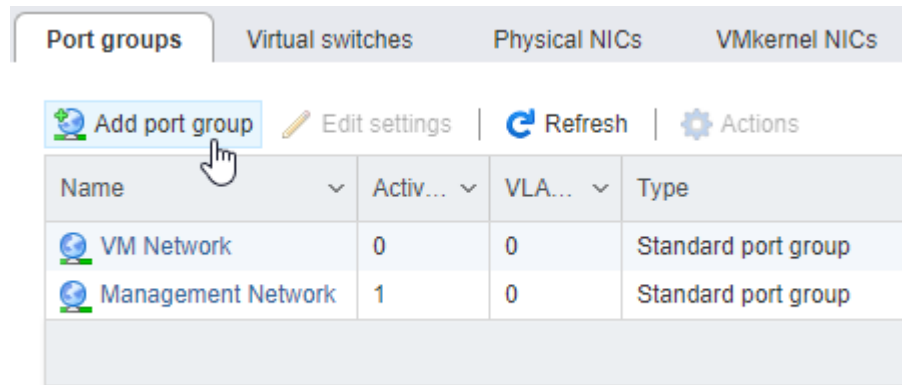


3. Introduzca el nombre del conmutador y expanda **Seguridad**. Seleccione **Aceptar** para el **modo Promiscuous, Cambios en la dirección MAC y Transmisiones falsificadas**.

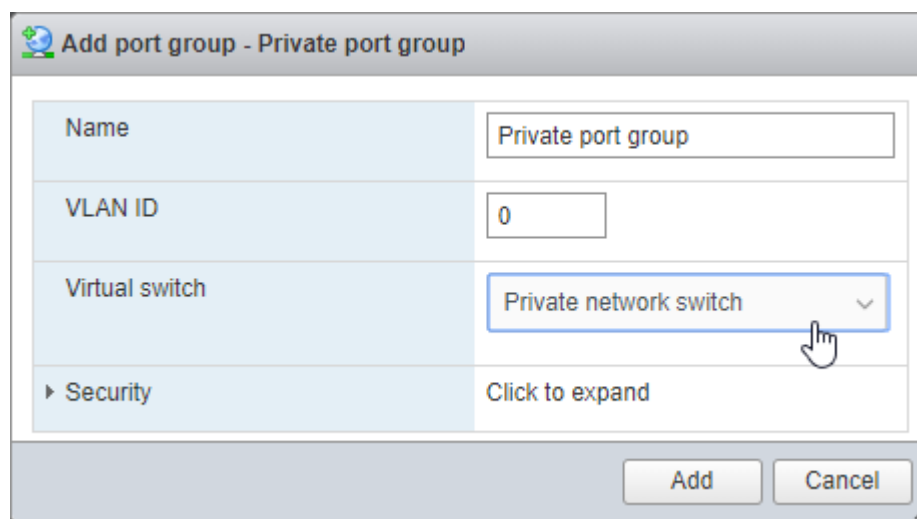


Para crear un grupo de puertos, siga estos pasos:

1. Abra la pestaña **Grupo de puertos** y haga clic en **Añadir grupo de puertos** en la barra de herramientas.



2. Introduzca el nombre del grupo de puertos. Seleccione el conmutador virtual creado anteriormente.





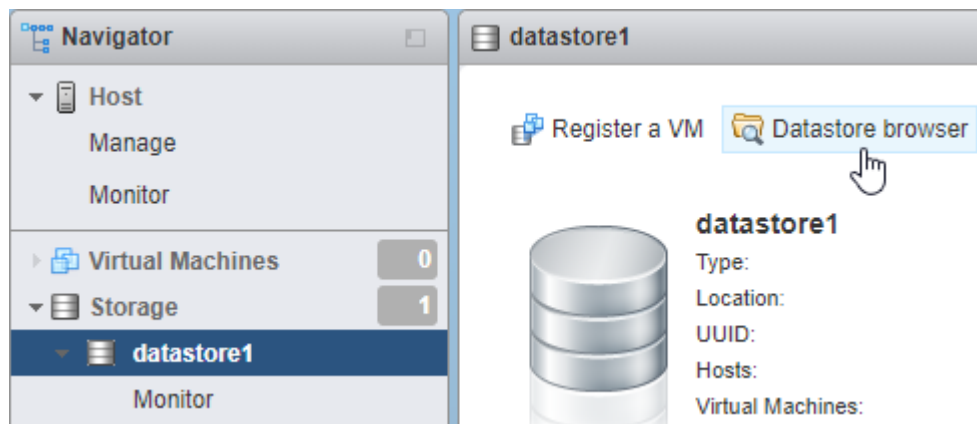
## CAPÍTULO 3

# Creación de equipos virtuales

Primero, obtenga la imagen Acronis Cyber Infrastructure (2 archivos VMDK). Para hacerlo, visite la página del producto y envíe una solicitud.

A continuación, cargue los dos archivos VMDK en el almacén de datos de VMware vSphere:

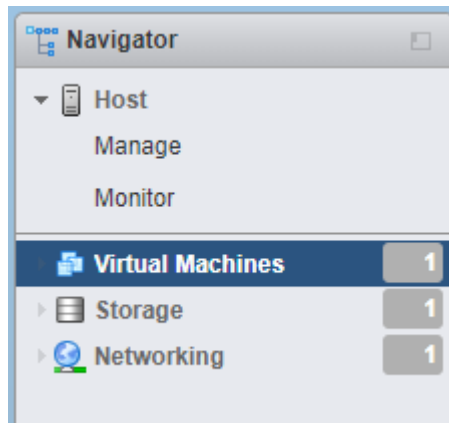
1. En el panel **Navegador**, haga clic en el almacén de datos requerido. Haga clic en **Navegador del almacén de datos** en su barra de herramientas.
2. En la ventana **Navegador del almacén de datos**, cree un directorio con el nombre de su equipo virtual.



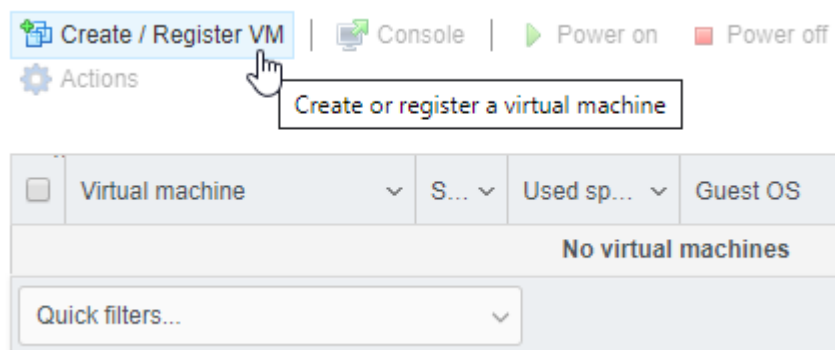
3. Cargue en este directorio la imagen Acronis Cyber Infrastructure (dos archivos VMDK).

Siga estos pasos si desea crear un equipo virtual para Acronis Cyber Infrastructure:

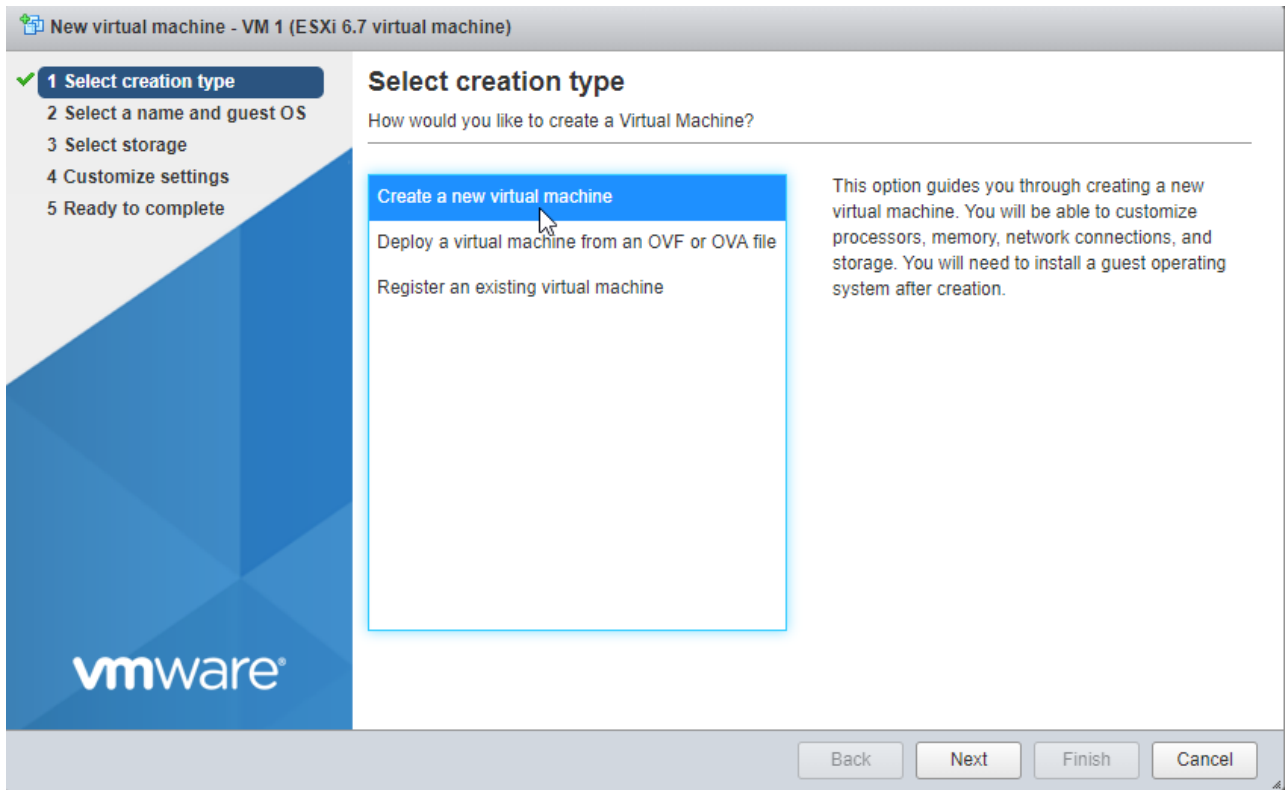
1. En Host Client, haga clic en **Equipos virtuales** en el menú izquierdo.



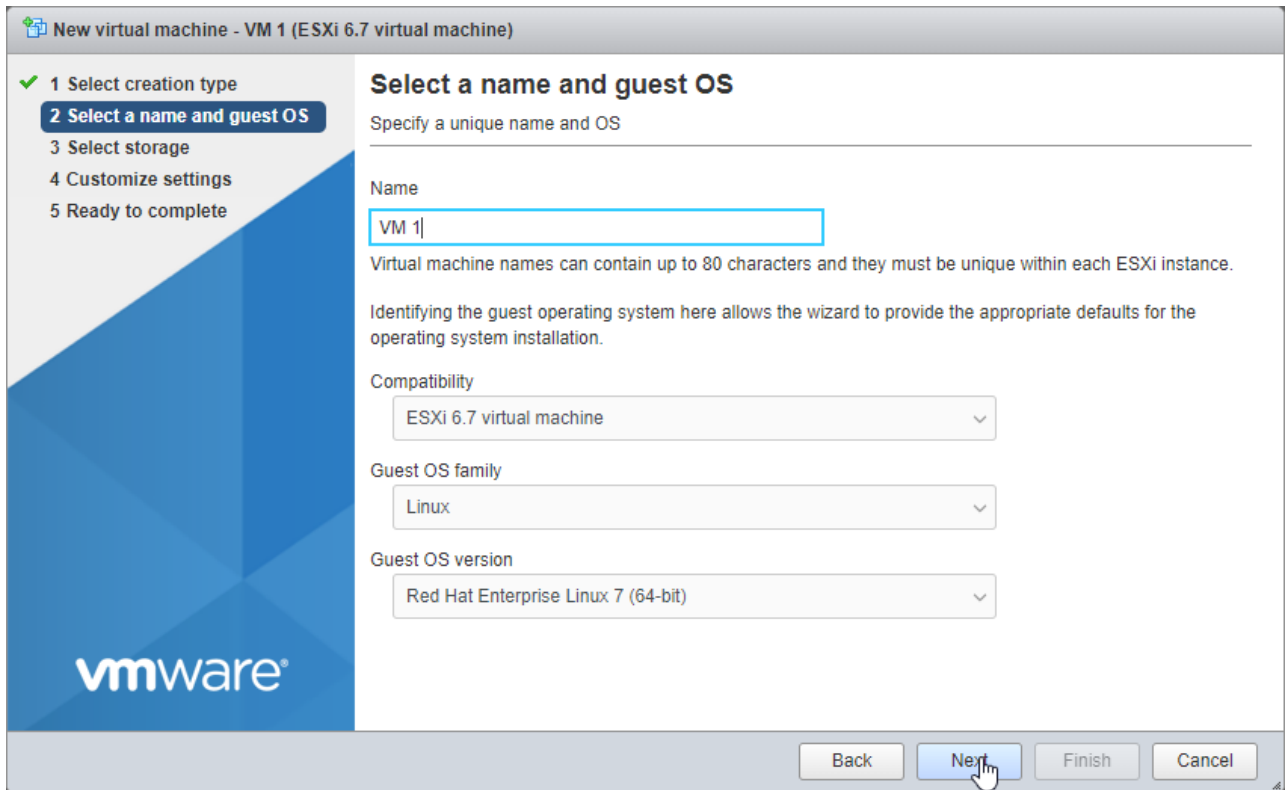
2. Haga clic en **Crear/Registrar equipo virtual** en la barra de herramientas.



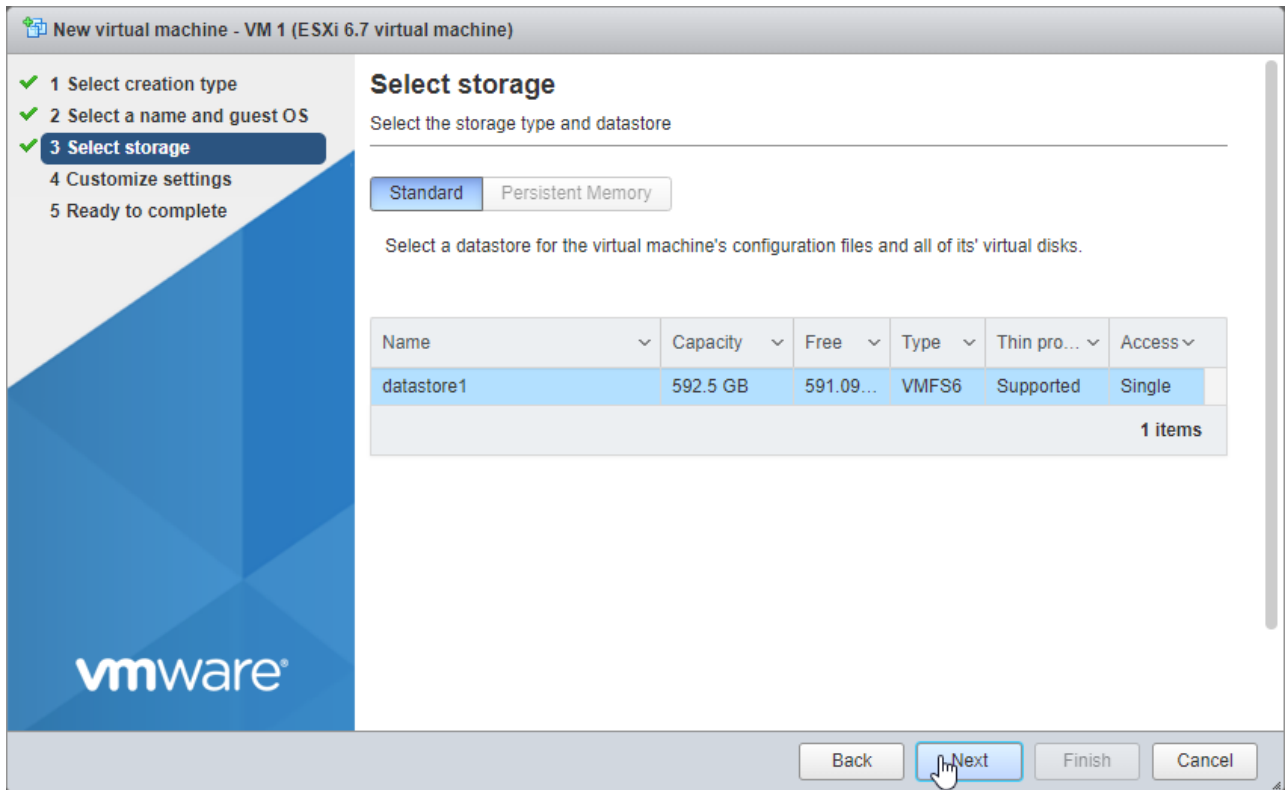
3. En el paso 1 del asistente **Máquina virtual nueva**, seleccione **Crear una nueva máquina virtual**. Haga clic en **Siguiente**.



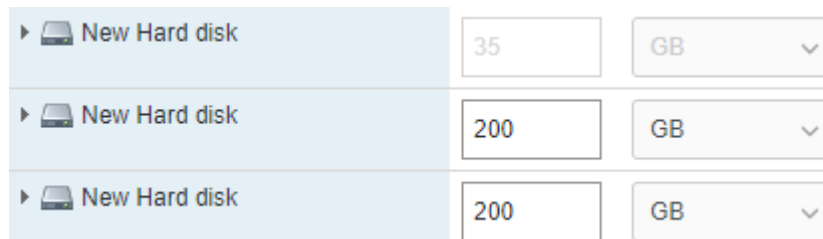
4. En el paso 2, introduzca un nombre para el equipo virtual y seleccione el SO invitado. Haga clic en **Siguiente**.



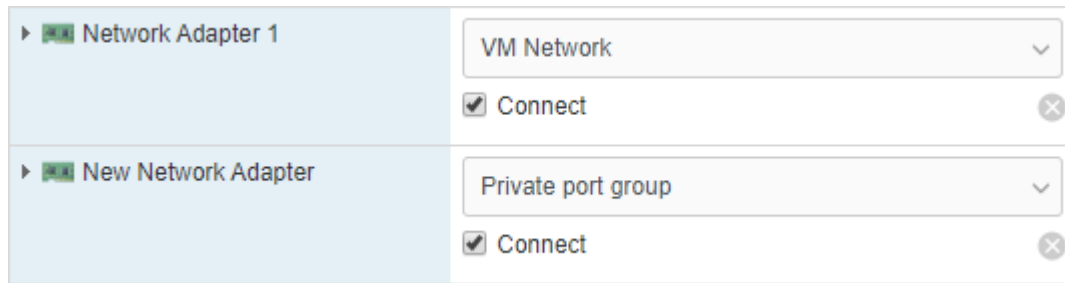
5. En el paso 3, seleccione el tipo de almacenamiento y el almacén de datos. Asegúrese de que el almacén de datos tiene espacio libre suficiente.



6. En el paso 4, extraiga el disco rígido existente y haga clic en **Agregar disco rígido** en la barra de herramientas. Seleccione **Disco rígido existente** y vaya a la imagen que cargó anteriormente en el almacén de datos. Haga clic en **Seleccionar**.
7. Haga clic de nuevo en **Agregar disco rígido** en la barra de herramientas. Seleccione **Nuevo disco rígido estándar**. Establezca su tamaño en 200 GB. Repita este paso para añadir un disco rígido de más de 200 GB. En total, debe tener tres discos rígidos: 35 GB, 200 GB y 200 GB.



8. En la ventana **Personalizar la configuración**, haga clic en **Agregar adaptador de red** en la barra de herramientas. Asegúrese de que un adaptador está conectado a la red pública y el otro al grupo de puertos privado que ha creado.



9. En el paso 5, compruebe la configuración y haga clic en **Terminar**.

10. Seleccione el equipo virtual en el menú **Navegador** e inícielo.

Repita estos pasos para crear tantos equipos virtuales como necesite, en función de su caso concreto (consulte [Requisitos](#) (página 1)).

## CAPÍTULO 4

# Implementación de Acronis Cyber Infrastructure en equipos virtuales

Cuando se inicie el equipo virtual, haga lo siguiente:

1. Inicie sesión como usuario de almacenamiento con la contraseña predeterminada (que es contraseña). Se le pedirá que cambie la contraseña en ese mismo momento. Por ejemplo:

```
You are required to change your password immediately (root enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user storage-user.
Changing password for storage-user.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

En Contraseña UNIX (actual) escriba la contraseña; en Nueva contraseña y Vuelva a escribir la nueva contraseña escriba una nueva contraseña. La contraseña cambiará tanto para el usuario de almacenamiento como para el usuario raíz.

2. Inicie sesión de nuevo como usuario de almacenamiento con la nueva contraseña y cambie al usuario raíz:

```
$ sudo su
```

3. Configure y habilite la interfaz de red eth1:

```
# cat > /etc/sysconfig/network-scripts/ifcfg-eth1 << EOF
ARPCHECK="no"
BOOTPROTO="static"
IPADDR=192.168.1.<nodo>
NETMASK=255.255.255.0
DEVICE="eth1"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
NAME="eth1"
ONBOOT="yes"
EOF
# ifup eth1
```

Donde <nodo> es el número de nodo: 2 para el nodo de gestión, 3 para el primer nodo secundario y así sucesivamente.

4. Compruebe que la dirección IP se ha asignado y la interfaz está activada, p. ej., con `ip -4 a show eth1`.

Cualquier otra configuración varía según el rol del nodo. Tendrá que implementar un solo nodo de gestión y es posible que también desee implementar dos o cuatro nodos secundarios.

## 4.1 Implementación del nodo de gestión

1. Para registrar el nodo de gestión e inicializar su panel de administración, ejecute como usuario raíz:

```
# echo '<passwd>' | /usr/libexec/vstorage-ui-backend/bin/configure-backend.sh \
-i <int_net> -x <ext_net>
# systemctl start vstorage-ui-backend
# systemctl start vstorage-ui-agent
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_IP>
```

Donde <passwd> es la contraseña de administrador deseada; <int\_net> es la interfaz de red interna (privada); <ext\_net> es la interfaz de red externa (pública); y <mn\_IP> es la dirección IP del nodo de gestión.

2. Reinicie el equipo virtual. La dirección IP del panel de administración se mostrará en el mensaje de bienvenida del terminal. Ahora puede iniciar sesión en el panel de administración en el puerto 8888. Utilice el nombre de usuario `admin` y la contraseña raíz del nodo de gestión que proporcionó en el paso anterior.

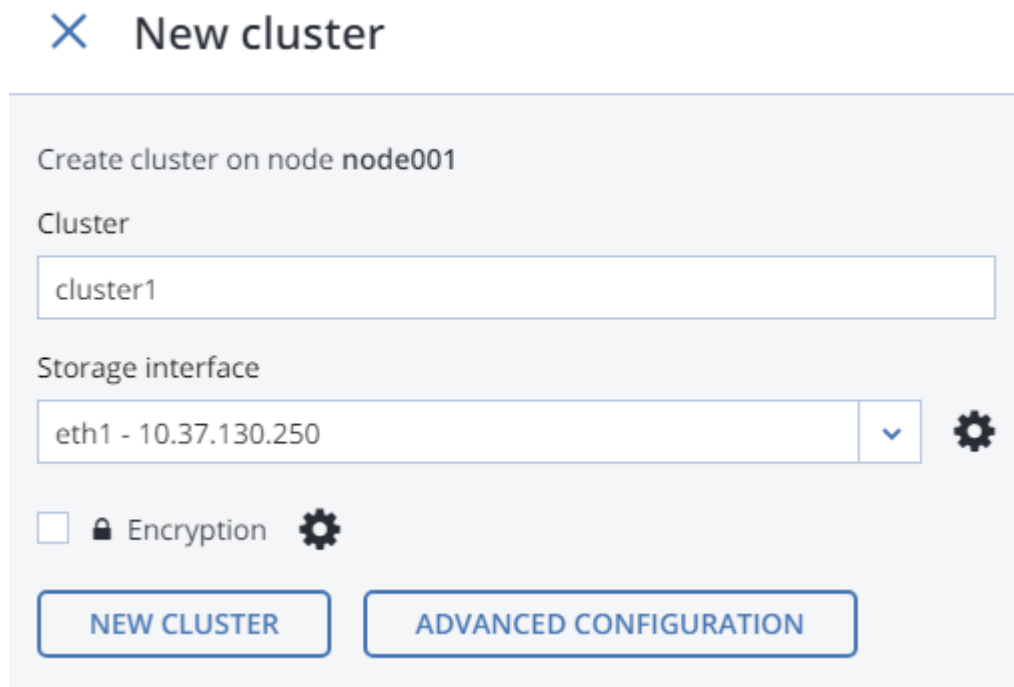
En el panel de administración verá el nodo que ha implementado en la lista **SIN ASIGNAR** de la pantalla **INFRAESTRUCTURA > Nodos**.



3. En la pantalla **INFRAESTRUCTURA > Redes**, haga clic en **Editar**. Haga disponible para la red pública el tipo de tráfico **API de procesamiento** y haga clic en **Guardar**.

Ahora, debe crear el clúster de almacenamiento. Realice lo siguiente:

1. Abra la pantalla **INFRAESTRUCTURA > Nodos** y haga clic en un nodo de la lista **SIN ASIGNAR**.
2. En la pantalla de información general del nodo, haga clic en **Crear clúster**.
3. En el campo **Clúster**, introduzca un nombre para el clúster. El nombre solo puede contener letras latinas (a-z, A-Z), números (0-9), guiones bajos ("\_") y guiones ("-").



**×** New cluster

Create cluster on node **node001**

Cluster

cluster1

Storage interface

eth1 - 10.37.130.250

Encryption

**NEW CLUSTER** **ADVANCED CONFIGURATION**

4. Haga clic en **NUEVO CLÚSTER**.

El clúster de almacenamiento está preparado. Ahora puede implementar nodos secundarios si su situación lo requiere. Si necesita un único nodo para Backup Gateway, vaya a *Conexión del software Acronis Backup a los back-end de almacenamiento mediante Backup Gateway* (página 19).

## 4.2 Implementación de nodos secundarios

Para implementar un nodo secundario en un equipo virtual, haga lo siguiente:

1. Obtenga la dirección IP del nodo de gestión y el token del panel de administración. Abra **INFRAESTRUCTURA > Nodos**. Haga clic en **AGREGAR NODO** para acceder a una pantalla con la dirección IP del nodo de gestión y el token.
2. Abra el terminal del equipo virtual y registre el nodo secundario en el panel de administración del modo siguiente:

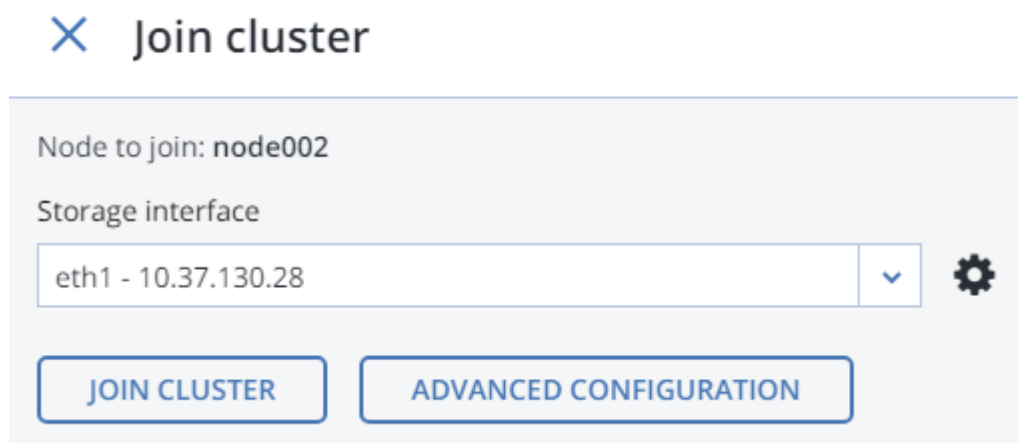
```
# /usr/libexec/vstorage-ui-agent/bin/register-storage-node.sh -m <mn_addr> -t <token>
```

Donde <mn\_addr> es la dirección IP del nodo de gestión; y <token> es el token obtenido en el panel de administración.

En el panel de administración, el nodo secundario recién registrado aparecerá en la lista **SIN ASIGNAR** de la pantalla **INFRAESTRUCTURA > Nodos**.

3. Añada el nodo secundario al clúster de almacenamiento:
  - 3.1. En la pantalla **INFRAESTRUCTURA > Nodos**, haga clic en un nodo sin asignar.
  - 3.2. En la pantalla de información general del nodo, haga clic en **Unir clúster**.
  - 3.3. Asegúrese de que está seleccionada la interfaz de red conectada a una red con el tipo de tráfico **Almacenamiento** en la lista desplegable **Interfaz de almacenamiento**.

Si no están configuradas las interfaces de red del nodo, haga clic en el icono de rueda dentada y asigne una red con el tipo de tráfico **Almacenamiento** a la interfaz de red de un nodo.



- 3.4. Haga clic en **Unir clúster** para que Acronis Cyber Infrastructure asigne los roles a los discos de forma automática y añada el nodo al clúster actual. O bien, haga clic en **Configuración avanzada** para asignar los roles a cada unidad manualmente.

Repita estos pasos en cada nodo secundario. Cuando todos estén en el clúster de almacenamiento, puede habilitar la alta disponibilidad para el nodo de gestión en la pantalla **CONFIGURACIÓN > Nodo de gestión > ALTA DISPONIBILIDAD DE GESTIÓN**.

Ahora puede configurar Acronis Cyber Infrastructure para el escenario deseado. En el Manual del administrador <admins\_guide:index> se proporcionan instrucciones para realizar diversas tareas de configuración.

## CAPÍTULO 5

# Añadir espacio a Acronis Cyber Infrastructure

Antes de crear discos nuevos, tenga en cuenta las siguientes recomendaciones en cuanto a su tamaño:

1. Si tiene un clúster para varios nodos, estos deben tener el mismo tamaño por motivos de redundancia. Así, los datos se repartirán de una forma más uniforme entre ellos. Para obtener más información, consulte [Understanding Allocatable Disk Space](#).
2. Que los discos tengan el mismo tamaño ayuda a distribuir las cargas de manera más uniforme. Dentro de un clúster, el uso del disco es proporcional al tamaño del disco. Por ejemplo, si tiene un disco de 10 TB y un disco de 2 TB, el 50 % de la carga del clúster utilizará 5 TB y 1 TB respectivamente.

Si desea aumentar el espacio físico de su clúster de almacenamiento, puede agregar nuevos discos virtuales a sus nodos. No utilice la opción **extender disco** de VMware vSphere en su equipo virtual de Acronis Cyber Infrastructure, ya que el sistema de archivos no cambiará de tamaño de manera proporcional. Cree una nueva unidad de disco virtual y agréguela a su equipo virtual como se escribe a continuación.

Añada una unidad de disco virtual a su equipo virtual según se describe en [Añadir un disco duro a un equipo virtual](#). A continuación, se mostrará en los discos del nodo del panel de administración de Acronis Cyber Infrastructure.

En el panel de administración, siga estos pasos para configurar la nueva unidad de disco:

1. En la pantalla **INFRAESTRUCTURA > Nodos**, haga clic en el nodo en el que se encuentra la unidad de disco que ha creado. Haga clic en la sección **DISCOS>** para ver todos los discos del nodo.
2. El disco con el rol **Sin asignar** es el que acaba de crear. Selecciónelo y haga clic en **Asignar** en el menú de la derecha.

3. En la pantalla **Seleccionar rol**, seleccione el rol **Almacenamiento** y el nivel, y habilite la suma de comprobación si es necesario. Para obtener más información, consulte [Assigning Disk Roles Manually](#).

### ✕ Choose role

Storage

Metadata

Cache

Metadata+Cache

Unassigned

Caching and checksumming

Enable checksumming

Tier

Tier 0

## CAPÍTULO 6

# Conexión del software Acronis Backup a los back-end de almacenamiento mediante Backup Gateway

El punto de acceso de almacenamiento de Backup Gateway (también denominado “puerta de enlace”) está diseñado para proveedores de servicio que usan Acronis Backup Cloud o Acronis Backup Advanced y desean organizar un almacenamiento local para los datos con copia de seguridad de sus clientes.

Backup Gateway permite a un proveedor de servicios configurar fácilmente el almacenamiento para el formato de datos para deduplicación que usa Acronis.

Backup Gateway es compatible con los siguientes back-end de almacenamiento:

- clústeres de almacenamiento con redundancia de software mediante codificación de borrado
- Recursos compartidos de NFS
- nubes públicas, incluidas varias soluciones S3 así como Microsoft Azure, OpenStack Swift y Google Cloud Platform

Aunque su elección debería basarse en el entorno y los requisitos, se recomienda que mantenga los datos de copia de seguridad de Acronis en el clúster de almacenamiento local. En este caso, puede tener el mejor rendimiento gracias a las optimizaciones de WAN y a la localidad de los datos. El hecho de mantener las copias de seguridad en un recurso compartido de NFS o un cloud público implica la inevitable transferencia de datos y otras sobrecargas, lo que reduce el rendimiento general.

Tenga en cuenta lo siguiente:

- Al configurar Backup Gateway, necesitará proporcionar las credenciales de su cuenta de administrador en el software de copia de seguridad de Acronis.
- En los casos en los que no se use un almacenamiento local sino externo (por ejemplo, NFS) con Backup Gateway, dicho almacenamiento externo debería proporcionar la redundancia. Backup Gateway no proporciona redundancia de datos ni realiza la deduplicación de datos por sí mismo.
- Para registrar Backup Gateway en Acronis Backup Cloud, deshabilite la autenticación de doble factor (2FA) de su cuenta de socio.

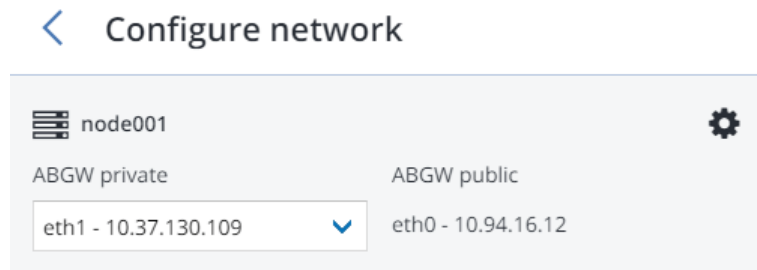
## 6.1 Conexión al clúster de almacenamiento local mediante Backup Gateway

Antes de continuar, asegúrese de que su almacenamiento de destino tenga suficiente espacio para las copias de seguridad existentes y nuevas.

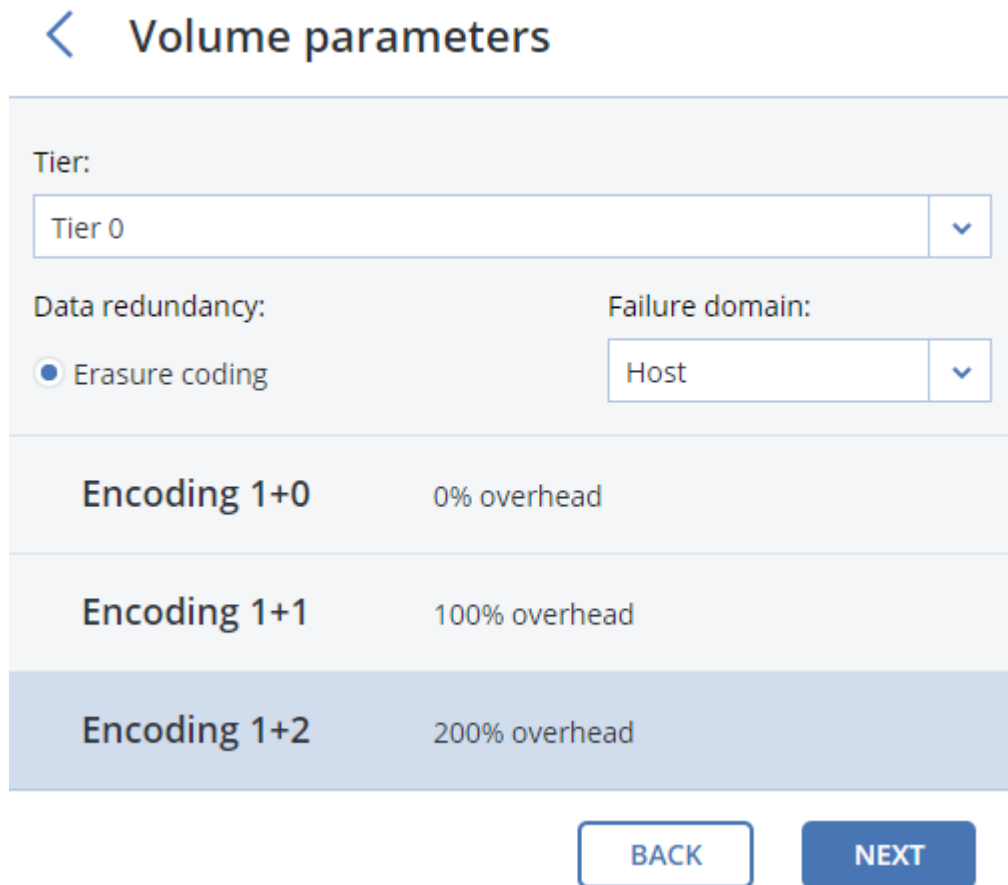
Para configurar Backup Gateway, siga los siguientes pasos:

1. En la pantalla **INFRAESTRUCTURA > Redes**, asegúrese de que se han añadido los tipos de tráfico **ABGW privado** y **ABGW público** a las redes que vaya a utilizar.
2. En el menú de la izquierda, haga clic en **SERVICIOS DE ALMACENAMIENTO > Almacenamiento de la copia de seguridad**.
3. Seleccione los nodos para ejecutar los servicios de puerta de enlace y haga clic en **Crear puerta de enlace** en el menú derecho.
4. Seleccione **Este clúster de Acronis Cyber Infrastructure** como tipo de almacenamiento.
5. Asegúrese de que está seleccionada la interfaz de red correcta en la lista desplegable. Haga clic en **SIGUIENTE**.

Si fuese necesario, haga clic en el icono de rueda dentada y configure las interfaces de red del nodo en la pantalla **Configuración de red**.



6. En la pestaña **Parámetros de volumen**, seleccione el nivel deseado, el dominio de fallo y el modo de redundancia de datos. Para obtener más información, consulte Understanding Storage Tiers, Understanding Failure Domains y Understanding Data Redundancy.



La redundancia por replicación no es compatible con Backup Gateway. Se ha deshabilitado la modificación del esquema de redundancia para la codificación de borrado, ya que puede reducir el rendimiento del clúster. Esto se debe a que volver a codificar requiere una gran cantidad de recursos del clúster durante un período de tiempo prolongado. Si de todos modos desea cambiar el esquema de redundancia, póngase en contacto con el soporte técnico.



Haga clic en **SIGUIENTE**.

7. En la pestaña **Configuración DNS**, especifique el nombre de DNS externo para esta puerta de enlace, por ejemplo, `puertadeenlacedecopiadeseguridad.ejemplo.com`. Asegúrese de que cada nodo que ejecuta el servicio de puerta de enlace tiene un puerto abierto para las conexiones de Internet salientes y las conexiones entrantes del software de copia de seguridad de Acronis. Los agentes de copia de seguridad usarán esta dirección y puerto para cargar los datos de copia de seguridad.

---

**Importante:** Configure su Servidor DNS de acuerdo con el ejemplo sugerido en el panel de administración.

---

---

**Importante:** Cada vez que cambie los nodos en el clúster de Backup Gateway, ajuste la configuración de DNS según corresponda.

---

< DNS configuration

DNS name

backup.example.com

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backup.example.com. (
2018120313 ; serial
1h ; refresh
30m ; retry
7d ; expiration
1h ) ; minimum
```

BACK NEXT

Haga clic en **Siguiente**.

8. En el panel **Registrar en software de copia de seguridad**, especifique la siguiente información de su producto Acronis:

**Importante:** Asegúrese de que la autenticación de doble factor (2FA) está deshabilitada en su cuenta de socio. También puede deshabilitarla para un determinado usuario en un inquilino que tenga habilitada la autenticación de doble factor, tal y como se describe en la [Documentación de Acronis Cyber Cloud](#), y especificar las credenciales de usuario.

---

- En **Dirección**, especifique la dirección del portal de gestión de Acronis Backup Cloud (por ejemplo, <https://cloud.acronis.com/>) o el nombre de host o la dirección IP y el puerto del servidor de gestión de Acronis Backup Advanced (por ejemplo, <http://192.168.1.2:9877>).
- En **Cuenta**, especifique las credenciales de una cuenta de socio en el cloud o del administrador de una organización en el servidor de gestión local.

9. Por último, haga clic en **LISTO**.

## 6.2 Conexión a recursos compartidos de NFS externos mediante Backup Gateway

Tenga en cuenta las siguientes limitaciones:

- Acronis Cyber Infrastructure no proporciona redundancia de datos sobre los volúmenes NFS. Dependiendo de la implementación, los recursos compartidos de NFS pueden usar su propia redundancia de hardware o software.
- En la versión actual de Acronis Cyber Infrastructure, solo el nodo de clúster puede almacenar copias de seguridad en un volumen NFS.

Antes de continuar, asegúrese de lo siguiente:

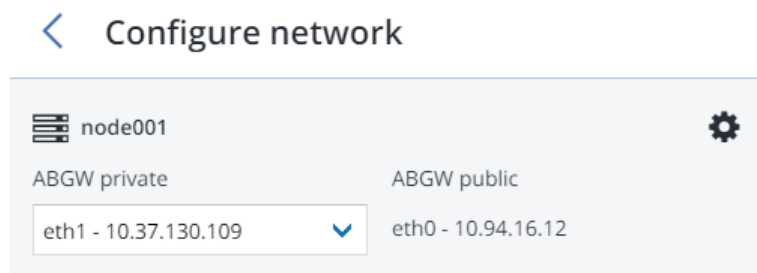
1. El recurso compartido de NFS tiene suficiente espacio para copias de seguridad.
2. Solo una puerta de enlace usa cada exportación NFS. En especial, no configure dos instalaciones de Acronis Cyber Infrastructure para usar la misma exportación NFS para almacenamiento de copias de seguridad.

Para configurar Backup Gateway, siga los siguientes pasos:

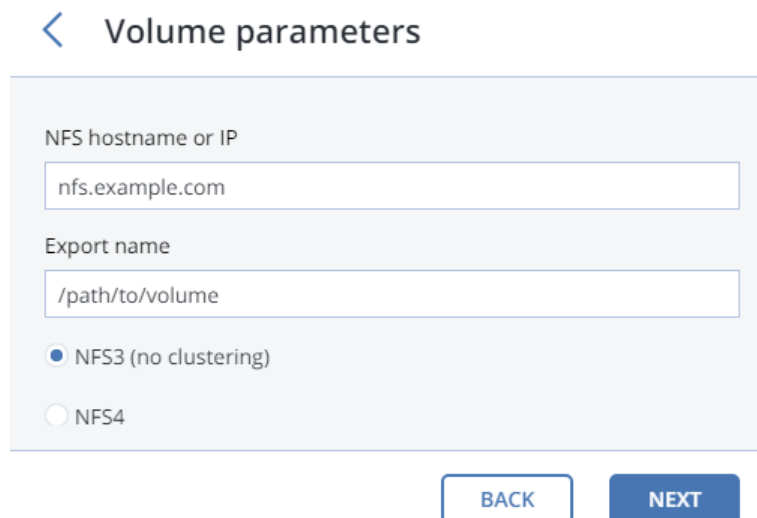
1. En la pantalla **INFRAESTRUCTURA > Redes**, asegúrese de que se han añadido los tipos de tráfico **ABGW privado** y **ABGW público** a las redes que vaya a utilizar.

2. En el menú de la izquierda, haga clic en **SERVICIOS DE ALMACENAMIENTO > Almacenamiento de la copia de seguridad**.
3. Seleccione los nodos para ejecutar los servicios de puerta de enlace y haga clic en **Crear puerta de enlace** en el menú derecho.
4. Seleccione **Sistema de archivos de red** como tipo de almacenamiento.
5. Asegúrese de que está seleccionada la interfaz de red correcta en la lista desplegable. Haga clic en **SIGUIENTE**.

Si fuese necesario, haga clic en el icono de rueda dentada y configure las interfaces de red del nodo en la pantalla **Configuración de red**.



6. En la pestaña **Parámetros de volumen**, especifique el nombre de host o la dirección IP del recurso compartido NFS así como el nombre de la exportación. Haga clic en **SIGUIENTE**.



7. En la pestaña **Configuración DNS**, especifique el nombre de DNS externo para esta puerta de enlace, por ejemplo, puertadeenlacedecopiadeseguridad.ejemplo.com. Asegúrese de que cada nodo que ejecuta el servicio de puerta de enlace tiene un puerto abierto para las conexiones de Internet salientes y las

conexiones entrantes del software de copia de seguridad de Acronis. Los agentes de copia de seguridad usarán esta dirección y puerto para cargar los datos de copia de seguridad.

**Importante:** Configure su Servidor DNS de acuerdo con el ejemplo sugerido en el panel de administración.

**Importante:** Cada vez que cambie los nodos en el clúster de Backup Gateway, ajuste la configuración de DNS según corresponda.

< DNS configuration

DNS name

backup.example.com

This may require changing the DNS server configuration, which may look as follows:

```
$TTL 1h
@ IN SOA ns1.myhoster.com. root.backup.example.com. (
  2018120313 ; serial
  1h ; refresh
  30m ; retry
  7d ; expiration
  1h ) ; minimum
```

BACK NEXT

Haga clic en **Siguiente**.

8. En el panel **Registrar en software de copia de seguridad**, especifique la siguiente información de su producto Acronis:

**Importante:** Asegúrese de que la autenticación de doble factor (2FA) está deshabilitada en su cuenta de socio. También puede deshabilitarla para un determinado usuario en un inquilino que tenga

habilitada la autenticación de doble factor, tal y como se describe en la [Documentación de Acronis Cyber Cloud](#), y especificar las credenciales de usuario.

---

- En **Dirección**, especifique la dirección del portal de gestión de Acronis Backup Cloud (por ejemplo, <https://cloud.acronis.com/>) o el nombre de host o la dirección IP y el puerto del servidor de gestión de Acronis Backup Advanced (por ejemplo, <http://192.168.1.2:9877>).
- En **Cuenta**, especifique las credenciales de una cuenta de socio en el cloud o del administrador de una organización en el servidor de gestión local.

9. Por último, haga clic en **LISTO**.

## 6.3 Conexión al sistema de almacenamiento público en el cloud a través de Backup Gateway

Con Backup Gateway, puede hacer que Acronis Backup Cloud o Acronis Backup Advanced almacenen copias de seguridad en varias nubes públicas y en soluciones locales de almacenamiento de objetos:

- Amazon S3
- IBM Cloud
- Alibaba Cloud
- Iij
- Cleversafe
- Cloudian
- Microsoft Azure
- Almacenamiento de objetos de Swift
- SoftLayer (Swift)
- Google Cloud Platform
- Wasabi
- Otras soluciones que utilizan S3

Sin embargo, en comparación con el clúster de almacenamiento local, almacenar datos de copia de seguridad en un cloud público aumenta la latencia de todas las solicitudes de E/S a copias de seguridad y reduce el rendimiento. Por este motivo, se recomienda usar el clúster de almacenamiento local como back-end de almacenamiento.

Las copias de seguridad son datos estáticos con un modelo de acceso específico: no se accede a los datos de manera frecuente pero deben estar disponibles de inmediato cuando se acceda a ellos. Para este caso de uso, es rentable elegir clases de almacenamiento diseñadas para el almacenamiento a largo plazo con un acceso infrecuente a los datos. Las clases de almacenamiento recomendadas incluyen las siguientes:

- **Acceso infrecuente** para Amazon S3
- **Almacenamiento de blobs estáticos** para Microsoft Azure
- **Nearline Storage** y **Coldline Storage** para Google Cloud Platform

Las clases de almacenamiento de archivos comprimidos como Amazon S3 Glacier, Azure Archive Blob, o Google Archive no se pueden utilizar porque no proporcionan acceso instantáneo a los datos. La alta latencia de acceso (varias horas) hace que sea técnicamente imposible explorar archivos comprimidos, restaurar datos de forma rápida y crear copias de seguridad incrementales. Incluso aunque el almacenamiento de archivos comprimidos es, por lo general, muy rentable, tenga en mente que existen distintos factores de coste. De hecho, el coste total del almacenamiento en la nube pública consiste en pagos por almacenar datos, operaciones, tráfico, recuperación de datos y eliminación temprana, entre otros. Por ejemplo, un servicio de almacenamiento de archivos comprimidos puede cobrar seis meses de almacenamiento por una sola operación de recuperación de datos. Si se espera acceder a los datos almacenados de manera más frecuente, los costes añadidos aumentan significativamente el coste total del almacenamiento de datos. Para evitar una tasa de recuperación de datos baja y para ahorrar costes, recomendamos utilizar Acronis Cyber Cloud para almacenar los datos de las copias de seguridad.

### 6.3.1 Requisitos y restricciones importantes

1. Al funcionar con clouds públicos, Backup Gateway usa el almacenamiento local como área de almacenamiento provisional y para guardar la información de servicio. Esto quiere decir que los datos que se van a cargar a un cloud público primero se almacenan localmente y luego envían a su destino. Por este motivo, es fundamental que el almacenamiento local sea persistente y redundante para que los datos no se pierdan. Hay varias formas de garantizar la persistencia y la redundancia del almacenamiento local. Puede implementar Backup Gateway en varios nodos de clúster y seleccionar un buen modo de redundancia. Si se implementa Acronis Cyber Infrastructure con la puerta de enlace en

un único nodo físico, puede hacer que el almacenamiento local sea redundante al replicarlo en discos locales. Si se implementa Acronis Cyber Infrastructure con la puerta de enlace en un equipo virtual, asegúrese de que la solución de virtualización en la que se ejecuta lo hace redundante.

2. Asegúrese de que el clúster de almacenamiento local tiene suficiente espacio lógico para el almacenamiento provisional. Por ejemplo, si realiza copias de seguridad a diario, proporcione suficiente espacio para realizar copias de seguridad durante un día y medio como mínimo. Si el total de copias de seguridad diarias es 2 TB, proporcione al menos 3 TB de espacio lógico. El almacenamiento sin formato necesario variará según el modo de codificación: 9 TB (3 TB por nodo) en el modo 1+2, 5 TB (1 TB por nodo) en el modo 3+2, etc.
3. Si va a almacenar copias de seguridad en un cloud de Amazon S3, tenga en cuenta que Backup Gateway puede a veces bloquear el acceso a este tipo de copias de seguridad debido a la consistencia eventual de Amazon S3. Esto significa que Amazon S3 puede, en ocasiones, devolver datos obsoletos, ya que necesita tiempo para representar la versión más reciente de los datos accesibles. Backup Gateway detecta estos retrasos y protege la integridad de las copias de seguridad al bloquear el acceso hasta que se actualiza el cloud.
4. Utilice un contenedor de objetos para cada clúster de Backup Gateway.

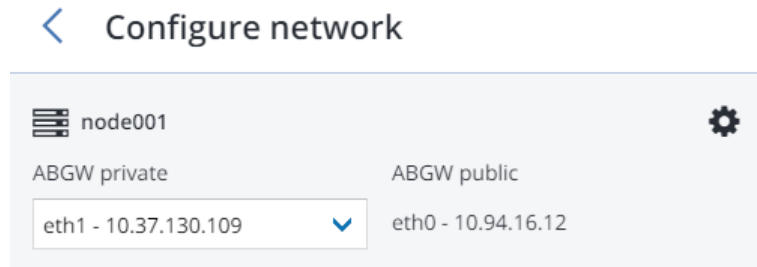
### 6.3.2 Configuración de Backup Gateway

Antes de continuar, asegúrese de que su almacenamiento de destino tenga suficiente espacio para copias de seguridad.

Para configurar Backup Gateway, siga los siguientes pasos:

1. En la pantalla **INFRAESTRUCTURA > Redes**, asegúrese de que se han añadido los tipos de tráfico **ABGW privado** y **ABGW público** a las redes que vaya a utilizar.
2. En el menú de la izquierda, haga clic en **SERVICIOS DE ALMACENAMIENTO > Almacenamiento de la copia de seguridad**.
3. Seleccione los nodos para ejecutar los servicios de puerta de enlace y haga clic en **Crear puerta de enlace** en el menú derecho.
4. Seleccione **Cloud público** como el tipo de almacenamiento.
5. Asegúrese de que está seleccionada la interfaz de red correcta en la lista desplegable. Haga clic en **SIGUIENTE**.

Si fuese necesario, haga clic en el icono de rueda dentada y configure las interfaces de red del nodo en la pantalla **Configuración de red**.



6. En el panel **Parámetros del cloud público**, siga los siguientes pasos:

- 6.1. Seleccione un proveedor de cloud público. Si su proveedor es compatible con S3, pero no está en la lista, pruebe **Compatible con AuthV2 (S3)** o **Compatible con AuthV4 (S3)**.
- 6.2. En función del proveedor, especifique **Región**, **URL de autenticación (Keystone)** o **URL del extremo**.
- 6.3. En el caso del almacenamiento de objetos Swift, especifique la versión del protocolo de autenticación y los atributos que requiere.
- 6.4. Especifique las credenciales del usuario. En el caso de Google Cloud, seleccione un archivo JSON con las claves para cargarlo.
- 6.5. Especifique la carpeta (bucket, contenedor) en la que se almacenarán las copias de seguridad. La carpeta especificada debe ser grabable.

Utilice un contenedor de objetos para cada clúster de Backup Gateway.

Haga clic en **SIGUIENTE**.

7. En el panel **Registrar en software de copia de seguridad**, especifique la siguiente información de su producto Acronis:

---

**Importante:** Asegúrese de que la autenticación de doble factor (2FA) está deshabilitada en su cuenta de socio. También puede deshabilitarla para un determinado usuario en un inquilino que tenga habilitada la autenticación de doble factor, tal y como se describe en la [Documentación de Acronis Cyber Cloud](#), y especificar las credenciales de usuario.

---



- En **Dirección**, especifique la dirección del portal de gestión de Acronis Backup Cloud (por ejemplo, <https://cloud.acronis.com/>) o el nombre de host o la dirección IP y el puerto del servidor de gestión de Acronis Backup Advanced (por ejemplo, <http://192.168.1.2:9877>).
- En **Cuenta**, especifique las credenciales de una cuenta de socio en el cloud o del administrador de una organización en el servidor de gestión local.

8. Por último, haga clic en **LISTO**.