



Conceptos básicos de Veeam Backup and Replication Y Mejores Prácticas

Agenda

1. Introducción
2. Arquitectura y componentes principales
3. Características avanzadas y componentes opcionales
4. Configuración general del producto
5. Concepto y configuración de trabajos
6. Capacidades de restauración
7. Seguridad
8. Consejos y trucos
9. Recursos adicionales

Sección 01

Introducción

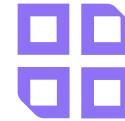
Capacidades Principales, Plataformas Compatibles, Licenciamiento

Veeam Data Platform

	Fundamento Seguro	Ciber Resiliencia				Resiliencia Empresarial		
	Protección de Datos de Confianza Cero	Asistencia y remediación basada en IA	Detectar + Identificar amenazas	Seguridad y Observabilidad	Perspectivas de GenAI	Orquestación de recuperación y cumplimiento	Evaluación de amenazas	
Protección de Datos y Recuperación Verificada	Asistencia a demanda	Detección de malware con Tecnología IA	Herramientas de escaneo de IoC	Integraciones de seguridad	Ánalisis, descubrimiento y generación de informes	Centro de Amenazas de Veeam	Tendencias y soporte de decisiones	Recuperación y validación orquestadas
Foundation	✓	✓	✓	—	—	—	—	—
Advanced	✓	✓	✓	✓	✓	✓	✓	—
Premium	✓	✓	✓	✓	✓	✓	✓	✓
 Veeam Backup & Replication  Veeam ONE  Veeam Recovery Orchestrator  Coveware Recon Scanner			<ul style="list-style-type: none"> Suscripción a Coveware Incident Response con contrato de nivel de servicio de 15 minutos Garantía contra ransomware de hasta 5 millones de USD con Veeam Technical Account Manager Equipo SWAT disponible las 24 horas, los 7 días de la semana, los 365 días del año y gerente de cuenta de soporte dedicado Servicios de incorporación, diseño e implementación y controles de evaluación de seguridad trimestrales 					

Plataformas Compatible

Para Veeam Backup &
Replication v12.3



Sin Agentes (Virtual)

- VMware vSphere 6.x – 8.0U2
- VMware Cloud Director 10.1 – 10.5.x
- Microsoft Windows Server Hyper-V 2012 – 2022
 - Azure Stack HCI
 - *Compatible con Microsoft Hyper-V Server (hipervisor gratuito)
 - *Las instalaciones de Server Core son totalmente compatibles
 - Nutanix AOS 6.5 or later
 - Red Hat Virtualization 4.4 SP1 only (RHVM 4.5.0 or later)
 - Oracle Linux Virtualization 4.5.4 or later
 - Proxmox Virtual Environment 8.2 or later

Plataformas Compatible

Para Veeam Backup &
Replication v12.3



Agentes (Cargas de trabajo físicas o virtuales)

- Microsoft Windows Server 2008 R2 SP1 – 2022
- Microsoft Windows 7 SP1 – 11 24H2
 - *Se admiten las instalaciones de Server Core
- La mayoría de las distribuciones de Linux más populares ([Lista Completa](#))
- Mac OS 10.13.6 High Sierra – 15 Sequoia
- IBM AIX 7.1 – 7.3 TL2
- Oracle Solaris 10 1/13, 11.0 – 11.4
 - * Compatible con SPARK y x86

Plataformas Compatible

Para Veeam Backup &
Replication v12.3



Datos No estructurados

- File Shares (SMB and NFS)
- Enterprise NAS systems:
 - NetApp Data ONTAP (SnapDiff support)
 - Lenovo ThinkSystem DM Series
 - Dell PowerScale (Anteriormente Isilon)
 - Nutanix Files Storage
- Depósitos de almacenamiento de objetos:
 - Repositorios de almacenamiento de objetos compatibles con S3
 - Almacenamiento de objetos Amazon S3
 - Almacenamiento Blob de Microsoft Azure
 - ONTAP FSx

Plataformas Compatibles

by Veeam Backup &
Replication v12.3



Bases de Datos – Plugins

- MS SQL 2014 SP3 – 2022
- Oracle 11gR2 – 23c
- SAP HANA 1.0 and 2.0 both on Linux and Power (Consulte la Guía del usuario)
- MongoDB 5.0 – 8.0
- IBM db2 10.5, 11.1, 11.5 on Linux, Power and AIX

Other workloads

- EntralD

Licenciamiento

Dos **modelos** de licenciamiento

Por-Socket

Modelo heredado. Aún disponible para clientes existentes.

Veeam Backup & Replication se licencia por el número de sockets de CPU en los hosts protegidos.

La licencia sólo es necesaria para los hosts de origen, es decir, los hosts en los que residen las máquinas virtuales de las que realiza copias de seguridad o réplicas. Los hosts de destino (para trabajos de replicación y migración) no necesitan licencia.

Basado por instancias (VUL)

Nuevo modelo. Es más flexible y puede utilizarse en diferentes productos.

Las instancias son unidades que puede utilizar para proteger sus cargas de trabajo virtuales, físicas o basadas en la nube.

Debe obtener una licencia con el número total de instancias para las cargas de trabajo que planea proteger en Veeam Backup & Replication.

Licenciamiento

Dos [tipos](#) de Licenciamiento

Perpetuo

Licencia permanente. El periodo de soporte y mantenimiento se incluye con la licencia y se especifica en meses o años.

La Licencia Perpetua incluye un contrato de Soporte y Mantenimiento Básico o de Producción durante el primer año.

El plazo máximo de prepago de Soporte y Mantenimiento para una Licencia Perpetua es de tres años.

Suscripción

Licencia que expira al final del plazo de suscripción.

La licencia de suscripción incluye un contrato de soporte y mantenimiento de la producción durante todo el periodo de vigencia de la licencia.

El plazo de la licencia de suscripción suele ser de 1 a 3 años a partir de la fecha de emisión de la licencia.

El plazo máximo de prepago de una licencia de suscripción es de cinco años.

Arquitectura y componentes básicos

Descripción General de Los Componentes, Revisión del Proceso de Instalación, Flujo de Trabajo de las Copias de Seguridad, Desglose Exhaustivo de los Componentes, Diseño

Componentes

Arquitectura y Componentes Básicos

Descripción General



Consola
VBR



Backup Proxy



Backup Server



Backup
Repository

Instalación

Arquitectura y Componentes Básicos

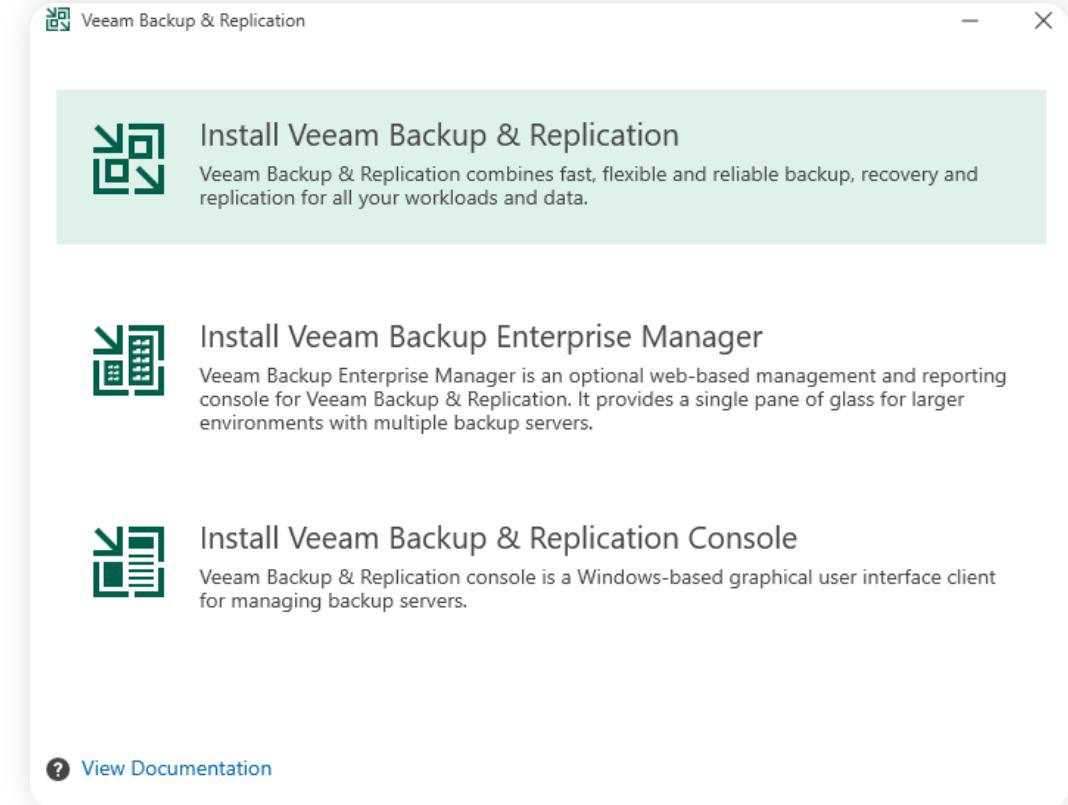
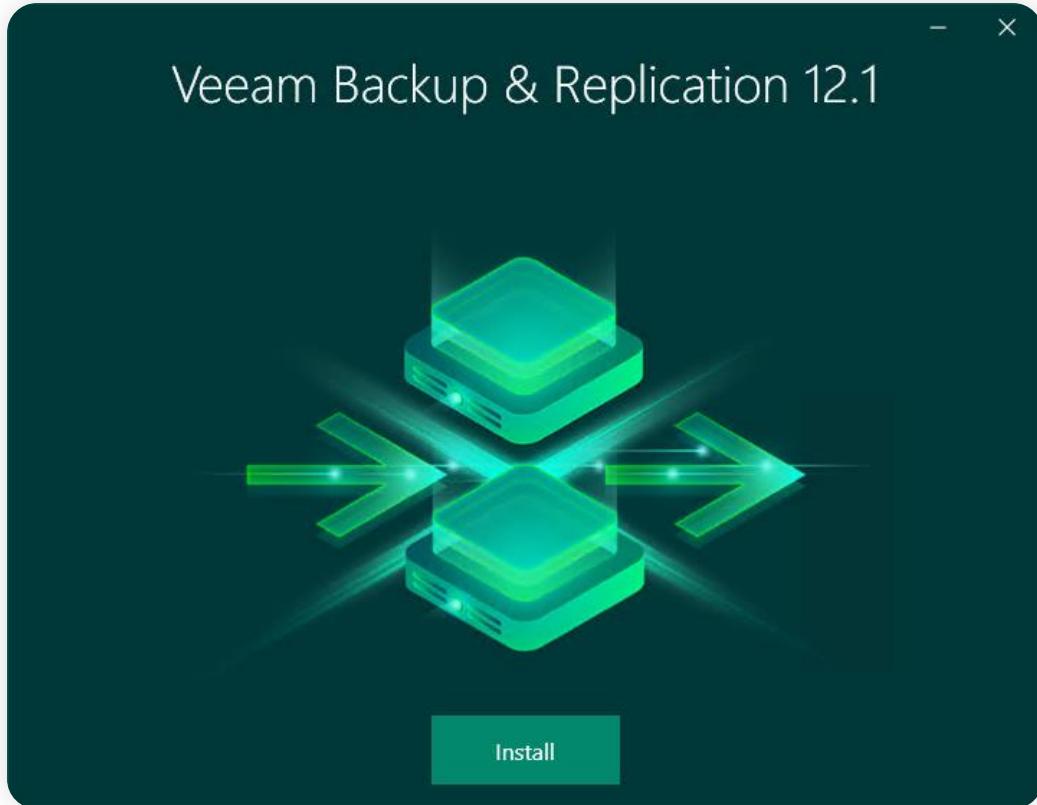
Instalación

Descargue la versión más reciente del archivo .ISO desde <https://my.veeam.com/my-products>. Regístrese si es necesario.

The image displays two main screenshots of the Veeam My Account interface. The left screenshot shows the 'Log In to Access Your Account' page, which includes fields for email and password, and links for 'SEE WHAT'S NEW' and 'DOWNLOAD'. The right screenshot shows the 'Product downloads' page, listing various Veeam products like Veeam Data Platform, Veeam Recovery Orchestrator, and Veeam ONE, each with a 'DOWNLOAD' button. A sidebar on the right of the download page contains navigation icons.

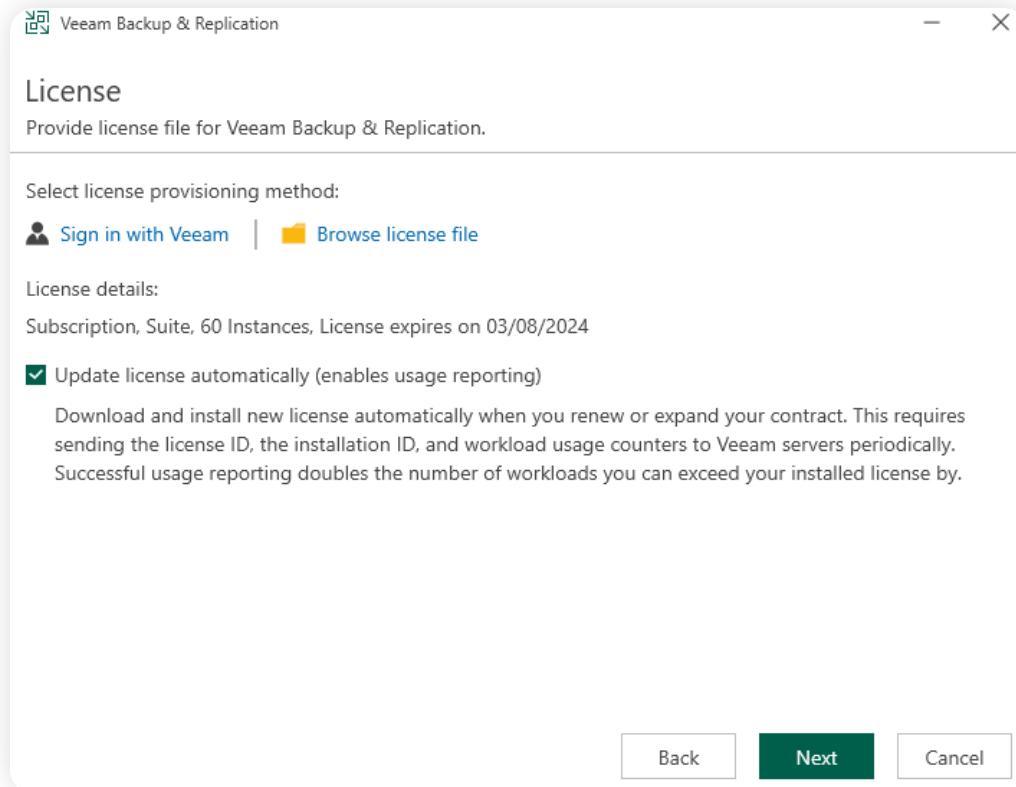
Arquitectura y Componentes Básicos

Instalación



Arquitectura y Componentes Básicos

Instalación



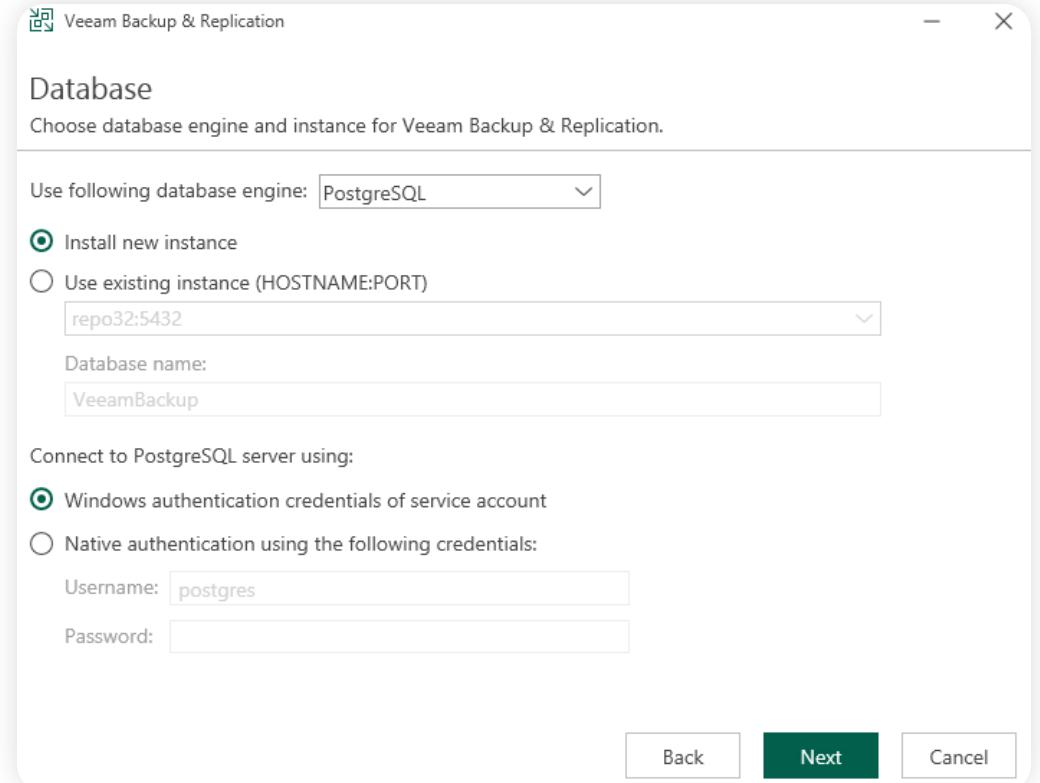
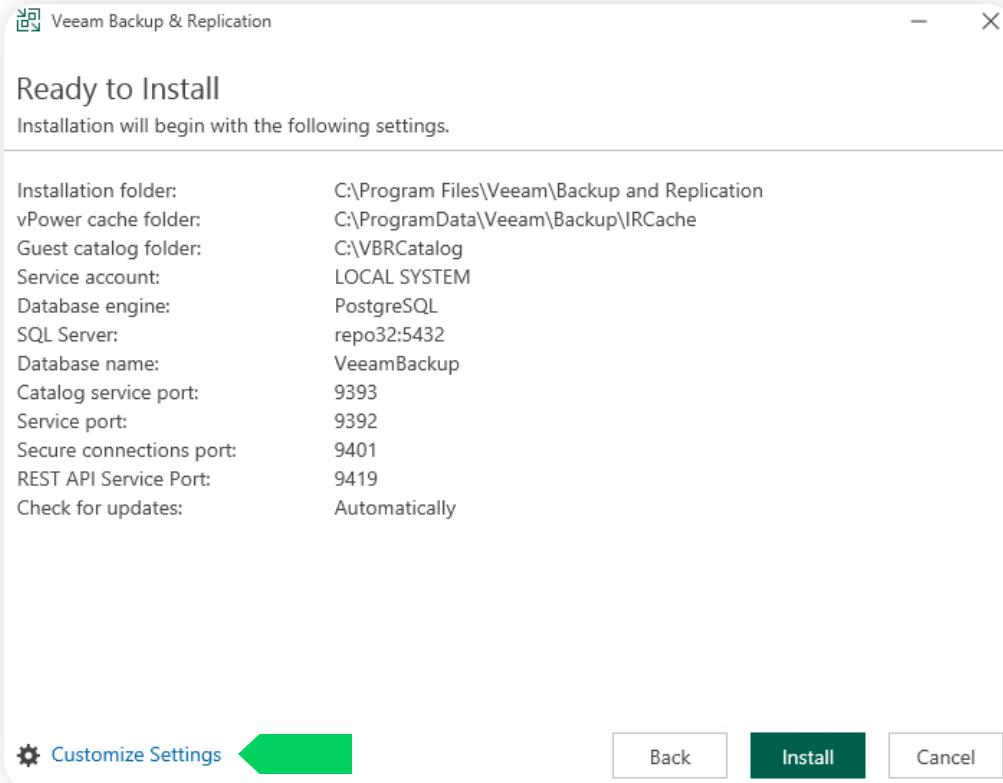
The screenshot shows the 'System Configuration Check' step. It informs the user that the system is being verified for potential installation problems. A message box states: 'Setup could not automatically install required system prerequisites. Please install missing components and click "Retry" to continue.' Below this, a table lists system requirements and their status:

Requirement	Status
Microsoft .NET Framework 4.7.2	Passed
Microsoft Visual C++ 2015-2019 Redistributable	Passed
Microsoft System CLR Types for SQL Server 2014	Failed
Microsoft Report Viewer Redistributable 2015	Passed
Microsoft PowerShell v5.1	Passed
Microsoft Universal C Runtime	Passed
Microsoft .NET Runtime 6.0.10	Passed
Microsoft ASP.NET Core Shared Framework 6.0.10	Passed

At the bottom are 'Back', 'Retry', and 'Cancel' buttons.

Arquitectura y Componentes Básicos

Instalación



Base de Datos de Configuración

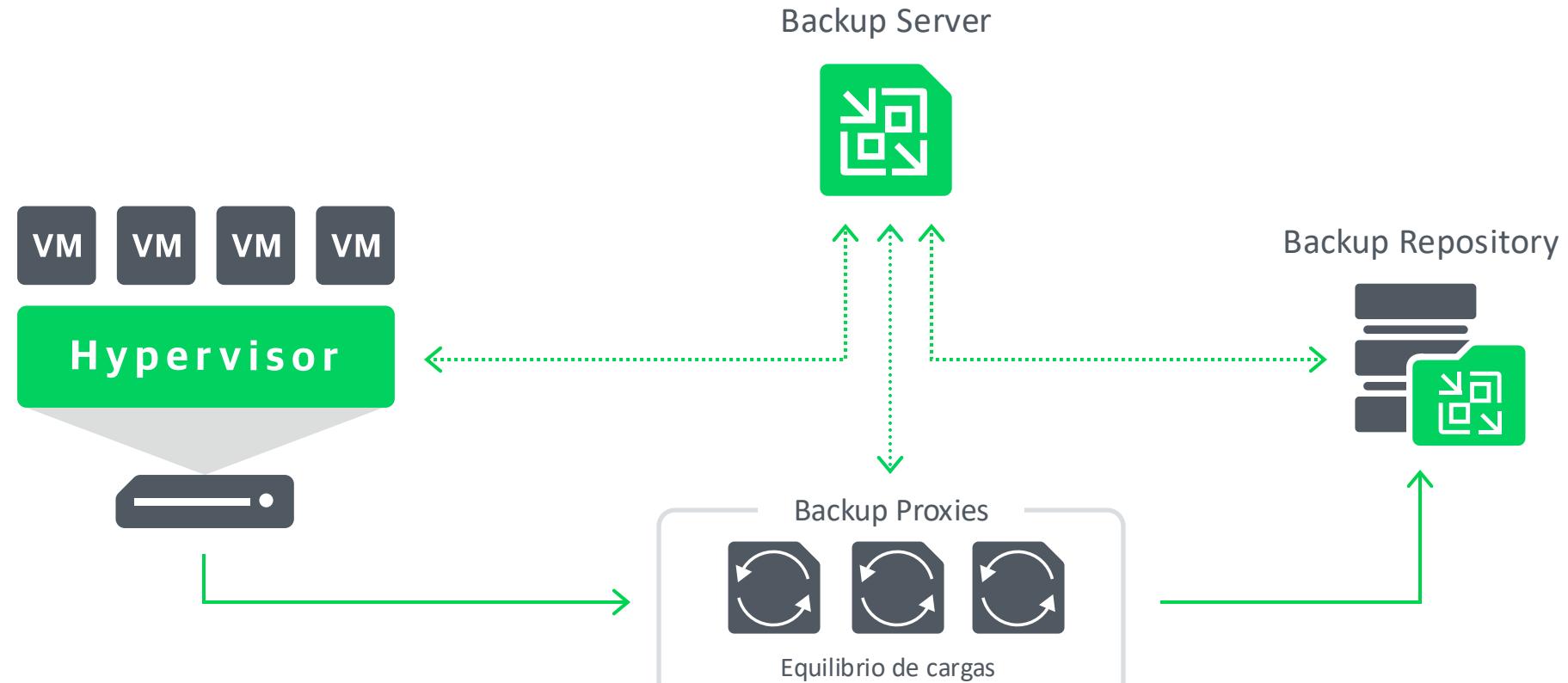
Base de Datos de Configuración

- Almacena datos sobre la infraestructura de copia de seguridad, trabajos y sesiones.
- Desde la v.12, el instalador de VBR instala por defecto PostgreSQL. Se puede cambiar a Microsoft SQL.
- DB se puede migrar de MSSQL a PostgreSQL y viceversa.
- DB puede instalarse localmente (en la misma máquina que el servidor de copia de seguridad) o remotamente.
- La copia de seguridad de la base de datos de configuración es la forma en que VBR se “respalda a sí mismo”.
- DB se puede restaurar en otro servidor VBR.

Desglose Detallado de Componentes

Arquitectura y Componentes Básicos

Ejemplo de Copia de Seguridad



Backup Proxy

Arquitectura y Componentes Básicos

Backup Proxy

Tipos

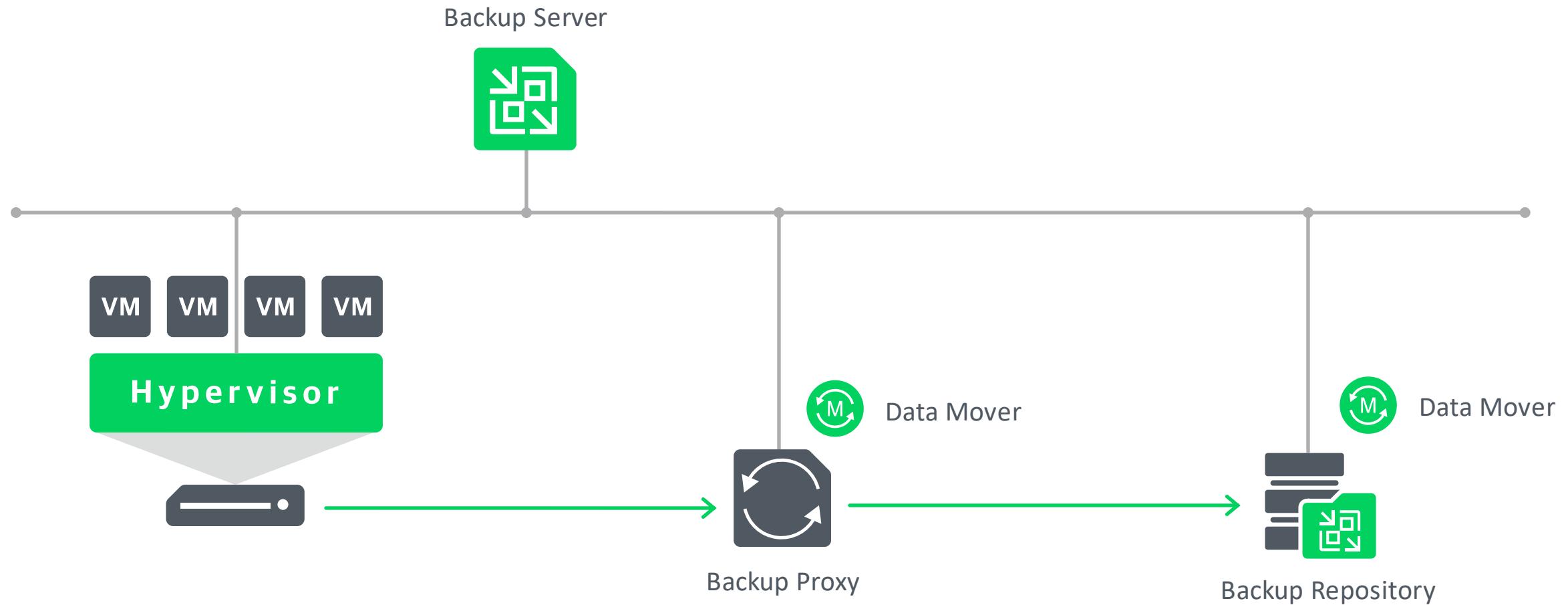
- VMware
- VMware CDP
- Hyper-V On-host
- Hyper-V Off-host
- Nutanix AHV (Appliance)
- Red Hat Virtualization (Appliance)
- Proxmox (Worker)
- General Purpose (NAS, File shares, Physical Servers Off-host backup)

Funciones

- Recuperación de datos de máquinas virtuales del almacenamiento de producción
- Compresión
- Deduplicación
- Encriptación
- Enviar datos al repositorio de copias de seguridad (copia de seguridad) o a otro proxy de copias de seguridad (replicación)

Arquitectura y Componentes Básicos

Backup Proxy



Backup Proxy (VMware)

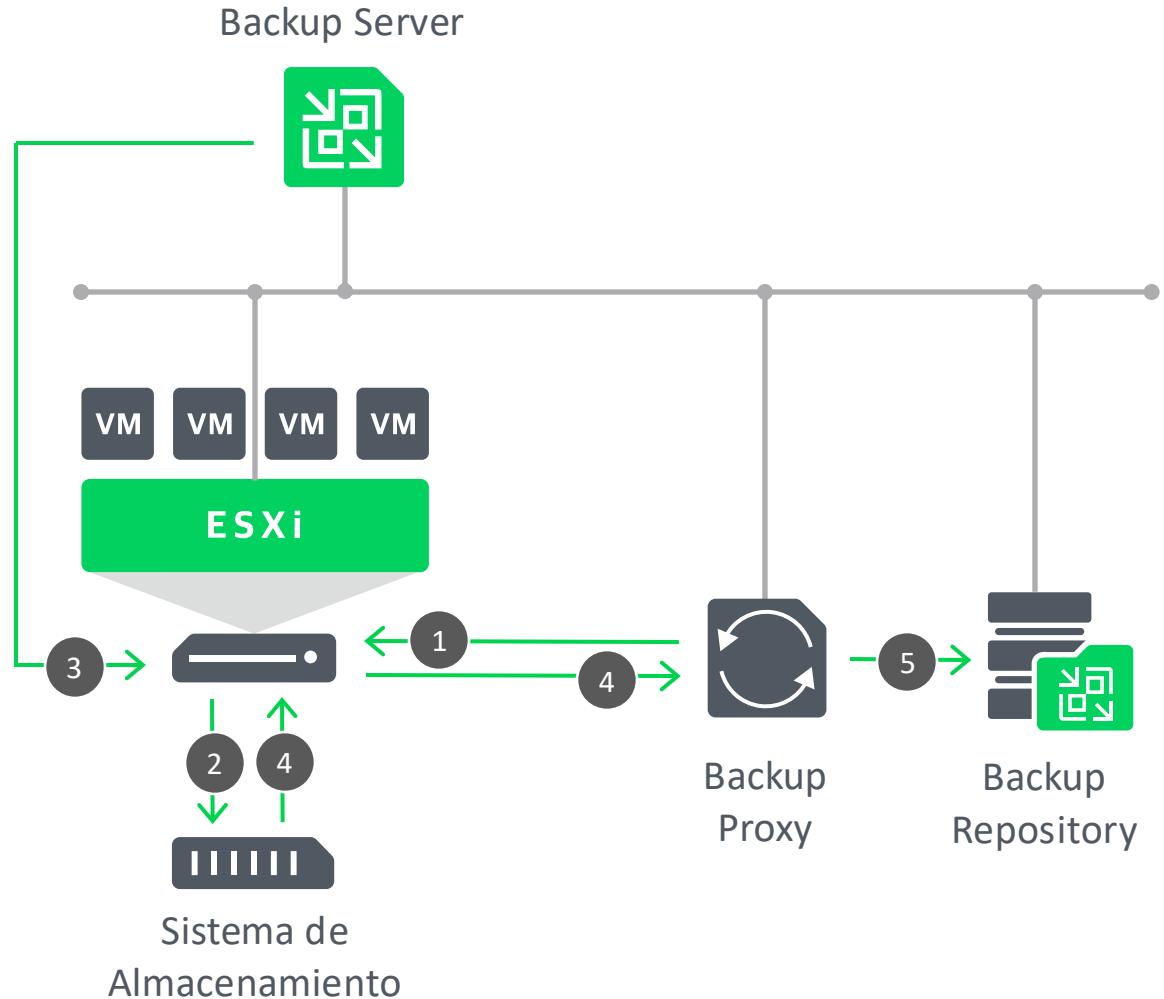
Arquitectura y Componentes Básicos

VMware Backup Proxy Modos de Transporte

Red

En este modo, los datos se recuperan a través del host ESXi a través de LAN utilizando el protocolo de dispositivo de bloque de red (NBD).

1. El proxy envía una solicitud al host ESXi para ubicar la máquina virtual en el almacén de datos.
2. El host ESXi localiza la VM.
3. VBR le indica a VMware vSphere que cree una instantánea.
4. El host ESXi copia bloques de datos de la máquina virtual desde el almacenamiento de origen y los envía al proxy a través de LAN.
5. El Proxy envía los datos al Repositorio.



Arquitectura y Componentes Básicos

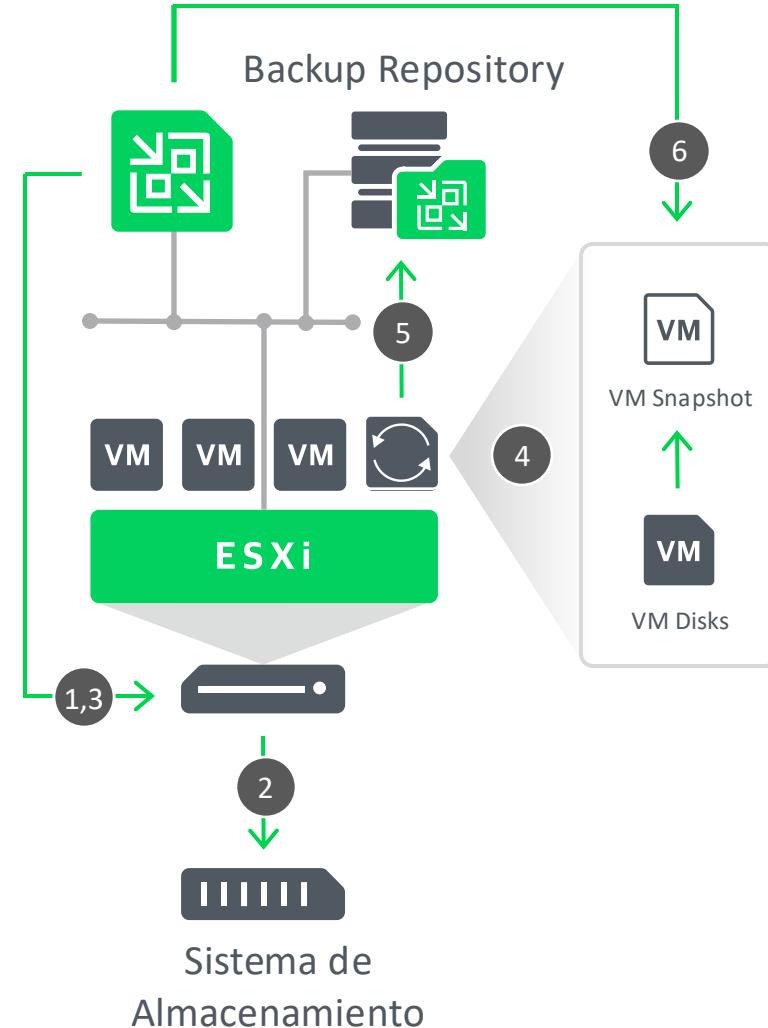
VMware Backup Proxy Modos de Transporte

Virtual Appliance

Este modo proporciona un mejor rendimiento que el modo de red.

El servidor de respaldo envía una solicitud al host ESXi para ubicar la máquina virtual en el almacén de datos.

1. El host ESXi localiza la máquina virtual.
2. VBR activa VMware vSphere para crear una instantánea de la máquina virtual.
3. Los discos de la máquina virtual se conectan (se agregan en caliente) al proxy.
4. VBR lee los datos directamente desde los discos conectados al proxy.
5. Cuando se completa el procesamiento de la máquina virtual, los discos de la máquina virtual se desconectan del proxy y se elimina la instantánea de la máquina virtual.



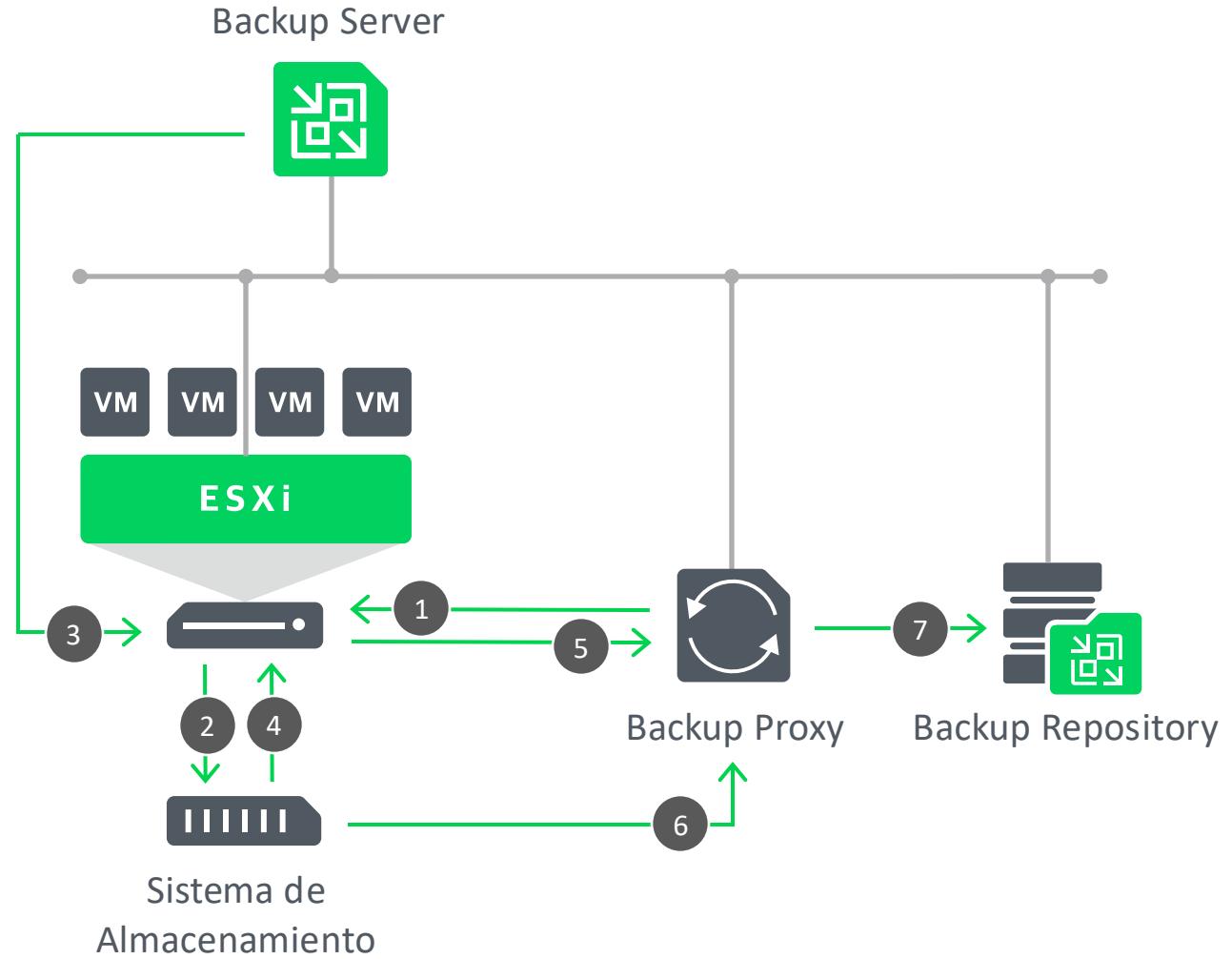
Arquitectura y Componentes Básicos

VMware Backup Proxy Modos de Transporte

Acceso Directo Al Almacenamiento

En este modo, VBR utiliza VMware VADP para el transporte directo de datos de VM a través de SAN (FC, FCoE, iSCSI).

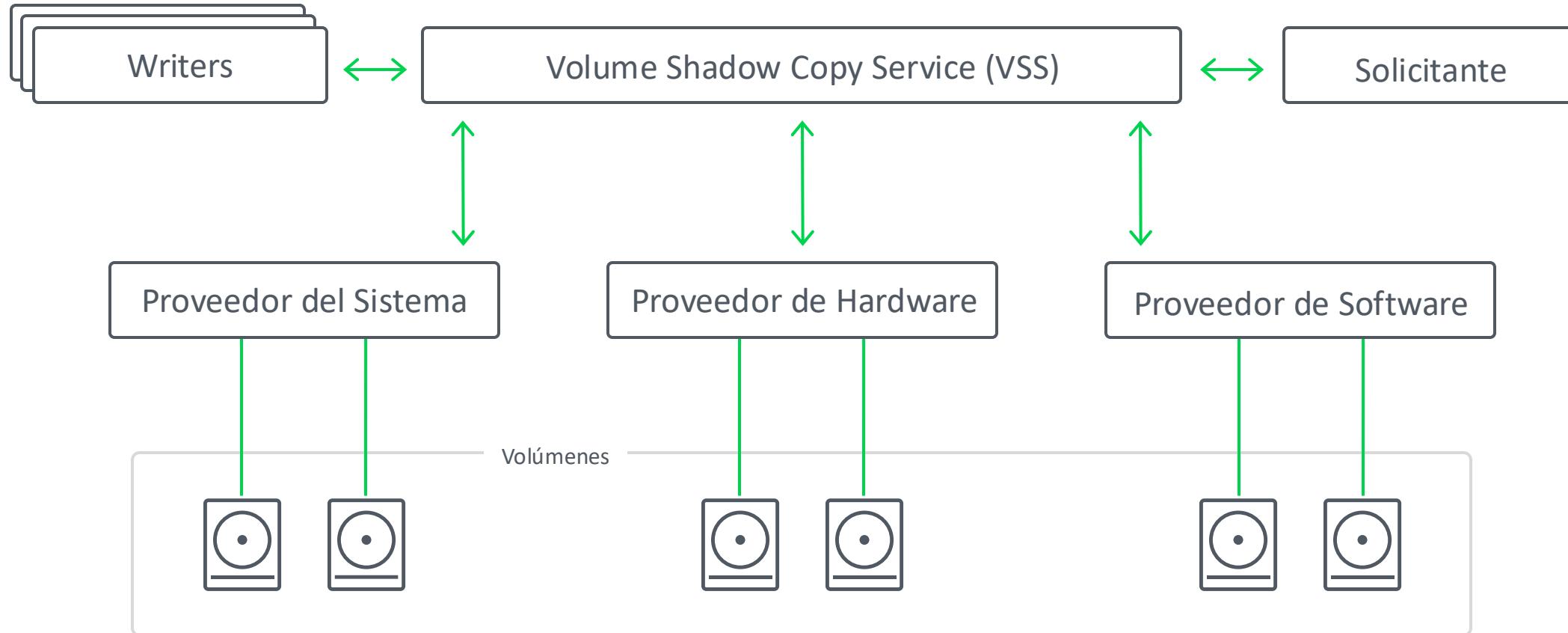
1. El proxy solicita la ubicación de la máquina virtual a ESXi.
2. El host ESXi ubica la máquina virtual.
3. El VBR activa una instantánea de la máquina virtual.
4. El host ESXi recupera metadatos sobre el diseño de los discos de la máquina virtual en el almacenamiento.
5. El host ESXi envía metadatos al proxy.
6. El proxy usa metadatos para copiar bloques de datos de la máquina virtual directamente desde el almacenamiento de origen.
7. El proxy procesa los bloques de datos copiados y los envía al destino.



Backup Proxy (Hyper-V)

Arquitectura y Componentes Básicos

Volume Shadow Copy Service (VSS)



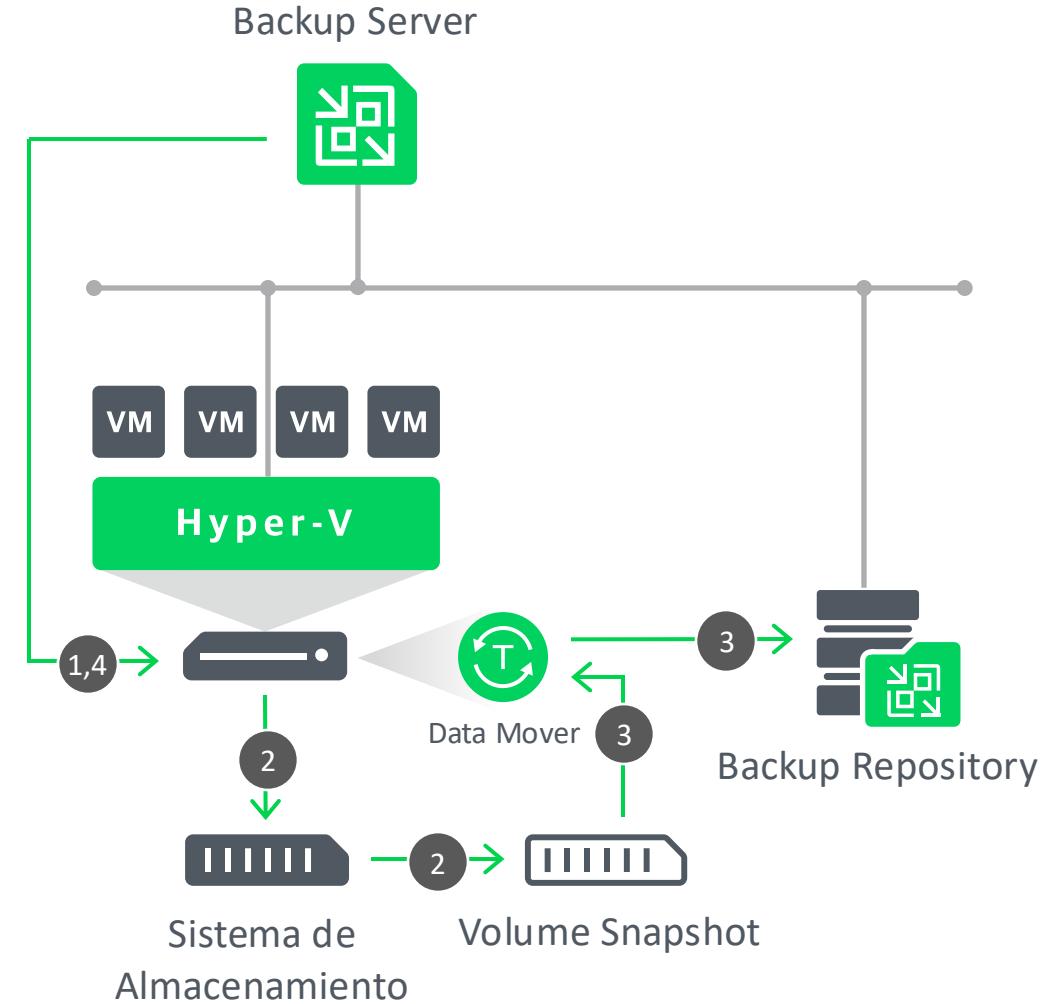
Arquitectura y Componentes Básicos

Hyper-V Modos de Respaldo

On-Host

El procesamiento de los datos de copia de seguridad ocurre en el nodo Hyper-V que aloja las máquinas virtuales, utilizando shadow copies no-transportables, utilizando el proveedor de software VSS.

1. VBR consulta VM y del host de virtualización de Microsoft Hyper-V.
2. VBR indica a Microsoft Hyper-V VSS que cree una copia de la máquina virtual en un momento dado, utilizando un snapshot de volumen o un punto de control de la VM.
3. Veeam Transport Service lee los datos de la máquina virtual desde el snapshot o punto de control y los transfiere al repositorio de copias de seguridad.
4. Después de la transferencia de datos, VBR solicita a Microsoft Hyper-V VSS operaciones de limpieza.



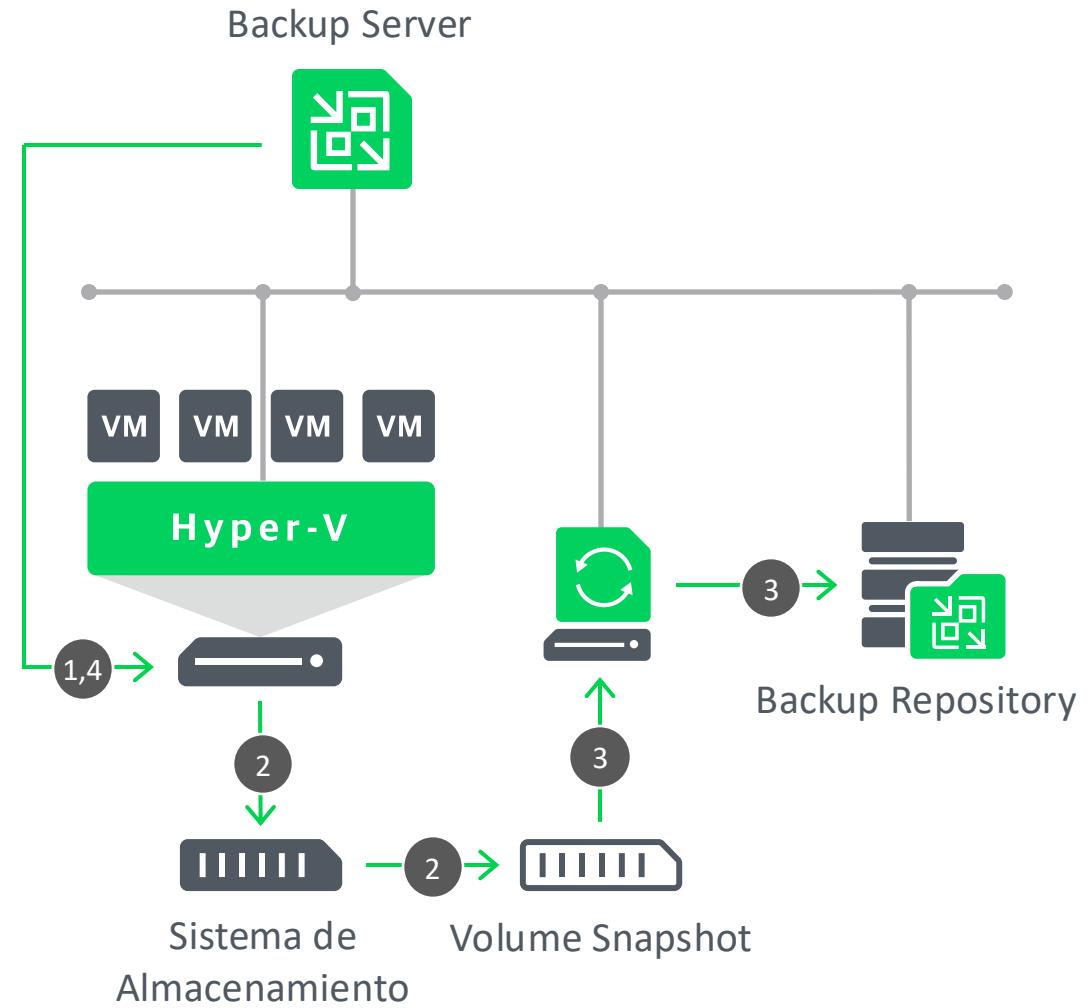
Arquitectura y Componentes Básicos

Hyper-V Modos de Respaldo

Off-Host

El procesamiento de datos para las copias de seguridad se delega en un nodo Hyper-V independiente y no agrupado, utilizando shadow copies a través del proveedor de Hardware VSS ofrecido por el proveedor de almacenamiento SAN.

1. VBR consulta los detalles de la máquina virtual y del host de virtualización de Microsoft Hyper-V.
2. VBR indica a Microsoft Hyper-V VSS que cree una copia puntual de la máquina virtual mediante un snapshot de volumen o un punto de control de la máquina virtual.
3. Veeam Off-host Proxy lee los datos de la VM desde el snapshot o punto de control y los transfiere al repositorio de backup.
4. Despues de la transferencia de datos, VBR solicita a Microsoft Hyper-V VSS que realice operaciones de limpieza.



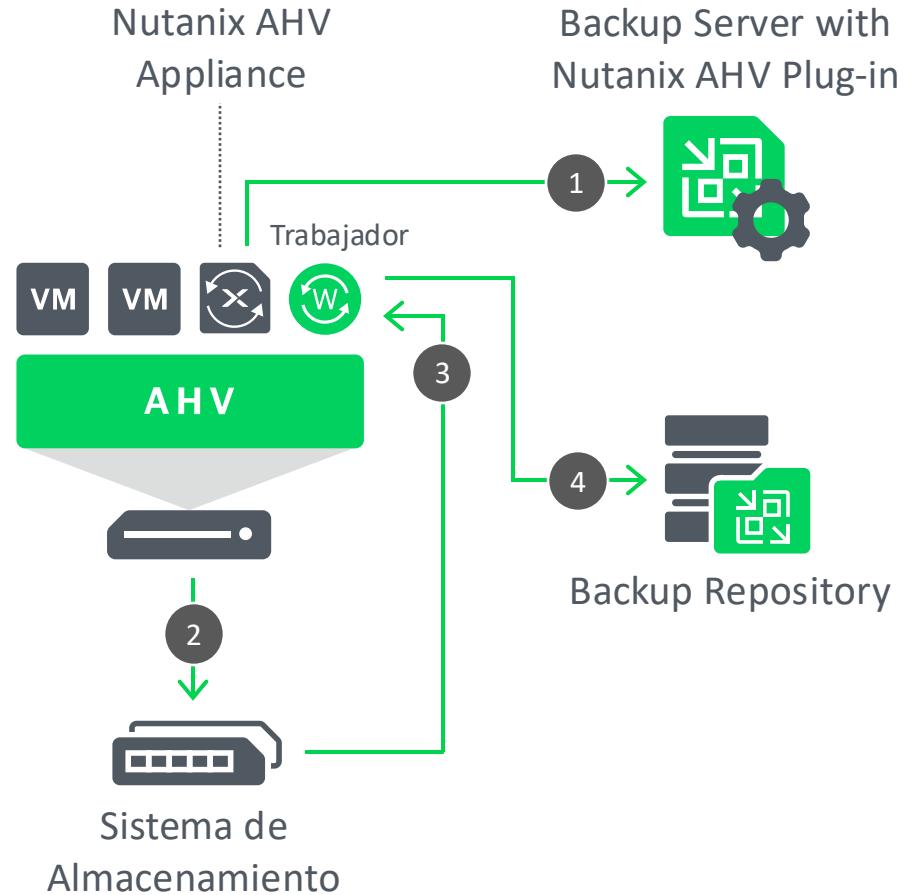
Backup para Nutanix, Red Hat, Oracle Linux, Proxmox VE

Arquitectura y Componentes Básicos

Nutanix AHV

Veeam Backup para Nutanix AHV utiliza las capacidades nativas de Nutanix AHV para crear copias de seguridad a nivel de imagen y no instala software de agente dentro de las máquinas virtuales para recuperar los datos.

1. El backup appliance de Nutanix AHV inicia un trabajo de copia de seguridad, transmitiendo los datos de sesión a VBR.
2. Utilizando la API REST de Nutanix, se vincula con el clúster AHV de Nutanix, generando snapshots para todas las máquinas virtuales o dominios de protección designados. Después establece un grupo de volúmenes en el clúster AHV de Nutanix.
3. El appliance Nutanix AHV despliega un trabajador, montando discos VM en el trabajador a través de iSCSI.
4. El trabajador recupera los datos de la máquina virtual a nivel de bloque, aplicando compresión y deduplicación, y transmite los datos al repositorio de copias de seguridad.

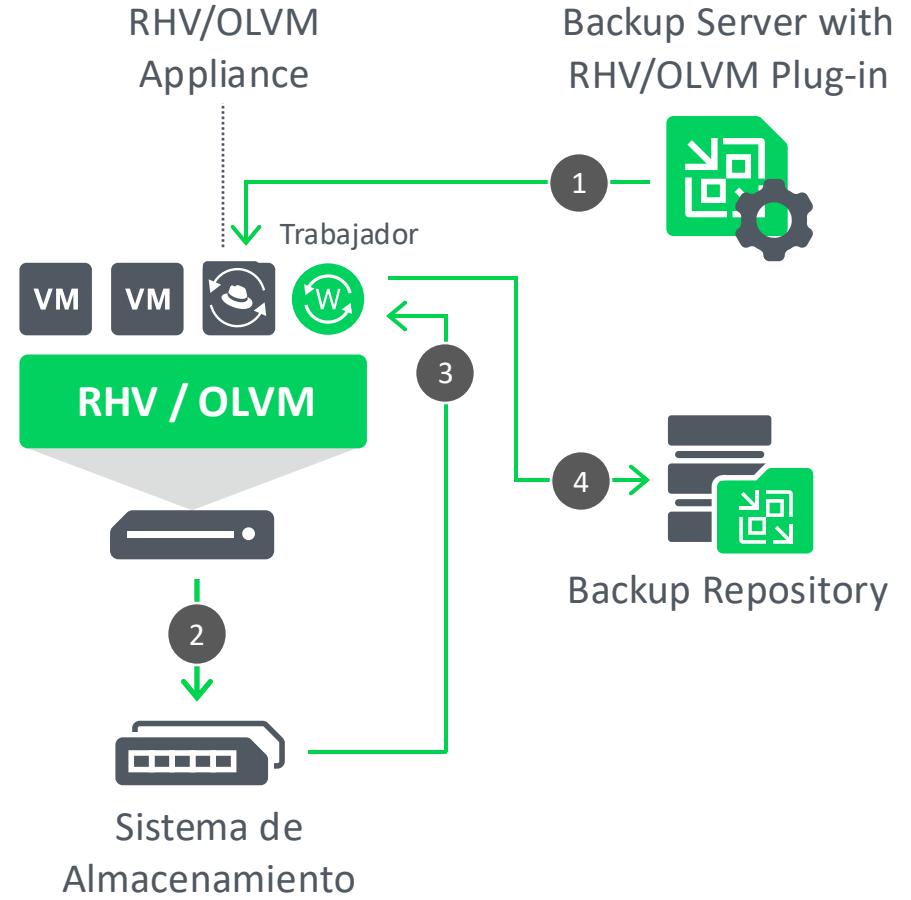


Arquitectura y Componentes Básicos

Red Hat Virtualization & Oracle Linux Virtualization Manager (oVirt)

Veeam Backup para RHV/OLVM utiliza las capacidades nativas de oVirt para crear copias de seguridad a nivel de imagen y no instala software de agente dentro de las máquinas virtuales para recuperar los datos.

1. VBR inicia un trabajo de copia de seguridad, transmitiendo los datos al backup appliance.
2. El backup appliance interactúa con el gestor de virtualización a través de la API REST, generando snapshots para las máquinas virtuales designadas. Posteriormente, establece una sesión de transferencia de imágenes, proporcionando la URL correspondiente.
3. El backup appliance despliega un trabajador, utilizando la URL proporcionada para recuperar los datos de la máquina virtual.
4. El trabajador aplica compresión y deduplicación a los datos de la máquina virtual antes de transmitirlos al repositorio de copia de seguridad designado.

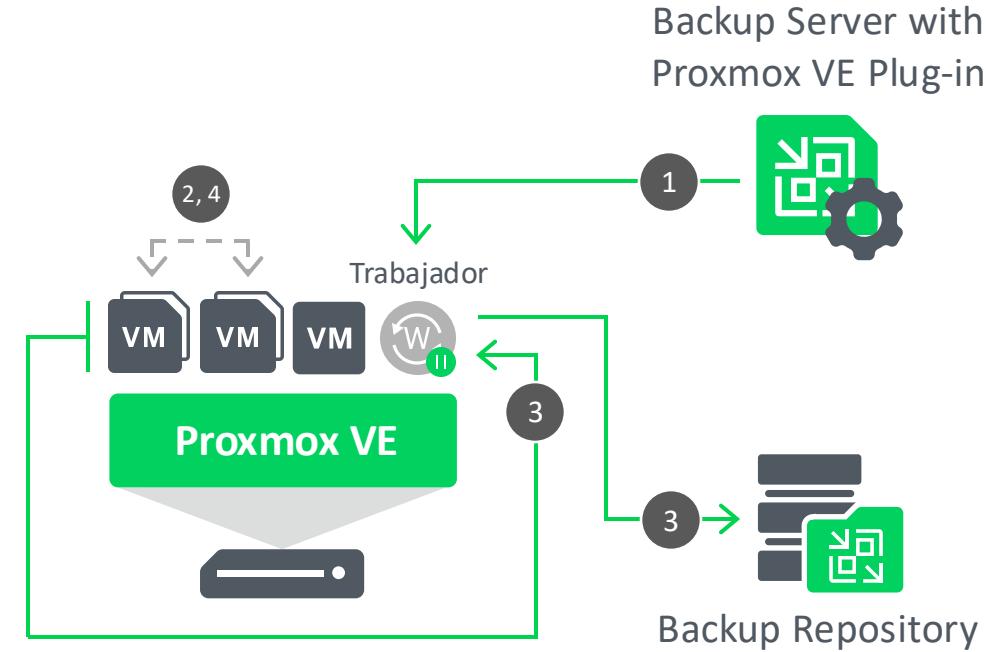


Arquitectura y Componentes Básicos

Proxmox VE

Veeam Backup para Proxmox VE utiliza capacidades nativas para crear copias de seguridad a nivel de imagen y no instala software de agente dentro de las máquinas virtuales para recuperar los datos.

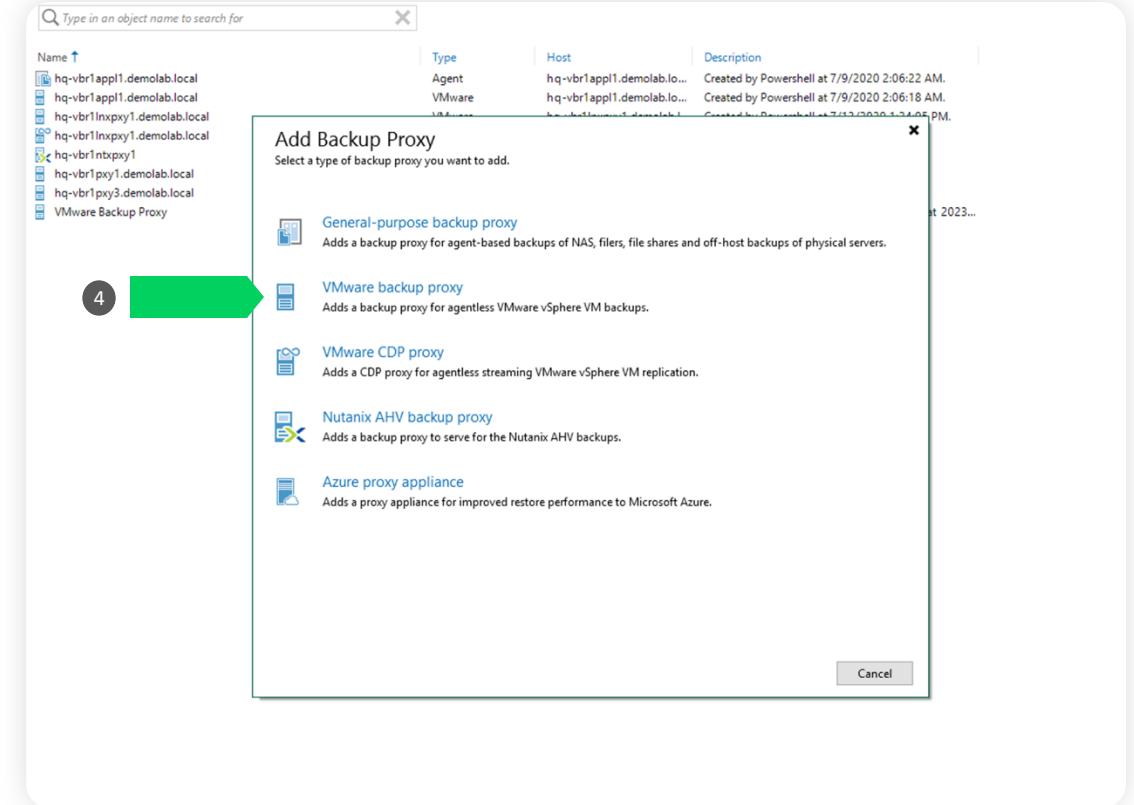
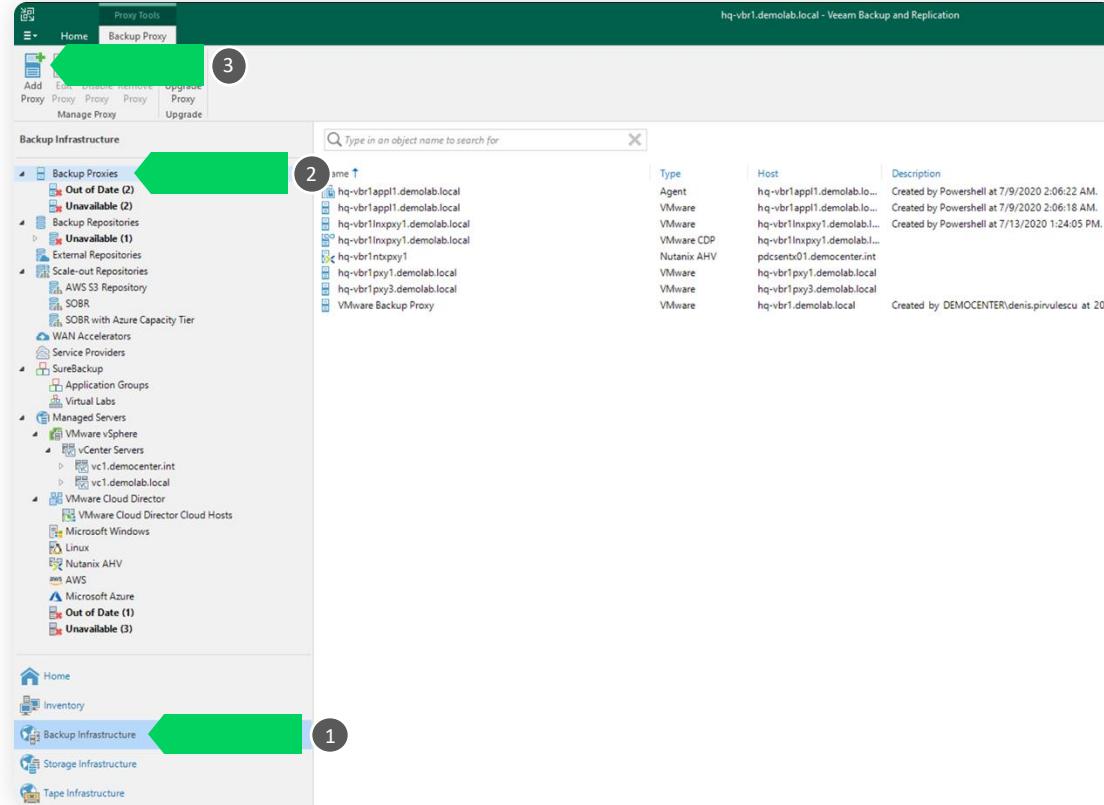
1. Lanza un trabajador en el host donde se encuentra la máquina virtual. Si no hay ninguno desplegado allí, Veeam Backup para Proxmox VE utiliza un trabajador de otro host conectado.
2. Se conecta al servidor Proxmox VE y crea un snapshot de copia en escritura de la máquina virtual procesada.
3. El trabajador lee los datos de los discos de la máquina virtual, los compara con la snapshot creada en el paso 2, excluye los cambios y transfiere la data al repositorio de destino en el formato nativo de Veeam.
4. Elimina la snapshot creada y suspende el trabajador cuando finaliza la sesión de copia de seguridad.



Cómo añadir un Backup Proxy

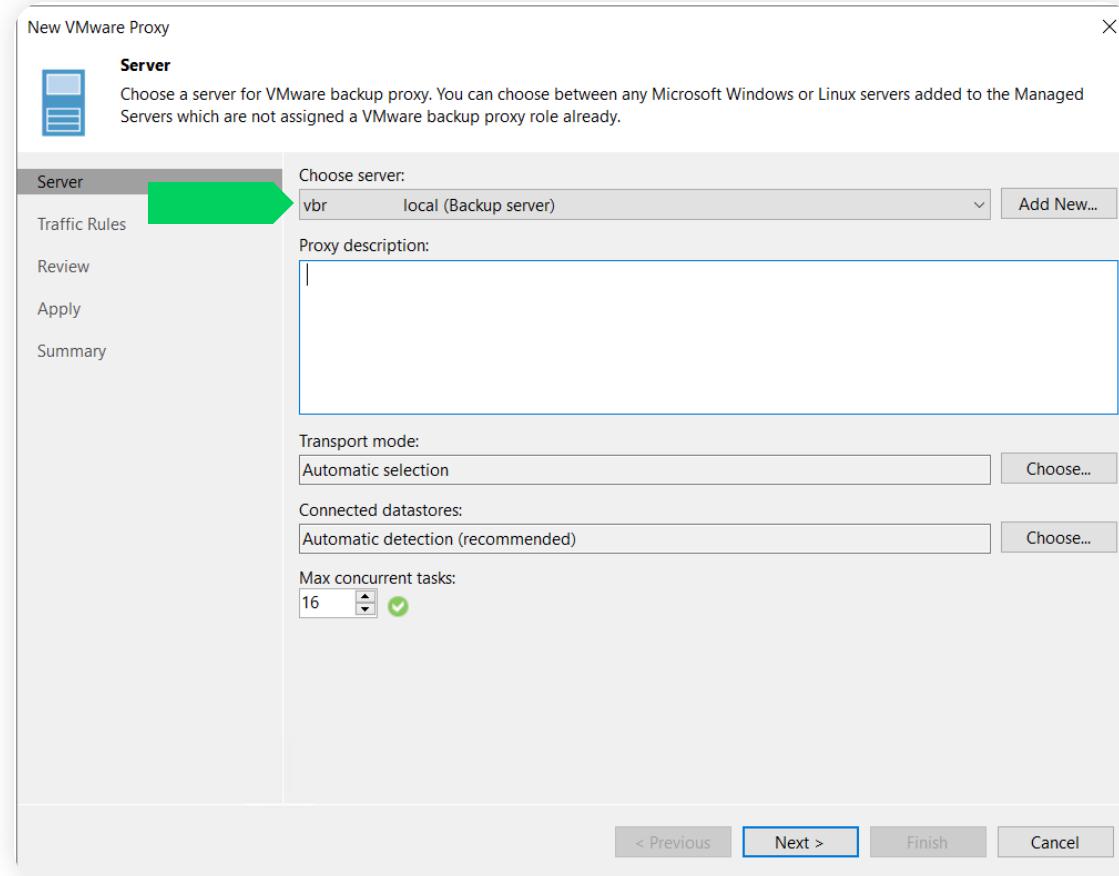
Arquitectura y Componentes Básicos

Cómo añadir un Backup Proxy? Ejemplo VMware.



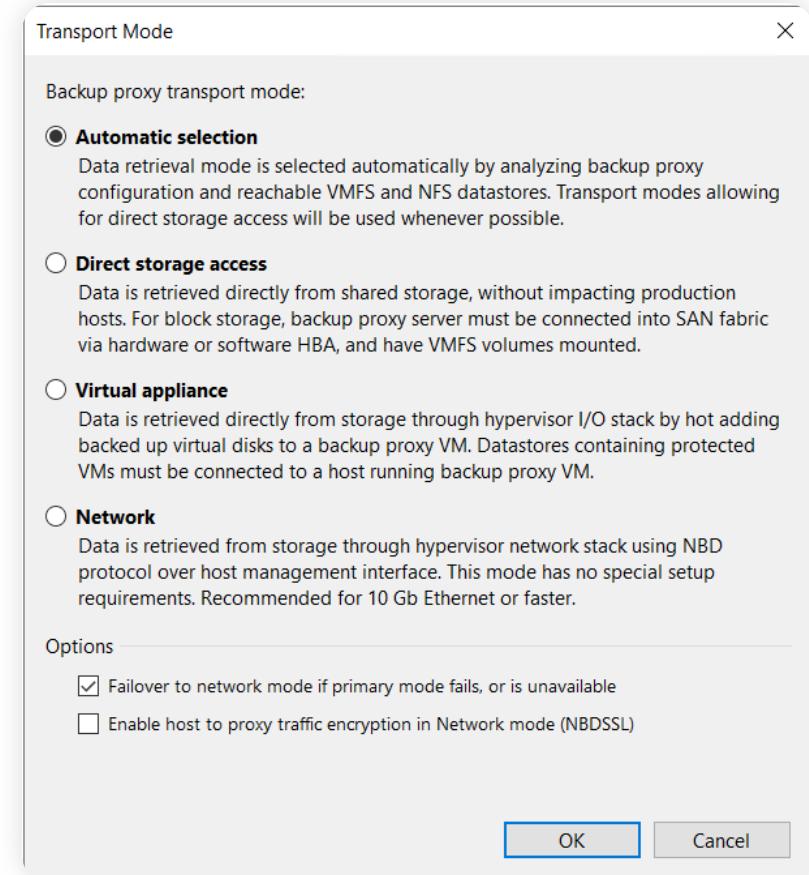
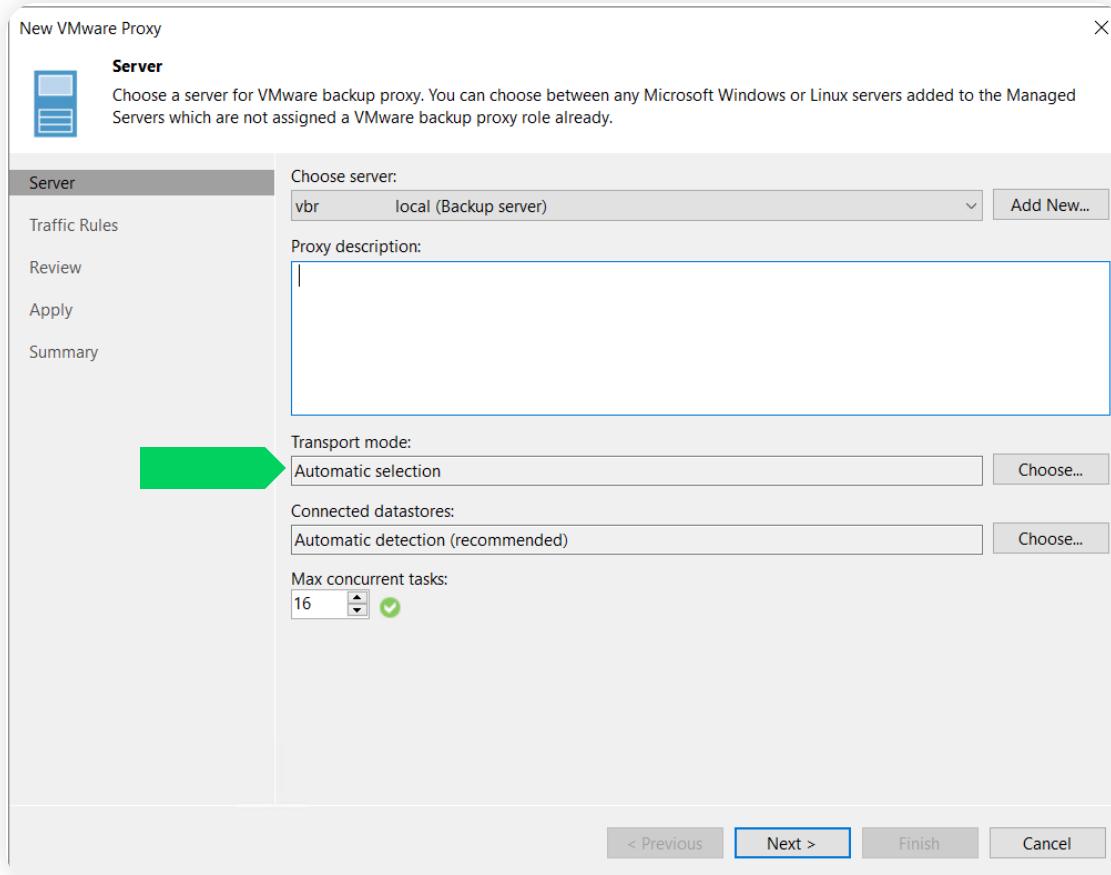
Arquitectura y Componentes Básicos

Cómo añadir un Backup Proxy? Ejemplo VMware.



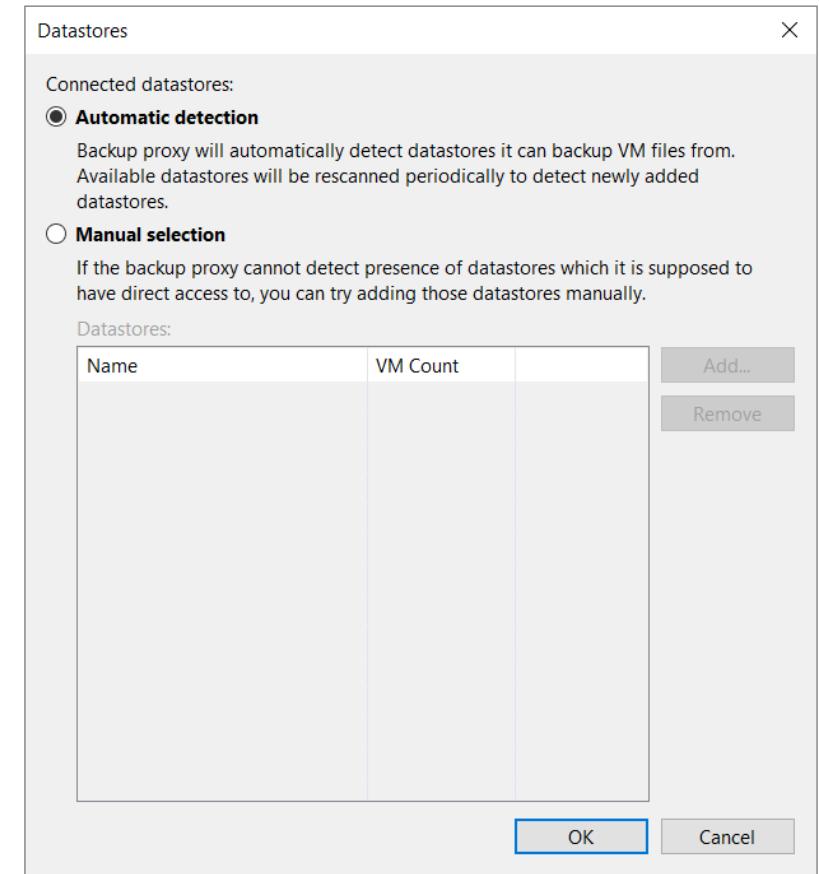
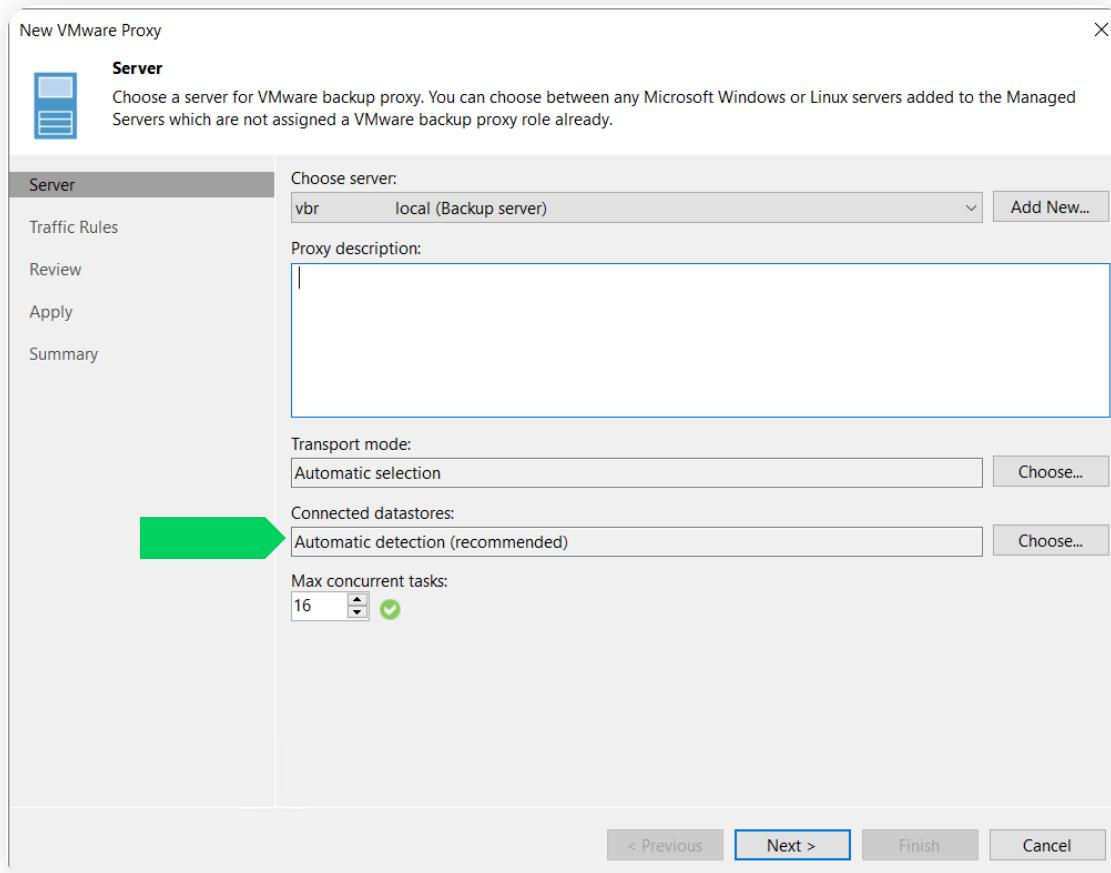
Arquitectura y Componentes Básicos

Cómo añadir un Backup Proxy? Ejemplo VMware.



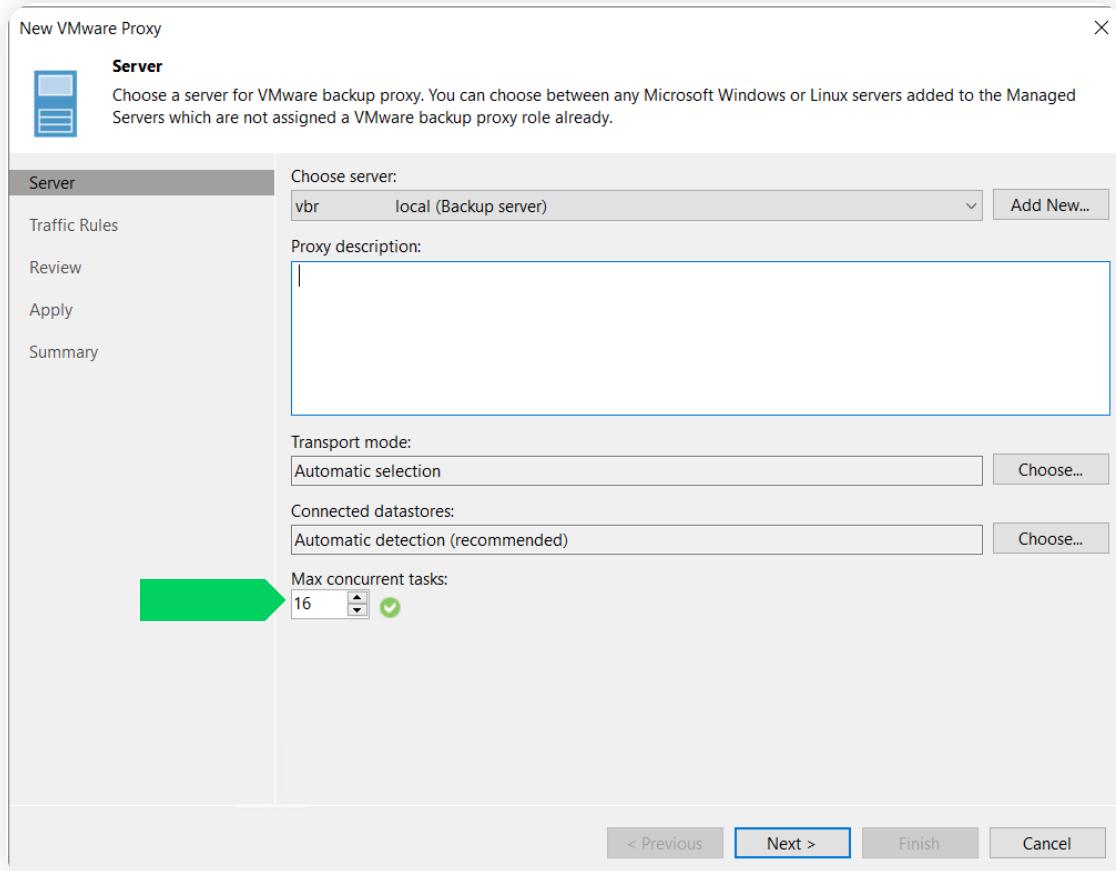
Arquitectura y Componentes Básicos

Cómo añadir un Backup Proxy? Ejemplo VMware.



Arquitectura y Componentes Básicos

Cómo añadir un Backup Proxy? Ejemplo VMware.



Veeam Backup & Replication crea un task por cada disco VM.

El número recomendado de tasks simultáneas se calcula automáticamente en función de los recursos disponibles: 1 CPU Core = 2 tasks concurrentes.

La mejor práctica es reservar 2 CPU y 2 GB de RAM para las necesidades del sistema operativo.

Así, para una CPU de 4 núcleos, se recomienda configurar 4 tasks concurrentes ($(4 \text{ CPUs} - 2 \text{ CPUs}) \times 2 = 4$), para una CPU de 8 núcleos - 12 tasks concurrentes ($(8 \text{ CPUs} - 2 \text{ CPUs}) \times 2 = 12$).

Backup Repository

Arquitectura y Componentes Básicos

Backup Repository

Un repositorio es una ubicación de almacenamiento donde se guardan los archivos de copia de seguridad, las copias de los datos de las máquinas virtuales y los metadatos necesarios para la restauración.

El repositorio puede ser una ubicación local o remota, y sirve como espacio de almacenamiento centralizado para los datos de copia de seguridad y replicación.

Almacenamiento Directo

- Microsoft Windows server
- Linux server
- Repositorio Reforzado (Linux)

Network Attached Storage

- SMB (CIFS) share
- NFS share

Deduplicating Storage Appliances

- Dell Data Domain
- ExaGrid
- Fujitsu ETERNUS CS800
- HPE StoreOnce
- Infinidat InfiniGuard
- Quantum DxI

Almacenamiento de objetos

- S3 Compatible
- Amazon S3
- Google Cloud Storage
- IBM Cloud Object Storage
- Microsoft Azure Storage
- Wasabi Cloud Storage

Arquitectura y Componentes Básicos

Backup Repository

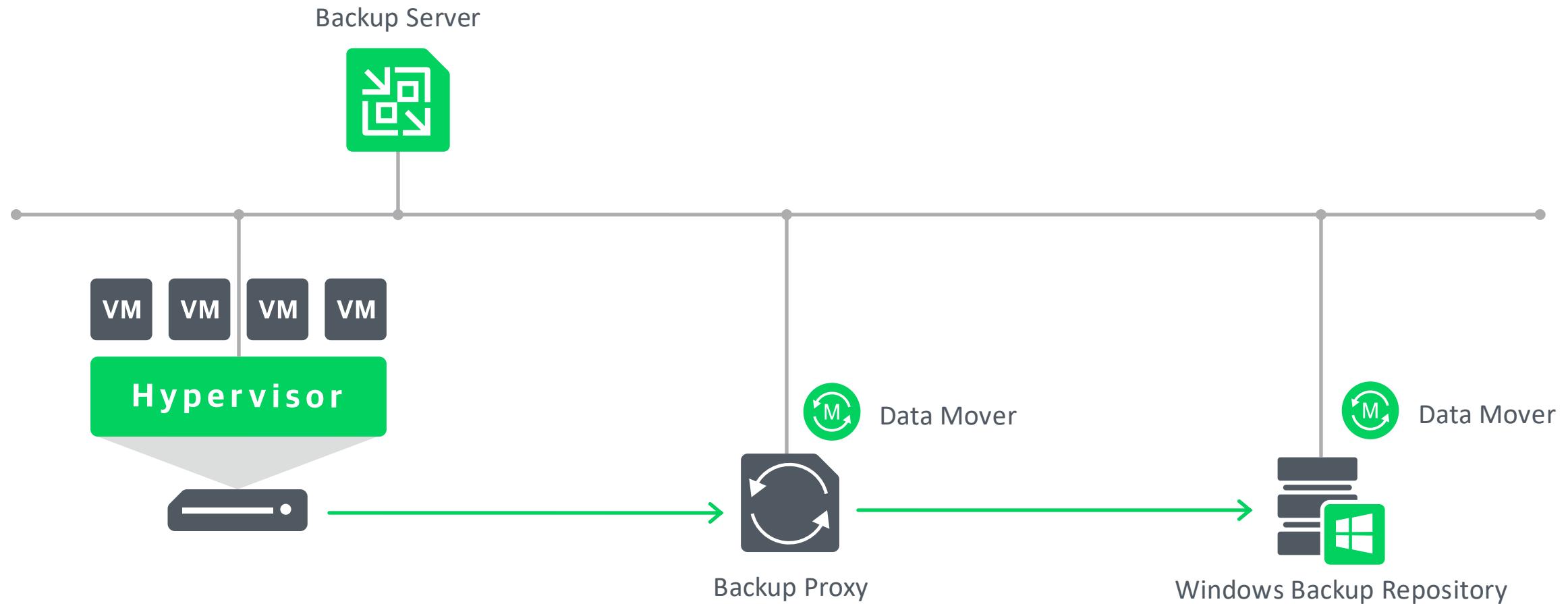
Hay muchos tipos de archivos que puedes encontrar en el repositorio de copias de seguridad. Aquí está la lista de los más utilizados:

- .vbm** – backup chain metadata file
- .vbk** – full backup file
- .vib** – incremental backup file
- .vrh** – reverse incremental backup file
- .bco** – Respaldo de configuración. file
- .vsb** – virtual full backup for tapes
- .vlb** – archived log backup file
- .vsm** – Microsoft SQL transaction log backup
- .vom** – Oracle database log file
- .vpm** – PostgreSQL transaction log backup

- .vab** – enterprise plug-ins backup file
- .vasm** – enterprise plug-ins backup metadata file
- .vacm** – enterprise plug-ins backup job metadata file
- .vblob** – file that stores data from the file share (NAS) backup job
- .vindex** – binary metadata file that describes backup files (names and versions) of file share backup job
- .vslice** – binary metadata that describes allocation of data in VLOB backup files

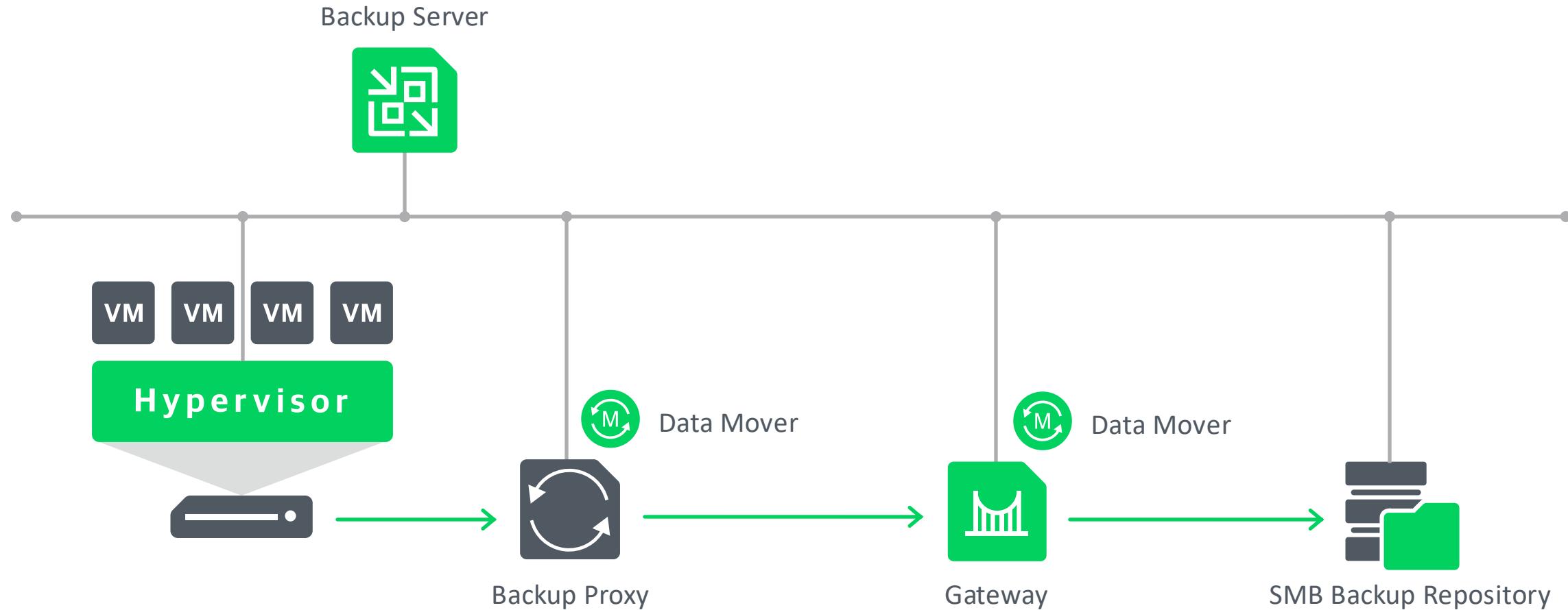
Arquitectura y Componentes Básicos

Ejemplo de Repositorio de Copias de Seguridad de Windows



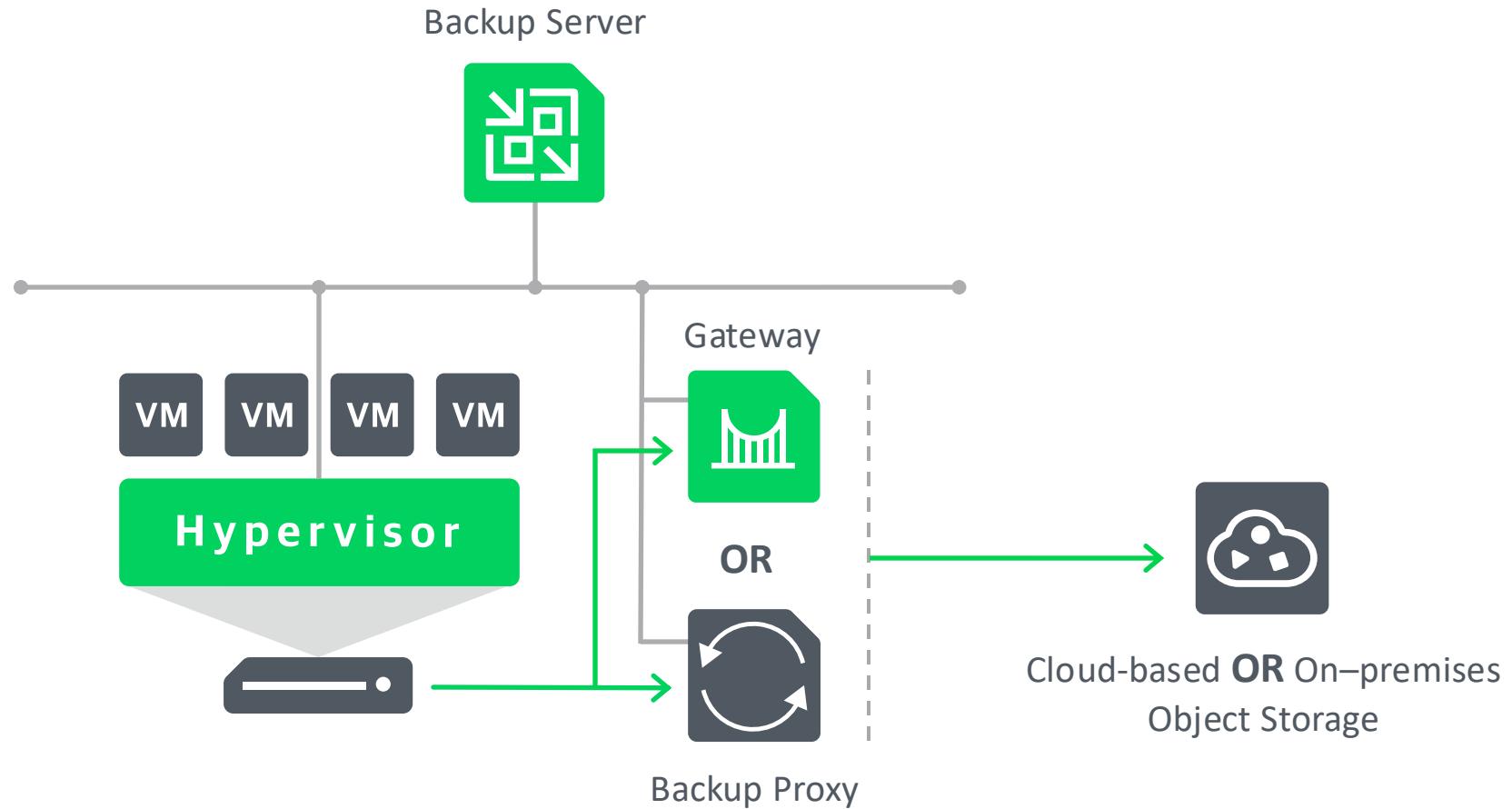
Arquitectura y Componentes Básicos

Ejemplo de Repositorio de Copias de Seguridad SMB



Arquitectura y Componentes Básicos

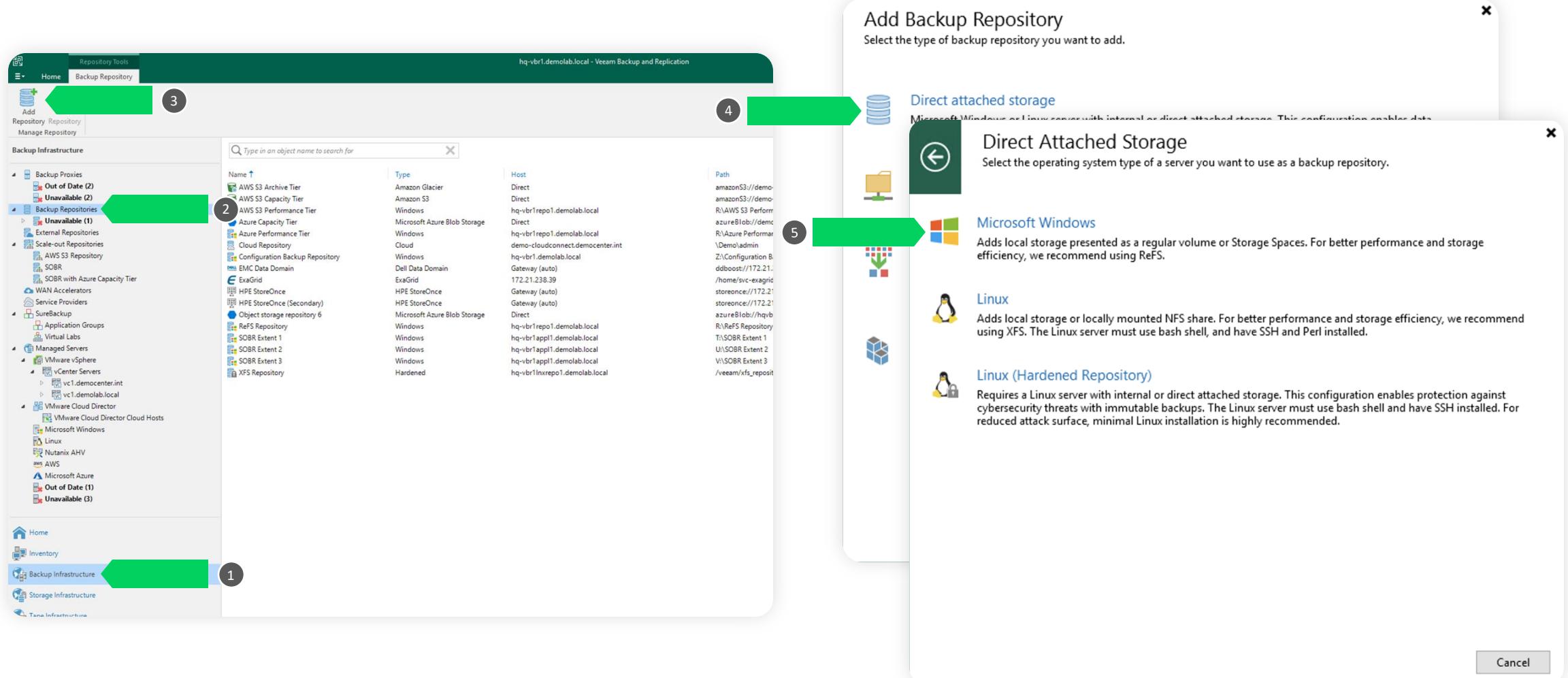
Ejemplo de Repositorio de Almacenamiento de Objetos



Cómo añadir un Repositorio de Copias de Seguridad

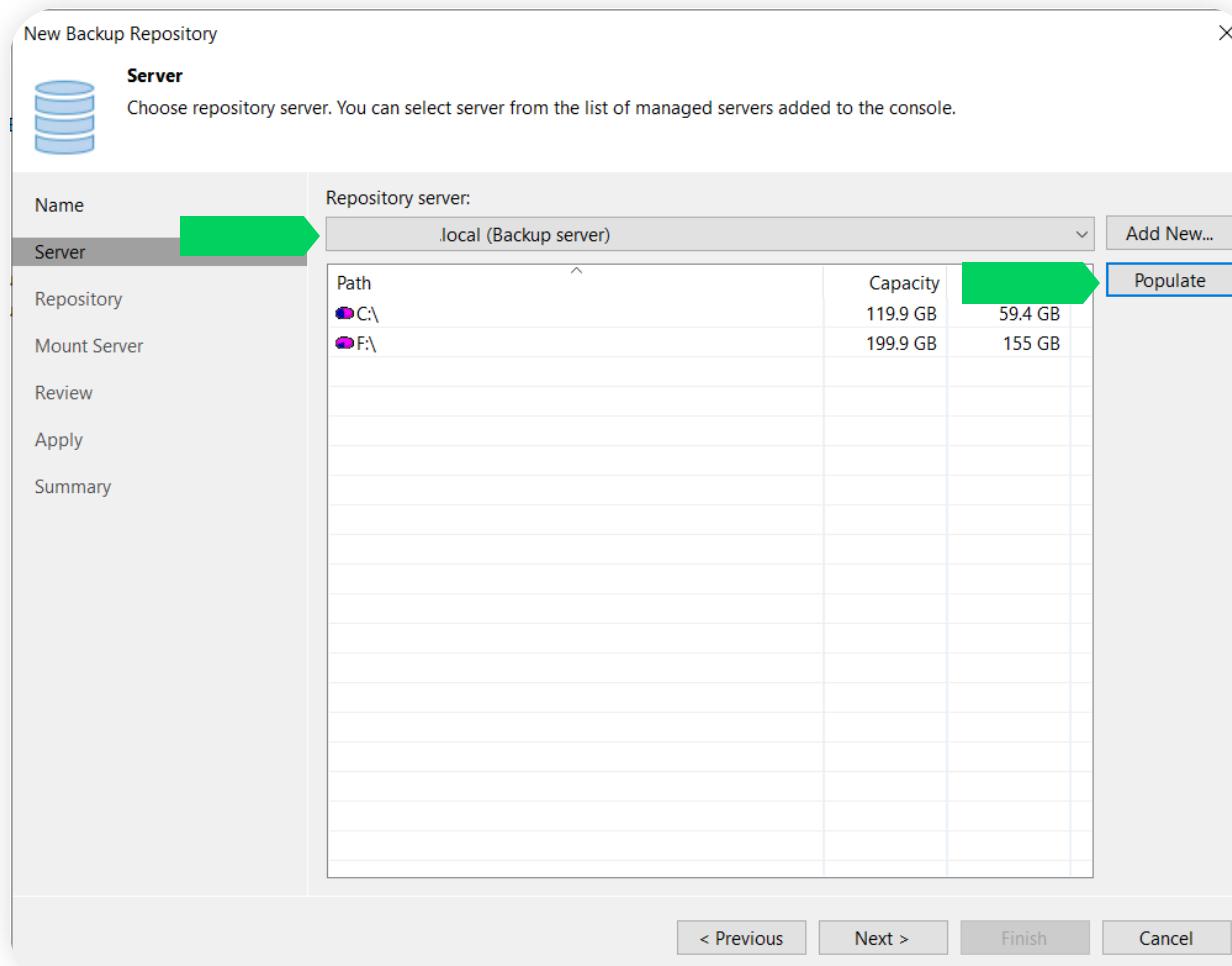
Arquitectura y Componentes Básicos

¿Cómo añadir un repositorio? Ejemplo de Direct Attached Storage.



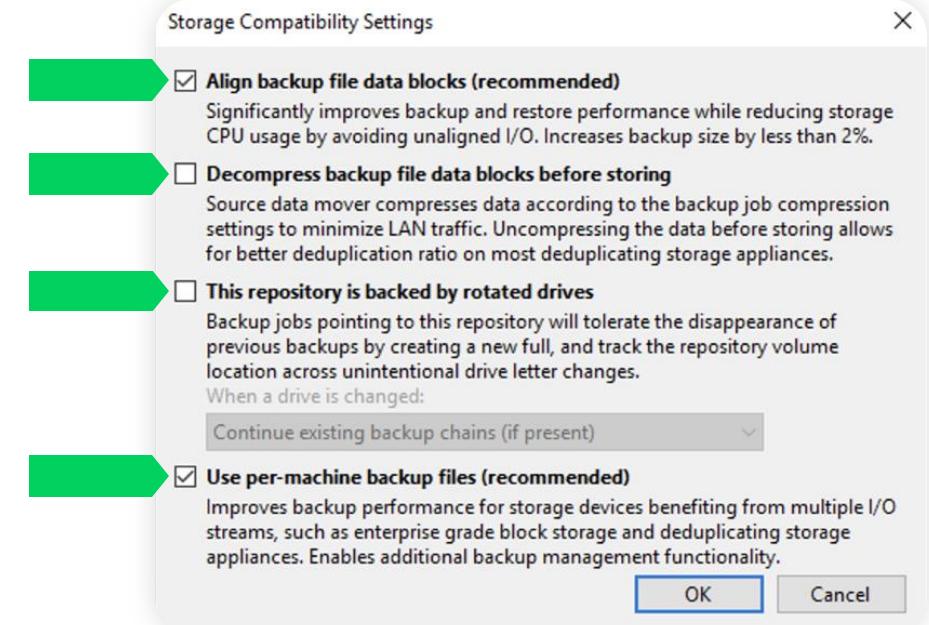
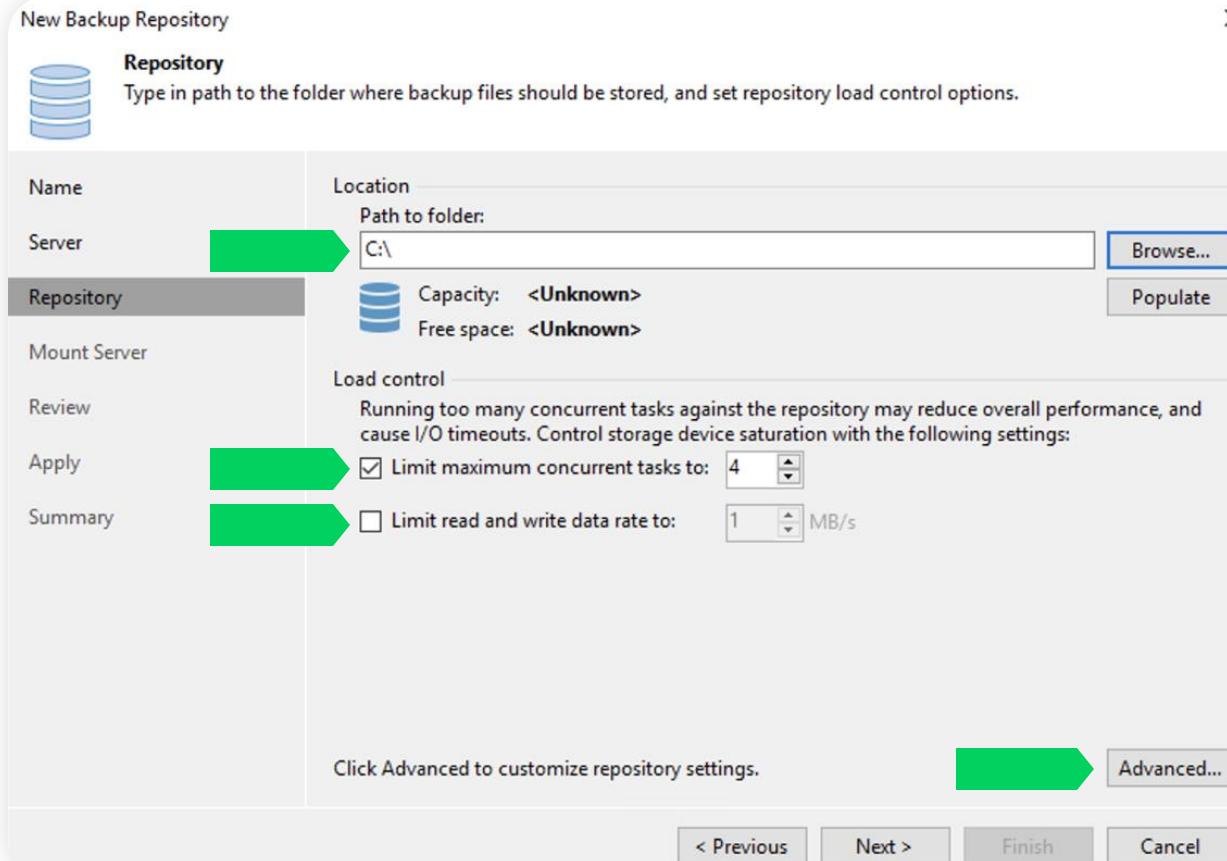
Architecture & Core Components

¿Cómo añadir un repositorio? Ejemplo de Direct Attached Storage.



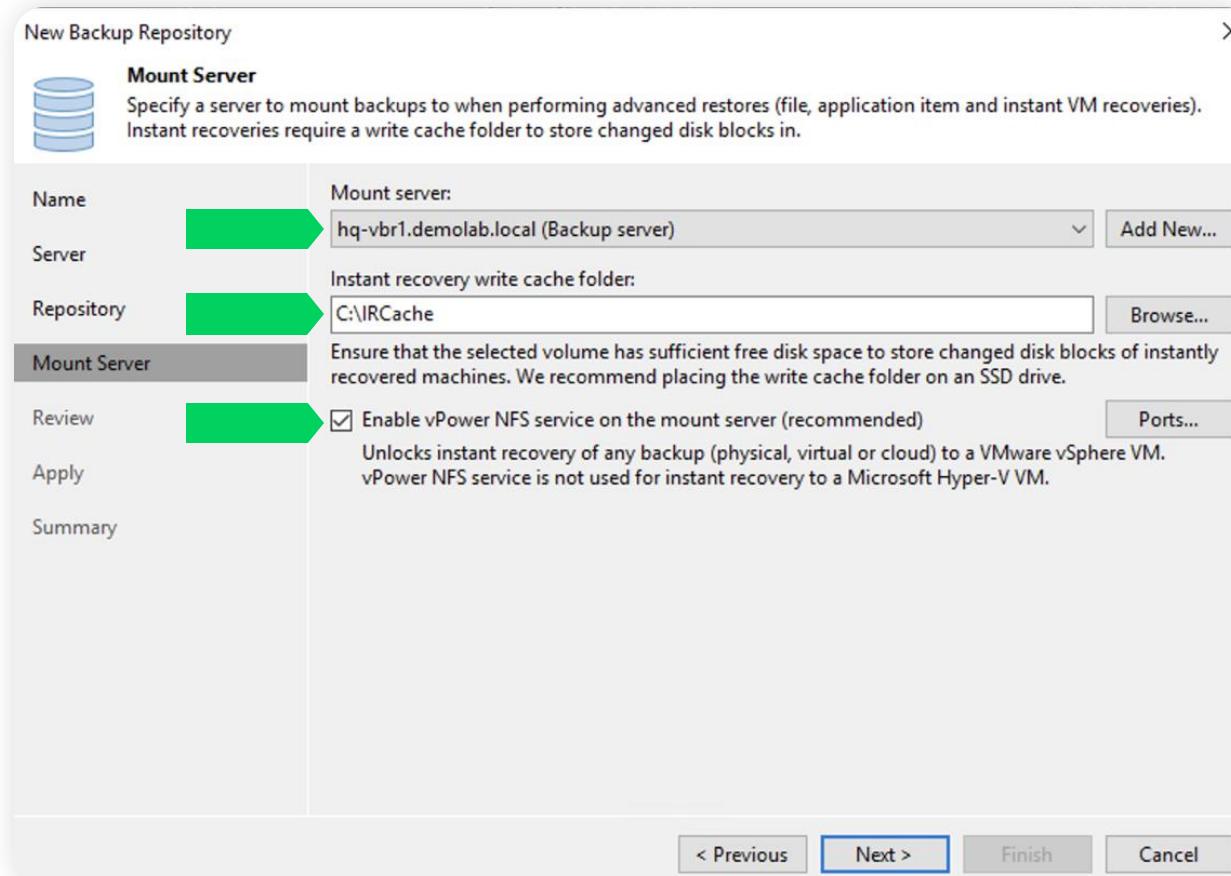
Architecture & Core Components

¿Cómo añadir un repositorio? Ejemplo de Direct Attached Storage.



Architecture & Core Components

¿Cómo añadir un repositorio? Ejemplo de Direct Attached Storage.



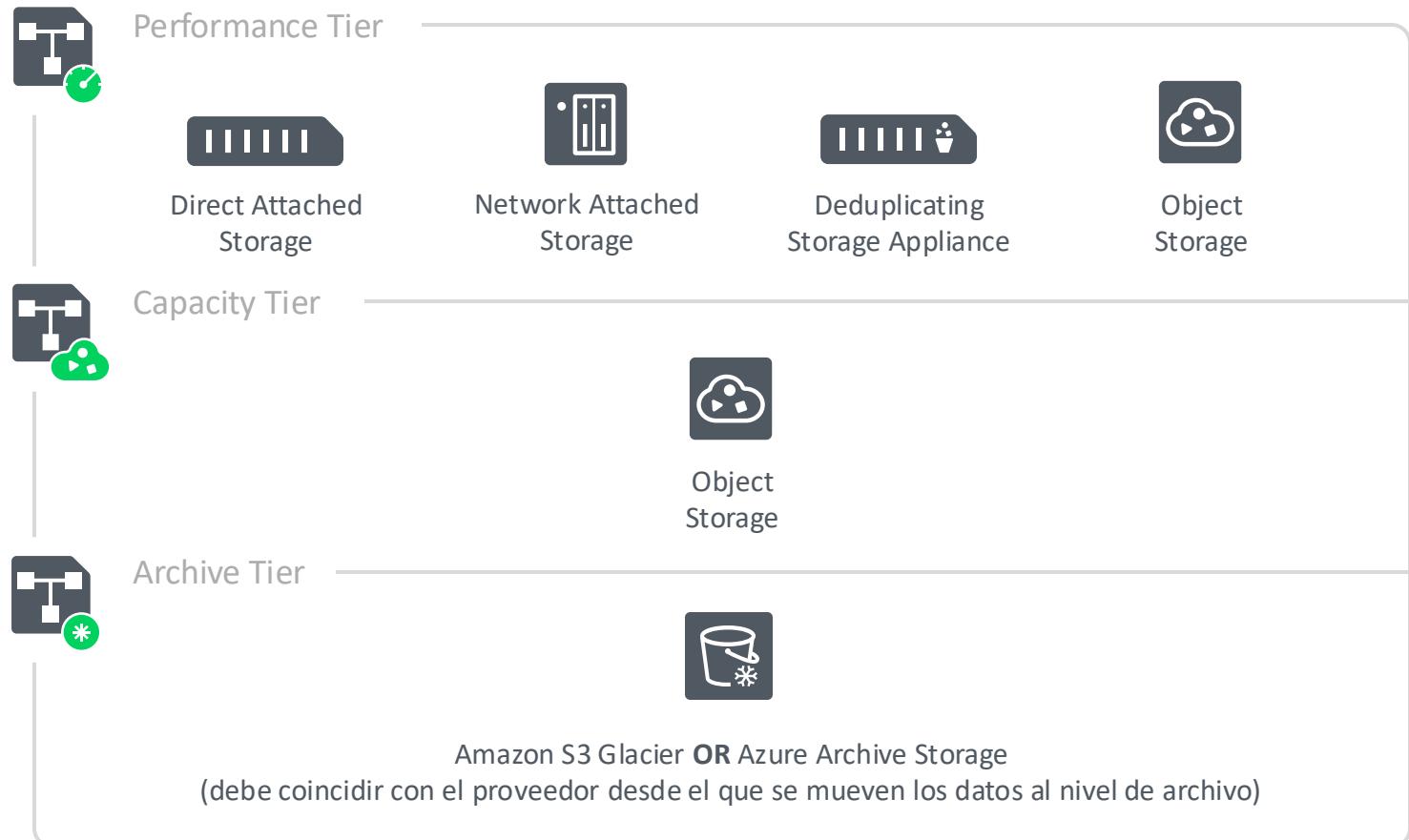
Scale-Out Backup Repository

Arquitectura y Componentes Básicos

Scale-Out Backup Repository

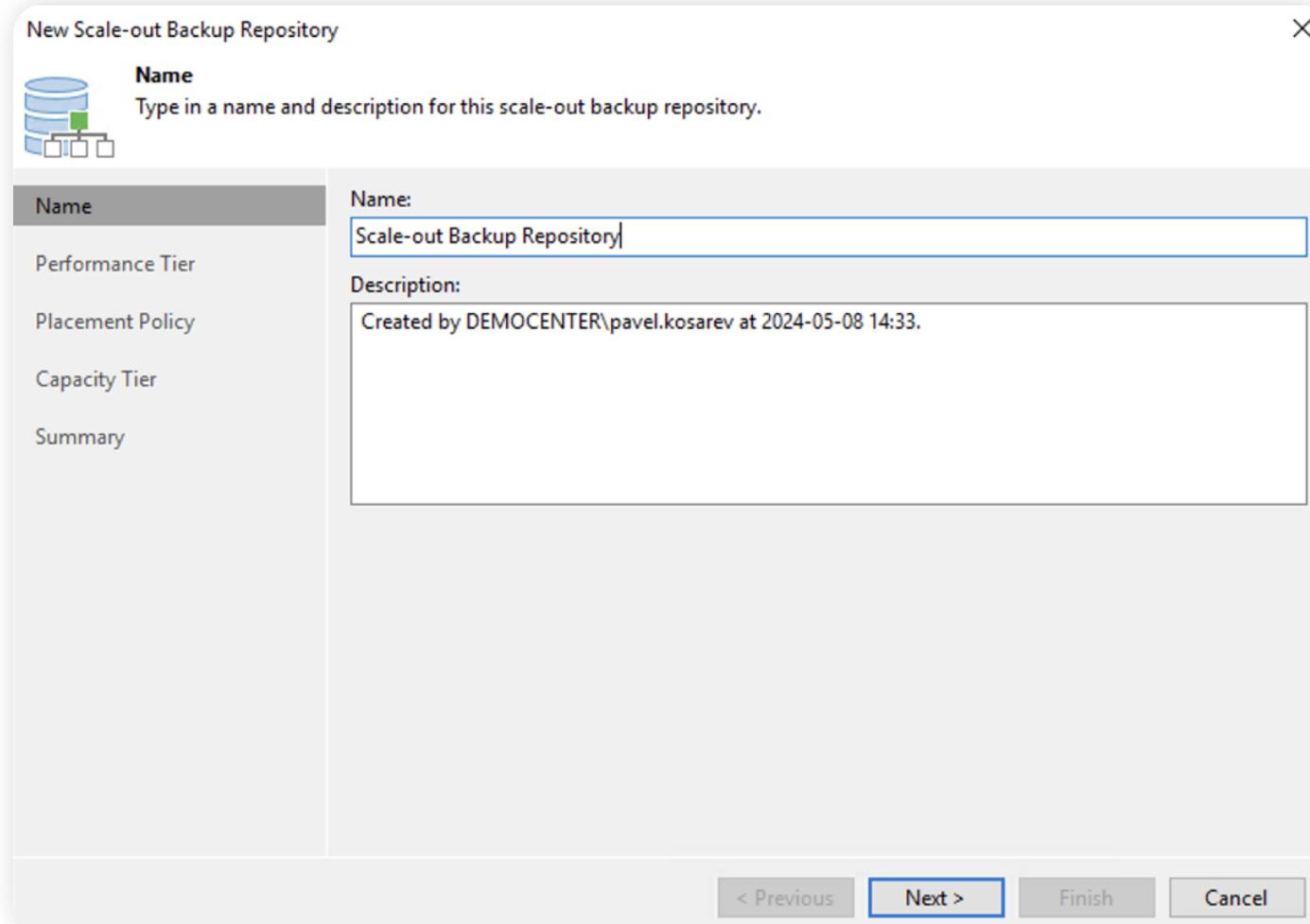
Un sistema de repositorio escalable con soporte de almacenamiento **multinivel**.

Incluye un nivel de **performance** (almacenamiento local o compartido) y puede ampliarse con niveles de **capacidad** y **archivado**, lo que proporciona un escalado horizontal para diversas necesidades de almacenamiento.



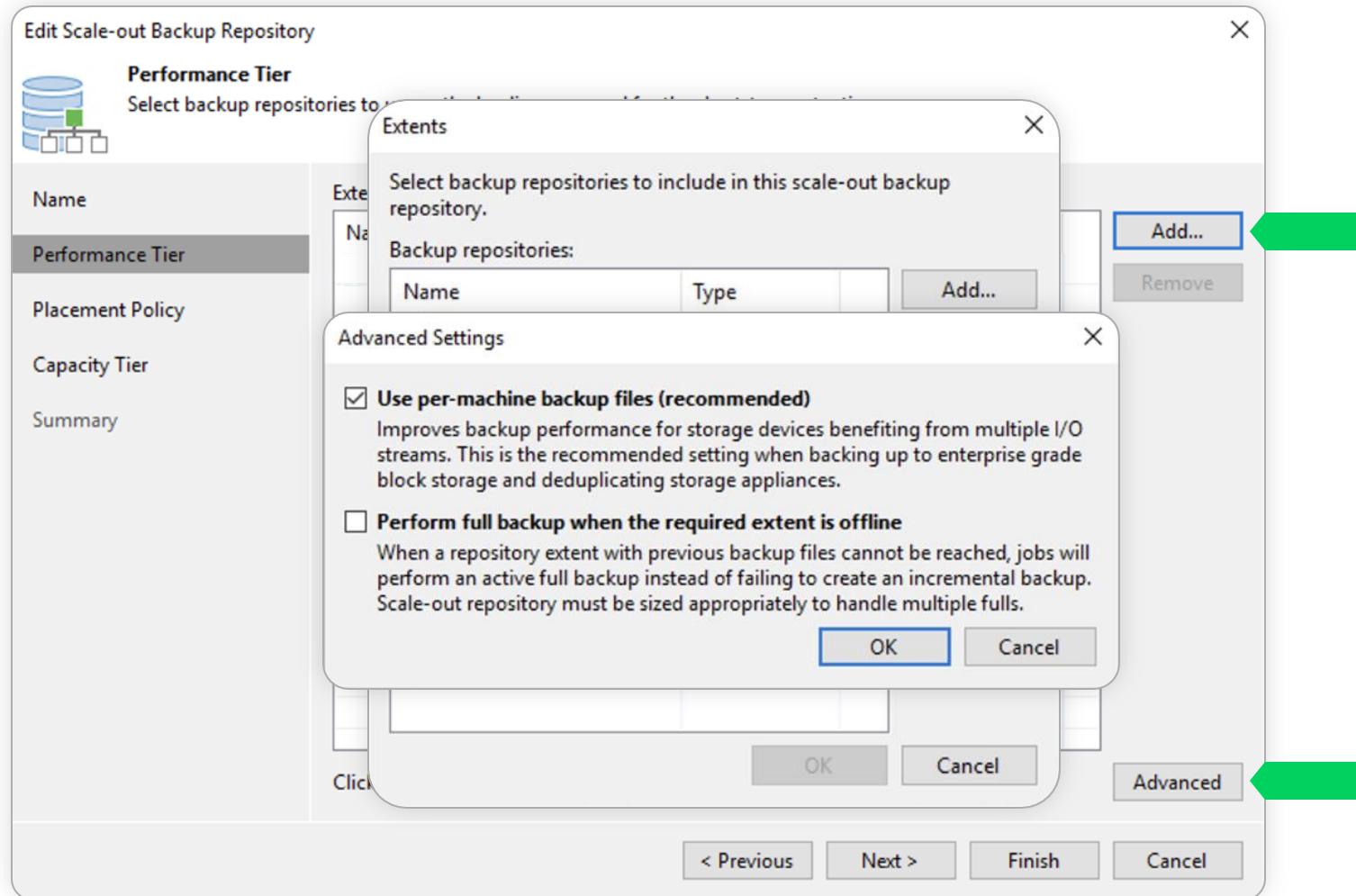
Arquitectura y Componentes Básicos

¿Cómo añadir/configurar el repositorio de copias de seguridad Scale-Out?



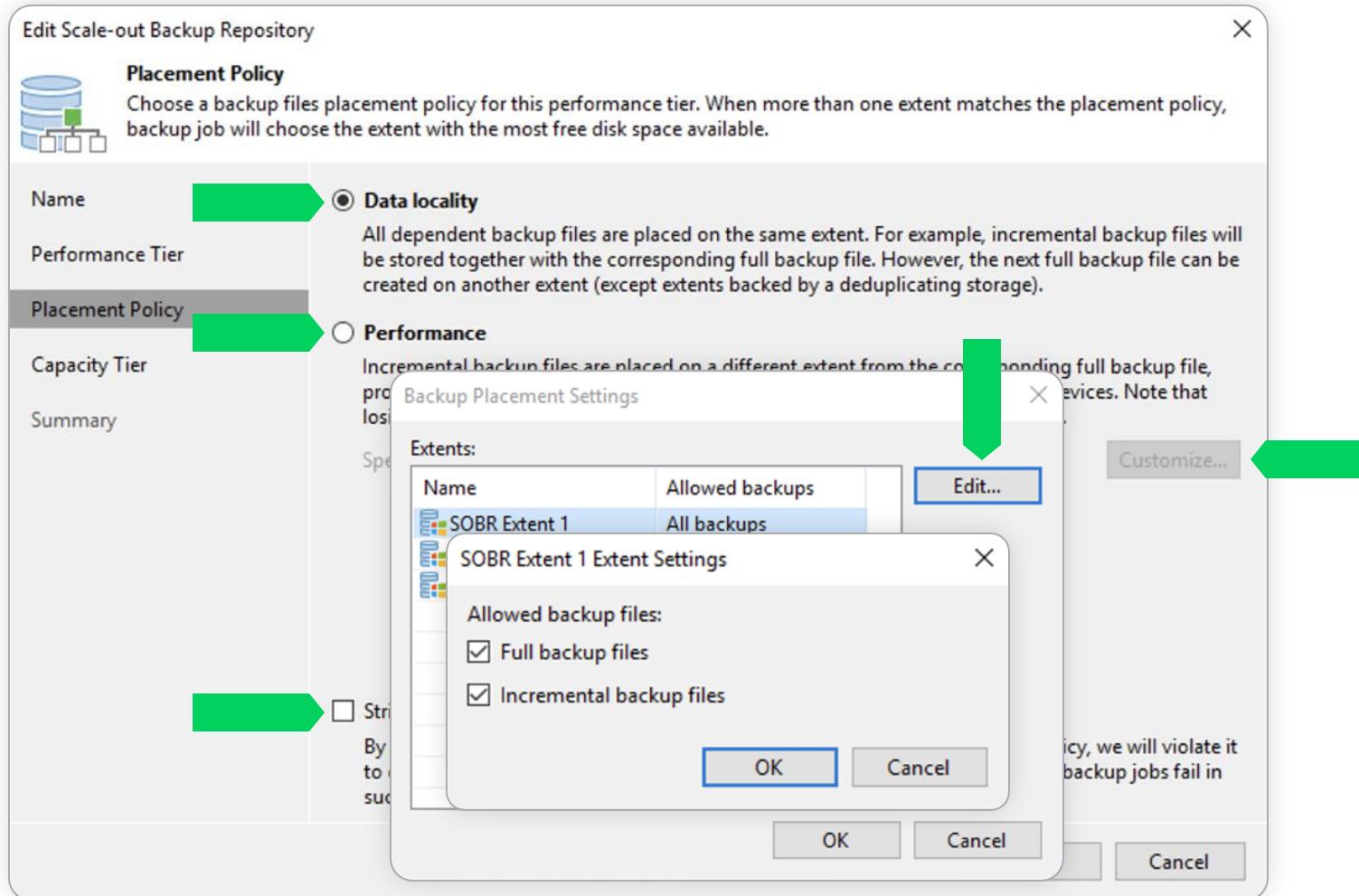
Arquitectura y Componentes Básicos

¿Cómo añadir/configurar el repositorio de copias de seguridad Scale-Out?



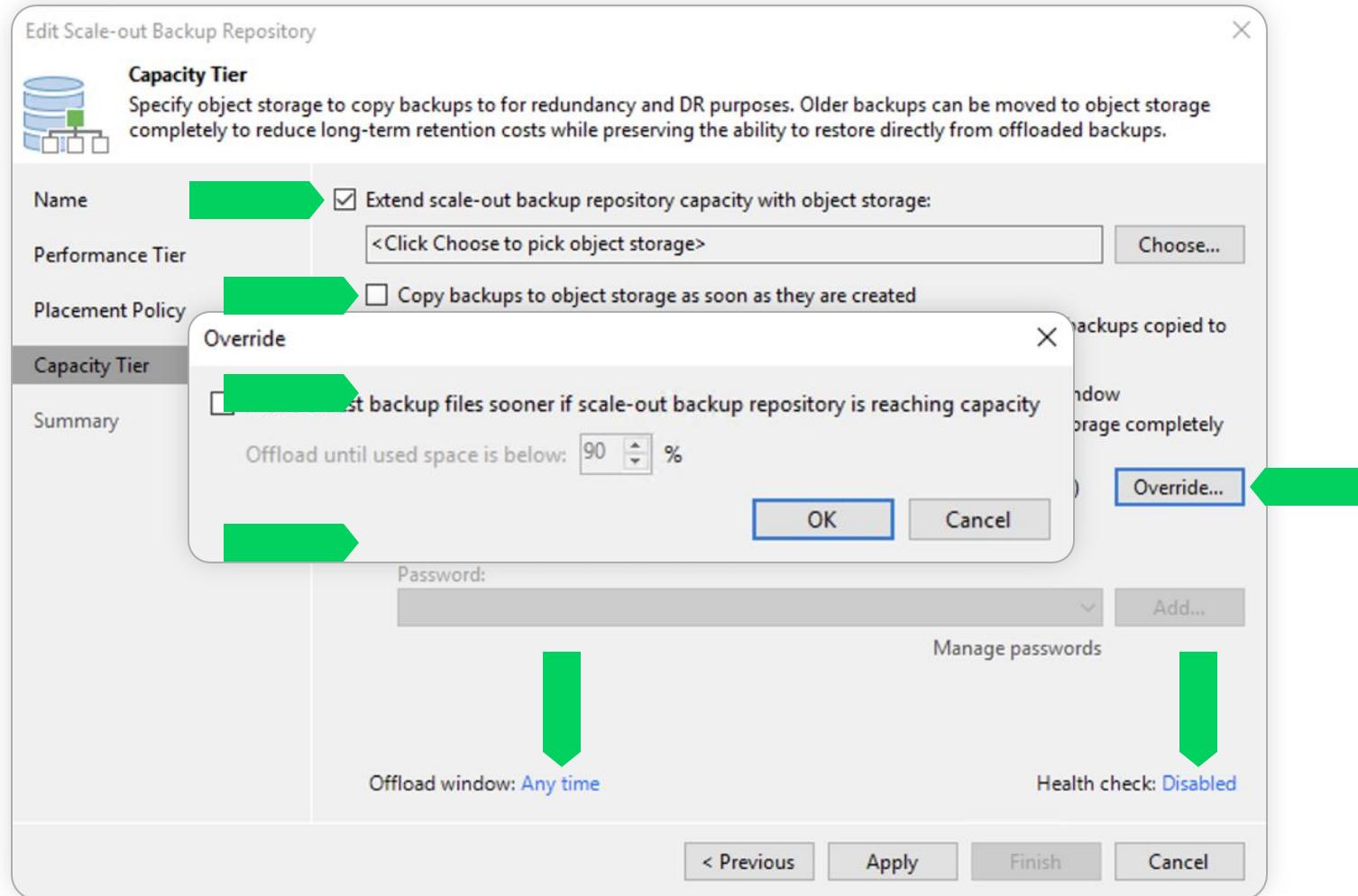
Arquitectura y Componentes Básicos

¿Cómo añadir/configurar el repositorio de copias de seguridad Scale-Out?



Arquitectura y Componentes Básicos

¿Cómo añadir/configurar el repositorio de copias de seguridad Scale-Out?



SureBackup, SureReplica & Virtual Lab

Funciones Avanzadas

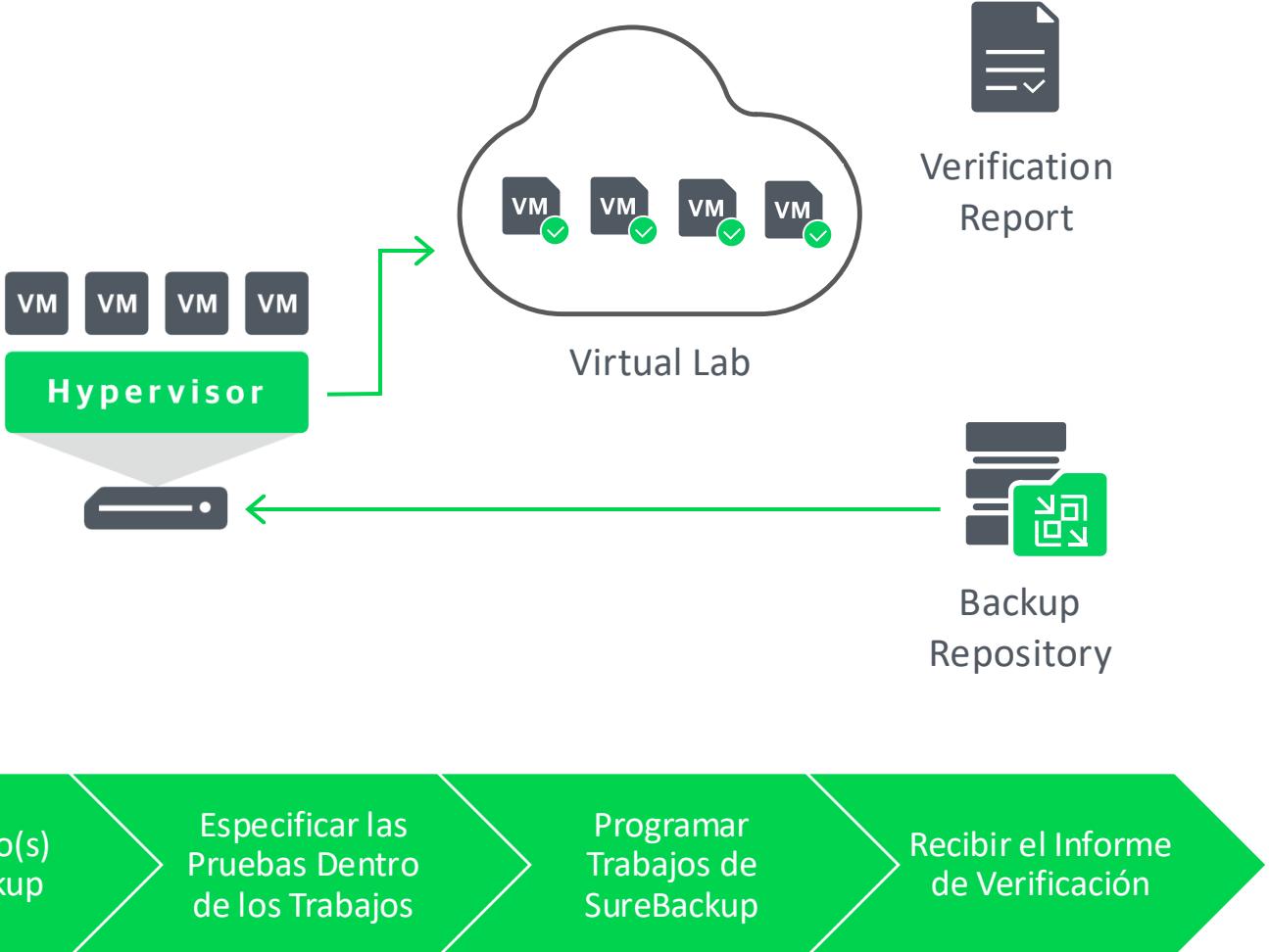
SureBackup, SureReplica & On-Demand Sandbox

SureBackup

Permite realizar automáticamente pruebas de recuperabilidad, verificación y análisis de contenido de las copias de seguridad realizadas correctamente.

¿Cómo?

1. Inicia las máquinas virtuales en un entorno de laboratorio virtual aislado.
2. Realiza un conjunto de pruebas.
3. Envía un informe de estado a su buzón de correo electrónico.



Funciones Avanzadas

SureBackup Modos de Verificación

Full Recoverability Testing

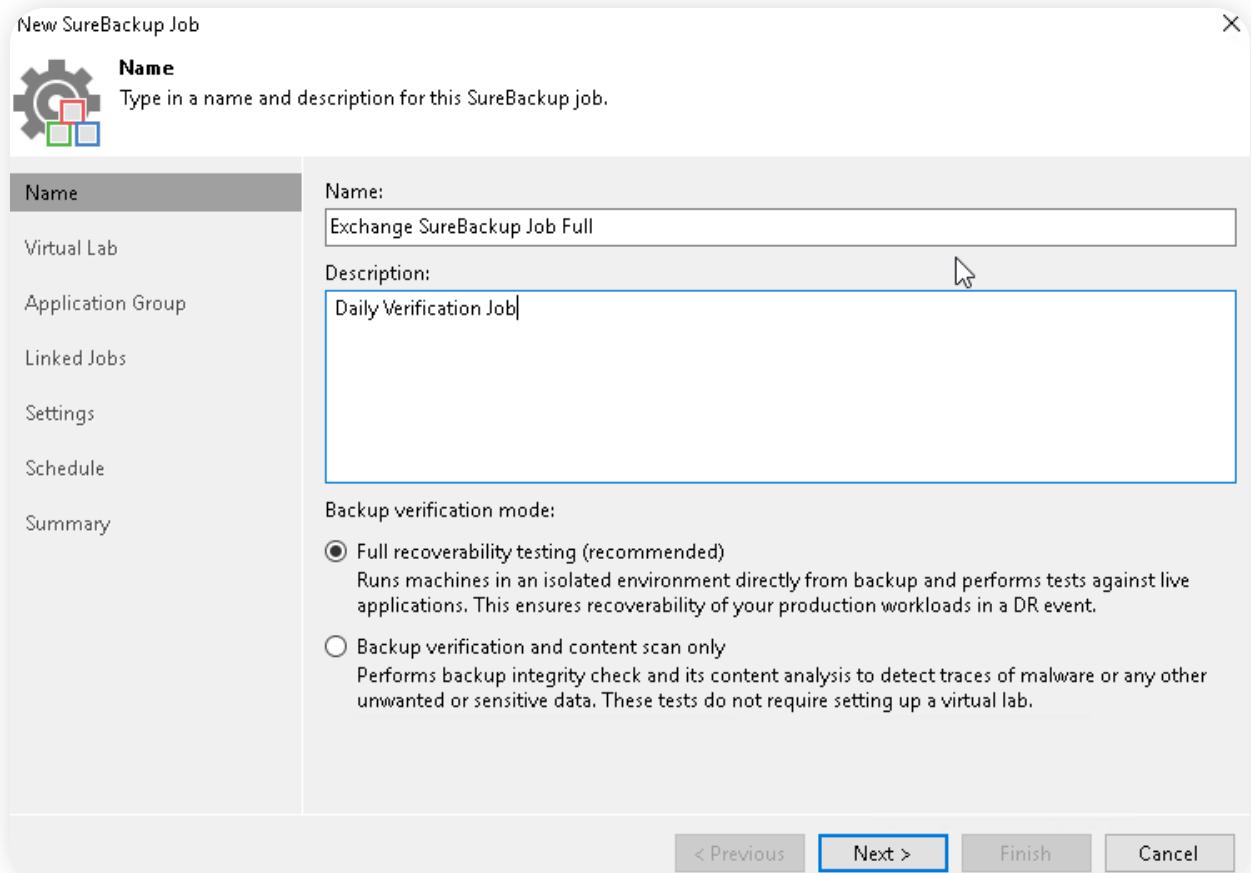
Pruebas completas de recuperabilidad

Veeam Backup & Replication publica los equipos en el entorno aislado y realiza la verificación según los scripts seleccionados.

Backup verification and content scan only

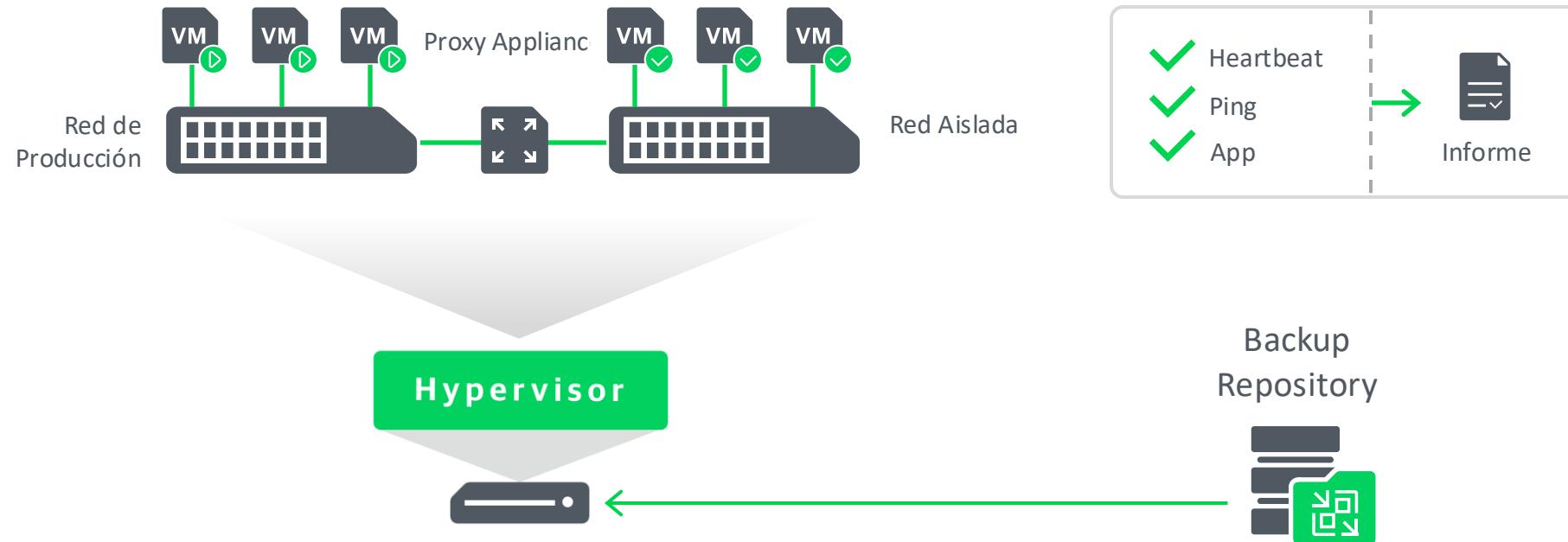
Sólo verificación de copias de seguridad y escaneo de contenidos

Si no se publican las máquinas en un laboratorio virtual, Veeam Backup & Replication realiza una comprobación de la integridad de la copia de seguridad y su análisis de contenido para detectar rastros de malware o cualquier otro dato no deseado o sensible.



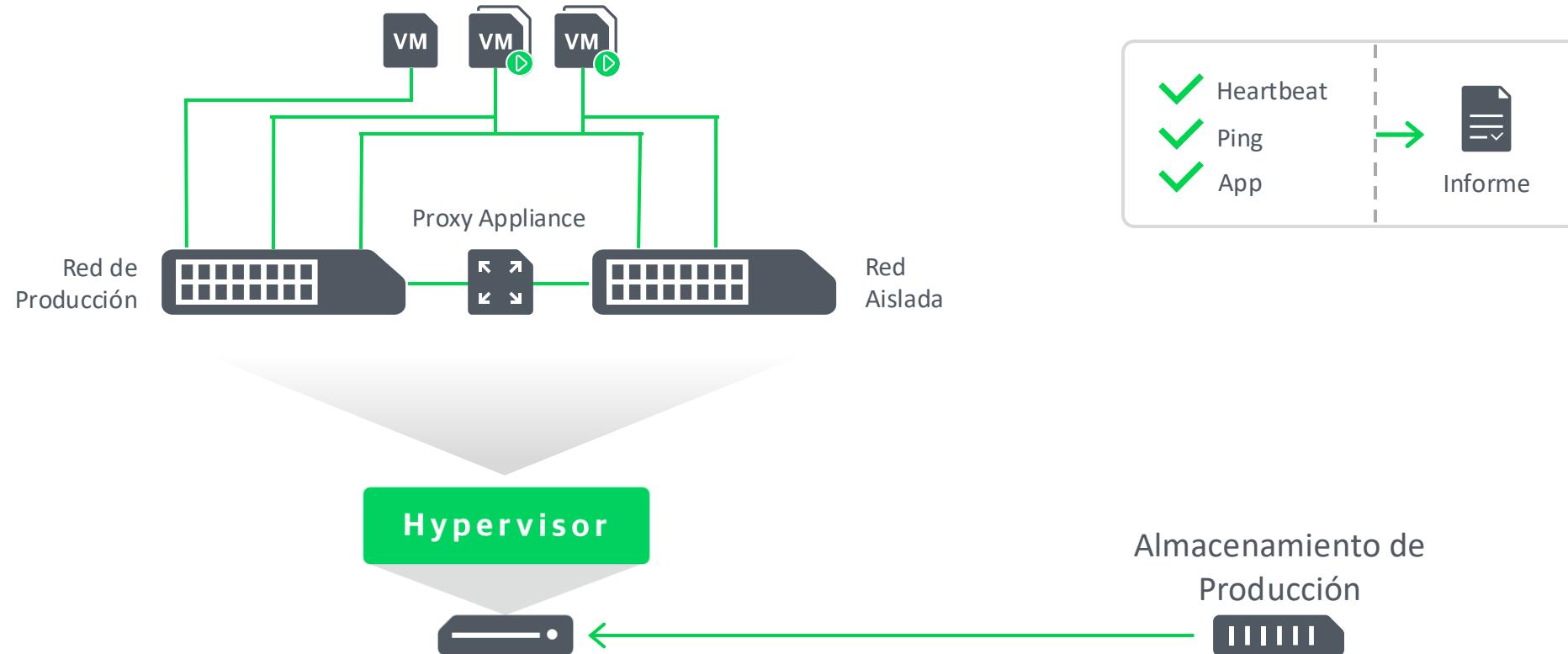
Funciones Avanzadas

SureBackup Workflow



Funciones Avanzadas

SureReplica Workflow (VMware only)

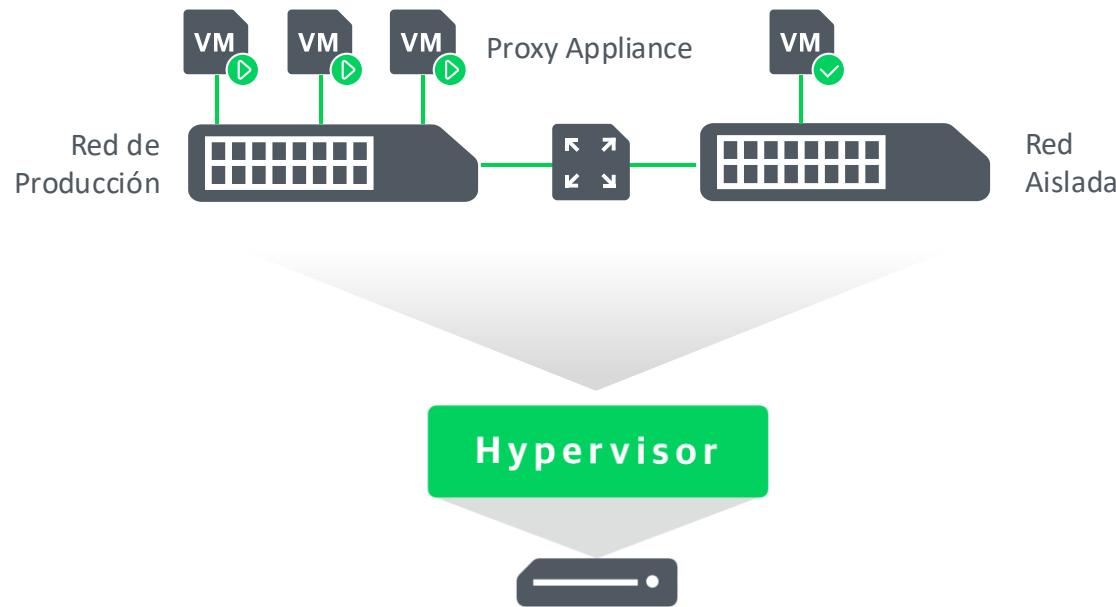


Funciones Avanzadas

On-Demand Sandbox

Inicie una copia de su entorno de producción en cualquier momento para diversos fines de **prueba, seguridad, formación o resolución de problemas.**

Todos los cambios realizados en las máquinas virtuales se escriben en redo logs (para copias de seguridad de máquinas virtuales e instantáneas de almacenamiento) o se guardan en archivos delta (para réplicas de máquinas virtuales). Redo Logs y los archivos delta se eliminan después de terminar de trabajar con el entorno de pruebas bajo demanda y apagarlo.



Inmutabilidad

Inmutabilidad

Definición de Inmutabilidad:

- La inmutabilidad se refiere al estado de los datos que impide modificarlos o borrarlos.

Ventajas de la inmutabilidad:

- Garantiza la integridad y seguridad de los datos.
- Ofrece protección frente al ransomware y los borrados accidentales.

Tipos de repositorios inmutables compatibles

- Amazon, S3-compatible y Azure object storage repositories.
- Repositorio Reforzado.
- HPE StoreOnce.
- Dell Data Domain

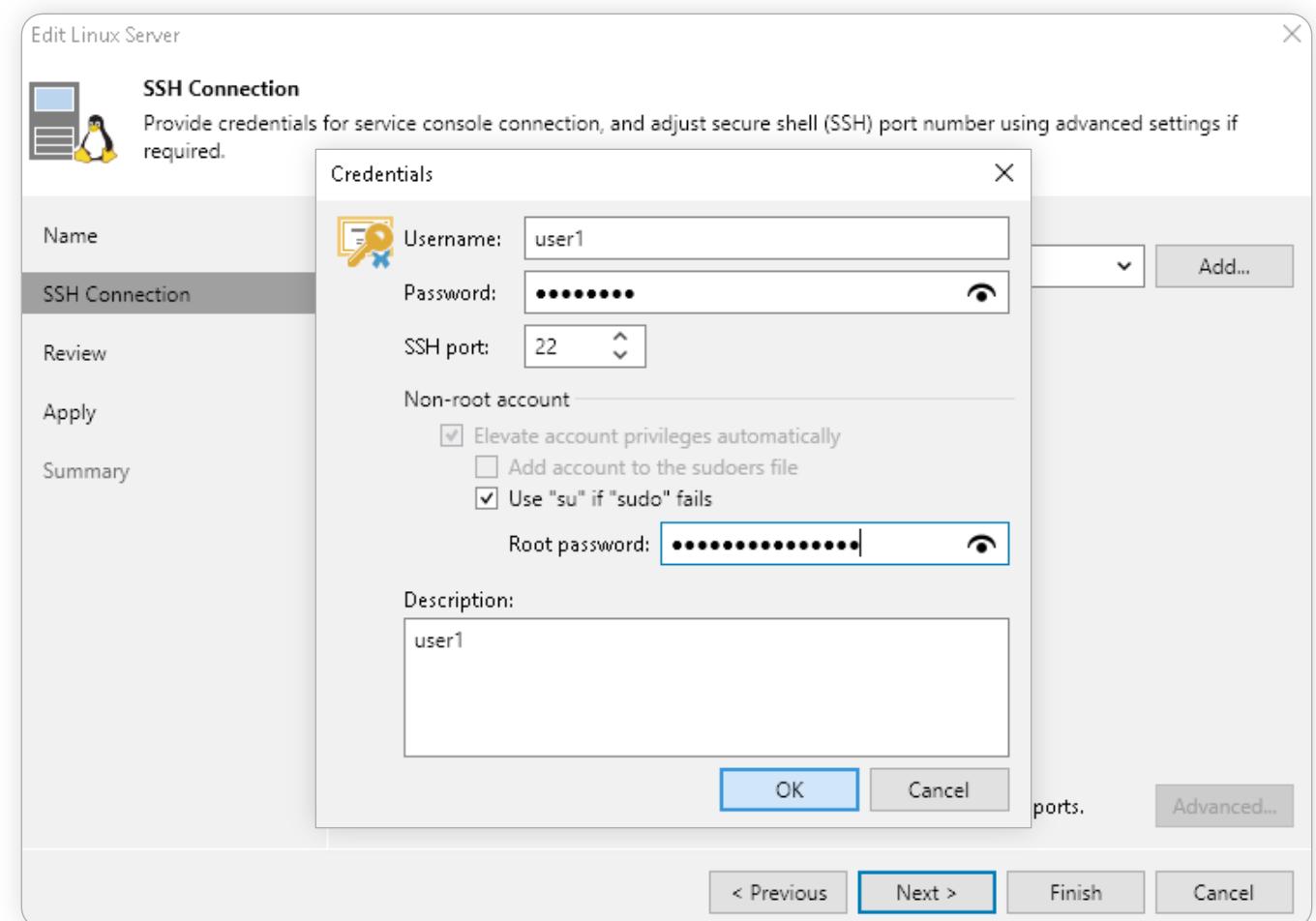
Inmutabilidad

Añadir Repositorio Linux Reforzado

En el paso Conexión SSH del asistente, especifique las **credenciales de un solo uso** para conectarse al servidor Linux y desplegar Veeam Data Mover.

Veeam Backup & Replication **no almacena estas credenciales** en la base de datos de configuración.

NOTA: La cuenta de usuario que utilice debe ser una cuenta non-root. Además, debe tener el directorio **home** creado en el servidor Linux.

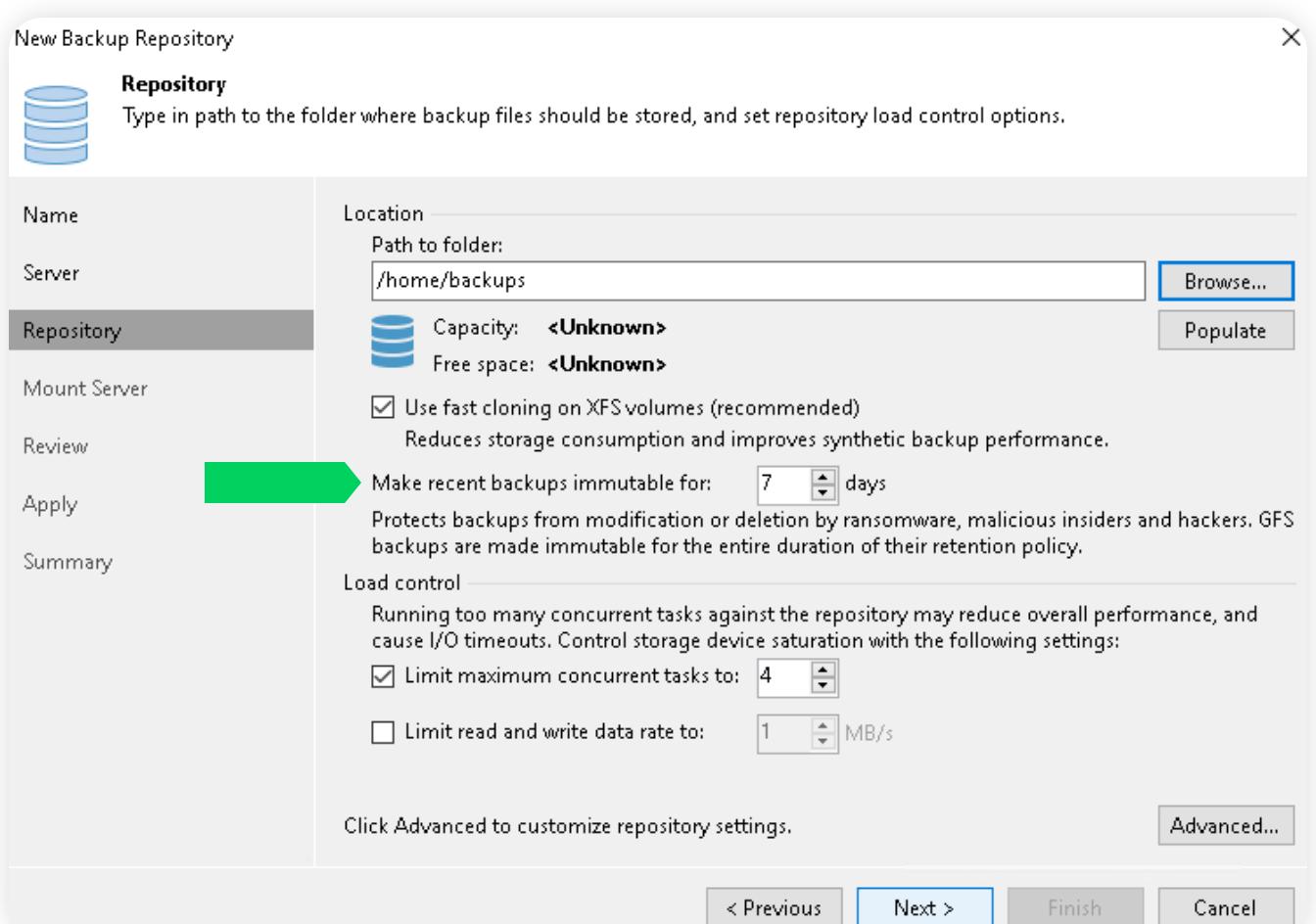


Inmutabilidad

Añadir Repositorio Linux Reforzado

Cuando se añade un repositorio reforzado, se especifica el periodo de tiempo durante el cual los archivos de copia de seguridad deben ser inmutables.

Durante este periodo, los archivos de copia de seguridad almacenados en este repositorio **no pueden modificarse ni borrarse**.



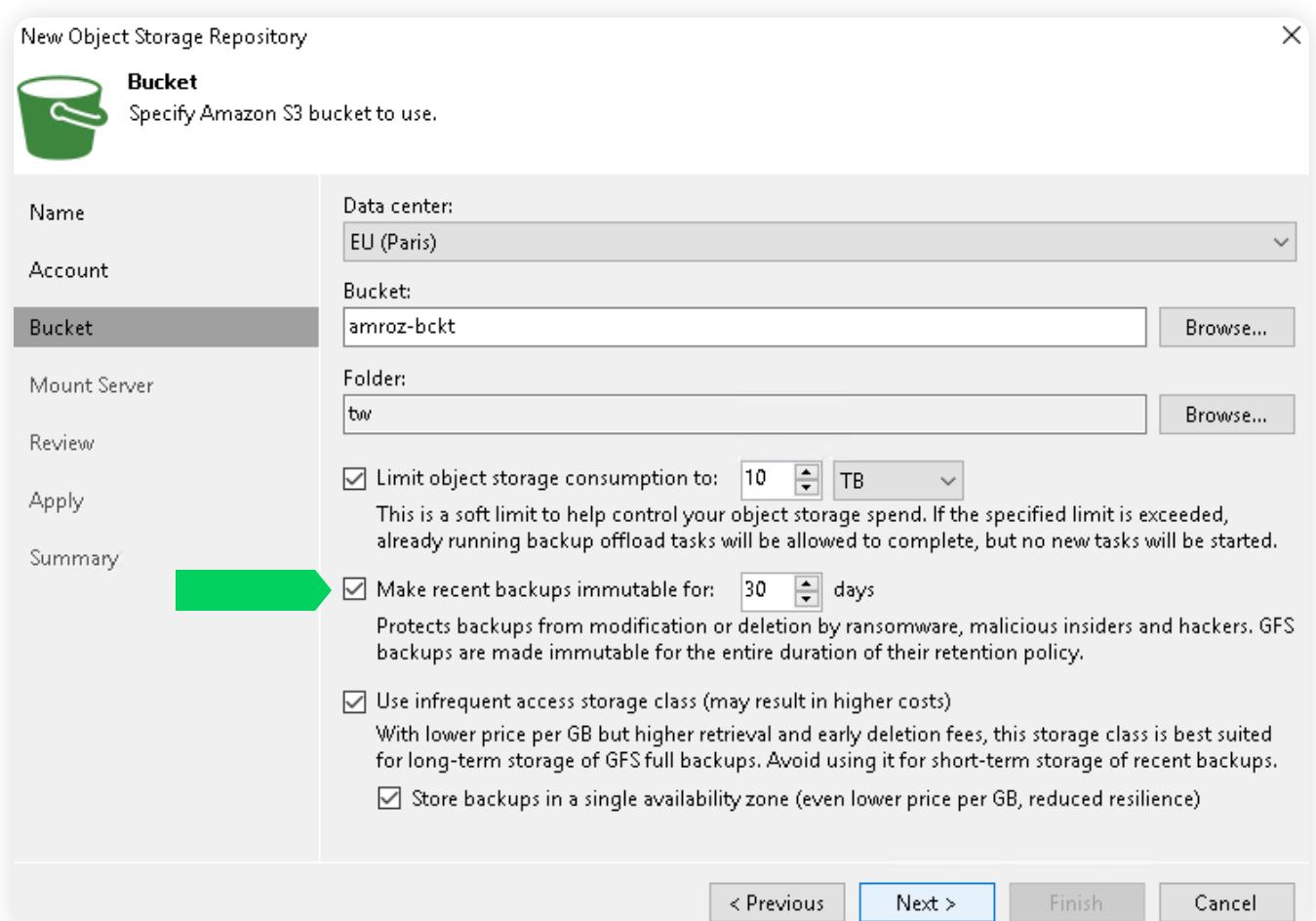
Inmutabilidad

Hacer copias de seguridad inmutables con almacenamiento de objetos

Para que los datos sean inmutables, Veeam Backup & Replication utiliza la tecnología que impide que los datos se borren y permite conservar varias versiones de los objetos.

La **tecnología seleccionada depende del tipo de almacenamiento de objetos:**

- Object lock and Versioning – Para Amazon S3 Storage, S3 Compatible, IBM Cloud, Wasabi Cloud.
- Version-level WORM and blob versioning – Para Azure Storage.



Integración de Almacenamiento

Integración de Almacenamiento

Tipos de Integración

Integración VMware

Copia de seguridad de máquinas virtuales VMware vSphere.

Orqueste snapshots a través de arrays de almacenamiento.

Restaurar datos a partir de snapshots de almacenamiento con Veeam Backup & Replication.

Integración NAS

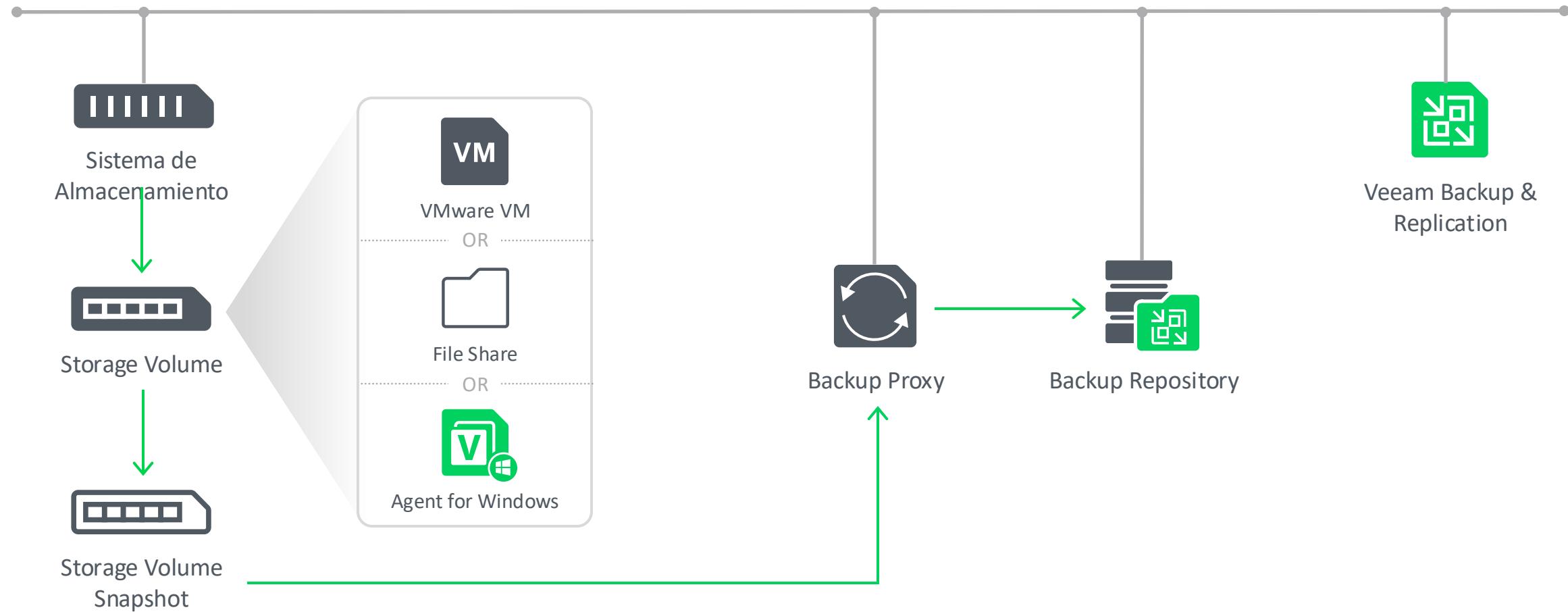
Realice copias de seguridad de archivos NAS compartidos sin esfuerzo.

Integración Veeam Agent for Windows

Crear copias de seguridad de Veeam Agent para equipos Windows.

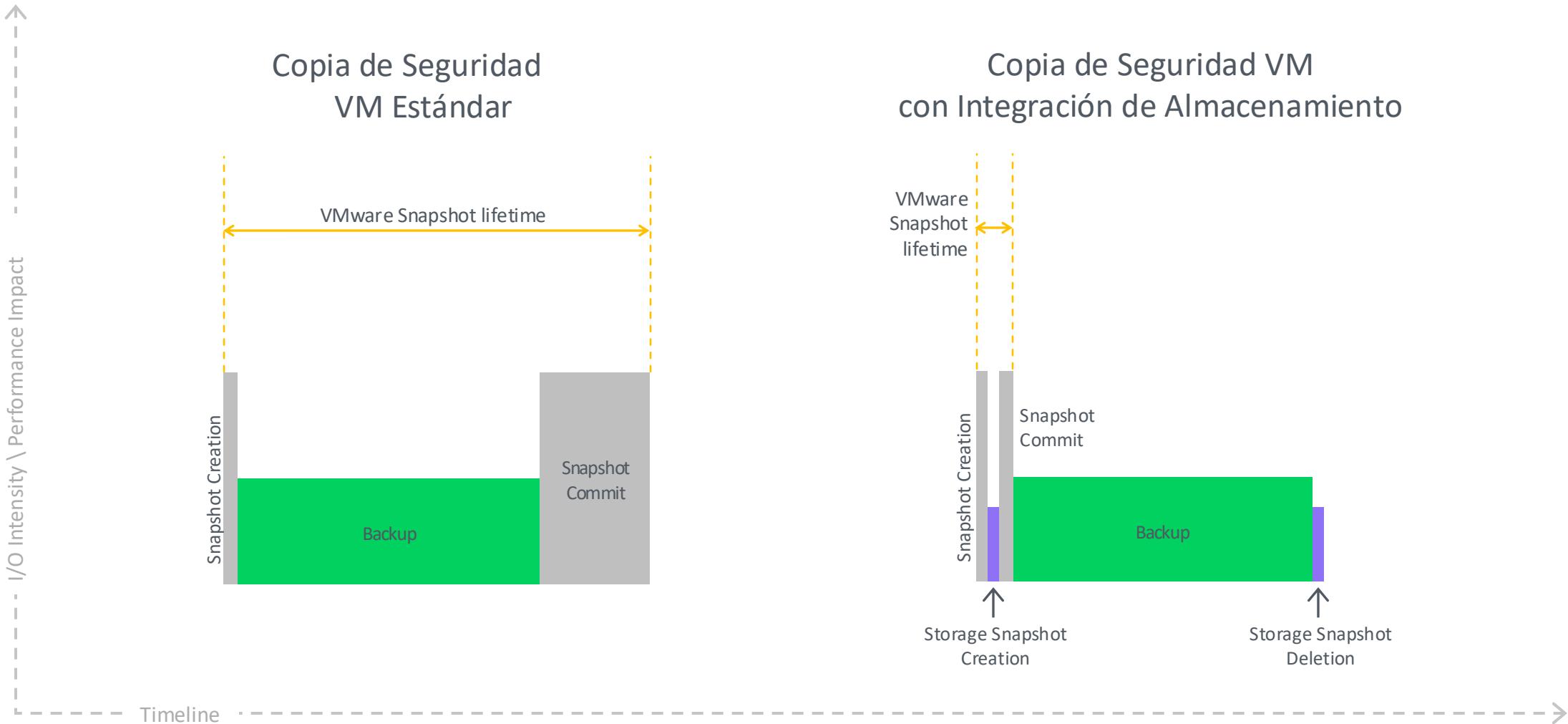
Integración de Almacenamiento

Perspectiva General de la Infraestructura



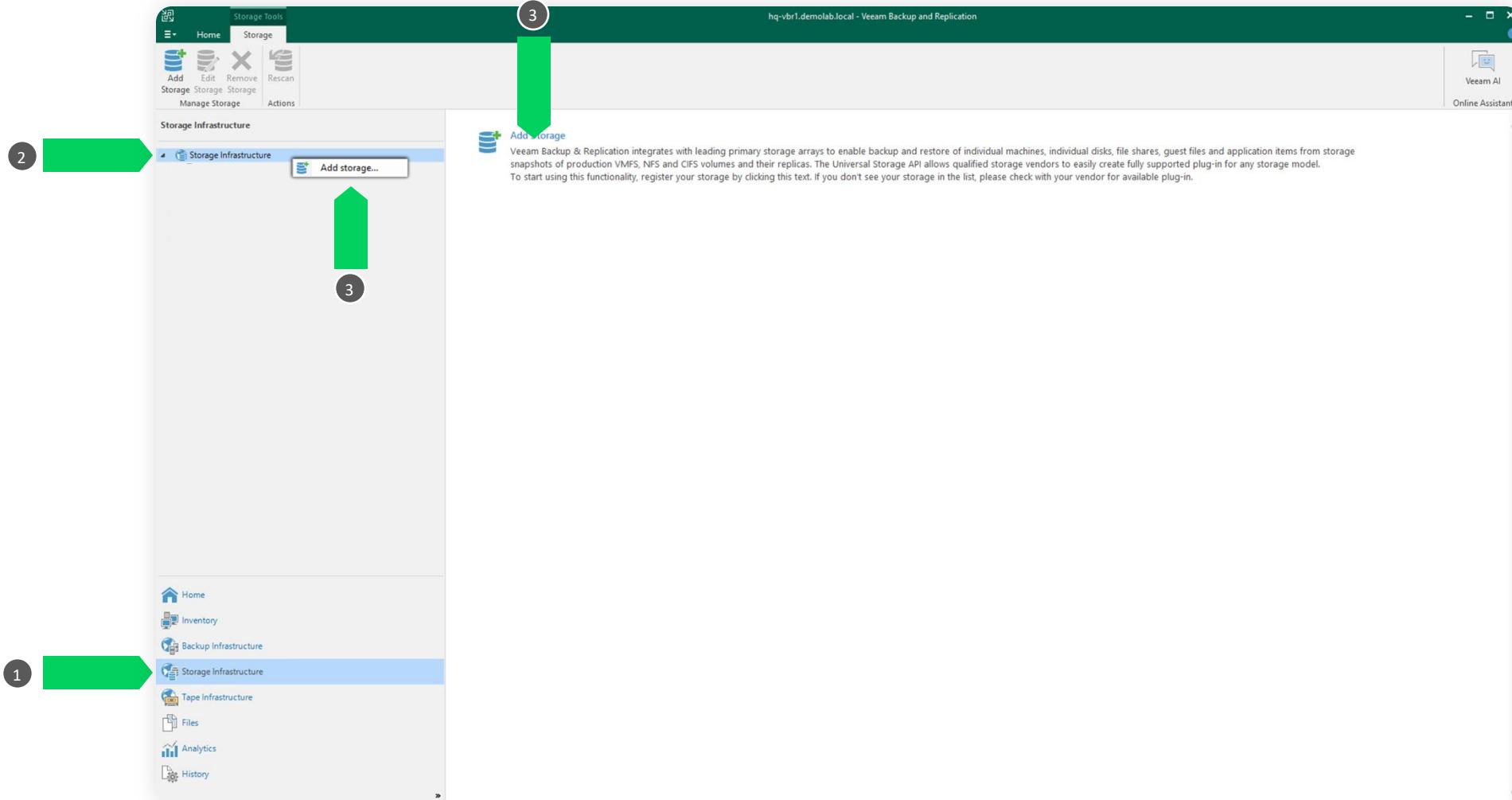
Integración VMware

Representación Cronológica



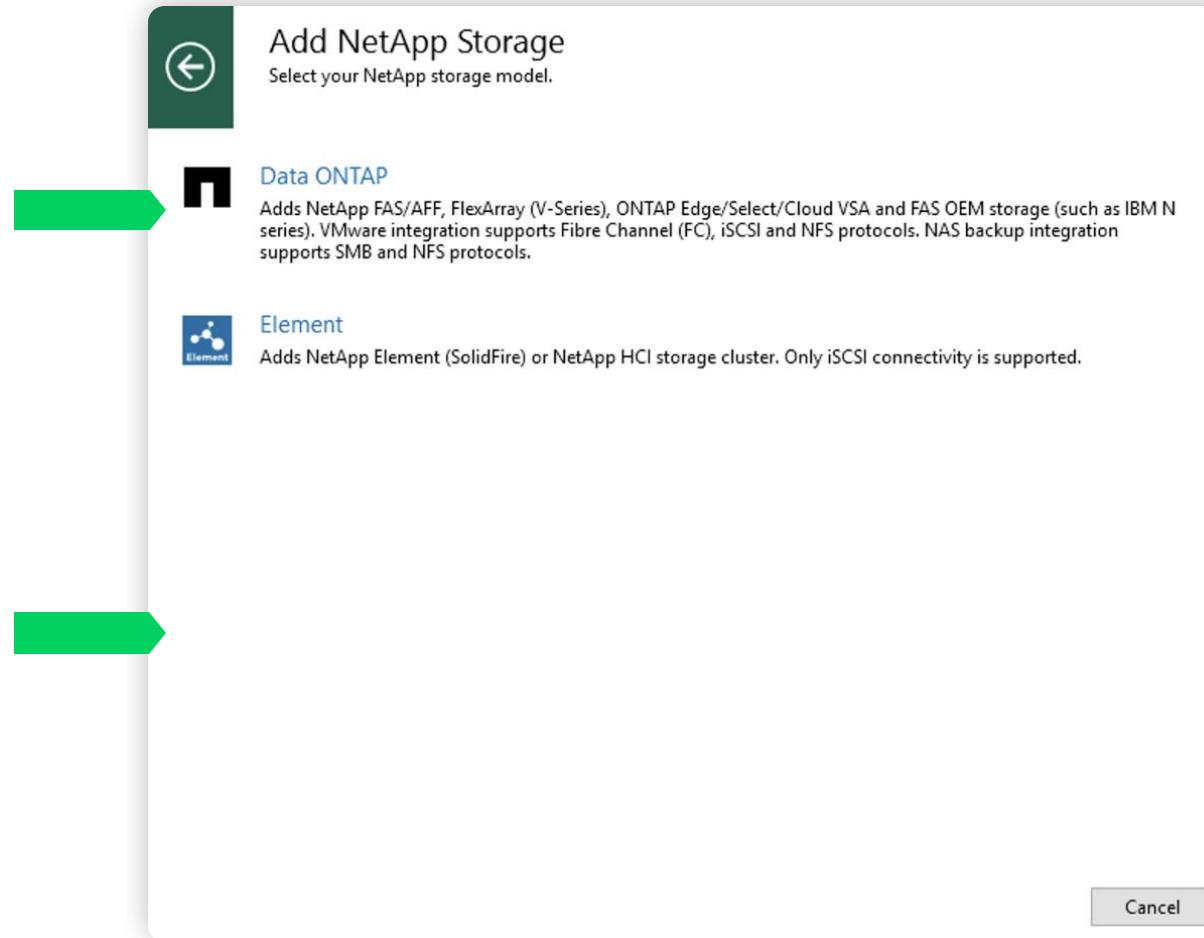
Integración de Almacenamiento

¿Cómo se configura?



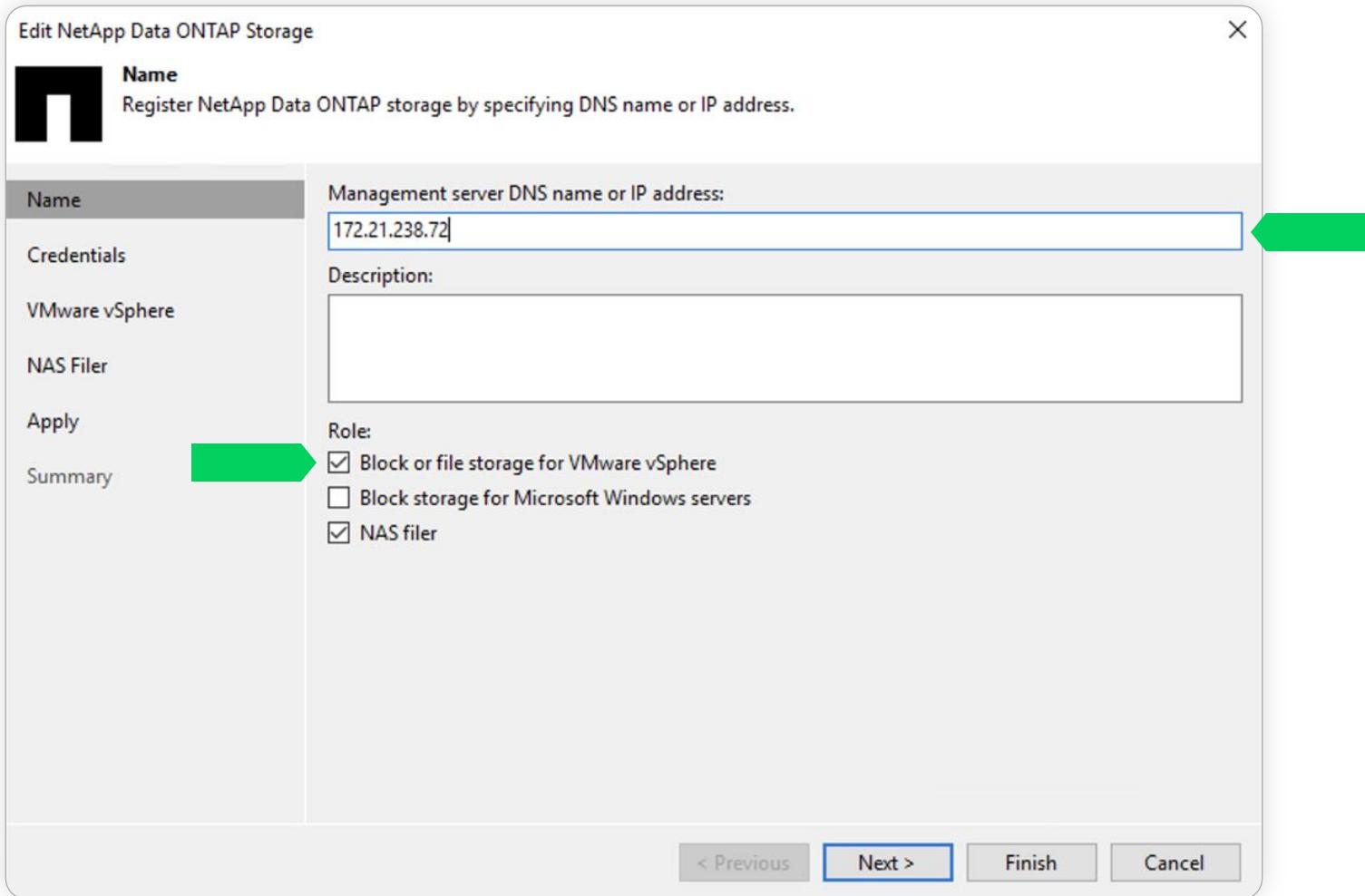
Integración de Almacenamiento

¿Cómo se configura?



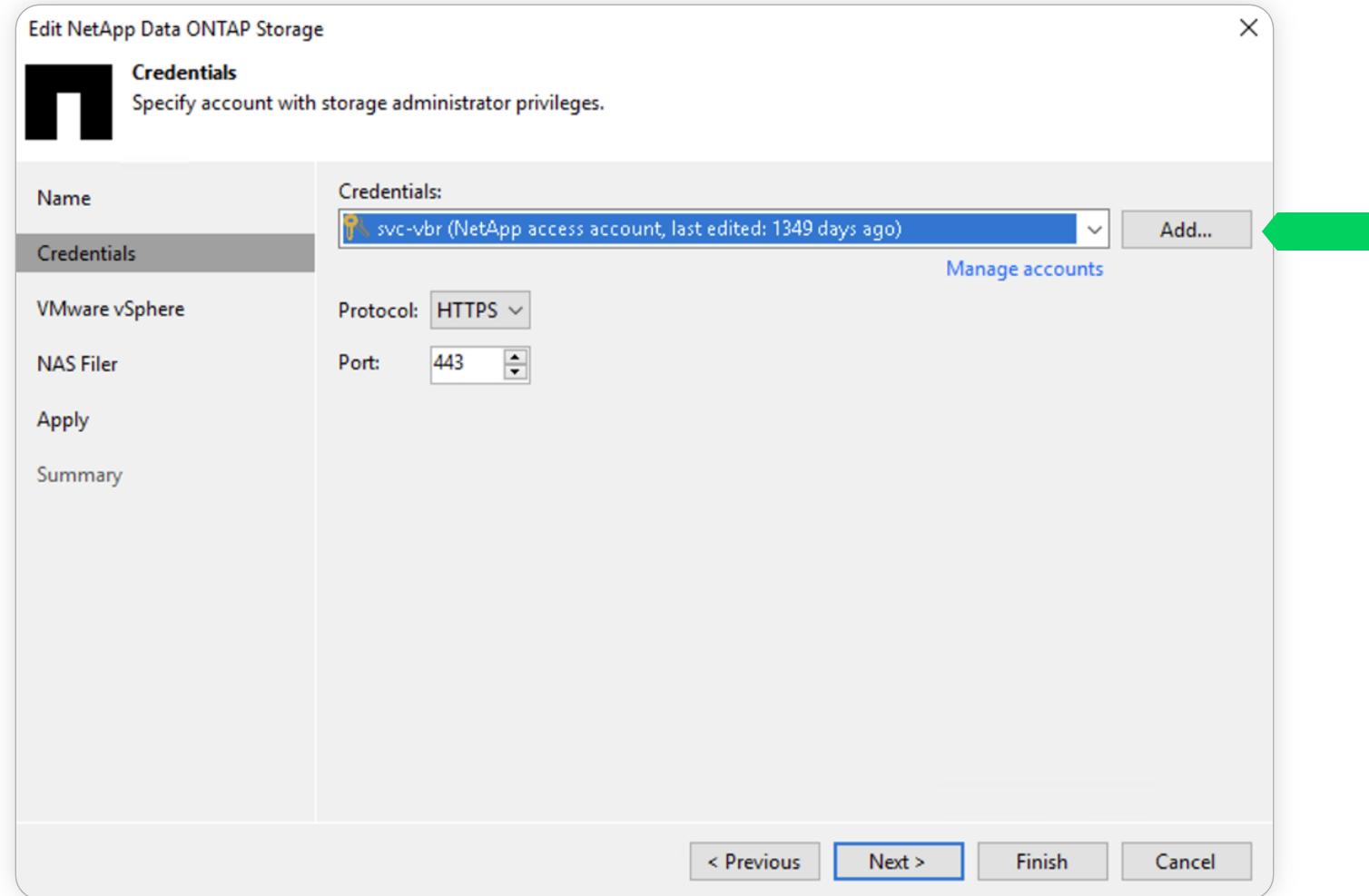
Integración de Almacenamiento

¿Cómo se configura?



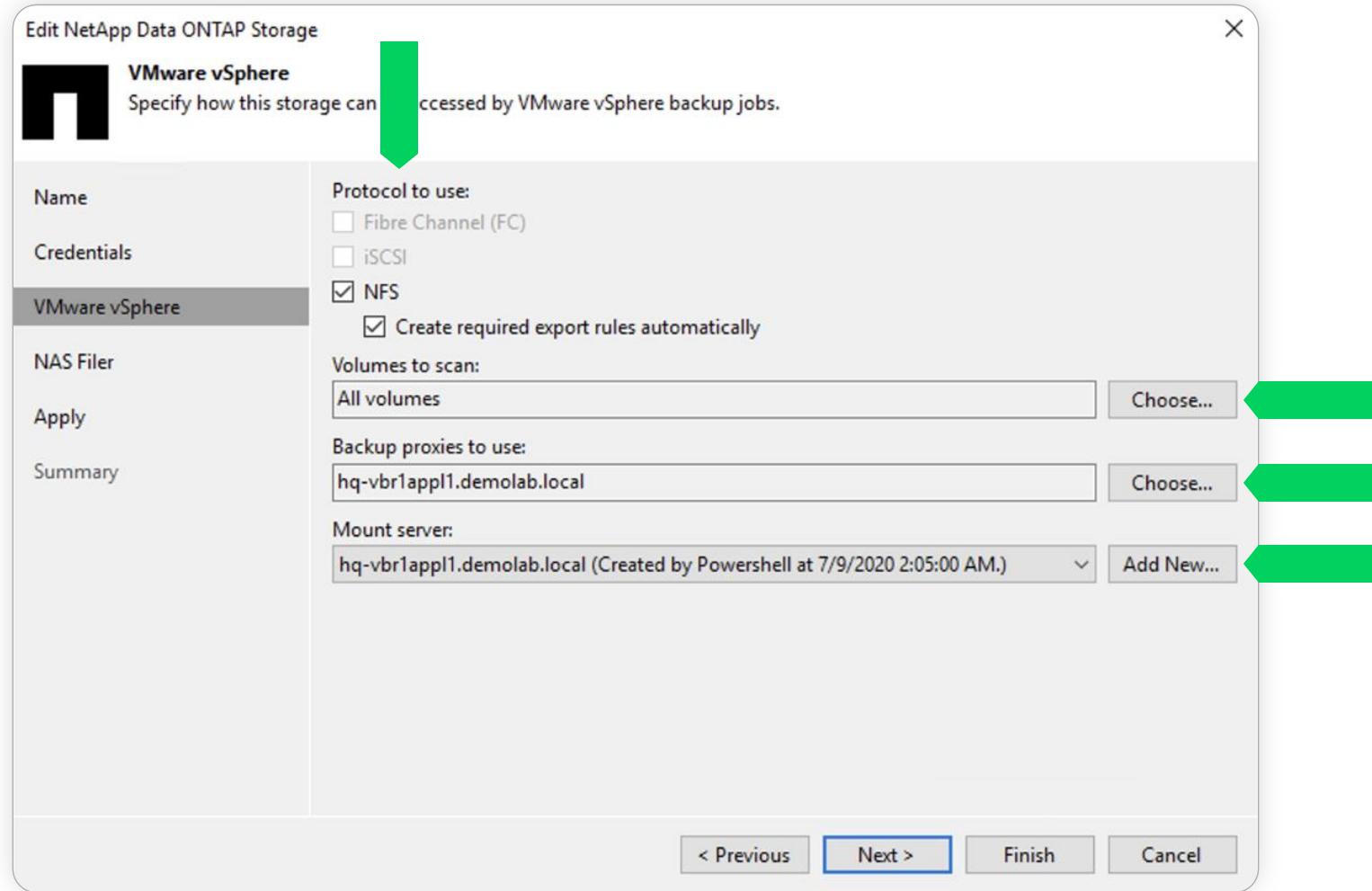
Integración de Almacenamiento

¿Cómo se configura?



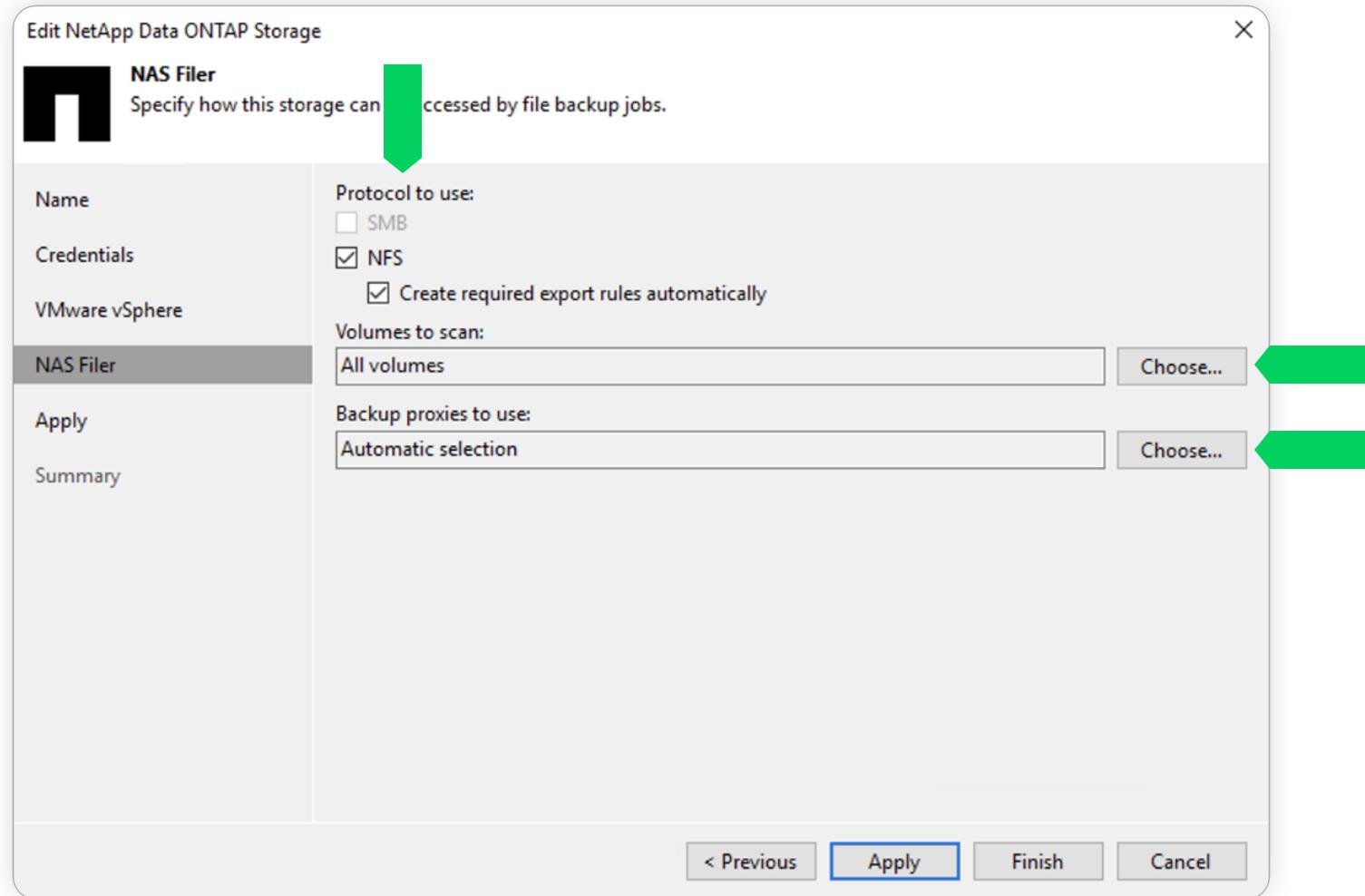
Integración de Almacenamiento

¿Cómo se configura?



Integración de Almacenamiento

¿Cómo se configura?

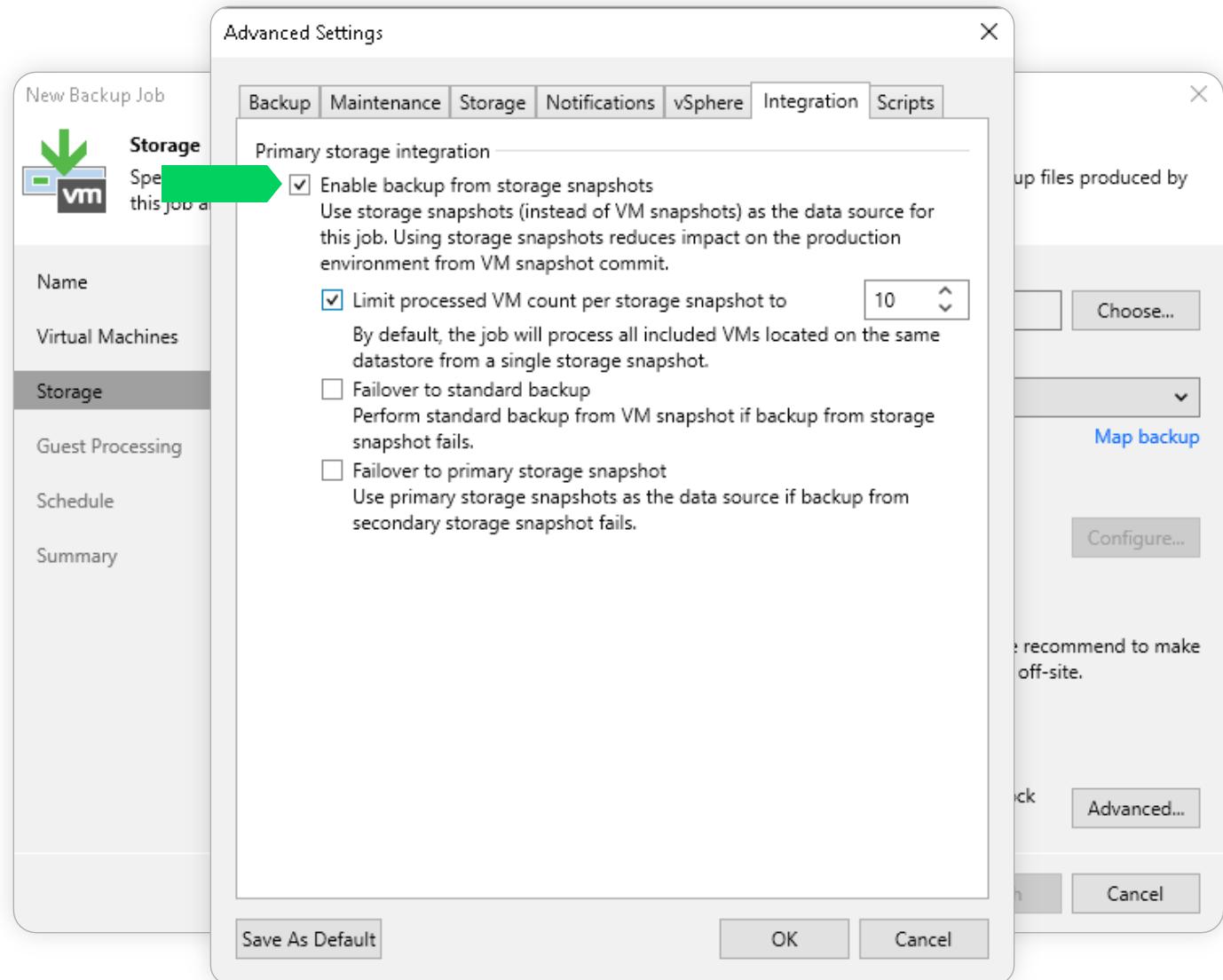


Integración de Almacenamiento

La pestaña **Integración** de la configuración de la tarea de copia de seguridad le permite determinar si desea utilizar la tecnología de copia de seguridad desde snapshot para crear la copia de seguridad. Está **activada por defecto**.

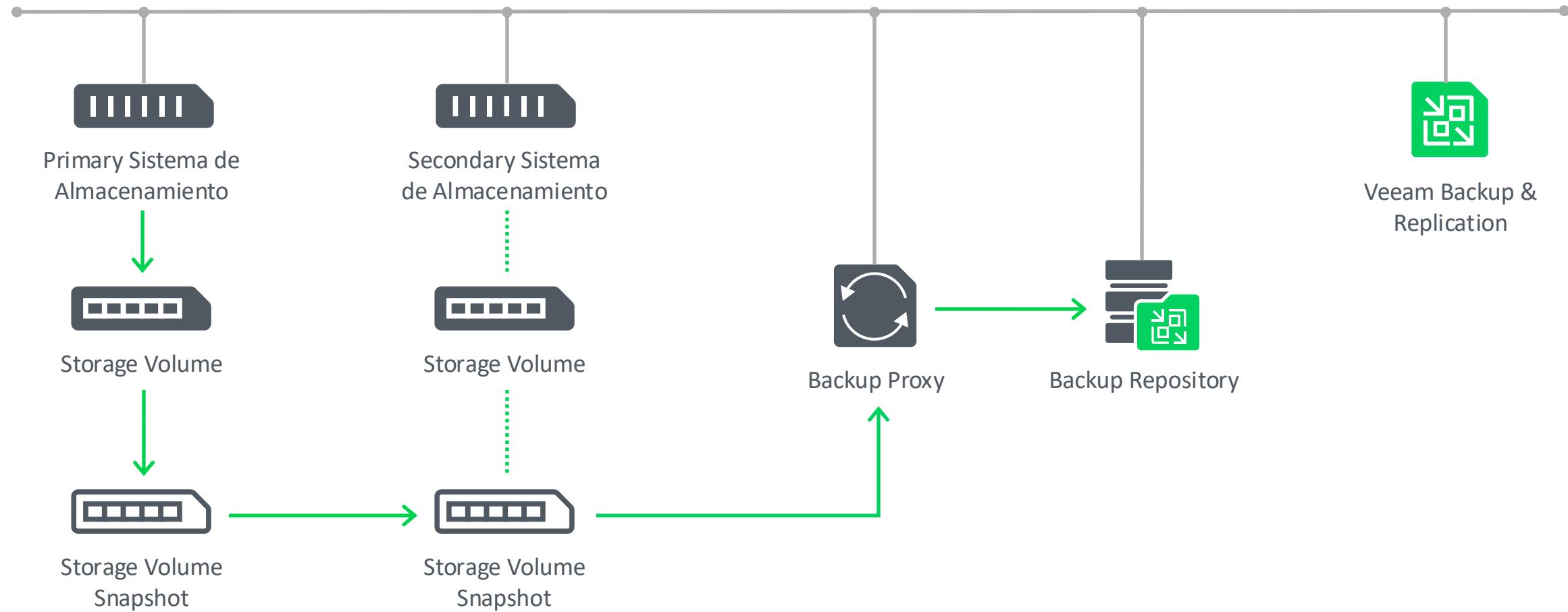
La copia de seguridad a partir de snapshots permite aprovechar las snapshots para el procesamiento de datos de máquinas virtuales.

La tecnología **mejora RPO** y reduce el **impacto de las actividades de copia de seguridad** en el entorno de producción.

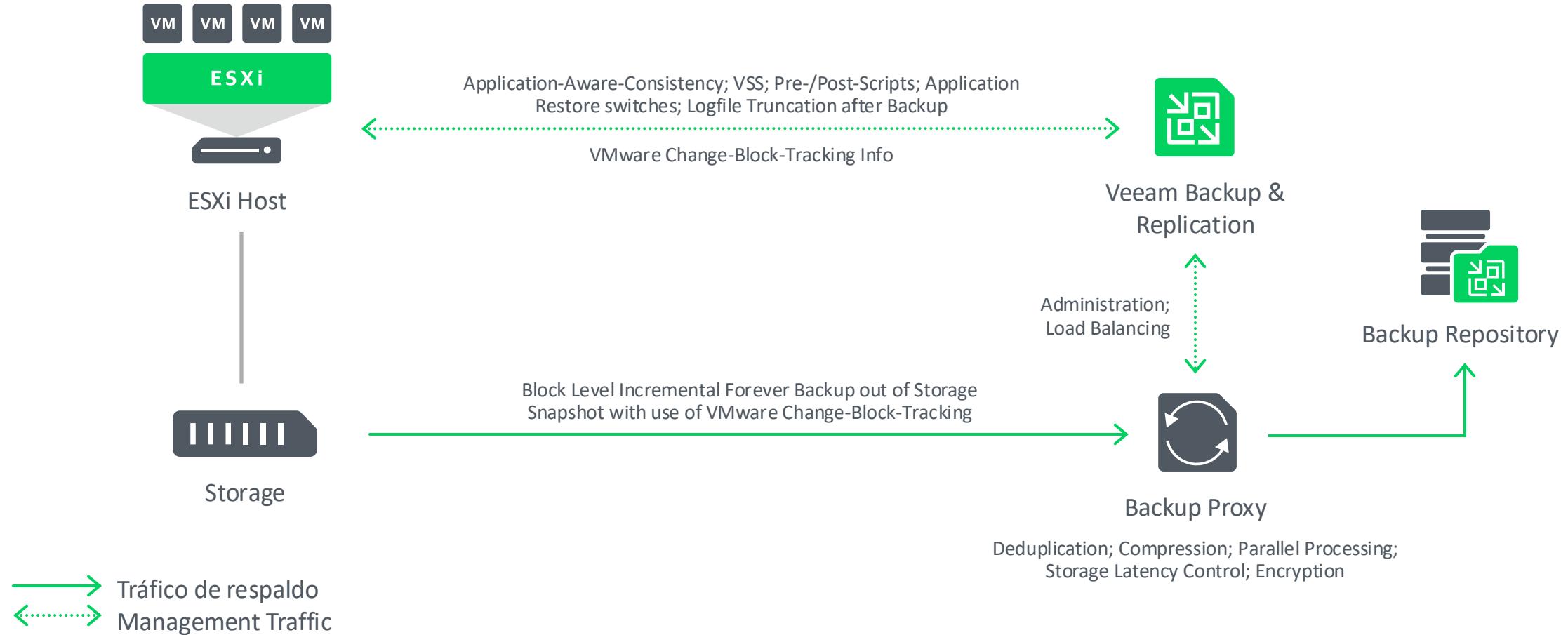


Integración de Almacenamiento

Copia de seguridad de snapshot del Almacenamiento Secundario



Copia de Seguridad Basada en Snapshots de Almacenamiento



Cinta (Brevemente)

Cinta

Veeam Backup & Replication soporta operaciones de cinta nativas.

Dispositivos de cinta compatibles: Linear Tape-Open (LTO3 – LTO9) bibliotecas IBM 3592 (TS1160 & TS1170).

Propósito: archivo de datos a largo plazo y/o requisitos de cumplimiento.

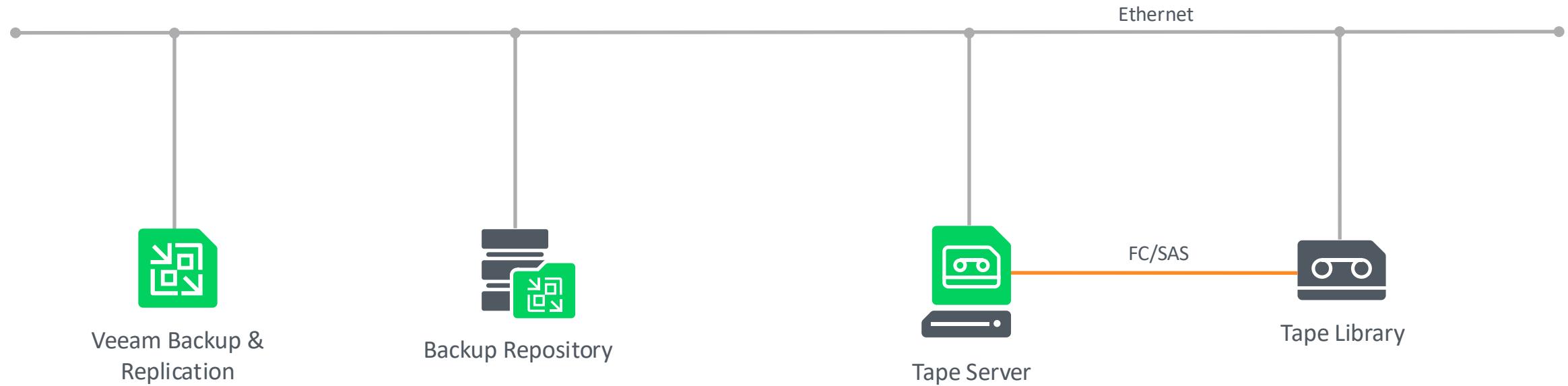
Estrategia de Copia de Seguridad : se adhiere al método de copia de seguridad «3-2-1»: 3 copias, 2 tipos de soporte, 1 ubicación externa.

Tipos de datos compatibles para archivar :

- Respaldos de VMs
- Respaldos de Veeam Agent
- Repositorios de copia de seguridad completos, incluyendo repositorios Linux Reforzados
- Datos no estructurados:
 - Volúmenes de almacenamiento mediante NDMP
 - Archivos Compartidos SMB y NFS
 - Almacenamiento de Objetos

Cinta

Resumen de la Infraestructura



WAN Accelerator

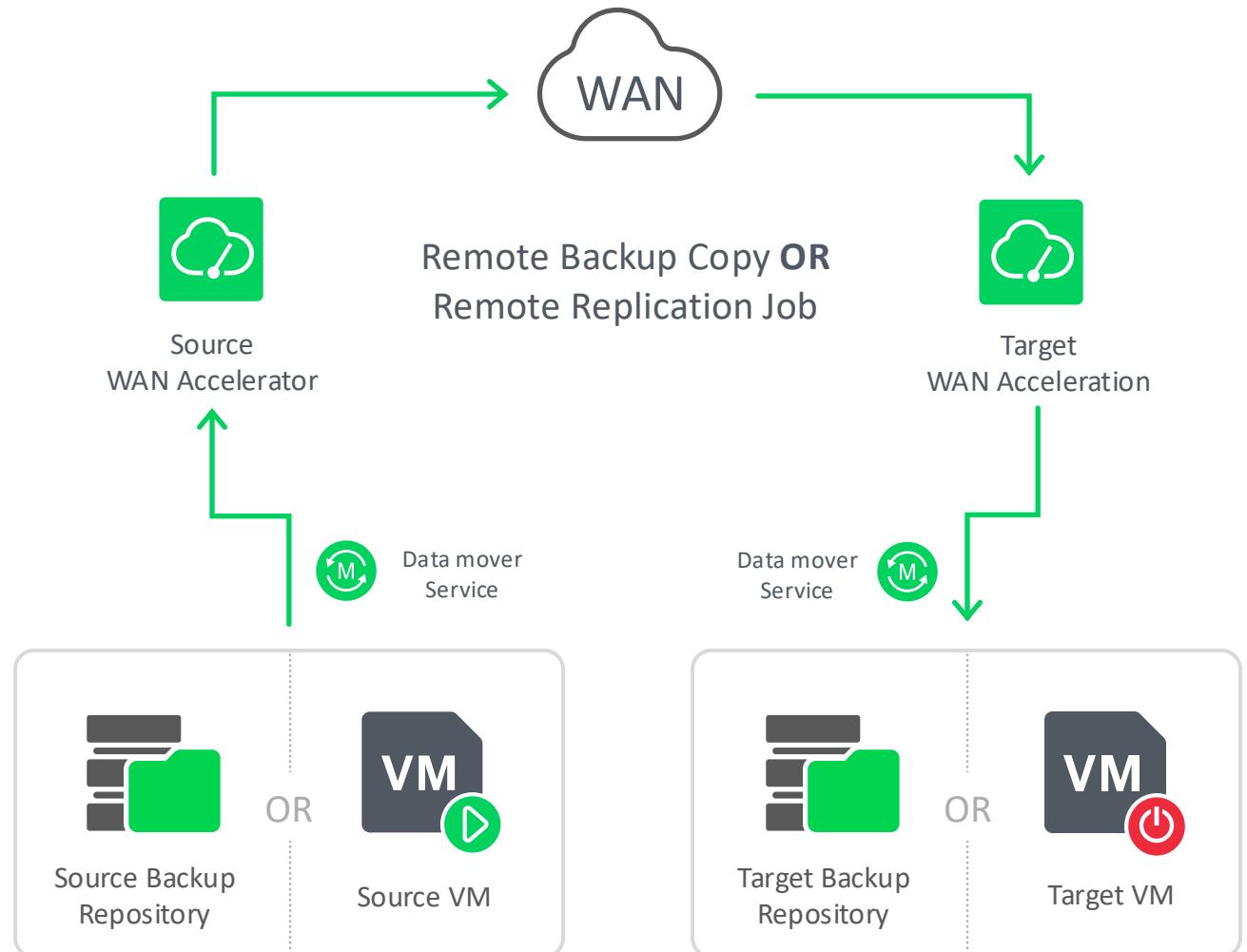
WAN Accelerator

Veeam Backup & Replication ofrece tecnología WAN acceleration que combine:

- Compresión del tráfico de red
- Carga multi-streaming
- Deduplicación global de datos
- Deduplicación de tamaño de bloque variable

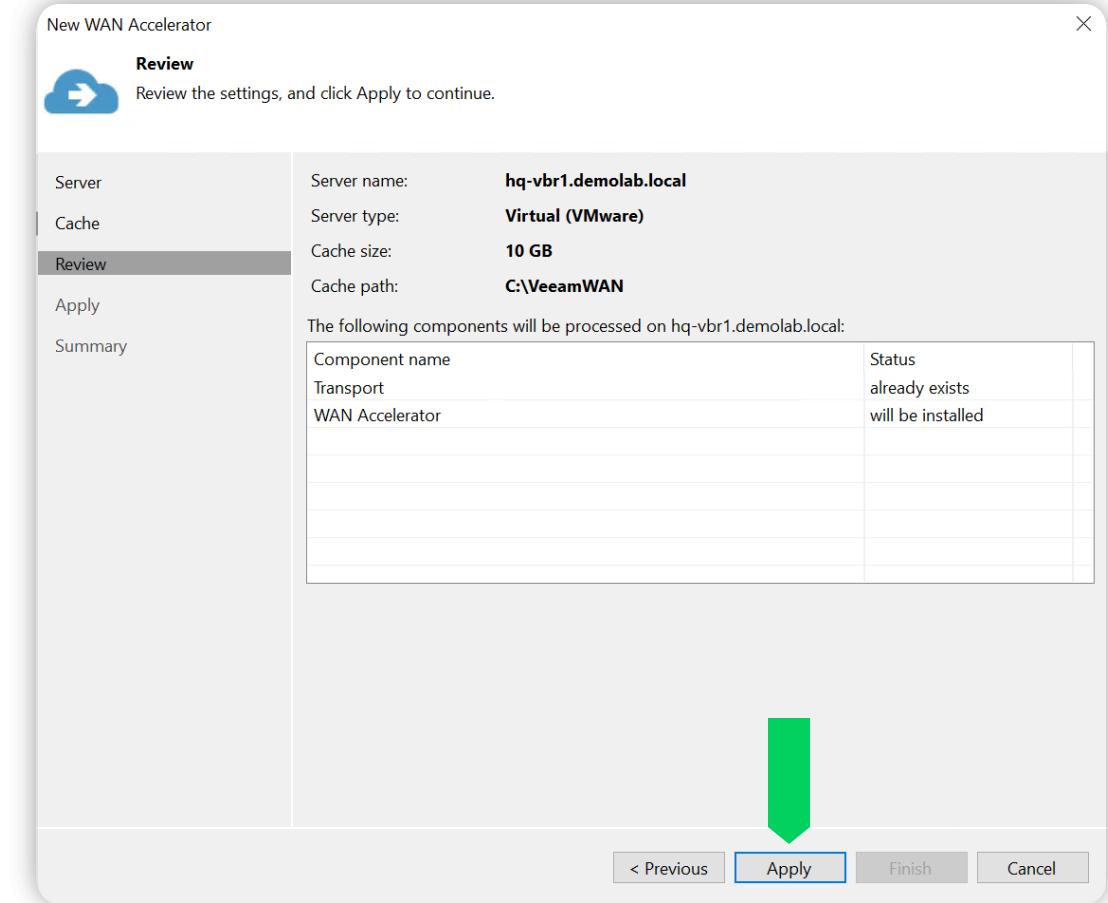
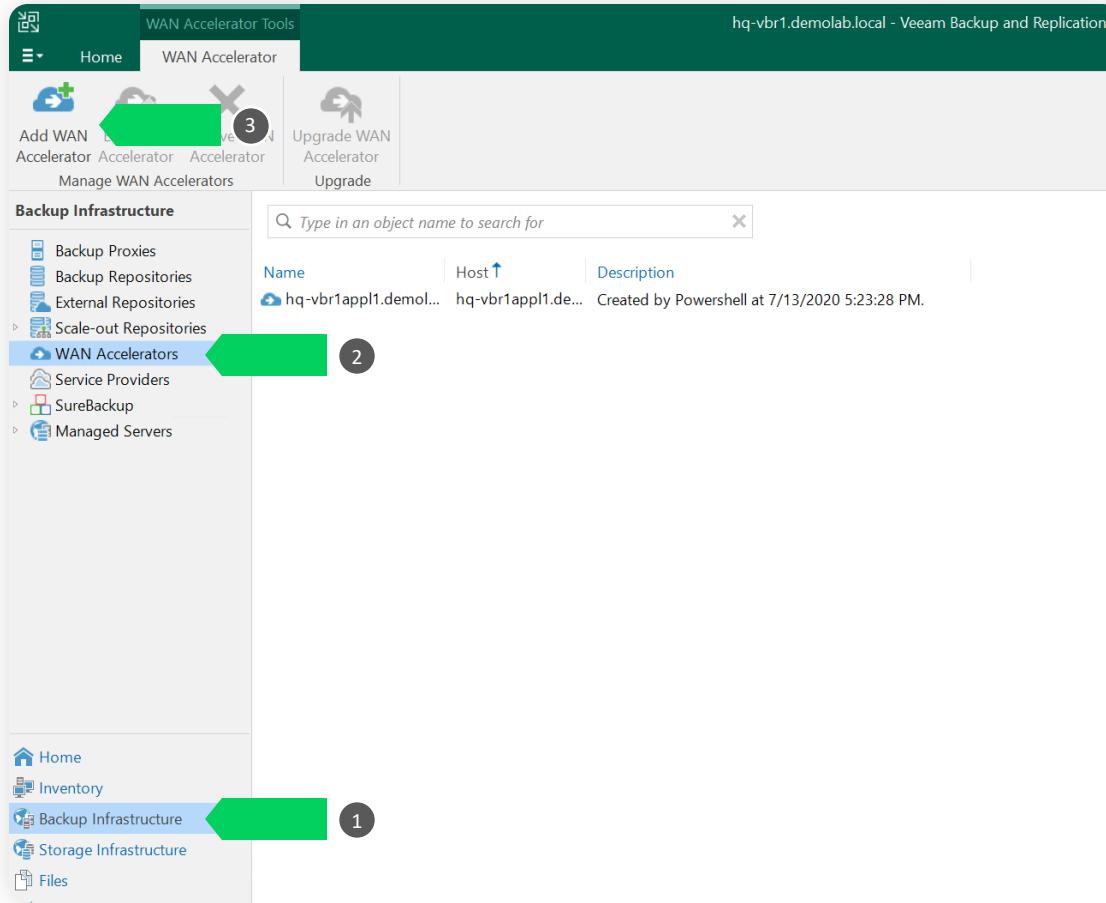
Esta combinación de tecnologías reduce el volumen de datos transferidos, lo que ayuda a transportarlos más rápidamente.

- **High Bandwidth Mode** es diseñado para conexiones WAN más rápido que 100Mbps.
- **Low Bandwidth Mode** es diseñado para conexiones WAN más lento que 100Mbps.



WAN Accelerator

¿Cómo desplegar?



WAN Accelerator

¿Cómo empezar a utilizarlo?

The image shows two overlapping 'Edit Job' dialog boxes from Veeam software, both titled 'Data Transfer'. The left dialog is for a 'Backup Copy Job' and the right one is for a 'Replication Job'. Both dialogs have tabs for 'Job', 'Objects', 'Target', 'Data Transfer' (which is selected), 'Schedule', and 'Summary'. A large green arrow points from the 'Data Transfer' tab on the left to the 'Data Transfer' tab on the right, indicating that the configuration is identical for both types of jobs.

Edit Backup Copy Job

Data Transfer
Choose how object data should be transferred from source to target backup.

Job

Objects

Target

Data Transfer 

Schedule

Summary

Direct
Object data will be sent directly from source to target without copying backups on-site, and off-site over a fast link.

Through built-in WAN accelerators
Object data will be sent to target repository through both source and target sites. This mode provides significant bandwidth savings.

Source WAN accelerator:

Target WAN accelerator:

Edit Replication Job

Data Transfer
Choose how VM data should be transferred to the target site.

Name

Virtual Machines

Destination

Network

Job Settings

Data Transfer 

Seeding

Guest Processing

Schedule

Summary

Direct
Best for local and off-site replication over fast links.

Through built-in WAN accelerators
Best for off-site replication over slow links due to significant bandwidth savings.

Source WAN accelerator:

Target WAN accelerator:

< Previous

Next >

Finish

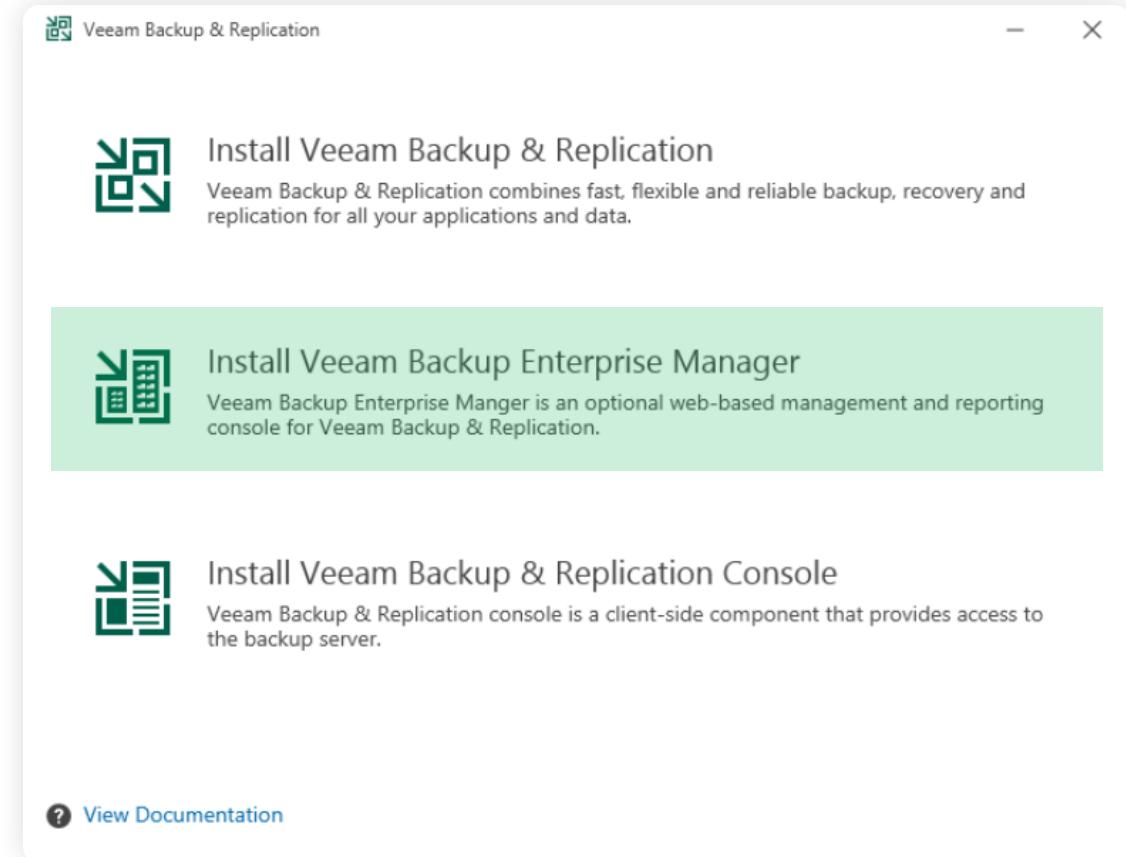
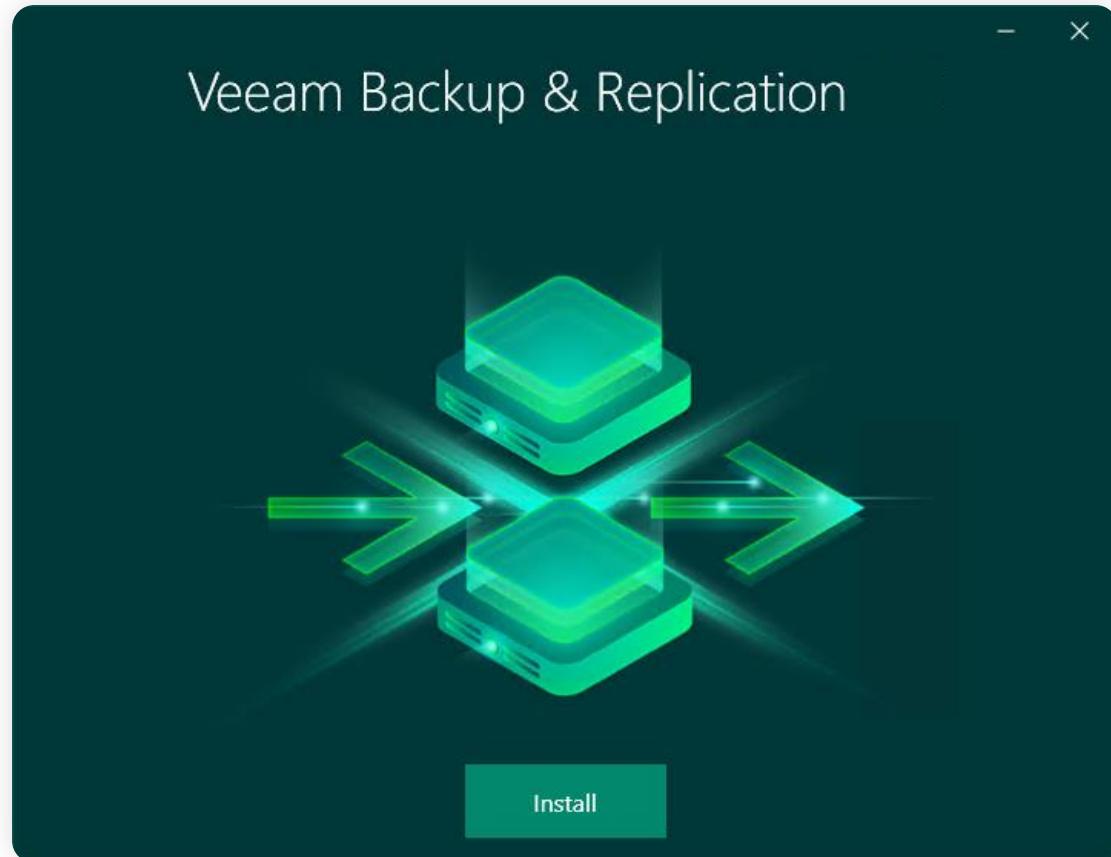
Cancel

Enterprise Manager

Veeam Enterprise Manager

Instalación

Veeam Enterprise Manager se incluye en el mismo .ISO que Veeam Backup & Replication.



Veeam Enterprise Manager

Instalación

Veeam Backup Enterprise Manager

System Configuration Check

System is being verified for potential installation problems.

! To finalize required components installation, system reboot is required.
Installation process will continue automatically.

Requirement	Status
Microsoft .NET Framework 4.7.2	Passed
Microsoft Visual C++ 2015-2019 Redistributable	Reboot required
Microsoft System CLR Types for SQL Server 2014	Passed
IIS URL Rewrite Module 2	Passed
Microsoft IIS	Passed
Default Document Component	Passed
Directory Browsing Component	Passed
HTTP Errors Component	Passed
Static Content Component	Passed
Windows Authentication Component	Passed
WebSocket Protocol Component	Passed
ASP.NET 4.5 Component	Passed

Back Reboot Cancel

Veeam Backup Enterprise Manager

License

Provide license file for Veeam Backup Enterprise Manager.

Select license provisioning method:

Sign in with Veeam | Browse license file

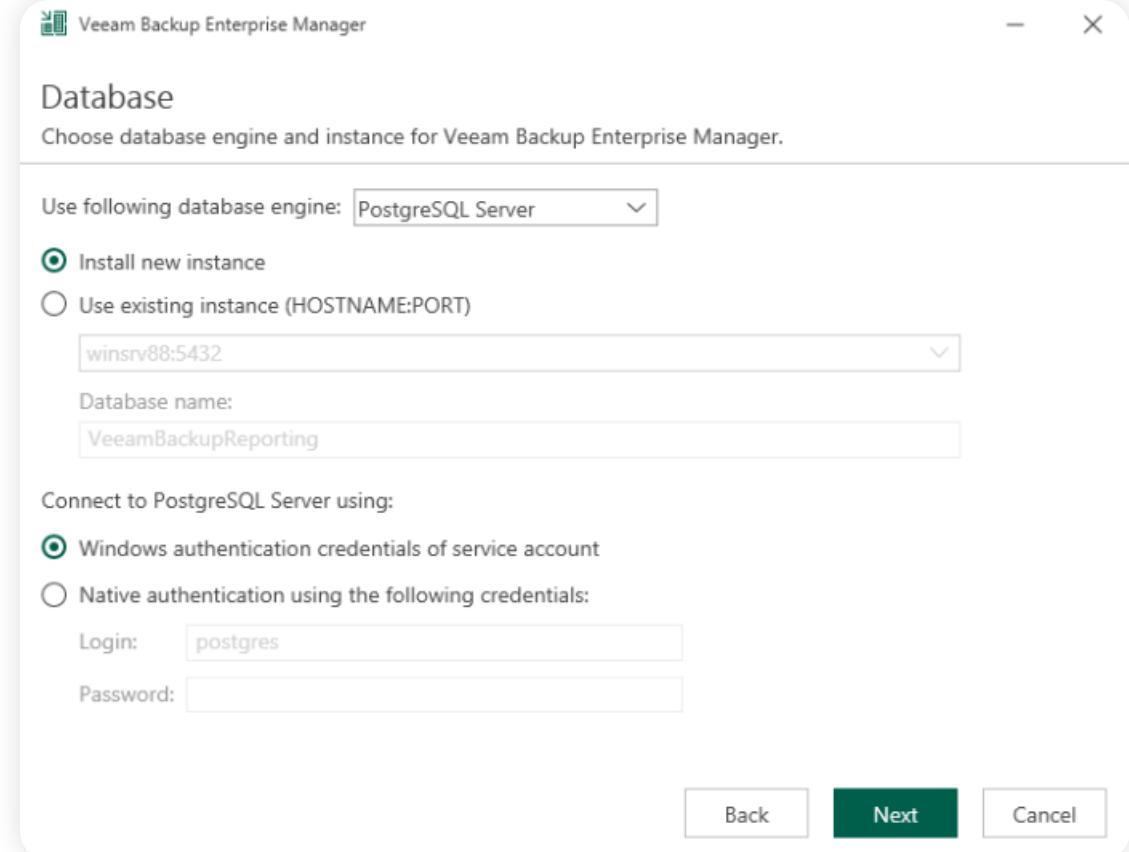
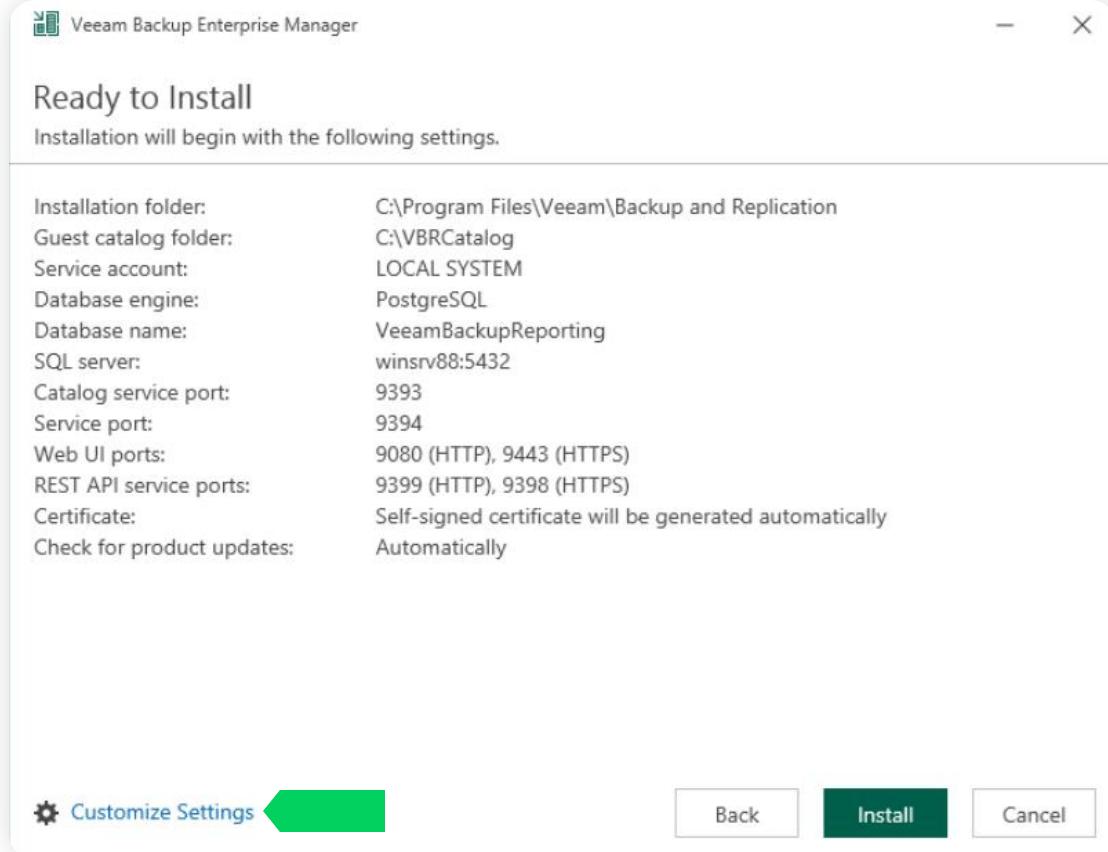
License details:
Subscription, Suite, 100 Instances, License expires on 31/12/2024

Update license automatically (enables usage reporting)
Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

Back Next Cancel

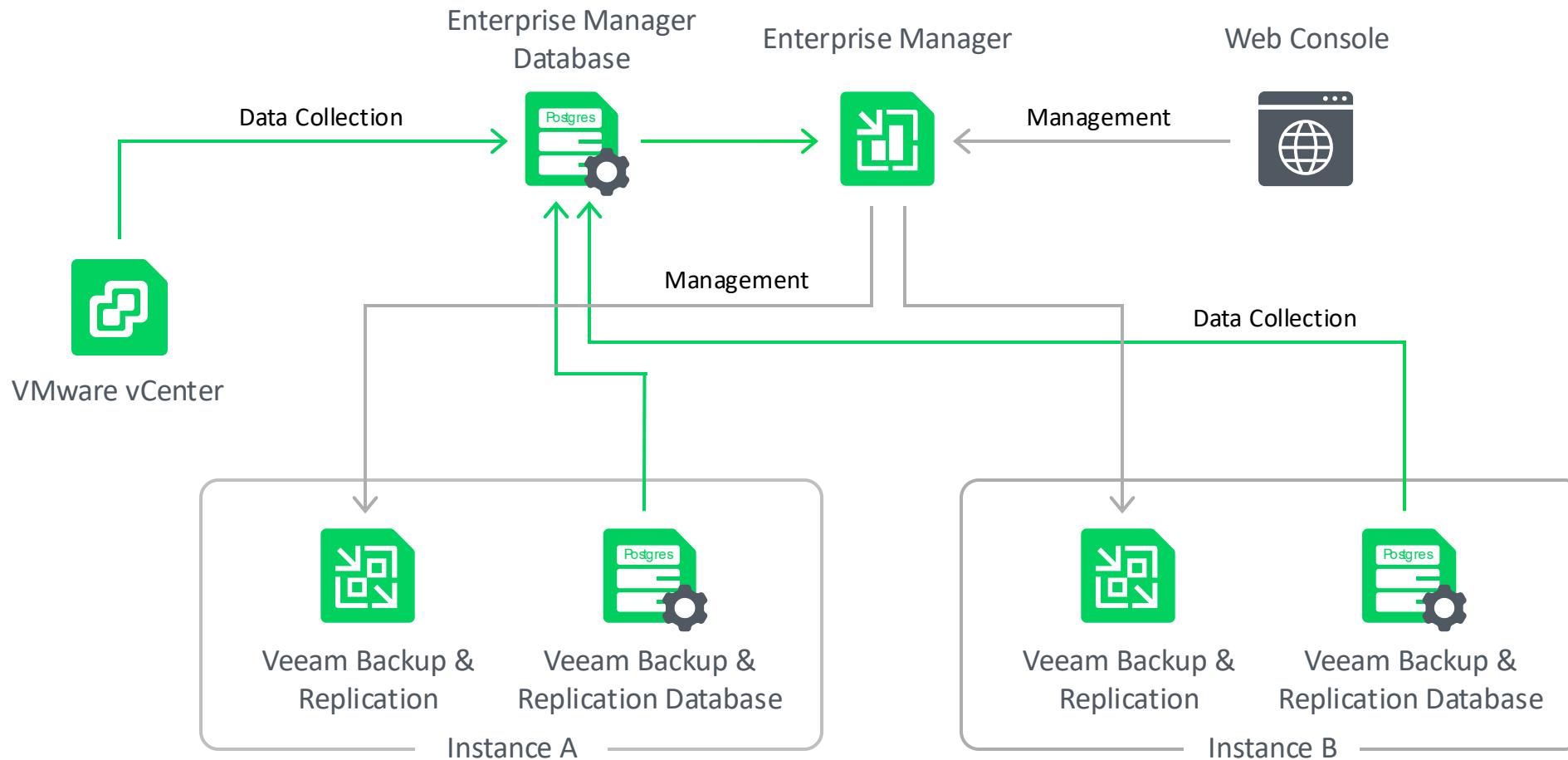
Veeam Enterprise Manager

Instalación



Veeam Enterprise Manager

Ejemplo de Despliegue (Relaciones Lógicas)



Veeam Enterprise Manager

Capacidades

The screenshot shows the Veeam Enterprise Manager interface for restoring mailbox items. The top navigation bar includes links for Dashboard, Reports, Jobs, Policies, Unstructured Data, Machines, Files, Items (selected), and Requests. The user is logged in as DEMOCENTER\achraf.akrout. A green arrow points upwards from the 'Items' tab to the 'Mailbox Items' section.

In the 'Mailbox Items' section, there is a 'Username:' field containing 'Enter username' with a magnifying glass icon. Below it is an 'Accounts:' section with a yellow header bar stating 'Available accounts will be shown after specifying a username'. A green arrow points upwards from this section towards the 'History' button.

The main restore area has a 'Restore point:' dropdown set to 'No restore point selected' with a calendar icon. It includes a 'History' button with a circular arrow icon. Below are sections for selecting 'Items:' (Mail, Calendar, Contacts) and a checkbox for 'Only restore missing items created or received' with a date range dropdown set to 'Yesterday'. A 'Restore' button is at the bottom.

Veeam Enterprise Manager

Capacidades. Configuración.

The screenshot shows the Veeam Enterprise Manager interface with the 'Self-Service' menu item selected. A modal dialog titled 'Delegation Mode' is open, overlaid on the main configuration screen. The dialog contains settings for delegation modes based on vSphere tags, roles, or privileges. The main configuration screen shows a list of accounts with their respective quotas and delegation modes.

Delegation Mode Options:

- vSphere tags: Users can manage all VMs with tags specified in the corresponding self-service configuration.
- vSphere role: Select Role...
- VM privilege: Select Privilege...

Account Configuration Table:

Quota	Per-user
100 GB	No
100 GB	No
200 GB	No
20 GB	No
10 GB	No
100 GB	No
100 GB	No
100 GB	No
100 GB	No
100 GB	No
100 GB	No
100 GB	No

Veeam Enterprise Manager

Capacidades. Configuración.

The screenshot shows the Veeam Enterprise Manager interface. The top navigation bar includes links for Dashboard, Reports, Jobs, Services, Unstructured Data, Machines (highlighted in green), Files, Items, and Requests. A green arrow points to the 'Machines' tab. On the left, a sidebar lists various configuration options: Exit Configuration, Backup Servers, vCenter Server, Self-Service, Sessions, Roles, Settings, Licensing (highlighted in green), Notifications, and About. Another green arrow points to the 'Licensing' option. The main content area displays a summary of backup instances for the host 'hq-vbr1.demolab.local'. It shows 46 instances in total, with 22 being virtual machines. A green arrow points to the 'Virtual Machines' section. A table provides details for each VM instance, including its name, number of instances, type (vSphere), job name, and last processed date. The table data is as follows:

Name	Instances	Type	Job name	Last processed
demo-linuxvm101	1	vSphere	VMware - Backup from 3PAR Snapshot	01/08/2024
demo-linuxvm102	1	vSphere	VMware - Backup from IBM Snapshot	01/08/2024
demo-linuxvm103	1	vSphere	VMware - Backup from NetApp Snapshot	01/08/2024
demo-linuxvm107	1	vSphere	VMware - Backup from VNX Snapshot	01/08/2024
demo-linuxvm109	1	vSphere	VMware - Backup from ETERNUS Snapshot	01/08/2024
demo-sql106	1	vSphere	VMware - Backup from Pure Snapshot	01/08/2024
demo-winvm101	1	vSphere	VMware - Backup from 3PAR Snapshot	01/08/2024
demo-winvm102	1	vSphere	VMware - Backup from IBM Snapshot	01/08/2024
demo-winvm103	1	vSphere	VMware - Backup from NetApp Snapshot	01/08/2024
demo-winvm105	1	vSphere	VMware - Backup from Nimble Snapshot	01/08/2024
demo-winvm106	1	vSphere	VMware - Backup from Pure Snapshot	01/08/2024
demo-winvm107	1	vSphere	VMware - Backup from VNX Snapshot	01/08/2024
demo-winvm108	1	vSphere	VMware - Backup from VSAN	01/08/2024
demo-winvm109	1	vSphere	VMware - Backup from ETERNUS Snapshot	01/08/2024
exch1	1	vSphere	VMware - Backup to XFS Repository	01/08/2024
fc1	1	vSphere	VMware - Backup to YFS Repository	01/08/2024

Menú Principal

Menú Principal

Credenciales & Contraseñas

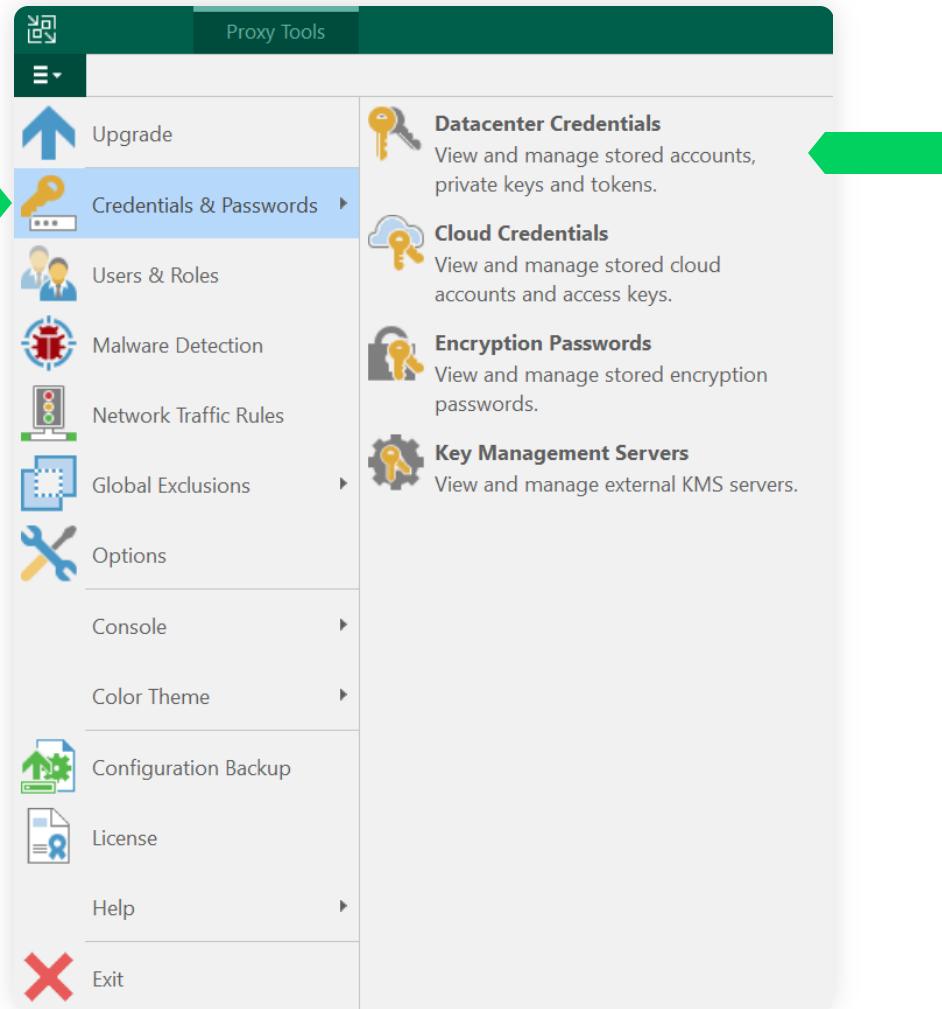
The screenshot shows the Veeam Backup & Replication software interface. A green arrow with the number '1' points to the 'Backup Proxy' tab in the top navigation bar. The main pane displays the 'Backup Infrastructure' section, specifically the 'Backup Proxies' list. The list includes the following entries:

Name	Type	Host
hq-vbr1appl1.demolab.local	Agent	hq-vb
hq-vbr1appl1.demolab.local	VMware	hq-vb
hq-vbr1lnxpxy1.demolab.local	VMware	hq-vc
hq-vbr1pxy1.demolab.local	VMware	hq-vb
hq-vbr1pxy3.demolab.local	VMware	hq-vb
hq-vbr1ntbpxy1	Nutanix AHV	pdcse

The left sidebar contains a tree view of the backup infrastructure, with 'Backup Proxies' selected. The bottom navigation bar shows the following items: Home, Inventory, Backup Infrastructure (selected), Storage Infrastructure, Tape Infrastructure, and Files. The status bar at the bottom indicates '6 proxies'.

Menú Principal

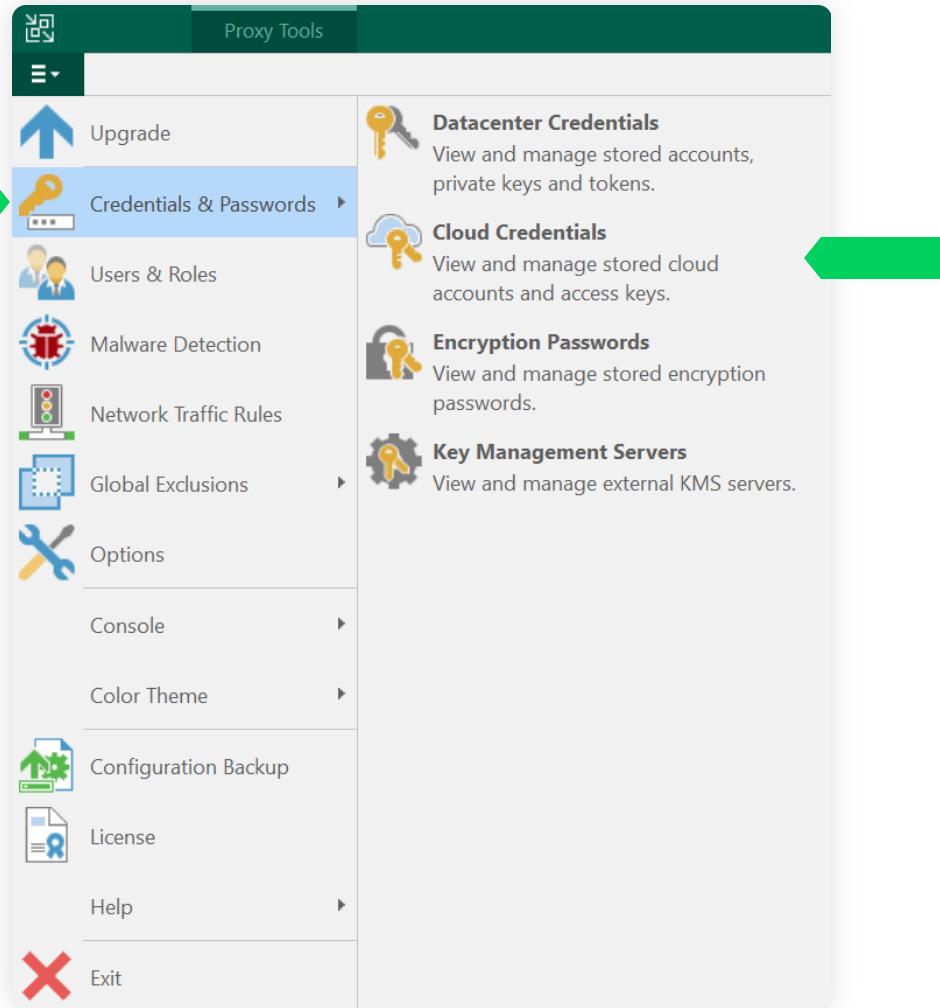
Credenciales & Contraseñas



Puede utilizar esta opción para crear y mantener una lista de registros de credenciales que planea utilizar para conectarse a los componentes de la infraestructura de copia de seguridad.

Menú Principal

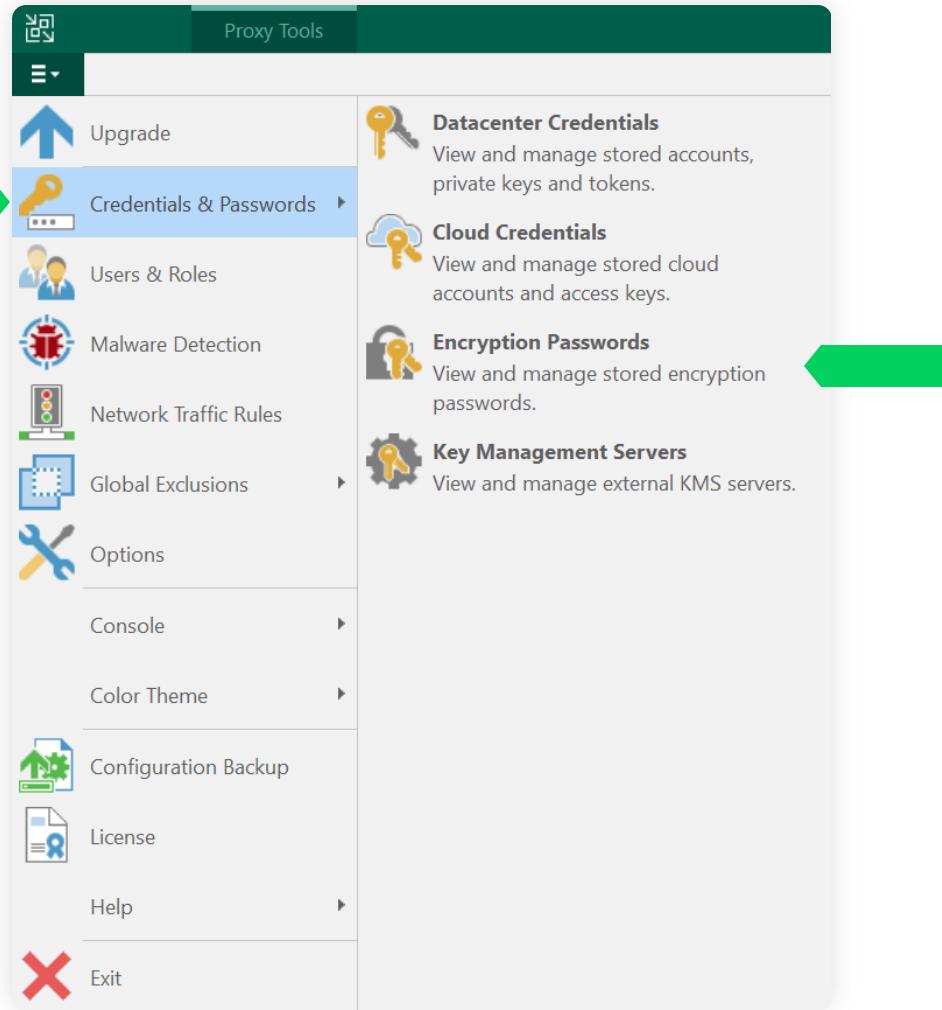
Credenciales & Contraseñas



Puedes utilizar esta opción para crear y mantener una lista de registros de credenciales que planeas utilizar para conectarte a servicios en la nube.

Menú Principal

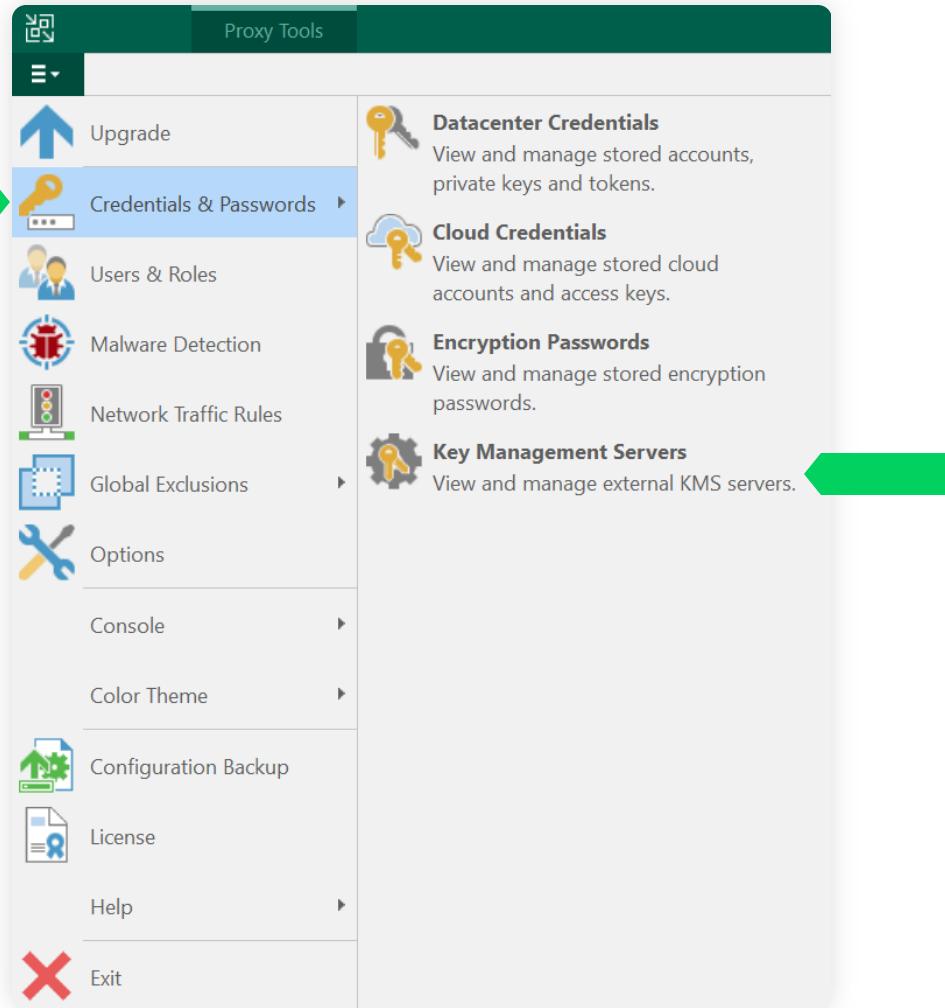
Credenciales & Contraseñas



Puede utilizar esta opción para crear y mantener una lista de contraseñas que planea utilizar para el cifrado de datos.

Menú Principal

Credenciales & Contraseñas



Puede utilizar esta opción para añadir servidores KMS y utilizar claves KMS.

Menú Principal

Usuarios y Roles

The screenshot shows the Veeam Backup & Replication software interface. A green arrow labeled '1' points to the 'Backup Infrastructure' section in the left sidebar. The main pane displays a table of backup proxies with columns for Name, Type, and Host. The table includes entries for various hosts like hq-vbr1appl1, hq-vbr1lnpxy1, hq-vbr1pxy1, hq-vbr1pxy3, and hq-vbr1ntpxy1, categorized by type (Agent, VMware, Nutanix AHV) and host.

Name	Type	Host
hq-vbr1appl1.demolab.local	Agent	hq-vb
hq-vbr1appl1.demolab.local	VMware	hq-vb
hq-vbr1lnpxy1.demolab.local	VMware	hq-vb
hq-vbr1pxy1.demolab.local	VMware	hq-vb
hq-vbr1pxy3.demolab.local	VMware	hq-vb
hq-vbr1ntpxy1	Nutanix AHV	pdcse

Backup Infrastructure

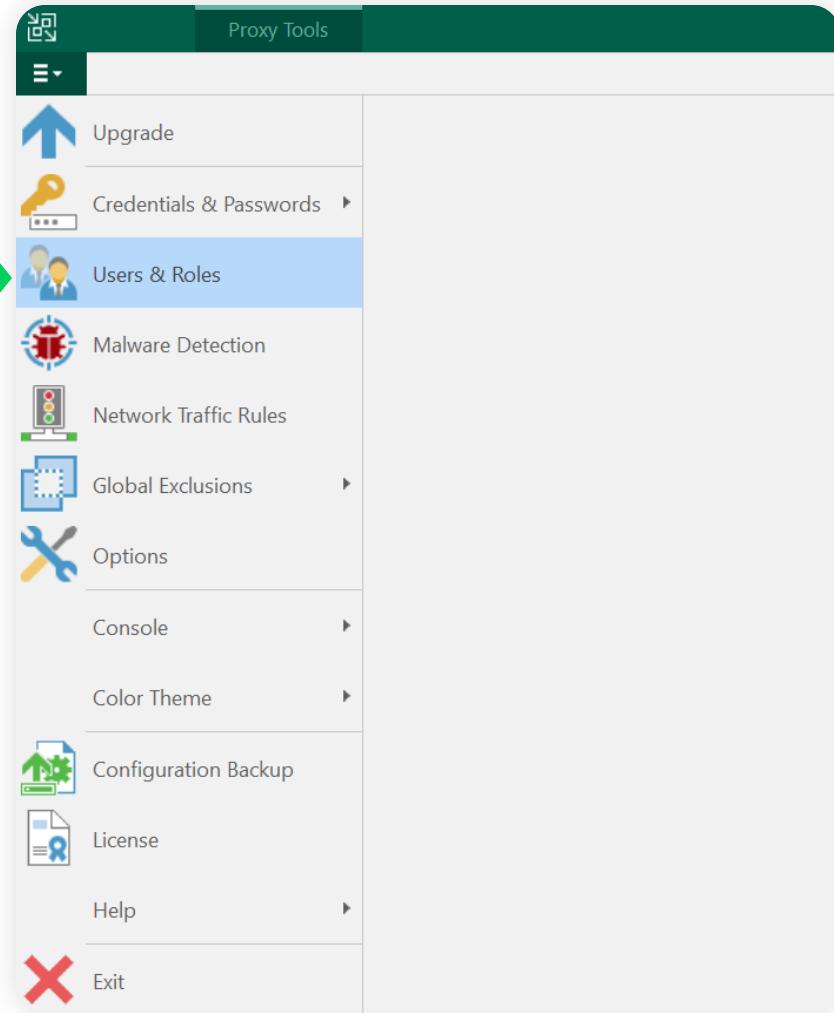
- Backup Proxies
- Backup Repositories
- External Repositories
- Scale-out Repositories
 - AWS S3 Repository
 - SOBR
 - SOBR with Azure Capacity Tiers
- WAN Accelerators
- Service Providers
- SureBackup
 - Application Groups
 - Virtual Labs
- Managed Servers
 - VMware vSphere
 - vCenter Servers
 - vc1.democenter.int
 - vc1.demolab.local
 - VMware Cloud Director

Navigation: Home, Inventory, Backup Infrastructure (selected), Storage Infrastructure, Tape Infrastructure, Files.

6 proxies

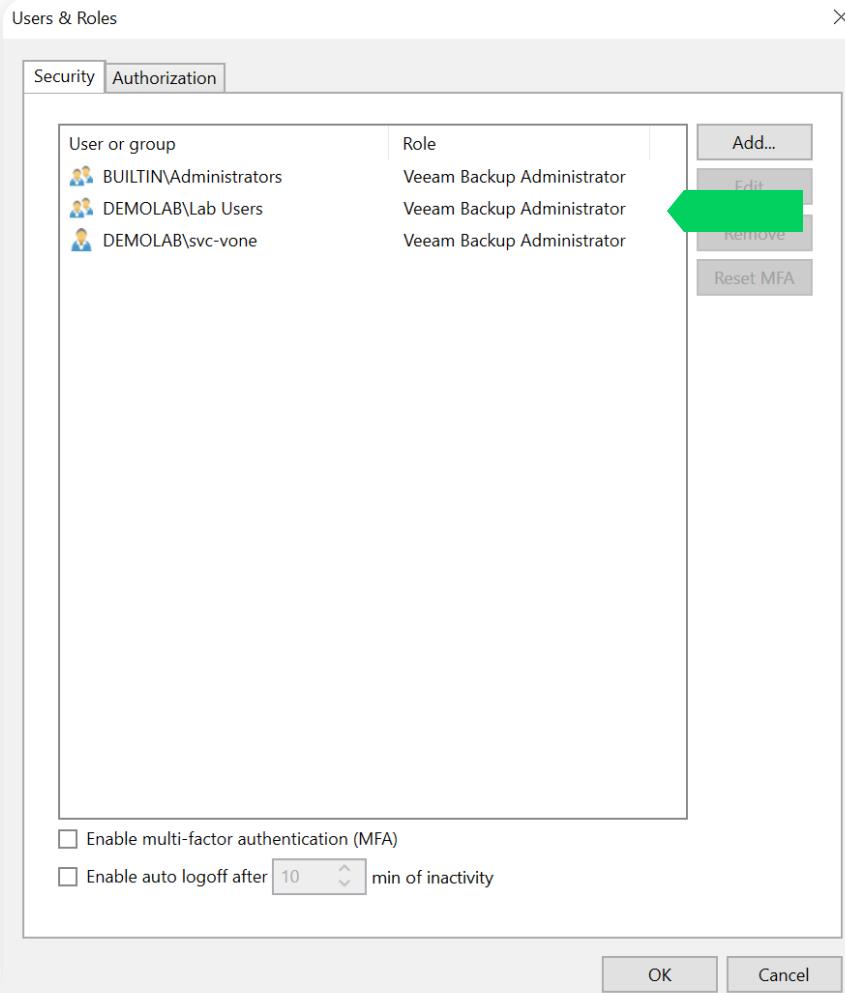
Menú Principal

Usuarios y Roles



Menú Principal

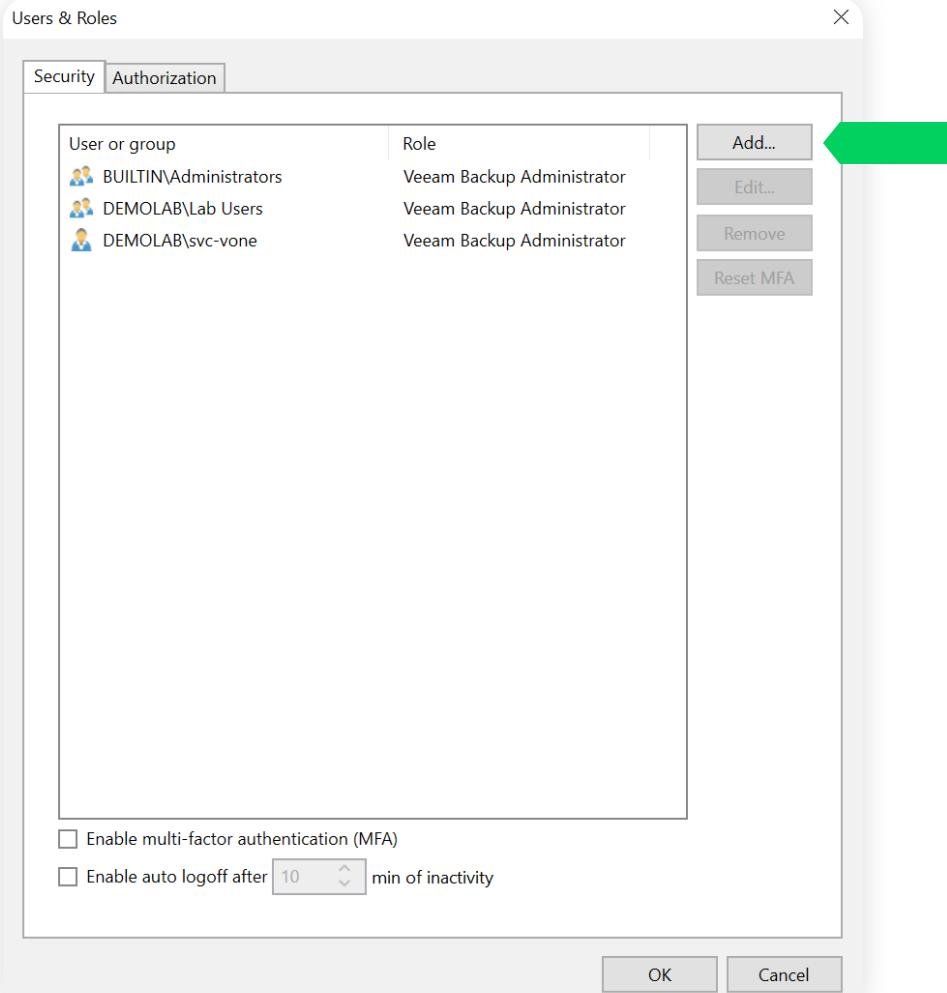
Usuarios y Roles



Se puede observar una lista de todos los usuarios y grupos de usuarios con sus roles específicos; los roles definirán las operaciones de Veeam Backup & Replication que tienen derecho a realizar.

Menú Principal

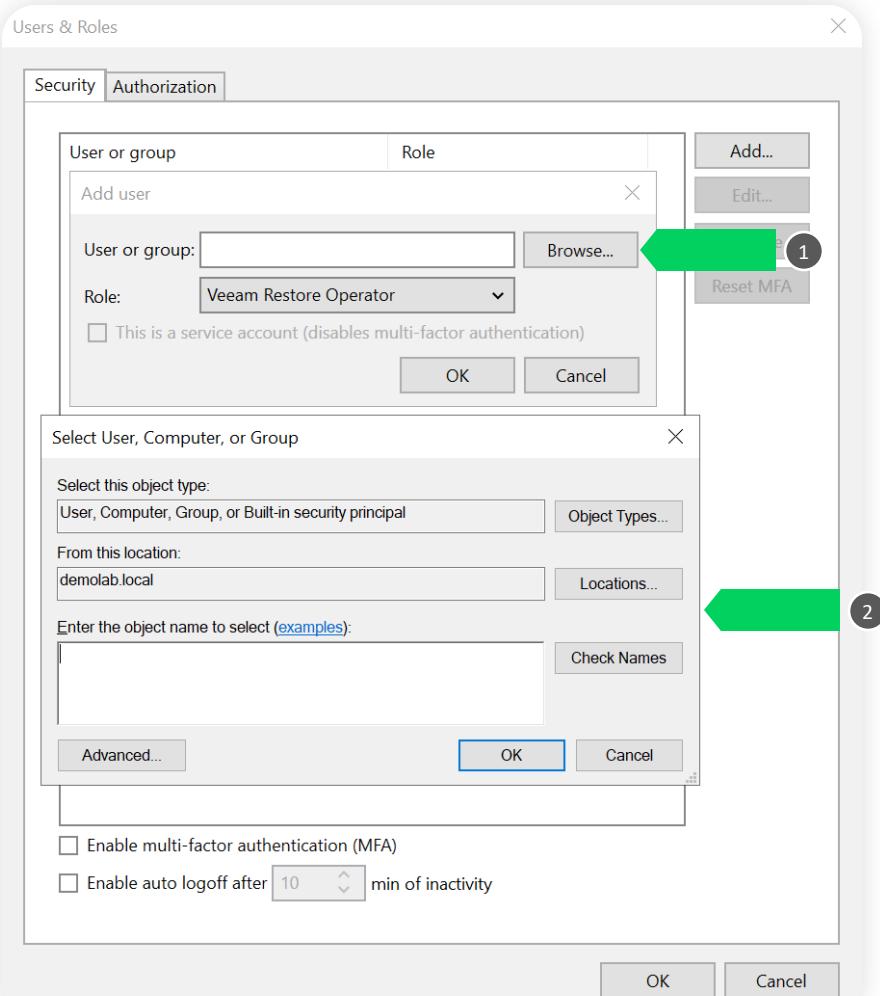
Usuarios y Roles



Puede añadir nuevos usuarios o grupos de usuarios.

Menú Principal

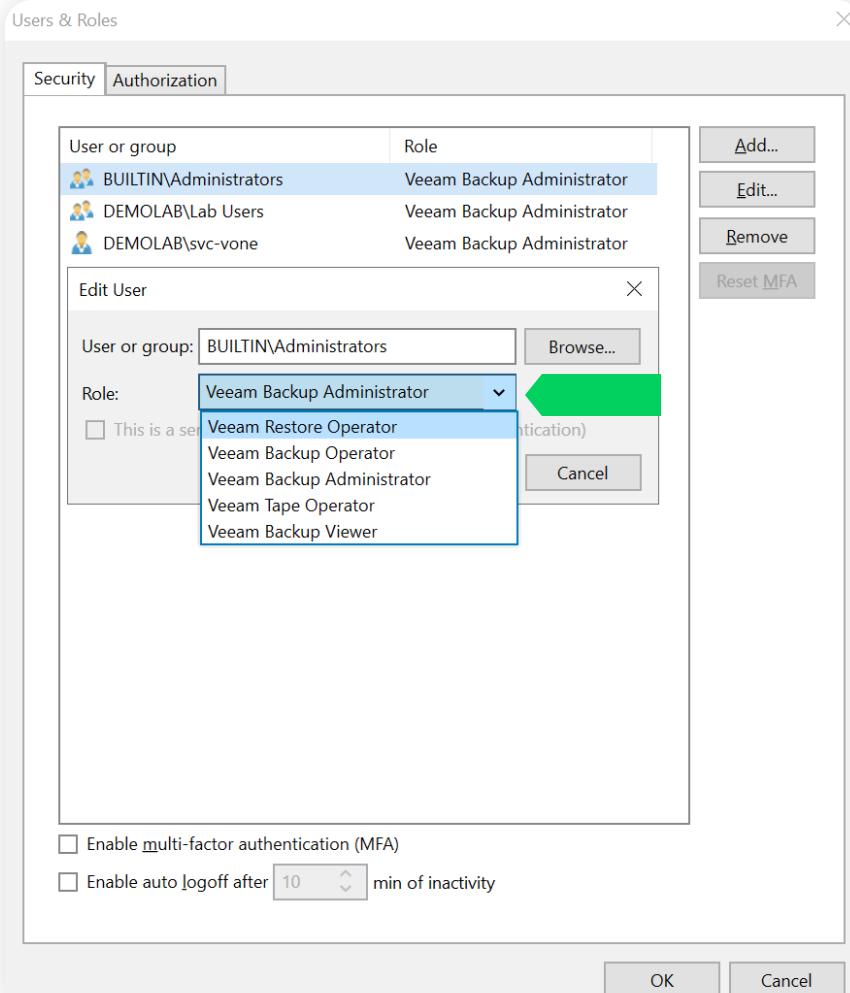
Usuarios y Roles



Puede añadir el usuario o grupo de usuarios especificándolo en el formato DOMINIO\USUARIO o buscarlo.

Menú Principal

Usuarios y Roles



Editando un usuario o grupo de usuarios existente permitirá cambiar el formato DOMINIO/USUARIO y el rol.

Respecto a los roles, hay cinco opciones:

- **Restore operator** – que permite que los procesos de restauración sean realizados por el usuario/grupo de usuarios específico
- **Backup operator** – responsable de iniciar y detener los trabajos de copia de seguridad, así como de exportar y copiar copias de seguridad y crear copias de seguridad VeeamZIP
- **Backup administrator** – capaz de realizar todas las actividades administrativas y con acceso completo a todo lo añadido a la infraestructura de copia de seguridad
- **Tape operator** – responsable de cualquier operación de cinta y de iniciar o detener trabajos de cinta
- **Backup viewer** – que tiene el acceso de «sólo lectura» a la consola

Menú Principal

Reglas de la Red Global

The screenshot shows the Veeam Backup & Replication software interface. A green arrow labeled '1' points to the 'Backup Proxy' tab in the top navigation bar. The main content area displays the 'Global Network Rules' configuration, which lists various proxies and their details. The interface includes a sidebar with navigation links like Home, Inventory, and Backup Infrastructure.

1

Proxy Tools

Home Backup Proxy

Add Edit Disable Remove Upgrade

Proxy Proxy Proxy

Manage Proxy Upgrade

Backup Infrastructure

Type in an object name to search for

Name	Type	Host
hq-vbr1appl1.demolab.local	Agent	hq-vb
hq-vbr1appl1.demolab.local	VMware	hq-vb
hq-vbr1lnpxy1.demolab.local	VMware	hq-vb
hq-vbr1pxy1.demolab.local	VMware	hq-vb
hq-vbr1pxy3.demolab.local	VMware	hq-vb
hq-vbr1ntpxy1	Nutanix AHV	pdcse

Backup Proxies

Backup Repositories

External Repositories

Scale-out Repositories

- AWS S3 Repository
- SOBR
- SOBR with Azure Capacity Tiers

WAN Accelerators

Service Providers

- SureBackup
 - Application Groups
 - Virtual Labs

Managed Servers

- VMware vSphere
 - vCenter Servers
 - vc1.democenter.int
 - vc1.demolab.local
 - VMware Cloud Director

Home

Inventory

Backup Infrastructure

Storage Infrastructure

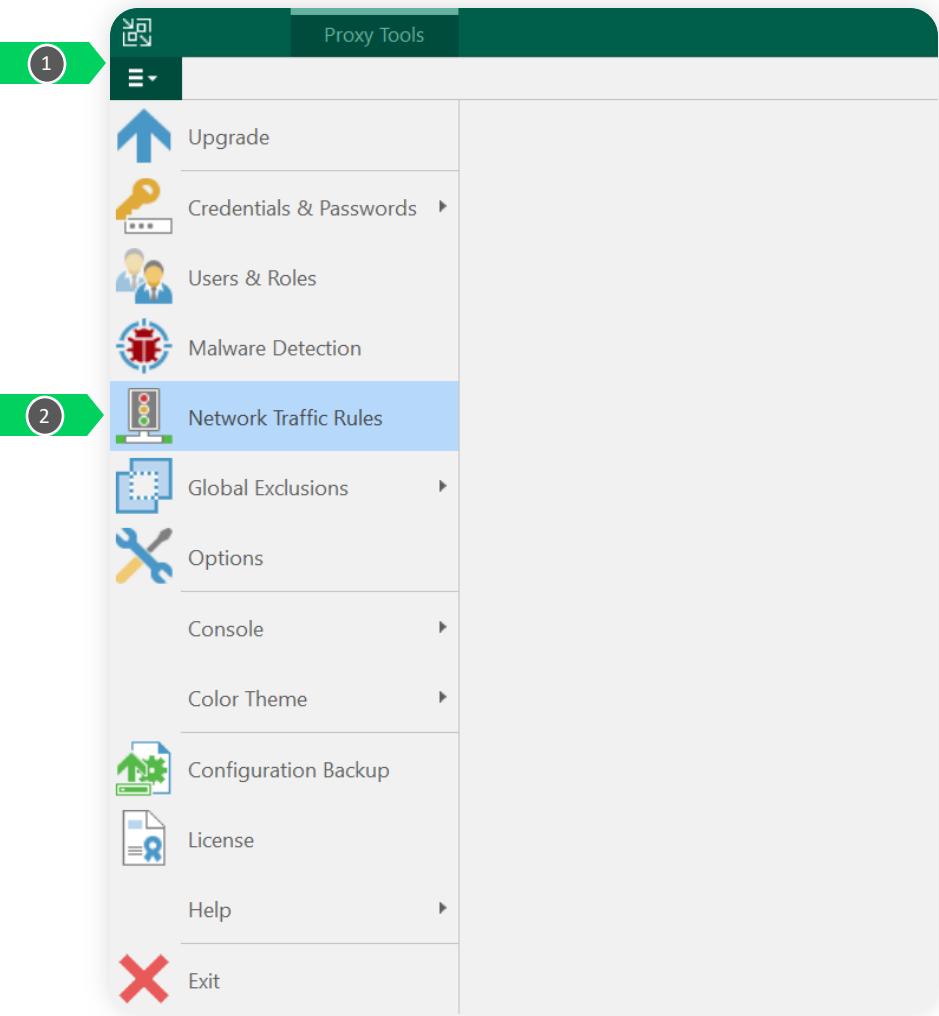
Tape Infrastructure

Files

6 proxies

Menú Principal

Reglas de la Red Global



Menú Principal

Reglas de la Red Global

Global Network Traffic Rules

Network traffic rules:

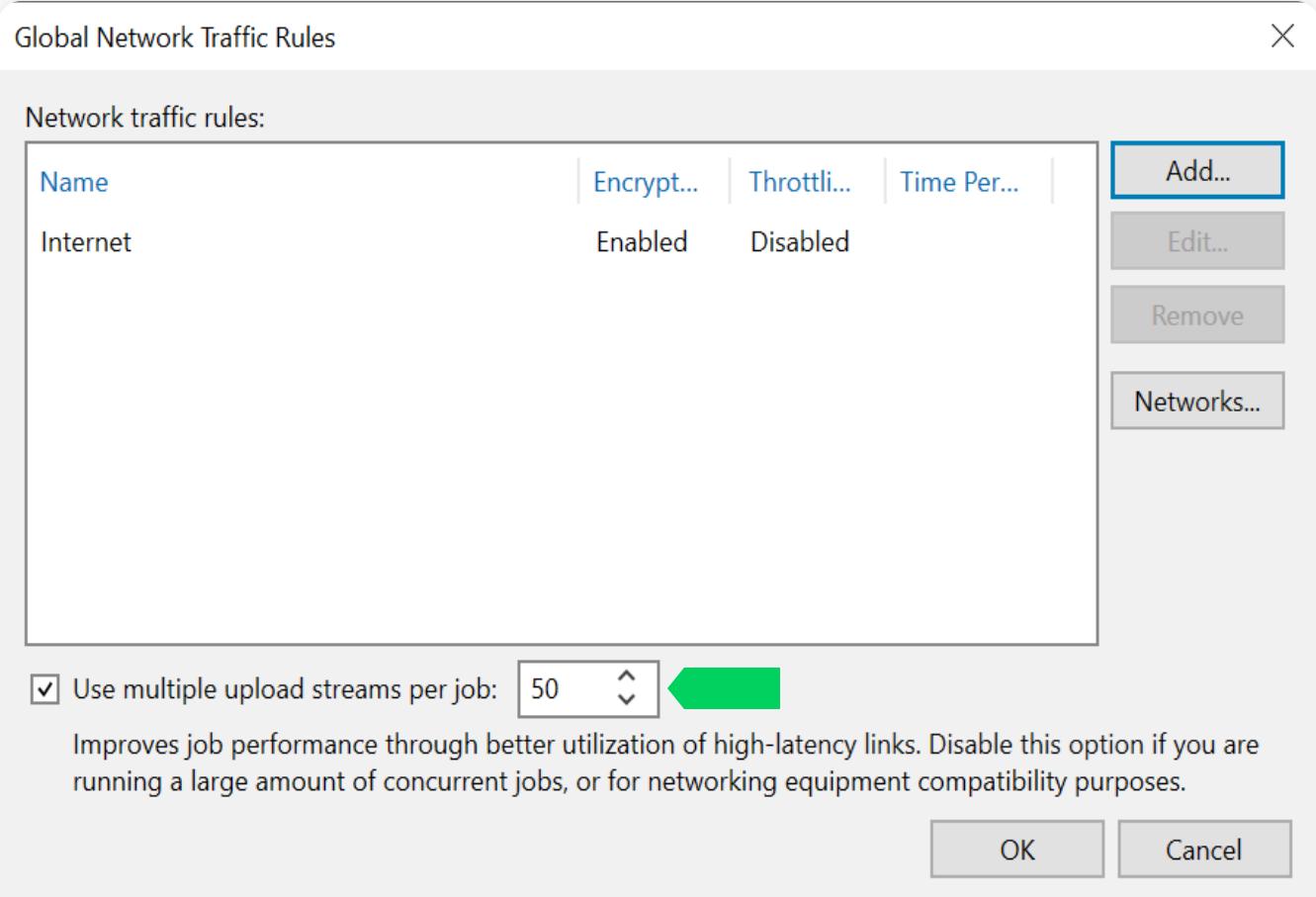
Name	Encrypt...	Throttli...	Time Per...
Internet	Enabled	Disabled	

Add... Edit... Remove Networks...

Use multiple upload streams per job: 50 ↕

Improves job performance through better utilization of high-latency links. Disable this option if you are running a large amount of concurrent jobs, or for networking equipment compatibility purposes.

OK Cancel

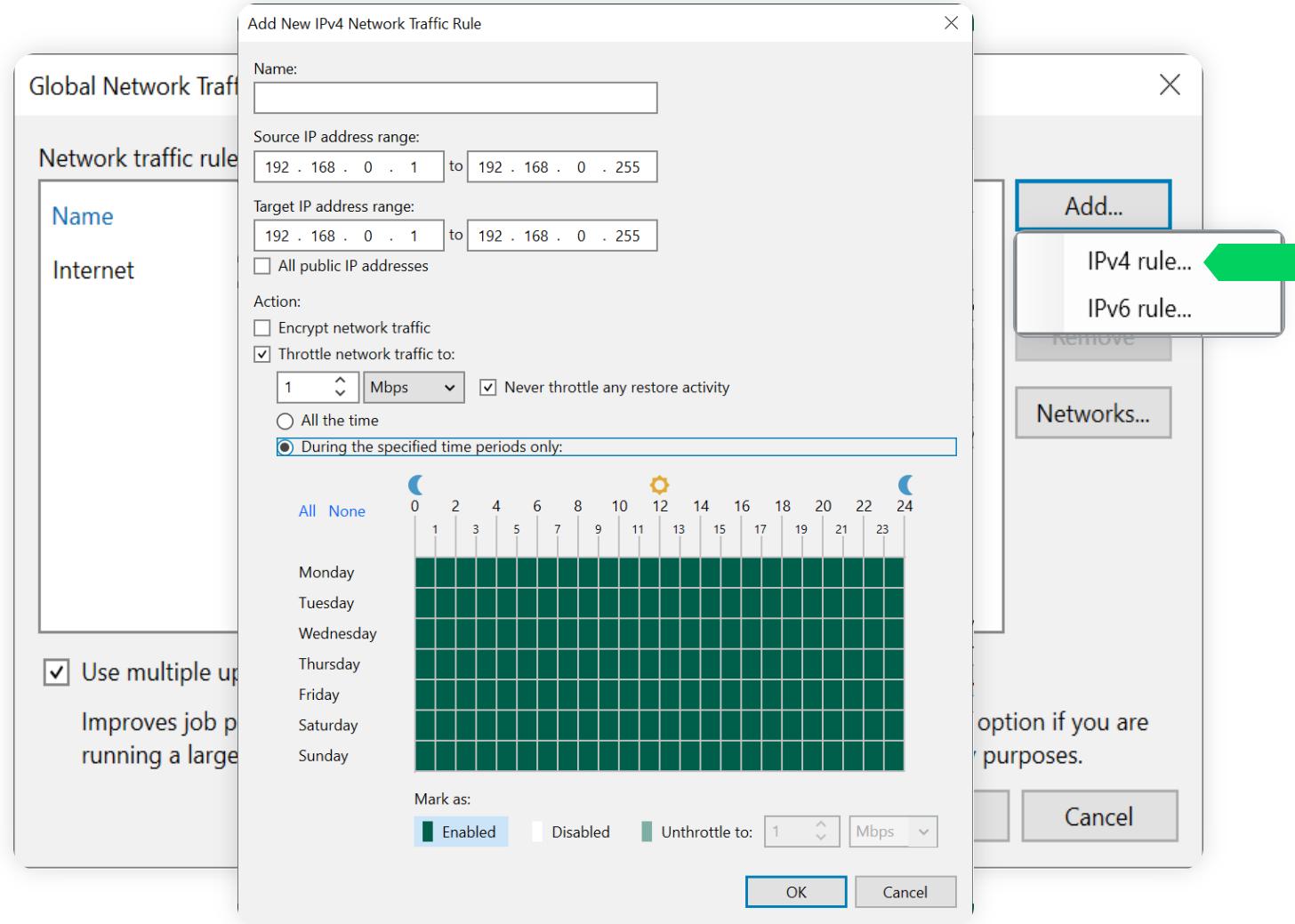


Por defecto, Veeam Backup & Replication utiliza la transferencia de datos multihilo para cada sesión de trabajo, desde el origen al destino a través de varias conexiones TCP/IP.

Si la capacidad de la red no es suficiente para soportar varias conexiones de transferencia de datos, puede desactivar la transferencia de datos multiproceso o cambiar el número de conexiones TCP/IP.

Menú Principal

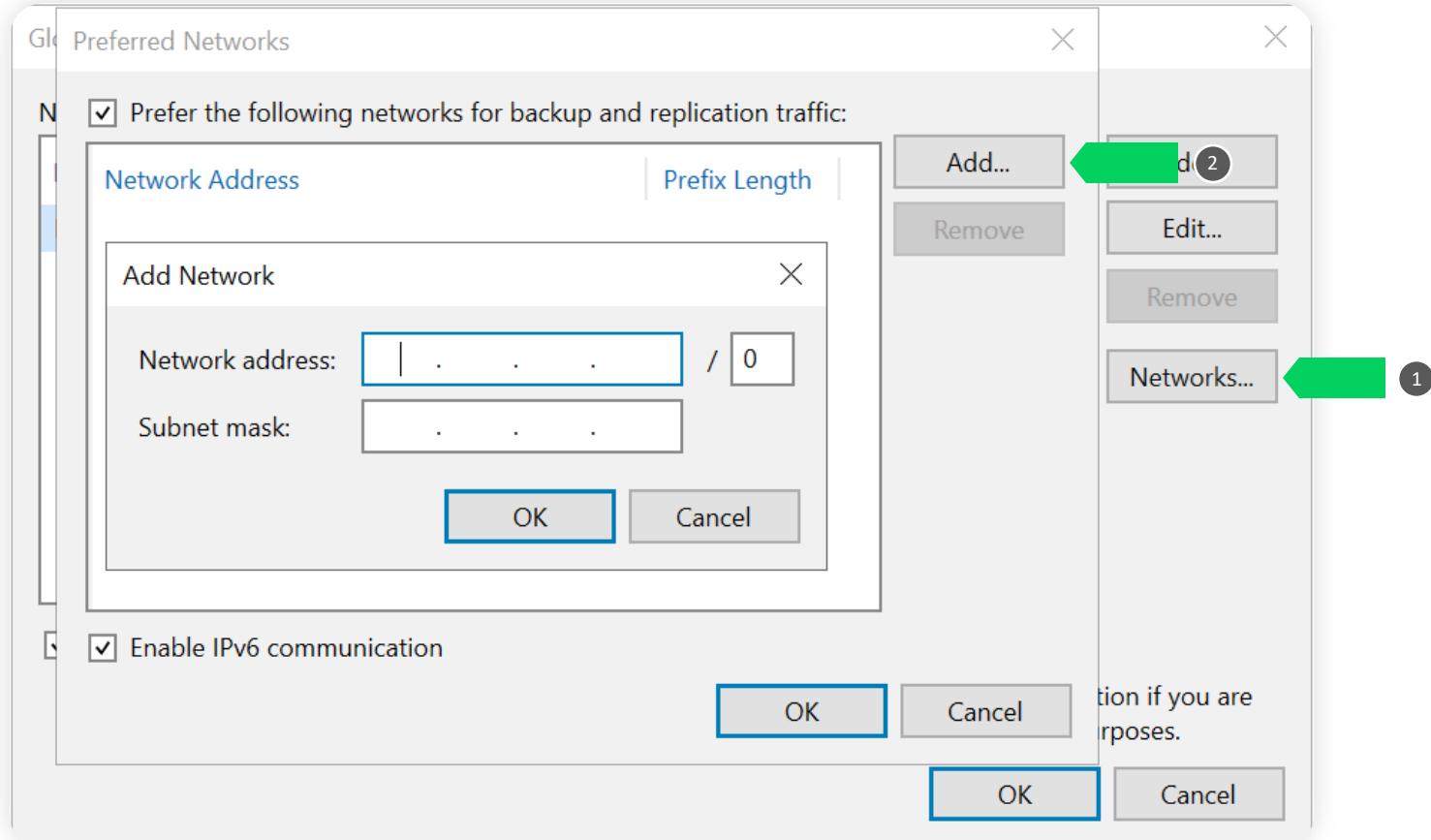
Reglas de la Red Global



Puede añadir diferentes reglas IPv4/6 especificando el rango para el origen y el destino y aplicando la encriptación del tráfico de red o limitándolo durante períodos específicos.

Menú Principal

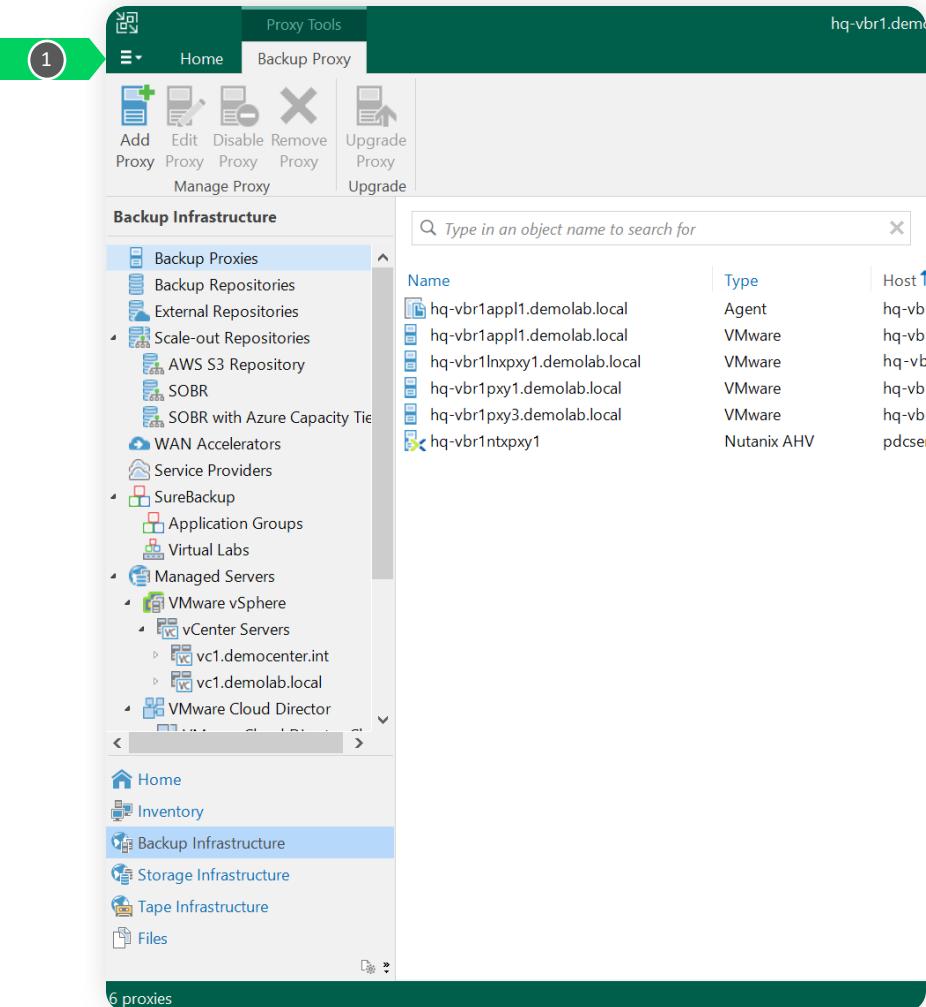
Reglas de la Red Global



También existe la posibilidad de especificar la red preferida para el tráfico de copia de seguridad y replicación.

Menú Principal

Exclusiones VM



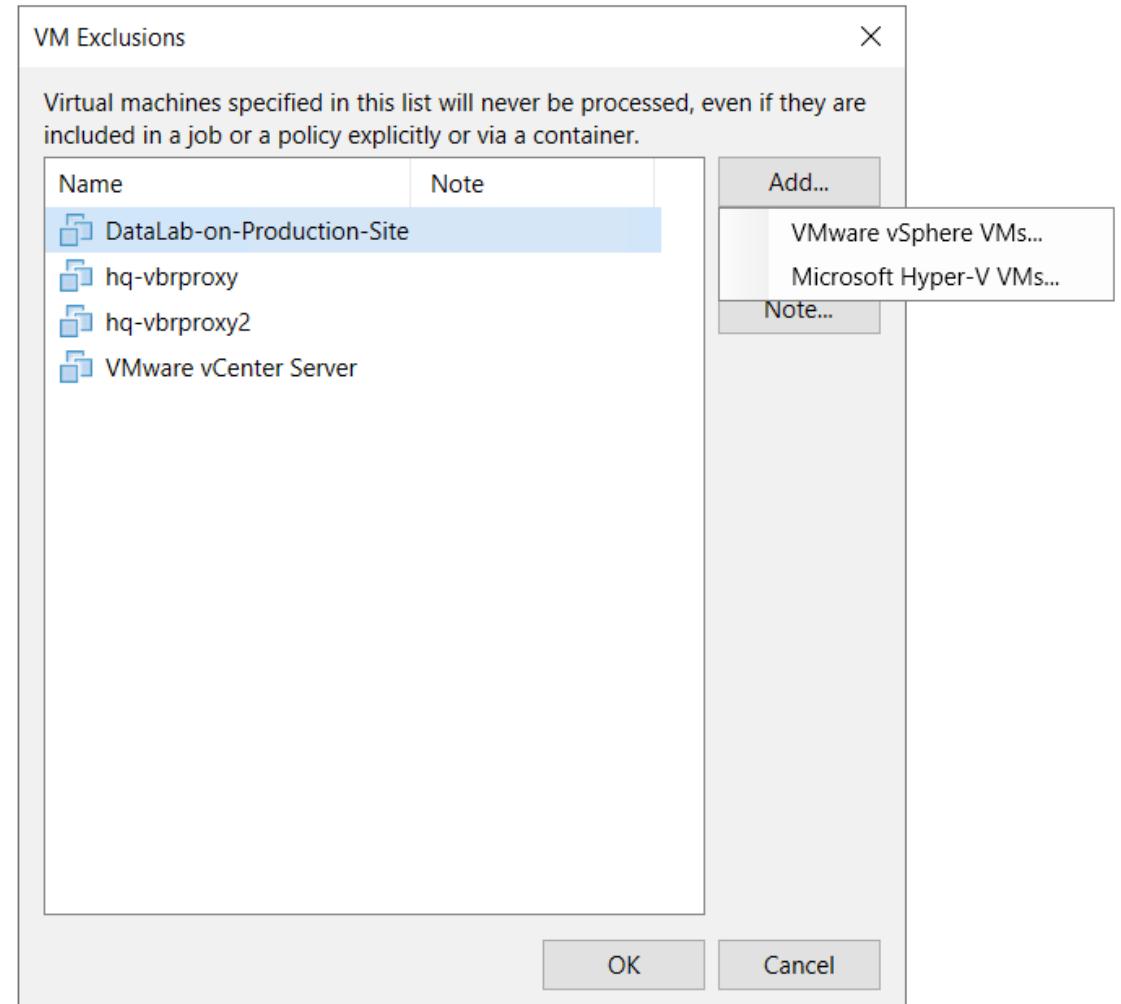
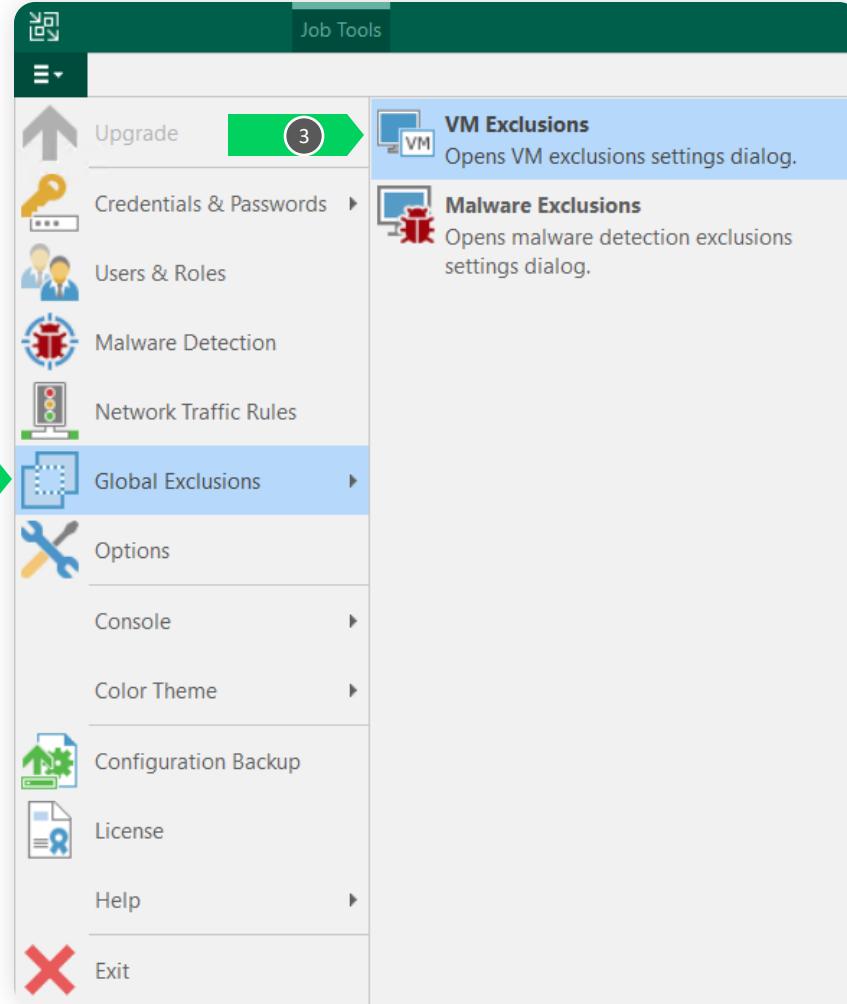
The screenshot shows the Veeam Backup & Replication software interface. The top navigation bar includes 'Proxy Tools', 'Home', 'Backup Proxy' (which is selected), and 'Backup Infrastructure'. Below the navigation bar is a toolbar with icons for 'Add', 'Edit', 'Disable', 'Remove', 'Upgrade', 'Proxy', 'Proxy', 'Proxy', and 'Manage Proxy'. The main pane displays the 'Backup Infrastructure' section, specifically the 'Backup Proxies' list. A search bar at the top of the list allows for searching by object name. The list contains the following entries:

Name	Type	Host
hq-vbr1appl1.demolab.local	Agent	hq-vb
hq-vbr1appl1.demolab.local	VMware	hq-vb
hq-vbr1lnxpxy1.demolab.local	VMware	hq-vc
hq-vbr1pxy1.demolab.local	VMware	hq-vb
hq-vbr1pxy3.demolab.local	VMware	hq-vb
hq-vbr1ntbpxy1	Nutanix AHV	pdcse

The left sidebar contains a tree view of the backup infrastructure, with 'Backup Proxies' currently selected. Other items in the tree include 'Backup Repositories', 'External Repositories', 'Scale-out Repositories', 'AWS S3 Repository', 'SOBR', 'SOBR with Azure Capacity Tiers', 'WAN Accelerators', 'Service Providers', 'SureBackup', 'Managed Servers', 'VMware vSphere', 'vCenter Servers', 'VMware Cloud Director', and 'Cloud Connectors'. The bottom left corner shows a status message '6 proxies'.

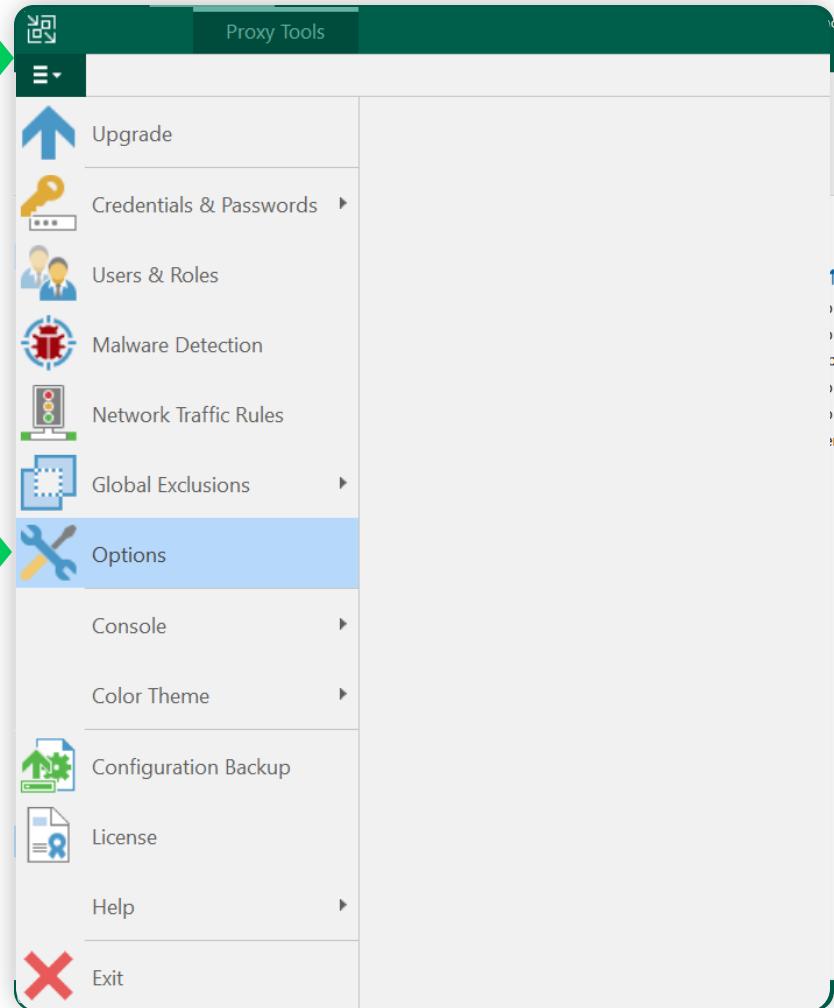
Menú Principal

Exclusiones VM



Menú Principal

Opciones



Menú Principal

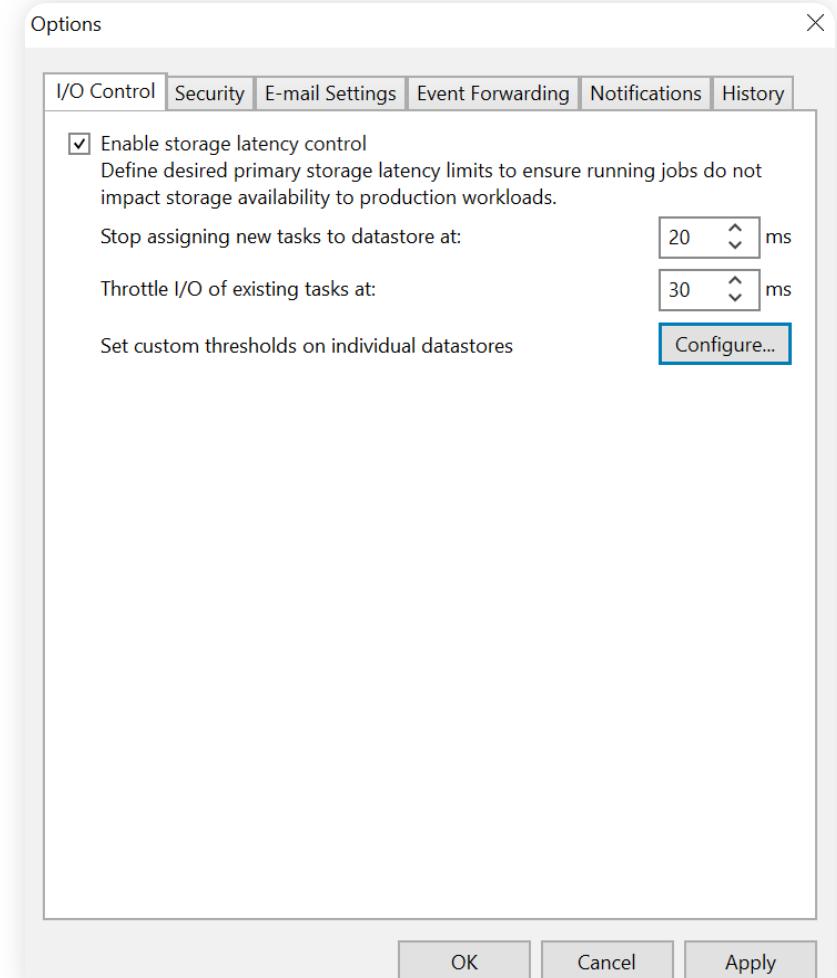
Opciones. Control I/O.

Cuando Storage Latency Control está activado, Veeam Backup & Replication supervisa la latencia de lectura del almacenamiento en los almacenes de datos de producción durante las actividades de protección de datos y recuperación ante desastres. Para supervisar la latencia del almacenamiento, Veeam Backup & Replication utiliza métricas en tiempo real del hipervisor donde residen las máquinas virtuales.

Stop assigning new tasks to datastore at – el límite de latencia de I/O en el que Veeam Backup & Replication no debe asignar nuevas tareas dirigidas al datastore.

Throttle I/O of existing tasks at – el límite de latencia de I/O en el que Veeam Backup & Replication debe reducir la velocidad de recuperación o escritura de datos en/desde el almacén de datos.

Las mismas opciones pueden configurarse para almacenes de datos individuales.



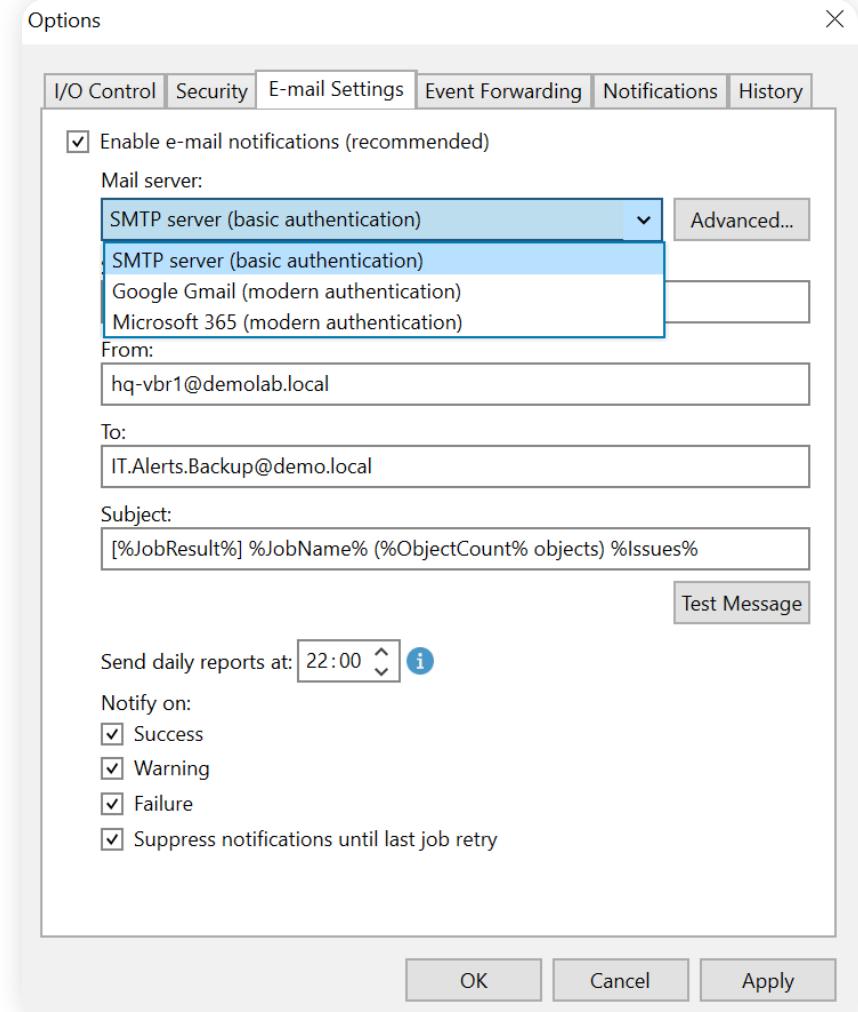
Menú Principal

Opciones. Ajustes de Correo Electrónico.

Veeam Backup & Replication también ofrece la posibilidad de enviar correos electrónicos que contengan informes diarios sobre el último estado de los trabajos de backup.

Por el momento, soportamos SMTP, Google Gmail y Microsoft 365 como los servidores de correo que se pueden utilizar para este fin.

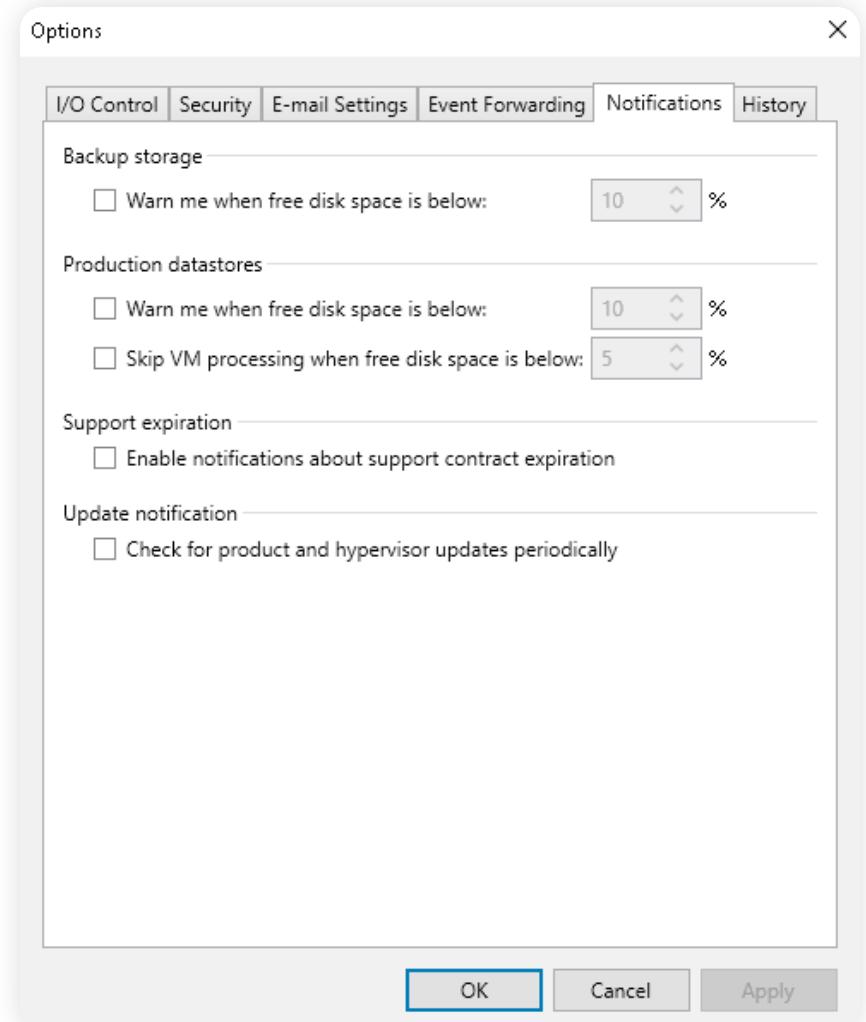
Desde esta pestaña se puede configurar el asunto del correo electrónico, los destinatarios, la dirección de correo electrónico del remitente y lo que debe contener el informe en cuanto al último estado que debe incluirse.



Menú Principal

Opciones. Notificaciones.

Veeam Backup & Replication también puede mostrar notificaciones directamente dentro de la consola cada vez que se alcanzan umbrales en el almacenamiento de copias de seguridad en los repositorios o datastores de producción, faltan 14 días para que finalice el soporte para la licencia instalada y está disponible la actualización para los hipervisores.

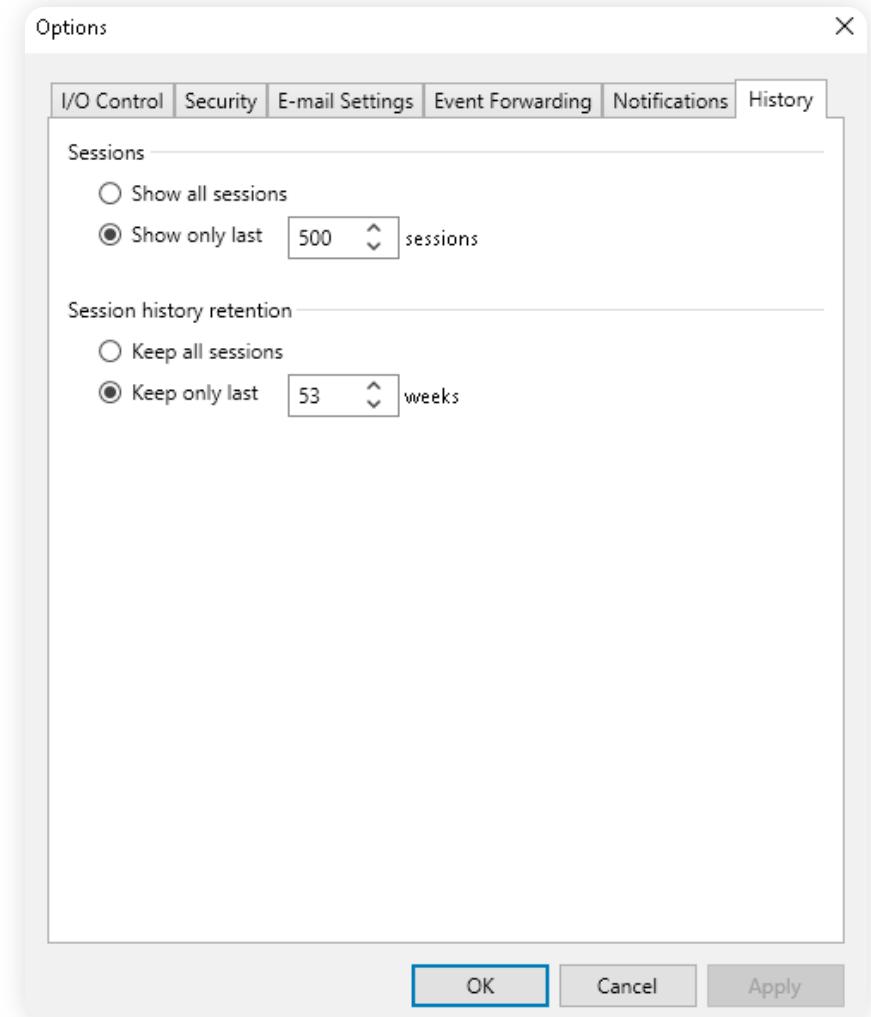


Menú Principal

Opciones. Historia.

El área **Sesiones** controla cuántas entradas deben ser visibles en la pestaña Historial de la consola de Veeam Backup & Replication.

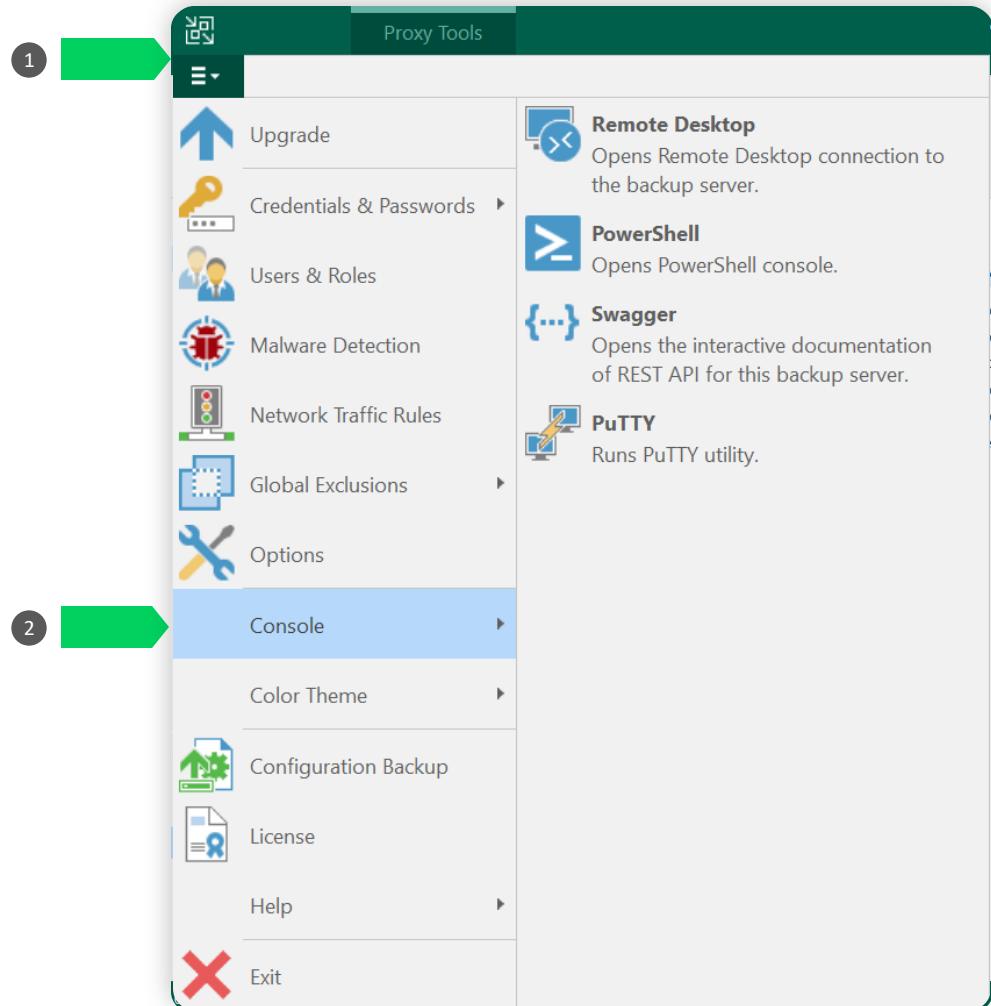
El área **Retención del historial** de sesiones dicta durante cuánto tiempo debe conservarse la información de la sesión en la base de datos.



Menú Principal

Consola.

Veeam Backup & Replication ofrece la posibilidad de abrir una conexión Remote Desktop al servidor de backup, abrir la consola PowerShell, ejecutar la utilidad PuTTY y abrir la documentación interactiva o las API REST para el servidor de backup directamente desde la consola.



Menú Principal

Respaldo de configuración.

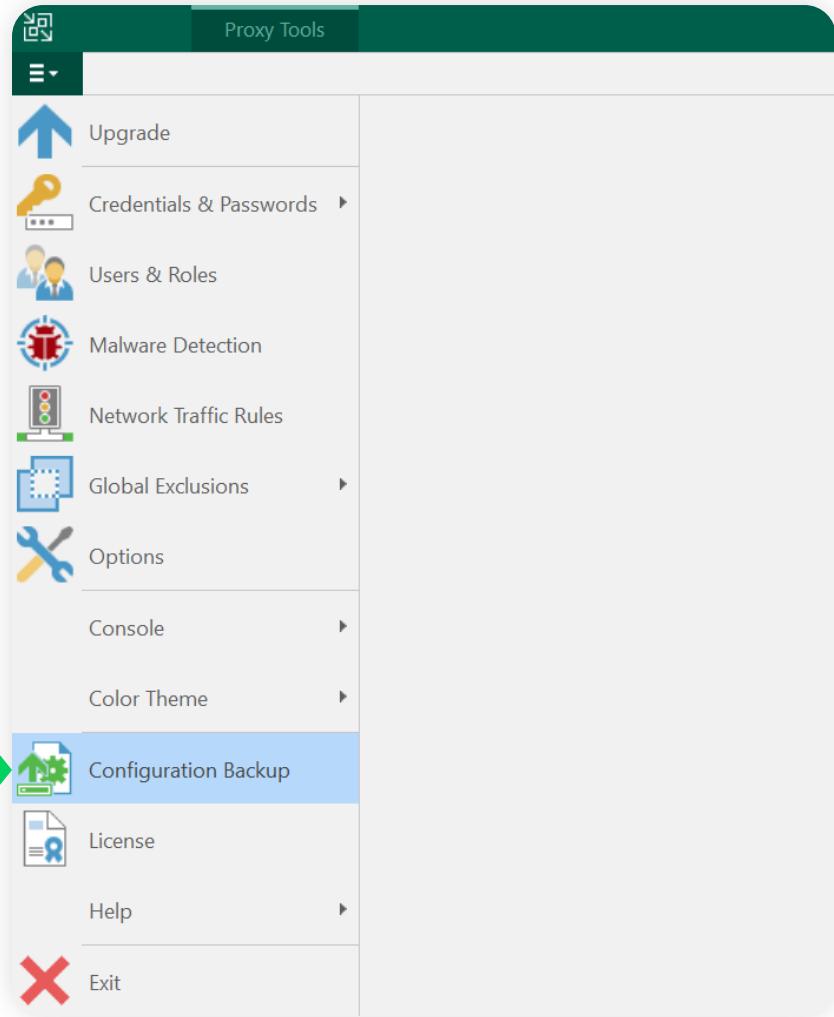
The screenshot shows the Veeam Backup & Replication software interface. A green arrow labeled '1' points to the 'Backup Proxy' tab in the top navigation bar. The main pane displays the 'Backup Infrastructure' tree view, with 'Backup Proxies' selected. A search bar at the top of the list allows searching for object names. The list shows the following proxies:

Name	Type	Host
hq-vbr1appl1.demolab.local	Agent	hq-vb
hq-vbr1appl1.demolab.local	VMware	hq-vb
hq-vbr1lnpxy1.demolab.local	VMware	hq-vb
hq-vbr1pxy1.demolab.local	VMware	hq-vb
hq-vbr1pxy3.demolab.local	VMware	hq-vb
hq-vbr1ntpxy1	Nutanix AHV	pdcse

The bottom left corner indicates there are 6 proxies.

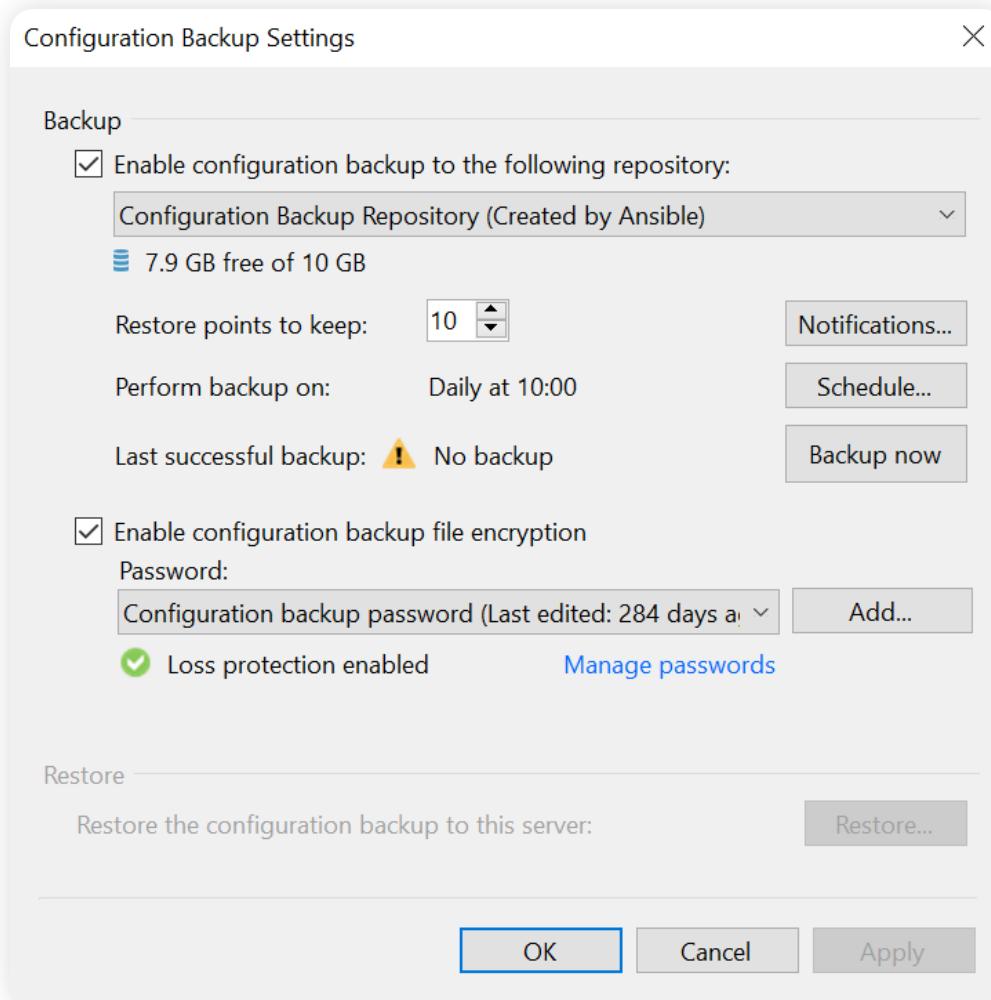
Menú Principal

Respaldo de configuración.



Menú Principal

Respaldo de configuración.



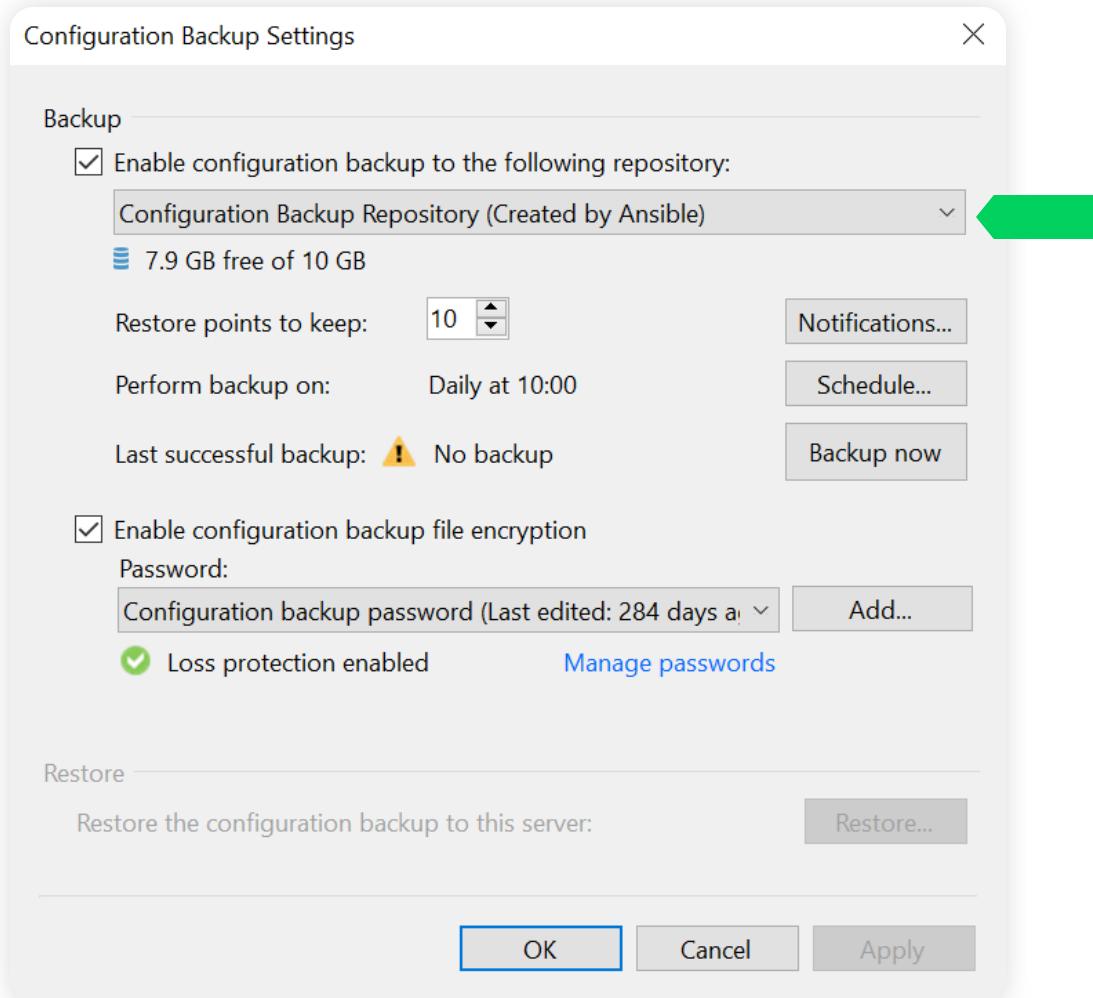
Veeam Backup & Replication almacena todos los cambios que se realizaron dentro de una consola en un servidor específico como una copia de seguridad de la configuración.

Si el servidor principal de Veeam Backup & Replication falla por algún motivo, se puede utilizar la copia de seguridad de configuración para restaurar rápidamente la configuración a una nueva.

Este método también es aconsejable si el servidor de Veeam Backup & Replication debe ser reemplazado o cambiado en el futuro.

Menú Principal

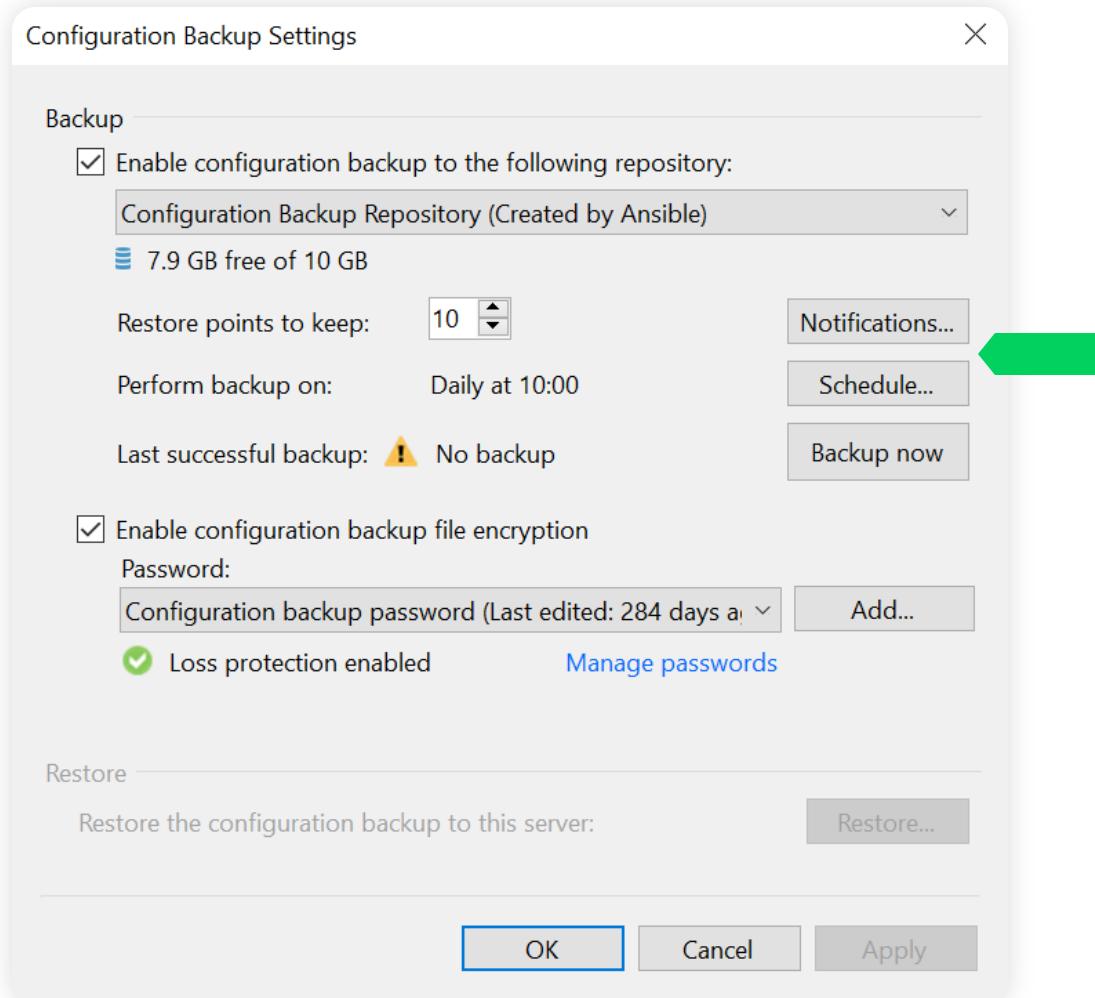
Respaldo de configuración.



Para almacenar el Respaldo de configuración, debe seleccionarse un repositorio.

Menú Principal

Respaldo de configuración.

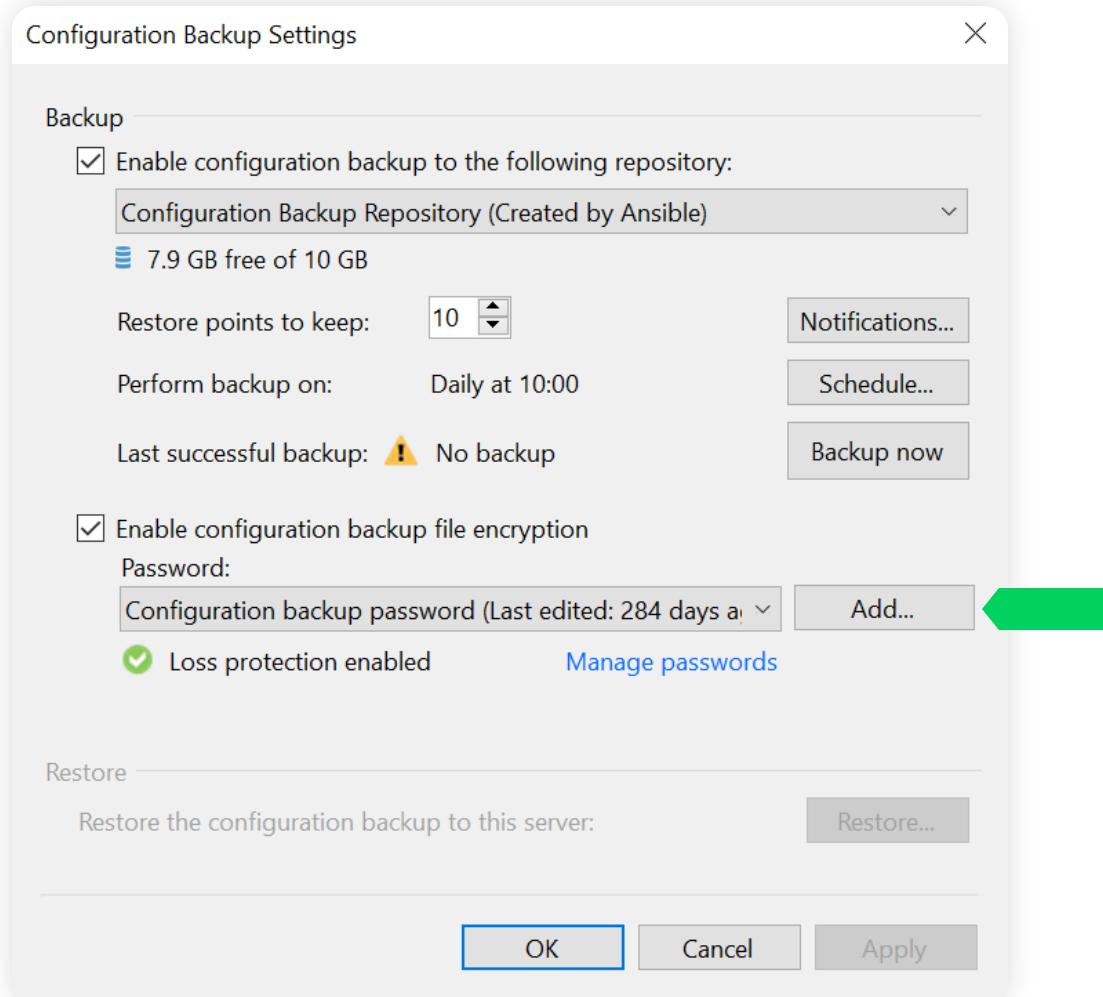


Las notificaciones SNMP y de E-mail para el Respaldo de configuración. pueden ser enviadas automáticamente.

También es una buena práctica programar la copia de seguridad para que se realice automáticamente, en lugar de confiar en las copias de seguridad manuales.

Menú Principal

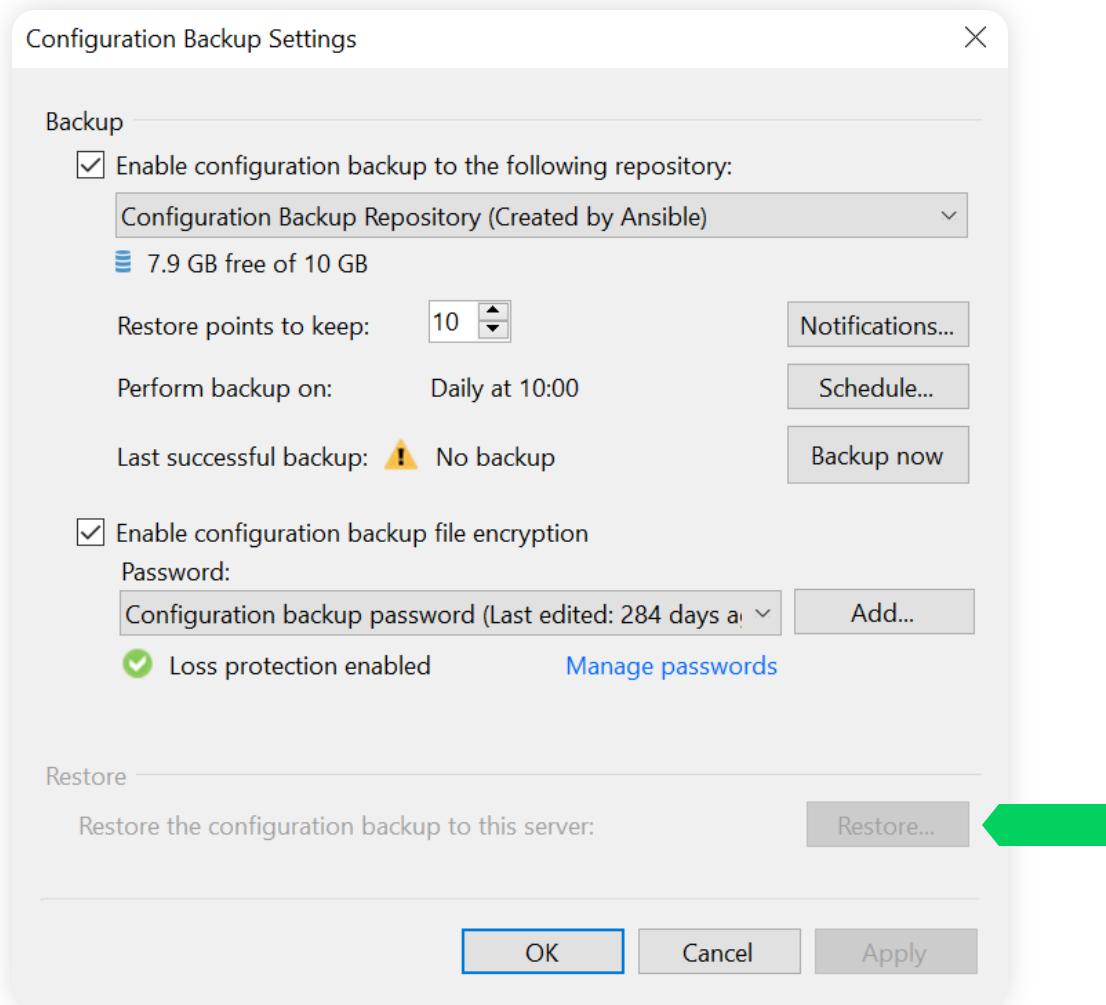
Respaldo de configuración.



Otra buena práctica es proteger el Respaldo de configuración mediante encriptación. Si se pierde la contraseña de cifrado, sólo Veeam Backup Enterprise Manager puede ayudar a recuperarla.

Menú Principal

Respaldo de configuración.



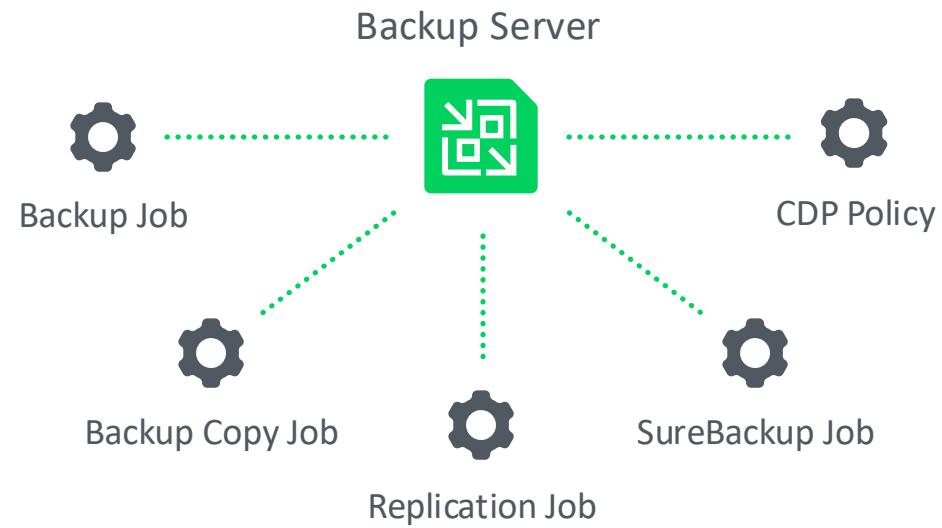
La restauración de la copia de seguridad de la configuración sólo puede realizarse desde esta ventana para cargar la configuración en un nuevo servidor.

Trabajos

El Concepto de Trabajos

En Veeam Backup and Replication, los trabajos engloban una serie de tareas de gestión de datos, incluidas las operaciones de **backup**, **replicación** y **restauración**. Una vez configurados, los trabajos automatizarán el proceso, garantizando que los datos críticos estén protegidos de forma regular y fiable contra pérdidas o corrupción.

En lo que respecta a la asignación de recursos de la infraestructura de backup, **el servicio Resource Scheduler Service** de Veeam Backup & Replication identifica la prioridad de los trabajos que esperan recursos libres en función de su tipo, prioridad y hora de inicio programada.



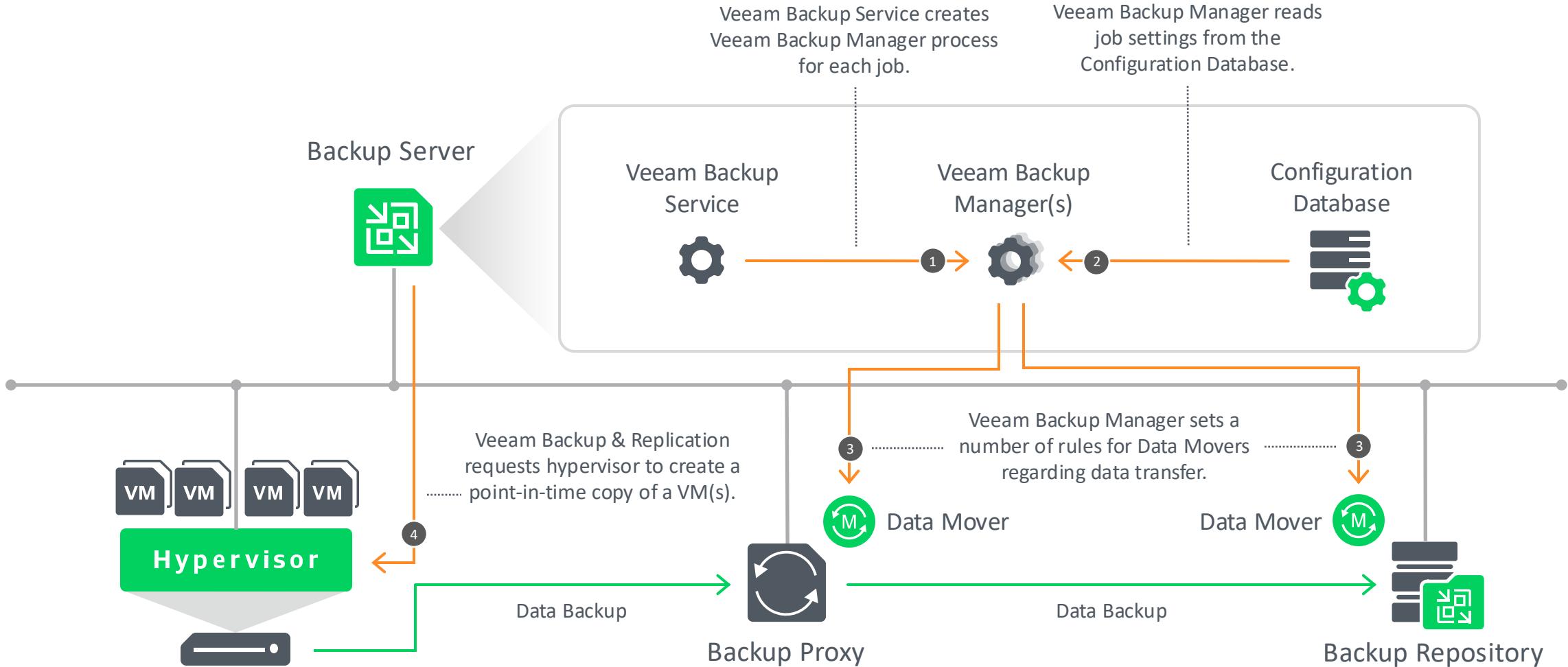
Priorización de trabajos

Aquí tienes una lista simplificada ordenada de mayor a menor prioridad:

- 1. Trabajos de Restauración de Datos** - estos trabajos tienen la máxima prioridad y son los primeros en obtener recursos libres del sistema.
- 2. Políticas CDP Continuous Data Protection.**
- 3. Trabajos del Sistema en Segundo Plano** (SnapshotDeleter, por ejemplo).
- 4. Trabajos de Copia de Seguridad Rápida** - estos trabajos tienen la segunda prioridad más alta.
- 5. Trabajos de Alta Prioridad** - los trabajos con la opción de Alta Prioridad activada tienen la tercera prioridad más alta. Es posible habilitar la opción Alta prioridad para los siguientes trabajos: trabajos de copia de seguridad, trabajos de replicación, trabajos de agentes gestionados por el servidor de copia de seguridad, trabajos de copia de seguridad de archivos.
- 6. Trabajos regulares de copia de seguridad y trabajos de replicación.**
- 7. Trabajos de copia de seguridad y trabajos de archivo** - estos trabajos tienen la prioridad más baja y son los últimos en obtener recursos libres del sistema.

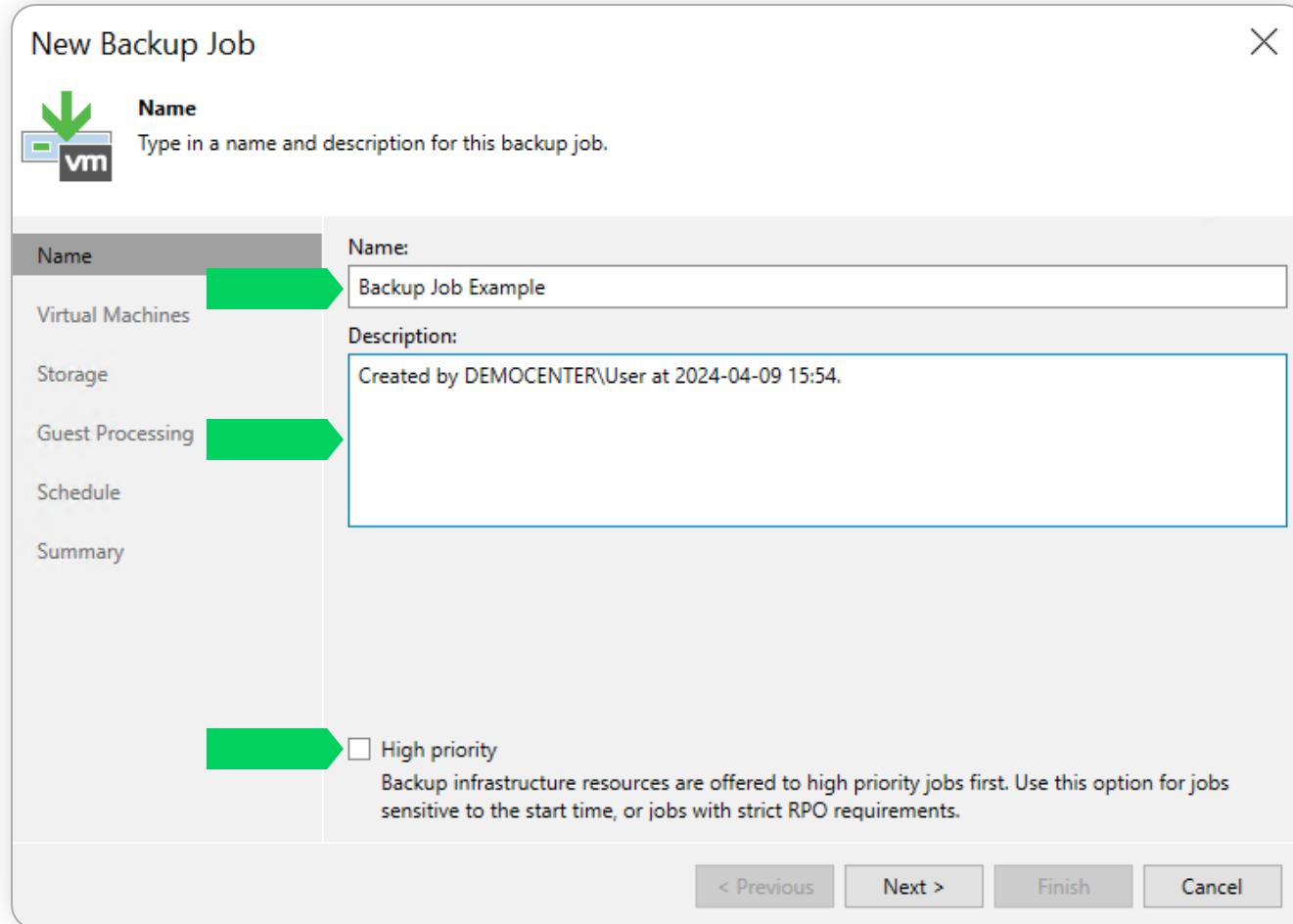
Trabajos

Ejemplo de proceso de backup



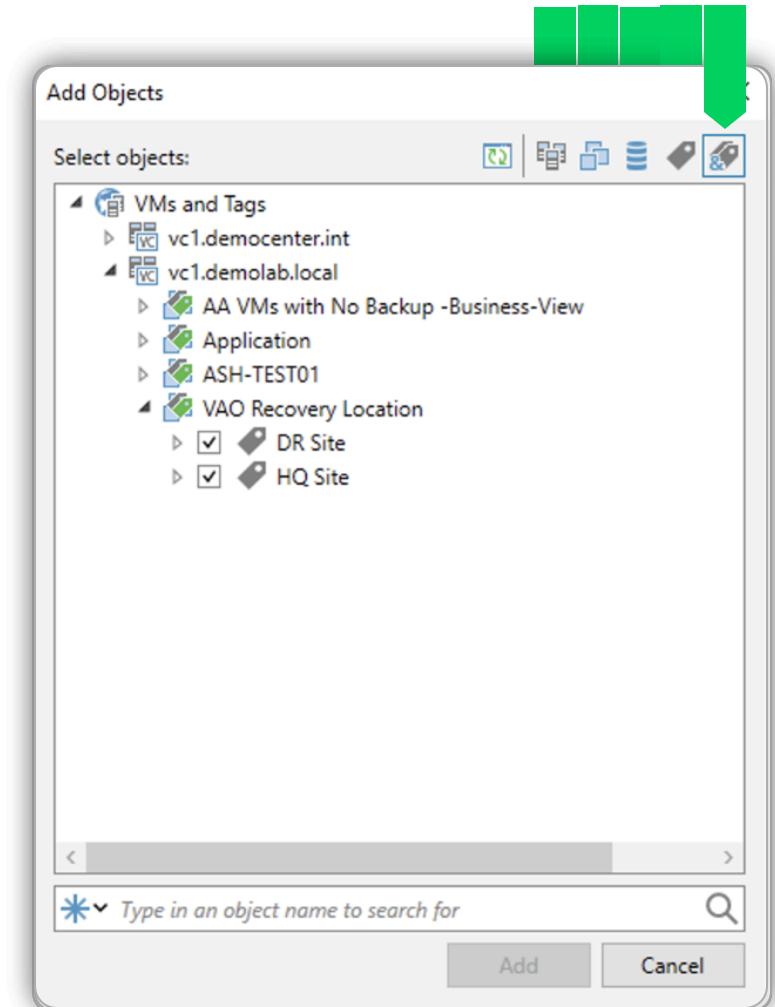
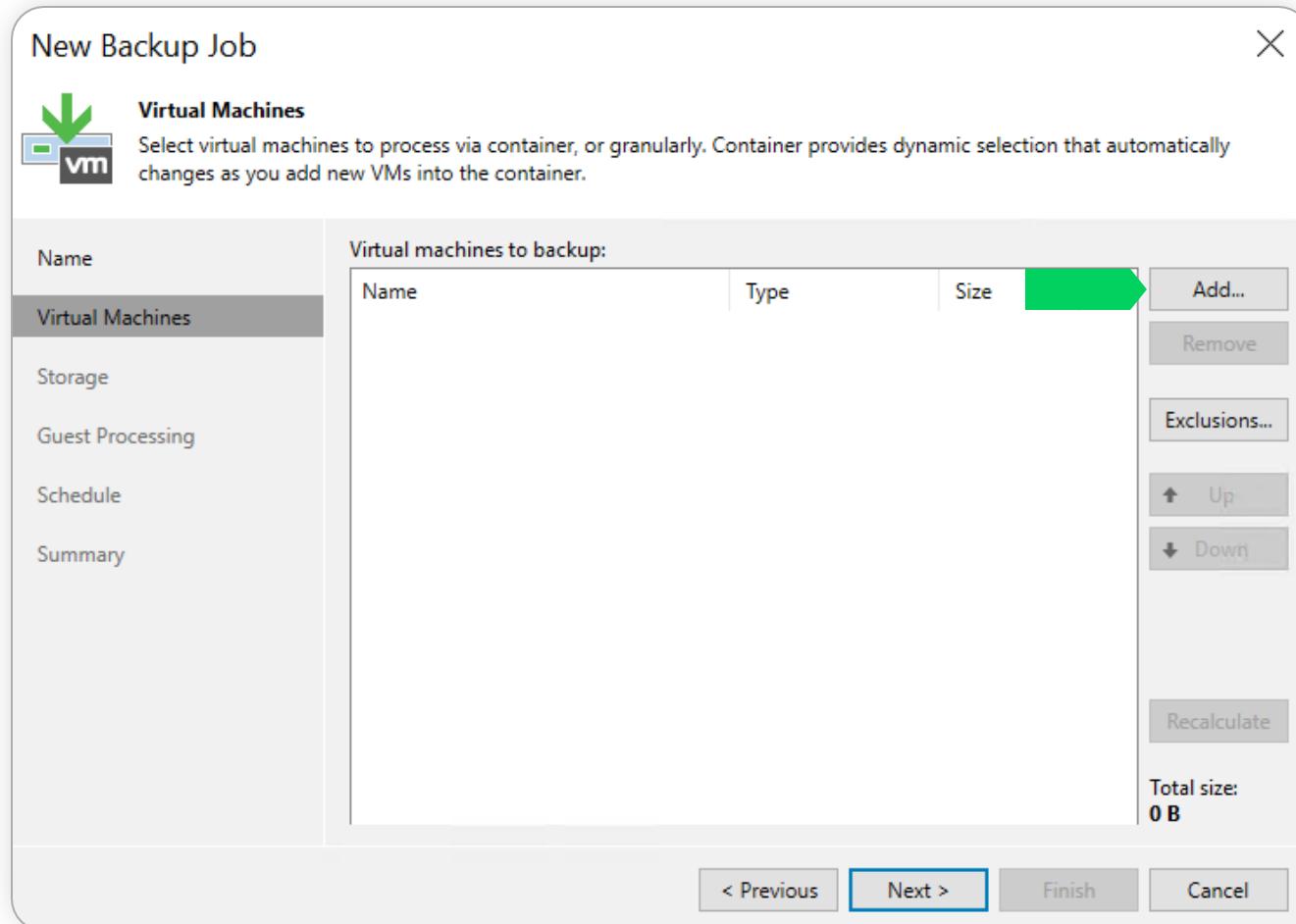
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



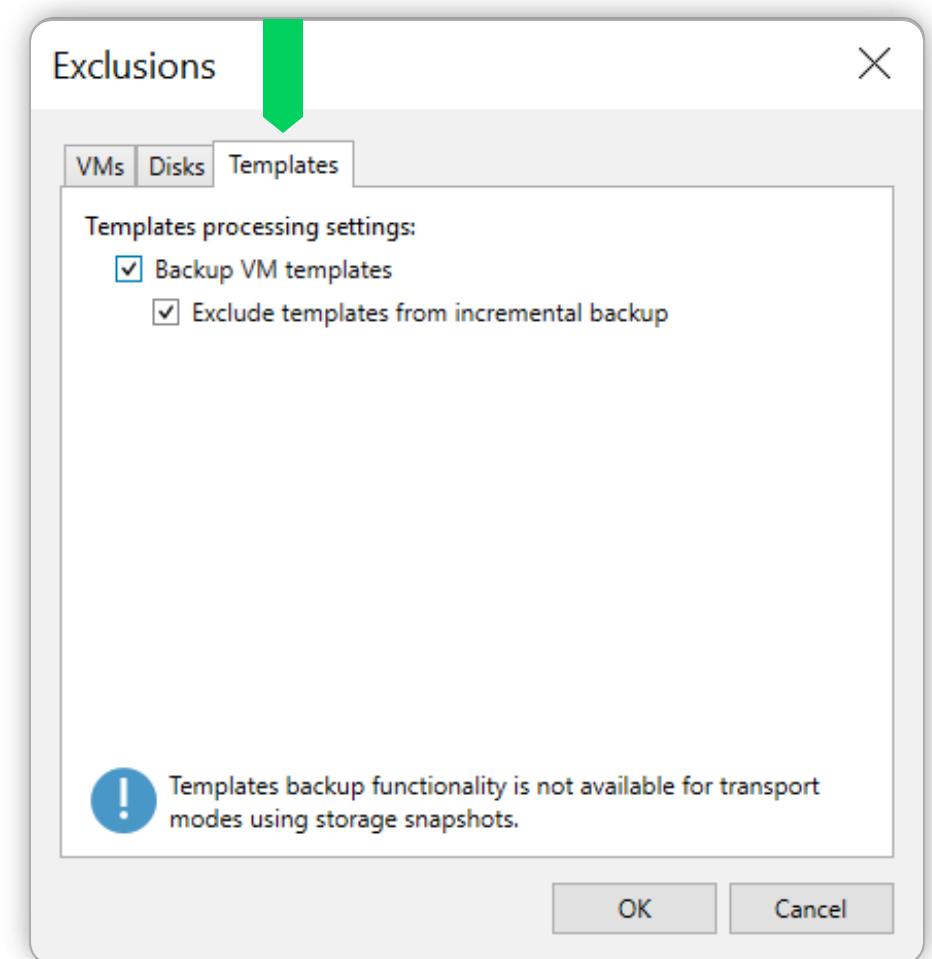
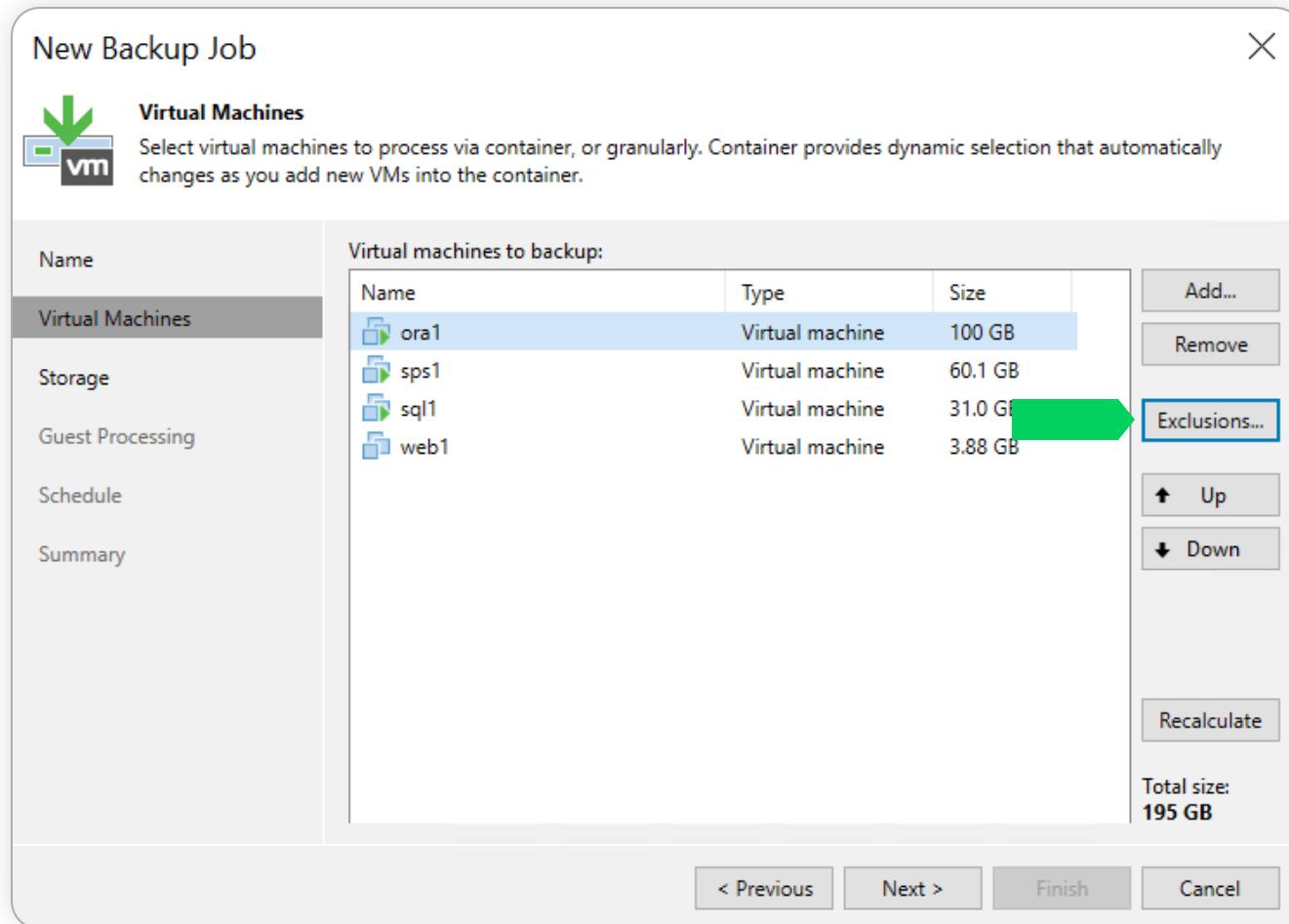
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



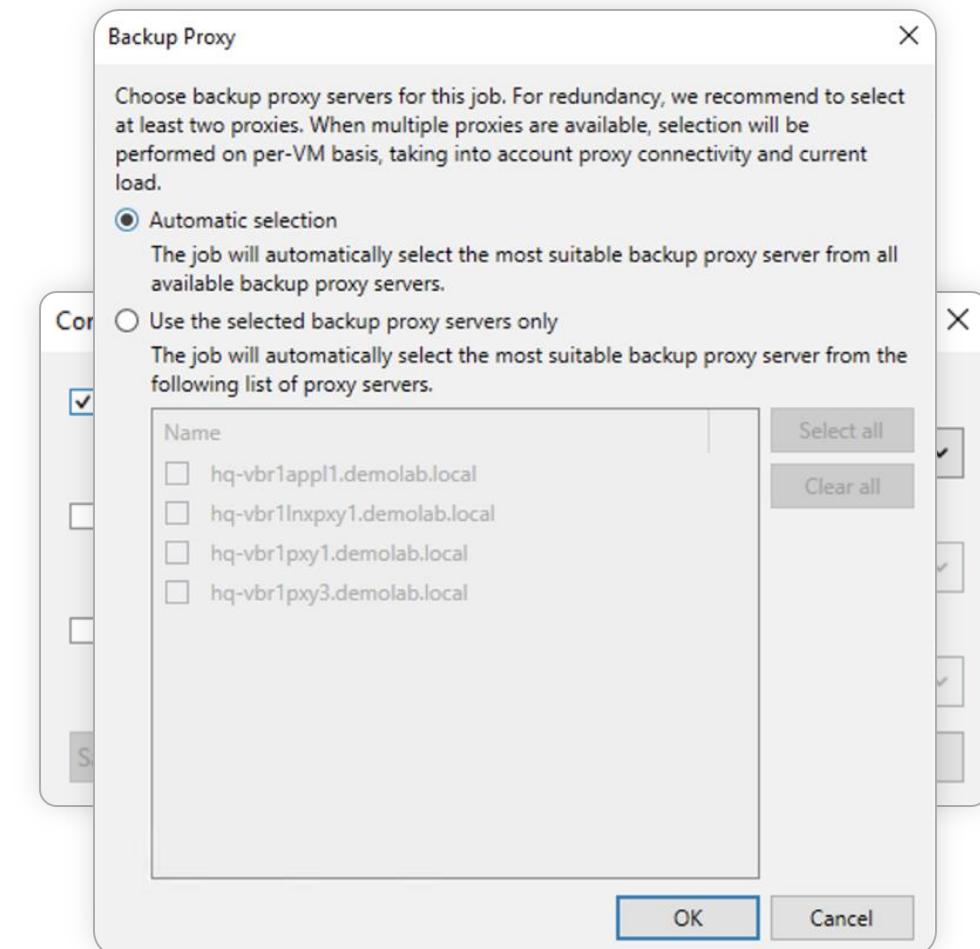
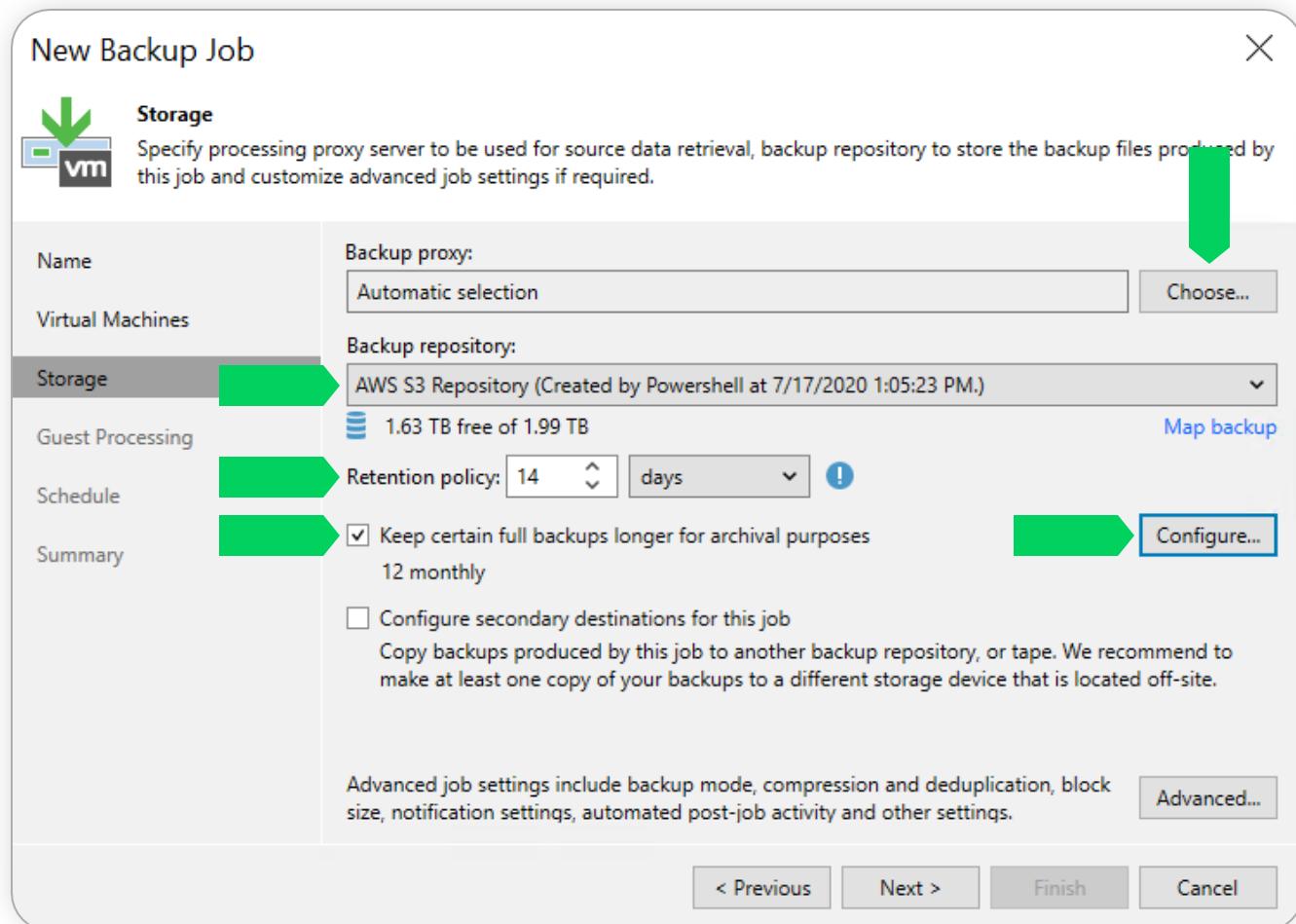
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



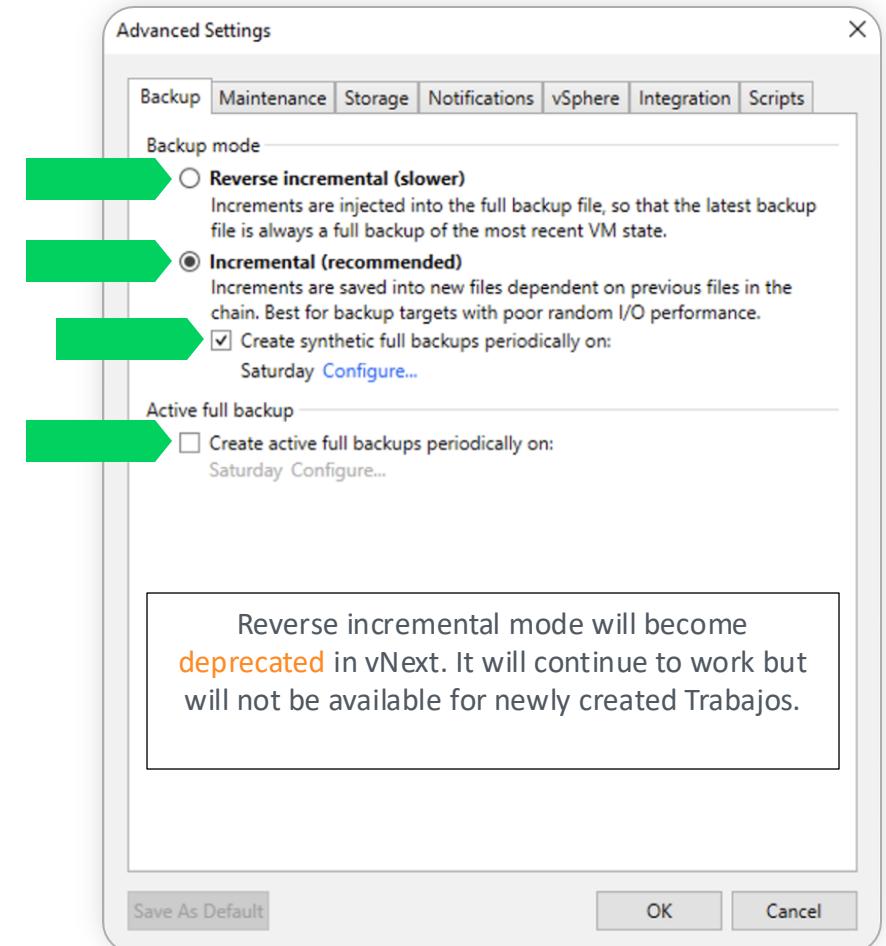
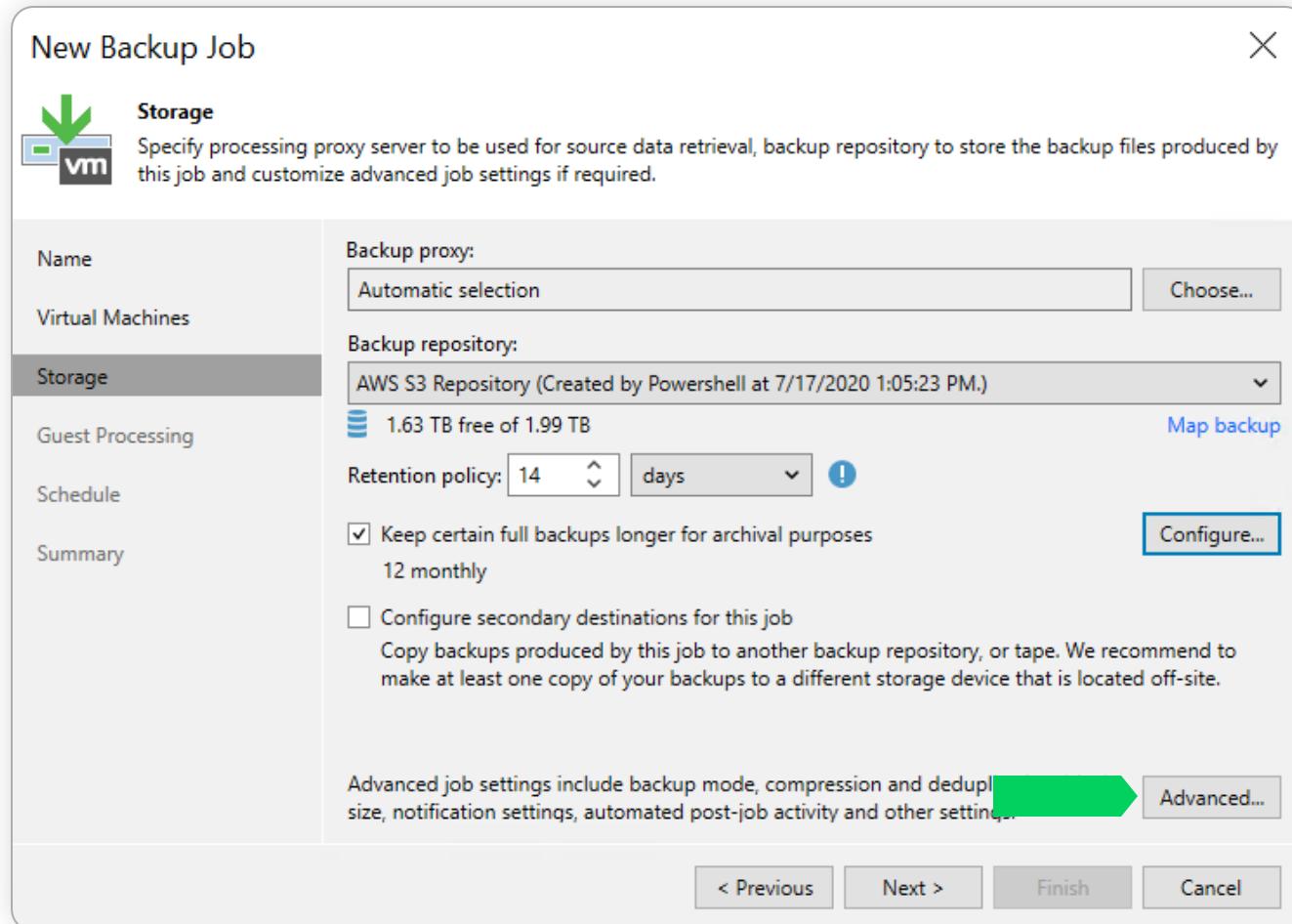
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



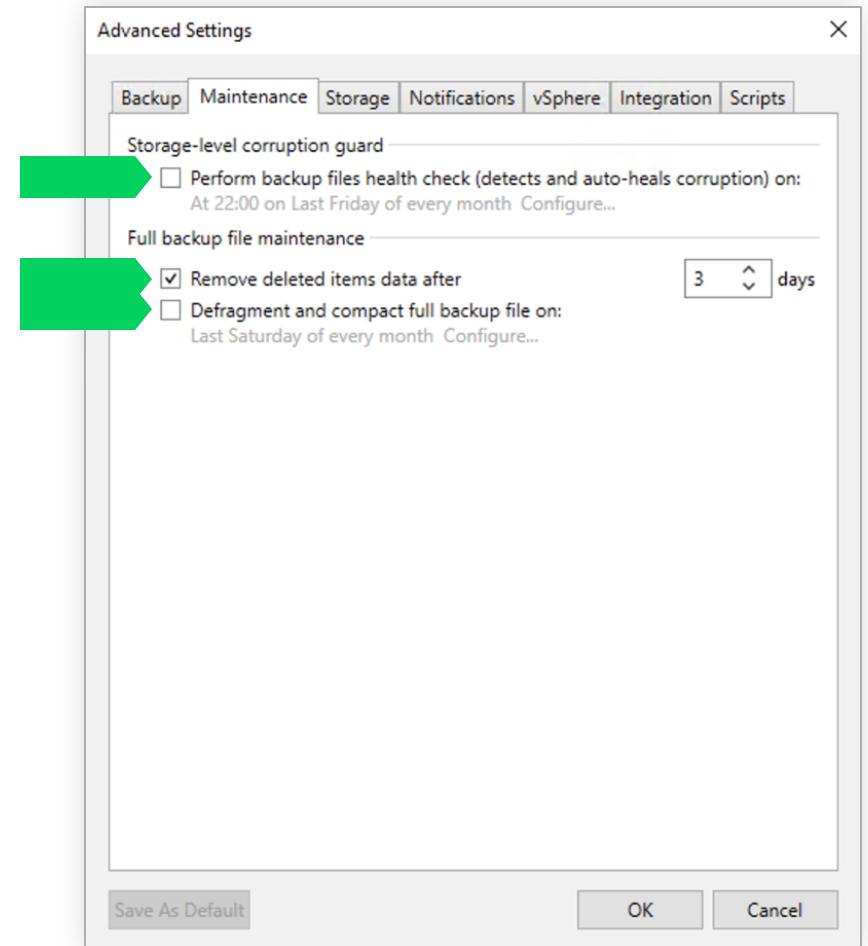
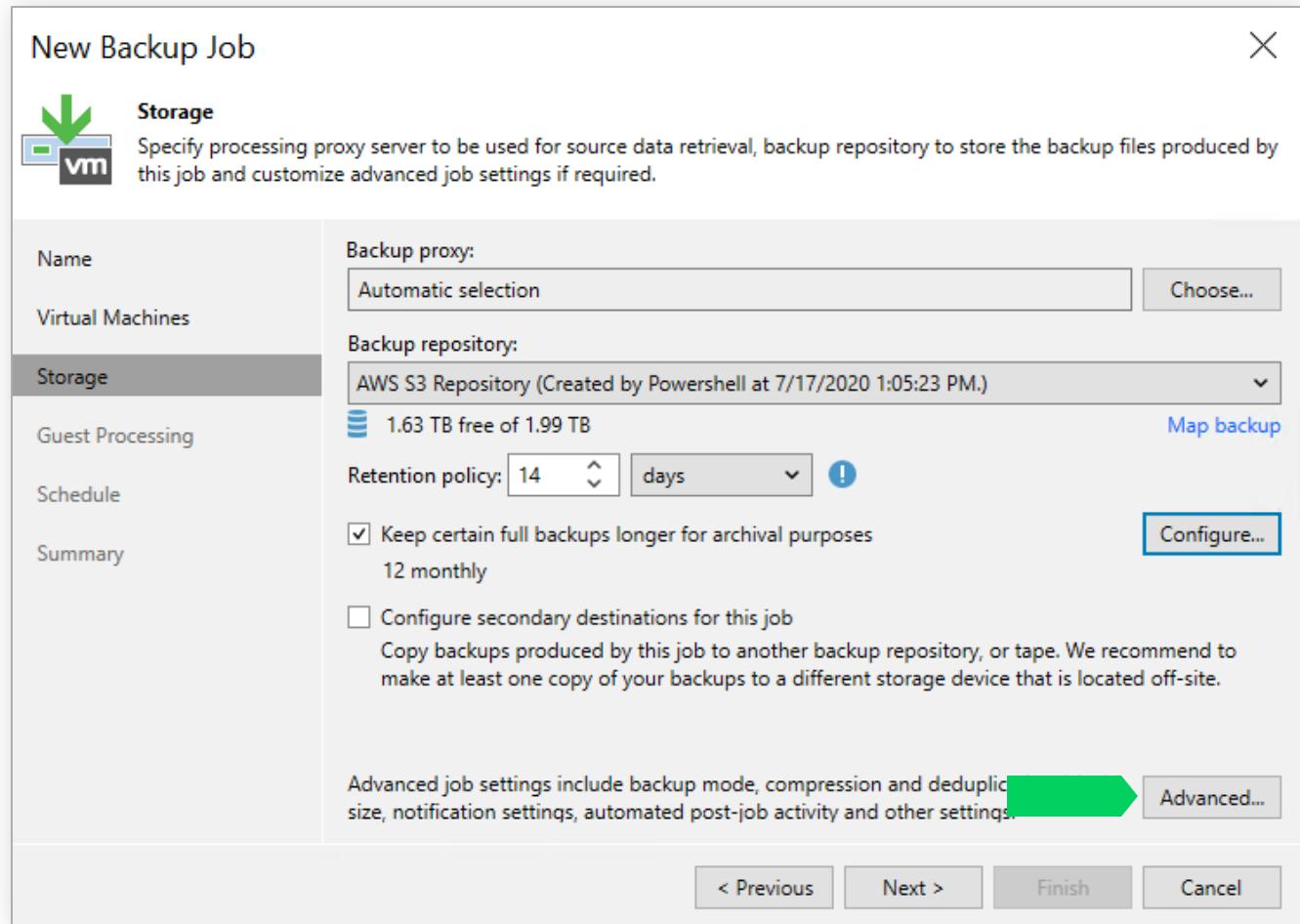
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



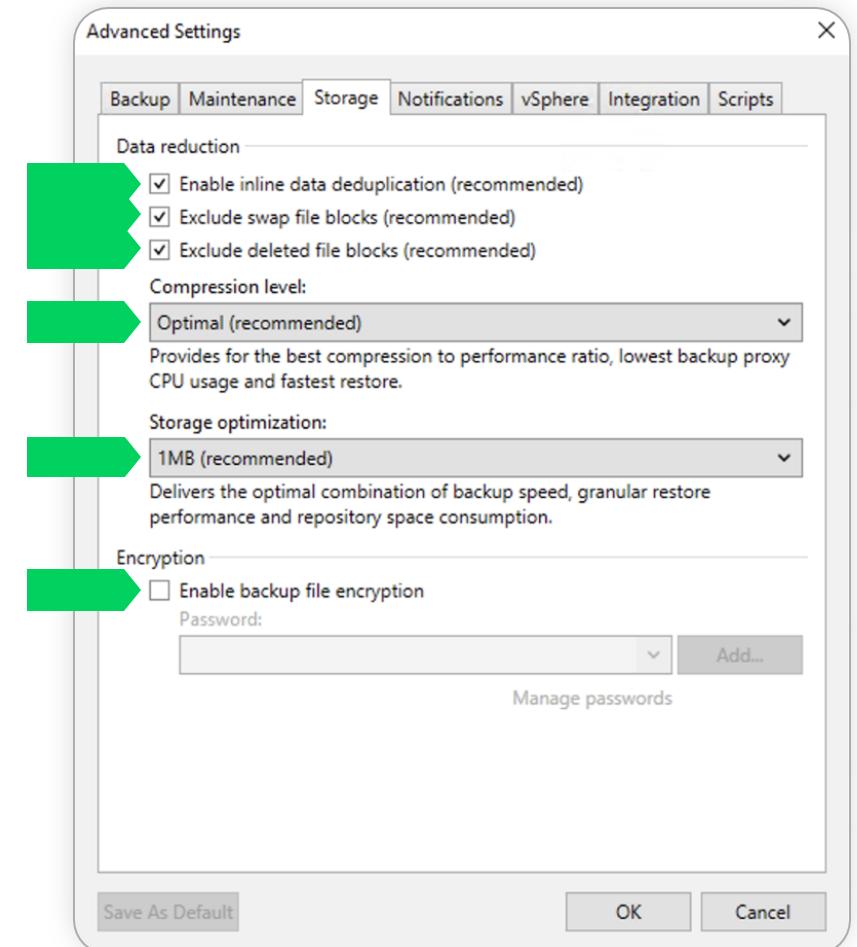
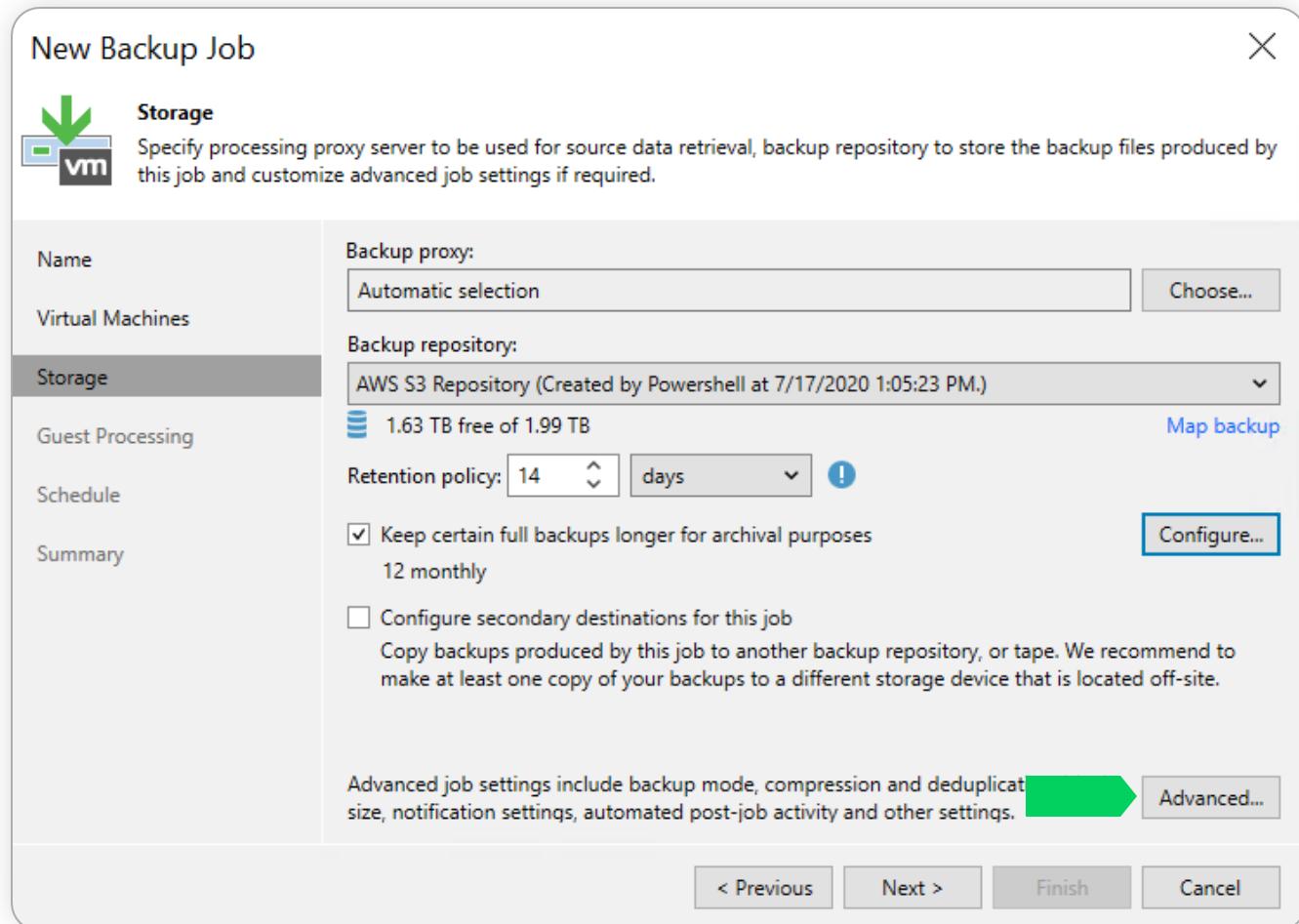
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



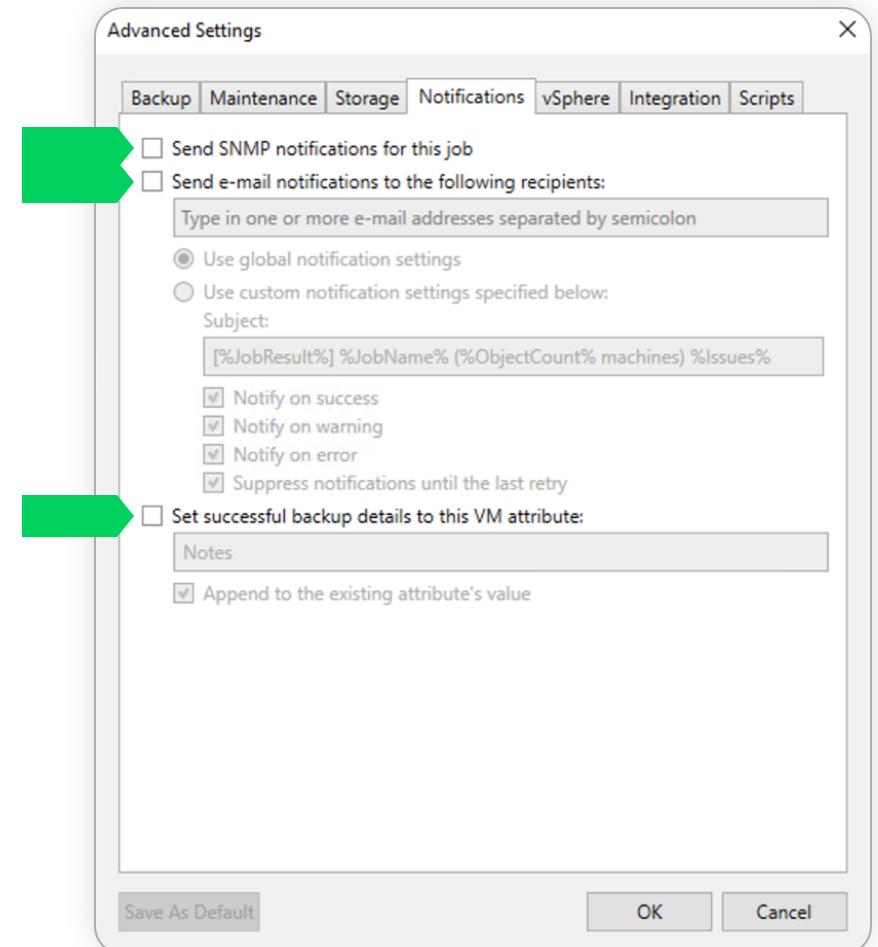
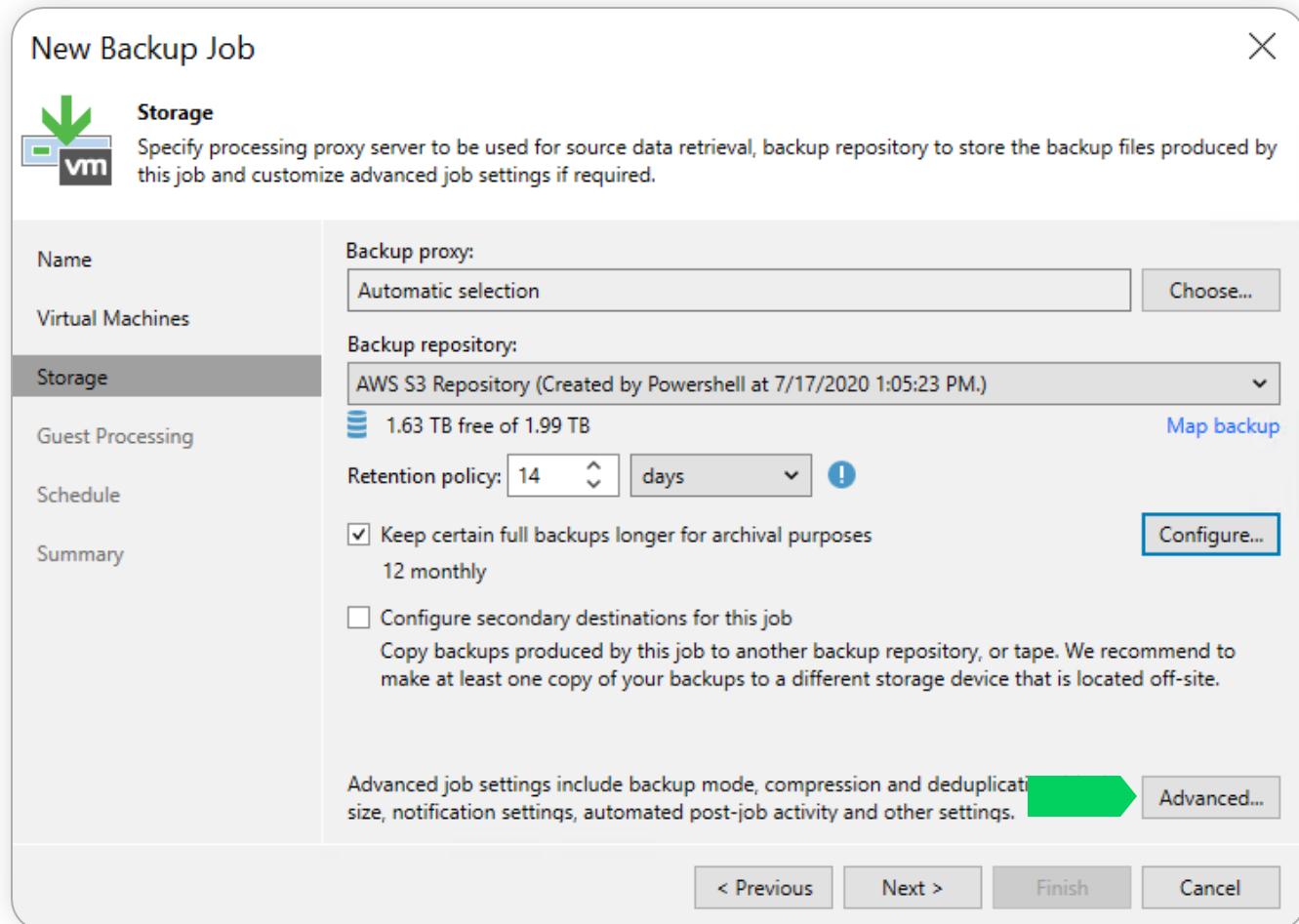
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



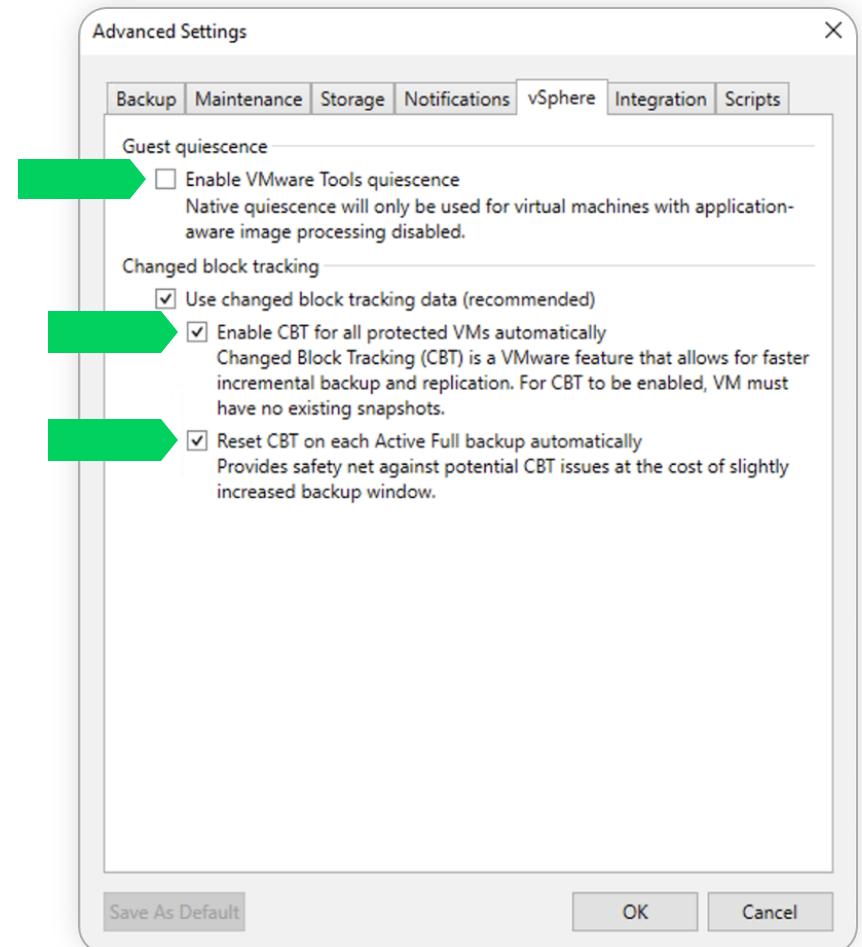
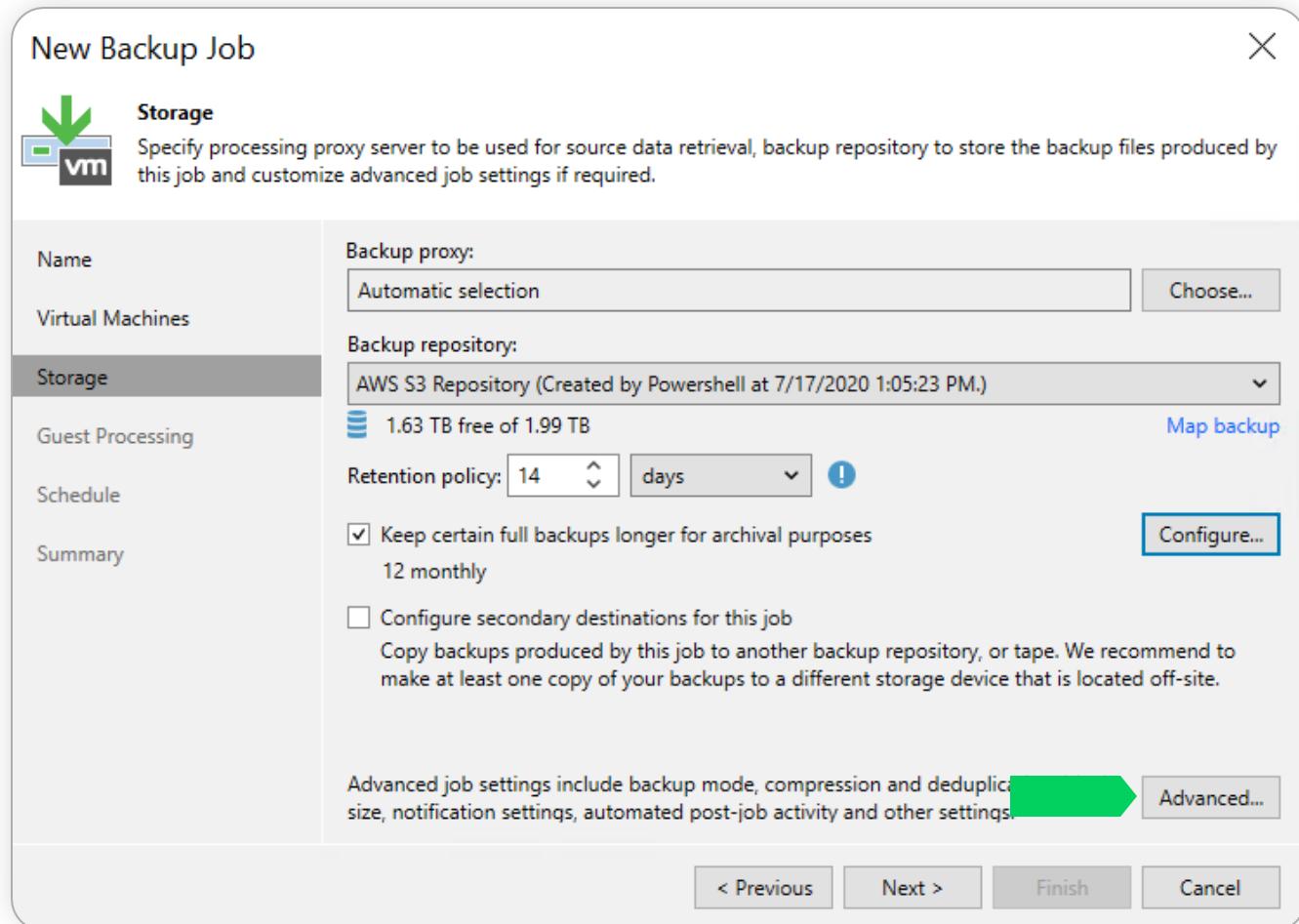
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad

New Backup Job

Storage
Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Name: Backup proxy: Choose...

Virtual Machines: Automatic selection

Storage: AWS S3 Repository (Created by Powershell at 7/17/2020 1:05:23 PM.)

Guest Processing: 1.63 TB free of 1.99 TB

Schedule: Retention policy: 14 days

Summary: Keep certain full backups longer for archival purposes
12 monthly
 Configure secondary destinations for this job
Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication size, notification settings, automated post-job activity and other settings. [Advanced...](#)

< Previous Next > Finish Cancel

Advanced Settings

Backup Maintenance Storage Notifications vSphere Integration Scripts

Primary storage integration

Enable backup from storage snapshots
Use storage snapshots (instead of VM snapshots) as the data source for this job. Using storage snapshots reduces impact on the production environment from VM snapshot commit.

Limit processed VM count per storage snapshot to 10
By default, the job will process all included VMs located on the same datastore from a single storage snapshot.

Failover to standard backup
Perform standard backup from VM snapshot if backup from storage snapshot fails.

Failover to primary storage snapshot
Use primary storage snapshots as the data source if backup from secondary storage snapshot fails.

Save As Default OK Cancel

Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad

New Backup Job

Storage
Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Name: Backup proxy:

Virtual Machines:

Storage:
1.63 TB free of 1.99 TB

Retention policy: days

Keep certain full backups longer for archival purposes
12 monthly

Configure secondary destinations for this job
Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication size, notification settings, automated post-job activity and other settings.

< Previous

Advanced Settings

Backup **Maintenance** **Storage** **Notifications** **vSphere** **Integration** **Scripts**

Job scripts

Run the following script before the job:

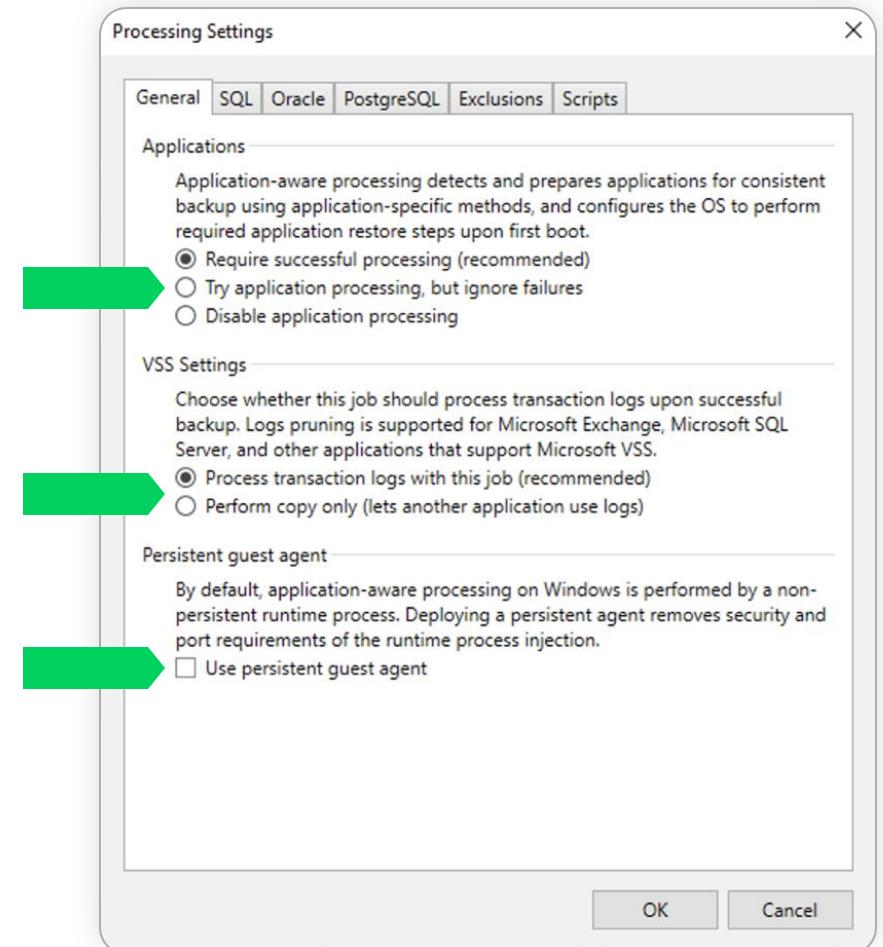
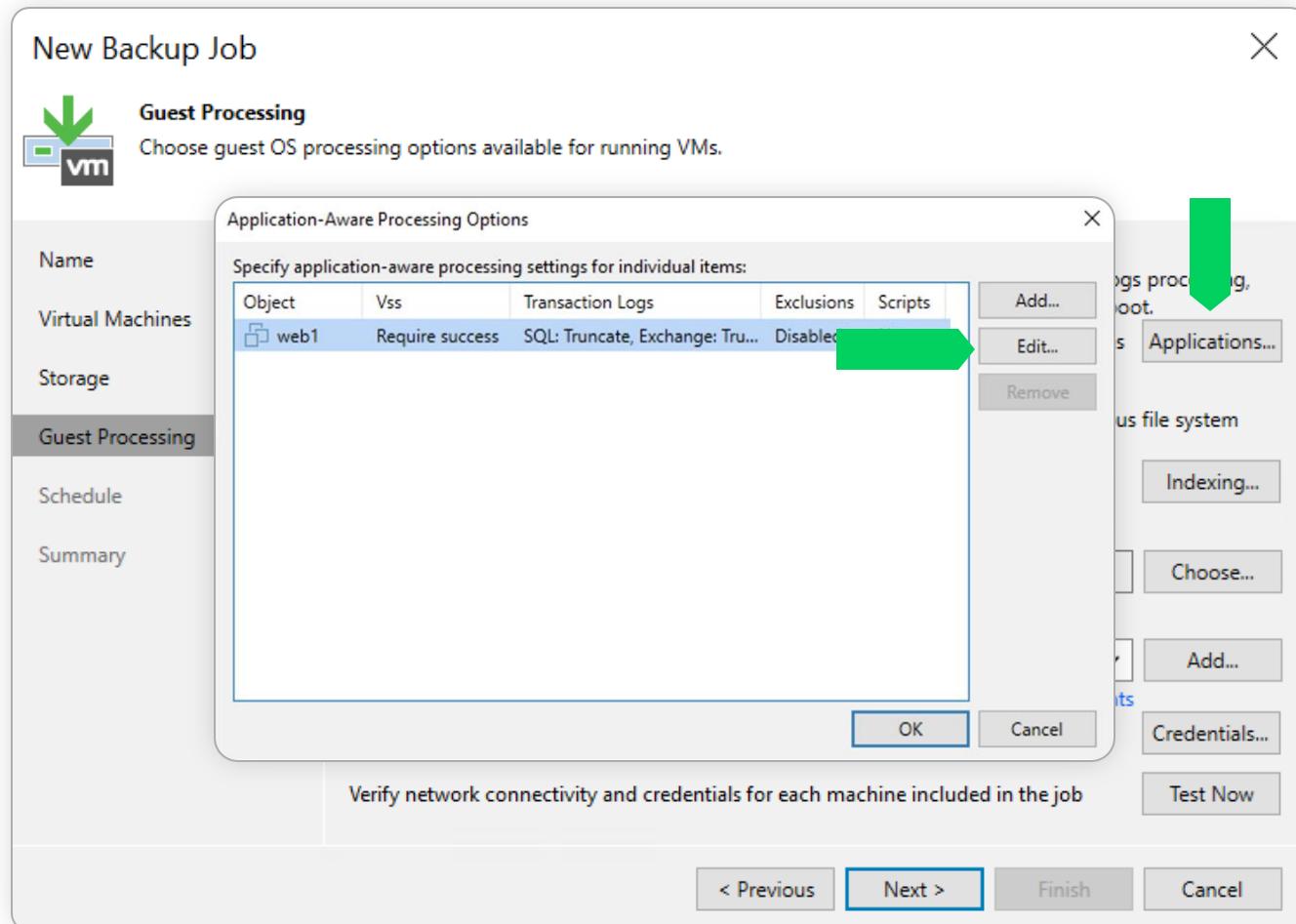
Run the following script after the job:

Run scripts every backup session

Run scripts on the selected days only
Saturday

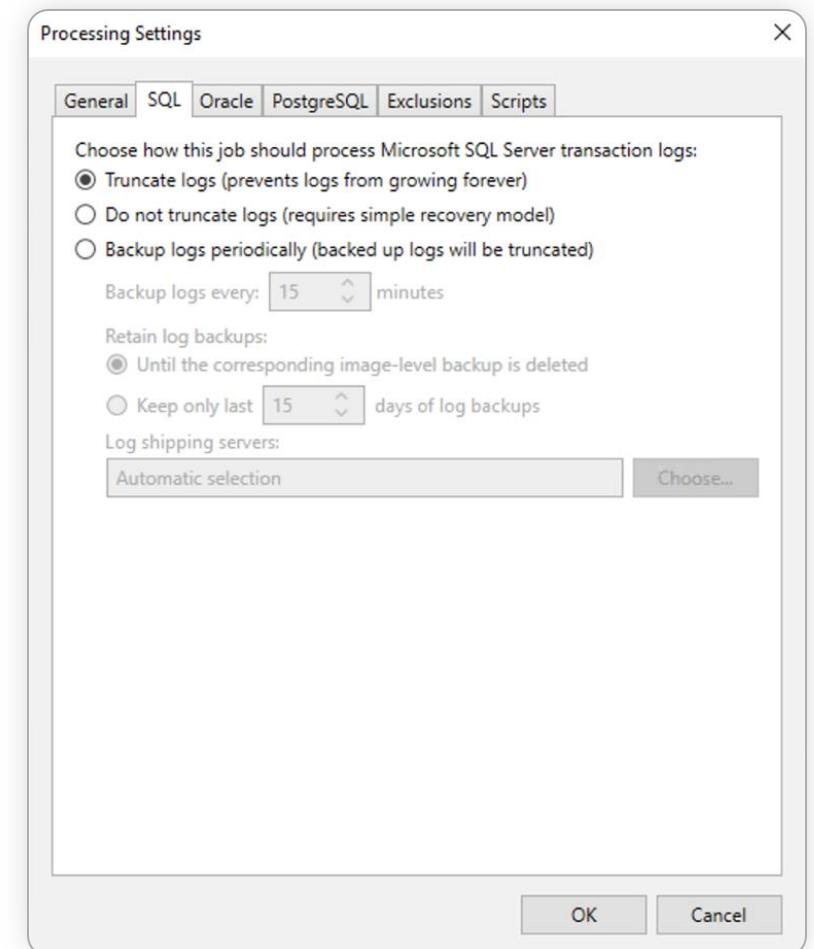
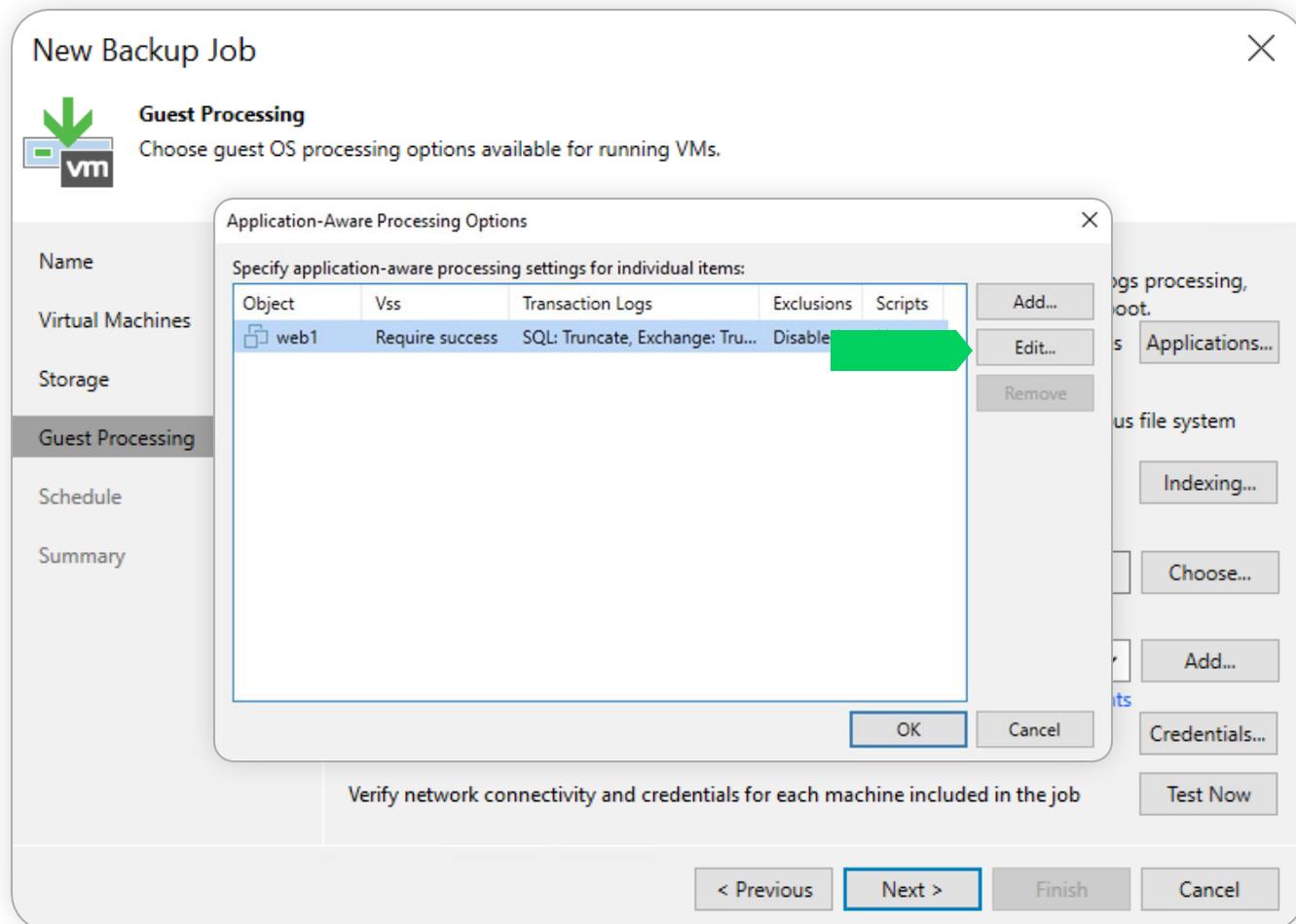
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



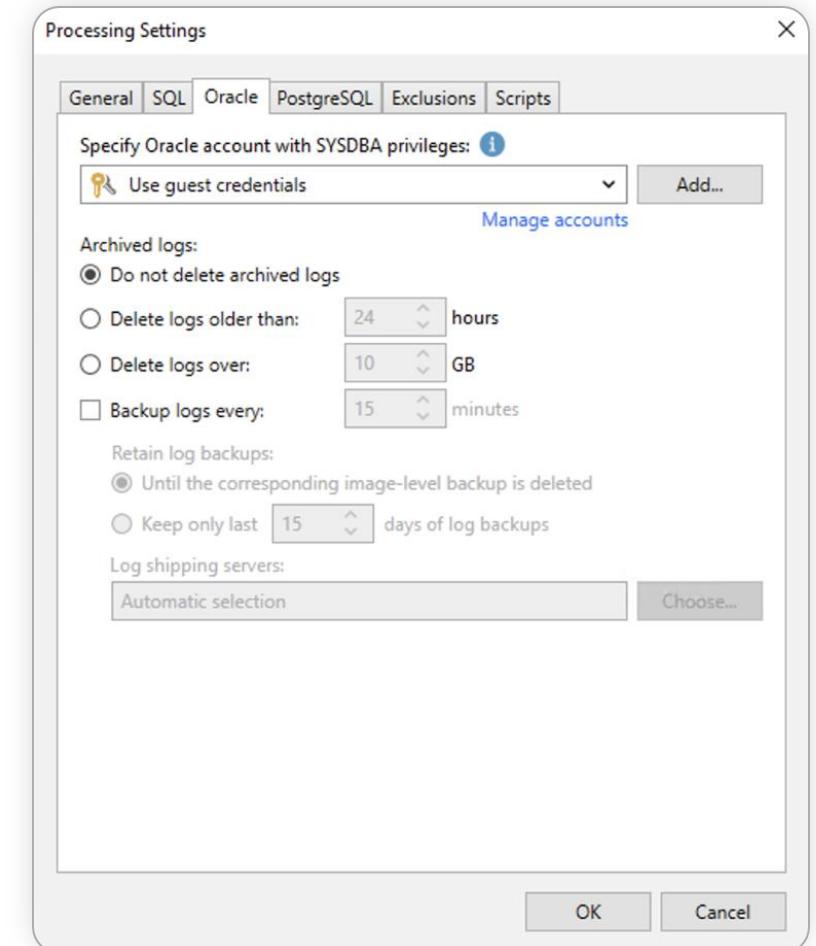
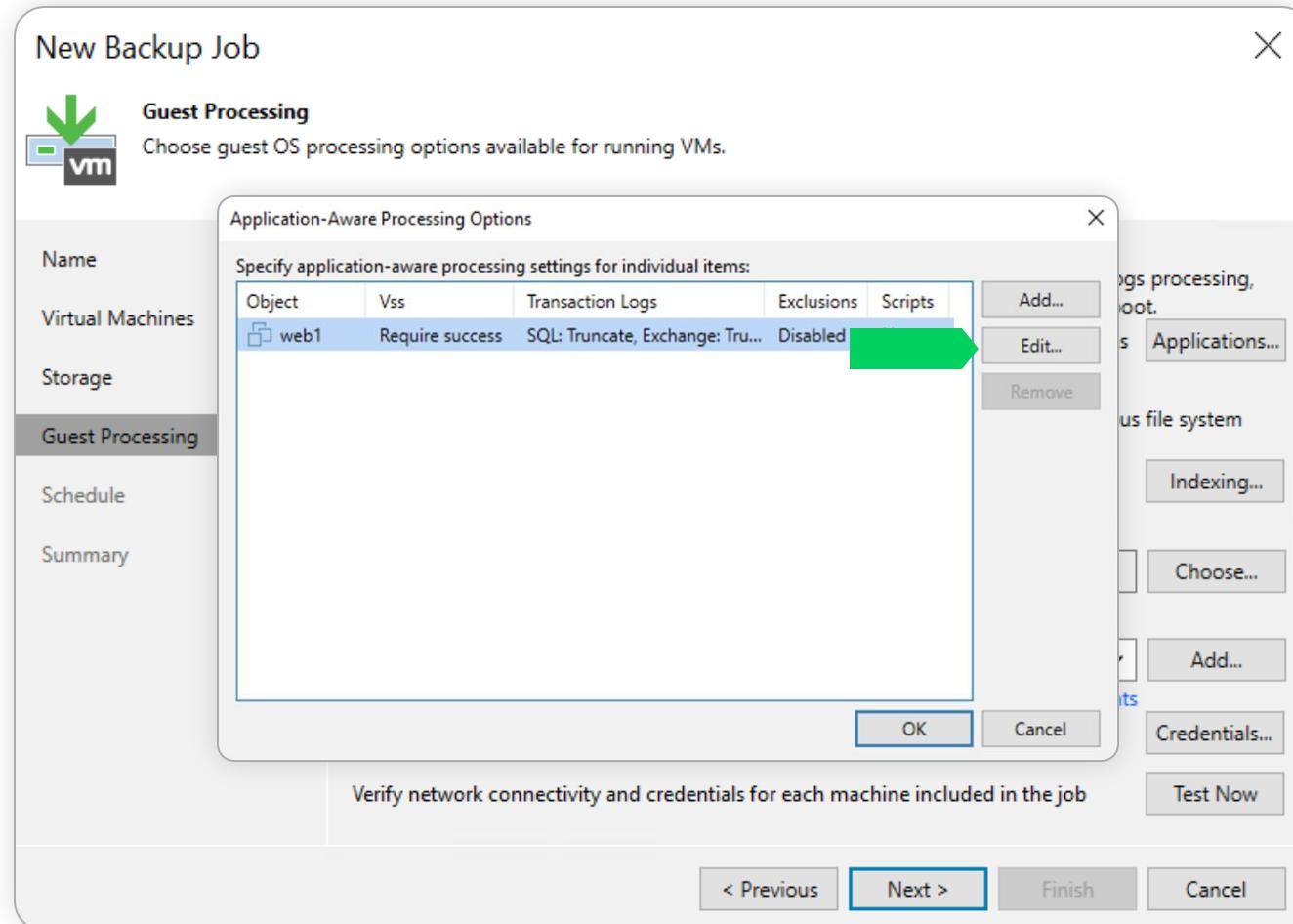
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



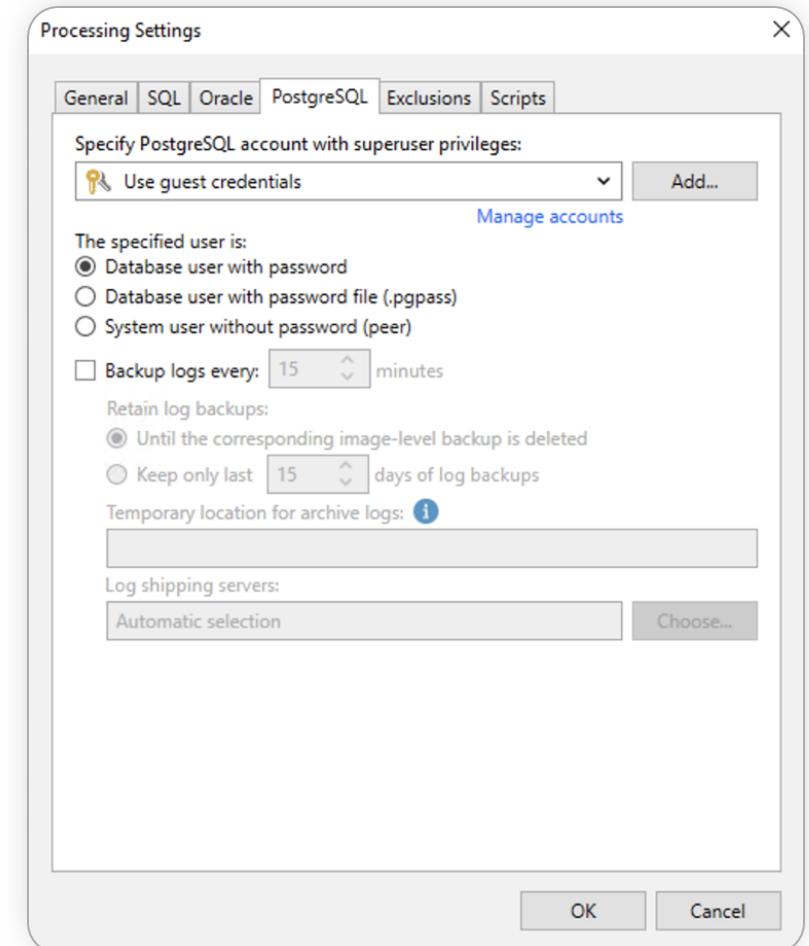
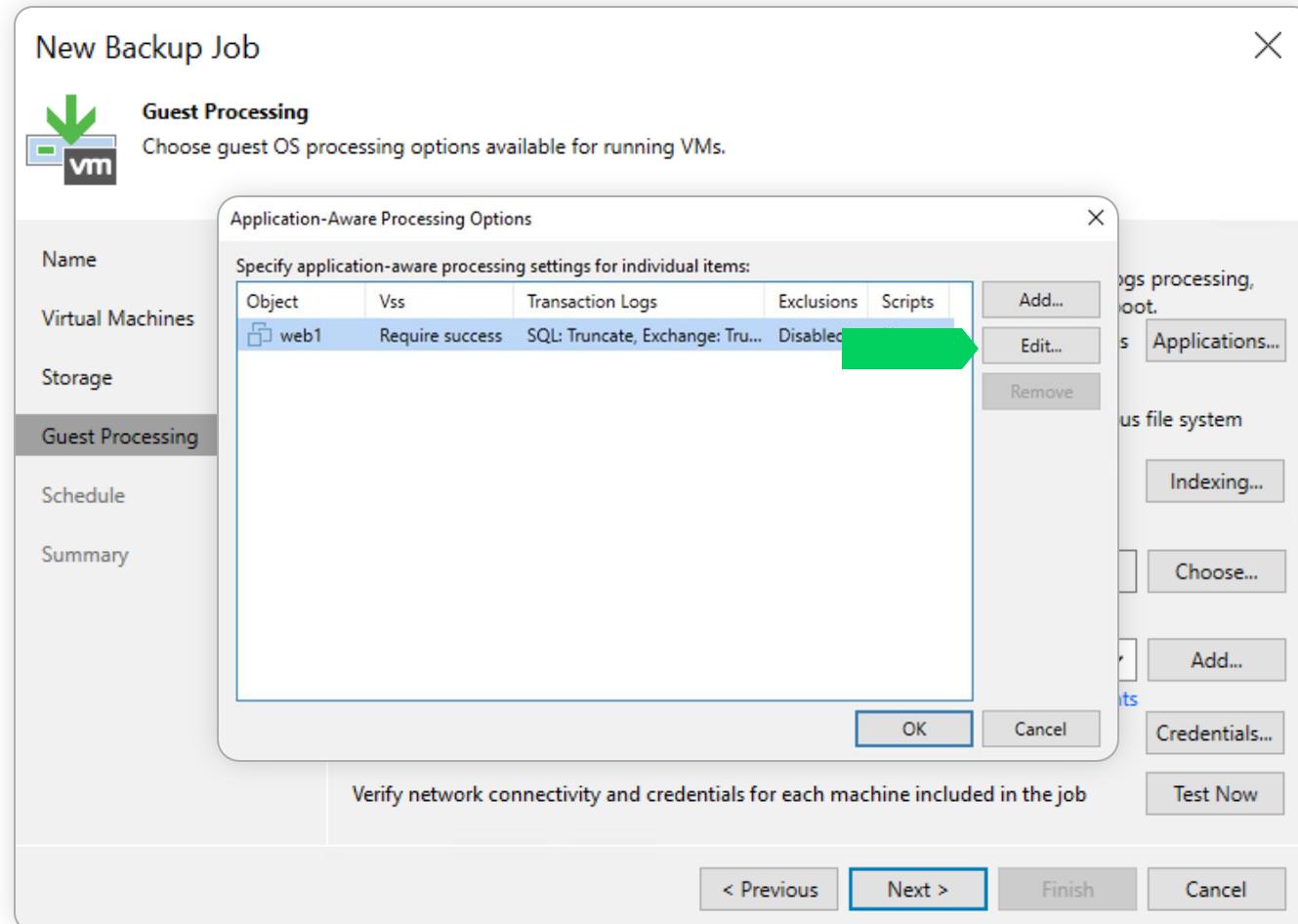
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



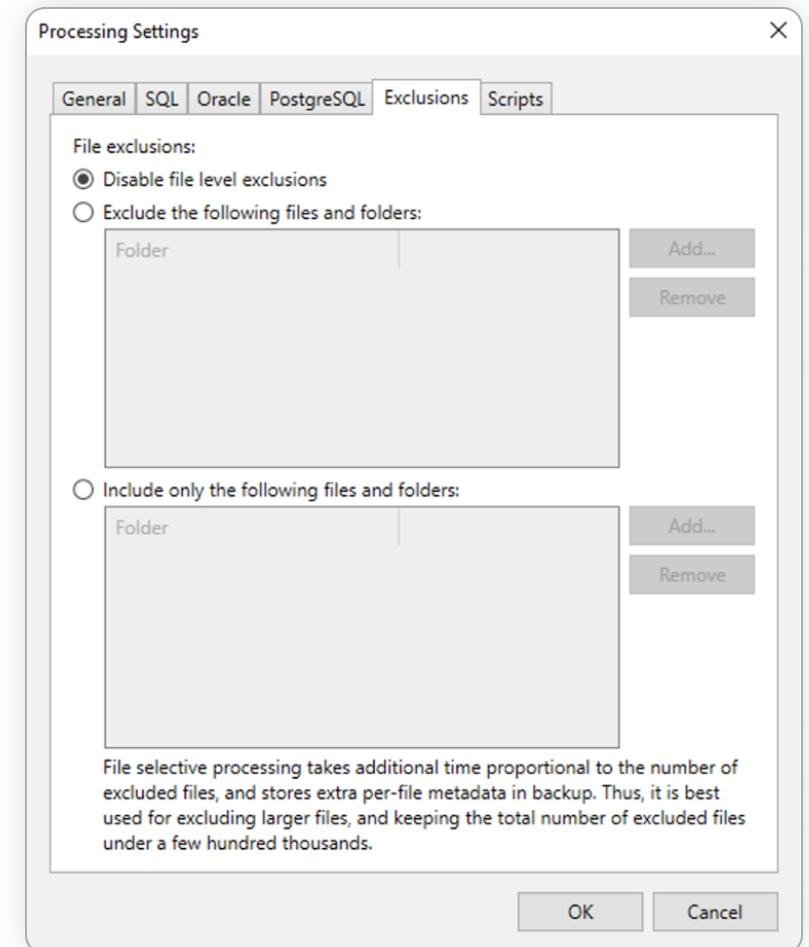
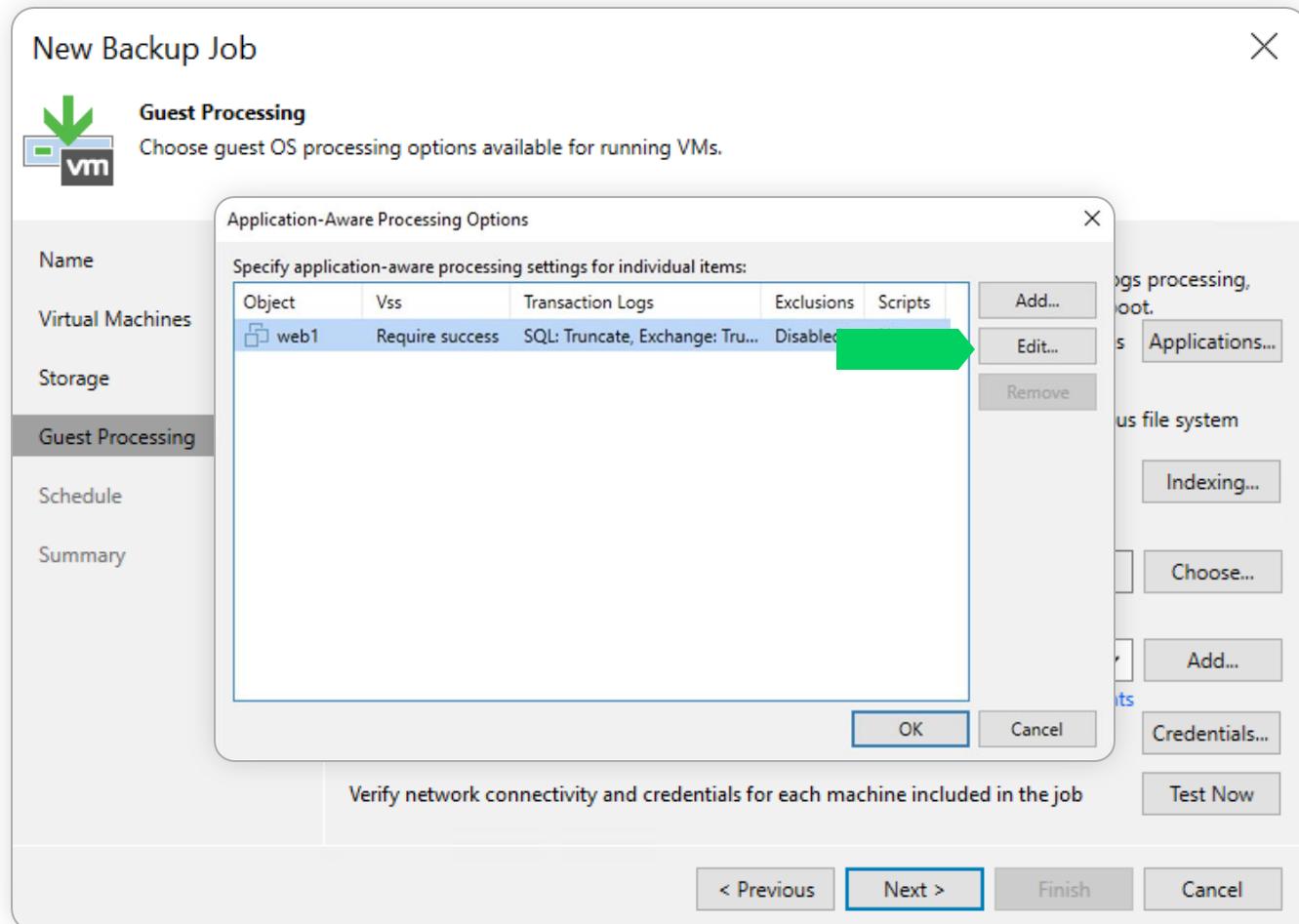
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



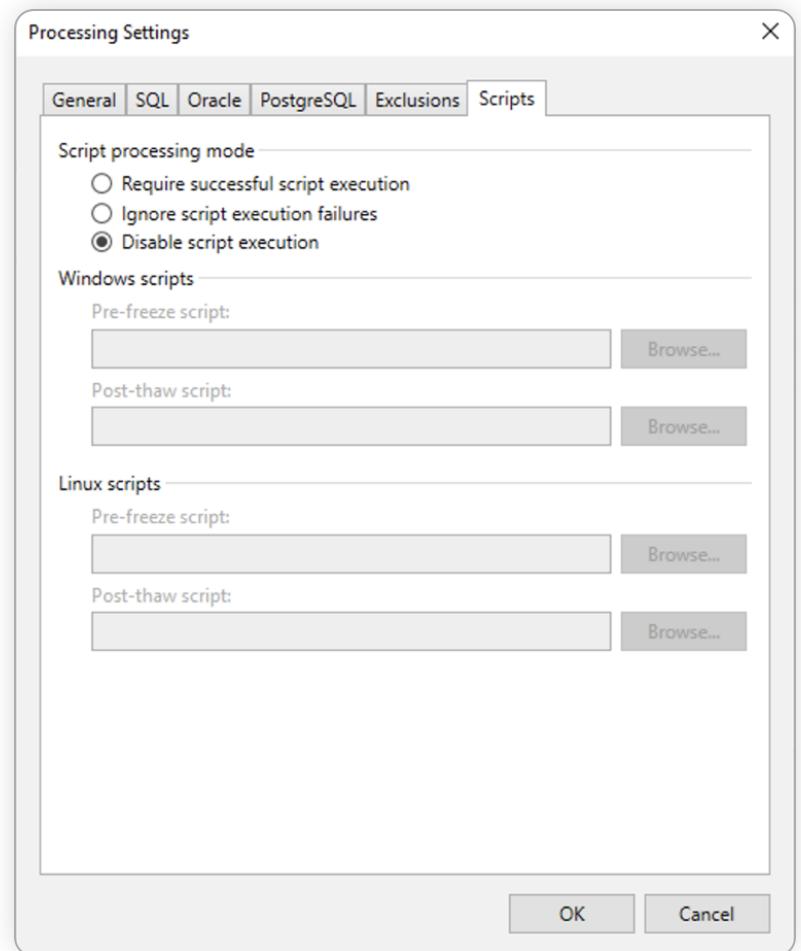
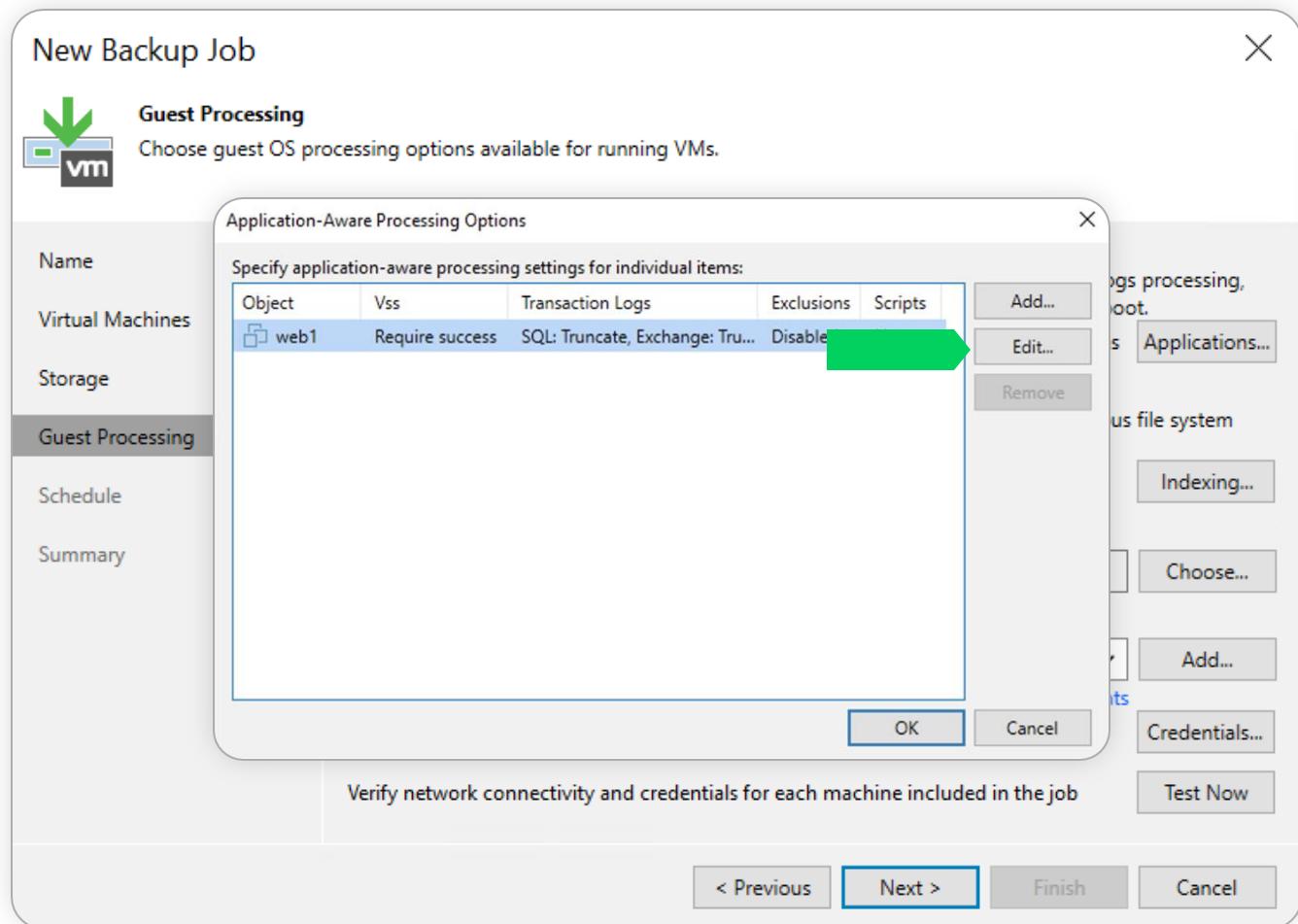
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



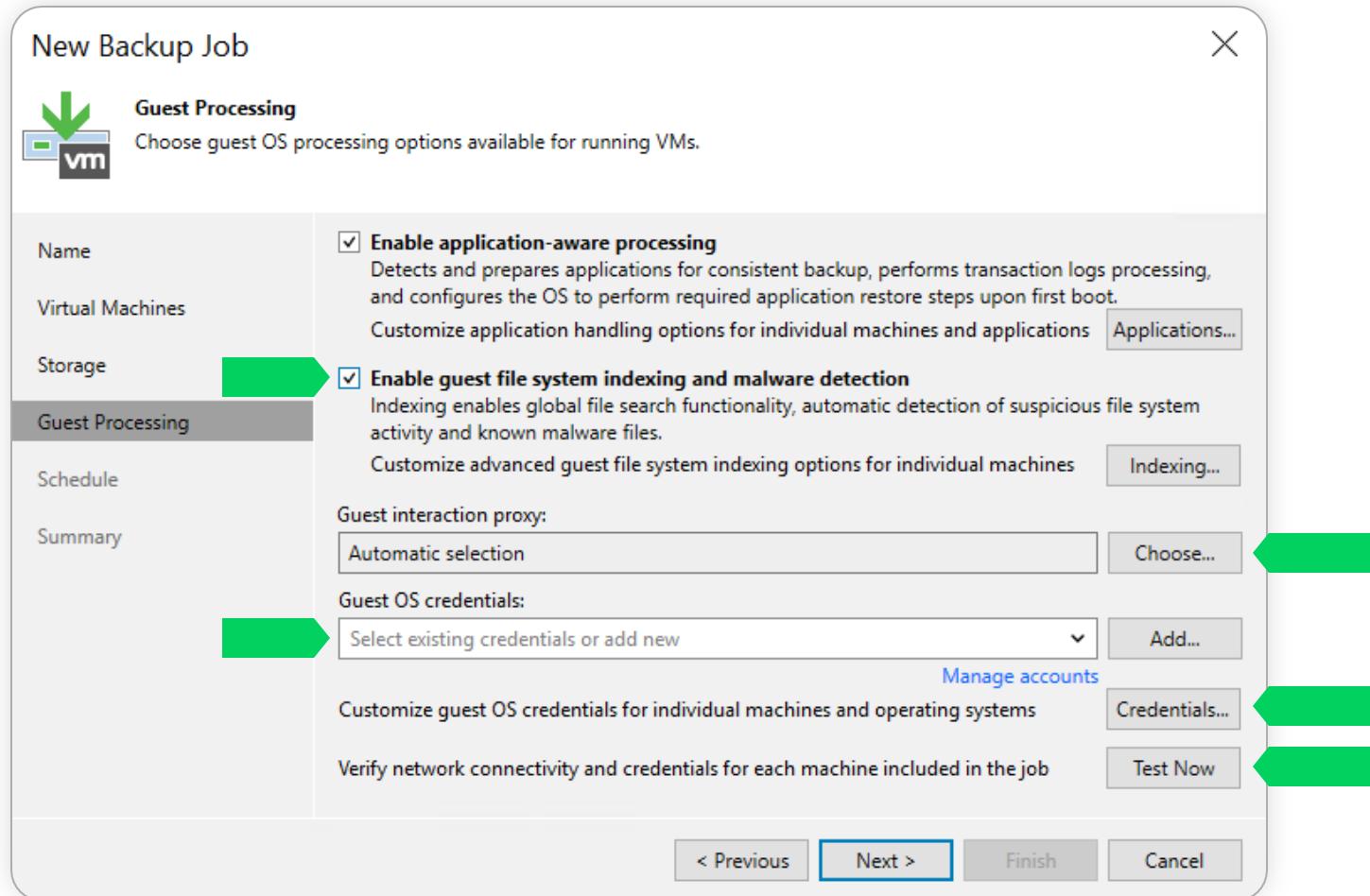
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



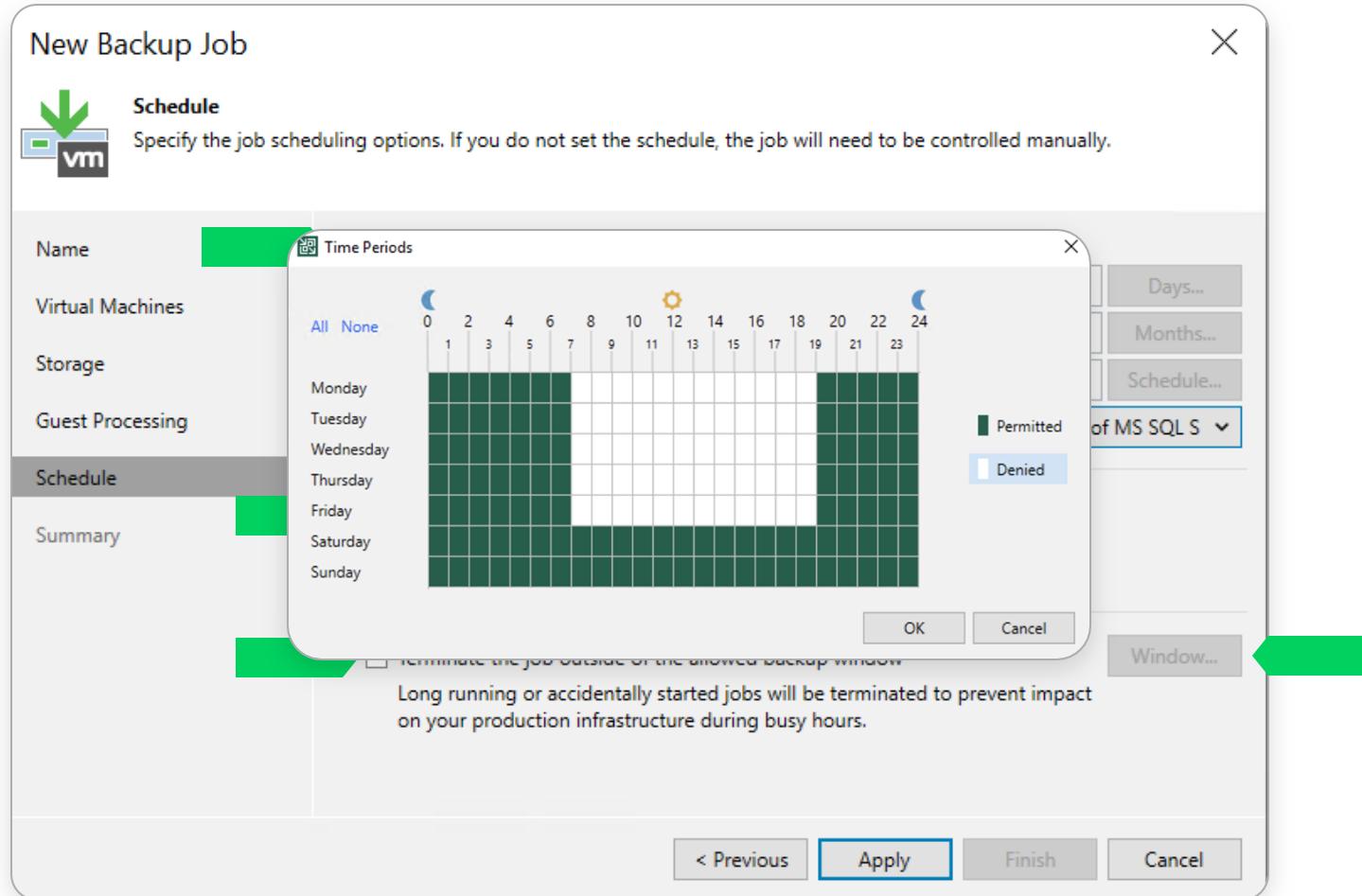
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



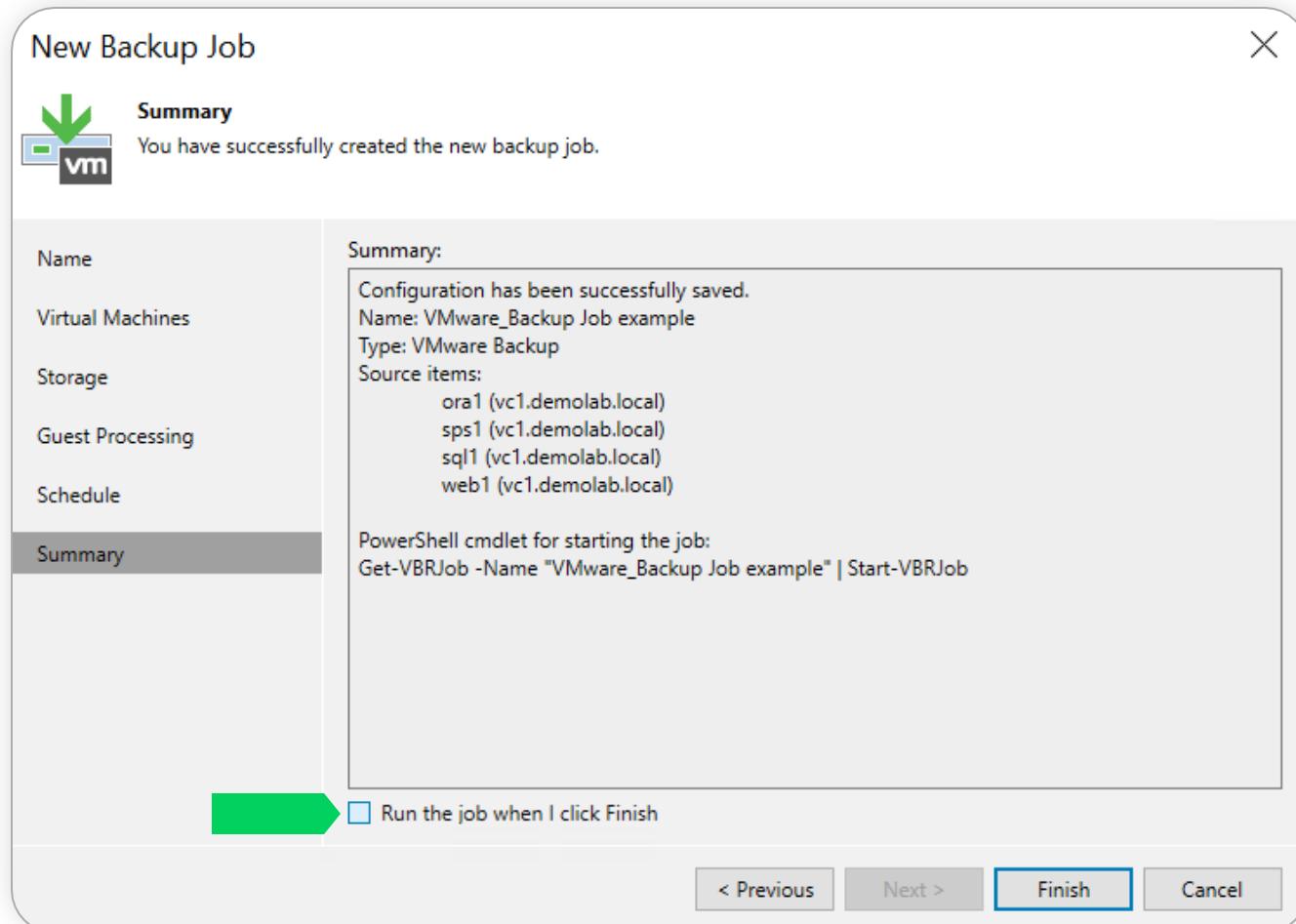
Trabajos

Ejemplo de proceso de creación de un trabajo de copia de seguridad



Trabajos

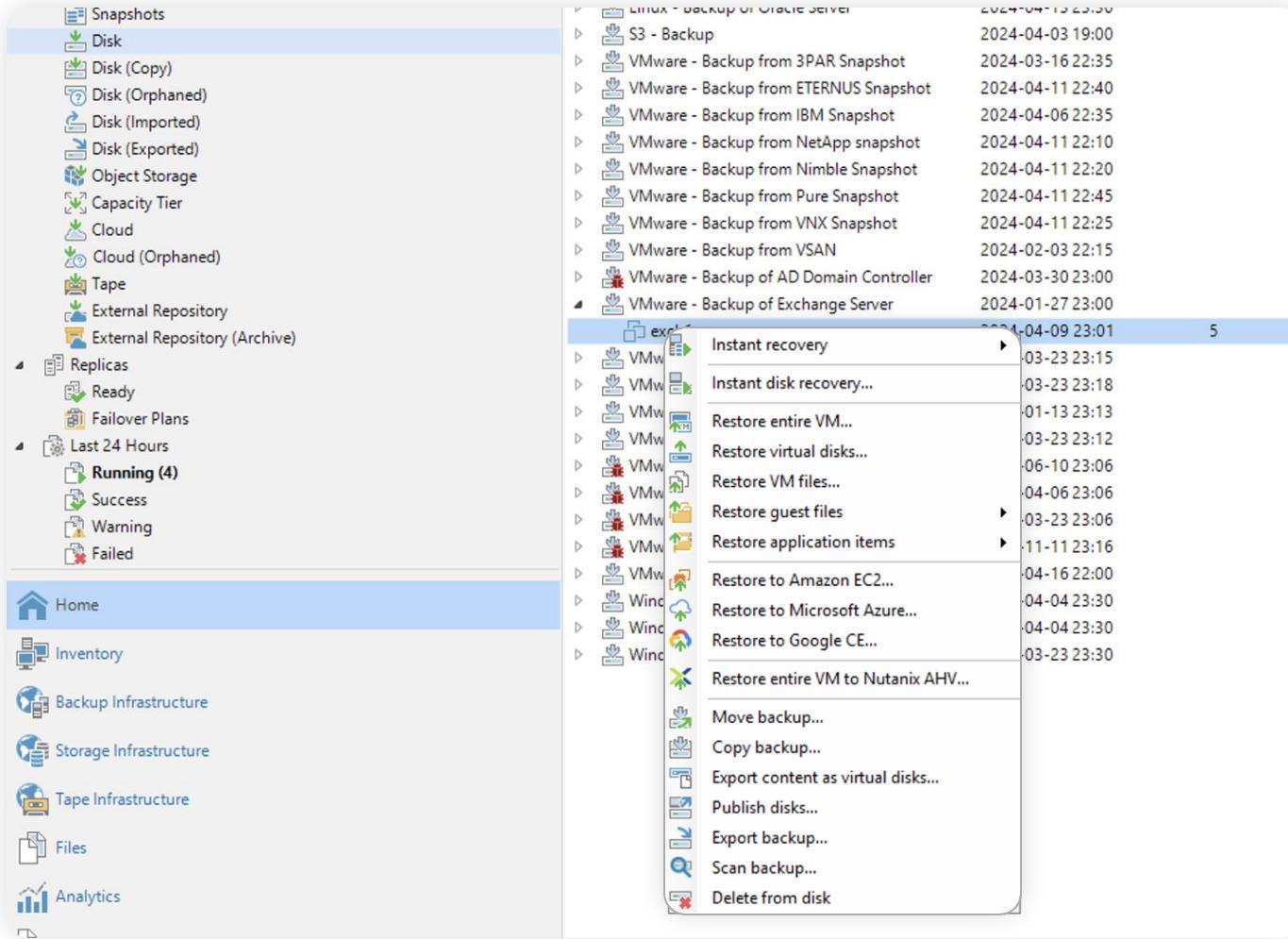
Ejemplo de proceso de creación de un trabajo de copia de seguridad



Restaurar

Restaurar

Numerosas opciones de restauración para reducir el tiempo de restauración.



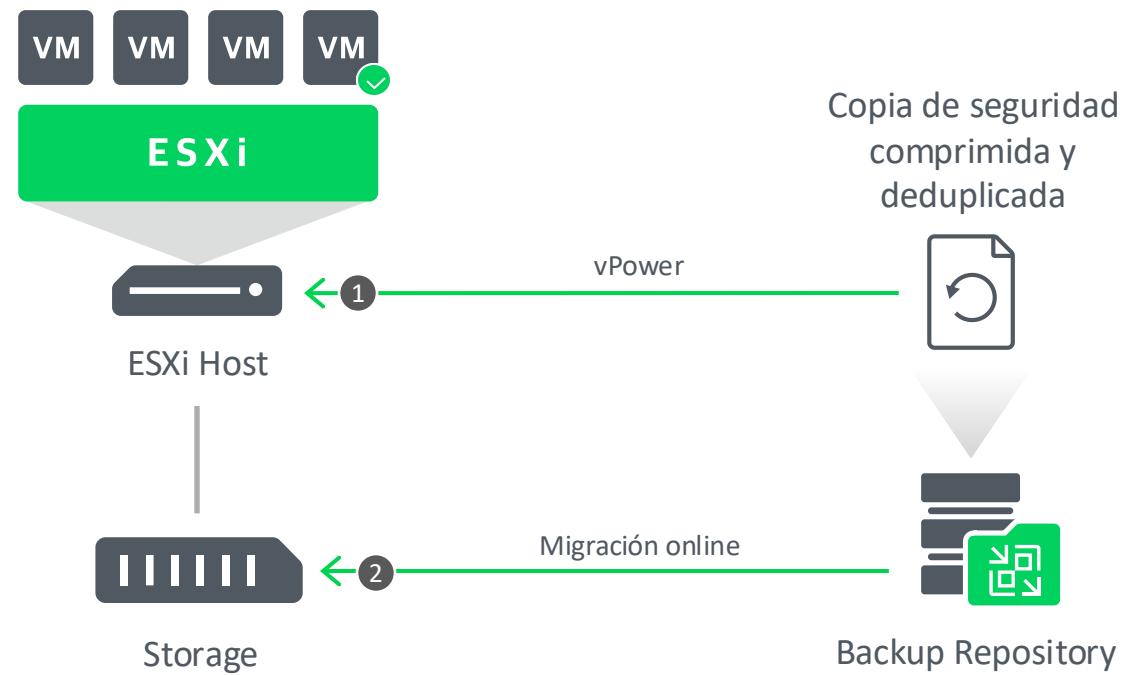
- Restauración de toda la VM
- Recuperación instantánea
- Restauración de discos virtuales
- Recuperación instantánea de discos
- Restauración de archivos VM
- Restauración de archivos guest
- Restauración de elementos de aplicación
- Restauración en Amazon EC2; Azure; Google CE
- Restauración a Nutanix AHV
- Exportar contenido como discos virtuales
- Publicar discos

Recuperación Instantánea

Con Instant Recovery, puede restaurar casi **inmediatamente** una máquina virtual en su entorno de producción ejecutándola directamente desde el archivo de copia de seguridad comprimido y deduplicado.

Instant Recovery ayuda a mejorar los objetivos de tiempo de recuperación, minimizar las interrupciones y el tiempo de inactividad de las máquinas virtuales de producción.

Instant Recovery puede utilizarse para restaurar datos de forma **cruzada entre hipervisores**, así como para recuperar **desde un servidor físico a una VM**.

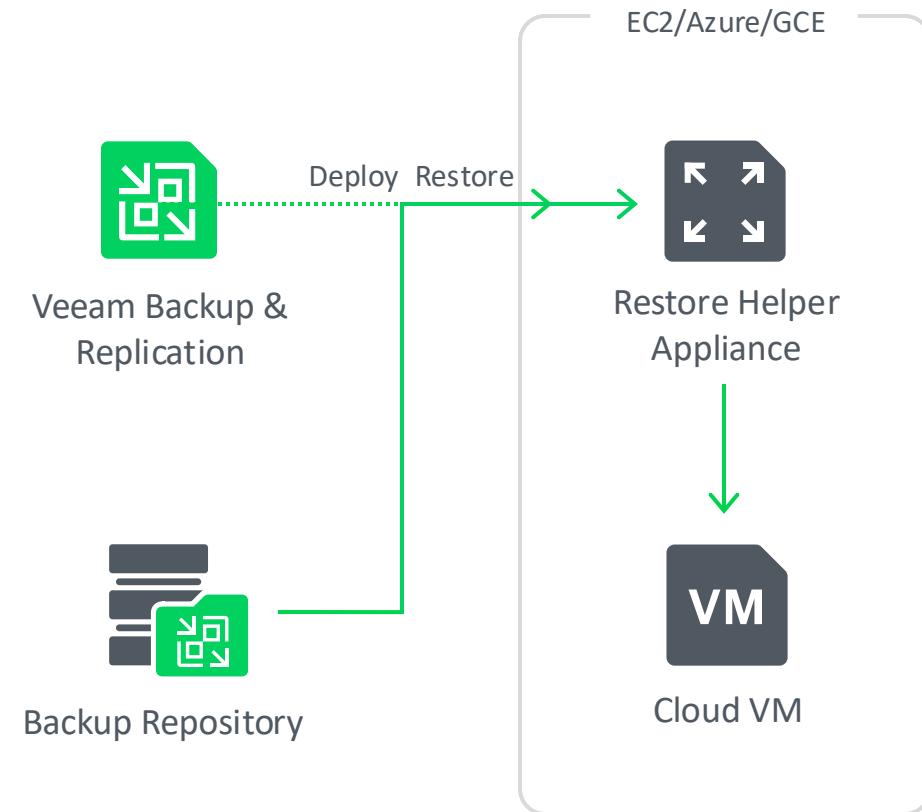


Restaurar a Amazon EC2/Azure/Google CE

Permite restaurar **máquinas virtuales y cargas de trabajo físicas** en la nube.

En el caso de **Amazon EC2 y Google CE**, VBR despliega automáticamente el helper appliance sólo durante el proceso de restauración y lo elimina inmediatamente después. El helper appliance **es opcional**, aunque puede mejorar significativamente el **rendimiento de la restauración**.

El Helper Appliance de **Azure son obligatorios y persistentes**. Una vez finalizado el proceso de restauración, el Helper Appliance se apagan y permanecen en Azure. El Appliance permanecen apagado hasta que se inicia un nuevo proceso de restauración.



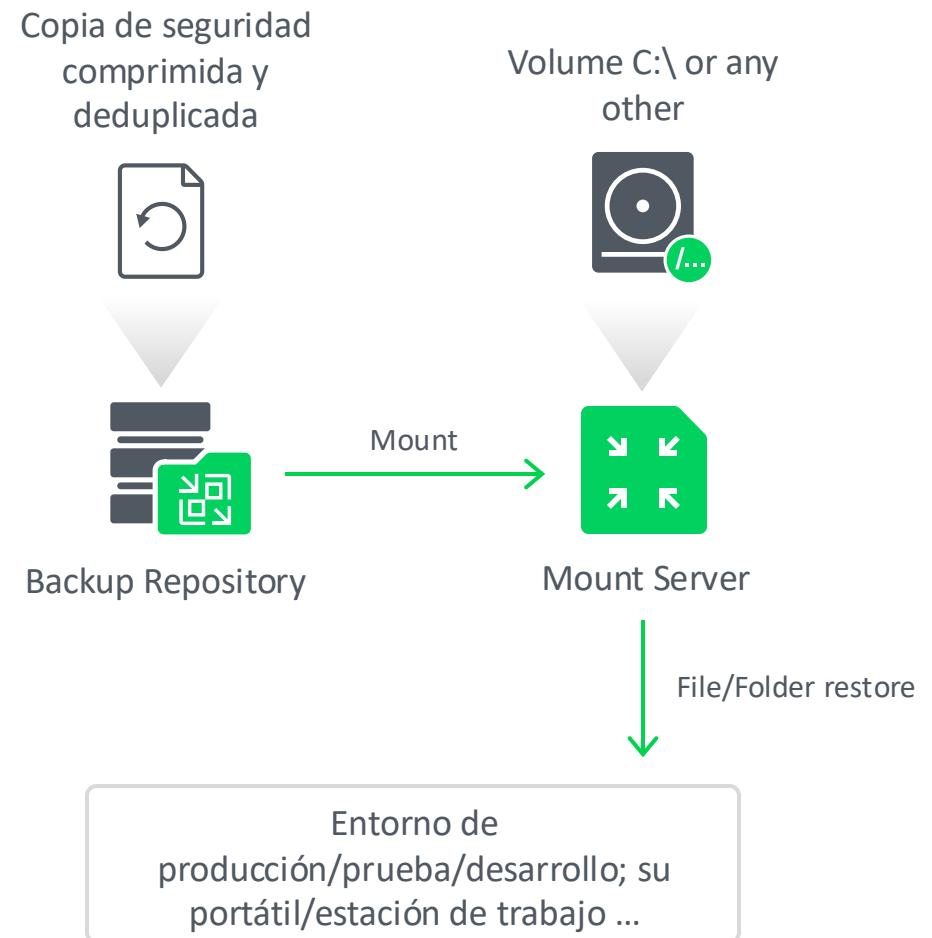
Restauración de Archivos de Guest (FLR)

Es posible restaurar **archivos específicos** directamente desde el SO guest, sin restaurar toda la máquina virtual o el servidor físico.

Formas de recuperación soportadas: Copias de seguridad, réplicas, snapshots de almacenamiento, instantáneas AHV de Nutanix.

Sistemas de archivos soportados:

- **Windows:** FAT, FAT32, NTFS, ReFS
- **Linux:** ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs, NTFS
- **BSD, Mac, Solaris** también son compatibles



Restauración de los Elementos de Aplicación

Los exploradores están disponibles para las siguientes aplicaciones:

Microsoft Active Directory

Microsoft SQL Server

Oracle PostgreSQL

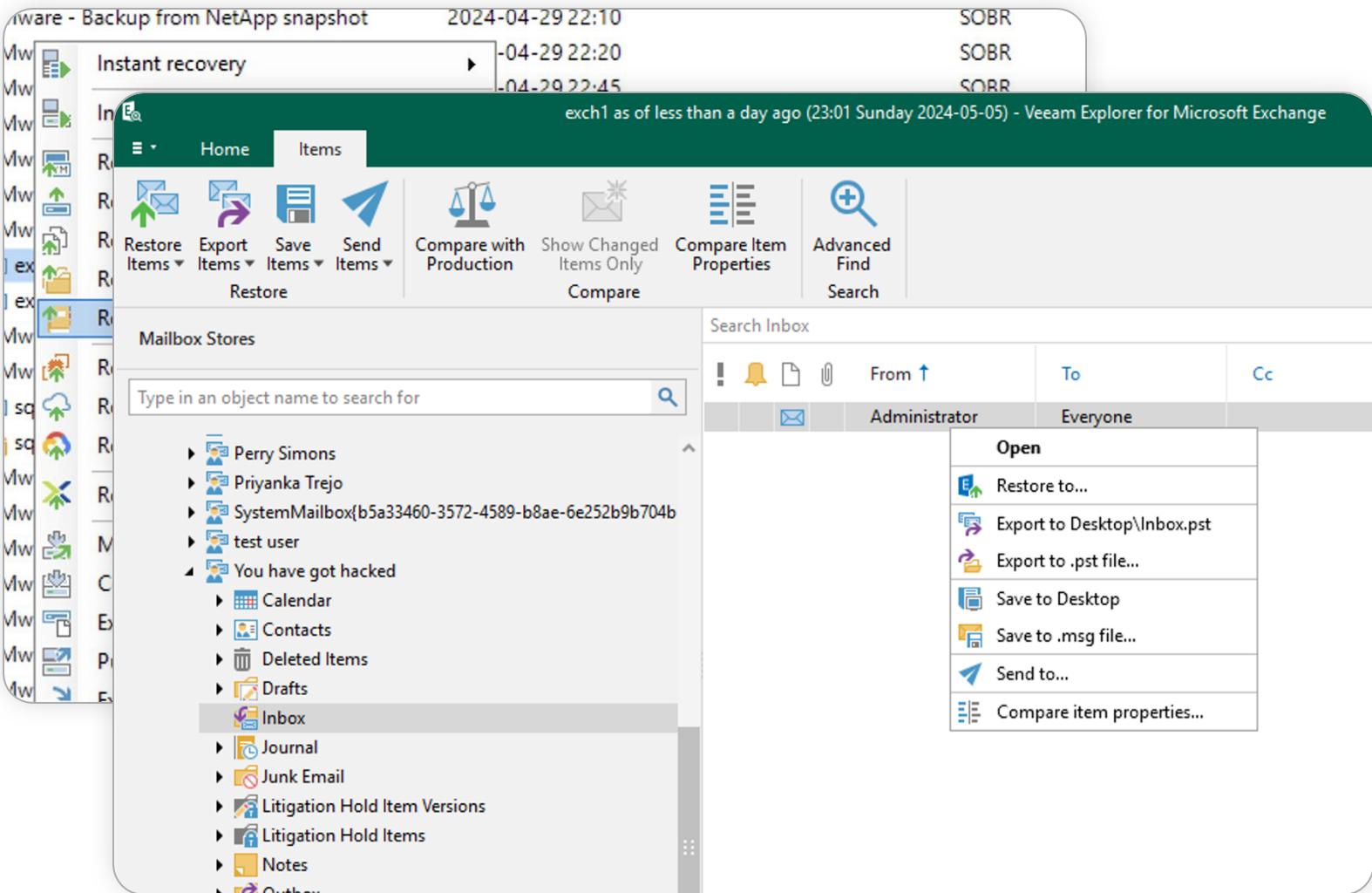
Microsoft Exchange

Microsoft SharePoint

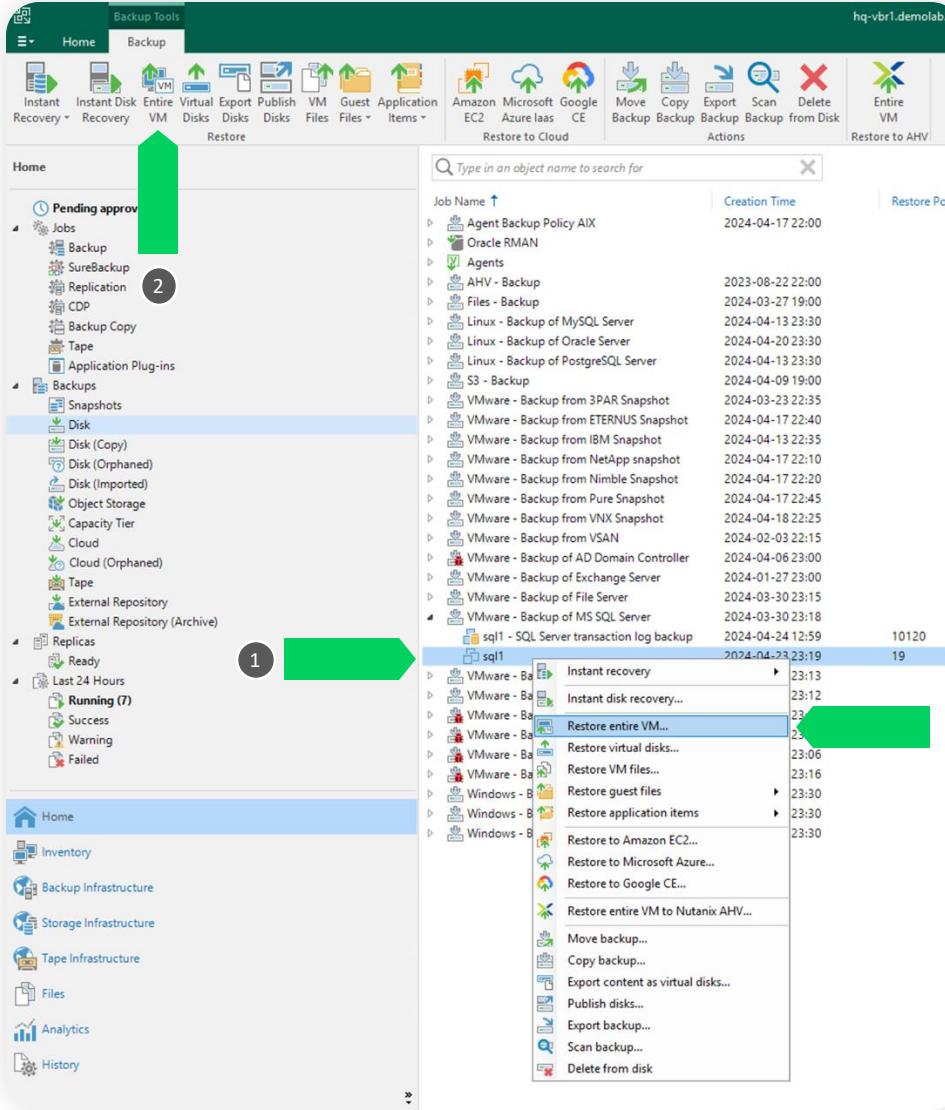
Microsoft OneDrive for Business

Microsoft Teams

Para utilizarlos, asegúrese de que sus copias de seguridad y réplicas se crean con application-aware processing activado.



¿Cómo restaurar una máquina virtual?



¿Cómo restaurar una máquina virtual?

Entire VM Restore

Virtual Machines
Select virtual machines to be restored. You can add individual virtual machines from backup files, or containers from live environment (containers will be automatically expanded into plain VM list).

Restore Points

Available restore points for sql1:

Job	Type	Location
VMware - Backup of MS SQL Server - sql1 (SOBR)	Increment	Performance Tier
less than a day ago (23:19 Tuesday 2024-04-23)	Increment	Performance Tier
1 day ago (23:19 Monday 2024-04-22)	Increment	Performance Tier
2 days ago (23:19 Sunday 2024-04-21)	Increment	Performance Tier
3 days ago (23:19 Saturday 2024-04-20)	Full (W)	Performance Tier
4 days ago (23:19 Friday 2024-04-19)	Increment	Performance Tier
5 days ago (23:19 Thursday 2024-04-18)	Increment	Performance Tier
6 days ago (23:19 Wednesday 2024-04-17)	Increment	Performance Tier
7 days ago (23:23 Tuesday 2024-04-16)	Increment	Performance Tier
8 days ago (23:19 Monday 2024-04-15)	Increment	Performance Tier
9 days ago (23:19 Sunday 2024-04-14)	Increment	Performance Tier
10 days ago (23:19 Saturday 2024-04-13)	Full (W)	Performance Tier
11 days ago (23:28 Friday 2024-04-12)	Increment	Performance Tier
12 days ago (23:19 Thursday 2024-04-11)	Increment	Performance Tier
13 days ago (23:19 Wednesday 2024-04-10)	Increment	Performance Tier
14 days ago (23:21 Tuesday 2024-04-09)	Increment	Performance Tier
15 days ago (23:20 Monday 2024-04-08)	Increment	Performance Tier
16 days ago (23:21 Sunday 2024-04-07)	Increment	Performance Tier

Add... Point... Remove

OK Cancel

< Previous Next > Finish Cancel

¿Cómo restaurar una máquina virtual?

Entire VM Restore

 **Restore Mode**
Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.

Virtual Machines  **Restore to the original location**
Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error.

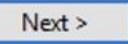
Restore Mode  **Restore to a new location, or with different settings**
Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.

Host
Resource Pool
Datastore
Folder
Network

Secure Restore

Reason

Summary  **Quick rollback (restore changed blocks only)**
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

< Previous  Next > Finish Cancel

¿Cómo restaurar una máquina virtual?

Entire VM Restore

Host

By default, original host is selected as restore destination for each VM. You can change host by selecting desired VM and clicking Host. Use multi-select (Ctrl-click and Shift-click) to select multiple VMs at once.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Reason

Summary

VM location:

Name	Host
sql1	hq-esx2.demolab.local

Select multiple VMs and click Host to apply changes in bulk.

Host...

< Previous Next > Finish Cancel

¿Cómo restaurar una máquina virtual?

Entire VM Restore

 Resource Pool
By default, original resource pool is selected as restore destination for each VM. You can change resource pool by selecting desired VM and clicking Pool. Use multi-select (Ctrl-click and Shift-click) to select multiple VMs at once.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Reason

Summary

VM resource pool:

Name	Resource Pool
sql1	Resources

Select multiple VMs and click Pool to apply changes in bulk. **Pool...**

< Previous Next > Finish Cancel



¿Cómo restaurar una máquina virtual?

Entire VM Restore

Datastore
By default, original datastore and disk type are selected for each VM file. You can change them by selecting desired VM file, and clicking Datastore or Disk Type. Use multi-select (Ctrl-click and Shift-click) to select multiple VMs at once.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Reason

Summary

Files location:

File	Size	Datastore	Disk type
sql1	[688.1 GB f...		
Configuration	[688.1 GB f...	Same as source	
Hard disk 1	[688.1 GB f...	Same as source	
Hard disk 2	[688.1 GB f...	Same as source	
Hard disk 3	[688.1 GB f...	Same as source	

Disk Type Settings

Restored VM disk type:

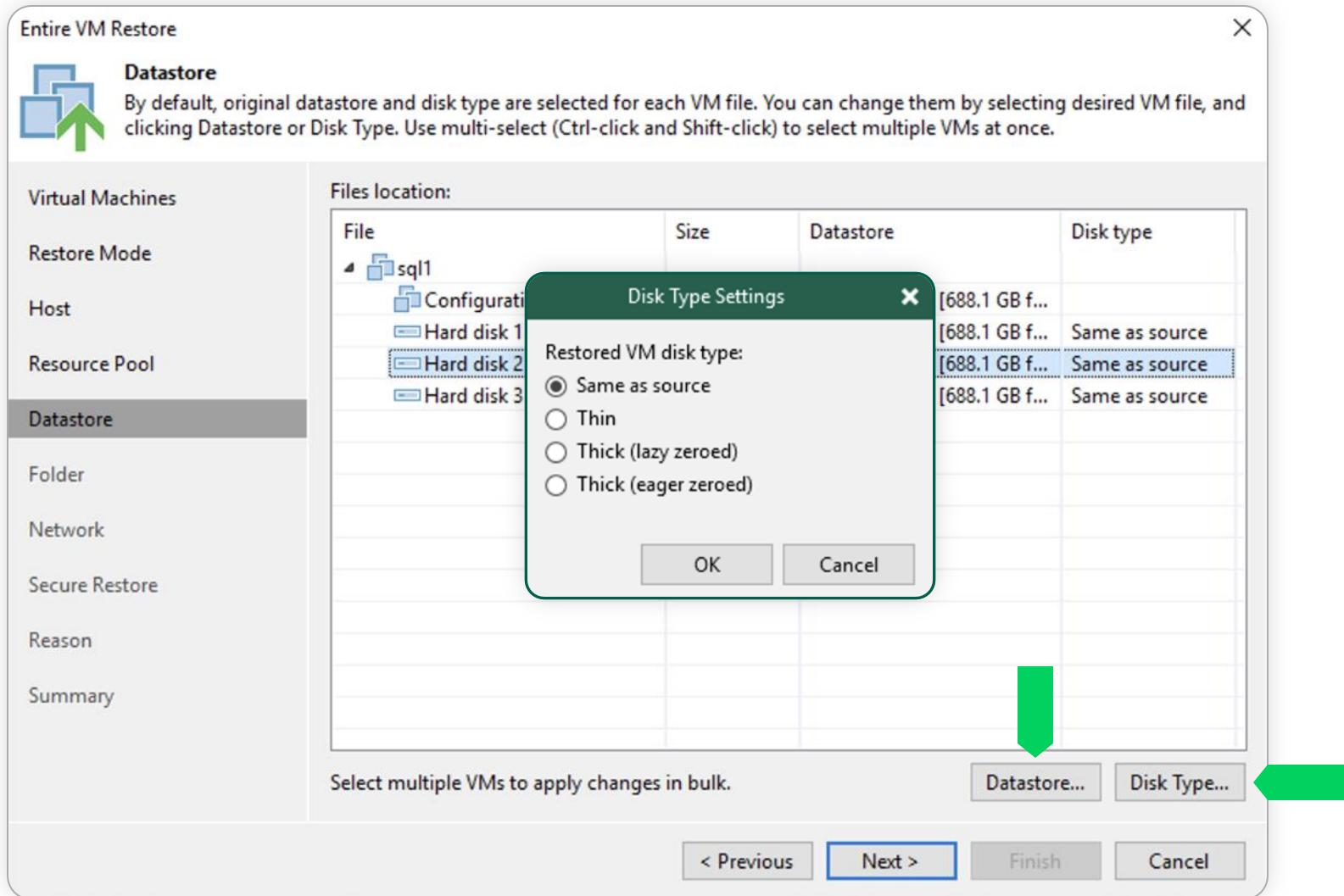
Same as source
 Thin
 Thick (lazy zeroed)
 Thick (eager zeroed)

OK Cancel

Select multiple VMs to apply changes in bulk.

Datastore... Disk Type...

< Previous Next > Finish Cancel



A screenshot of the Veeam Backup & Replication software interface during an 'Entire VM Restore' process. The left sidebar shows navigation options like Virtual Machines, Host, Resource Pool, Datastore (which is selected and highlighted in grey), Folder, Network, Secure Restore, Reason, and Summary. The main area displays a table of files for a VM named 'sql1'. The table includes columns for File, Size, Datastore, and Disk type. There are four hard disk entries, all currently set to 'Same as source'. A modal dialog titled 'Disk Type Settings' is open over the table, showing four radio button options: 'Same as source' (selected), 'Thin', 'Thick (lazy zeroed)', and 'Thick (eager zeroed)'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. A large green arrow points downwards from the 'Disk Type Settings' dialog towards the 'Disk Type...' button located at the bottom right of the main window. The bottom of the window features standard navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

¿Cómo restaurar una máquina virtual?

Entire VM Restore

Folder

By default, original VM folder is selected as restore destination for each VM. You can change folder by selecting desired VM and clicking Folder. Use multi-select (Ctrl-click and Shift-click) to select multiple VMs at once.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Reason

Summary

VM Folder:

Name	New Name	Folder
sql1	sql1	vm

Select multiple VMs to apply settings change in bulk.

Restore VM tags
Select this option to restore VM tags that were assigned to the VM when backup was taken.

Next >

Finish

Cancel

¿Cómo restaurar una máquina virtual?

Entire VM Restore

Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Reason

Summary

Network connections:

Source	Target
sql1	hq-lan (dvs-hq)

Select multiple VMs to apply settings change in bulk.

Network... Disconnect

< Previous Next > Finish Cancel

The screenshot shows the 'Network' configuration step of the Veeam Entire VM Restore wizard. It displays a table of network connections for a single VM named 'sql1'. The 'Source' column lists 'sql1' and its network 'hq-lan (dvs-hq)'. The 'Target' column also lists 'hq-lan (dvs-hq)'. At the bottom of the dialog, there are two buttons: 'Network...' and 'Disconnect'. A green arrow points down to the 'Network...' button, and another green arrow points left from the 'Disconnect' button towards the 'Network...' button, highlighting the action of mapping networks.

¿Cómo restaurar una máquina virtual?

Entire VM Restore

Secure Restore

Scan the selected backup for malware, such as computer viruses or ransomware, prior to performing the restore. This requires a compatible antivirus installed on the mount server specified for the corresponding backup repository.



Virtual Machines	Content scan
Restore Mode	<input checked="" type="checkbox"/> Scan the restore point with an antivirus engine <input checked="" type="checkbox"/> Scan the restore point with the following YARA rule:
Host	<input type="text" value="FindFileByHash.yara"/>
Resource Pool	Copy YARA rules location to clipboard
Datastore	Scan options: <input checked="" type="radio"/> Proceed with recovery but disable network adapters <input type="radio"/> Abort VM recovery <input type="checkbox"/> Continue scanning all remaining files after the first occurrence
Folder	
Network	
Secure Restore	
Reason	
Summary	

< Previous Next > Finish Cancel

¿Cómo restaurar una máquina virtual?

Entire VM Restore

 **Reason**
Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.

Virtual Machines Restore reason:

Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Reason
Summary

Do not show me this page again

< Previous Next > Finish Cancel

¿Cómo restaurar una máquina virtual?

Entire VM Restore

 **Summary**
Review the restore settings and click Finish to start the restore process.

Virtual Machines **Summary:**

Original machine name: sql1
New machine name: sql1_restore_demo
Restore point: less than a day ago (23:19 Tuesday 2024-04-23)
Target host: hq-esx2.demolab.local
Target resource pool: Resources
Target VM folder: vm
Target datastore: hq-datastore1
Network mapping:
 hq-lan (dvs-hq) -> hq-lan (dvs-hq)

Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Reason

Proxy: Automatic selection

 Power on target VM after restoring

< Previous Next > **Finish** Cancel

Seguridad

Mejores Prácticas: Seguridad y Resiliencia

Security & Compliance Analyzer (Analizador de Seguridad y Cumplimiento)

Veeam Backup & Replication proporciona una herramienta integrada para garantizar que la configuración de su servidor de backup siga las **mejores prácticas de seguridad** para los componentes de la infraestructura de backup de Veeam basados en los sistemas operativos Microsoft Windows Server y Linux.

Incluye **11 Comprobaciones de Seguridad** y **19 Comprobaciones de Configuración del producto**

The screenshot shows the Veeam Security & Compliance Analyzer interface. On the left is a navigation pane with tabs for Home, View, and various backup and replication jobs. The main area displays a table of best practices categorized into 'Backup infrastructure security' and 'Product configuration'. Each row includes a status indicator (e.g., Passed, Not implemented, Failed) and a detailed description. To the right of the table is a sidebar with buttons for Analyze, Schedule, Suppress, Reset, and Reset All. Below the table is a 'Last run...' button. The top right corner shows the title '- Veeam Backup and Replication'.

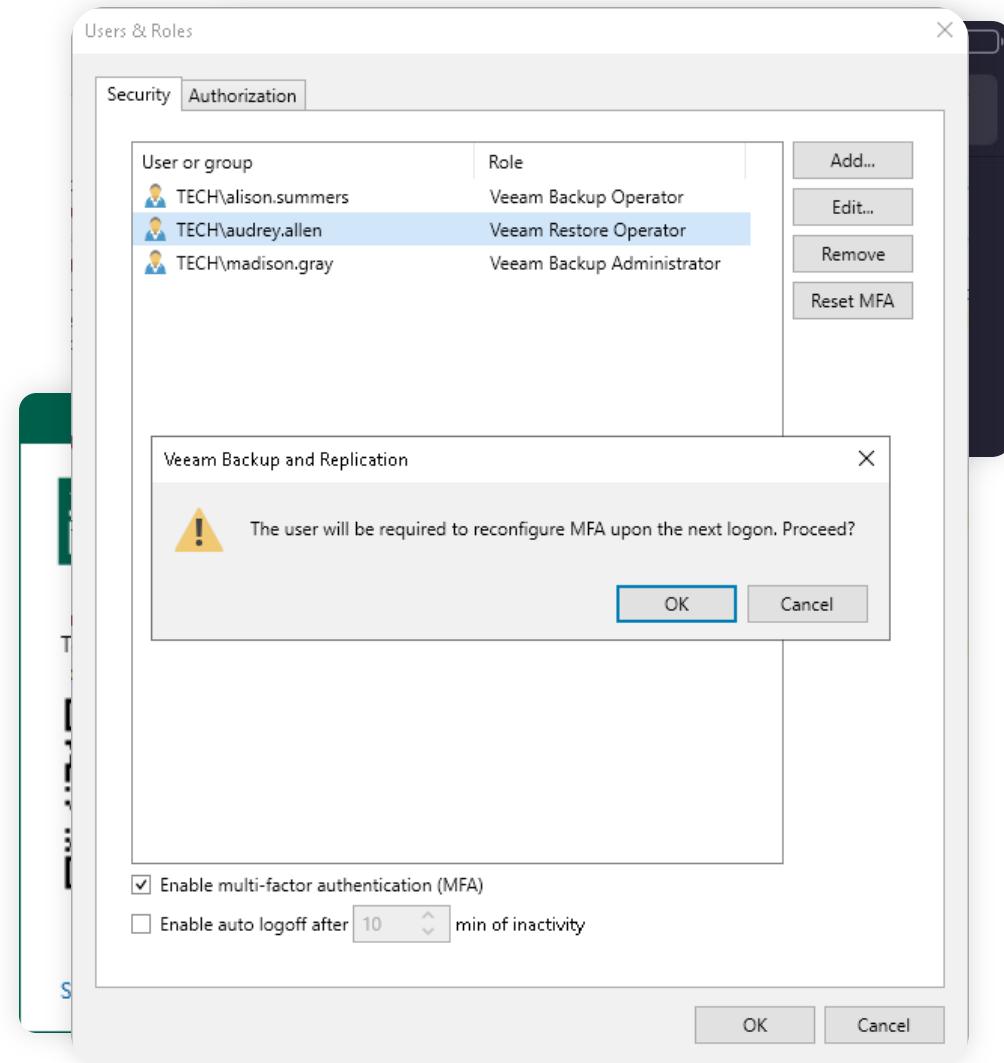
Best Practice	Status
Remote Desktop Service (TermService) should be disabled	Not implemented
Remote Registry service (RemoteRegistry) should be disabled	Not implemented
Windows Remote Management (WinRM) service should be disabled	Not implemented
Windows Firewall should be enabled	Passed
WDigest credentials caching should be disabled	Passed
Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled	Not implemented
Deprecated versions of SSL and TLS should be disabled	Not implemented
Windows Script Host should be disabled	Not implemented
SMBv1 protocol should be disabled	Passed
Link-Local Multicast Name Resolution (LLMNR) should be disabled	Not implemented
SMBv3 signing and encryption should be enabled	Not implemented
Product configuration	
MFA for the backup console should be enabled	Not implemented
Immutable or offline (air gapped) media should be used	Not implemented
Password loss protection should be enabled	Passed
Backup server should not be a part of the production domain	Unable to detect
Email notifications should be enabled	Not implemented
All backups should have at least one copy (the 3-2-1 backup rule)	Not implemented
Reverse incremental backup mode is deprecated and should be avoided	Passed
Unknown Linux servers should not be trusted automatically	Not implemented
The configuration backup must not be stored on the backup server	Not implemented
Host to proxy traffic encryption should be enabled for the Network transport mode	Passed
Hardened repositories should not be hosted in virtual machines	Passed
Network traffic encryption should be enabled in the backup network	Passed
Linux servers should have password-based authentication disabled	Passed
Backup services should be running under the LocalSystem account	Passed
Configuration backup should be enabled and use encryption	Not implemented
Credentials and encryption passwords should be rotated at least annually	Passed
Hardened repositories should have the SSH Server disabled	Passed
S3 Object Lock in the Governance mode doesn't provide true immutability	Passed
Backup jobs to cloud repositories should use encryption	Passed

Mejores Prácticas: Seguridad y Resiliencia

Multi-Factor Authentication (Autenticación Multifactor)

Veeam Backup & Replication es compatible con la autenticación multifactor (MFA) para la verificación adicional del usuario.

Como segundo método de verificación, se utiliza una contraseña de un solo uso (OTP) generada en la aplicación del autenticador móvil. Combinado con las credenciales de inicio de sesión y contraseña, crea un entorno más seguro y protege las cuentas de los usuarios frente a posibles ataques.

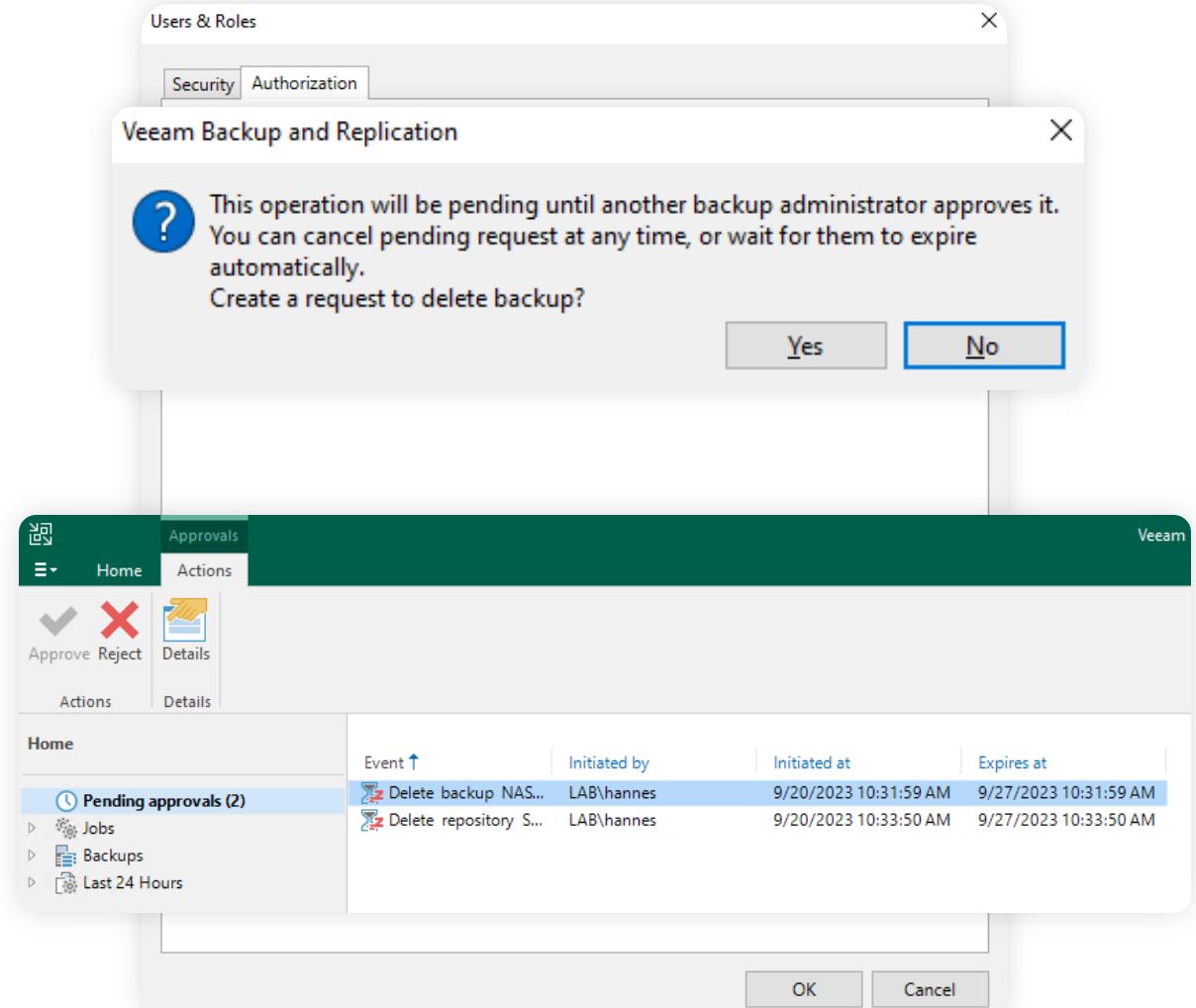


Mejores Prácticas: Seguridad y Resiliencia

Four-Eyes Authorization (Autorización de Cuatro Ojos)

Esta función evita la **eliminación accidental o errónea de copias de seguridad o repositorios de copia de seguridad completos, cambios en los usuarios, roles y otras configuraciones de acceso** mediante la consola, al requerir la aprobación de un **segundo administrador de Veeam Backup** antes de que se puedan aplicar los cambios solicitados a estas configuraciones sensibles del servidor de copia de seguridad.

Todos los eventos relacionados con la autorización de cuatro ojos se muestran en la **vista Histórial**, en el nodo **Eventos de Autorización**.

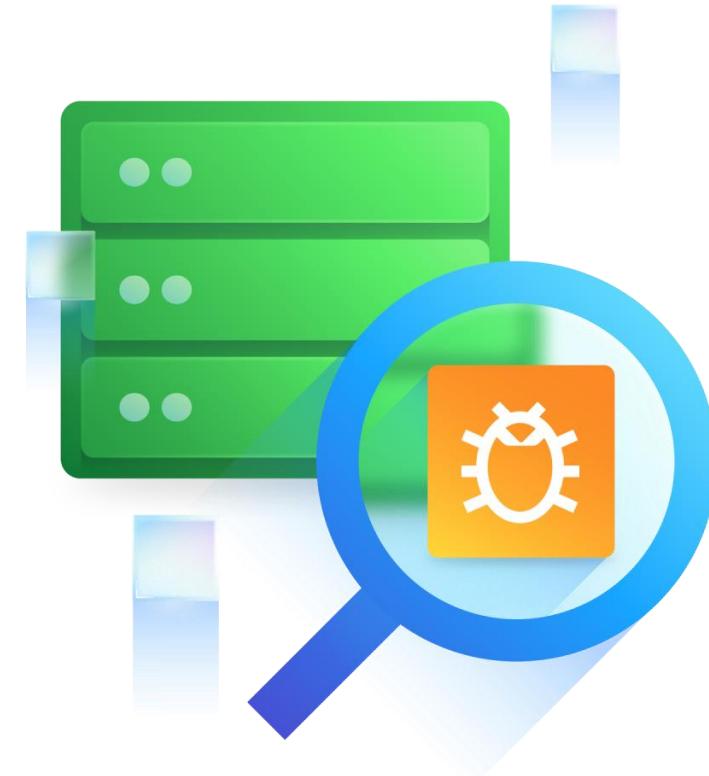


Mejores Prácticas: Seguridad y Resiliencia

Malware Detection (Detección de Malware)

La detección de malware con Veeam se enfoca en detectar malware y actividad sospechosa tanto en la infraestructura de producción como en la de backup y enviar notificaciones al respecto.

A partir de la versión 12.1 de Veeam, podemos identificar incluso el malware durmiente en producción. También es posible escanear las copias de seguridad ya realizadas y almacenadas en el repositorio.



Mejores Prácticas: Seguridad y Resiliencia

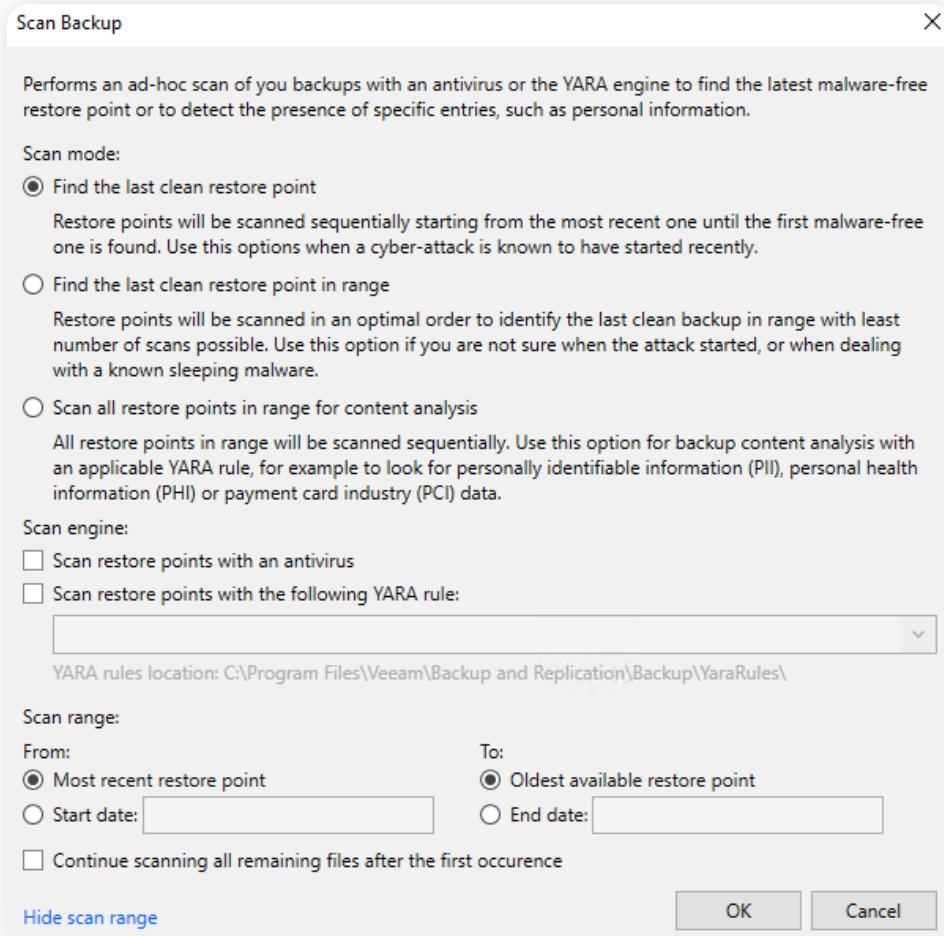
Malware Detection. Análisis a pedido de Malware y Contenido.

Aprovecha el **Antivirus** y/o el análisis **YARA**.

Ofrece **tres modos de escaneo** con múltiples alcances:

- Buscar (primera) copia(s) de seguridad limpia(s)
- Buscar copia de seguridad limpia en el rango
- Buscar contenido (por ejemplo, números de tarjetas de crédito)

El escaneo se realiza en el **servidor de montaje**.



Mejores Prácticas: Seguridad y Resiliencia

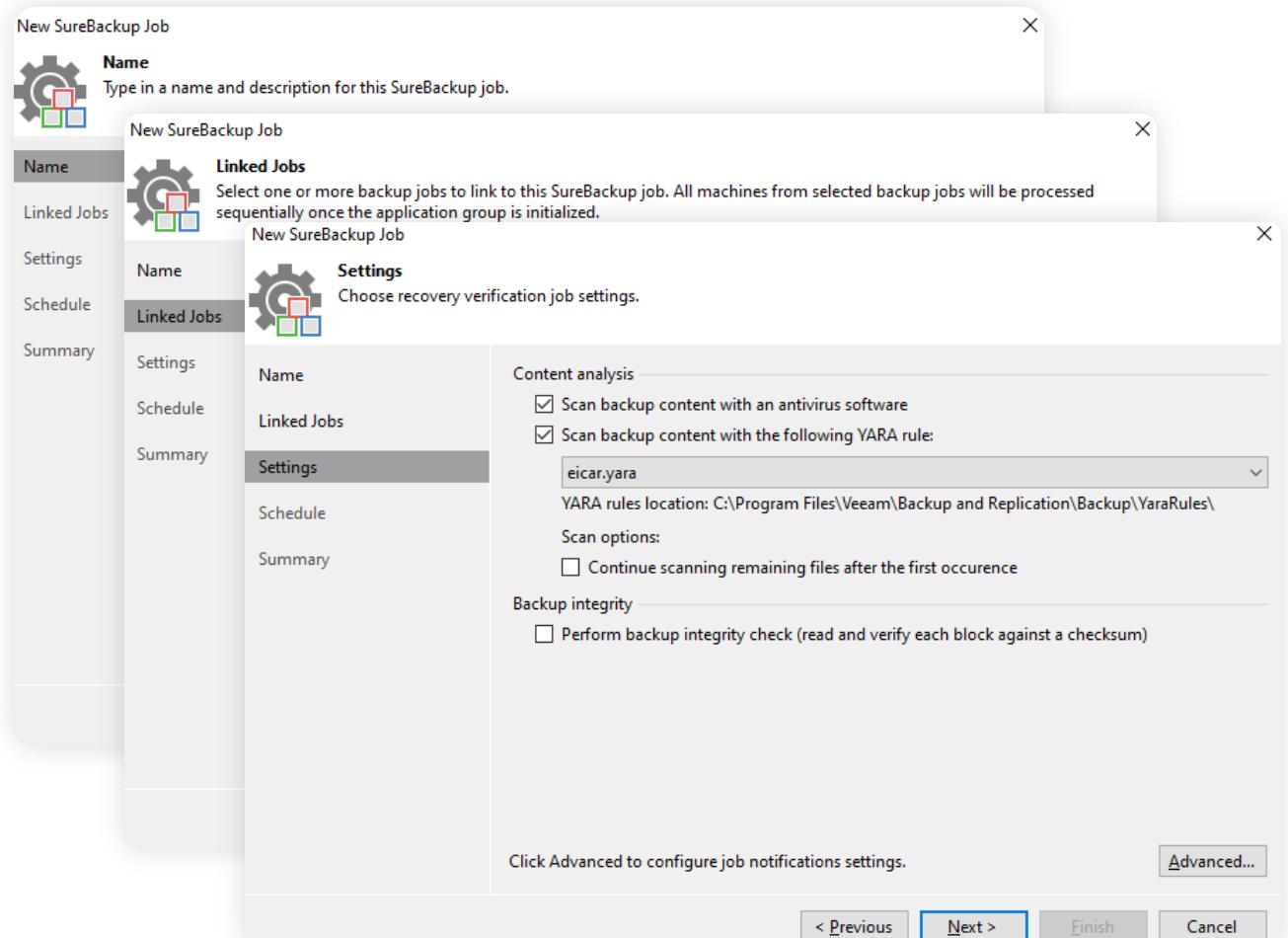
Malware Detection. Análisis Automatizados de Malware y Contenidos.

Activado en un trabajo de **SureBackup**.

Aprovecha el análisis **Antivirus** y/o **YARA**.

Analiza **todo el trabajo de copia de seguridad** (es posible realizar exclusiones).

El análisis se realiza en el **servidor de montaje**.



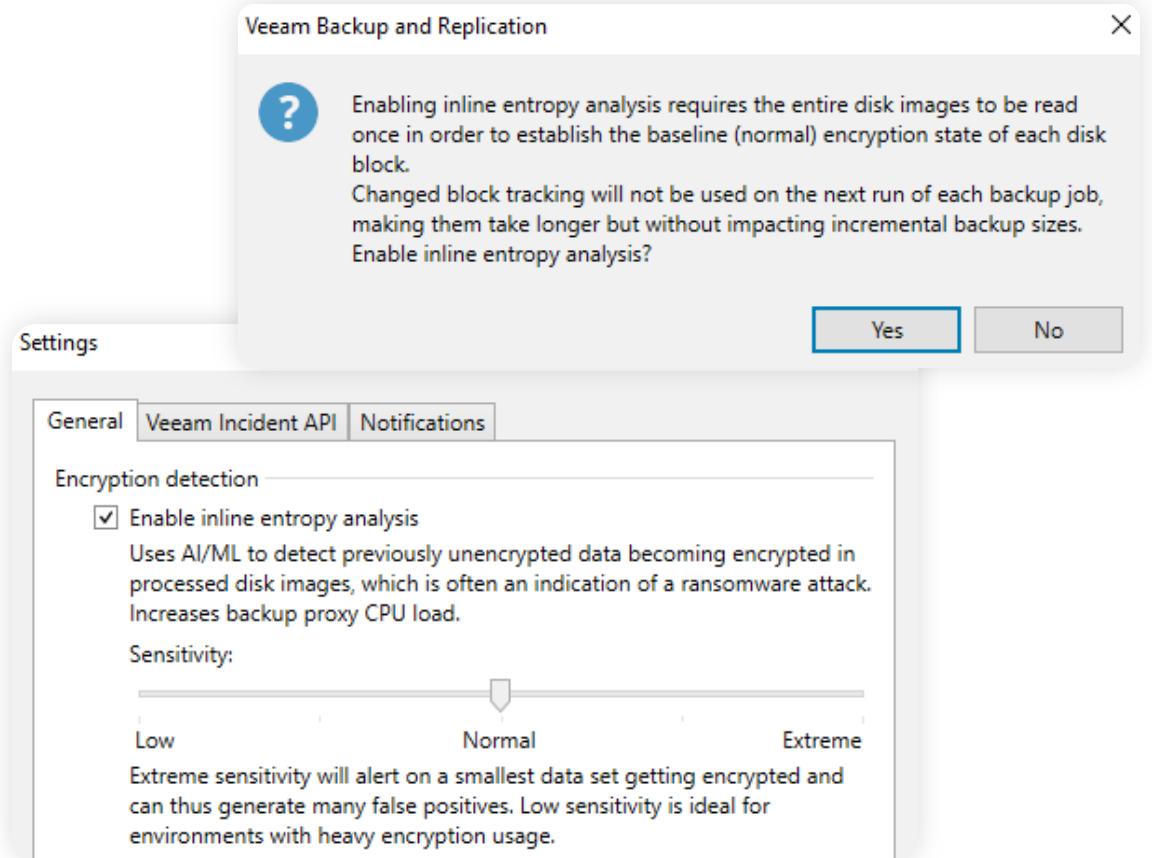
Mejores Prácticas: Seguridad y Resiliencia

Malware Detection. Escaneo en Línea: Cifrado y Análisis de Texto.

Analiza los datos a nivel de bloque durante la copia de seguridad.

Mediante un **modelo de aprendizaje automático entrenado** y un **análisis de entropía** de bajo impacto, Veeam puede **detectar datos cifrados por ransomware**.

El mismo motor **detecta otros signos de malware o ciberataque**, como enlaces Onion, directamente en el stream de backup.



Mejores Prácticas: Seguridad y Resiliencia

Malware Detection. Cómo funciona el Escaneo en Línea.

Backup Properties BJ-malwaretest (Default Backup Repository)

Objects:

Name	Original Size
HK-1944-rn-enc	177 GB
HK-1944-rn-ren	178 GB

Total size: 356 GB

Restore points:

Date	Type	Status
9/20/2023 10:13:06 AM	Increment	Suspicious
9/20/2023 8:48:16 AM	Increment	Suspicious
9/20/2023 7:48:34 AM	Increment	OK
9/20/2023 7:34:44 AM	Increment	OK
9/20/2023 7:25:06 AM	Increment	OK
9/19/2023 6:45:49 PM	Full	OK

Restore points: 6

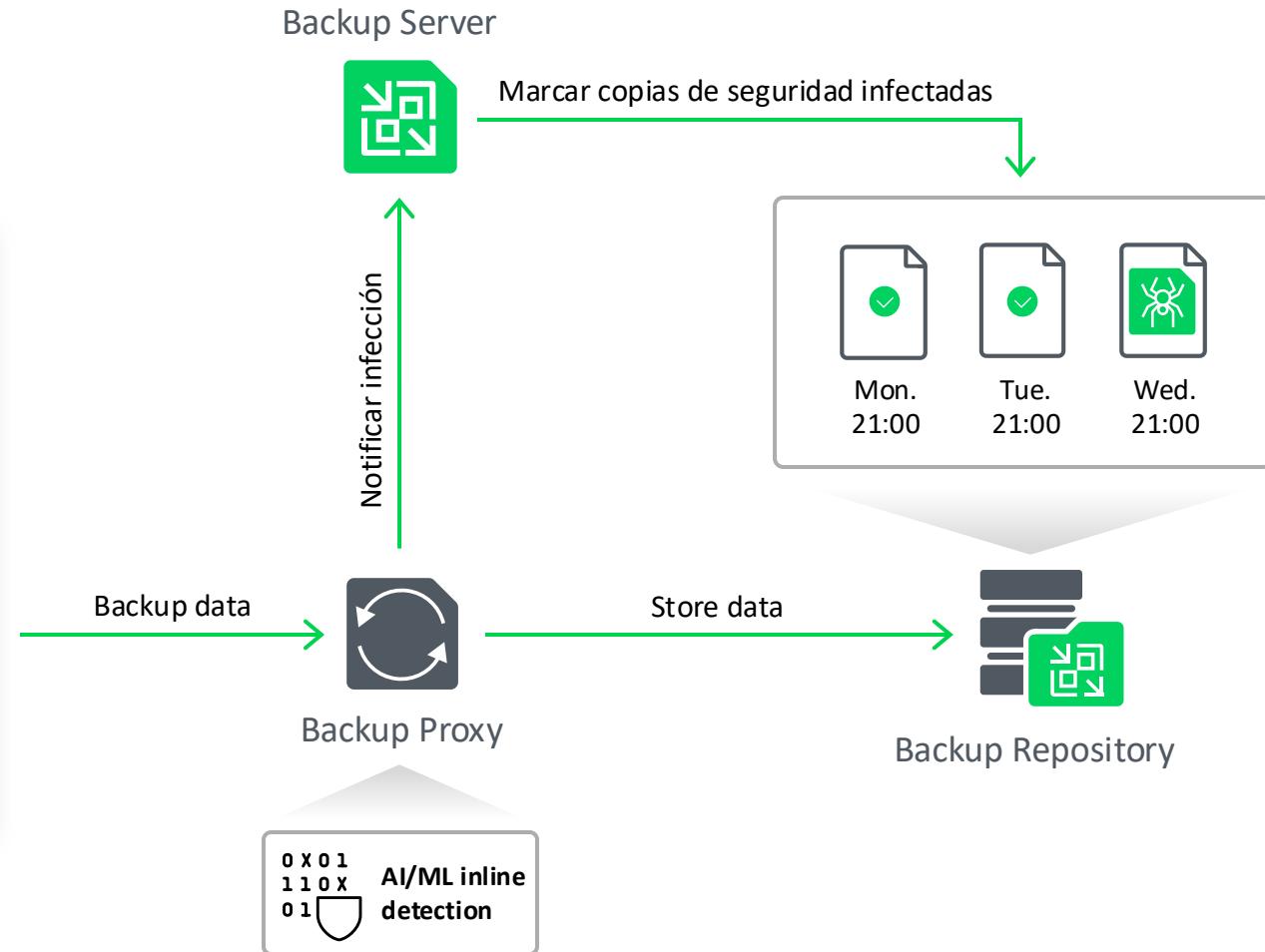
Files:

Name	Data Size	Backup Size	Deduplication	Compression	Date
HK-1944-rn-enc.vm-108443D2023-0...	0 B	0 B	1.0 x	1.0 x	9/20/2023 10:06:24 AM
HK-1944-rn-enc.vm-108443D2023-0...	800 MB	445 MB	1.0 x	1.8 x	9/20/2023 8:41:09 AM
HK-1944-rn-enc.vm-108443D2023-0...	1.59 GB	667 MB	1.0 x	2.5 x	9/20/2023 7:46:15 AM
HK-1944-rn-enc.vm-108443D2023-0...	2.01 GB	948 MB	1.0 x	2.2 x	9/20/2023 7:32:15 AM
HK-1944-rn-enc.vm-108443D2023-0...	1.11 GB	398 MB	1.0 x	2.9 x	9/20/2023 7:22:32 AM
HK-1944-rn-enc.vm-108443D2023-0...	260 GB	99.0 GB	1.4 x	1.8 x	9/19/2023 6:32:42 PM

Backup size: 201 GB

Copy path Malware

Close

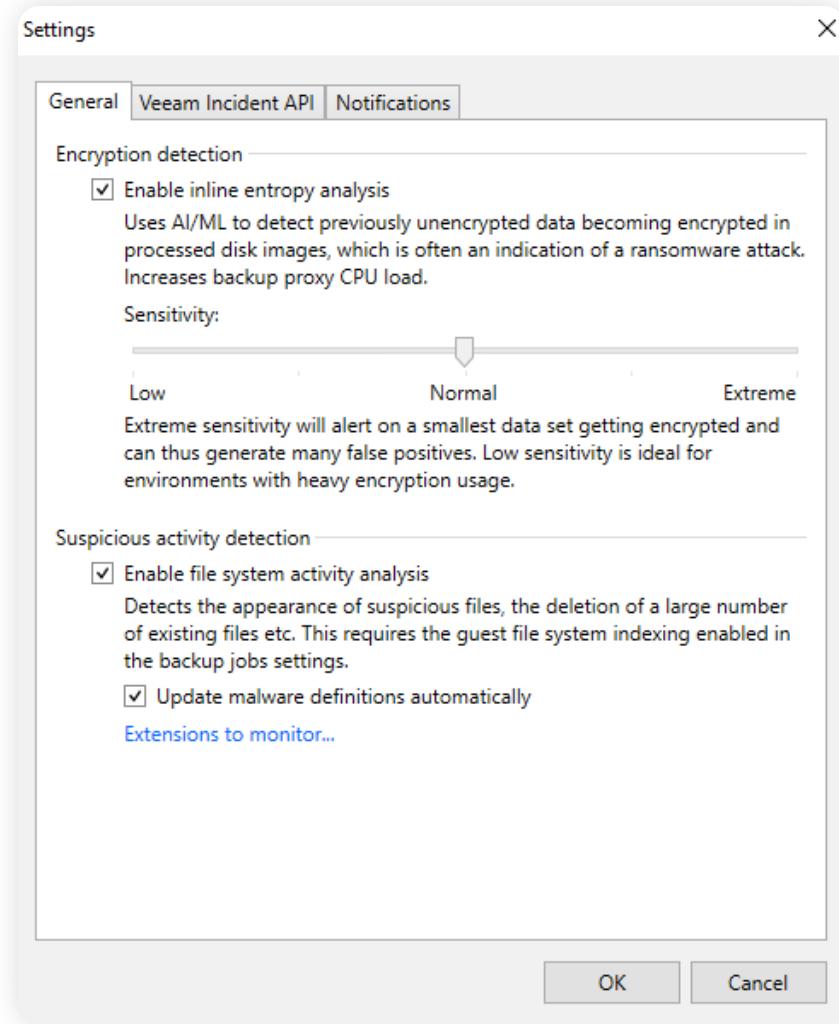


Mejores Prácticas: Seguridad y Resiliencia

Malware Detection. Detección mediante Índice de Guest.

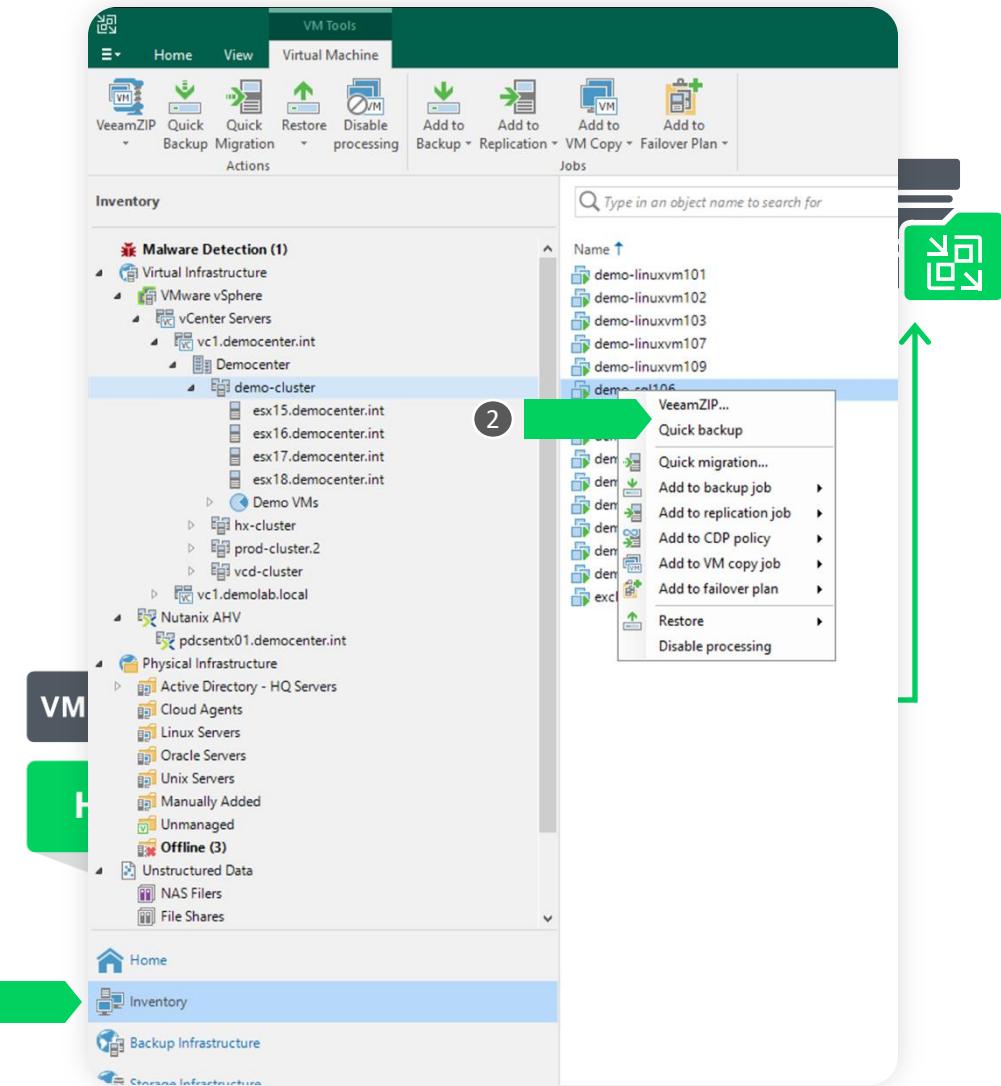
También se conoce como **Detección de Actividad Sospechosa** en el Sistema de Archivos por su capacidad de buscar archivos con extensiones de malware conocidas, notas de rescate y señales similares de presencia de malware.

Analiza la actividad del sistema de archivos comparando los índices de guest para detectar cambios sospechosos, como eliminaciones masivas o cambios de nombre de archivos conocidos.



Trucos y Consejos

Quick Backup & VeeamZIP



Quick Backup ofrece copias de seguridad incrementales bajo demanda para VMs sin necesidad de configurar un nuevo trabajo. Agrega un punto de restauración adicional a las cadenas de copias de seguridad existentes, adecuado tanto para copias de seguridad incrementales como incrementales inversas. Sin embargo, requiere una copia de seguridad completa previa de los equipos virtuales.

VeeamZIP funciona como una copia de seguridad completa de VM, creando un archivo de copia de seguridad completa independiente (.vbk). Puedes almacenar este archivo en varias ubicaciones, pero ten en cuenta: los archivos de copia de seguridad de VeeamZIP aparecen en “Backups - Disk (Exported)” en la vista de inicio.

Quick Backup y VeeamZIP pueden crearse desde la **vista Inventory**.

Enterprise Manager + vCenter

Veeam Plug-in for VMware vSphere Client **simplifica la administración de backup para los administradores de vSphere**. Les permite comprobar el estado de Veeam Backup & Replication, supervisar los resultados de los trabajos y ver las estadísticas de almacenamiento directamente en vSphere Client.

Los administradores pueden **identificar las máquinas virtuales desprotegidas, planificar la capacidad y crear puntos de restauración** utilizando VeeamZIP y Quick Backup.

Detalles de Configuración:

- vSphere Client 7.0.0 or earlier – instalación local en vCenter Server.
- vSphere Client 7.0.1 or later – instalación remota en Veeam Backup Enterprise Manager server.



Enterprise Manager + vCenter

The screenshot shows the Veeam Backup & Replication interface running within the vSphere Client. The top navigation bar includes the vSphere Client logo, a 'Menu' dropdown, a search bar, and various system icons.

Veeam Backup & Replication

Summary

Summary **Settings**

Veeam Backup & Replication

Backup servers: 2
Proxy servers: 6
Repository servers: 5
Running jobs: 0
Scheduled jobs: 13

Successful VM Backups 15 (83%)
VMs with warnings 3 (17%)
Failed VMs 0 (0%)

VMs Overview

- Protected VMs:** 11
 - Backed Up
 - Replicated
- Restore points:** 14
 - Full backup size
 - Incremental backup size
 - Replica restore points size
 - Source VMs size
 - Successful backup sessions ratio

Last 24 Hours **View Protected VMs Report...**

Job Statistics

- Running jobs:** 0
- Scheduled jobs:** 13
 - Backup
 - Replica
- Total jobs runs:** 13
 - Successful jobs
 - Jobs with warnings
 - Jobs with errors
- Max job duration:** 3 hours 52 mins

Last 24 Hours **View Latest Backup Job Status Report...**

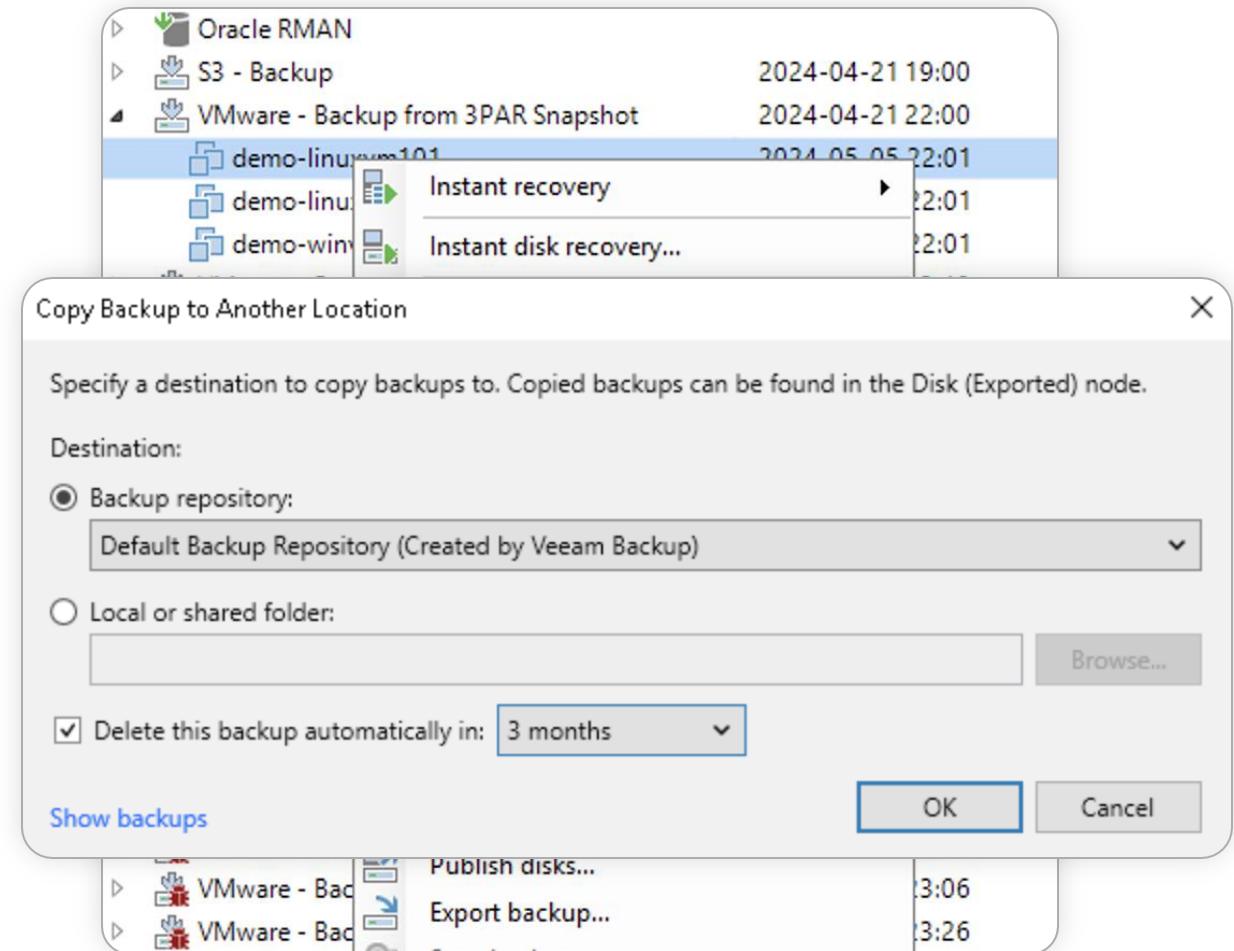
Recent Tasks **Alarms**

Copy and Move Backup

Veeam Backup & Replication permite mover todas las copias de seguridad de un trabajo de copia de seguridad a otro repositorio o mover cargas de trabajo específicas y sus copias de seguridad a otro trabajo.

Ejemplos de uso:

- Mover copias de seguridad a otro repositorio
- Mover copias de seguridad a otro trabajo
- Copiar copias de seguridad a otro repositorio
- Migrar ReFS a XFS para un Repositorio Reforzado
- Migrar NTFS a ReFS
- Reequilibrar Repositorio Scale-Out
- Evacuación de la extensión del repositorio Scale-Out

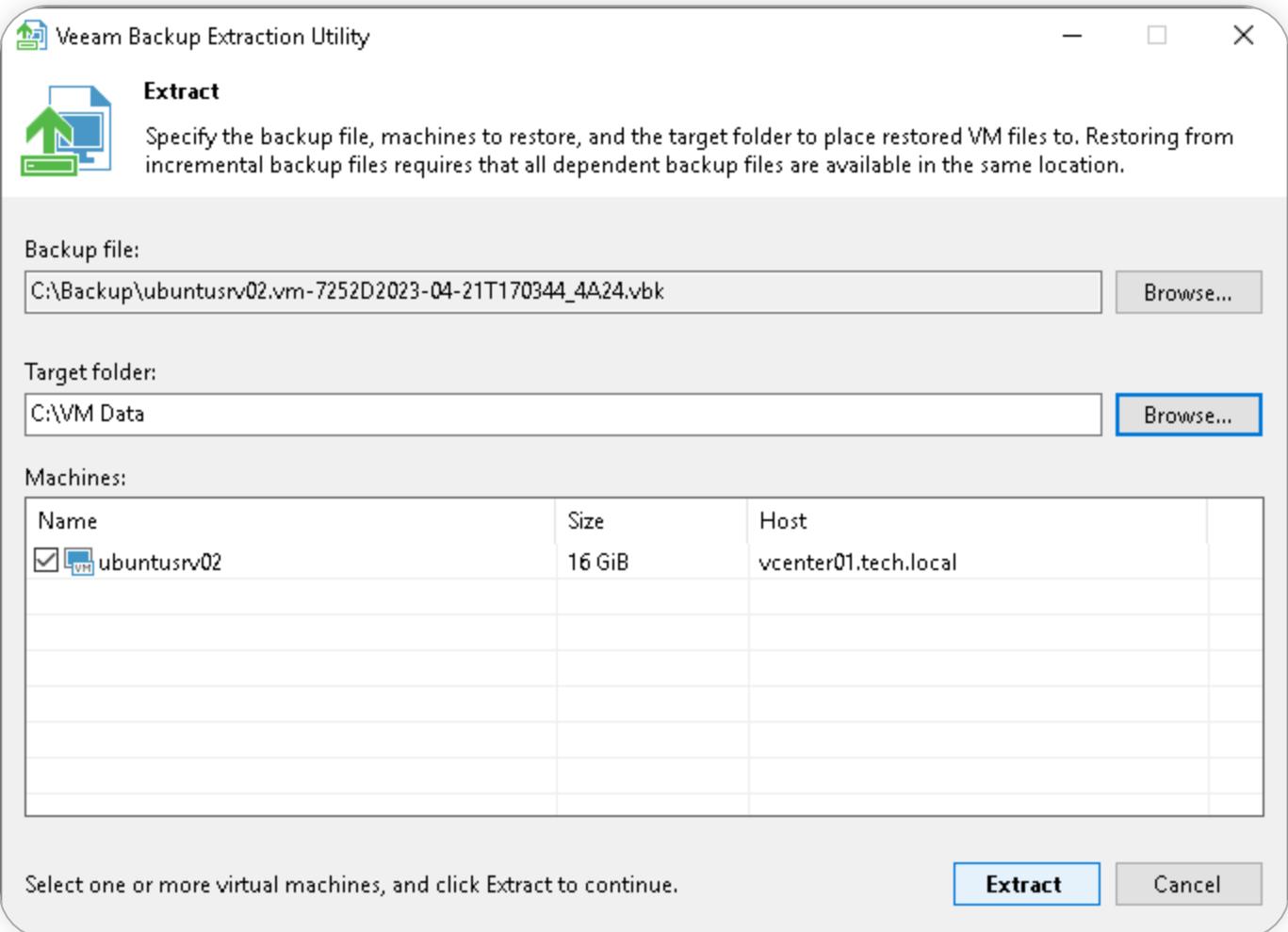


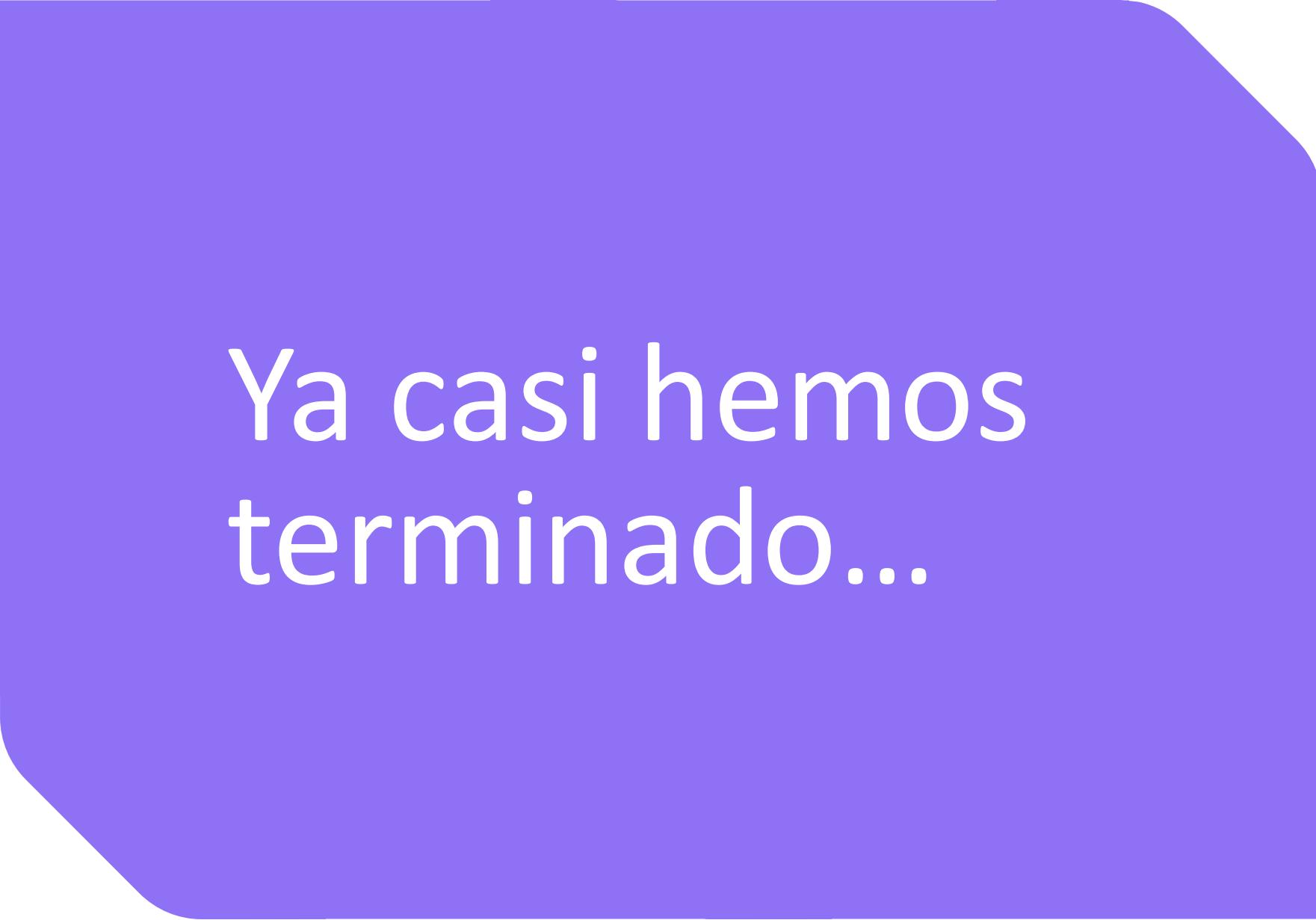
Veeam Extract Utility

- Herramienta independiente para recuperación
- GUI o CLI

Ejemplos de uso:

Recupere máquinas aunque se eliminen las copias de seguridad de Veeam Backup & Replication o Veeam Backup & Replication no esté instalado.





Ya casi hemos
terminado...

¿Quieres experiencia práctica?

 Intelligent offsite backups with Veeam Data Platform

 Embrace DevOps with Extensibility and

 Ransomware Defense with Immutable Veeam

 Test drive Veeam Backup and Replication V12

 Machine Learning, Terraform, Microsoft Teams BOT & Ransomware clean room with Veeam API

Learn how to achieve advanced capabilities with the Veeam REST API. Topics covered include how to address the malware challenge with Veeam clean room, leveraging Machine Learning for backup data analysis, and how to meet DevOps challenges with integrating Terraform with Veeam, amongst other topics.

Product: Veeam Backup and Replication
Use Cases: Data Recovery, Data Security, Data Mobility
Technical Level: Advanced

REQUEST LAB

 Getting Started With Veeam-Powered Managed

 Avoid platform lock-in with Veeam Flexible data recovery

Learn how to achieve data recovery and data mobility flexibilities with Veeam Data Platform. Topics include Microsoft Active Directory backups and Recovery with Veeam, recover data from on-premises to AWS, instant recovery from VMware vSphere to Microsoft Hyper-V, Secure Restore for Anti Virus and Malware scans and NAS data recovery, amongst other topics.

Product: Veeam Backup and Replication
Use Cases: Data Mobility, Data Flexibility
Technical Level: Intermediate

REQUEST LAB

 Test Drive Veeam Recovery Scenarios

 AI Powered Ransomware Threat Management with Veeam Data Platform

Learn about Artificial Intelligence powered Ransomware threat management capabilities now available with Veeam Data Platform (12.1 update). Key topics include AI powered inline malware detection, YARA rules support for malware detection, automated malware detection with YARA rules & Anti-virus software and immutable data backups to combat Ransomware challenge.

Product: Veeam Backup and Replication
Use Cases: Data Security
Technical Level: Intermediate

REQUEST LAB



[https://go.veeam.com/
hands-on-lab-
experience#renewal](https://go.veeam.com/hands-on-lab-experience#renewal)

Veeam Certified Engineer (VMCE)

- Instructor o a la carta
- Disponible en 100 países
- Teoría y laboratorios
- <https://www.veeam.com/support/training/vmce-training.html>

Recursos Adicionales

- Calculadoras (<https://www.veeam.com/calculators>)
- Centro de Ayuda (<https://www.veeam.com/support/help-center-technical-documentation.html>)
- Mejores prácticas de VBR (<https://bp.veeam.com/vbr/>)
- KB: Seguridad (<https://www.veeam.com/knowledge-base.html?type=security>)
- R&D Foros (<https://forums.veeam.com/>)



Follow us!



Join the community hub:

