Su camino hacia la resiliencia con Veeam Kasten

Una hoja de ruta para sus primeros 100 días y más allá.

Esta guía acompaña a los administradores de TI en el proceso de implementación, configuración y puesta en marcha de Veeam Kasten *para Kubernetes*. Ya sea que se instale mediante Helm o Marketplace, el proceso de implementación está diseñado para ser rápido, seguro y accesible. Para el día 100, tendrá un entorno de backup nativo de Kubernetes con exportaciones inmutables offsite, integrado con sus conjuntos de herramientas y aplicaciones, así como un manual de recuperación documentado.

Su viaje de 100 días

FASE 1 **Fundamento** **Días 1-14**	**FASE 2** **Fortalecer lo básico** **Días 15-45**	**FASE 3** **Optimizar y reforzar** **Días 46-75**	**FASE 4** **Demostrar valor** **Días 76-100**
M1: Dimensionamiento y planificación	M4: Gestión centralizada	M7: Integración de observabilidad	M10: Pruebas de recuperación
M2: Desplegar Veeam Kasten	M5: Procesamiento con reconocimiento de aplicaciones	M8: Resiliencia mejorada	M11: Documentación e informes
M3: Primeros trabajos de backup	M6: Mejores prácticas de políticas	M9: Cerrar las brechas de cobertura	M12: Higiene continua

Hoja de ruta de un vistazo

Fase	Nombre	Línea de tiempo	Enfoque
FASE 1	Fundamento	Días 1-14	Planear el entorno, implementar Veeam Kasten y ejecutar los primeros trabajos de backup.
FASE 2	Fortalecer lo básico	Días 15-45	Gestión centralizada, procesamiento con reconocimiento de aplicaciones y Mejores prácticas de políticas.
FASE 3	Optimizar y fortalecer	Días 46-75	Observabilidad, resiliencia y DR, y cerrar las brechas de cobertura.
FASE 4	Demostrar valor	Días 76-100	Pruebas de recuperación, documentación y buenas prácticas continuas.

Cómo usar esta guía

Los días son pautas, no plazos estrictos. Los entornos pequeños pueden comprimir la Fase 1 a una semana, y los complejos pueden extender la Fase 3.

Cada hito se basa en el anterior, por lo que se recomienda seguir los pasos en orden.

Los cuadros de llamada a lo largo del documento destacan puntos de decisión, opciones de arquitectura y problemas comunes que vale la pena tener en cuenta.

Contenido

FASE 1 • Días 1-14

Fundamento

Objetivo: infraestructura dimensionada, desplegada y primeras cargas de trabajo protegidas.

Hito 1: Dimensionamiento y planificación

Antes de desplegar cualquier cosa, invierta tiempo en la planificación. La mayoría de los desafíos relacionados con la implementación de un entorno estable y bien protegido se pueden evitar si se presta la debida atención a este paso.

Inventario de cargas de trabajo

- Documente el recuento total de cargas de trabajo y máquinas virtuales (VM), la huella de datos (por ejemplo, tamaño de volumen/recuento de archivos) y la tasa de cambio diaria estimada.
- Identifique sus cargas de trabajo más críticas. Estos determinan los objetivos de punto de recuperación y de objetivos de tiempo de recuperación (RPO y RTO).
- Tome nota de todas las bases de datos y cargas de trabajo que puedan beneficiarse del procesamiento con reconocimiento de aplicaciones.

Dimensionamiento y planificación de la implementación de Veeam Kasten

- Veeam Kasten cuenta con requisitos del sistema mínimos y los valores predeterminados suelen ser suficientes.
- Elija el método de implementación, ya sea Marketplace/Operator (recomendado cuando sea posible) o Helm. Se puede cambiar de método después de la instalación si es necesario.
- Verifique que su versión de Kubernetes sea compatible con la última versión de Veeam Kasten. De lo contrario, primero tendrá que actualizar o usar una versión anterior.
- Determine si este entorno es aislado. Si es así, es posible que las imágenes de Veeam Kasten deban cargarse en un registro local que esté disponible sin conexión a través del mercado de su proveedor, o que nuestro registro deba ser autorizado en la lista blanca.
- Planificar su red de backup aislando el tráfico de backup en una VLAN dedicada es una mejor práctica de seguridad, y es posible con Kubernetes en función de su CNI.

Helm vs. Marketplace

Helm: es la opción más flexible y compatible con todas las distribuciones de Kubernetes.

Marketplace/Operador: el ciclo de vida de implementación y actualización es más simple y admite los mismos parámetros de personalización que Helm. También se usa comúnmente con Red Hat OpenShift.

La desventaja: existe un posible retraso en la recepción de nuevos lanzamientos a través del marketplace. Las actualizaciones están disponibles inmediatamente en Helm, pero los proveedores del marketplace suelen retrasar los nuevos lanzamientos por uno o varios días para realizar pruebas de validación.

Arquitectura de almacenamiento de cargas de trabajo

- **Almacenamiento compatible con snapshots:** Veeam Kasten es compatible con prácticamente cualquier CSI controlador de almacenamiento que soporte snapshots, así como integraciones de almacenamiento directo.
- **Otro tipo de almacenamiento (por ejemplo, NFS genérico, disco local, etc.):** Veeam Kasten aún puede proteger estas cargas de trabajo, pero la falta de una verdadera funcionalidad de snapshot afecta la fiabilidad y el rendimiento de los backups. Recomendamos encarecidamente que actualice a volúmenes con funcionalidades de snapshot, pero GSB o NFS tar pueden utilizarse si acepta sus limitaciones inherentes.

Arquitectura de almacenamiento de backup: resumen de opciones

La elección del almacenamiento determina la resiliencia y la disponibilidad de los datos de backup. Aquí se muestra un resumen de los pros y los contras de cada tipo de almacenamiento de backup que puede configurar como un perfil de ubicación.

Veeam Kasten + Veeam Vault

Los snapshots se exportan a un almacenamiento de objetos inmutable, off-site y aislado lógicamente mediante Veeam Vault. No se necesita configuración ni mantenimiento avanzados.

Veeam Kasten + Repositorio de Veeam Backup & Replication

Los snapshots se exportan a la infraestructura gestionada por Veeam Backup & Replication, incluidos los repositorios Hardened de Veeam y los Scale-out Backup Repositories (SOBRs). Se requiere el modo de bloqueo. **Nota:** Las versiones pre-9.x también requieren un pequeño perfil de ubicación adicional (Vault/Object/NFS/CIFS) para metadatos.

Veeam Kasten + Almacenamiento de objetos

Los snapshots se exportan a almacenamiento de objetos (por ejemplo, S3, cloud), que debe configurarse como offsite e inmutable.

Veeam Kasten + NFS/CIFS

Los snapshots exportados directamente a NFS/CIFS generalmente no pueden ser inmutables, incluso en dispositivos compatibles con WORM, ya que se requeriría la versión para que esto sea posible. Esta opción es totalmente compatible, pero no se recomienda a menos que también disponga de duplicación o copias inmutables offsite.

Veeam Kasten + Múltiples perfiles de ubicación

Los snapshots se exportan a dos o más ubicaciones. Si se diseña correctamente, usando al menos una opción inmutable, esta puede ser la ruta más resistente. **Nota:** Las versiones anteriores a 9.x requieren múltiples políticas, utilizando un perfil de ubicación por política.

Los modos de almacenamiento determinan las funcionalidades

Según el tipo de almacenamiento, es posible que tenga disponibles las siguientes opciones:

Modo de volumen: archivo o bloque. Ambos son compatibles con Veeam Kasten (p. ej., Ceph FS o RBD).

Modo de exportación: archivo o bloque. Ambos son posibles con Veeam Kasten.

Si un volumen está en modo de bloque, puede exportar sus snapshots en modo de bloque. Ofrece características especiales, como CBT (cuando esté disponible) y exportaciones a un repositorio de Veeam Backup & Replication.

Uso de Veeam Backup & Replication + Veeam Infrastructure Appliance (VIA) como repositorio reforzado

Para quienes no cuentan con almacenamiento inmutable existente, integrar Veeam Kasten con Veeam Backup & Replication y desplegar VIA podría ser una opción razonable para lograr la inmutabilidad local.

Un repositorio reforzado proporciona backups locales inmutables, lo que significa que el ransomware no puede cifrarlas ni eliminarlas durante el período de retención. El OS está reforzado contra el acceso no autorizado y debería ejecutarse idealmente en un servidor físico protegido en lugar de una VM.

Tradicionalmente, un repositorio reforzado requiere la instalación y el endurecimiento manual de una distribución de Linux. VIA elimina completamente esta barrera, ya que está pre-reforzado y se despliega mediante una ISO de arranque. También puede autoinstalarse en hardware compatible o comprarse a través de un proveedor como un dispositivo certificado.

Hito 2: Desplegar Veeam Kasten

Desplegar Veeam Kasten

- Utilice la herramienta de pre-verificación para comprobar que se cumplen los requisitos (Opcional).
- Método Marketplace/operador: consulte los detalles de las instrucciones aquí.
- Método Helm: consulte los detalles de las instrucciones aquí.

Integración de acceso al panel de control y autenticación

- Para acceder al panel de control externamente, agregue un Ingress o una ruta a Veeam Kasten.
- Las mejores prácticas recomiendan integrar con el proveedor de autenticación de su distribución (por ejemplo, OpenShift Auth); también son posibles otras opciones como LDAP directo.
- Una vez que el panel de control de Veeam Kasten esté visible, puede continuar con los pasos que se indican a continuación.

Conecte Infraestructura a Veeam Kasten

- Si corresponde, (vSphere/nube/others) agregue un perfil de infraestructura para la integración directa de almacenamiento.
- Agregue un perfil de ubicación para definir el destino de backup.

Hito 3: Primeros trabajos de backup

Backups en entornos de Kubernetes

Los snapshots de almacenamiento son una característica potente que Kubernetes comprende y puede gestionar de manera nativa, si las admite tu aprovisionador de almacenamiento.

Veeam Kasten hace uso de estas funcionalidades o de la integración directa para activar snapshots que residen localmente en el dispositivo de almacenamiento. Veeam Kasten puede entonces usar estos snapshots para exportar datos de forma fiable a un perfil de ubicación externo (por ejemplo, NFS, S3, repositorio VBR, Vault, etc.).

Este método permite la máxima velocidad y consistencia, mientras utiliza características nativas y API de Kubernetes para lograr la máxima compatibilidad.

Requisitos para empezar

Veeam Kasten, como aplicación nativa de Kubernetes, necesita que el usuario que la instala tenga acceso a kubectl en el entorno objetivo, privilegios de administrador del clúster e idealmente acceso a la interfaz de administración de su distribución, si la tiene.

Consejo: Si encuentra algún error, puede encontrar soluciones en nuestros sitios Community y sitios KB.

- Más información sobre la protección de las VM de KubeVirt si es aplicable a su entorno.
- Cree su primera política de backup y apunte al perfil de ubicación.
- Establezca una política de retención adecuada para comenzar: 1 snapshot local diaria, con exportaciones al perfil de ubicación configuradas para una retención de 1 diaria, 4 semanales y 3 mensuales.
- Programe el trabajo para que se ejecute fuera de las horas pico y asegúrese de que no entre en conflicto con ningún periodo de mantenimiento.
- Realice la primera ejecución del trabajo manualmente y monitoree el proceso hasta completarlo.
- Verifique que el trabajo haya finalizado sin advertencias ni errores antes de pasar a la Fase 2.

Su primera prueba de restauración: ¡no la omita!

Antes de pasar a la Fase 2, realice una restauración en una aplicación no crítica para confirmar la capacidad de recuperación.

No estará protegido hasta que haya verificado que puede restaurar. Esto toma minutos y puede prevenir días de problemas más adelante.

Exportación VS local

Recuerde que los snapshots solo son locales para su dispositivo de almacenamiento. Esto significa:

- No son un verdadero backup.
- Retener más snapshots locales significa consumir más almacenamiento primario.

Por lo tanto, es importante exportar los snapshots a un perfil de ubicación, el cual puede tener una política de retención configurada de forma independiente.

Al exportar snapshots, todos los datos se deduplican, comprimen, cifran y guardan automáticamente de forma incremental.

FASE 2 • Días 15-45

Fortalecer lo básico

Objetivo: protección consistente, copia off-site y visibilidad en todo su entorno.

Hito 4: Gestión centralizada (MCM)

El gestor multiclúster (MCM) permite la visibilidad y la gestión centralizadas de varios clústeres. Cada clúster tendrá instalado Veeam Kasten para proteger las cargas de trabajo y las instancias podrán unirse.

- Una vez que se haya implementado otro clúster que ejecute Veeam Kasten, promueva una instancia de Kasten a Primaria y utilice un token de unión para vincularlas (instrucciones). Asegúrese de que los certificados autofirmados estén reconocidos como confiables para evitar errores.
- Vea todos los clústeres unidos a través del panel de control de MCM.
- Defina políticas globales y perfiles globales si desea tener una configuración coherente distribuida en todo su entorno.
- Agregue su clave de licencia empresarial al clúster principal de MCM. Las licencias se distribuirán sin problemas a todos los demás clústeres sin necesidad de ninguna otra configuración.

Hito 5: Procesamiento con reconocimiento de aplicaciones

El procesamiento con reconocimiento de aplicaciones mediante Kanister Blueprints garantiza que los backups coherentes frente a bloqueos se vuelvan consistentes con las aplicaciones o se exporten lógicamente. Esto es crucial para bases de datos como PostgreSQL, MongoDB, MySQL, Elastic, entre otras.

- Discuta los requisitos y el acceso de la aplicación con su equipo de aplicaciones.
- Encuentre ejemplos de modelos predefinidos que puede personalizar, o cree los suyos propios.
- Añada el modelo a Veeam Kasten.
- Asocie el modelo con las cargas de trabajo manualmente o creando una vinculación de modelo.
- Pruebe un backup y restaurar usando su modelo para verificar la recuperación de aplicación de extremo a extremo.

Tipos de backup

Coherente frente a bloqueos (por defecto): este tipo de backup captura el completo sistema de archivos en un momento preciso, normalmente a través de snapshots de proveedores de almacenamiento. Esto ofrece mayor coherencia de datos que la copia básica de archivos, pero las escrituras durante la copia o las transacciones no confirmadas todavía podrían perderse.

Consistente con las aplicaciones: este tipo de backup normalmente pone la aplicación en estado de reposo brevemente utilizando las herramientas nativas de la aplicación para asegurar que todo se escriba en el volumen antes de crear el snapshot.

Lógico: este tipo de backup utiliza las herramientas nativas de la aplicación para crear un volcado lógico o exportación de sus datos como archivo. A menudo, esto se envía a una ubicación externa como S3 en lugar del volumen en sí.

Los modelos son potentes e infinitamente flexibles. Además, al ser de código abierto, puede crear uno para cualquier aplicación o flujo de trabajo si aún no existe.

Hito 6: Mejores prácticas en materia de políticas

En este hito, creará trabajos adicionales para proteger todas sus cargas de trabajo y utilizará configuraciones avanzadas para garantizar su confiabilidad.

Mejores prácticas (para la mayoría de los escenarios)

- Utilice varios trabajos con etiquetas para seleccionar aplicaciones en lugar de una política comodín que proteja todo.
- Use políticas basadas en VM en lugar de políticas basadas en espacios de nombres al proteger VM de KubeVirt.
- Si desea realizar backups de los recursos de ámbito del clúster, cree una política aparte solo para esos backups.
- Defina una ventana de backup para garantizar que las cargas de trabajo de producción no se vean afectadas durante las horas críticas.
- Considere programar trabajos con escalonamiento para mejorar el rendimiento.
- Configure la protección de backup inmutable.
- Exclusiones / filtros de recursos si es necesario.
- Opcional Recursos globales, Ajustes preestablecidos de políticas

Otros Consejos

Para trabajos ejecutados manualmente, a menos que se especifique un tiempo de expiración, cualquier artefacto deberá ser eliminado manualmente.

Aunque el trabajo se haya configurado con hora local, todas las horas se convierten a UTC y los horarios de las políticas no se ajustan por el horario de verano.

Revise sus cálculos El cálculo de retención no siempre es obvio. Por ejemplo, conservar 24 snapshots horarios tomados a intervalos de 15 minutos solo permite retener 6 horas de snapshots, no 24 horas.

FASE 3 • Días 46-75

Optimizar y fortalecer

Objetivo: cerrar brechas de protección, optimizar RTO/RPO y aumentar la visibilidad.

Hito 7: Integración de observabilidad

- Habilite Red Hat ACM Observability la integración si corresponde.
- Exportar métricas a sistemas de monitorización externos (p. ej., Grafana, Datadog, Thanos, etc.).
- Cree alertas y paneles de control dentro de sus sistemas de monitorización (ejemplo de Grafana).
- Habilite Reporting.

Hito 8: resiliencia mejorada y recuperación ante desastres (DR)

Tener un backup de todas las cargas de trabajo también debe incluir un backup de Veeam Kasten en sí, lo cual puede lograrse mediante Kasten Disaster Recovery (KDR). Esto no debe confundirse con tener un entorno de recuperación ante desastres (DR) o un plan de DR, los cuales deben considerarse de acuerdo con la resiliencia requerida.

KDR (backup del catálogo de Veeam Kasten)

- Habilite Kasten DR: esto guarda el catálogo de backup de Veeam Kasten para que las restauraciones sean posibles incluso si ya no se puede acceder a la instalación de Kasten. Esto es importante, ya que los archivos de backup de Veeam Kasten no son independientes y requieren el catálogo y la clave de cifrado para restaurar.
- Configure el Kasten DR en "Exportar snapshots del catálogo local" y guarde la siguiente información en un lugar seguro: frase de contraseña, ID de clúster, detalles del perfil de ubicación de KDR y credenciales.

DR para sus cargas de trabajo

- Determine el nivel de resiliencia necesario en función de sus RTO/RPO deseados.
- Si un RTO/RPO de 1+ días es aceptable, solo tener backups y reconstruir el entorno según sea necesario podría ser una solución razonable.
- Si los RTO/RPO deben medirse en horas o minutos, se debe prestar especial atención al diseño de un plan. A continuación se presentan algunos ejemplos.

Ejemplos de configuraciones de DR (dependiendo del RTO/RPO requerido)

- **Aplicación desprotegida:** no hay puntos de restauración (p. ej., no hay snapshots locales ni exportaciones).

  Resultado: la recuperación no es posible.

- **Solo exportación:** las exportaciones de KDR y los puntos de restauración exportados existen en un perfil de ubicación offsite.

  Resultado: para recuperar, primero reconstruya un entorno de Kubernetes, instale Veeam Kasten, restaure el catálogo de Kasten y, a continuación, restaure las aplicaciones desde los puntos de restauración exportados.

- **Entorno DR + Importación:** Veeam Kasten está instalado y una política de importación se ejecuta regularmente para importar los puntos de restauración en un catálogo local.

  Resultado: los puntos de restauración son visibles en una ubicación secundaria y están listos para ser restaurados. Se consumen recursos mínimos hasta que se necesitan.

- **Entorno de recuperación ante desastres (DR) + Importar + Restaurar, escalado a cero réplicas:** Veeam Kasten está instalado, la política de Importar + Restaurar se ejecuta regularmente para importar los puntos de restauración al catálogo local y luego restaurar las aplicaciones en el entorno de Kubernetes. A continuación, las aplicaciones se restauran, pero con Transforms se configuran las réplicas en 0 en todas las cargas de trabajo.

  Resultado: las aplicaciones se restauran en Kubernetes (a través de pods, volúmenes persistentes, y todos los recursos seleccionados). Sin embargo, las réplicas están establecidas en cero, por lo que se consumen recursos mínimos hasta que se necesiten, excepto por el almacenamiento.

- **Entorno de recuperación ante desastres (DR) + Importación + Restauración, completo:** Veeam Kasten está instalado; la política de Importación + Restauración se ejecuta regularmente para importar los puntos de restauración a un catálogo local y luego restaurar las aplicaciones en el entorno de Kubernetes.

  Resultado: las aplicaciones se restauran en Kubernetes (incluyendo pods, PVs y todo lo seleccionado), funcionando exactamente como en producción y listas para ser aprovechadas plenamente.

Planificación ante desastres

Veeam Kasten es agnóstico respecto a la distribución, lo que significa que puede restaurar a y desde cualquier distribución de Kubernetes, incluso entre distribuciones completamente diferentes como Tanzu y Azure. Sin embargo, las restauraciones requieren que exista un entorno de Kubernetes funcional para ejecutarse; Kasten no puede arrancar por sí mismo. Asegúrese de crear un plan de desastres adecuado para estar preparado en caso de que se produzca un incidente y verifique regularmente que su plan cumple sus objetivos.

Hito 9: Ajuste fino

- **Revise el panel de control de Veeam Kasten:** aborde todas las cargas de trabajo desprotegidas antes de realizar cualquier otro ajuste.
- **Revise los horarios de los trabajos para detectar conflictos:** escalone los tiempos de inicio para evitar la contención de recursos.
- Confirme que todos los trabajos se están completando dentro de la ventana de backup definida.
- **Valide el cumplimiento de RPO:** ¿todas las cargas de trabajo críticas generan puntos de restauración dentro de su ventana objetivo de recuperación?
- Confirme que todas las cargas de trabajo se exportan a al menos una ubicación inmutable.
- Habilite la recolección de basura para eliminar acciones antiguas puede mejorar el rendimiento del catálogo.
- ¡Pruebe su proceso de actualización! Las nuevas versiones de Veeam Kasten se lanzan aproximadamente cada dos semanas.

FASE 4 • Días 76-100

Demostrar valor y poner en marcha

Objetivo: verificar la capacidad de recuperación, establecer una higiene continua y demostrar el ROI.

Hito 10: Pruebas de recuperación

El único backup que importa es aquel del que pueda restaurar. La fase 4 es donde se demuestra — con evidencia documentada — que su entorno cumple con sus compromisos de RTO y RPO.

Pruebas de restauración granular y completa

- Pruebe la restauración de un espacio de nombres completo o la restauración de VM desde una exportación. Simule la pérdida total en las instalaciones locales para validar su copia offsite.
- Pruebe la recuperación de elementos de la aplicación: restaure una base de datos y ejecute consultas de base de datos para comprobar que los datos están intactos.
- Pruebe la restauración a nivel de archivo (si lo desea): recupere archivos individuales desde una exportación a una ubicación de prueba.
- Pruebe su plan de DR completo de extremo a extremo, anote cualquier problema para mejorar, y documente exhaustivamente el proceso de manera que se asegure de que su plan de DR y el acceso a él estén disponibles.
- Registre los tiempos de recuperación reales y compárelos con sus objetivos de RTO. Documentar los resultados.

Mejores prácticas para las pruebas de recuperación

Siempre restaure en un entorno fuera de producción y nunca sobrescriba cargas de trabajo en funcionamiento durante una prueba.

Documente qué se restauró, desde qué punto de restauración, a qué destino y cuánto tiempo tardó.

Estos resultados son la prueba de la capacidad de recuperación. Guárdelos para revisiones de cumplimiento normativo, auditorías e informes de gestión.

Además, si está restaurando en el mismo entorno, incluso en espacios de nombres diferentes, tenga en cuenta que ciertos recursos (especialmente los servicios de red) pueden entrar en conflicto. Asegúrese de revisar su configuración antes de restaurar, restaurar en un entorno diferente y/o use Transforms para evitar conflictos.

Restaurar en diferentes entornos

Si se restaura desde/hacia diferentes sitios, distribuciones de Kubernetes, plataformas u otros entornos, Transforms puede ser útil para modificar su configuración de manera transparente durante la restauración. Por ejemplo, si va a cambiar rutas de red de producción a DR, o cambiar clases de almacenamiento. No se requieren cambios manuales para que las restauraciones se ejecuten inmediatamente con una configuración modificada o en un nuevo entorno.

Hito 11: Documentación y informes

- Habilite Reporting, si aún no lo ha hecho.
- Documente su arquitectura de backup final, incluida la lista de políticas, las ubicaciones de exportación, los horarios y las políticas de retención.
- Revise su consumo de almacenamiento de Veeam Vault y asegúrese de que su uso se corresponda con su presupuesto previsto.
- Archive los resultados de las pruebas de recuperación junto con la documentación de la arquitectura.

Hito 12: Establecer una cadencia de higiene continua

Para el día 100, su entorno debería estar estable y completamente documentado. Con estos hábitos, se mantendrá de esa manera:

- **Semanal:** revise el panel de control de Veeam Kasten e investigue los trabajos con errores o con advertencias antes de que se acumulen.
- **Mensual:** revise las últimas versiones de Kasten y actualice regularmente.
- **Trimestralmente:** realice una prueba de recuperación documentada y alterne entre distintos tipos de cargas de trabajo cada trimestre.
- **Anualmente:** revise la arquitectura de backup en función de los requisitos empresariales actuales.
- **Antes de la renovación:** revise el uso de licencias en su panel de control de Kasten (por ejemplo, el total a través de MCM o en cada clúster individualmente) para confirmar que está dentro de los límites de su licencia.

Próximos pasos

¿Está listo para más?

- Visite Veeam University
- Explore los casos de éxito de sus colegas
- Contactar con Éxito del cliente
- Comparta su historia de resiliencia de datos con Veeam

Apéndice: Referencia rápida

Componentes clave: Integración con Veeam

- **Veeam Software Appliance (VSA):** dispositivo reforzado con Veeam Backup & Replication preinstalado. Despliegue como OVA (VM) o ISO (físico). Puede actuar como un repositorio inmutable autónomo o funcionar con otros dispositivos o almacenamiento de backup, incluidos VIA dedicados.
- **Veeam Infrastructure Appliance (VIA):** dispositivo pre-reforzado desplegado como un repositorio reforzado dedicado u otro rol. Proporciona inmutabilidad local sin necesidad de tener conocimientos de Linux. Un rol por dispositivo.
- **Veeam Backup & Replication:** motor principal de backup, alojado en el VSA. Gestiona trabajos, repositorios, proxies y operaciones de recuperación.
- **Scale-out Backup Repository:** estructura lógica que combina un Performance Tier local (por ejemplo, VIA) y un Capacity Tier (por ejemplo, Vault/S3/NFS) en un único destino de backup.
- **Veeam Vault:** almacenamiento inmutable de objetos en la nube para copias offsite. Está administrado por Veeam, por lo que no se requiere una cuenta de nube independiente.

Términos clave

- **RPO:** pérdida de datos máxima aceptable, medida en tiempo. Determina la frecuencia de la Programación del backup.
- **RTO:** tiempo de inactividad máximo aceptable antes de que una carga de trabajo deba ser recuperada.
- **Inmutabilidad:** datos de backup que no pueden modificarse ni eliminarse durante un periodo de retención definido. Protege contra el cifrado por ransomware de los archivos de backup.
- **Repositorio reforzado de Veeam:** un repositorio de backup basado en Linux con inmutabilidad aplicada a nivel del OS. Proporcionado listo para usar por VIA, sin necesidad de administración de Linux.
- **KubeVirt:** un proyecto de código abierto que permite a Kubernetes ejecutar y gestionar VMs junto con cargas de trabajo contenerizadas. Esto permite que las VMs se ejecuten en plataformas de Kubernetes como OpenShift Virtualization y SUSE Harvester, que pueden ser protegidas por Veeam Kasten.
- **Procesamiento con reconocimiento de aplicaciones:** procesamiento que crea puntos de Backup consistente con las aplicaciones, algo que Veeam Kasten puede hacer utilizando modelos.
- **Modelo:** Kanister Blueprints es un mecanismo de código abierto para describir tareas personalizadas para la gestión de datos a nivel de aplicación en Kubernetes.

Recursos útiles

- Veeam Help Center
- portal para clientes de Veeam (descargas)
- Veeam Community Forums
- Artículos de Veeam KB
- Documentos de Veeam Kasten
- Documentación de Kanister Blueprints

Acerca de Veeam Software

Veeam es la empresa de confianza en datos e inteligencia artificial, especializada en ayudar a las organizaciones a garantizar que sus datos y su IA sean plenamente comprendidos, protegidos y resilientes para permitir la aceleración de la IA segura a escala. Como líder del mercado tanto en resiliencia de datos como en gestión de la postura de seguridad de datos, Veeam está diseñado para la convergencia de la identidad, los datos, la seguridad y los riesgos de IA.

Con sede en Seattle y oficinas en más de 30 países, Veeam protege a más de 550 000 clientes en todo el mundo, incluyendo al 82% de las empresas Fortune 500,

Más información en www.veeam.com o siga a Veeam on LinkedIn @veeam-software y X @veeam.