



Protección de cargas de trabajo en GCP / GCVE

NetApp Solutions

NetApp
April 26, 2024

This PDF was generated from <https://docs.netapp.com/es-es/netapp-solutions/ehc/gcp-app-dr-sc-cvs-veeam.html> on April 26, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Protección de cargas de trabajo en GCP / GCVE 1
 - Recuperación ante desastres coherente con las aplicaciones con NetApp SnapCenter y replicación de Veeam 1
 - Recuperación ante desastres de aplicaciones con replicación de SnapCenter, Cloud Volumes ONTAP y Veeam 5

Protección de cargas de trabajo en GCP / GCVE

Recuperación ante desastres coherente con las aplicaciones con NetApp SnapCenter y replicación de Veeam

Autores: Suresh Thoppay, NetApp

Descripción general

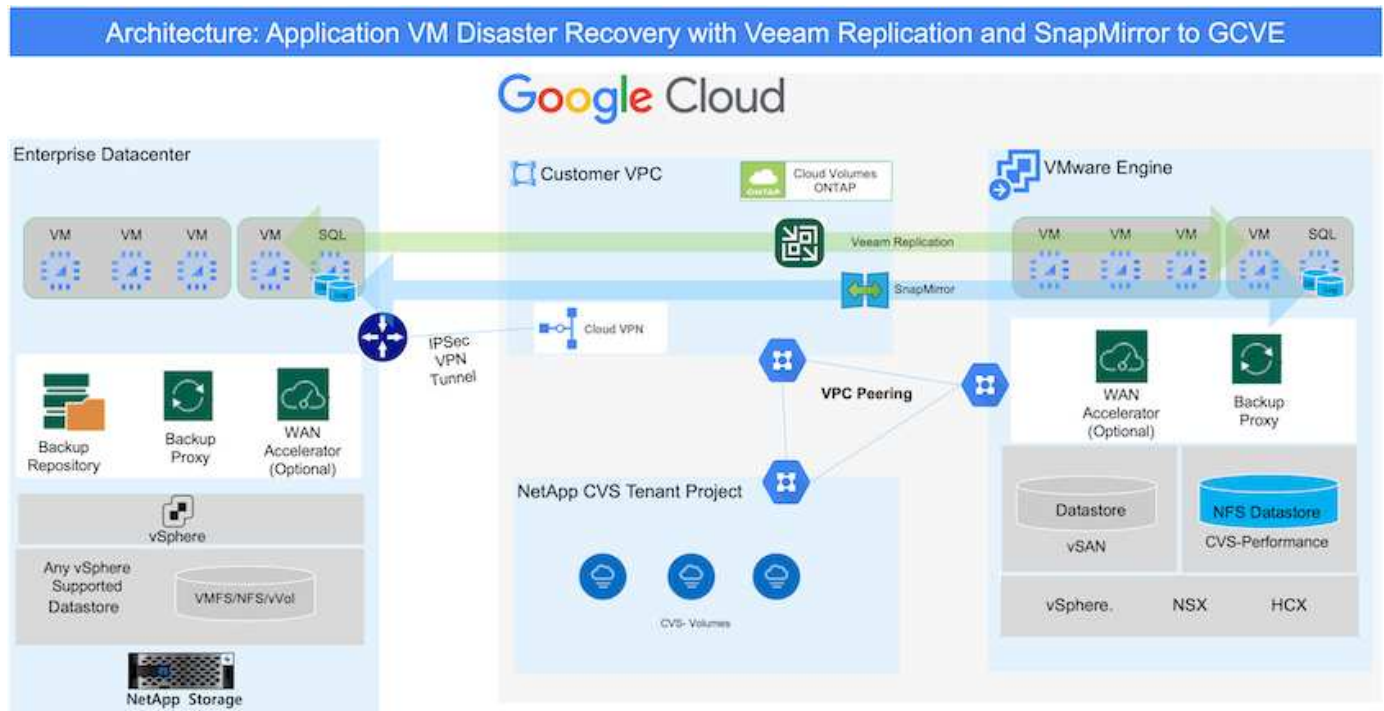
Muchos clientes están buscando una solución de recuperación ante desastres eficaz para sus VM de aplicaciones alojadas en VMware vSphere. Muchos de ellos utilizan su solución de backup existente para realizar la recuperación durante el diaster.

Muchas veces esa solución aumenta el objetivo de tiempo de recuperación y no cumple con sus expectativas. Para reducir el objetivo de punto de recuperación y el objetivo de tiempo de recuperación, la replicación de Veeam VM se puede utilizar incluso desde on-premises a GCVE, siempre y cuando la conectividad de red y el entorno con los permisos adecuados estén disponibles.

NOTA: Veeam VM Replication no protege los dispositivos de almacenamiento conectados a invitados de VM como montajes iSCSI o NFS dentro de la VM invitada. Necesidad de protegerlos por separado.

Para la replicación consistente de las aplicaciones para SQL VM y para reducir el RTO, utilizamos SnapCenter para orquestar las operaciones de snapmirror de volúmenes de bases de datos y registros de SQL.

Este documento proporciona un enfoque paso a paso para configurar y realizar la recuperación ante desastres que utiliza SnapMirror, Veeam y Google Cloud VMware Engine (GCVE) de NetApp.



Supuestos

Este documento se centra en el almacenamiento invitado para datos de aplicaciones (también conocido como «guest» conectado) y asumimos que el entorno local utiliza SnapCenter para realizar backups coherentes con

las aplicaciones.



Este documento es aplicable a cualquier solución de backup o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las prácticas recomendadas para crear normativas de backup que cumplan los acuerdos de nivel de servicio de la organización.

Para la conectividad entre el entorno local y la red de Google Cloud, utilice las opciones de conectividad como interconexión dedicada o VPN en la nube. Los segmentos se deben crear en función del diseño VLAN en las instalaciones.



Existen múltiples opciones para conectar los centros de datos en las instalaciones a Google Cloud, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la documentación de Google Cloud para conocer el método de conectividad apropiado de las instalaciones a Google.

Implementar la solución DR

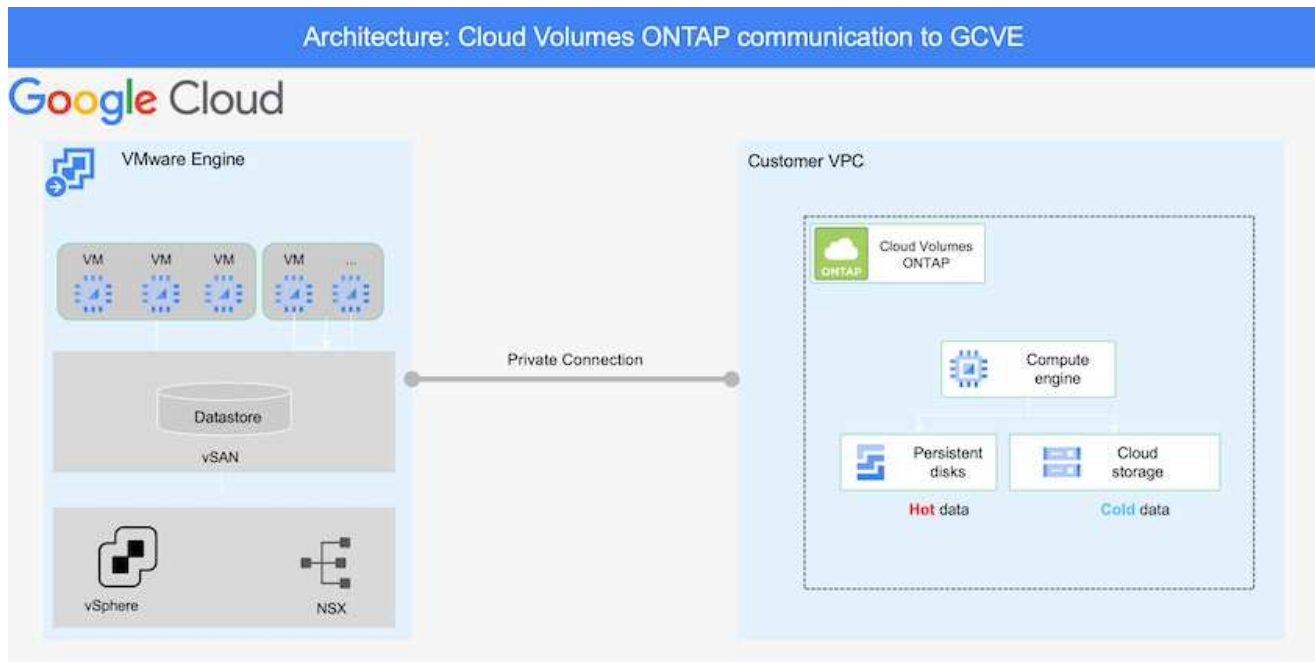
Descripción general de la puesta en marcha de soluciones

1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovisiona Cloud Volumes ONTAP con el tamaño de instancia correcto mediante BlueXP en la suscripción y la red virtual adecuadas.
 - a. Configurar SnapMirror para los volúmenes correspondientes de las aplicaciones.
 - b. Actualice las políticas de backup en SnapCenter para activar actualizaciones de SnapMirror después de los trabajos programados.
3. Instale el software Veeam y empiece a replicar máquinas virtuales a la instancia de Google Cloud VMware Engine.
4. Durante un desastre, interrumpa la relación de SnapMirror mediante BlueXP y activa la conmutación al nodo de respaldo de máquinas virtuales con Veeam.
 - a. Vuelva a conectar las LUN iSCSI y los montajes NFS para los equipos virtuales de la aplicación.
 - b. Ponga en marcha aplicaciones en línea.
5. Invoque la conmutación tras recuperación al sitio protegido mediante la resincronización inversa de SnapMirror una vez que se haya recuperado el sitio principal.

Detalles de la implementación

Configurar CVO en Google Cloud y replicar volúmenes a CVO

El primer paso consiste en configurar Cloud Volumes ONTAP en Google Cloud ("cvo") Y replicar los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retentions de instantánea deseadas.



Para obtener una muestra de instrucciones paso a paso acerca de la configuración de SnapCenter y la replicación de los datos, consulte ["Configurar la replicación con SnapCenter"](#)

[Revisión de la protección de SQL VM con SnapCenter](#)

Configurar los hosts GCVE y el acceso a datos CVO

Dos factores importantes que se deben tener en cuenta al implementar un SDDC son el tamaño del clúster SDDC en la solución GCVE y durante cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costes operativos generales. SDDC puede ser de tan solo tres hosts, hasta un clúster de varios hosts en una puesta en marcha a escala completa.

El servicio Cloud Volume de NetApp para almacén de datos NFS y las bases de datos y el registro Cloud Volumes ONTAP para SQL pueden implementarse en cualquier VPC y GCVE deben tener conexión privada con ese VPC para montar almacén de datos NFS y tener conexión de máquinas virtuales a LUN de iSCSI.

Para configurar GCVE SDDC, consulte ["Poner en marcha y configurar el entorno de virtualización en Google Cloud Platform \(GCP\)"](#). Como requisito previo, compruebe que los equipos virtuales invitados que residen en los hosts GCVE pueden consumir datos de Cloud Volumes ONTAP una vez establecida la conectividad.

Una vez que Cloud Volumes ONTAP y GCVE se hayan configurado correctamente, comience a configurar Veeam para automatizar la recuperación de las cargas de trabajo en las instalaciones en GCVE (máquinas virtuales con VMDK de aplicación y máquinas virtuales con almacenamiento en invitado) mediante la función Veeam Replication y aprovechando SnapMirror para las copias de los volúmenes de aplicación en Cloud Volumes ONTAP.

Instale Veeam Components

Según el escenario de implementación, se debe poner en marcha el servidor de backup de Veeam, el repositorio de backup y el proxy de backup. En este caso de uso, no es necesario poner en marcha el almacén de objetos para Veeam y tampoco se requiere ningún repositorio de escalado horizontal.

["Consulte la documentación de Veeam para conocer el procedimiento de instalación"](#)

Para obtener más información, consulte ["Migración con Veeam Replication"](#)

Configure la replicación de VM con Veeam

Tanto el vCenter en las instalaciones como el vCenter de GCVE deben registrarse con Veeam.

["Configure el trabajo de replicación de máquina virtual de vSphere"](#) En el asistente Guest Processing, seleccione Desactivar el procesamiento de aplicaciones, ya que utilizará SnapCenter para los procesos de backup y recuperación con reconocimiento de aplicaciones.

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692>

Conmutación al nodo de respaldo de Microsoft SQL Server VM

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0>

Ventajas de esta solución

- Usa la replicación eficiente y resiliente de SnapMirror.

- Recupera a cualquier punto disponible en el tiempo con la retención de copias Snapshot de ONTAP.
- Existe una automatización completa a disposición de todos los pasos necesarios para recuperar de cientos a miles de VM, desde los pasos de almacenamiento, computación, red y validación de aplicaciones.
- SnapCenter utiliza mecanismos de clonado que no cambian el volumen replicado.
 - Esto evita el riesgo de daños en los datos de los volúmenes y las Snapshot.
 - Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
 - Aprovecha los datos de recuperación ante desastres para flujos de trabajo que van más allá de la recuperación ante desastres, como las fases de desarrollo y pruebas, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas para solucionar problemas.
- La replicación de Veeam permite cambiar las direcciones IP de las máquinas virtuales en el sitio de recuperación ante desastres.

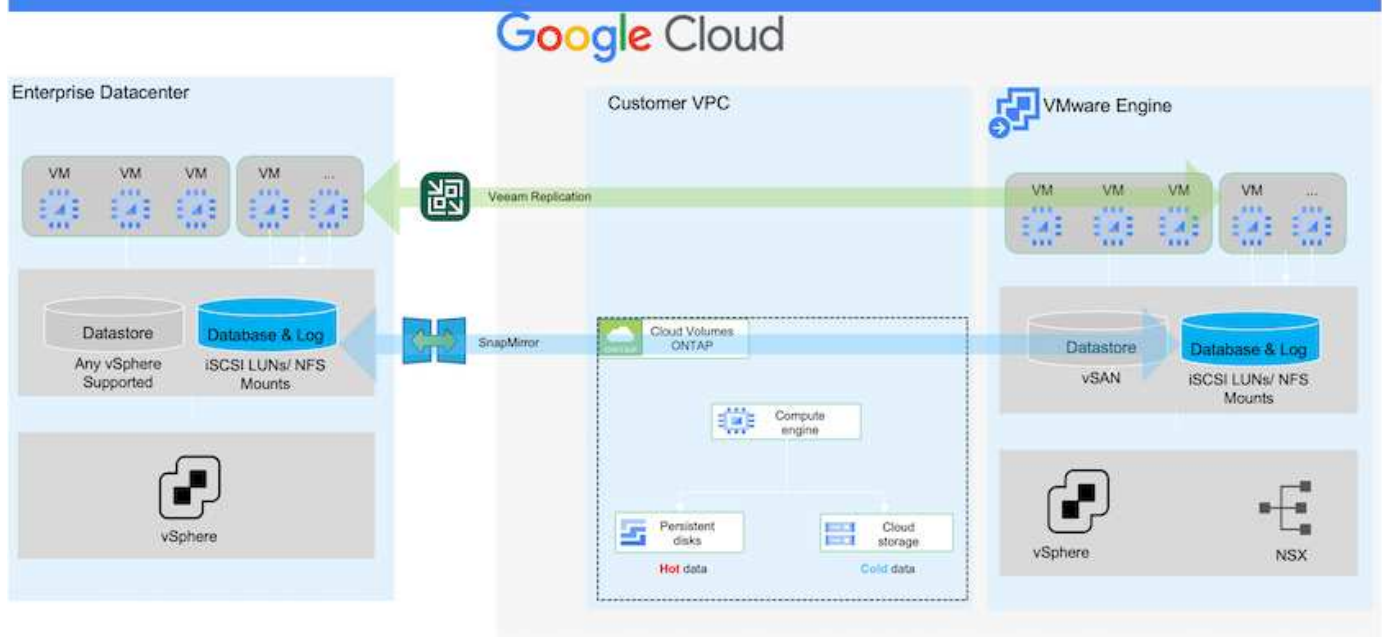
Recuperación ante desastres de aplicaciones con replicación de SnapCenter, Cloud Volumes ONTAP y Veeam

Autores: Suresh Thoppay, NetApp

Descripción general

La recuperación ante desastres en el cloud es un método resiliente y rentable de proteger las cargas de trabajo contra interrupciones del sitio y eventos dañados por datos como ransomware. Con SnapMirror de NetApp, las cargas de trabajo de VMware en las instalaciones que utilizan el almacenamiento conectado a invitado se pueden replicar a Cloud Volumes ONTAP de NetApp que se ejecuta en Google Cloud. Así se tratan los datos de aplicaciones; sin embargo, ¿qué ocurre con los equipos virtuales mismos? La recuperación ante desastres debería cubrir todos los componentes dependientes, incluidos equipos virtuales, VMDK, datos de aplicaciones, etc. Para ello, se puede utilizar SnapMirror y Veeam para recuperar sin problemas cargas de trabajo replicadas de las instalaciones a Cloud Volumes ONTAP a la vez que se utiliza almacenamiento VSAN para VMDK de máquinas virtuales.

Este documento proporciona un enfoque paso a paso para configurar y realizar la recuperación ante desastres que utiliza SnapMirror, Veeam y Google Cloud VMware Engine (GCVE) de NetApp.



Supuestos

Este documento se centra en el almacenamiento invitado para datos de aplicaciones (también conocido como «guest» conectado) y asumimos que el entorno local utiliza SnapCenter para realizar backups coherentes con las aplicaciones.



Este documento es aplicable a cualquier solución de backup o recuperación de terceros. Dependiendo de la solución utilizada en el entorno, siga las prácticas recomendadas para crear normativas de backup que cumplan los acuerdos de nivel de servicio de la organización.

Para la conectividad entre el entorno local y la red de Google Cloud, utilice las opciones de conectividad como interconexión dedicada o VPN en la nube. Los segmentos se deben crear en función del diseño VLAN en las instalaciones.



Existen múltiples opciones para conectar los centros de datos en las instalaciones a Google Cloud, lo que nos impide esbozar un flujo de trabajo específico en este documento. Consulte la documentación de Google Cloud para conocer el método de conectividad apropiado de las instalaciones a Google.

Implementar la solución DR

Descripción general de la puesta en marcha de soluciones

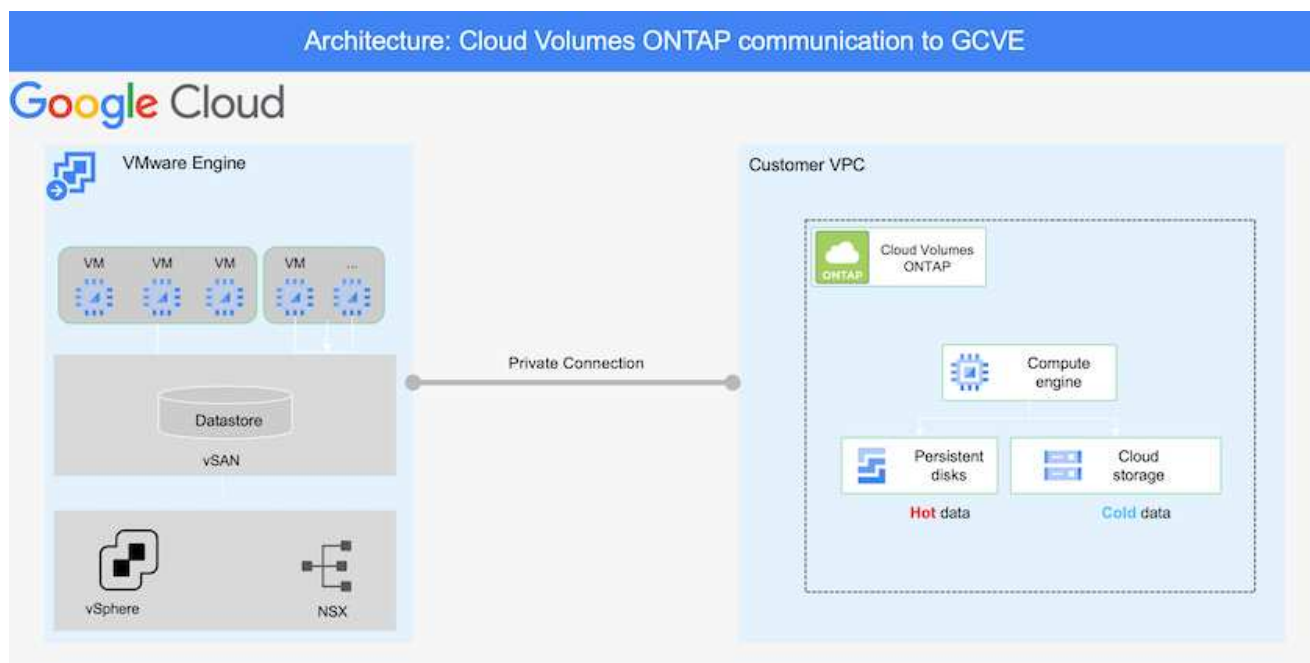
1. Asegúrese de que se realiza el backup de los datos de la aplicación mediante SnapCenter con los requisitos de punto de recuperación necesarios.
2. Aprovechne Cloud Volumes ONTAP con el tamaño de instancia correcto usando Cloud Manager dentro de la suscripción y la red virtual adecuadas.
 - a. Configurar SnapMirror para los volúmenes correspondientes de las aplicaciones.
 - b. Actualice las políticas de backup en SnapCenter para activar actualizaciones de SnapMirror después de los trabajos programados.

3. Instale el software Veeam y empiece a replicar máquinas virtuales a la instancia de Google Cloud VMware Engine.
4. Durante un evento de desastre, rompa la relación de SnapMirror mediante Cloud Manager y active la conmutación al nodo de respaldo de máquinas virtuales con Veeam.
 - a. Vuelva a conectar las LUN ISCSI y los montajes NFS para los equipos virtuales de la aplicación.
 - b. Ponga en marcha aplicaciones en línea.
5. Invoque la conmutación tras recuperación al sitio protegido mediante la resincronización inversa de SnapMirror una vez que se haya recuperado el sitio principal.

Detalles de la implementación

Configurar CVO en Google Cloud y replicar volúmenes a CVO

El primer paso consiste en configurar Cloud Volumes ONTAP en Google Cloud ("**cvo**") Y replicar los volúmenes deseados en Cloud Volumes ONTAP con las frecuencias y retentions de instantánea deseadas.



Para obtener instrucciones paso a paso de ejemplo sobre la configuración de SnapCenter y la replicación de datos, consulte ["Configurar la replicación con SnapCenter"](#)

[Configurar la replicación con SnapCenter](#)

Configurar los hosts GCVE y el acceso a datos CVO

Dos factores importantes que se deben tener en cuenta al implementar un SDDC son el tamaño del clúster SDDC en la solución GCVE y durante cuánto tiempo mantener el SDDC en servicio. Estas dos consideraciones clave para una solución de recuperación ante desastres ayudan a reducir los costes operativos generales. SDDC puede ser de tan solo tres hosts, hasta un clúster de varios hosts en una puesta en marcha a escala completa.

Cloud Volumes ONTAP se puede implementar en cualquier VPC y GCVE debe tener una conexión privada a ese VPC para que la máquina virtual se conecte a los LUN de iSCSI.

Para configurar GCVE SDDC, consulte ["Poner en marcha y configurar el entorno de virtualización en Google Cloud Platform \(GCP\)"](#). Como requisito previo, compruebe que los equipos virtuales invitados que residen en los hosts GCVE pueden consumir datos de Cloud Volumes ONTAP una vez establecida la conectividad.

Una vez que Cloud Volumes ONTAP y GCVE se hayan configurado correctamente, comience a configurar Veeam para automatizar la recuperación de las cargas de trabajo en las instalaciones en GCVE (máquinas virtuales con VMDK de aplicación y máquinas virtuales con almacenamiento en invitado) mediante la función Veeam Replication y aprovechando SnapMirror para las copias de los volúmenes de aplicación en Cloud Volumes ONTAP.

Instale Veeam Components

Según el escenario de implementación, se debe poner en marcha el servidor de backup de Veeam, el repositorio de backup y el proxy de backup. En este caso de uso, no es necesario poner en marcha el almacén de objetos para Veeam y tampoco se requiere ningún repositorio de escalado horizontal. https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Consulte la documentación de Veeam para conocer el procedimiento de instalación"]

Configure la replicación de VM con Veeam

Tanto el vCenter en las instalaciones como el vCenter de GCVE deben registrarse con Veeam. ["Configure el trabajo de replicación de máquina virtual de vSphere"](#) En el asistente Guest Processing, seleccione Desactivar el procesamiento de aplicaciones, ya que utilizará SnapCenter para los procesos de backup y recuperación con reconocimiento de aplicaciones.

[Configure el trabajo de replicación de máquina virtual de vSphere](#)

Conmutación al nodo de respaldo de Microsoft SQL Server VM

[Conmutación al nodo de respaldo de Microsoft SQL Server VM](#)

Ventajas de esta solución

- Usa la replicación eficiente y resiliente de SnapMirror.
- Recupera a cualquier punto disponible en el tiempo con la retención de copias Snapshot de ONTAP.
- Existe una automatización completa a disposición de todos los pasos necesarios para recuperar de cientos a miles de VM, desde los pasos de almacenamiento, computación, red y validación de

aplicaciones.

- SnapCenter utiliza mecanismos de clonado que no cambian el volumen replicado.
 - Esto evita el riesgo de daños en los datos de los volúmenes y las Snapshot.
 - Evita interrupciones de replicación durante los flujos de trabajo de pruebas de recuperación ante desastres.
 - Aprovecha los datos de recuperación ante desastres para flujos de trabajo que van más allá de la recuperación ante desastres, como las fases de desarrollo y pruebas, pruebas de seguridad, pruebas de parches y actualizaciones, y pruebas para solucionar problemas.
- La replicación de Veeam permite cambiar las direcciones IP de las máquinas virtuales en el sitio de recuperación ante desastres.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.