Mejores prácticas para la infraestructura de nube híbrida

Su guía sobre la seguridad de los backups en la nube híbrida, su implementación y mucho más.

Contenido

Introducción

Los entornos de nube híbrida ofrecen una solución potente para las organizaciones que desean equilibrar la flexibilidad de la computación en la nube con el control y la seguridad de la infraestructura en las instalaciones. Al integrar los recursos de la nube pública y privada, la nube híbrida permite a las empresas optimizar su estrategia de TI y garantizar la escalabilidad y la rentabilidad, al tiempo que mantiene los datos y las aplicaciones críticos en un entorno seguro y controlado. Este enfoque permite a las organizaciones adaptarse con agilidad a las diferentes cargas de trabajo y demandas, aprovechar las últimas innovaciones en la nube y cumplir con los requisitos normativos. Como resultado, la nube híbrida proporciona un marco adaptable y resiliente para promover la continuidad del negocio, mejorar la eficiencia operativa e impulsar la innovación.

Implementación

Evaluación y planificación

Antes de comenzar a implementar soluciones de nube híbrida, primero debe evaluar su infraestructura de TI, aplicaciones y requisitos de datos actuales. Esto implica evaluar el hardware, el software, las configuraciones de red y las soluciones de almacenamiento de datos existentes para comprender mejor sus capacidades y limitaciones. Determine qué aplicaciones son críticas para sus operaciones, incluidas sus necesidades de rendimiento y cómo interactúan con sus datos. Esta evaluación integral ayudará a identificar brechas y áreas en las que las soluciones en la nube pueden mejorar la eficiencia, la escalabilidad o la rentabilidad.

A continuación, defina objetivos claros e identifique por qué su organización específica se beneficiará de la adopción de un entorno de nube híbrida. Tenga en cuenta factores como la optimización de la carga de trabajo, la redundancia de la ubicación y las necesidades empresariales específicas como el cumplimiento o la soberanía de datos. Por ejemplo, puede intentar aprovechar la nube para aplicaciones de alta demanda mientras mantiene los datos confidenciales en las instalaciones. Al establecer objetivos bien definidos, también puede alinear mejor su estrategia en la nube con las necesidades de su organización para asegurarse de que el modelo elegido sea compatible con los requisitos actuales y futuros.

Diseño de arquitectura

Diseñar una arquitectura híbrida o multicloud requiere coordinarse con los objetivos de la organización y los requisitos de cumplimiento, a la vez que se aprovechan las ventajas que ofrecen los servicios en la nube. Comience por esbozar una arquitectura que integre los recursos locales con los entornos en la nube de una manera que cumpla con sus objetivos empresariales. Tenga en cuenta factores como la localización de los datos, el rendimiento de las aplicaciones y el cumplimiento para diseñar una solución que equilibre estas necesidades de forma eficaz.

Asegúrese también de aprovechar las ventajas inherentes de los servicios en la nube, como la flexibilidad, la escalabilidad, la seguridad y el ahorro de costos. Por ejemplo, utilice la escalabilidad de la nube para manejar picos de carga y asegúrese de que su arquitectura pueda adaptarse a las cambiantes demandas del negocio. Implemente soluciones de conectividad como redes privadas virtuales (VPN) o conexiones directas para facilitar una comunicación segura y confiable entre su infraestructura en las instalaciones y los entornos en la nube. Este enfoque de diseño ayudará a crear una configuración híbrida o multicloud eficiente y sin problemas.

Integración de seguridad

Integrar la seguridad en un entorno híbrido o multicloud es fundamental para proteger sus datos y aplicaciones. Desarrolle una estrategia de seguridad integral que utilice las sólidas características de seguridad de la nube, como la inmutabilidad, el cifrado de datos, los controles de acceso y la gestión de identidades. Esta estrategia debe abarcar tanto sus sistemas en las instalaciones locales como sus entornos de nube para garantizar una protección sólida frente a las amenazas.

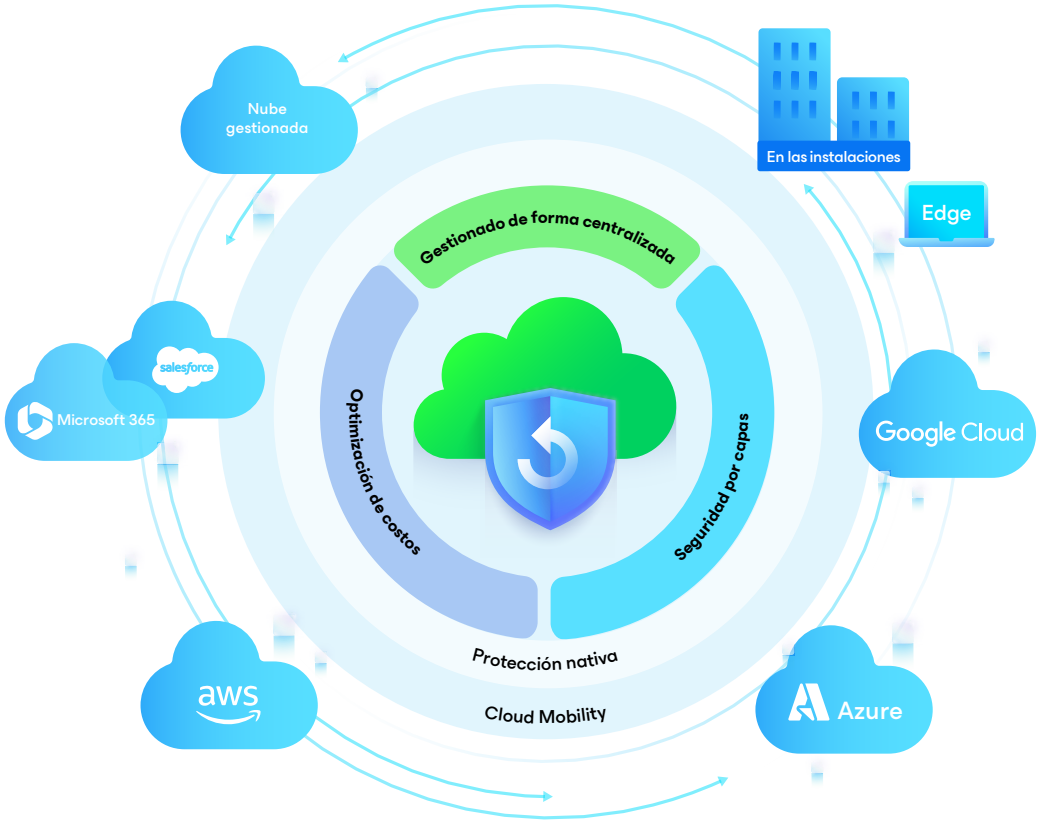
Asegúrese también de incorporar herramientas y servicios de seguridad nativos de la nube junto con las medidas de seguridad existentes en las instalaciones para mejorar la protección general. Por ejemplo, utilice las funciones de seguridad integradas de su proveedor de servicios en la nube para la detección de amenazas en tiempo real y el cumplimiento automatizado. Además, asegúrese de actualizar de manera periódica sus políticas de seguridad y realizar auditorías para mantener el cumplimiento de los estándares de la industria y mitigar los riesgos emergentes. Este mantenimiento continuo ayuda a proteger su infraestructura de las amenazas de seguridad en constante evolución.

Backup y recuperación ante desastres

Una estrategia integral de backup y recuperación ante desastres (DR) es esencial para garantizar la continuidad del negocio tanto en sus entornos en las instalaciones como en la nube. Comience por implementar un plan de backup integral que cubra todos sus datos y aplicaciones críticos y que garantice que tanto sus datos en la nube como en las instalaciones tengan backups de forma regular y sean fácilmente recuperables.

Luego, asegúrese de aprovechar los servicios de DR basados en la nube para mejorar su estrategia de DR general. Estos servicios pueden brindar opciones de recuperación rápida y minimizar el tiempo de inactividad para aplicaciones y datos críticos. La implementación de soluciones de backup automatizadas y replicaciones basadas en la nube también garantiza que su plan de DR pueda responder rápidamente ante eventos imprevistos. Pruebe regularmente sus procedimientos para validar su eficacia y asegurarse de que sus funcionalidades de recuperación cumplen con los requisitos de continuidad de negocio.

Veeam ofrece varias características y capacidades para ayudar a las organizaciones a implementar un entorno resiliente de nube híbrida. Con una amplia gama de funciones de seguridad, que incluyen inmutabilidad, cifrado, control de acceso basado en roles (RBAC) y autenticación multifactor (MFA), las organizaciones pueden proteger sus datos críticos sin importar dónde residan, protegiendo así los backups y mitigando el riesgo. El compromiso de Veeam con la protección de datos se ejemplifica aún más con su pionera Regla 3-2-1-0-0, que garantiza la protección de los datos independientemente de su ubicación en la nube híbrida. La independencia de la plataforma, la portabilidad de datos y la portabilidad de licencias ofrecen a los usuarios la libertad y flexibilidad necesarias para seguir esta regla y permitir transferencias de datos sin complicaciones entre entornos locales y de nube.



Mantenimiento

Gobierno y cumplimiento normativo

Un gobierno eficaz es esencial para gestionar entornos de TI híbridos. Comience por desarrollar políticas de gobierno integrales que cubran la asignación de recursos, la gestión de costos y el cumplimiento. Las políticas de gobierno también deben definir procedimientos para mantener el cumplimiento en diversas plataformas y tecnologías con el fin de garantizar que se cubran todas las partes del entorno híbrido.

Una vez que haya establecido sus políticas, debe mantenerlas mediante auditorías periódicas y controles de cumplimiento. Deben programarse con frecuencia para garantizar que sus sistemas y procesos se ajusten a regulaciones como el RGPD y la HIPAA. Estas auditorías ayudan a identificar lagunas o áreas en las que su entorno híbrido puede no cumplir con los estándares de cumplimiento, lo que le permite abordar los problemas de forma proactiva y evitar posibles sanciones.

Además, la implementación del control de acceso basado en roles (RBAC) es vital para gestionar el acceso dentro de un entorno híbrido. RBAC le permite aplicar el principio de privilegio mínimo y garantizar que los usuarios solo tengan el acceso necesario para realizar sus funciones laborales. Al definir los roles y los permisos con claridad, minimiza el riesgo de acceso no autorizado a datos y sistemas confidenciales. Este enfoque no solo refuerza la seguridad, sino que también simplifica la administración del acceso de los usuarios en diversos entornos.

Monitorización y administración

Para mantener la visibilidad y el control sobre las infraestructuras locales y en la nube, debe implementar herramientas de supervisión completas. Estas herramientas deberían proporcionar información sobre el rendimiento, la disponibilidad y el estado del sistema en todo su entorno híbrido. Las soluciones de monitorización eficaces facilitan el seguimiento del estado de los recursos, la detección de anomalías y la obtención de una comprensión más clara de cómo interactúan los diferentes componentes.

Esta información puede proporcionar a su organización KPI, que incluyen los objetivos de tiempo de recuperación y los objetivos de punto de recuperación (RTO y RPO). Son cruciales para garantizar que su entorno híbrido cumpla con los objetivos de continuidad del negocio y recuperación ante desastres. Además, esta información puede rastrear la utilización de los recursos para asegurarse de que se están utilizando de manera eficiente e identificar posibles cuellos de botella o activos infrautilizados. La revisión periódica de estos KPI puede ayudarle a mantener un rendimiento óptimo y a planificar futuras necesidades de recursos.

Por último, con el aumento de los ciberataques, es conveniente implementar sistemas de alerta proactivos para identificar y abordar rápidamente los problemas a medida que surgen. Los procesos de reparación automatizados pueden ayudar a resolver problemas sin intervención manual, reduciendo así el tiempo de inactividad y minimizando el impacto en las operaciones. Al establecer alertas para problemas críticos y configurar respuestas automatizadas, puede garantizar un entorno de TI híbrido más receptivo y resiliente. Este enfoque ayuda a mantener altos niveles de rendimiento y disponibilidad, a la vez que permite a su equipo de TI centrarse en iniciativas estratégicas en lugar de en la resolución de problemas rutinaria.

Veeam proporciona a las organizaciones políticas de backup altamente flexibles para gestionar automáticamente los datos de los backups en función de lo vitales que sean, su ubicación o las etiquetas, lo que libera recursos y garantiza la resiliencia y la recuperabilidad, incluso a escala empresarial. Además, Veeam proporciona monitorización, alertas y análisis exhaustivos no solo para los datos alojados en la nube, sino también para todo el conjunto de datos. Tanto si su entorno proviene de una única nube, o de la nube híbrida o multicloud, Veeam le proporciona una visión unificada y centralizada de su postura de protección de datos para que pueda sentirse seguro y cumplir con la normativa.

Optimización

Optimización de recursos

La optimización eficaz de los recursos es esencial para equilibrar el costo y el rendimiento en entornos híbridos. Para lograrlo, evalúe y ajuste regularmente cómo se utilizan sus recursos en su infraestructura local y en la nube. Esto implica analizar los patrones de uso para identificar los recursos infrautilizados o sobreabastecidos y ajustarlos para alinearlos con sus necesidades reales. Implemente estrategias para escalar sus recursos dinámicamente en función de la demanda en tiempo real, lo que le asegura que solo paga por lo que usa y maximiza la eficiencia de su infraestructura.

Aproveche las herramientas nativas de la nube que están diseñadas para manejar con facilidad las cargas de trabajo dinámicas y las fluctuaciones de la demanda. Implemente mecanismos de escalado automático que ajusten el número de instancias o recursos activos en función del tráfico actual y los requisitos de carga de trabajo. Esto puede ayudar a asegurarse de que puede adaptarse a las horas pico de uso sin aprovisionamiento excesivo en períodos más tranquilos. Del mismo modo, utilice el equilibrio de carga para distribuir las cargas de trabajo de manera uniforme entre los servidores para evitar que un solo recurso se convierta en un cuello de botella y mejorar el rendimiento y la confiabilidad generales.

Para obtener un mejor control sobre su gasto en la nube, emplee estrategias de etiquetado de recursos y asignación de costos. El etiquetado le permite categorizar y realizar un seguimiento de los recursos en función de varios criterios, como el departamento, el proyecto o el entorno. Esta visibilidad ayuda a monitorizar los patrones de uso e identificar áreas en las que se pueden reducir los costos. Implemente estrategias de asignación de costos para asignar gastos a unidades de negocio o proyectos específicos, lo que le proporciona una comprensión más clara de dónde se gasta su dinero y permite una elaboración de presupuestos y una planificación financiera más precisas.

Mejoras continuas

La nube cambia constantemente, por lo que las organizaciones deben evaluar y perfeccionar sus estrategias de nube híbrida para obtener la mejor protección. Revise periódicamente la arquitectura de la nube, las políticas de la nube y las prácticas de la nube para asegurarse de que se alinean con la evolución de los objetivos empresariales y los avances tecnológicos.

Las métricas de rendimiento son fundamentales en el proceso de revisión para evaluar la eficiencia y la eficacia de su entorno híbrido. Analice métricas clave como los tiempos de respuesta, el rendimiento y la utilización de recursos para identificar los cuellos de botella del rendimiento. Al identificar las áreas en las que su rendimiento está rezagado, puede tomar medidas específicas para resolver problemas, optimizar la asignación de recursos y mejorar el rendimiento general de su sistema. Este enfoque proactivo también garantiza que su entorno híbrido siga teniendo capacidad de respuesta y satisfaga las necesidades de su organización.

Las organizaciones también pueden usar los beneficios que ofrecen los proveedores de la nube para ayudar a monitorear y mejorar sus entornos. Aproveche estas herramientas integradas para obtener información sobre el rendimiento de su infraestructura en la nube y recomendaciones para mejorarla. Por ejemplo, los proveedores de servicios en la nube suelen ofrecer recomendaciones automatizadas para dimensionar de manera adecuada las instancias, optimizar el almacenamiento y mejorar la seguridad. Al aprovechar estos recursos, puede obtener información valiosa e implementar las mejores prácticas para mantener un entorno de nube híbrida eficiente y de alto rendimiento.

Con Veeam, las organizaciones pueden optimizar la asignación y utilización de los recursos para garantizar que estos se asignen de manera eficiente y efectiva tanto en las instalaciones como en los entornos de nube. Esta optimización permite a las organizaciones lograr ahorros de costos y maximizar el retorno de sus inversiones en TI. Además, las organizaciones se mantendrán al día con los últimos avances en tecnologías de nube híbrida que optimizan aún más el rendimiento, la escalabilidad y la resiliencia de la nube híbrida.

¿Por qué Veeam?

Veeam es la opción ideal para administrar entornos de nube híbrida debido a sus numerosas características y funcionalidades. En primer lugar, Veeam ofrece una única plataforma que permite a las organizaciones gestionar y proteger sin problemas sus datos en entornos en las instalaciones locales y basados en la nube. Este enfoque unificado elimina la necesidad de contar con múltiples herramientas y simplifica el proceso de gestión, lo que le permite ahorrar tiempo y recursos.

El cumplimiento y el gobierno son factores cruciales en cualquier entorno de TI, especialmente en configuraciones de nube híbrida. Veeam proporciona capacidades integrales para mantener el cumplimiento. Con Veeam, las organizaciones pueden fácilmente establecer y aplicar políticas de gobierno, monitorizar el acceso y uso de los datos, y asegurarse de que cumplen con regulaciones como el RGPD y la HIPAA.

Como se mencionó anteriormente, la seguridad es una prioridad absoluta, y Veeam hace todo lo posible para abordar esta preocupación. Ofrece sólidas medidas de seguridad como cifrado, backup seguro y opciones de recuperación para ayudar a los usuarios a garantizar que sus datos permanezcan protegidos durante la transmisión y el almacenamiento. Además, las características de seguridad integradas de Veeam ofrecen una defensa multicapa contra las ciberamenazas y el acceso no autorizado a datos críticos.

La rentabilidad es otra ventaja de usar Veeam para entornos de nube híbrida. Las capacidades eficientes de administración, compresión y optimización de datos de Veeam ayudan a reducir los costos de almacenamiento al eliminar datos redundantes y optimizar el uso del almacenamiento. También ofrece opciones de licencias flexibles para que las organizaciones puedan elegir el modelo más rentable que se ajuste a sus necesidades específicas.

La herramienta de monitorización y alerta de Veeam, Veeam ONE, proporciona información en tiempo real sobre el rendimiento, el estado y la capacidad del entorno de nube híbrida. A través de la monitorización proactiva y las alertas automatizadas, los equipos de TI pueden identificar y resolver rápidamente los problemas para evitar posibles tiempos de inactividad o pérdida de datos.

Acerca de Veeam Software

Veeam®, el líder n.º 1 del mercado mundial en resiliencia de datos, cree que todas las empresas deberían ser capaces de recuperarse para avanzar después de una interrupción con la confianza y el control de todos sus datos cuando y donde los necesiten. Veeam llama a esto resiliencia radical, y estamos obsesionados en crear formas innovadoras de ayudar a nuestros clientes a conseguirlo. Las soluciones de Veeam están diseñadas específicamente para potenciar la resiliencia de datos al proporcionar backup de datos, recuperación de datos, libertad de datos, seguridad de datos e inteligencia de datos. Con Veeam, los líderes de TI y seguridad descansan tranquilos sabiendo que sus aplicaciones y datos están protegidos y siempre disponibles en sus entornos de nube, virtuales, físicos, SaaS y de Kubernetes. Con sede en Seattle y oficinas en más de 30 países, Veeam protege a más de 550 000 clientes en todo el mundo, incluido el 74 % de las empresas de Global 2000, que confían en Veeam para mantener sus negocios en funcionamiento. La resiliencia radical comienza con Veeam. Más información en www.veeam.com o siga a Veeam en LinkedIn @veeam-software y X @veeam.

Para ver a Veeam en acción en un entorno de nube híbrida, haga clic aquí para ver nuestra demostración.