Creación de una estrategia para una nube única, híbrida y multinube en el sector educativo

AWS Guía prescriptiva

AWS Guía prescriptiva: Creación de una estrategia para una nube única, híbrida y multinube en el sector educativo

Table of Contents

Creación de una estrategia para una nube única, híbrida y multinube en el sector educativo

Amazon Web Services (colaboradores)

Septiembre de 2023 (historia del documento)

Las instituciones educativas pretenden respaldar funciones como el aprendizaje remoto, la investigación, la experiencia de los estudiantes, el conocimiento de los datos y la administración con la agilidad, el ahorro de costos, la seguridad y la resiliencia que ofrece la computación en la nube. Muchas organizaciones evalúan las implementaciones híbridas y multinube como parte de esta transformación digital.

En esta documentación se proporcionan recomendaciones sobre la creación de una estrategia de gobernanza y tecnología única, híbrida y multinube para los líderes ejecutivos y los responsables de la toma de decisiones de instituciones educativas que estén evaluando sus opciones de traspaso a la nube. Esta guía se basa en la experiencia de AWS al trabajar con más de 14 000 instituciones educativas de todos los tamaños de todo el mundo, desde escuelas primarias y secundarias hasta centros de educación superior.

Descripción general de

A medida que las instituciones educativas se transforman digitalmente para ofrecer servicios y experiencias diferenciados a sus estudiantes, padres, profesores, personal y comunidad, se enfrentan a una multitud de decisiones técnicas. Muchas organizaciones ya han tomado la decisión de adoptar la nube para aumentar la agilidad, la elasticidad, la resiliencia, la seguridad y el ahorro de costos. En función de las relaciones e inversiones existentes entre los distintos equipos, la mayoría de las organizaciones utilizan alguna combinación de centros de datos en las instalaciones, instalaciones de coubicación y proveedores de servicios en la nube. Dada la disponibilidad de varias opciones de nube, las instituciones educativas suelen decidir entre modelos de implementación única, híbrida y multinube (se definen en la sección Estrategias de implementación de la nube).

La multinube, que es el uso de servicios de un mínimo de dos proveedores de servicios en la nube, no es infrecuente en muchas instituciones actualmente. Es posible que su equipo de TI prefiera un proveedor de nube, mientras que otros grupos, departamentos o usuarios individuales podrían elegir otros proveedores o ya los utilicen. Las instituciones educativas que no tienen ninguna estrategia

clara que las guíe hacia el modelo de implementación de la nube adecuado se enfrentan a muchos desafíos. Por ejemplo, una complejidad innecesaria, el aumento de la demanda de personal, una gobernanza incoherente y enfoques con el mínimo común denominador que las limitan al subconjunto de capacidades básicas que son comunes entre proveedores. Cada desafío frena la innovación y ralentiza la transformación digital.

Por el contrario, si cuenta con una estrategia de nube que lo guíe hacia el uso de una tecnología única, híbrida y multinube, puede cumplir con los requisitos de su misión educativa y, al mismo tiempo, aprovechar las ventajas de la nube de forma operativamente sostenible para lograr el éxito a largo plazo. Para crear esta estrategia, recomendamos lo siguiente:

- Seleccione un proveedor de nube principal y estratégico.
- Establezca un centro de excelencia (CCoE) en la nube.
- Diferencie entre aplicaciones de software como servicio (SaaS) y servicios de nube básicos.
- Establezca los requisitos de seguridad y gobernanza para cada proveedor de servicios en la nube.
- Adopte soluciones administradas nativas en la nube siempre que sea posible y práctico.
- Implemente arquitecturas híbridas cuando las inversiones en las instalaciones existentes incentiven el uso continuado.
- Reserve el uso multinube solo para las cargas de trabajo que no puedan cumplir con los requisitos técnicos o empresariales a través de un proveedor de nube.

Estas prácticas recomendadas se analizan de forma detallada en la sección Recomendaciones de esta documentación. Cada recomendación es importante, pero las prioridades de su institución dependerán de la fase de la adopción de la nube en la que se encuentre. Por ejemplo, si acaba de empezar a adoptar la nube, concéntrese en seleccionar un proveedor de nube principal y estratégico, establecer una CCo E y adoptar soluciones gestionadas y nativas de la nube. Si ya utiliza un proveedor de nube, céntrese en establecer los requisitos básicos de seguridad y gobernanza, y considere la posibilidad de utilizar arquitecturas híbridas cuando sus inversiones actuales en centros de datos incentiven el uso continuado. Si su organización ya utiliza varios proveedores de nube, céntrese en diferenciar las aplicaciones de SaaS y reservar las implementaciones multinube para las raras cargas de trabajo que realmente las requieran.

Contenido

Estrategias de implementación de la nube

AWS define la computación en la nube como la entrega bajo demanda de recursos de TI a través de Internet con precios de pago por uso. En lugar de comprar, poseer y mantener centros de datos y servidores físicos, puede acceder a los servicios tecnológicos, como la potencia de computación, el almacenamiento y las bases de datos, según sea necesario desde un proveedor de servicios en la nube. La computación en la nube permite a las instituciones educativas evitar tareas pesadas indiferenciadas, como la adquisición de hardware, el mantenimiento y la planificación de la capacidad. Al adoptar e implementar soluciones en la nube, puede elegir entre varios modelos: nube única, nube híbrida y multinube.

Nube única

Este modelo utiliza un único proveedor de servicios en la nube. Las aplicaciones y cargas de trabajo de una nube única pueden implementarse directamente en la nube o alojarse previamente en otro entorno y migrarse a la nube. Estas cargas de trabajo pueden utilizar servicios de infraestructura de nivel inferior del proveedor de nube o también aprovechar los servicios administrados de nivel superior. En cualquier caso, este modelo adopta un único proveedor de nube y solo utiliza los servicios de nube de ese proveedor.

Nube híbrida

Un modelo de nube híbrida distribuye los recursos entre el centro de datos en las instalaciones de una organización y al menos un proveedor de servicios en la nube. Por lo general, el objetivo de este modelo es extender la infraestructura de una organización a la nube y, al mismo tiempo, mantener la conectividad privada con los sistemas internos existentes que residen en las instalaciones.

Multinube

Un modelo multinube distribuye los recursos entre un mínimo de dos proveedores de servicios en la nube y utiliza sus servicios. Una organización puede optar por un enfoque multinube, pero lo más frecuente es que esto se deba a que los equipos, departamentos o miembros del personal individuales tienen sus propias preferencias sobre los distintos proveedores de nube.

Recomendaciones

Ahora que ya tiene los conocimientos básicos sobre la nube única, híbrida y multinube, en esta sección se proporcionan recomendaciones detalladas para elegir un modelo.

- Selección de un proveedor de nube principal y estratégico
- Establecer una CCo E
- Diferenciación entre aplicaciones de SaaS y servicios de nube básicos
- Establecimiento de los requisitos de seguridad y gobernanza para cada proveedor de servicios en la nube
- Adopción de servicios administrados nativos en la nube siempre que sea posible y práctico
- Implementación de arquitecturas híbridas cuando las inversiones en las instalaciones existentes incentiven el uso continuado
- Reserva del uso multinube solo para las cargas de trabajo que no puedan cumplir con los requisitos técnicos o empresariales a través de un proveedor de nube

Selección de un proveedor de nube principal y estratégico

La adopción de la nube ofrece una gran cantidad de beneficios esenciales para la modernización, la rentabilidad y la innovación de la TI. Sin embargo, la adopción de tecnologías de nube más allá de las aplicaciones SaaS limitadas puede plantear desafíos que las instituciones educativas deben planificar cuidadosamente para evitar complejidades y costos innecesarios. Los cambios tecnológicos y empresariales que implica la implementación de las cargas de trabajo en la nube requieren la formación del personal y los ajustes de la infraestructura principal, lo que incluye las redes, la seguridad, la gobernanza y las operaciones.

El mejor enfoque para tratar estos desafíos de manera eficaz, especialmente si su organización se encuentra en las primeras etapas del traspaso a la nube, es seleccionar un proveedor de nube principal y estratégico que respalde la mayoría de sus cargas de trabajo. Comience con una adopción centrada en el proveedor para que pueda simplificar y acelerar la obtención de los beneficios de la nube. La selección de un proveedor de nube principal no es una decisión exclusiva ni irreversible. Permite a su organización evolucionar la adopción de la nube de forma iterativa. Para comenzar, céntrese en unos pocos servicios y, a continuación, amplíe a otros servicios en la nube cuando sea necesario, sin retrasar los beneficios generales de la nube. Este enfoque maximiza

la capacidad de la organización para aprovechar las capacidades de un proveedor, concentrar y desarrollar las habilidades de los empleados y las relaciones con socios externos, y simplificar la administración de proveedores.

Hemos visto a algunos clientes embarcarse en un traspaso a la nube a la vez que intentaban adoptar varios proveedores de servicios en la nube, pero más tarde lamentaron esa decisión y la complejidad que supuso. Gartner comparte esta información en su artículo, 6 Steps for Planning a Cloud Strategy, cuyo paso 2 es la priorización de un proveedor principal en arquitecturas multinube.

Cada proveedor de nube presenta diferentes modelos operativos y de soporte, administración de identidades y accesos, redes, operaciones, capacidades de cumplimiento, etc. Es mejor dominar un modelo operativo de un proveedor de nube a la vez. Puede incorporar servicios en la nube adicionales de forma iterativa e incremental más tarde, cuando sea racional hacerlo. Existen varios factores que pueden influir en su decisión de adoptar un proveedor de nube principal, pero puede utilizar las siguientes preguntas clave para guiar su elección.

- ¿Qué variedad y profundidad de servicios ofrece el proveedor?

  Los distintos proveedores de servicios en la nube ofrecen distintos servicios. Como mínimo, asegúrese de que el proveedor principal tenga las capacidades necesarias para satisfacer todos sus requisitos funcionales, así como sus necesidades operativas transversales, como la seguridad, la gobernanza y la automatización. Seleccione un proveedor que ofrezca estas capacidades con un historial demostrado de innovación y excelencia operativa. Tenga en cuenta no solo las aplicaciones, sino también los datos. Piense en los futuros patrones de transferencia e integración de datos para limitar el costo, la latencia y la complejidad de desplazar grandes cantidades de datos entre proveedores. Elija un proveedor que tenga la mayor variedad y profundidad de servicios posibles para satisfacer sus necesidades actuales de aplicaciones y datos, así como para obtener nuevos casos de uso que puedan satisfacer las necesidades de su institución según cambien con el tiempo.
- ¿El proveedor puede satisfacer todas sus necesidades de seguridad y cumplimiento?

  En el sector educativo, la seguridad y el cumplimiento son fundamentales para cualquier implementación de tecnología. Elija un proveedor de servicios en la nube que pueda satisfacer todas sus necesidades de seguridad y cumplimiento. Herramientas como AWS Artifact pueden ayudarlo a evaluar a los proveedores, ya que ofrecen un recurso centralizado para el acceso bajo demanda a los informes de seguridad y cumplimiento. Tenga en cuenta no solo la seguridad y el cumplimiento de la infraestructura y los servicios del proveedor de nube, sino también lo fácil que le resulte diseñar soluciones seguras y compatibles al usar esos servicios. Debería

preferir un proveedor que ofrezca una combinación de soluciones prediseñadas, inicios rápidos y recomendaciones para acelerar la adopción segura de la nube.

- ¿El proveedor cuenta con una sólida red de socios?

  Ninguna organización se somete sola a la transformación de la nube. Para acelerar la adopción, debe utilizar los servicios y la experiencia del proveedor de nube, así como su red de socios. Esta red incluye socios tecnológicos que proporcionan software que se ejecuta en la tecnología de la nube, se integra con ella o es compatible con ella, así como socios consultores que pueden ayudarlo a diseñar, crear, ejecutar y administrar sus propias aplicaciones en la nube. Descubrirá que muchos proveedores de tecnología educativa, proveedores de software independientes (ISVs), consultores y revendedores con los que ya trabaja son miembros de la red de socios del proveedor de la nube. Debería preferir un proveedor de servicios en la nube que cuente con la red de socios con competencias acreditadas más sólida. Contar con socios con experiencia técnica y en el sector demostrada es fundamental.

- ¿Qué soporte y formación ofrece el proveedor?

  Para adoptar con éxito cualquier tecnología nueva, necesita mecanismos para solicitar formación y ayuda, que incluyan prácticas recomendadas, directrices de configuración y resolución de problemas de reparación de averías. Elegir un proveedor de servicios en la nube que ofrezca opciones de soporte y formación sólidas lo preparará para tener éxito. Explore el modelo y los recursos de soporte oficiales del proveedor, así como los recursos disponibles de terceros o de la comunidad, como blogs, foros, videos y guías prácticas. Tenga en cuenta no solo los programas de soporte técnico del proveedor, sino también los programas que se centran en la transformación empresarial y cultural. Por ejemplo, el marco de adopción de la AWS nube (AWS CAF) ayuda a las organizaciones a transformarse digitalmente al centrarse en perspectivas que incluyen los procesos empresariales y las personas, no solo la tecnología. Debería preferir un proveedor de servicios en la nube que ofrezca opciones de formación extensas y una comunidad y un modelo de soporte confiables y demostrados.

Establezca una E CCo

Considere la posibilidad de desarrollar su función de liderazgo en la nube mediante una oficina de transformación o un centro de excelencia (CCoE) en la nube. A CCo E desarrolla y promueve un enfoque para implementar la tecnología de nube a escala en toda la organización. Para que la adopción de la nube sea exitosa, CCo diseñe su E de manera que incluya representantes que puedan hablar en nombre de los equipos y departamentos involucrados. Comience poco a poco

y evolucione gradualmente la CCo E para satisfacer sus necesidades a medida que avanza en el proceso de transformación. Los representantes de su proveedor de servicios en la nube principal, como su administrador de AWS cuentas y su arquitecto de soluciones, pueden proporcionarle recursos que lo guíen en la creación de su empresa E. CCo Una CCo E acelera su capacidad para adquirir experiencia en la materia, lograr la aceptación, ganarse la confianza de toda la organización y establecer directrices eficaces para cumplir con los requisitos de su misión. No existe una estructura organizativa única que funcione para todas las instituciones, pero las siguientes preguntas le ayudarán a diseñar su propia E. CCo

- ¿A quién debes incluir en tu CCo E?

  En sus inicios, una CCo E podría incluir solo a un puñado de pioneros y campeones de la nube. Puede que la CCo E siga siendo pequeña, pero debería evolucionar para incluir a líderes que puedan defender tanto las funciones empresariales como las funciones técnicas que se ven afectadas por la adopción de la nube. Las funciones empresariales incluyen la administración de cambios, los requisitos de las partes interesadas, la gobernanza, la formación, las adquisiciones y las comunicaciones. Los miembros de los equipos administrativos e instructivos de la institución suelen representar estas funciones. Las funciones técnicas incluyen la infraestructura, la automatización, las herramientas operativas, la seguridad, el rendimiento y la disponibilidad. Los miembros de los equipos de TI de la institución suelen representar estas funciones. La CCo E también debería tratar de implicar a los proveedores y socios, según sea necesario, para que aporten su experiencia en la materia. La CCo E es una organización viva. Es probable que su suscripción, forma y función cambien con el tiempo, e incluso podrían disolverse en algún momento de su madurez futura.
- ¿Cómo interactúa la CCo E con sus partes interesadas?

  La CCo E está al servicio de otros equipos y su único objetivo es informar y permitir una adopción exitosa de la nube. Considere la posibilidad de integrar partes de la CCo E en varios departamentos, escuelas y funciones. Esto permite el acceso a una gama más amplia de recursos y comentarios internos más rápidos. Céntrese en crear asociaciones y abrir líneas de comunicación entre las partes interesadas desde el principio para establecer una relación de confianza en la institución y eliminar los silos organizativos. La CCo E debería tener mecanismos definidos para comunicarse con las partes interesadas, recopilar comentarios y capacitar a los usuarios. Las métricas de éxito de la CCo E deberían reflejar dicha colaboración y comunicación. Si se mide a un equipo solo por la creación de tecnología, se creará más tecnología, pero su uso y sus resultados pasarán a ser una cuestión de última hora. En lugar de eso, tus métricas deberían medir aspectos como el número de equipos que se vuelven autosuficientes gracias al trabajo de

la CCo E, el número de veces que la CCo E se encuentra en la senda crítica de las iniciativas, la cantidad de eventos de formación celebrados o el grado de adopción de los resultados de la CCo E. Una CCo E bien construida y confiable puede ser un trampolín hacia una transformación organizacional más amplia que se base en la confianza.

- ¿Cómo se debe establecer una CCo E?

  La mayoría de las organizaciones comienzan su adopción de la nube con proyectos piloto específicos y seleccionados. Establezca una CCo E como parte de estos proyectos. Un buen comienzo es fundamental para definir el éxito de todo el proceso.

  - Comience con un problema empresarial. La tecnología por el bien de la tecnología es una mala estrategia. Si experimenta con tecnologías de nube, identifique un caso de uso empresarial convincente, por pequeño que parezca. A continuación, analice ese caso de uso para establecer objetivos claros sobre cómo la tecnología puede ayudarlo. No implemente la solución en un silo. Obtenga información constante de las partes interesadas de la empresa antes y durante la implementación del proyecto. Todos los proyectos de nube exitosos se basan en una estrecha colaboración con las unidades institucionales que utilizarán la tecnología.
  - Comience con algo pequeño. Elija un proyecto de bajo riesgo que sea bidireccional. Esto significa que el proyecto es reversible y cualquier error se puede corregir rápidamente. Los proyectos piloto tienen que ver con la experimentación. Evitar proyectos a gran escala de alto riesgo le permite controlar mejor la implementación y los resultados. Ayuda a centrarse en problemas específicos y definibles en lugar de objetivos amplios. Por ejemplo, si la automatización es el objetivo final, intente automatizar tareas específicas en lugar de tareas completas.
  - Defina y mida el resultado. Establezca métricas claras para evaluar el progreso y el rendimiento de cada proyecto. Defina el estado final deseado con suficiente antelación para evitar que las expectativas de las partes interesadas no coincidan. Colabore estrechamente con las partes interesadas de la empresa y otros líderes de la organización para definir las expectativas y los beneficios medibles. También es importante traducir los resultados a un lenguaje no técnico. Hable en términos de objetivos institucionales, por ejemplo, cómo el proyecto mejoró la retención y redujo la pérdida de clientes, cómo redujo los costos y aumentó la velocidad de entrega, etc.
  - Comience desde la zona de confort. Elija un proyecto de un dominio con el que su institución esté familiarizada. De esta forma, puede asegurarse de que el proyecto tenga objetivos significativos y comprensibles con un impacto real. Un proyecto de este tipo generará confianza y obtendrá mejores resultados a largo plazo para la organización. Por ejemplo, si ya tiene experiencia en análisis de datos, puede comenzar con un proyecto de análisis para iniciar su

traspaso a la nube y, al mismo tiempo, aprovechar sus habilidades actuales. Cada institución tiene una experiencia diferente y necesita encontrar sus componentes únicos para crear una estrategia de transformación digital exitosa.

Diferenciación entre aplicaciones de SaaS y servicios de nube básicos

La mayoría de las instituciones educativas ya han adoptado aplicaciones de software como servicio (SaaS). El SaaS proporciona a su institución una solución completa que ejecuta y administra el proveedor de servicios. Las aplicaciones de SaaS más comunes incluyen aplicaciones de productividad, como el procesamiento de textos y el correo electrónico, pero también existen opciones de SaaS para muchas cargas de trabajo críticas, como la planificación de recursos empresariales (ERP), los sistemas de información para estudiantes (SIS) y los sistemas de administración del aprendizaje (LMS). Cuando su institución adopta una oferta de SaaS, su equipo de TI no tiene que pensar en cómo se mantiene el servicio o cómo se administra la infraestructura: los usuarios solo consumen el servicio. Este modelo de entrega reduce la carga administrativa que recae sobre el personal de TI. Muchas instituciones optan por adoptar un enfoque de “SaaS primero” en su estrategia de TI, especialmente si sus equipos de TI carecen del tiempo, los recursos o las habilidades para autoalojar la misma aplicación de manera suficiente. Incluso si tiene los recursos para autoalojar, podría ser más rentable adoptar una solución de SaaS e invertir en otros proyectos.

Cuando usa aplicaciones de SaaS, su equipo de TI no tiene que administrar la infraestructura subyacente, por lo que el lugar en el que el proveedor aloja la aplicación (el centro de datos en las instalaciones, el proveedor de nube principal o un proveedor de nube alternativo) pierde importancia. Después de elegir un proveedor de nube principal estratégico, puede optar por utilizar una oferta de SaaS alojada en otro proveedor de nube o en las instalaciones, en el centro de datos del proveedor. Por el contrario, incluso si sus aplicaciones de SaaS están alojadas en un proveedor de nube, puede elegir un proveedor de nube principal estratégico distinto en función de la solidez del proveedor para sus cargas de trabajo que no sean de SaaS. La distinción entre los entornos de alojamiento es menos importante para el SaaS que para las aplicaciones autoalojadas. Sin embargo, debe tener en cuenta las siguientes preguntas clave al evaluar cómo el SaaS se adapta a la nube como parte de la estrategia de TI.

- ¿La aplicación de SaaS tiene alta disponibilidad y es escalable?

Muchos proveedores ya tomaron la decisión de adoptar la nube para sus ofertas de SaaS. De este modo, el proveedor puede aprovechar los beneficios de la nube que representan más disponibilidad y escalabilidad. Además, como el proveedor puede adoptar el modelo de responsabilidad compartida de la nube en lugar de administrar y mantener la infraestructura física, puede invertir más tiempo y recursos en la entrega de nuevas características. Por estos beneficios, debería preferir proveedores que prioricen la nube y ofrezcan soluciones alojadas en la nube.

- ¿La aplicación de SaaS puede cumplir con sus requisitos de seguridad?

  Al evaluar el SaaS, es importante conocer qué datos almacena la aplicación, cómo se utilizan y qué controles de seguridad existen para protegerlos. Si bien es posible que no tenga el control directo sobre el almacenamiento de datos del mismo modo que en su propio entorno autoalojado, debe asegurarse de que el proveedor cuente con mecanismos y controles para gestionar los datos de forma adecuada. Tenga en cuenta qué características de seguridad están integradas en la solución de SaaS y cuáles de ellas requieren una configuración adicional. La nube permite a los proveedores de SaaS crear soluciones más disponibles y escalables, y también pueden crear soluciones más seguras gracias al modelo de responsabilidad compartida. Debería preferir a los proveedores que aprovechan las herramientas y los servicios de seguridad en la nube como parte de sus soluciones.

- ¿Quién es el propietario de los datos de la aplicación de SaaS y cómo puede acceder a ellos?

  Cuando usa SaaS, confía en que el proveedor gestionará adecuadamente los datos de su institución. Asegúrese de revisar las condiciones del servicio y los acuerdos de nivel de servicio de las aplicaciones de SaaS para comprender sus factores clave, como la propiedad, la disponibilidad y la durabilidad de los datos. Evalúe los mecanismos para hacer copias de seguridad o exportar sus datos, ya que son especialmente importantes si decide cambiar de proveedor o si el proveedor deja de prestar el servicio.

- ¿Sus otros servicios y aplicaciones autoalojadas pueden integrarse con la aplicación de SaaS independientemente del entorno?

  Al adoptar una solución de SaaS, es fácil suponer que los servicios y las aplicaciones que comparten el mismo entorno de alojamiento (es decir, las aplicaciones que utilizan el mismo proveedor de nube o centro de datos del mismo proveedor) tendrán una integración más fluida. Sin embargo, la mayoría de las soluciones de SaaS actuales tienen un amplio soporte para integraciones de API y de terceros, así que no se limite a las soluciones que se alojan en el mismo entorno. Si existen las integraciones necesarias, las soluciones no tienen por qué compartir el mismo entorno subyacente. Por ejemplo, supongamos que utilizas una solución SaaS como

Google Drive o Microsoft OneDrive para almacenar archivos de estudiantes en la nube. Para proporcionar escritorios virtuales y streaming de aplicaciones a sus alumnos, puede determinar si Amazon WorkSpaces Applications es la opción que mejor se adapta a sus necesidades. Si bien estos servicios se ejecutan en entornos diferentes, WorkSpaces Applications tiene integraciones nativas con Google Drive y Microsoft OneDrive, por lo que sus alumnos pueden seguir utilizando el almacenamiento existente.

- ¿La aplicación de SaaS admite la administración centralizada de identidades?

  Para evitar que el equipo de TI tenga que administrar almacenes de identidades dispares y que los usuarios tengan que recordar varios conjuntos de credenciales, asegúrese de que las soluciones de SaaS admitan la integración con sus soluciones existentes de administración de identidades o inicio de sesión único. La administración de identidades fragmentada reduce la productividad y puede causar malas prácticas de seguridad, como el aumento de privilegios y la falta de seguridad en las contraseñas. Si la solución de SaaS que desea no admite el inicio de sesión único ni su almacén de identidades existente, evalúe si el valor empresarial de adoptar la solución supera el aumento de la carga para los usuarios y el personal.

- ¿Cómo puede proteger la comunicación de red con la aplicación de SaaS?

  En algunos casos, es posible que necesite una aplicación autoalojada para comunicarse con una aplicación de SaaS. Por lo general, esta comunicación se realizará a través APIs de mecanismos de autenticación y autorización adecuados. Sin embargo, según los entornos de alojamiento de las dos aplicaciones, es posible que se necesiten mecanismos alternativos o adicionales para simplificar o proteger la comunicación. Por ejemplo, si autoaloja una aplicación con un proveedor de nube y necesita integrarla con una aplicación de SaaS alojada en el mismo proveedor de nube, este puede ofrecer varias opciones de conexión. Es posible que puedas usar conexiones de interconexión específicas de la nube o interfaces privadas o privadas APIs, por ejemplo, AWS PrivateLinkpara evitar que esa comunicación atraviese la Internet pública. Del mismo modo, si su aplicación en las instalaciones tiene una conexión de red dedicada a un proveedor de nube a través de un servicio como AWS Direct Connect, puede usar esa misma conexión para comunicarse con las aplicaciones de SaaS alojadas en el mismo proveedor de nube.

Establecimiento de los requisitos de seguridad y gobernanza para cada proveedor de servicios en la nube

Las instituciones educativas tienen varios objetivos de cumplimiento, gobernanza y ciberseguridad que deben alcanzar. Los riesgos de no cumplir con estos objetivos pueden incluir la pérdida de la reputación institucional, multas pecuniarias, el pago de rescates, filtraciones de información confidencial, el robo de propiedad intelectual y la pérdida total de funciones esenciales o un uso limitado de estas. Gracias al modelo de responsabilidad compartida, las instituciones que adoptan los servicios en la nube pueden reducir la carga administrativa al delegar parte de la responsabilidad de la seguridad de la infraestructura al proveedor de servicios en la nube. Además, puede beneficiarse de servicios de seguridad nativos en la nube diseñados específicamente que ofrecen características que no suelen estar disponibles, son difíciles de administrar o tienen un costo prohibitivo en una implementación en las instalaciones. Algunos ejemplos incluyen servicios como la protección AWS WAFde aplicaciones web, AWS Shieldla protección contra la denegación de servicio distribuida y Amazon GuardDuty para la detección de amenazas. DDo Una estrategia exitosa de seguridad y gobernanza en la nube permite a los equipos de TI y seguridad centrarse en crear sistemas que sean seguros por diseño, ayuda a la institución a adaptarse rápidamente a los cambiantes requisitos de la misión y proporciona a los profesores e investigadores entornos seguros para revolucionar el aprendizaje y la innovación. Para evaluar sus requisitos de seguridad y gobernanza, tenga en cuenta las siguientes preguntas clave.

- ¿A qué marcos de cumplimiento deben ajustarse sus cargas de trabajo?

  Las instituciones educativas deben cumplir con muchos marcos de cumplimiento debido a la multitud de partes interesadas y cargas de trabajo que soportan. Entre estos marcos de cumplimiento, se incluyen la Ley de Derechos Educativos y Privacidad de la Familia (FERPA), la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA), el Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP), la Certificación del modelo de madurez de ciberseguridad (CMMC), el Reglamento sobre el Tráfico Internacional de Armas (ITAR), los Servicios de Información de la Justicia Criminal (CJIS) y el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) de EE. UU. En algunos casos, como con la CMMC, la financiación de las becas de investigación no se libera hasta que las cargas de trabajo pertinentes estén certificadas como conformes. Cada marco es único y puede aplicarse solo a un subconjunto de cargas de trabajo. Asegúrese de conocer los requisitos que debe cumplir cada carga de trabajo y de poder cumplir esos requisitos en el entorno de cada carga de trabajo. En los entornos de nube, asegúrese de comprender sus responsabilidades en comparación con las responsabilidades

del proveedor de la nube. Debe tener los conocimientos, los recursos y las habilidades necesarios para lograr y mantener el cumplimiento.

- ¿Qué mecanismos tiene para hacer cumplir la normativa en varios proveedores de servicios en la nube sin inhibir la innovación?

  Si su institución académica es nueva en la nube, le recomendamos que seleccione un proveedor principal de servicios en la nube estratégicos y se centre en comprender cómo diseñar, crear y operar entornos de nube que sean seguros por diseño. Lo ideal es que los controles de seguridad que se incrustan automáticamente en los sistemas de autoservicio permitan a los usuarios implementar rápidamente entornos de nube seguros con una intervención mínima de los equipos de TI. Centrarse en un solo proveedor limita la cantidad de recursos y tiempo que debe invertir para garantizar la seguridad y el cumplimiento. Las instituciones que tienen más éxito eligen un proveedor de servicios en la nube que pueda satisfacer la mayoría de los requisitos de cumplimiento, cuente con una sólida red de socios, ofrezca soluciones de cumplimiento prediseñadas y ofrezca una automatización de autoservicio segura. Si debe garantizar la seguridad y el cumplimiento con distintos proveedores de servicios en la nube, necesitará una inversión adicional para desarrollar las habilidades y los recursos necesarios para administrar el cumplimiento en cada entorno. Si cada proveedor de servicios en la nube usa un entorno fundamental o zona de aterrizaje diferente, debe entender qué estándares y requisitos de cumplimiento puede admitir cada zona de aterrizaje, lo que podría determinar si algunas cargas de trabajo se pueden alojar en ese proveedor. Puede administrar el cumplimiento de cada proveedor por separado o utilizar soluciones personalizadas o de socios que puedan centralizar la administración en todos los proveedores. AWS Marketplace proporciona soluciones listas para usar que también pueden cumplir con sus requisitos de cumplimiento.

- ¿Cómo puede evaluar y controlar el costo y el uso con varios proveedores de nube?

  Si su institución académica es nueva en la nube, le recomendamos que establezca mecanismos de control y visibilidad de los costos para comprender mejor qué servicios en la nube se utilizan, a quién pertenecen los recursos de la nube, cuál es su propósito y qué posibles ahorros de costos se pueden lograr al optimizar el consumo. Las instituciones pueden lograr un importante retorno de la inversión al asociarse con su proveedor de servicios en la nube para migrar y modernizar los sistemas esenciales, ya que pueden negociar acuerdos empresariales, beneficiarse de los precios por volumen y aprovechar la experiencia del proveedor de servicios en la nube. Si necesita controlar los costos y el uso con varios proveedores, considere cómo puede agregar y analizar los costos y el uso de cada proveedor, ya sea con procesos y herramientas internos o mediante soluciones de socios. Muchas organizaciones están empezando a identificar las operaciones

financieras en la nube (FinOps) como una función clave y están dedicando recursos a promover e implementar capacidades para la gestión y optimización de los costes de la nube.

- ¿Cuenta con mecanismos para administrar fácilmente los permisos de los usuarios a lo largo del tiempo?

  Recomendamos que las instituciones académicas comprendan las principales necesidades de las partes interesadas cuando se acerquen por primera vez a la nube. Los usuarios de los sistemas institucionales incluyen estudiantes, profesores, investigadores, personal de TI, administración, seguridad, público general y colaboradores externos. Debe identificar las necesidades principales de estos usuarios y asegurarse de contar con los mecanismos adecuados para concederles acceso a los servicios en la nube. Los diferentes tipos de usuarios requieren diferentes tipos de acceso a los servicios en la nube. Por ejemplo, los estudiantes, el profesorado y el público general necesitan acceder a las aplicaciones; el personal de TI, los administradores y el personal de seguridad necesitan acceder a la infraestructura en la nube; los investigadores y sus colaboradores externos necesitan acceder a entornos de investigación seguros; los profesores necesitan acceder a entornos de enseñanza seguros e incluso podrían querer proporcionar a los estudiantes un acceso práctico a las tecnologías de la nube. Debe disponer de herramientas para administrar de forma centralizada estas identidades de forma automatizada y utilizar los procesos establecidos para identificar, conceder y revocar permisos a medida que los roles y las responsabilidades cambian con el tiempo.

- ¿Cuenta con mecanismos para integrar adecuadamente los nuevos sistemas con su solución de administración de identidades?

  Recomendamos que las instituciones académicas faciliten la integración de los nuevos sistemas con sus sistemas de administración de identidades. Esto ofrece a la institución la flexibilidad necesaria para admitir varias funciones esenciales, ya que permite a las partes interesadas adquirir y crear sistemas que puedan integrarse fácilmente en el sistema de administración de identidades. Al simplificar el proceso de integración, será menos probable que las partes interesadas utilicen sus propias medidas de control de acceso, que podrían no aplicar las prácticas recomendadas de seguridad, como el inicio de sesión único, las claves de acceso y la autenticación multifactor (MFA). Asegúrese de que el sistema de administración de identidades pueda interoperar con los sistemas necesarios mediante integraciones nativas o protocolos estándares del sector.

- ¿Cuenta con mecanismos que permitan una detección y respuesta eficaces a los incidentes?

Las instituciones educativas suelen ser blanco de ciberataques y ransomware. Para ayudar a detectar estos incidentes y responder a ellos de forma eficaz, recomendamos un enfoque bifurcado:

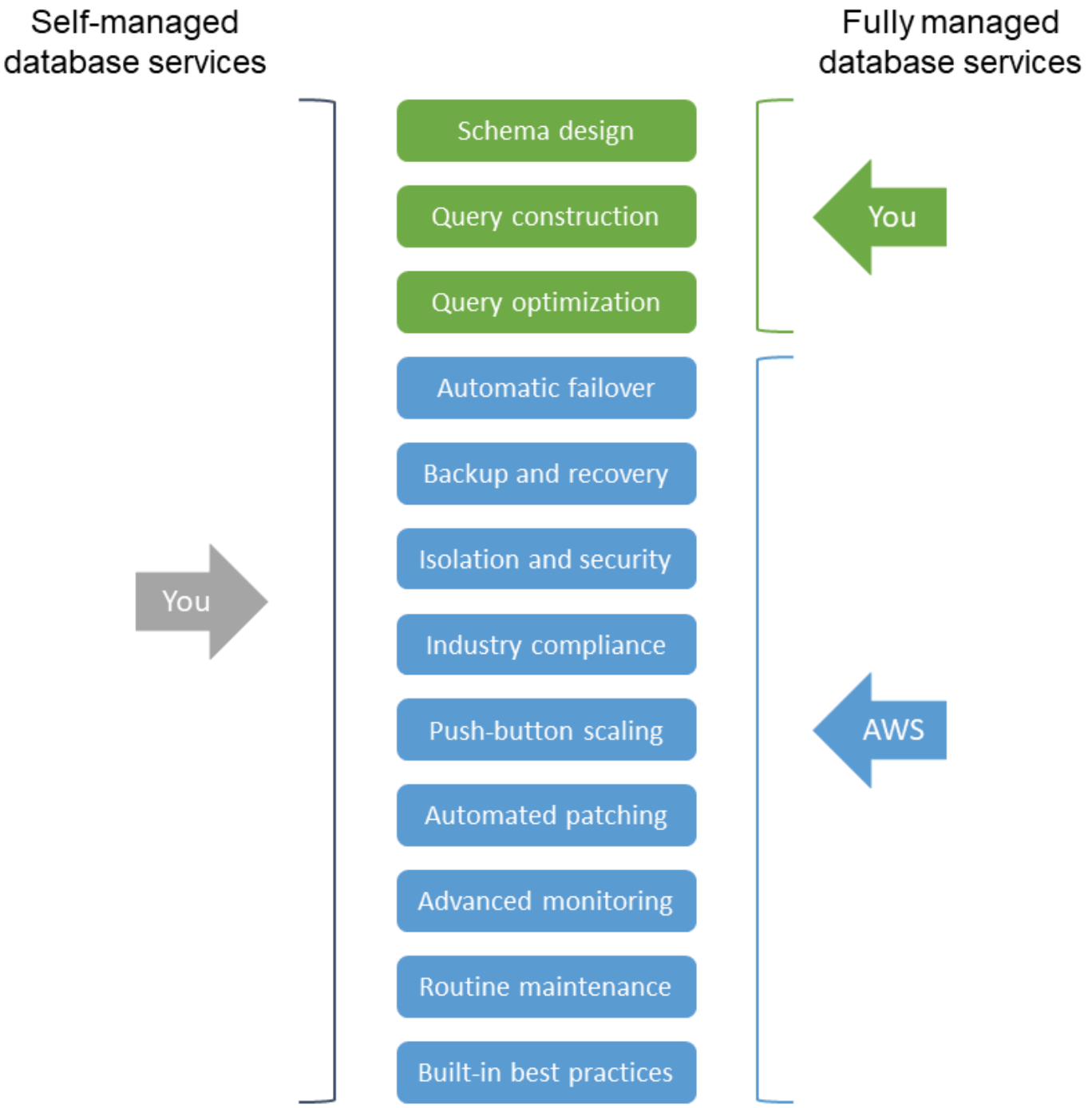
- Centre sus esfuerzos en las medidas preventivas en forma de controles de seguridad que se incrustan automáticamente en los entornos de nube.
- Implemente capacidades de detección que ayuden a los equipos de respuesta a ciberincidentes a detectar, contener y mitigar las brechas de seguridad de manera oportuna.

Al igual que con el cumplimiento, debe asegurarse de contar con los recursos, las habilidades y las herramientas necesarias para detectar, prevenir y responder a los eventos en cada entorno. Al centrarse en un solo proveedor de nube principal, puede limitar los recursos necesarios. Las instituciones académicas que no cuenten con un equipo de operaciones de seguridad maduro deberían recurrir a proveedores de software independientes, proveedores de detección y respuesta administradas y consultores de ciberseguridad para obtener ayuda en estas áreas.

Adopción de servicios administrados nativos en la nube siempre que sea posible y práctico

Si se plantea inicialmente cómo aprovechar los servicios en la nube, utilizar servicios de infraestructura y herramientas de desarrollo con los que sus equipos estén familiarizados puede parecer el mejor camino a seguir. Sin embargo, seleccionar servicios administrados nativos en la nube, especialmente las opciones sin servidor, puede reducir considerablemente los costos, el esfuerzo y la complejidad.

Los servicios administrados nativos en la nube eliminan muchas de las tareas de TI indiferenciadas que requieren tiempo y esfuerzo del personal, que podrían dedicarse mejor a actividades centradas en la misión. Además, a medida que los proveedores mejoran las capacidades de sus servicios, sus soluciones heredan mejoras incrementales en eficiencia, seguridad, resiliencia, rendimiento y otras características de forma natural. Por ejemplo, un servicio de base de datos completamente administrado es un sistema de administración de bases de datos relacionales que cuenta con muchas características, pero no es necesario aprovisionar ni administrar el servidor ni el sistema operativo subyacentes en los que se ejecuta la base de datos. Esto elimina las tareas administrativas que se suelen requerir cuando se mantiene una base de datos relacional en su propio centro de datos o en un servidor virtual autoadministrado que se aprovisiona en la nube. En el siguiente diagrama se ilustra esta diferencia.



Los beneficios de eliminar la administración de la infraestructura son evidentes al comparar cualquier servicio administrado nativo en la nube con un enfoque autoadministrado comparable. Como resultado, siempre que necesite implementar componentes en los que se ejecutarán las aplicaciones adquiridas o desarrolladas de forma personalizada, debe utilizar servicios administrados nativos en la nube para reducir el tiempo y el esfuerzo.

Cuando su equipo sea responsable de crear, implementar o administrar soluciones en la nube, utilice servicios administrados nativos en la nube para aprovechar al máximo las capacidades e innovaciones diferenciadas de su proveedor de nube. Esta estrategia le permite seleccionar, integrar e implementar los servicios en la nube de manera que reduce el tiempo y el esfuerzo que requieren estos proyectos y, al mismo tiempo, aumenta su resiliencia y seguridad. Para que la estrategia de nube tenga éxito, considere la posibilidad de adoptar estos componentes básicos nativos en la nube al migrar soluciones personalizadas a la nube, desarrollar nuevas soluciones en la nube o implementar software con licencia en la nube. Cuando evalúe las opciones de servicios administrados nativos en la nube, tenga en cuenta las siguientes preguntas clave.

- ¿Necesita dedicar más tiempo y esfuerzo del personal a las funcionalidades básicas de su misión educativa?

  La administración de los servidores, incluso los virtuales, requiere tiempo y atención para garantizar que estén actualizados con las actualizaciones y los parches del software del sistema. El uso de servicios administrados que se encarguen de estas tareas le permite destinar el tiempo del personal de TI a actividades que se ajusten más directamente a la misión de su institución. Por ejemplo, si necesita implementar contenedores, considere la posibilidad de utilizar un servicio administrado sin servidor, como AWS Fargate, para no tener que configurar ni mantener los servidores. Al eliminar la necesidad de adquirir, aprovisionar y administrar la infraestructura subyacente, podrá centrarse en ofrecer nuevas funcionalidades, optimizar el rendimiento y mejorar la experiencia del usuario. Tenga en cuenta esta ventaja al comparar los servicios administrados con las opciones autoadministradas.
- ¿Qué esfuerzo tendrá que hacer su equipo para adoptar los servicios administrados nativos en la nube?

  Diseñar e implementar soluciones con servicios administrados nativos en la nube puede requerir una curva de aprendizaje, pero estos esfuerzos se verán recompensados con una reducción de los costos, el tiempo y la complejidad a lo largo de la vida útil de la solución. Debido a la pay-as-you-go naturaleza de la computación en nube que requiere demanda, los servicios nativos de la nube le permiten realizar iteraciones y experimentar rápidamente de forma más ágil y, al mismo tiempo, evitar inversiones iniciales. Esto se traduce en una mayor innovación y en unos plazos más cortos para el proyecto. Sin embargo, para aprovechar estos beneficios de manera efectiva, considere lo que podría ser necesario para adoptar y usar el servicio, como capacitar al personal sobre los patrones de uso óptimos y refactorizar el código para adaptarlo a los servicios específicos. APIs Incluso si el servicio utiliza un código abierto o estándar del sector APIs, es posible que tengas que

refactorizar o configurar tu aplicación para gestionar la disparidad de funciones o las discordancias entre versiones.

- ¿Cómo implementa y administra la infraestructura actualmente? ¿Necesita mantener ese nivel de control?

  Existen varias formas de alojar y administrar la infraestructura en la nube, como el uso de hosts bare metal, máquinas virtuales, servicios de contenedores administrados y ofertas sin servidor. Incluso si actualmente utiliza una infraestructura similar, como máquinas virtuales o contenedores, en su entorno en las instalaciones, considere si un enfoque alternativo sería adecuado para determinadas cargas de trabajo. Por ejemplo, en lugar de ejecutar todas las aplicaciones en máquinas virtuales, considere la posibilidad de incluir las aplicaciones en contenedores y aprovechar los servicios de contenedores administrados, como Amazon Elastic Container Service (Amazon ECS). Esto puede requerir una refactorización, pero puede utilizar una herramienta como AWS App2Container para simplificar y facilitar la inclusión en contenedores. Para ir un paso más allá, en lugar de implementar servidores o contenedores para todos los componentes, considere el uso de opciones completamente sin servidor. Las tecnologías sin servidor cuentan con un escalado automático, una alta disponibilidad integrada y un modelo de pay-for-use facturación para aumentar la agilidad y optimizar los costes. Al mismo tiempo, eliminan la necesidad de administrar los servidores y planificar la capacidad. Los servicios de computación sin servidor, como AWS Lambda, son fundamentales para las arquitecturas sin servidor. Lambda admite lenguajes de programación más comunes y permite a los desarrolladores centrarse en el código de la aplicación en lugar de administrar la infraestructura. Explore estas opciones para cada carga de trabajo y tenga en cuenta factores como la curva de aprendizaje, los gastos generales de administración, el costo y las licencias.
- ¿Tiene que implementar y administrar la infraestructura de algún software con licencia?

  Al implementar y administrar software con licencia de proveedores de software independientes (ISVs), puede parecer lógico imitar la implementación local con la infraestructura de nube. Por ejemplo, podría considerar la posibilidad de sustituir las máquinas virtuales en las instalaciones por máquinas virtuales alojadas en la nube. Si bien se trata de una opción viable, considere la posibilidad de sustituir algún componente de la arquitectura por servicios administrados nativos en la nube. Por ejemplo, es posible que pueda sustituir un servidor de bases de datos autoadministrado por un servicio de bases de datos completamente administrado que reduzca la carga administrativa y ejecute el mismo motor de base de datos. Muchos ISVs ya utilizan arquitecturas de nube que aprovechan los servicios gestionados e incluso pueden ofrecer plantillas prediseñadas para simplificar la implementación. Siempre ISVs que sea posible, preferiría ofrecer

orientación y soporte prescriptivos para las implementaciones en la nube. Antes de implementar software con licencia en la nube, asegúrese de consultar sus opciones con su ISV para saber en qué se diferencian las licencias del entorno de nube de las licencias en las instalaciones.

- ¿Le preocupa que el uso de un servicio administrado pueda suponer la dependencia del proveedor?

  Muchos servicios gestionados y nativos de la nube están diseñados para cumplir con los estándares comunes del sector y. APIs Por ejemplo, los servicios de análisis como AWS GlueAmazon EMR se basan en marcos de procesamiento y almacenamiento estándar del sector, como Apache Spark y Apache Parquet. AWS Lambdaadmite de forma nativa código Java, Go, Microsoft PowerShell, Node.js, C#, Python y Ruby. Amazon Relational Database Service (Amazon RDS) admite varias versiones de motores de bases de datos comunes, como SQL Server, Oracle, PostgreSQL y MySQL. Cuando los servicios son propietarios APIs, nativos o asociados, es posible que haya soluciones disponibles para interactuar con ellos APIs mediante protocolos comunes e independientes de la nube. Por ejemplo, Amazon Simple Storage Service (Amazon S3) tiene una API específica del servicio para la integración directa, pero también puede interactuar con ella mediante protocolos de almacenamiento estándar, como el sistema de archivos de red (NFS), Server Message Block (SMB) y la interfaz de sistemas informáticos pequeños de Internet (iSCSI) cuando usa AWS Storage Gateway. Debe seguir centrándose en elegir el servicio administrado nativo en la nube que mejor se adapte a sus necesidades y, al mismo tiempo, reduzca al máximo la sobrecarga operativa, pero quizá prefiera los servicios que utilizan o ponen a disposición los estándares y protocolos comunes del sector.

Implementación de arquitecturas híbridas cuando las inversiones en las instalaciones existentes incentiven el uso continuado

La mayoría de las instituciones educativas han invertido en centros de datos en las instalaciones de diversa escala para alojar aplicaciones empresariales, soluciones de almacenamiento de datos, entornos de computación de usuario final (EUC) y recursos de computación compartidos. Todos los recursos de estos centros de datos están sujetos a diferentes ciclos de actualización, en los que debe tener en cuenta el crecimiento futuro y aprovisionar la capacidad suficiente para adaptarse a los picos de escala, lo que puede ser necesario solo pocas veces al año. Como resultado, los recursos suelen permanecer inactivos hasta el siguiente ciclo de actualización. Planificar, presupuestar, adquirir e implementar hardware nuevo puede llevar semanas, si no meses o más. Este largo proceso frena la innovación y puede retrasar el aprendizaje y la investigación.

La computación en la nube resuelve muchos de estos desafíos. La nube proporciona recursos de pay-as-you-go TI bajo demanda, por lo que puede adaptar mejor la capacidad actual a las demandas reales sin necesidad de una gran planificación ni inversión iniciales. Sin embargo, si ya ha hecho una inversión importante en hardware y recursos en las instalaciones, debería intentar utilizar esos recursos de manera eficiente y aumentarlos según sea necesario con la tecnología de nube en un modelo híbrido.

Una estrategia de nube híbrida exitosa aprovecha las inversiones existentes y, al mismo tiempo, proporciona mayor agilidad, escalabilidad y fiabilidad de lo que esas inversiones por sí solas pueden soportar. Las siguientes consideraciones le ayudarán a comenzar.

- Cuando debe alojar una nueva carga de trabajo, ¿piensa primero en la nube?

  La forma de uso de la infraestructura en la nube pública y privada en conjunto define su estrategia de nube híbrida. Un enfoque que prioriza la nube no significa que la nube sea la mejor opción para todas sus cargas de trabajo. Sin embargo, al planificar nuevas cargas de trabajo, considere la nube como la primera opción, especialmente para las cargas de trabajo que requieren nueva tecnología o que superan la capacidad de almacenamiento y procesamiento disponible en las instalaciones. Las cargas de trabajo que tienen patrones de uso transitorios e incoherentes, que necesitan resultados rápidos, que son fáciles de transportar o que requieren el hardware más reciente son las candidatas ideales para la escalabilidad y la elasticidad de la nube. Además, considere si la carga de trabajo se beneficiaría de algún servicio administrado nativo en la nube que no esté disponible en las instalaciones, incluso si tiene capacidad disponible.
- ¿Conoce el TCO del entorno en las instalaciones y colabora con su director financiero a la hora de efectuar nuevas inversiones?

  Le recomendamos que comprenda el costo total de propiedad (TCO) real que implica mantener su propio centro de datos en las instalaciones. La propiedad y el funcionamiento de la infraestructura en las instalaciones conllevan muchos costos ocultos, que incluyen no solo el hardware, el software y el soporte, sino también las instalaciones, los servicios públicos, los seguros y las horas del personal. Estos costos pueden afectar negativamente a la productividad del personal, a la resiliencia operativa y a la agilidad empresarial. Evalúe sus estructuras de licencias actuales y también sus periodos de renovación y mantenimiento. Colaborar con su director financiero puede ayudarle a identificar todos los costos ocultos cuando planee llevar a cabo nuevas inversiones. Algunas licencias pueden ofrecer la opción Traiga su propia licencia (BYOL) en la nube o pueden ser más o menos propicias para los servicios en la nube. Comprender el TCO real de su infraestructura actual le ayuda a priorizar la adopción de la nube para las cargas de trabajo que

tienen el mayor impacto en el TCO total de su organización. Su equipo de AWS cuentas dispone de herramientas fácilmente disponibles para ayudarle a comprender mejor su TCO local.

- ¿Qué infraestructura necesitará para admitir las implementaciones híbridas?

  Para adoptar con éxito los modelos híbridos, necesitará herramientas básicas de red, seguridad e infraestructura. Asegúrese de poder mantener una conectividad de red adecuada con su proveedor de servicios en la nube. Esto podría lograrse mediante una combinación de conectividad a Internet existente, redes privadas virtuales (VPNs), conexiones dedicadas (por ejemplo, proveedores de conectividad de terceros) o Internet2 y redes regionales de investigación y educación. Direct Connect Asegúrese de contar con una administración de identidad y acceso unificada en todos sus entornos en las instalaciones y en la nube. Establezca herramientas y procesos para aplicar barreras de protección, costos y uso coherentes.

- ¿El personal de TI está preparado para operar implementaciones híbridas?

  Los servicios en la nube pueden requerir habilidades específicas que su equipo podría no tener. Para limitar la formación y la capacitación necesarias para formar a su personal de TI a fin de adoptar la nube de manera efectiva, considere si el proveedor de nube ofrece algún servicio que reutilice las habilidades existentes y cree en base a ellas tanto en las instalaciones como en la nube. Por ejemplo, si usa y conoce Kubernetes, podría considerar el uso de Amazon Elastic Kubernetes Service (Amazon EKS) o Amazon EKS Anywhere. Si utilizas Amazon para ONTAP y estás familiarizado con NetApp él, podrías considerar la posibilidad de utilizar Amazon FSx para NetApp ONTAP. Del mismo modo, considere también si las soluciones de los socios actuales que utiliza tienen integraciones nativas o son compatibles con entornos de nube.

- ¿Puede transferir el almacenamiento a largo plazo o la computación de bajo uso de las instalaciones a la nube?

  El almacenamiento en la nube ofrece varias opciones rentables para el almacenamiento de datos a largo plazo. Por ejemplo, Amazon Simple Storage Service (Amazon S3) ofrece varios niveles de almacenamiento optimizados para distintos casos de uso. Si la institución debe conservar determinados datos durante un periodo de tiempo prolongado, considere el uso de soluciones de almacenamiento en frío como Amazon Glacier. Al transferir estos datos al almacenamiento en la nube, se puede liberar un valioso almacenamiento en las instalaciones de alto rendimiento. Servicios como AWS Storage Gateway facilitan el acceso de las aplicaciones en las instalaciones a los niveles de almacenamiento en la nube a través de protocolos estándar como SMB, NFS e iSCSI. Del mismo modo, considere la posibilidad de reducir la carga de cualquier tarea de computación que tenga un uso poco frecuente o bajo. Si cuenta con servidores

en las instalaciones dedicados a este tipo de tareas, puede usar servicios de computación en la nube escalables, en los que los recursos se aprovisionan bajo demanda y solo paga por lo que utiliza. Estas opciones de almacenamiento a largo plazo y de bajo costo y de procesamiento de bajo consumo también hacen que la nube sea ideal para las copias de seguridad y la recuperación ante desastres. Puede utilizar almacenamiento y procesamiento seguros, duraderos y escalables en la nube para proteger sus datos y recuperarse rápidamente en caso de desastre sin tener que mantener por su cuenta la infraestructura de almacenamiento y computación necesaria.

- ¿Dispone de capacidad suficiente en las instalaciones para experimentar e innovar?

  La falta de elasticidad y agilidad en los entornos en las instalaciones de tamaño fijo puede limitar los servicios y la tecnología disponibles para los usuarios. Si tiene ciclos de actualización estrictos, es posible que las nuevas cargas de trabajo tengan que esperar hasta el siguiente ciclo para su implementación. Este modelo operativo puede limitar la experimentación y ralentizar la innovación. Cuando tenga una carga de trabajo nueva o novedosa que deba probarse, considere la posibilidad de utilizar servicios en la nube elásticos y escalables. Los recursos de la nube se pueden aprovisionar y desaprovisionar bajo demanda y solo paga por lo que utiliza, de modo que puede experimentar y responder rápido a los errores y, al mismo tiempo, minimizar el riesgo organizativo.

- ¿Tiene requisitos únicos de cumplimiento o rendimiento que lo obligan a mantener los datos en las instalaciones?

  Las cargas de trabajo con requisitos estrictos de latencia o residencia de datos pueden requerir que mantenga los datos en las instalaciones o lo más cerca posible de los usuarios. Para estos casos de uso, puede priorizar el uso de los recursos existentes en las instalaciones. Sin embargo, considere si su proveedor de nube ofrece servicios periféricos o mecanismos para utilizar la tecnología basada en la nube en las instalaciones. Los servicios periféricos ofrecen procesamiento, análisis y almacenamiento de datos más cerca de sus propios puntos de conexión y le permiten implementar herramientas fuera de los centros de datos estándar de los proveedores de nube. Por ejemplo, AWS ofrece servicios como Zonas locales de AWS y AWS Wavelength para implementar aplicaciones en ubicaciones específicas más cercanas a los usuarios finales. También puede incorporar los servicios y la funcionalidad de la nube a su centro de datos existente con servicios como AWS Outposts, AWS Storage Gateway, Amazon ECS Anywhere y Amazon EKS Anywhere.

Reserva del uso multinube solo para las cargas de trabajo que no puedan cumplir con los requisitos técnicos o empresariales a través de un proveedor de nube

Multinube se refiere al uso de servicios en la nube de varios (dos o más) proveedores de servicios en la nube. Tener una estrategia multinube puede ofrecer ciertos beneficios, como la opción de aprovechar las capacidades diferenciadas de varios proveedores de nube o la capacidad de cumplir con los requisitos de soberanía de datos que un único proveedor de nube podría no cumplir. Sin embargo, para cada proveedor que utilice, asegúrese de contar con las personas, las habilidades, la formación y los conjuntos de herramientas adecuados para utilizar ese proveedor de manera eficaz. Además, si desea utilizar una estrategia multinube para una carga de trabajo específica, necesitará recursos adicionales para integrar e interoperar los servicios necesarios de cada proveedor de nube. Le recomendamos que considere el uso de un entorno multinube solo cuando los beneficios superen el aumento de la inversión. Para determinar si debe elegir una estrategia multinube, tenga en cuenta las siguientes preguntas clave.

- ¿Dispone de los recursos y las habilidades para explorar los servicios que ofrecen los distintos proveedores de nube?

  Cuando varios proveedores de nube ofrecen diversos productos y servicios, su personal necesita las habilidades esenciales para aprovechar las capacidades de cada proveedor. El uso de los servicios de un único proveedor de nube puede requerir la mejora de las habilidades y la formación del personal, en función de los servicios y las características que utilice. Si se está planteando una estrategia multinube, evalúe sus recursos actuales para determinar qué habilidades adicionales necesitaría para utilizar los servicios de varios proveedores de nube de manera eficaz. Es posible que tenga que aumentar el personal o invertir más tiempo y dinero en mejorar las habilidades y la formación, más allá de lo que requeriría un único proveedor de nube. Si ya cuenta con equipos o usuarios individuales que utilizan distintos proveedores de nube, considere las ventajas organizativas de consolidarlos en un proveedor de nube principal. case-by-case
- ¿Qué sobrecarga adicional supondría una arquitectura multinube concreta?

  Un factor común de la multinube es el deseo de utilizar un servicio administrado específico de un proveedor que tenga capacidades que puedan diferenciarse de los servicios de otro proveedor de nube. Por ejemplo, es posible que quiera usar un proveedor de nube para sus necesidades de infraestructura y el servicio administrado de otro proveedor para servicios de dominio y directorio. Sin embargo, aunque ese único servicio administrado reduzca la carga administrativa y simplifique

la administración de ese componente de la arquitectura, podría suponer una sobrecarga adicional para otras cargas de trabajo, como la refactorización del código, las necesidades de conectividad privada o las tareas de integración manual. Identifique esta sobrecarga adicional desde el principio y asegúrese de que no compense ni eclipse los beneficios que su equipo puede obtener de un servicio diferenciado.

- ¿Cómo centralizará la supervisión y la administración entre los proveedores de nube?

  Cuando comience a implementar aplicaciones y funcionalidades mediante recursos de distintos proveedores de nube, tenga en cuenta cómo etiquetará, supervisará y administrará los recursos. Cada proveedor tendrá sus propias herramientas, que quizá pueda ampliar a otros entornos. Por ejemplo, puede usar Amazon CloudWatch para monitorear métricas y registros clave, crear alarmas y visualizar sus aplicaciones e infraestructura en entornos de nube única, híbrida y multinube. También puede utilizar AWS Systems Manager para mejorar la visibilidad y el control de los recursos, diagnosticar y corregir rápidamente los problemas operativos y automatizar procesos como la actualización y la aplicación de parches a máquinas virtuales en todos los entornos. Si tiene requisitos que las herramientas de un proveedor no pueden satisfacer, puede buscar soluciones de socios, pero estas podrían suponer un costo o esfuerzo de integración adicional.
- ¿Cómo se puede administrar la infraestructura como código con automatización cuando se utilizan diferentes proveedores de nube?

  Al ejecutar recursos en la nube, el aprovisionamiento y la administración automatizados de los recursos le ayudan a administrar varios entornos de manera eficiente. Las herramientas de automatización APIs y las nativas varían según los proveedores de nube. Si es posible, considere la posibilidad de utilizar un conjunto común de herramientas de orquestación e implementación que puedan adaptarse a los recursos de diferentes proveedores de nube. Esto proporciona una mayor flexibilidad y simplifica las operaciones en varias nubes. Sin embargo, podría ser más sencillo utilizar la automatización nativa de cada proveedor por separado y establecer procesos organizativos para garantizar un uso adecuado.
- ¿Tiene requisitos normativos y de cumplimiento que debe satisfacer cada proveedor de nube?

  Es posible que tenga consideraciones normativas que dicten cómo se deben almacenar y gestionar los datos. Céntrese en estandarizar las políticas (como el tráfico de red, el almacenamiento y la seguridad) que se puedan aplicar automáticamente a cada entorno de nube de varios proveedores de nube. Tenga en cuenta cómo se comunicarán sus aplicaciones con sus datos y alójelo en el mismo proveedor. Si sus aplicaciones y datos están fragmentados entre distintos proveedores, será difícil garantizar que se satisfagan los requisitos normativos y de

cumplimiento. Suele ser mejor que las aplicaciones estén lo más cerca posible de los datos para minimizar la latencia de la red, maximizar el rendimiento de los datos y limitar la salida de datos, a la vez que se simplifican los controles de seguridad y acceso.

- ¿Puede minimizar el TCO y maximizar los descuentos en los precios al implementar aplicaciones en varios proveedores de nube?

  Es importante tener en cuenta el costo total de propiedad (TCO) al considerar el uso de un entorno multinube. Ejecutar aplicaciones en varios proveedores de nube puede aumentar los costos operativos y los gastos administrativos necesarios para mantener y administrar los recursos en cada entorno. Además, al distribuir el uso entre varios proveedores, es más difícil aprovechar los descuentos en los precios por volumen o los acuerdos empresariales de un proveedor específico. Tenga en cuenta estos factores al determinar si los beneficios de un entorno multinube justifican el aumento del TCO.

Ejemplos de casos de uso

Para comprender mejor la aplicación de estos principios en diferentes escenarios, analicemos algunos ejemplos de casos de uso. Estos casos de uso se basan en la forma en que las instituciones educativas del mundo real adoptan los servicios en la nube.

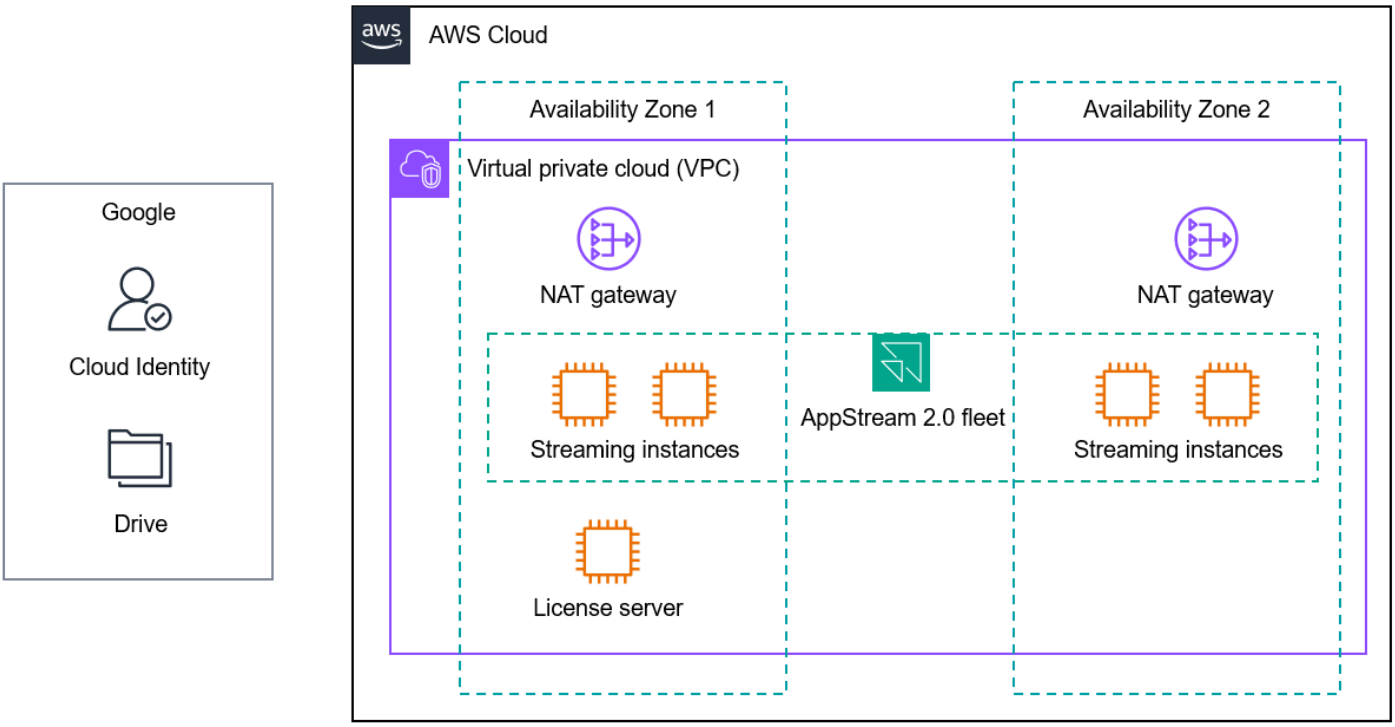
- Laboratorios de equipos virtuales
- Predicción del éxito de los estudiantes
- Federación de identidades e inicio de sesión único
- Ampliación en la nube para la computación de investigación

Laboratorios de equipos virtuales

A pesar de la popularidad de las herramientas de aprendizaje basadas en la web y de la abundancia de dispositivos de usuario, como computadoras portátiles, Chromebooks y tabletas, la mayoría de las instituciones educativas mantienen laboratorios de equipos físicos para aplicaciones heredadas o que consumen muchos recursos. Estos laboratorios de equipos suelen ser imprescindibles para los planes de estudio de ciencias, tecnología, ingeniería y matemáticas (STEM), educación técnica y profesional (CTE), arte y educación plástica, ingeniería y otros planes de estudio similares. Los centros educativos pueden ampliar o sustituir los laboratorios de equipos físicos por escritorios virtuales basados en la nube o servicios de transmisión de aplicaciones para garantizar que todos los estudiantes tengan acceso a las aplicaciones que necesitan en cualquier momento, desde cualquier lugar y desde cualquier dispositivo. Esto mejora la equidad digital, permite el aprendizaje remoto, garantiza una experiencia del usuario uniforme y asegura el acceso remoto, a la vez que reduce los costos.

En la educación primaria y secundaria (K-12), muchos colegios estadounidenses utilizan Amazon WorkSpaces Applications, un servicio de transmisión de aplicaciones y escritorios totalmente gestionado, para ofrecer laboratorios de computación virtuales que proporcionan acceso a Adobe Creative Cloud, el software de Autodesk, los planes de estudio de STEM y CTE, como Project Lead the Way (PLTW), y más. Muchas organizaciones de educación primaria y secundaria ya administran el inicio de sesión único y el almacenamiento de archivos de los estudiantes a través de Google Workspace y Google Drive, que son aplicaciones de SaaS. Estas instituciones pueden configurar el inicio de sesión único entre Google Workspace y Applications mediante la federación SAML 2.0. WorkSpaces También pueden configurar la integración nativa entre WorkSpaces las aplicaciones

y Google Drive para que los estudiantes puedan usar el almacenamiento existente. El siguiente diagrama ilustra la implementación de WorkSpaces las aplicaciones para este caso de uso.



Esta arquitectura sigue estas recomendaciones:

- Seleccione un proveedor de nube principal y estratégico. Esta arquitectura utiliza servicios en la nube de un proveedor de nube principal. Aunque incluye la integración con aplicaciones de SaaS que no están alojadas en el mismo proveedor, esas integraciones se llevan a cabo mediante configuraciones sencillas. Los conocimientos y habilidades en la nube solo son necesarios para implementar y administrar los servicios del proveedor de nube principal.
- Diferencie entre aplicaciones de SaaS y servicios de nube básicos. Google Workspace y Google Drive no están alojados en el mismo proveedor de nube que AppStream 2.0, pero eso es aceptable porque esta implementación proporciona las integraciones necesarias. El inicio de sesión único permite la administración centralizada de identidades y se configura de forma segura mediante SAML 2.0. Para habilitar el almacenamiento persistente en la nube para los estudiantes, es necesario realizar cambios de configuración sencillos en Google Drive y en WorkSpaces las Aplicaciones.
- Establezca los requisitos de seguridad y gobernanza para cada proveedor de servicios en la nube. Los servicios e integraciones que se utilizan en esta arquitectura ayudan a cumplir los requisitos de seguridad y gobernanza de una institución. El tráfico de transmisión está cifrado. La federación

a través de Google Workspace permite una administración de identidades centralizada. Los servicios de red como Amazon Virtual Private Cloud (Amazon VPC) admiten la configuración de subredes, enrutamiento y firewalls. Puede filtrar el contenido mediante la configuración de DNS, los agentes, los dispositivos virtuales o los servicios administrados, como el firewall de DNS de Amazon Route 53 Resolver . Puede usar servicios como los que ayudan AWS Control Towera garantizar que la cuenta de AWS que aloja WorkSpaces las aplicaciones cumpla con las barreras y los controles organizacionales estándar.

- Adopte soluciones gestionadas y nativas de la nube siempre que sea posible y práctico. WorkSpaces Applications es un servicio gestionado para la transmisión de aplicaciones y escritorios. Puede transmitir escritorios y aplicaciones sin preocuparse por el aprovisionamiento, el escalado o el mantenimiento de los servidores. Instale las aplicaciones, conecte las soluciones de identidad, red y almacenamiento adecuadas y, a continuación, administre y transmita esas aplicaciones de forma centralizada a los usuarios. De este modo, elimina gran parte del trabajo pesado e indiferenciado que se requeriría para administrar su propia solución de transmisión de escritorios virtuales.

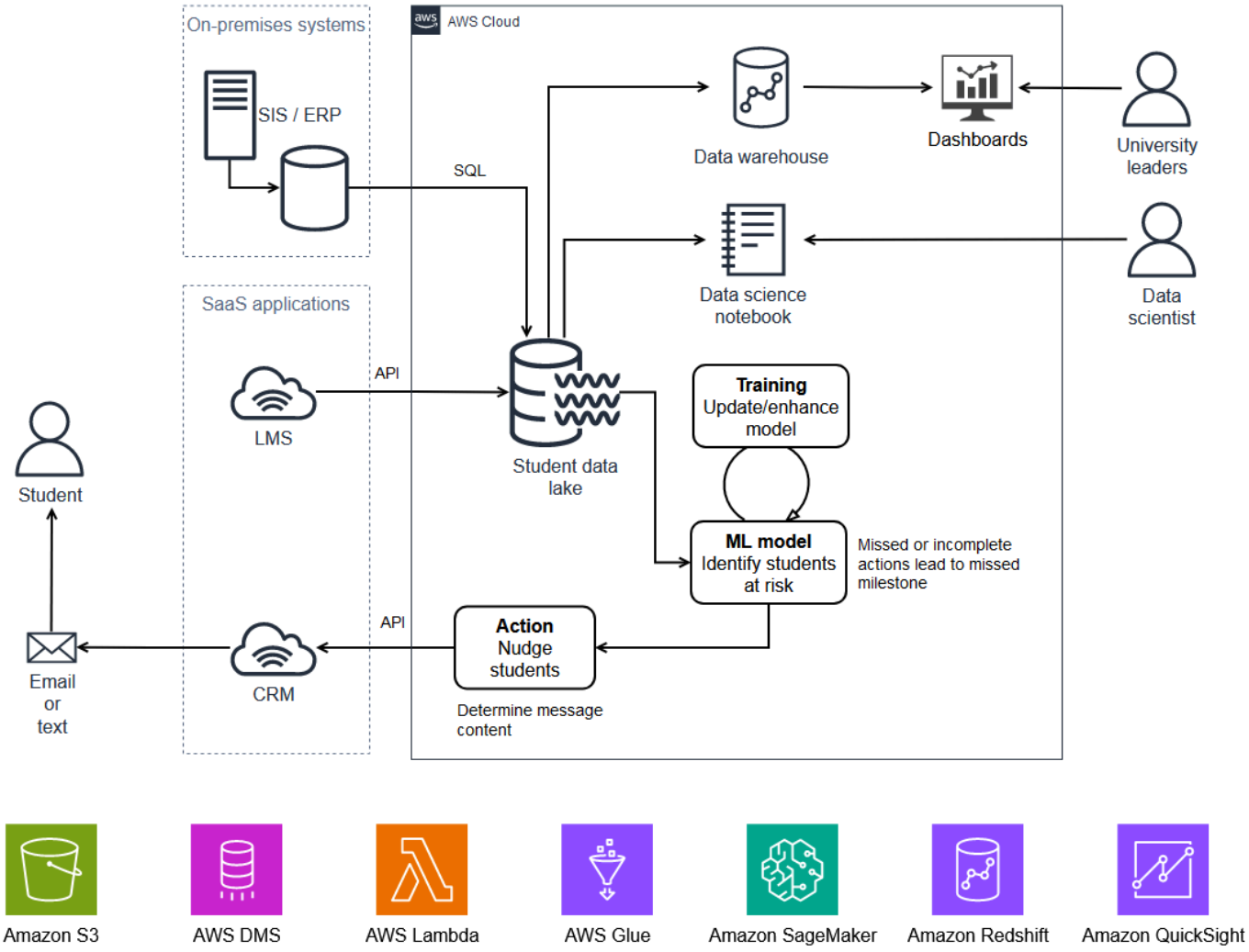
Predicción del éxito de los estudiantes

Una universidad del Medio Oeste de EE. UU. descubrió que algunas actividades clave para los estudiantes de primer año predicen en gran medida su éxito, tanto en el primer semestre de clases como en la obtención de la licenciatura. La universidad quería implementar un sistema que observara la finalización de estas actividades y, cuando se acercaban o superaban los plazos clave, quería animar a los estudiantes a completar estos pasos.

Los datos del sistema de administración del aprendizaje (LMS) de SaaS fueron una entrada clave para esta solución, pero resultó difícil acceder a los datos y procesarlos con las herramientas de almacenamiento de datos del equipo de TI de la universidad. Además, los mensajes a los estudiantes tenían que enviarse a través del sistema de administración de relaciones con los clientes (CRM) de la institución basado en la nube. Para crear una solución funcional y evaluar la eficacia de las peticiones enviadas a los estudiantes, la universidad tuvo que iniciar los mensajes a través del sistema de CRM y recopilar datos a partir de él.

La universidad desarrolló e implementó una solución en un único entorno de nube. La solución es una combinación de servicios administrados nativos en la nube, servidores en la nube aprovisionados e integraciones con sistemas en las instalaciones y aplicaciones de SaaS basadas en la nube. Como se muestra en el siguiente diagrama, la solución incorpora los datos del sistema

de información estudiantil (SIS), LMS y CRM en un lago de datos. Utiliza estos datos para identificar a los estudiantes que corren el riesgo de no participar en actividades clave, les envía mensajes a través del sistema de CRM y proporciona un panel a los líderes de la universidad.



Esta arquitectura sigue estas recomendaciones:

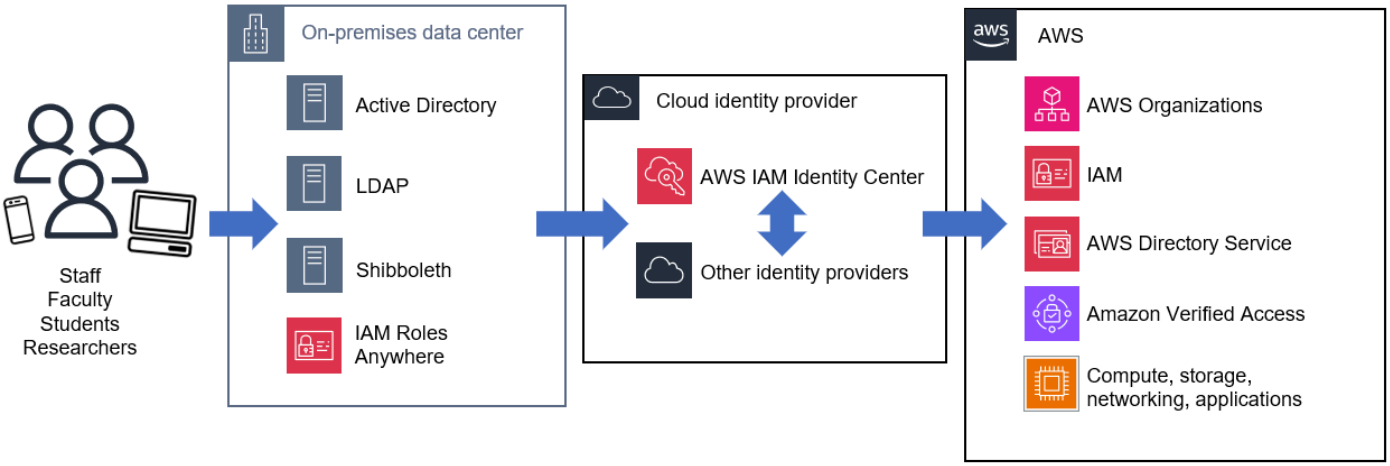
- Seleccione un proveedor de nube principal y estratégico. El proveedor de nube estratégico de la universidad aloja toda la solución implementada. De este modo, el personal empresarial y de TI se puede centrar en desarrollar habilidades en un conjunto único e integrado de capacidades en la nube.
- Diferencie entre aplicaciones de SaaS y servicios de nube básicos. La universidad diferencia entre las aplicaciones de SaaS y los principales servicios de análisis en la nube, y utiliza integraciones con las aplicaciones de SaaS para recopilar datos e iniciar las comunicaciones adecuadas.

- Establezca los requisitos de seguridad y gobernanza para cada proveedor de servicios en la nube. La universidad garantiza la seguridad de todos los componentes de la arquitectura mediante el uso de barreras de protección y controles, lo que incluye el cifrado en tránsito y en reposo, para gestionar los datos de los estudiantes de forma adecuada.
- Adopte soluciones administradas nativas en la nube siempre que sea posible y práctico. Los servicios gestionados nativos de la nube se utilizan para la ingesta, el almacenamiento, la base de datos y la funcionalidad de extracción, transformación y carga (ETL) de datos, lo que reduce el tiempo necesario para desarrollar el flujo de trabajo de procesamiento de end-to-end datos.

Federación de identidades e inicio de sesión único

Garantizar una administración de identidades coherente en todos los sistemas principales es clave para adoptar cualquier tecnología de forma exitosa y segura. Las instituciones educativas están adoptando cada vez más soluciones de identidad e inicio de sesión único basadas en la nube, como AWS IAM Identity CenterMicrosoft Entra ID (anteriormente Azure Active Directory), Okta,, Ping Identity JumpCloud OneLogin, CyberArk para simplificar la administración de identidades, reducir la carga operativa y aplicar de forma centralizada las mejores prácticas, como la autenticación multifactor y el acceso con privilegios mínimos.

Muchas de estas instituciones aún mantienen servicios de administración de identidades y directorios, como Active Directory y Shibboleth, para sus entornos en las instalaciones. Se pueden integrar con soluciones basadas en la nube para permitir la administración centralizada de identidades y el inicio de sesión único para los estudiantes, los profesores y el personal. Los proveedores de soluciones en la nube deben tener plataformas sólidas de administración de easy-to-integrate identidades que le permitan federar las identidades a través de los proveedores de identidad en la nube con sus aplicaciones existentes, sus soluciones SaaS y sus servicios en la nube. En el siguiente diagrama se muestra un ejemplo de la arquitectura.



Esta arquitectura sigue estas recomendaciones:

- Seleccione un proveedor de nube principal y estratégico. Esta arquitectura se utiliza AWS como proveedor de nube principal. Al integrarse con un proveedor de identidades en la nube y los servicios de directorios y administración de identidades existentes en las instalaciones, esta arquitectura admite el aprovisionamiento y la administración automatizados del acceso tanto a los servicios del proveedor de nube principal como a otras aplicaciones y soluciones de SaaS. De este modo, se garantiza que los requisitos de seguridad y gobernanza se cumplan de manera coherente y fácil de administrar a medida que se agregan más aplicaciones y servicios a la cartera de tecnología de la institución.
- Diferencie entre aplicaciones de SaaS y servicios de nube básicos. Esta arquitectura integra varios tipos de sistemas de identidad basados en la nube, SaaS y locales para proporcionar acceso a los Nube de AWS servicios y otras aplicaciones. Muchas soluciones de inicio de sesión único y proveedores de identidades basadas en la nube también son aplicaciones de SaaS que pueden usar integraciones nativas y protocolos estándar, como SAML, para funcionar en todos los entornos.
- Establezca los requisitos de seguridad y gobernanza para cada proveedor de servicios en la nube. Esta arquitectura sigue las directrices sobre la administración de identidades y accesos emitidas por numerosos marcos de seguridad, como el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST), NIST 800-171 y NIST 800-53. Las integraciones con AWS Organizations, AWS Identity and Access Management (IAM) y otros servicios de cumplimiento, identidad y seguridad de AWS ayudan a proporcionar controles de acceso detallados y seguros que se basan en permisos de grupos.

- Adopte servicios administrados nativos en la nube siempre que sea posible y práctico. Esta arquitectura utiliza servicios administrados basados en la nube para la administración de identidades y el inicio de sesión único. De este modo, se reduce el tiempo y la energía que se invierten en la administración de la infraestructura y facilita el mantenimiento de estos sistemas críticos.
- Implemente arquitecturas híbridas cuando las inversiones en las instalaciones existentes incentiven el uso continuado. Esta arquitectura integra las inversiones en las instalaciones existentes en infraestructura para alojar cargas de trabajo de Active Directory, Lightweight Directory Access Control (LDAP) y Shibboleth, además de proporcionar una vía para trasladar eventualmente los servicios de identidad básicos a una infraestructura basada en la nube. Además, si tus cargas de trabajo locales necesitan un acceso a los AWS recursos basado en certificados, puedes usar Roles Anywhere.AWS Identity and Access Management

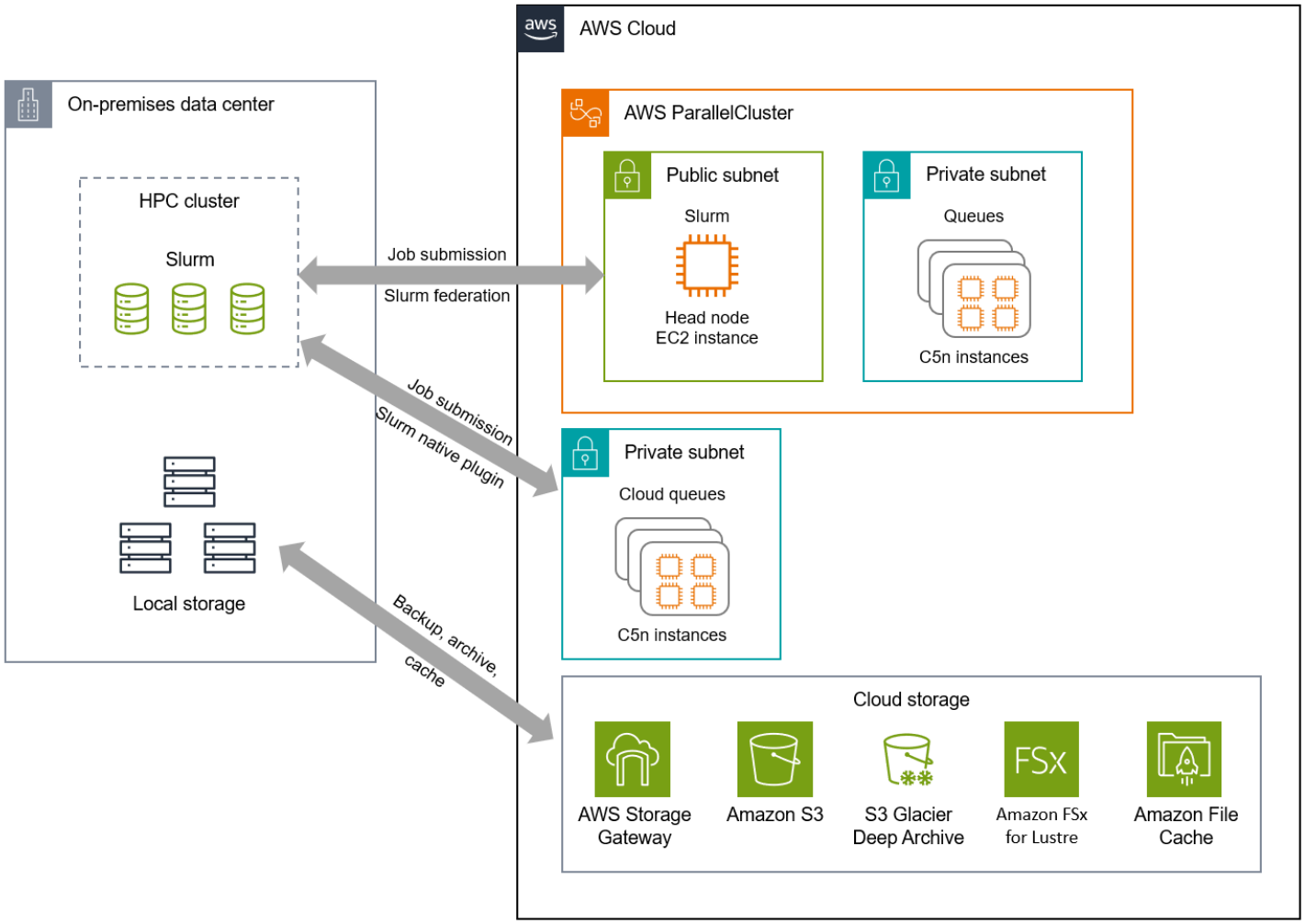
Ampliación en la nube para la computación de investigación

El grupo de investigación en computación de una institución de investigación estadounidense R1 (universidades de doctorado con una actividad investigadora muy elevada) llevaba muchos años ejecutando clústeres de computación de alto rendimiento (HPC) en las instalaciones con el programador Slurm. A excepción de algunas semanas de mantenimiento programado, los clústeres funcionaban con un porcentaje de uso del 80 % al 95 % y la mayoría de sus colas estaban llenas.

El creciente número de actividades de investigación en la institución generó desafíos en materia de capacidad. Algunos investigadores de alto perfil siempre efectuaban simulaciones de larga duración en determinadas colas, lo que aumentaba el tiempo de espera para otros usuarios. Los profesores recién contratados necesitaban ejecutar un gran número de simulaciones meteorológicas para crear un novedoso modelo de inteligencia artificial y machine learning (IA y ML) para la previsión meteorológica, pero necesitaban más capacidad de la disponible. El grupo de investigación en computación también estaba recibiendo más solicitudes de las últimas unidades de procesamiento gráfico (GPUs) para entrenar modelos de aprendizaje automático. A pesar de contar con financiación para nuevas GPUs unidades, el equipo tendría que esperar meses para obtener la aprobación necesaria para ampliar el espacio de los racks en el centro de datos.

Muchos investigadores no estaban dispuestos a eliminar los datos antiguos, por lo que la capacidad de almacenamiento local también suponía un desafío. Se necesitaba una opción de almacenamiento a largo plazo más escalable para liberar espacio de almacenamiento valioso y de alto rendimiento en las instalaciones.

La nube aborda estos desafíos con soluciones híbridas de computación y almacenamiento que permiten ampliar la computación para investigación en la nube cuando la capacidad en las instalaciones no sea suficiente. En el siguiente diagrama de arquitectura, se ilustran algunos enfoques basados en el uso intensivo de recursos de computación y de almacenamiento mediante herramientas como AWS ParallelCluster y AWS Storage Gateway.



Esta arquitectura sigue estas recomendaciones:

- Seleccione un proveedor de nube principal y estratégico. Esta arquitectura utiliza un proveedor de nube principal para evitar las restricciones del enfoque de mínimo común denominador. De esta forma, la institución puede aprovechar la innovación y los servicios nativos de computación y almacenamiento que ofrece el proveedor de nube principal. El equipo de investigación en computación puede centrarse en optimizar las cargas de trabajo en el entorno proporcionado por el proveedor de nube principal, y no en cómo trabajar en diferentes entornos de nube.

- Establezca los requisitos de seguridad y gobernanza para cada proveedor de servicios en la nube. Cada servicio y herramienta utilizados en esta arquitectura se puede configurar para cumplir con los requisitos de seguridad y gobernanza del equipo de computación de investigación, que incluyen la conectividad privada, el cifrado de datos en tránsito y en reposo, el registro de actividades, etc.
- Adopte servicios administrados nativos en la nube siempre que sea posible y práctico. Esta arquitectura ofrece la posibilidad de utilizar servicios de almacenamiento y computación administrados, así como herramientas para simplificar la administración de clústeres. De esta forma, el equipo de investigación en computación no tiene que preocuparse por administrar los clústeres o la infraestructura subyacente por sí solo, lo que puede resultar complejo y llevar mucho tiempo.
- Implemente arquitecturas híbridas cuando las inversiones en las instalaciones existentes incentiven el uso continuado. Esta arquitectura permite a la institución continuar utilizando los recursos en las instalaciones y aprovechar la nube para aumentar la capacidad y ampliar la potencia de computación bajo demanda. Con la nube, la institución puede ajustar el tipo de computación para maximizar la relación entre precio y rendimiento y acceder a la tecnología más reciente a fin de promover la innovación sin tener que efectuar una gran inversión inicial en hardware adicional en las instalaciones.

Siguientes pasos

La selección de un modelo de implementación adecuado para las cargas de trabajo en la nube requiere una reflexión cuidadosa. Utilice las recomendaciones que se describen en esta documentación para guiar su toma de decisiones y evitar errores comunes, como la complejidad innecesaria, el aumento de las exigencias del personal, la incoherencia en la gobernanza y los enfoques con el mínimo común denominador. Si sigue estas prácticas recomendadas, puede acelerar la adopción de la nube para cumplir y superar sus objetivos institucionales de forma más efectiva.

Recuerde seleccionar un proveedor de nube principal y estratégico y establecer un centro de excelencia (CCoE) en la nube para ayudar a impulsar la madurez organizacional y garantizar su éxito a largo plazo. Diferencie entre aplicaciones SaaS y servicios de nube básicos, e identifique los requisitos principales de seguridad y gobernanza para cada uno. Siempre que sea posible, adopte servicios administrados nativos en la nube e implemente arquitecturas híbridas cuando sus inversiones actuales en centros de datos incentiven el uso continuado. Por último, reserve el uso multinube solo para aquellas cargas de trabajo que realmente lo requieran.

AWS está bien posicionado para ayudarlo a administrar entornos de nube única, híbrida y multinube. Su institución puede usar soluciones AWS de administración y observabilidad como AWS Systems ManagerAWS Config, y Amazon CloudWatch para simplificar y centralizar la administración y el monitoreo de su infraestructura y aplicaciones, independientemente de su entorno. Con servicios de datos y análisis como Amazon Athena, AWS Glue y AWS DataSync, puede obtener información valiosa de todos los datos, independientemente de dónde se almacenan. Las soluciones híbridas, por ejemplo AWS OutpostsAWS Wavelength, le AWS Snow Familypermiten llevar la AWS infraestructura y los servicios a donde sea que los necesite. Herramientas como Amazon EKS Distro le ayudan a crear clústeres de Kubernetes autogestionados en AWS, de forma local o en otras nubes.

Al definir la estrategia de nube, tenga en cuenta los siguientes pasos:

1. Revise el marco de adopción de la AWS nube (AWS CAF) para identificar y priorizar las oportunidades de transformación, evaluar y mejorar su preparación para la nube y desarrollar su hoja de ruta de transformación de forma iterativa.
2. Identifique un sistema de implementación de la nube para comenzar como una prueba de concepto. Esto le ayudará a definir la base o el marco de la nube para validar cualquier suposición, así como permitir futuras implementaciones de la nube.

3. Involucre a su equipo AWS de cuentas para analizar sus objetivos de implementación de la nube. El equipo de AWS cuentas puede ayudarlo a proporcionar aclaraciones, sugerir enfoques, identificar las dependencias y también trabajar con sus equipos para planificar su viaje desde el concepto inicial hasta la implementación.

Colaboradores

Los colaboradores de esta guía son las siguientes personas:

- Kevin Arand, administrador sénior, arquitectura de soluciones, educación, AWS
- Kevin McCandless, arquitecto de soluciones sénior, educación primaria y secundaria, AWS
- Craig Jordan, arquitecto de soluciones jefe, educación, AWS
- Jesse Roberts, arquitecto de soluciones jefe, educación primaria y secundaria y SLG, AWS
- Jianjun Xu, arquitecto de soluciones jefe, educación, AWS
- Josh Badal, arquitecto de soluciones sénior, educación, AWS
- Raj Chary, arquitecto de soluciones sénior, educación, AWS

Documentación adicional

Para obtener información adicional, consulte los siguientes recursos:

- AWS Centro de arquitectura de
- Transformación de la nube del sector público
- AWS Cloud Adoption Framework (AWSCAF)
- Soluciones de AWS para nubes híbridas y multinube

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial	—	15 de septiembre de 2023

AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por la Guía AWS prescriptiva. Para sugerir entradas, utilice el enlace Enviar comentarios al final del glosario.

Números

Las 7 R

Siete estrategias de migración comunes para trasladar aplicaciones a la nube. Estas estrategias se basan en las 5 R que Gartner identificó en 2011 y consisten en lo siguiente:

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Amazon Aurora PostgreSQL-Compatible Edition.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: Migrar la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la nube de Nube de AWS.
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: Migrar el sistema de administración de las relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Oracle en una instancia de EC2 en la Nube de AWS.
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma en las instalaciones a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

- Retirar: retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios administrados.

ACID

Consulte atomicidad, consistencia, aislamiento, durabilidad.

migración activa-activa

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas (mediante una herramienta de replicación bidireccional o mediante operaciones de escritura doble) y ambas bases de datos gestionan las transacciones de las aplicaciones conectadas durante la migración. Este método permite la migración en lotes pequeños y controlados, en lugar de requerir una transición única. Es más flexible, pero requiere más trabajo que una migración activa-pasiva.

migración activa-pasiva

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas, pero solo la de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función de agregación

Función SQL que actúa en un grupo de filas y calcula un único valor de devolución para el grupo. Entre los ejemplos de funciones de agregación se incluyen `SUM` y `MAX`.

IA

Consulte inteligencia artificial.

AIOps

Consulte operaciones de inteligencia artificial

anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

antipatrones

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

control de aplicaciones

Enfoque de seguridad que permite usar de manera exclusiva aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para el proceso de detección y análisis de la cartera y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte ¿Qué es la inteligencia artificial?

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo AIOps se utiliza en la estrategia de AWS migración, consulte la guía de integración de operaciones.

cifrado asimétrico

Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

atomicidad, consistencia, aislamiento, durabilidad (ACID)

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

control de acceso basado en atributos (ABAC)

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABAC AWS en la documentación AWS Identity and Access Management (IAM).

origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

Zona de disponibilidad

Una ubicación distinta dentro de una Región de AWS que está aislada de los fallos en otras zonas de disponibilidad y que proporciona una conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

AWS Marco de adopción de la nube (AWS CAF)

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la Página web de AWS CAF y el Documento técnico de AWS CAF.

AWS Marco de calificación de la carga de trabajo (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS

Schema Conversion Tool ().AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

bot malicioso

Bot destinado a causar interrupciones o daños a personas u organizaciones.

BCP

Consulte planificación de la continuidad del negocio.

gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las llamadas sospechosas a la API y acciones similares. Para obtener más información, consulte Datos en un gráfico de comportamiento en la documentación de Detective.

sistema big-endian

Un sistema que almacena primero el byte más significativo. Consulte también endianidad.

clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

implementación azul/verde

Estrategia de implementación en la que se crean dos entornos separados, pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación se ejecuta en el otro entorno (verde). Esta estrategia lo ayuda a hacer reversiones rápidas con un impacto mínimo.

bot

Aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan la información de Internet. Otros bots, conocidos como bots maliciosos, tienen como objetivo causar interrupciones o daños a personas u organizaciones.

botnet

Redes de bots infectadas por malware y que están bajo el control de una sola parte, conocida como pastor de bots u operador de bots. Las botnets son el mecanismo más conocido para escalar los bots y su impacto.

branch

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte Acerca de las sucursales (GitHub documentación).

acceso de emergencia

En circunstancias excepcionales y mediante un proceso aprobado, es una forma rápida de que un usuario pueda acceder a un Cuenta de AWS sitio al que normalmente no tiene permisos de acceso. Para más información, consulte el indicador Implement break-glass procedures en la guía de AWS Well-Architected.

estrategia de implementación sobre infraestructura existente

La infraestructura existente en su entorno. Al adoptar una estrategia de implementación sobre infraestructura existente para una arquitectura de sistemas, se diseña la arquitectura en función de las limitaciones de los sistemas y la infraestructura actuales. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

caché de búfer

El área de memoria donde se almacenan los datos a los que se accede con más frecuencia.

capacidad empresarial

Lo que hace una empresa para generar valor (por ejemplo, ventas, servicio al cliente o marketing). Las arquitecturas de microservicios y las decisiones de desarrollo pueden estar impulsadas por las capacidades empresariales. Para obtener más información, consulte la sección Organizado en torno a las capacidades empresariales del documento técnico Ejecutar microservicios en contenedores en AWS.

planificación de la continuidad del negocio (BCP)

Plan que aborda el posible impacto de un evento disruptivo, como una migración a gran escala en las operaciones y permite a la empresa reanudar las operaciones rápidamente.

C

CAF

Consulte AWS Cloud Adoption Framework.

implementación canario

Lanzamiento lento e incremental de una versión para los usuarios finales. Cuando tenga mayor confianza en la nueva versión, la implementa y reemplaza la versión actual en su totalidad.

CCoE

Consulte Centro de excelencia en la nube.

CDC

Consulte captura de datos de cambios.

captura de datos de cambio (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Puede utilizar los CDC para diversos fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

ingeniería del caos

Introducción intencionada de fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

CI/CD

Consulte integración continua y entrega continua.

clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

cifrado del cliente

Cifrado de datos localmente, antes de que el objetivo los Servicio de AWS reciba.

Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las publicaciones de CCo E en el blog de estrategia Nube de AWS empresarial.

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar relacionada con la tecnología de computación de periferia.

modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte Creación de su modelo operativo de nube.

etapas de adopción de la nube

Las siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCo E, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinvención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la entrada del blog The Journey Toward Cloud-First & the Stages of Adoption en el blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte base de datos de administración de configuración.

repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Algunos repositorios en la nube comunes son GitHub o Bitbucket Cloud. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola canalización de CI/CD puede utilizar varios repositorios.

caché en frío

Una caché de búfer que está vacía no está bien poblada o contiene datos obsoletos o irrelevantes. Esto afecta al rendimiento, ya que la instancia de la base de datos debe leer desde la memoria principal o el disco, lo que es más lento que leer desde la memoria caché del búfer.

datos fríos

Datos a los que se accede con poca frecuencia y que suelen ser históricos. Al consultar este tipo de datos, normalmente se aceptan consultas lentas. Trasladar estos datos a niveles o clases de almacenamiento de menor rendimiento y menos costosos puede reducir los costos.

visión artificial (CV)

Campo de la IA que utiliza el machine learning para analizar y extraer información de formatos visuales, como imágenes y videos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

deriva de configuración

En el caso de una carga de trabajo, un cambio en la configuración con respecto al estado esperado. Podría provocar que la carga de trabajo deje de cumplir las normas y, por lo general, es gradual e involuntaria.

base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los datos de una CMDB se utilizan en la etapa de detección y análisis de la cartera de productos durante la migración.

paquete de conformidad

Un conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus controles de conformidad y seguridad. Puede implementar un paquete de conformidad como una entidad única en una región Cuenta de AWS y, o en una organización, mediante una plantilla YAML. Para obtener más información, consulta los paquetes de conformidad en la documentación. AWS Config

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD se describe comúnmente como una canalización. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar más rápido. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Consulte visión artificial.

D

datos en reposo

Datos que están estacionarios en la red, como los datos que se encuentran almacenados.

clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad

del AWS Well-Architected Framework. Para obtener más información, consulte Clasificación de datos.

deriva de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada a lo largo del tiempo. La deriva de datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

datos en tránsito

Datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red.

malla de datos

Marco de arquitectura que proporciona una propiedad de datos distribuida y descentralizada con una administración y una gobernanza centralizadas.

minimización de datos

El principio de recopilar y procesar solo los datos estrictamente necesarios. Practicar la minimización de los datos Nube de AWS puede reducir los riesgos de privacidad, los costos y la huella de carbono de la analítica.

perímetro de datos

Un conjunto de barreras preventivas en su AWS entorno que ayudan a garantizar que solo las identidades confiables accedan a los recursos confiables desde las redes esperadas. Para obtener más información, consulte Crear un perímetro de datos sobre. AWS

preprocesamiento de datos

Transformar los datos sin procesar en un formato que su modelo de ML pueda analizar fácilmente. El preprocesamiento de datos puede implicar eliminar determinadas columnas o filas y corregir los valores faltantes, incoherentes o duplicados.

procedencia de los datos

El proceso de rastrear el origen y el historial de los datos a lo largo de su ciclo de vida, por ejemplo, la forma en que se generaron, transmitieron y almacenaron los datos.

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

Sistema de administración de datos que respalda la inteligencia empresarial, como los análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para las consultas y los análisis.

lenguaje de definición de datos (DDL)

Instrucciones o comandos para crear o modificar la estructura de tablas y objetos de una base de datos.

lenguaje de manipulación de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

DDL

Consulte lenguaje de definición de bases de datos.

conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

defense-in-depth

Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la integridad y la disponibilidad de la red y de los datos que contiene. Al adoptar esta estrategia AWS, se añaden varios controles en diferentes capas de la AWS Organizations estructura para ayudar a proteger los recursos. Por ejemplo, un defense-in-depth enfoque podría combinar la autenticación multifactorial, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta

cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations .

Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

entorno de desarrollo

Consulte entorno.

control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte Controles de detección en Implementación de controles de seguridad en AWS.

asignación de flujos de valor para el desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSM amplía el proceso de asignación del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

tabla de dimensiones

En un esquema en estrella, tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos en una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se suelen utilizar para restringir consultas, filtrarlas y etiquetar los conjuntos de resultados.

desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

recuperación de desastres (DR)

Estrategia y proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos a causa de un desastre. Para obtener más información, consulte Recuperación ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Consulte lenguaje de manipulación de bases de datos.

diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Este concepto lo introdujo Eric Evans en su libro, Diseño impulsado por el dominio: abordando la complejidad en el corazón del software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

Detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración con línea de base. Por ejemplo, puedes usarlo AWS CloudFormation para detectar desviaciones en los recursos del sistema o puedes usarlo AWS Control Tower para detectar cambios en tu landing zone que puedan afectar al cumplimiento de los requisitos de gobierno.

DVSM

Consulte asignación de flujos de valor para el desarrollo.

E

EDA

Consulte análisis de datos de tipo exploratorio.

EDI

Consulte intercambio electrónico de datos.

computación en la periferia

La tecnología que aumenta la potencia de cálculo de los dispositivos inteligentes en la periferia de una red de IoT. En comparación con la computación en la nube, la computación de periferia puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

Intercambio automatizado de documentos comerciales entre organizaciones. Para más información, consulte ¿Qué es el intercambio electrónico de datos?

cifrado

Proceso de computación que transforma datos de texto plano, que son legibles por humanos, en texto cifrado.

clave de cifrado

Cadena criptográfica de bits aleatorios que se genera mediante un algoritmo de cifrado. Las claves pueden variar en longitud y cada una se ha diseñado para ser impredecible y única.

endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian almacenan primero el byte menos significativo.

punto de conexión

Consulte punto de conexión de servicio.

servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto final AWS PrivateLink y conceder permisos a otros Cuentas de AWS o a responsables AWS Identity and Access Management (de IAM). Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada

mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte Creación de un servicio de punto de conexión en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

planificación de recursos empresariales (ERP)

Sistema que automatiza y administra los procesos empresariales clave (como la contabilidad, MES y la administración de proyectos) de una empresa.

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte el cifrado de sobres en la documentación de AWS Key Management Service (AWS KMS).

entorno

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.
- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En un CI/CD proceso, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas AWS de seguridad de CAF incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

ERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para encontrar patrones, detectar anomalías y comprobar las suposiciones. El EDA se realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

F

tabla de hechos

Tabla central de un esquema en estrella. Almacena datos cuantitativos sobre operaciones empresariales. Por lo general, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

Fail Fast

Filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de los enfoques ágiles.

límite de aislamiento de errores

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para más información, consulte AWS Fault Isolation Boundaries.

rama de característica

Consulte rama.

características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, esto se expresa como una puntuación numérica que se puede calcular mediante diversas

técnicas, como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con. AWS

transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

peticiones con pocos pasos

Proporcionar a un LLM una pequeña cantidad de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que lleve a cabo una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, mediante el que los modelos aprenden a partir de ejemplos (pasos) incrustados en las peticiones. La técnica de peticiones con pocos pasos puede ser eficaz para las tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también peticiones desde cero.

FGAC

Consulte control de acceso detallado.

control de acceso preciso (FGAC)

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.

migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la captura de datos de cambio para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

FM

Consulte modelo fundacional.

Modelo fundacional (FM)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar una

amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para más información, consulte ¿Qué son los modelos fundacionales?

G

IA generativa

Subconjunto de modelos de IA que se entrenaron con grandes cantidades de datos y que pueden utilizar una simple petición de texto para crear contenido y artefactos nuevos, como imágenes, videos, texto y audio. Para más información, consulte ¿Qué es la IA generativa?

bloqueo geográfico

Consulte restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

En Amazon CloudFront, una opción para impedir que los usuarios de países específicos accedan a las distribuciones de contenido. Puede utilizar una lista de permitidos o bloqueados para especificar los países aprobados y prohibidos. Para obtener más información, consulta la sección Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, mientras que el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

imagen dorada

Instantánea de un sistema o software que se usa como plantilla para implementar nuevas instancias de ese sistema o software. Por ejemplo, en la fabricación, una imagen dorada se puede utilizar para aprovisionar software en varios dispositivos y ayuda a mejorar la velocidad, la escalabilidad y la productividad de las operaciones de fabricación de dispositivos.

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como implementación sobre infraestructura existente. Si está

ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y el cumplimiento en todas las unidades organizativas (OUs). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de permisos de IAM. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

HA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que utilice un motor de base de datos diferente (por ejemplo, de Oracle a Amazon Aurora). La migración heterogénea suele ser parte de un esfuerzo de rediseño de la arquitectura y convertir el esquema puede ser una tarea compleja. AWS ofrece AWS SCT, lo cual ayuda con las conversiones de esquemas.

alta disponibilidad (HA)

La capacidad de una carga de trabajo para funcionar de forma continua, sin intervención, en caso de desafíos o desastres. Los sistemas de alta disponibilidad están diseñados para realizar una conmutación por error automática, ofrecer un rendimiento de alta calidad de forma constante y gestionar diferentes cargas y fallos con un impacto mínimo en el rendimiento.

modernización histórica

Un enfoque utilizado para modernizar y actualizar los sistemas de tecnología operativa (TO) a fin de satisfacer mejor las necesidades de la industria manufacturera. Un histórico es un tipo de base de datos que se utiliza para recopilar y almacenar datos de diversas fuentes en una fábrica.

datos de reserva

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de machine learning. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo mediante la comparación de las predicciones del modelo con los datos de reserva.

migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS para SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, una revisión suele realizarse fuera del flujo de trabajo de DevOps publicación típico.

periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

I

IaC

Consulte infraestructura como código.

políticas basadas en identidades

Política asociada a uno o más directores de IAM que define sus permisos en el entorno. Nube de AWS

aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar o modificar la infraestructura existente o aplicarle revisiones. Las infraestructuras inmutables son de manera intrínseca más coherentes, fiables y predecibles que las infraestructuras mutables. Para más información, consulte la práctica recomendada Implementación mediante una infraestructura inmutable en el Marco de AWS Well-Architected.

VPC entrante (de entrada)

En una arquitectura de AWS cuentas múltiples, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

Industria 4.0

Término que introdujo Klaus Schwab en 2016 para referirse a la modernización de los procesos de fabricación mediante los avances en la conectividad, los datos en tiempo real, la automatización, el análisis, la IA y el ML.

infraestructura

Todos los recursos y activos que se encuentran en el entorno de una aplicación.

infraestructura como código (IaC)

Proceso de aprovisionamiento y administración de la infraestructura de una aplicación mediante un conjunto de archivos de configuración. La IaC se ha diseñado para ayudarlo a centralizar la administración de la infraestructura, estandarizar los recursos y escalar con rapidez a fin de que los entornos nuevos sean repetibles, fiables y consistentes.

Internet de las cosas industrial (T) IIo

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte Creación de una estrategia de transformación digital de la Internet de las cosas (IIoT) industrial.

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red VPCs entre Internet y las redes locales (en una misma o Regiones de AWS diferente). La arquitectura AWS de referencia de seguridad recomienda configurar su cuenta de red con entrada, salida e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte ¿Qué es IoT?.

interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con. AWS

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. La ITIL proporciona la base para la ITSM.

administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con las herramientas de ITSM, consulte la Guía de integración de operaciones.

ITIL

Consulte biblioteca de información de TI.

ITSM

Consulte administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

zona de aterrizaje

Una landing zone es un AWS entorno multicuenta bien diseñado, escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte Configuración de un entorno de AWS seguro y escalable con varias cuentas.

modelo de lenguaje de gran tamaño (LLM)

Modelo de IA de aprendizaje profundo que se entrenó previamente con una gran cantidad de datos. Un LLM puede llevar a cabo varias tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para obtener más información, consulte Qué son. LLMs

migración grande

Migración de 300 servidores o más.

LBAC

Consulte control de acceso basado en etiquetas.

privilegio mínimo

La práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.

migrar mediante lift-and-shift

Consulte Las 7 R.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Consulte también endianidad.

LLM

Consulte modelo de lenguaje de gran tamaño.

entornos inferiores

Consulte entorno.

M

machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte Machine learning.

rama principal

Consulte rama.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware podría interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso

no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los registradores de pulsaciones de teclas.

Servicios administrados

Servicios de AWS para lo cual AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y se accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios administrados. También se conocen como servicios abstractos.

sistema de ejecución de fabricación (MES)

Sistema de software para seguir, supervisar, documentar y controlar los procesos de producción que convierten las materias primas en productos acabados en la zona de producción.

MAP

Consulte Programa de aceleración de la migración.

mecanismo

Proceso completo mediante el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para hacer ajustes. Un mecanismo es un ciclo que se refuerza y mejora por sí mismo a medida que funciona. Para obtener más información, consulte Creación de mecanismos en el AWS Well-Architected Framework.

cuenta de miembro

Todas las Cuentas de AWS demás cuentas, excepto la de administración, que forman parte de una organización. AWS Organizations Una cuenta no puede pertenecer a más de una organización a la vez.

MES

Consulte sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (MQTT)

Un protocolo de comunicación ligero machine-to-machine (M2M), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.

microservicio

Un servicio pequeño e independiente que se comunica a través de una red bien definida APIs y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo,

un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte Integrar microservicios mediante AWS servicios sin servidor.

arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante un uso ligero. APIs Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte Implementación de microservicios en. AWS

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la estrategia de migración de AWS.

fábrica de migración

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen incluir a analistas y propietarios de operaciones, empresas, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan a pasos agigantados. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la discusión sobre las fábricas de migración y la Guía de fábricas de migración a la nube en este contenido.

metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son la subred de destino, el grupo de seguridad y AWS la cuenta.

patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: rehospede la migración a Amazon EC2 AWS con Application Migration Service.

Migration Portfolio Assessment (MPA)

Herramienta en línea que proporciona información a fin de validar los argumentos comerciales necesarios para migrar a la Nube de AWS. La MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores de los socios de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar sus puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas mediante el AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. La MRA es la primera fase de la estrategia de migración de AWS.

estrategia de migración

Enfoque utilizado para migrar una carga de trabajo a la Nube de AWS. Para más información, consulte la entrada Las 7 R de este glosario y también Mobilize your organization to accelerate large-scale migrations.

ML

Consulte machine learning.

modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia

y aprovechar las innovaciones. Para más información, consulte Strategy for modernizing applications in the Nube de AWS.

evaluación de la preparación para la modernización

Evaluación que ayuda a determinar la preparación para la modernización de las aplicaciones de una organización; identifica los beneficios, los riesgos y las dependencias; y determina qué tan bien la organización puede soportar el estado futuro de esas aplicaciones. El resultado de la evaluación es un esquema de la arquitectura objetivo, una hoja de ruta que detalla las fases de desarrollo y los hitos del proceso de modernización y un plan de acción para abordar las brechas identificadas. Para más información, consulte Evaluating modernization readiness for applications in the Nube de AWS.

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MPA

Consulte Migration Portfolio Assessment.

MQTT

Consulte Message Queuing Telemetry Transport.

clasificación multiclase

Un proceso que ayuda a generar predicciones para varias clases (predice uno de más de dos resultados). Por ejemplo, un modelo de ML podría preguntar “¿Este producto es un libro, un automóvil o un teléfono?” o “¿Qué categoría de productos es más interesante para este cliente?”.

infraestructura mutable

Modelo que actualiza y modifica la infraestructura actual para las cargas de trabajo de producción. Para mejorar la coherencia, la fiabilidad y la previsibilidad, el AWS Well-Architected Framework recomienda el uso de una infraestructura inmutable como práctica recomendada.

O

OAC

Consulte control de acceso de origen.

OAI

Consulte identidad de acceso de origen.

OCM

Consulte administración del cambio organizacional.

migración fuera de línea

Método de migración en el que la carga de trabajo de origen se elimina durante el proceso de migración. Este método implica un tiempo de inactividad prolongado y, por lo general, se utiliza para cargas de trabajo pequeñas y no críticas.

OI

Consulte integración de operaciones.

OLA

Consulte acuerdo de nivel operativo.

migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

Open Process Communications: arquitectura unificada (OPC-UA)

Un protocolo de machine-to-machine comunicación (M2M) para la automatización industrial. OPC-UA establece un estándar de interoperabilidad con esquemas de autenticación, autorización y cifrado de datos.

acuerdo de nivel operativo (OLA)

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse entre sí, para respaldar un acuerdo de nivel de servicio (SLA).

revisión de la preparación operativa (ORR)

Lista de comprobación de preguntas y prácticas recomendadas asociadas que son útiles para comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles errores. Para más información, consulte Operational Readiness Reviews (ORR) en el Marco de AWS Well-Architected.

tecnología operativa (TO)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En el sector de la fabricación, la integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

Proceso de modernización de las operaciones en la nube, que implica la planificación de la preparación, la automatización y la integración. Para obtener más información, consulte la Guía de integración de las operaciones.

registro de seguimiento organizativo

Un registro creado por y AWS CloudTrail que registra todos los eventos para todos los miembros Cuentas de AWS de una organización. AWS Organizations Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte Crear un registro para una organización en la CloudTrail documentación.

administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. La OCM ayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de personal, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la Guía de OCM.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas al bucket de S3.

identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando utiliza OAI, CloudFront crea un principal con el que Amazon S3 puede autenticarse. Los directores autenticados solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica. CloudFront Consulte también el OAC, que proporciona un control de acceso más detallado y mejorado.

ORR

Consulte revisión de la preparación operativa.

OT

Consulte tecnología operativa.

VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

P

límite de permisos

Una política de administración de IAM que se adjunta a las entidades principales de IAM para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte Límites de permisos en la documentación de IAM.

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos de información de identificación personal son los nombres, las direcciones y la información de contacto.

PII

Consulte información de identificación personal.

manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

PLC

Consulte controlador lógico programable.

PLM

Consulte administración del ciclo de vida del producto.

policy

Objeto que puede definir permisos (consulte política basada en identidad), especificar las condiciones de acceso (consulte política basada en recursos) o definir los permisos máximos para todas las cuentas de una organización de AWS Organizations (consulte política de control de servicio).

persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades.

evaluación de cartera

Proceso de detección, análisis y priorización de la cartera de aplicaciones para planificar la migración. Para obtener más información, consulte la Evaluación de la preparación para la migración.

predicate

Condición de consulta que devuelve `true` o `false`. En general, se encuentra en una cláusula `WHERE`.

inserción de predicados

Técnica de optimización de consultas en bases de datos que filtra los datos de la consulta antes de transferirlos. Esta técnica reduce la cantidad de datos de la base de datos relacional que se tienen que recuperar y procesar. Además, mejora el rendimiento de las consultas.

control preventivo

Un control de seguridad diseñado para evitar que ocurra un evento. Estos controles son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Para obtener más información, consulte Controles preventivos en Implementación de controles de seguridad en AWS.

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz para un Cuenta de AWS rol de IAM o un usuario. Para obtener más información, consulte Entidad principal en Términos y conceptos de roles en la documentación de IAM.

Privacidad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de desarrollo.

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o más VPCs. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Control de seguridad que se diseñó para evitar la implementación de recursos que no cumplan con la normativa. Estos controles analizan los recursos antes de aprovisionarlos. Si el recurso no cumple con los requisitos del control, no se aprovisiona. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en la sección Implementación de controles de seguridad en AWS.

administración del ciclo de vida del producto (PLM)

Administración de los datos y los procesos de un producto a lo largo de todo su ciclo de vida, desde el diseño, el desarrollo y el lanzamiento, pasando por el crecimiento y la madurez, hasta la reducción de su uso y su retirada.

entorno de producción

Consulte entorno.

controlador lógico programable (PLC)

En el sector de la fabricación, computadora adaptable y altamente fiable que supervisa las máquinas y automatiza los procesos de fabricación.

encadenamiento de peticiones

Uso de la salida de una petición de LLM como entrada para la siguiente petición a fin de generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en tareas secundarias o para refinar o ampliar de forma iterativa una respuesta preliminar. Ayuda a mejorar la precisión y la relevancia de las respuestas de un modelo y permite obtener resultados más detallados y personalizados.

seudonimización

El proceso de reemplazar los identificadores personales de un conjunto de datos por valores de marcadores de posición. La seudonimización puede ayudar a proteger la privacidad personal. Los datos seudonimizados siguen considerándose datos personales.

publish/subscribe (pub/sub)

Patrón que permite establecer comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un MES basado en microservicios, un microservicio puede publicar mensajes de eventos en un canal al que se pueden suscribir otros microservicios. El sistema puede agregar nuevos microservicios sin cambiar el servicio de publicación.

Q

plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos relacional SQL.

regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas,

restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

R

Matriz RACI

Consulte responsable, fiable, consultada e informada (RACI).

RAG

Consulte generación aumentada por recuperación.

ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

Matriz RASCI

Consulte responsable, fiable, consultada e informada (RACI).

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

Una copia de una base de datos que se utiliza con fines de solo lectura. Puede enrutar las consultas a la réplica de lectura para reducir la carga en la base de datos principal.

rediseñar

Consulte Las 7 R.

objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio.

refactorizar

Consulte Las 7 R.

Region

Conjunto de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para más información, consulte Specify which Regiones de AWS your account can use.

regresión

Una técnica de ML que predice un valor numérico. Por ejemplo, para resolver el problema de "¿A qué precio se venderá esta casa?", un modelo de ML podría utilizar un modelo de regresión lineal para predecir el precio de venta de una vivienda en función de datos conocidos sobre ella (por ejemplo, los metros cuadrados).

volver a alojar

Consulte Las 7 R.

versión

En un proceso de implementación, el acto de promover cambios en un entorno de producción.

reubicar

Consulte Las 7 R.

redefinir la plataforma

Consulte Las 7 R.

recomprar

Consulte Las 7 R.

resiliencia

Capacidad de una aplicación para resistir interrupciones o recuperarse de ellas. Al planificar la resiliencia en la Nube de AWS, la alta disponibilidad y la recuperación ante desastres son consideraciones comunes. Para más información, consulte Resiliencia en la Nube de AWS.

política basada en recursos

Una política asociada a un recurso, como un bucket de Amazon S3, un punto de conexión o una clave de cifrado. Este tipo de política especifica a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

matriz responsable, confiable, consultada e informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte Controles receptivos en Implementación de controles de seguridad en AWS.

retain

Consulte Las 7 R.

retirar

Consulte Las 7 R.

Generación aumentada de recuperación (RAG)

Tecnología de IA generativa mediante la que un LLM hace referencia a un origen de datos autorizado que se encuentra fuera de sus orígenes de datos de entrenamiento antes de generar una respuesta. Por ejemplo, un modelo de RAG podría hacer una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para más información, consulte ¿Qué es RAG (generación aumentada por recuperación)?

rotación

Proceso mediante el que periódicamente se actualiza un secreto para que resulte más difícil que un atacante pueda acceder a las credenciales.

control de acceso por filas y columnas (RCAC)

El uso de expresiones SQL básicas y flexibles que tienen reglas de acceso definidas. El RCAC consta de permisos de fila y máscaras de columnas.

RPO

Consulte objetivo de punto de recuperación.

RTO

Consulte objetivo de tiempo de recuperación.

manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

S

SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión Consola de administración de AWS o llamar a las operaciones de la AWS API sin tener que crear un usuario en IAM para todos los miembros de la organización. Para obtener más información sobre la federación basada en SAML 2.0, consulte Acerca de la federación basada en SAML 2.0 en la documentación de IAM.

SCADA

Consulte control de supervisión y adquisición de datos.

SCP

Consulte política de control de servicio.

secreta

En AWS Secrets Manager, información confidencial o restringida, como una contraseña o credenciales de usuario, que se almacena de forma cifrada. Se compone del valor del secreto y de sus metadatos. El valor del secreto puede ser binario, una sola cadena o varias cadenas. Para más información, consulte What's in a Secrets Manager secret? en la documentación de Secrets Manager.

seguridad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la seguridad durante todo el proceso de desarrollo.

control de seguridad

Barrera de protección técnica o administrativa que impide, detecta o reduce la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Existen cuatro tipos de controles de seguridad principales: preventivos, de detección, de respuesta y proactivos.

refuerzo de la seguridad

Proceso de reducir la superficie expuesta a ataques para hacerla más resistente a los ataques. Esto puede incluir acciones, como la eliminación de los recursos que ya no se necesitan, la implementación de prácticas recomendadas de seguridad consistente en conceder privilegios mínimos o la desactivación de características innecesarias en los archivos de configuración.

sistema de información sobre seguridad y administración de eventos (SIEM)

Herramientas y servicios que combinan sistemas de administración de información sobre seguridad (SIM) y de administración de eventos de seguridad (SEM). Un sistema de SIEM recopila, monitorea y analiza los datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

automatización de la respuesta de seguridad

Acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o corregirlo. Estas automatizaciones sirven como controles de seguridad preventivos o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. La modificación de un grupo de seguridad de VPC, la aplicación de revisiones a una instancia de Amazon EC2 o la rotación de credenciales son algunos ejemplos de acciones de respuesta automatizadas.

cifrado del servidor

Cifrado de los datos en su destino, por parte de Servicio de AWS quien los recibe.

política de control de servicio (SCP)

Política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPs defina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están permitidos o prohibidos. Para obtener más información, consulte las políticas de control de servicios en la AWS Organizations documentación.

punto de enlace de servicio

La URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte Puntos de conexión de Servicio de AWS en Referencia general de AWS.

acuerdo de nivel de servicio (SLA)

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

indicador de nivel de servicio (SLI)

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

objetivo de nivel de servicio (SLO)

Métrica objetivo que representa el estado de un servicio medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

Un modelo que describe la responsabilidad con AWS la que compartes la seguridad y el cumplimiento de la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el Modelo de responsabilidad compartida.

SIEM

Consulte sistema de administración de eventos e información de seguridad.

único punto de error (SPOF)

Error en un único componente crítico de una aplicación que puede interrumpir el sistema.

SLA

Consulte acuerdo de nivel de servicio.

SLI

Consulte indicador de nivel de servicio.

SLO

Consulte objetivo de nivel de servicio.

split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para

crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para más información, consulte Phased approach to modernizing applications in the Nube de AWS.

SPOF

Consulte único punto de error.

esquema en estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos de gran tamaño para almacenar datos transaccionales o medidos y una o varias tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para utilizarse en un almacén de datos o con fines de inteligencia empresarial.

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado. Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue presentado por Martin Fowler como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

Un intervalo de direcciones IP en la VPC. Una subred debe residir en una sola zona de disponibilidad.

control de supervisión y adquisición de datos (SCADA)

En el sector de la fabricación, sistema que utiliza hardware y software para supervisar los activos físicos y las operaciones de producción.

cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

pruebas sintéticas

Prueba de un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o supervisar el rendimiento. Puede usar Amazon CloudWatch Synthetics para crear estas pruebas.

petición del sistema

Técnica para proporcionar contexto, instrucciones o pautas a un LLM para dirigir su comportamiento. Las peticiones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

T

etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudar a administrar, identificar, organizar, buscar y filtrar recursos de . Para obtener más información, consulte Etiquetado de los recursos de AWS.

variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte entorno.

entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

puerta de enlace de tránsito

Un centro de tránsito de red que puede usar para interconectar sus redes con VPCs las locales. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración por usted. Para obtener más información, consulte AWS Organizations Utilización con otros AWS servicios en la AWS Organizations documentación.

ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

equipo de dos pizzas

Un DevOps equipo pequeño al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

U

incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos.

tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

entornos superiores

Consulte entorno.

V

succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

Emparejamiento de VPC

Una conexión entre dos VPCs que le permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte ¿Qué es una interconexión de VPC? en la documentación de Amazon VPC.

vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

W

caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

función de ventana

Función SQL que hace un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para las tareas de procesamiento, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

WORM

Consulte escritura única y lectura múltiple.

WQF

Consulte AWS Workload Qualification Framework.

escritura única y lectura múltiple (WORM)

Modelo de almacenamiento que escribe los datos una sola vez y evita que se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no los pueden cambiar. Esta infraestructura de almacenamiento de datos se considera inmutable.

Z

ataque de día cero

Ataque, normalmente de malware, que se aprovecha de una vulnerabilidad de día cero.

vulnerabilidad de día cero

Un defecto o una vulnerabilidad sin mitigación en un sistema de producción. Los agentes de amenazas pueden usar este tipo de vulnerabilidad para atacar el sistema. Los desarrolladores suelen darse cuenta de la vulnerabilidad a raíz del ataque.

peticiones desde cero

Proporcionar a un LLM instrucciones para llevar a cabo una tarea, pero sin ejemplos (pasos) que puedan ayudar a guiarlo. El LLM debe usar los conocimientos del entrenamiento previo para llevar a cabo la tarea. La eficacia de la petición desde cero depende de la complejidad de la tarea y de la calidad de la petición. Consulte también peticiones con pocos pasos.

aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.