

AWS Well-Architected Framework

# SAP Lens



# SAP Lens: AWS Well-Architected Framework

# Table of Contents

Información general .....	i
¿Cómo utilizar los enfoques? .....	1
Definiciones .....	3
Lista de verificación del contexto de la carga de trabajo .....	6
Principios de diseño de Well-Architected .....	7
Excelencia operativa .....	7
1. Diseñe la carga de trabajo de SAP para permitir la comprensión y la reacción a su estado .....	7
2. Reduzca los defectos, facilite la corrección y mejore el flujo de trabajo de cambio de SAP .....	22
3. Comprenda cómo operará la carga de trabajo .....	31
4. Valide y mejore su carga de trabajo de SAP con regularidad .....	38
Seguridad .....	46
5. Comprenda los estándares de seguridad y cómo se aplican a su carga de trabajo de SAP .....	47
6. Utilice controles de infraestructura y de software para reducir los errores de configuraciones de seguridad .....	53
7. Controle el acceso a sus cargas de trabajo de SAP a través de la identidad y los permisos .....	63
8. Proteja sus datos de SAP en reposo y en tránsito .....	72
9. Implemente una estrategia de seguridad para registrar, probar y responder a eventos de seguridad .....	79
Fiabilidad .....	83
10. Diseñe para tolerar errores .....	83
11. Detecte los errores y reaccione ante ellos .....	94
12. Haga un plan de recuperación de datos .....	106
Eficiencia de rendimiento .....	112
13. Seleccione la solución de computación óptima .....	113
14. Seleccione la solución de almacenamiento óptima .....	120
15. Evalúe las opciones de ajuste para el sistema operativo, la base de datos y la aplicación SAP .....	128
16. Comprenda las opciones de optimización y rendimiento en curso .....	136
Optimización de costos .....	143
17. Evalúe los patrones de arquitectura de SAP con un enfoque en la rentabilidad .....	143

18. Evalúe los recursos de computación de SAP para la eficiencia de costos .....	158
19. Optimice el uso de datos de SAP para la eficiencia de costos de almacenamiento .....	169
20. Administre los costos con visibilidad, planificación y administración .....	180
Conclusión .....	190
Colaboradores .....	191
Historial del documento .....	192
Principios de diseño por pilar .....	193
Excelencia operativa .....	193
Seguridad .....	193
Fiabilidad .....	193
Eficiencia de rendimiento .....	193
Optimización de costos .....	194
Avisos .....	195
AWS Glossary .....	196

# Información general

Fecha de publicación: 28 de octubre de 2021 ([Historial del documento](#))

En este documento, se describe SAP Lens para AWS Well-Architected Framework. Se trata de una colección de prácticas recomendadas y principios de diseño probados por el cliente para garantizar que las cargas de trabajo de SAP en AWS tengan una buena arquitectura. Utilice SAP Lens como complemento de [AWS Well-Architected Framework](#), el cual brinda las bases para crear aplicaciones y cargas de trabajo seguras, de alto rendimiento, resistentes y eficientes en AWS.

SAP Lens se basa en la información que AWS recopiló de clientes, socios de AWS y nuestra comunidad de especialistas de SAP. Este enfoque se diseñó para ayudarlo a adoptar un enfoque nativo en la nube para ejecutar SAP. En él, se destacan algunas de las áreas de mejoras más comunes, alineadas con los cinco pilares de AWS Well-Architected Framework: excelencia operativa, seguridad, fiabilidad, eficiencia del rendimiento y optimización de costos.

En este documento, nos referimos a SAP como el software que se ejecuta en AWS y que provee la empresa SAP, ampliamente conocida por sus aplicaciones de Enterprise Resource Planning (ERP, sistemas de planificación de recursos empresariales). El propósito de esta guía es examinar todo el software de SAP que se puede ejecutar en AWS, incluidos SAP Business Suite, SAP S/4HANA y los productos de soporte. Si alguna recomendación es específica para una aplicación o base de datos de SAP, se indicará (por ejemplo, base de datos de SAP HANA).

Este documento está dirigido a arquitectos de tecnología de SAP, arquitectos de la nube y miembros de equipos que crean, operan y mantienen sistemas SAP en AWS.

## ¿Cómo utilizar los enfoques?

Utilice este enfoque para evaluar las cargas de trabajo de SAP on AWS antes, durante y después de la implementación. Este enfoque brinda contenido adicional a AWS Well-Architected Framework y aclara cómo interpretar y adoptar las prácticas recomendadas fundamentales en los diseños de carga de trabajo de SAP.

Recomendamos usar este enfoque y el de AWS Well-Architected Framework en conjunto y trabajar en estrecha relación con sus equipos empresariales para tratar los requisitos de SAP y de su empresa. Para evitar la duplicación, hemos compartido enlaces a AWS Well-Architected Framework, donde se le proporciona una guía más completa o en un contexto que no es específico para SAP.

Para utilizar este enfoque, siga estos pasos:

1. Familiarícese con este documento y con el más amplio AWS Well-Architected Framework y los documentos técnicos sobre sus pilares.
2. Reúna la documentación de diseño, los procedimientos operativos y el historial de supervisión específicos de SAP (si están disponibles).
3. Compare la implementación y las operaciones de su carga de trabajo de SAP con las prácticas recomendadas descritas en este documento.
4. Consulte cada práctica recomendada, registre si se siguió y priorice la evaluación de aquellas que lo requieren.
5. Utilice las sugerencias proporcionadas como soluciones para tratar las áreas donde su carga de trabajo no presenta una buena arquitectura.

Si necesita orientación adicional de expertos, comuníquese con el equipo de cuentas de AWS para trabajar con un arquitecto de soluciones especializado en SAP.

Después de revisar su carga de trabajo, se le presentará una lista de prácticas recomendadas en la que se indica en qué aspectos la carga de trabajo posee una buena arquitectura y en cuales hace falta una mejora:

- Si hay componentes arquitectónicos que presentan una buena arquitectura, comparta su conocimiento con sus equipos para extenderlos a toda su organización.
- Si su carga de trabajo aún no sigue ciertas prácticas recomendadas, trátelas como riesgos y deudas técnicas para su empresa. Siga su proceso interno de administración de riesgos para supervisar y reducir continuamente estos riesgos.
- En el caso de las áreas que requieren un análisis más profundo o asistencia para solucionar estos problemas, comuníquese con los servicios profesionales de AWS o consulte a los socios de AWS que figuran en la [Lista de socios certificados por SAP de AWS](#).

Para obtener más detalles, consulte los siguientes enlaces y la siguiente información:

- Documentación de AWS: [Proceso de revisión: AWS Well-Architected Framework](#)

# Definiciones

Término	Descripción	Ejemplos (si corresponde)
Carga de trabajo de SAP	Una carga de trabajo es una colección de recursos de SAP con valor empresarial. En el contexto de SAP, esto comprende los componentes orientados al cliente de las aplicaciones SAP, así como los procesos de backend de SAP. Una carga de trabajo puede consistir en un subconjunto de recursos en una sola cuenta de AWS o puede tratarse de una colección de recursos que abarca varias cuentas de AWS.	
Producto de SAP	Un producto de SAP, la empresa de software empresarial que brinda soluciones para los procesos empresariales en todos los sectores. A veces denominado Soluciones de SAP .	SAP S/4HANA Edición en las instalaciones, Concur, Qualtrics
Sistema SAP	Grupo lógico de arquitectura (un conjunto de elementos que funcionan juntos como parte de un mecanismo mayor) que normalmente se identifica con un SAP System Identifier (SID, identificador del sistema SAP).	Sistema de ERP de producción
Identificador del sistema SAP (SAP SID / DB SID)	Una combinación de letras y números que se utiliza para identificar de forma única un sistema SAP.	PRD, HDB, PR1
Entorno de SAP	Grupo de uno o más productos de SAP o componentes tecnológicos. Están vinculados para formar un camino hacia la producción.	Entorno aislado, desarroll

Término	Descripción	Ejemplos (si corresponde)
		o, control de calidad, entrenamiento, prueba, preproducción y producción.
Instancia o host de SAP	Una instancia es una copia de una Amazon Machine Image (AMI, imagen de máquina de Amazon) que se ejecuta como un servidor virtual en la nube de AWS. En el contexto de SAP, se trata generalmente de una instancia de computación en el servicio de Amazon EC2.	
Componente técnico de SAP	Unidades administrativas que agrupan componentes de un sistema SAP que se ejecuta en una instancia o host. Son componentes básicos de arquitectura técnica de aplicaciones SAP.	Servidor de la aplicación (PAS o AAS), Base de datos SAP HANA, Web Dispatcher



Término	Descripción	Ejemplos (si corresponde)
Servicios (servicios de AWS)	Más de 200 servicios en la nube que se utilizan en combinaciones personalizadas para las necesidades empresariales u organizativas. Para obtener más información sobre muchos servicios de AWS, consulte el documento técnico Información general sobre Amazon Web Services.	Amazon EC2, Simple Storage Service (Amazon S3), Amazon EFS
Implementación de SAP / Patrón de implementación	Se utiliza para describir cómo se implementa SAP en lo que respecta a las opciones de las herramientas de aprovisionamiento de SAP (SUM, SWPM).	Altamente disponible (HA), distribuido, independiente
Calificación de SAPS (denominada "SAPS" en varias ubicaciones)	<p>El SAP Application Performance Standard (SAPS, estándar de rendimiento de la aplicación SAP) es una unidad de medida independiente del hardware que describe el rendimiento de la configuración de un sistema en un entorno de SAP. Se obtiene del punto de referencia de Sales and Distribution (SD, ventas y distribución), donde 100 SAPS equivale a 2000 elementos de la línea de pedidos procesados comercialmente en su totalidad por hora.</p> <p>Para obtener más información, consulte <a href="#">Puntos de partida de la Aplicación estándar de SAP</a>.</p>	Tipo de Instancia de Amazon EC2 <i>c5.large</i> proporciona 3650 SAPS.

Documentación de AWS: [Glosario de AWS](#)

# Lista de verificación del contexto de la carga de trabajo

Para comprender mejor el contexto de su empresa, necesita recopilar la siguiente información.

ID	Prioridad	Contexto de la carga de trabajo
<input type="checkbox"/> C1	Obligatorio	Nombre de la carga de trabajo
<input type="checkbox"/> C2	Obligatorio	Descripción que contiene los objetivos empresariales, los indicadores clave de rendimiento (KPIs) y los usuarios a los que está destinada la carga de trabajo.
<input type="checkbox"/> C3	Obligatorio	Propietario de la revisión que dirige la revisión del enfoque
<input type="checkbox"/> C4	Obligatorio	Propietario de la carga de trabajo que es responsable de mantener la carga de trabajo
<input type="checkbox"/> C5	Obligatorio	Partes interesadas empresariales que patrocinan la carga de trabajo
<input type="checkbox"/> C6	Obligatorio	Socios empresariales que tienen participación en la carga de trabajo, como socios legales, financieros y de seguridad de la información
<input type="checkbox"/> C7	Recomendado	Documento del diseño de la arquitectura que describe la carga de trabajo
<input type="checkbox"/> C8	Recomendado	ID de cuentas de AWS asociados con la carga de trabajo
<input type="checkbox"/> C9	Recomendado	Requisitos de cumplimiento normativo pertinentes para la carga de trabajo (si corresponde)

# Principios de diseño de Well-Architected

En esta sección, se describen los principios de diseño, las prácticas recomendadas y las sugerencias de mejoras que son pertinentes a la hora de diseñar y operar una carga de trabajo de SAP.

Recomendamos también que lea y aplique las guías que corresponden a cada pilar de Well-Architected, en las que se incluyen las prácticas recomendadas fundamentales para la excelencia operativa, la seguridad, la fiabilidad, la eficiencia del rendimiento y la optimización de costos, pilares que conciernen a todas las cargas de trabajo.

## Pilares

- [Excelencia operativa](#)
- [Seguridad](#)
- [Fiabilidad](#)
- [Eficiencia de rendimiento](#)
- [Optimización de costos](#)

Para obtener una lista completa de los principios de diseño, consulte [Principios de diseño organizados por pilar](#).

## Excelencia operativa

El pilar de la excelencia operativa se centra en la capacidad para desarrollar y ejecutar cargas de trabajo de forma eficaz, obtener información acerca de las operaciones y mejorar continuamente los procesos de soporte para ofrecer valor empresarial.

En esta sección, se proporciona un conjunto de recomendaciones y principios de diseño ideados específicamente para brindar orientación sobre las cargas de trabajo de SAP. Con el [pilar de la excelencia operativa](#) se ponen de manifiesto principios y recomendaciones generales de diseño que recomendamos que lea junto con la guía de SAP que sigue a continuación.

### 1. Diseñe la carga de trabajo de SAP para permitir la comprensión y la reacción a su estado

¿Cómo diseñar su carga de trabajo de SAP de manera tal que pueda comprender su estado?  
Diseñe su carga de trabajo de SAP de manera tal que brinde la información necesaria en todos los

componentes y así pueda comprender su estado interno y externo. Considere la infraestructura, la base o tecnología de SAP, el front end y los componentes de red. Diseñe enfoques de supervisión y registro que obtengan métricas para permitir la supervisión en tiempo real, así como registros históricos para permitir la corrección y el análisis posterior al evento.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 1.1	Obligatorio	Implemente los requisitos previos para la supervisión de SAP on AWS
<input type="checkbox"/> Práctica recomendada 1.2	Obligatorio	Implementar la supervisión de infraestructura para SAP
<input type="checkbox"/> Práctica recomendada 1.3	Obligatorio	Implementar la supervisión de aplicaciones individuales para SAP
<input type="checkbox"/> Práctica recomendada 1.4	Altamente recomendado	Implemente la supervisión de la configuración de la carga de trabajo
<input type="checkbox"/> Práctica recomendada 1.5	Altamente recomendado	Implementar la supervisión de la actividad del usuario
<input type="checkbox"/> Práctica recomendada 1.6	Altamente recomendado	Implementar la supervisión de dependencias

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 1.7	Recomendado	Implementar una supervisión de estado de panel de vidrio único en todas sus cargas de trabajo de SAP
<input type="checkbox"/> Práctica recomendada 1.8	Recomendado	Utilizar técnicas de respuesta y recuperación automatizadas para reaccionar a las alertas de supervisión

Para obtener más detalles, consulte los siguientes enlaces y la siguiente información:

- Documentación de AWS: [AWS Data Provider for SAP \(Proveedor de datos de AWS para SAP\)](#)
- Servicio de AWS: [Amazon CloudWatch](#)
- Blog de SAP on AWS: [Serverless Monitoring for SAP \(Supervisión sin servidor para SAP\)](#)
- Blog de SAP on AWS: [AWS DevOps for SAP - driving innovation and lowering costs \(DevOps en AWS para SAP: impulsar la renovación y reducir los costos\)](#)
- AWS Marketplace: [Productos y herramientas para la supervisión de SAP](#)
- Notas de SAP: [1656250 - SAP on AWS: Support Prerequisites \(SAP on AWS: prerequisites de soporte\)](#) [Se necesita acceso al portal de SAP]
- Documentación de SAP: [SAP Solution Manager 7.2 - Application Operations \(SAP Solution Manager 7.2: Operaciones de aplicaciones\)](#)

## Práctica recomendada 1.1: implemente los requisitos previos para la supervisión de SAP on AWS

Los requisitos de certificación de SAP para SAP on AWS se definen en la nota de SAP 1656250. En esta nota, se incluyen las instrucciones para configurar el proveedor de datos de AWS para SAP, habilitar la supervisión detallada de Amazon CloudWatch y utilizar la supervisión mejorada de SAP para las soluciones de SAP NetWeaver. Habilitar estos requisitos previos ayuda a garantizar que AWS y SAP puedan comprender e investigar completamente el estado de su carga de trabajo de SAP. Estos requisitos previos deben incorporarse a su estrategia general de supervisión de SAP.

### Sugerencia 1.1.1: verifique los requisitos previos de soporte de SAP

Verifique la nota de SAP 1656250 en el portal de soporte de SAP para conocer los requisitos de soporte más actualizados para las cargas de trabajo de SAP on AWS. Siga las instrucciones detalladas en esta nota.

- Notas de SAP: [1656250 - SAP on AWS: Support Prerequisites](#) [Se necesita acceso al portal de SAP]

### Sugerencia 1.1.2: instale el proveedor de datos de AWS para cargas de trabajo en SAP NetWeaver.

Es obligatorio instalar el proveedor de datos de AWS para SAP en cada una de sus instancias de EC2 que admiten cargas de trabajo de SAP NetWeaver. El proveedor de datos de AWS para SAP es un agente que recopila métricas relacionadas con el rendimiento de los servicios de AWS y las brinda al sistema de supervisión de aplicaciones interno de SAP. Las herramientas de SAP, como el código de transacción ST06n y la supervisión de Solution Manager, que utilizan métricas externas generalmente recopiladas del servicio SAPOSCOL, requieren que el proveedor de datos de AWS para SAP acceda a las métricas de AWS.

Existen costos indirectos asociados con la ejecución del proveedor de datos de AWS para SAP debido a la supervisión detallada y el aumento de las llamadas a la API que se necesitan para que SAP reciba datos de supervisión en intervalos específicos. Consulte [Installing the AWS Data Provider for SAP \(Instalación del proveedor de datos de AWS para SAP\)](#) para obtener más detalles. Por esta razón, quizá debería considerar únicamente habilitar el proveedor de datos de AWS para SAP en infraestructuras que no sean de producción cuando se requiera soporte y análisis de SAP.

- Documentación de AWS: [AWS Data Provider for SAP \(Proveedor de datos de AWS para SAP\)](#)

### Sugerencia 1.1.3: cree una estrategia de supervisión para sus cargas de trabajo de SAP

Decida cómo observará el estado actual e histórico de su aplicación SAP tanto desde una perspectiva de adentro hacia afuera como de una de afuera hacia adentro. Considere todos los componentes que trabajan juntos para brindar la experiencia del usuario final. Considere cómo obtendrá las métricas de los servicios subyacentes de computación, almacenamiento y redes de AWS, así como las métricas internas de la aplicación SAP, y cómo supervisará la fiabilidad y el rendimiento de los usuarios externos. Evalúe diferentes herramientas para cada componente y decida cómo puede reunir las en un solo lugar (por ejemplo, mediante el agregado de registros) para realizar análisis de causa raíz cuando sea necesario. Determine cómo utilizará esta información

para designar umbrales de alertas y medidas de corrección que se tomarán cuando se superen los umbrales.

Comprenda las capacidades de la supervisión de SAP Solution Manager, de las herramientas de supervisión de terceros y de los paneles de CloudWatch que puedan procesar métricas de supervisión de SAP personalizadas como punto de inicio para su diseño.

- Documentación de AWS: [SAP NetWeaver en AWS: Monitoring Guide \(Guía de supervisión\)](#)
- Blog de SAP on AWS: [Serverless Monitoring for SAP NetWeaver \(Supervisión sin servidor para SAP NetWeaver\)](#)
- Blog de SAP on AWS: [Serverless Monitoring for SAP HANA \(Supervisión sin servidor para SAP HANA\)](#)
- Video del servicio de AWS: [Gaining Better Observability of Your VMs with Amazon CloudWatch \(Obtención de una mejor observabilidad de sus máquinas virtuales con Amazon CloudWatch\)](#)
- AWS Marketplace: [Productos y herramientas para la supervisión de SAP](#)
- Documentación de SAP: [SAP Solution Manager 7.2 - Application Operations \(SAP Solution Manager 7.2: Operaciones de aplicaciones\)](#)
- Documentación de SAP: [SAP NetWeaver Alert Monitor \(Monitor de alertas de SAP NetWeaver\)](#)

## Práctica recomendada 1.2: implemente la supervisión de infraestructura para SAP

Configure la supervisión de su infraestructura para brindar información sobre los servicios de soporte que se utilizan para mantener su aplicación SAP en ejecución y brindar soporte a sus usuarios. Entre algunos ejemplos, se incluye la utilización de la CPU y la memoria, el uso del almacenamiento y del sistema de archivos y el rendimiento (IOPS y rendimiento) y el rendimiento de la red. Incluya todos los servicios básicos dependientes que utiliza SAP, como servicios de Active Directory en las instalaciones, DNS y herramientas de terceros, como software de alta disponibilidad (HA) y de copia de seguridad. Evalúe las herramientas de AWS y las herramientas específicas de SAP que se encuentran en AWS Marketplace que pueden ayudar a correlacionar y visualizar esta información, como DataDog, Splunk, DynaTrace y Avantra. Utilice esta información para identificar tendencias y determinar cuándo se requiere una acción de corrección.

Sugerencia 1.2.1: implemente las métricas y alarmas de CloudWatch para los servicios compatibles con SAP

Implemente métricas y umbrales de supervisión detallados de Amazon CloudWatch con alarmas para todos sus sistemas SAP. Estas métricas y alarmas deben incluir la supervisión de problemas

comunes que pueden afectar la disponibilidad y el rendimiento del sistema SAP. Las áreas comunes de supervisión de infraestructura se enfocan en instancias de Amazon Elastic Compute Cloud (EC2), volúmenes de Amazon Elastic Block Storage (Amazon EBS) y Elastic Load Balancing (ELB).

A continuación, se incluyen algunos elementos comunes de supervisión:

- Uso elevado de la CPU de Amazon EC2
- Uso elevado de la memoria de Amazon EC2
- Paginación de almacenamiento de Amazon EBS
- Rendimiento de almacenamiento de Amazon EBS
- IOPS de almacenamiento de Amazon EBS
- Porcentaje de espacio de almacenamiento libre y de volúmenes llenos de Amazon EBS
- Saturación de la red de Amazon EC2
- Estado del grupo objetivo y estado de ELB/ALB

Fije los umbrales de las alarmas con base en patrones saludables de utilización productiva histórica de su sistema. Revise y modifique continuamente los umbrales de su alarma para prevenir problemas.

Revise los siguientes recursos para comenzar:

- Blog de SAP on AWS: [Serverless Monitoring for SAP NetWeaver \(Supervisión sin servidor para SAP NetWeaver\)](#)
- Blog de SAP on AWS: [Serverless Monitoring for SAP HANA \(Supervisión sin servidor para SAP HANA\)](#)
- Documentación de AWS: [Creación de una métrica personalizada de CloudWatch](#)
- Documentación de AWS: [Creación de un panel de CloudWatch](#)
- Documentación de AWS: [Uso de las alarmas de Amazon CloudWatch](#)

Sugerencia 1.2.2: implemente la supervisión de cuotas de servicios de AWS para los servicios de SAP

Implemente una herramienta o proceso de supervisión para realizar seguimiento de [sus cuotas de servicio de AWS](#) para los recursos de SAP requeridos en su infraestructura. Tenga en cuenta que las infraestructuras SAP con frecuencia pueden usar una combinación de tipos de instancias de Amazon



EC2 y que esos tipos tienen una cuota [de servicio bajo demanda diferente](#) . Por ejemplo, los tipos de instancia de EC2 x1\* y u\* tienen una cuota de servicio diferente que es independiente de la cuota combinada para los tipos de instancias c5 , m5 y r5 . Al planificar cargas de trabajo nuevas o escalar cargas de trabajo existentes, asegúrese de que sus cuotas de servicio serán compatibles con dichas cargas de trabajo y comuníquese con AWS Support si necesita un aumento de la cuota.

- Documentación de AWS: [Referencia general de AWS: cuotas de servicio](#)
- Documentación de AWS: [Instancias bajo demanda: cuotas de servicio de Amazon Elastic Compute Cloud \(EC2\)](#)
- Documentación de AWS: [Requesting a quota increase - Service Quotas \(Solicitud de un aumento de cuotas: Service Quotas\)](#)

## Práctica Recomendada 1.3: implemente la supervisión de aplicaciones individuales para SAP

Configure la supervisión de su aplicación y base de datos de manera tal que pueda obtener información sobre su estado general e interno, y del logro de los resultados empresariales. Entre algunos ejemplos, se incluye el tiempo de respuesta de la transacción, los procesos de trabajo disponibles, la profundidad de la cola, los mensajes de error y volcado, los trabajos por lotes estancados y el rendimiento de la transacción. Utilice esta información para determinar cuándo se requiere una acción correctiva.

### Sugerencia 1.3.1: implemente la supervisión de bases de datos que admiten aplicaciones SAP

Supervise continuamente sus bases de datos de SAP y establezca alertas para problemas comunes que pueden afectar la disponibilidad y el rendimiento del sistema SAP. A continuación, se incluyen algunos elementos comunes de supervisión:

- Espacio libre en el área de datos
- Espacio libre en el área de registro
- Actividad de bloqueo excesiva
- Tasas de utilización de caché
- Tiempo de respuesta promedio a la consulta
- Parches de seguridad y correcciones urgentes requeridos
- Tamaños máximos de las tablas y crecimiento

Fije los umbrales de las alarmas con base en patrones saludables de utilización productiva histórica de su sistema. Revise y ajuste continuamente los límites de sus alarmas para prevenir problemas y reaccionar ante los cambios o el crecimiento de la carga de trabajo.

Para obtener más detalles sobre cómo habilitar la supervisión de su base de datos específica, consulte las guías de instalación y operación de su proveedor de software de base de datos.

Sugerencia 1.3.2: utilice transacciones y herramientas de SAP para comprender la aplicación SAP

Configure sus aplicaciones SAP de manera tal que estas puedan brindar información sobre su estado general e interno, y del logro de los resultados empresariales. Utilice esta información para determinar cuándo se necesita una respuesta. A continuación, se incluyen algunos elementos comunes de supervisión:

- Disponibilidad de los servicios de la aplicación (ASCS, PAS, AAS) y de la base de datos
- Número de usuarios activos y concurrentes
- Disponibilidad de procesos de trabajo para los usuarios
- Tiempo de respuesta de las transacciones de los usuarios
- Tiempo de respuesta de transacciones por lote y no interactivas
- Mensajes de error y volcado
- Trabajos fallidos
- Colas completas y lentas

Configure el [SAP EarlyWatch Alert reporting system \(Sistema de informes de SAP EarlyWatch Alert\)](#) en SAP Solution Manager para crear informes periódicos sobre el estado de sus sistemas SAP. Revise y solucione regularmente los problemas que se encuentran en estos informes para prevenir problemas y evitar interrupciones en el servicio de la carga de trabajo.

- Notas de SAP: [2729186 - General Process of EWA Generation \(Proceso general de generación de EWA\)](#) [Se necesita acceso al portal de SAP]
- Documentación de SAP: [SAP Solution Manager 7.2 - Application Operations \(SAP Solution Manager 7.2: Operaciones de aplicaciones\)](#)
- SAP Lens [eficiencia de rendimiento]: [Práctica recomendada 16.1: cuente con datos para evaluar el rendimiento](#)

Sugerencia 1.3.3: implemente la supervisión de sus mecanismos de recuperación y protección de datos

Implemente la supervisión de mecanismos que protejan sus datos de SAP en caso de error o desastre. A continuación, se incluyen algunos elementos comunes de supervisión:

- Alertas de creación de copias de seguridad periódicas de base de datos, por ejemplo, en Simple Storage Service (Amazon S3) con AWS Backup Agent
- Alertas sobre la replicación de la base de datos, por ejemplo, errores o retrasos que se producen al replicar el sistema HANA en las Availability Zones (AZ, zonas de disponibilidad)
- Alertas de creación de copias de seguridad de almacenamiento de archivos, por ejemplo, una instantánea de EBS, una copia de seguridad de Amazon EFS o una copia de seguridad de Amazon FSx
- Alertas de mecanismos de recuperación que brindan resiliencia de datos entre regiones, por ejemplo, buckets de Amazon S3 con replicación entre regiones, sincronización de Simple Storage Service (Amazon S3) o CloudEndure Disaster Recovery
- Alertas de cualquier mecanismo de recuperación que brinde resiliencia de datos en las cuentas, por ejemplo, los buckets de Amazon S3 con replicación de la misma región en un bucket de S3 WORM o cuenta de registro

Consulte los siguientes enlaces para obtener más información:

- Blog de AWS: [Monitor, Evaluate, and Demonstrate Backup Compliance with AWS Backup Audit Manager \(Supervise, evalúe y demuestre la conformidad de la copia de seguridad con AWS Backup Audit Manager\)](#)
- Documentación de SAP: [SAP HANA System Replication Verification and Monitoring \(Supervisión y verificación de la replicación del sistema SAP HANA\)](#)

Sugerencia 1.3.4: exponga los datos de supervisión de SAP al exterior de las herramientas de SAP para lograr una observabilidad independiente

Las herramientas de supervisión de SAP se limitan a la supervisión al nivel de la aplicación y del sistema operativo y no cubren la amplia gama de servicios de soporte que brindan una visión integral de la disponibilidad y el estado del servicio de SAP. Configure sus aplicaciones SAP para aportar métricas a una herramienta de visualización y supervisión externa de su preferencia que sea más completa.

Utilice las métricas recopiladas en las prácticas recomendadas anteriores y externalice estos resultados, de modo que tenga una herramienta independiente que pueda supervisar, alertar e informar sobre tendencias. Una herramienta independiente permite la observabilidad, el análisis de la causa raíz, los informes históricos y de tendencias sin estar asociada a la disponibilidad del sistema SAP (es decir, sin importar que SAP esté en modo de desastres o de fallas).

- Blog de SAP on AWS: [Serverless Monitoring for SAP NetWeaver \(Supervisión sin servidor para SAP NetWeaver\)](#)
- Blog de SAP on AWS: [Serverless Monitoring for SAP HANA \(Supervisión sin servidor para SAP HANA\)](#)
- Documentación de AWS: [Creación de una métrica personalizada de CloudWatch](#)
- AWS Marketplace: [Productos y herramientas para la supervisión de SAP](#)

## Práctica recomendada 1.4: implemente la supervisión de la configuración de la carga de trabajo

Diseñe y configure su carga de trabajo para brindar información sobre su configuración actual y sobre los cambios en dicha configuración. Entre algunos de los ejemplos, se incluyen instancias de EC2 nuevas o eliminadas, eventos de escalado, cambio de códigos, niveles de parche, configuración de grupos de seguridad y eliminación de recursos. Utilice esta información para determinar cuándo se requiere una respuesta y para decidir si se esperaba o permitía un cambio. Supervise las implicaciones de costos de los cambios de configuración y ajuste o analice los presupuestos si es necesario.

### Sugerencia 1.4.1: implemente la supervisión de la configuración de la carga de trabajo

Establezca y configure AWS CloudTrail para supervisar eventos críticos y de alta prioridad, especialmente en sus cuentas de producción de SAP. Entre algunos ejemplos de eventos, se incluyen nuevas instancias de Amazon EC2, desmantelamientos de instancias de Amazon EC2 o cambios en ellas, cambios en grupos de seguridad y eventos de cambio en la seguridad de AWS KMS y AWS IAM. Utilice estos eventos para configurar las alarmas de registro de CloudWatch (si es necesario) y tomar medidas en caso de que se produzca un cambio inesperado.

- Documentación de AWS: [¿Qué es AWS CloudTrail?](#)
- Servicio de AWS: [AWS CloudTrail](#)
- Documentación de AWS: [Monitoreo de archivos de registros de CloudTrail con Amazon CloudWatch Logs](#)

- Documentación de AWS: [Prácticas de seguridad recomendadas para AWS CloudTrail](#)

Sugerencia 1.4.2: implemente la aplicación de configuraciones a las cargas de trabajo y su corrección

Inicie y configure AWS Config para rastrear, evaluar y aplicar la política de configuración de los recursos de AWS compatibles con sus aplicaciones de producción de SAP. Entre algunos ejemplos comunes, se incluyen aplicar protección de solo lectura en buckets de S3 que contienen copias de seguridad de SAP, cifrar de forma obligatoria volúmenes de EBS de Amazon EC2, bloquear puertos de red comunes y verificar que todos los recursos tengan las etiquetas requeridas. Utilice las reglas administradas [de AWS Config](#) para mejorar la seguridad y cambiar la posición de control de su entorno de AWS compatible con SAP. Utilice etiquetas de AWS para implementar las reglas de configuración y aplicar la corrección automatizada donde sea posible.

- Servicio de AWS: [AWS Config](#)
- Documentación de AWS: [Introducción a AWS Config](#)
- Documentación de AWS: [Uso de reglas de AWS Config](#)
- Blog de SAP on AWS: [Audit your SAP systems with AWS Config – Part I \(Auditar sus sistemas SAP con AWS Config: parte I\)](#)
- Blog de SAP on AWS: [Audit your SAP systems with AWS Config – Part II \(Auditar sus sistemas SAP con AWS Config: parte II\)](#)
- Blog de SAP on AWS: [Tagging Recommendations for SAP on AWS \(Recomendaciones de etiquetado para SAP on AWS\)](#)

Sugerencia 1.4.3: implemente la supervisión de los costos de las cargas de trabajo

Instale y configure [AWS Budgets](#) con presupuestos personalizados que lo alerten cuando supera (o se prevé que supere) sus límites de facturación. Adapte sus presupuestos al gasto proyectado de su entorno de SAP y supervise cualquier anomalía a fin de prevenir costos excesivos. Supervise su uso y cobertura de instancias reservadas y Savings Plans mediante el uso de informes de presupuesto. Utilice etiquetas de AWS que lo ayuden a comprender la asignación de costos y el uso en su carga de trabajo de SAP.

- Blog de AWS: [Introducción a AWS Budgets](#)
- Blog de AWS: [AWS Budgets Reports \(Informes de AWS Budgets\)](#)
- Documentación de AWS: [AWS Cost Explorer](#)

- Documentación de AWS: [Detección de anomalías de costos de AWS](#)
- Blog de SAP on AWS: [Tagging Recommendations for SAP on AWS](#)

## Práctica recomendada 1.5: implemente la supervisión de la actividad del usuario

Configure sus aplicaciones SAP para brindar información sobre la actividad del usuario, por ejemplo, el tiempo de respuesta, la cantidad de usuarios activos, las tasas de abandono de transacciones y el tiempo de procesamiento de pedidos. Considere los enfoques de adentro hacia afuera (supervisar el tiempo de respuesta del diálogo interno de SAP) y los enfoques de afuera hacia adentro (implementar agentes o robots en las ubicaciones geográficas del usuario final) para comprender cómo repercute la conectividad en la experiencia. Utilice esta información para comprender cómo se usa la aplicación y los patrones de uso, y para determinar cuándo se requiere una respuesta debido a un rendimiento deficiente.

Sugerencia 1.5.1: implemente la supervisión de la experiencia del usuario desde las ubicaciones del usuario final

Considere enfoques de supervisión de afuera hacia adentro mediante la implementación de agentes de usuarios o robots en las ubicaciones geográficas de los usuarios finales para comprender cómo la red y la conectividad repercuten en la experiencia del usuario de SAP. Con frecuencia, este tipo de supervisión basada en la ubicación del usuario final puede brindar información y alertas tempranas de problemas que no se detectan en la infraestructura y las aplicaciones centrales.

Implemente herramientas de SAP o de terceros que brinden informes de la experiencia del usuario final para medir la capacidad de respuesta de su aplicación SAP desde las ubicaciones de los usuarios finales. Por ejemplo, SAP brinda supervisión de la experiencia del usuario final en Solution Manager, y múltiples productos de terceros permiten la implementación de robots (o scripts de supervisión) en ubicaciones remotas para medir la experiencia del usuario.

- Documentación de SAP: [SAP User Experience Monitoring \(Supervisión de la experiencia del usuario de SAP\)](#)
- AWS Marketplace: [Productos y herramientas para la supervisión de SAP](#)

## Práctica recomendada 1.6: implemente la supervisión de las dependencias

Configure su carga de trabajo para brindar información sobre el estado (por ejemplo, accesibilidad o tiempo de respuesta) de los recursos de los que depende. Entre algunos ejemplos de dependencias externas, se pueden encontrar interfaces (por ejemplo, SAP PI/PO), almacenes de datos externos,

DNS, componentes en las instalaciones, controladores de Active Directory y dispositivos de red. Utilice esta información para determinar cuándo se necesita una respuesta. Considere herramientas de supervisión de terceros que puedan brindar métricas de tecnologías cruzadas para supervisar el estado de las dependencias de un extremo a otro.

Sugerencia 1.6.1: implemente el seguimiento de estado de sus interfaces claves de SAP y de los procesos empresariales de sistemas cruzados.

Identifique y supervise las interfaces clave de las que depende su carga de trabajo de SAP. Supervise el estado de los puntos de conexión de estas interfaces, los errores, la longitud de la cola y las tasas de éxito. Utilice mecanismos previamente incorporados en SAP o herramientas de integración de terceros para configurar alertas de errores o retrasos en la interfaz e incorpórelas en sus herramientas de supervisión. Considere todas las rutas de la interfaz:

- Entre diferentes sistemas SAP alojados en AWS (a través de RFC o servicio web/HTTPS)
- Entre sistemas SAP alojados en AWS y sistemas en las instalaciones (HTTPS/SFTP: a través de SAP PI o una plataforma de integración de terceros)
- Entre sistemas SAP alojados en AWS y SAP Business Technology Platform (a través de SAP Cloud Connector)
- Entre sistemas SAP alojados en AWS y sistemas de partes externas (normalmente mediante HTTPS a través de Internet/VPN)

Considere utilizar Solution Manager Business Process Monitoring para la supervisión de dependencias en sistemas cruzados en toda su infraestructura SAP, así como en infraestructuras no vinculadas a SAP.

- Documentación de SAP: [SAP Business Process and Interface Monitoring \(Supervisión de interfaces y procesos empresariales de SAP\)](#)
- AWS Marketplace: [Productos y herramientas para la supervisión de SAP](#)

Sugerencia 1.6.2: implemente el seguimiento del estado de los servicios empresariales de los que depende SAP

Una carga de trabajo de SAP generalmente depende de varios servicios empresariales fundamentales para estar en buen estado para los usuarios empresariales. Considere utilizar estos servicios fundamentales en sus herramientas y enfoques de supervisión. Entre algunos ejemplos de servicios fundamentales, se incluyen Direct Connect para la conectividad del sistema en las



instalaciones, Active Directory para la autenticación o el Single Sign-On (SSO, inicio de sesión único), Network Time Protocol (NTP, protocolo de tiempo de red) para la sincronización de la hora y los servicios de antivirus y conectividad a un repositorio de parches del sistema operativo (por ejemplo, Microsoft Windows Update o SUSE parches).

- Blog de AWS: [Amazon CloudWatch Agent with AWS Systems Manager integration - unified metrics and log collection for Linux and Windows \(Amazon CloudWatch Agent con integración de AWS Systems Manager: métricas unificadas y recopilación de registros para Linux y Windows\)](#)
- Documentación de AWS: [Recopilación de métricas y registros de instancias de Amazon EC2 y en los servidores de las instalaciones con el agente de CloudWatch.](#)
- Documentación de AWS: [Capacidades de supervisión mejoradas para AWS Direct Connect](#)

## Práctica recomendada 1.7: implemente una supervisión de estado de panel de vidrio único en todas sus cargas de trabajo de SAP

Configure sus aplicaciones SAP, servicios de AWS y cualquier componente dependiente para brindar información sobre el flujo de transacciones en la carga de trabajo. Combine métricas de varios orígenes para crear una visualización de panel de vidrio único para el estado de su carga de trabajo de SAP y haga que este panel sea accesible para sus usuarios clave. Utilice esta información para determinar cuándo se requiere una respuesta y para ayudarlo a identificar rápidamente los factores que dan origen a un problema que afecta a su empresa.

Sugerencia 1.7.1: combine las métricas de la aplicación, la configuración de la carga de trabajo, las métricas del usuario y el estado de las dependencias en una sola ubicación.

Combine métricas de supervisión de aplicaciones, datos de configuración de cargas de trabajo, métricas sobre los usuarios e información sobre el estado de las dependencias en una sola ubicación o herramienta para realizar una supervisión integral tanto de su carga de trabajo de SAP como del estado de esta que esté orientada a los procesos empresariales para los usuarios finales. Esto se puede lograr a través del uso de SAP Solution Manager, paneles y métricas personalizados de CloudWatch o herramientas de supervisión de terceros.

La práctica recomendada es crear paneles de estado internos de la empresa que muestren tendencias o informes de estado categorizados con un sistema de visualización de semáforo que permitan una vista desglosada de la disponibilidad de la carga de trabajo. Una vista desglosada permite a los usuarios y operadores evaluar el componente específico de la pila tecnológica que podría estar causando problemas o bajo rendimiento.



- Documentación de AWS: [Creación de un panel de CloudWatch](#)
- Blog de SAP on AWS: [Serverless Monitoring for SAP NetWeaver \(Supervisión sin servidor para SAP NetWeaver\)](#)
- Blog de SAP on AWS: [Serverless Monitoring for SAP HANA \(Supervisión sin servidor para SAP HANA\)](#)
- AWS Marketplace: [Productos y herramientas para la supervisión de SAP](#)
- Documentación de SAP: [SAP Solution Manager 7.2 - Application Operations \(SAP Solution Manager 7.2: Operaciones de aplicaciones\)](#)

Práctica recomendada 1.8: utilice técnicas de respuesta y recuperación automatizadas para reaccionar a las alertas de supervisión

Automatice las respuestas a eventos para reducir los errores ocasionados por los procesos manuales, así como para garantizar las respuestas rápidas y coherentes.

Sugerencia 1.8.1: utilice servicios de automatización para automatizar sus respuestas a eventos

Hay varias formas de automatizar la ejecución de actividades de corrección cuando sus herramientas de supervisión desencadenan eventos. Generalmente, debería buscar encauzar todos los eventos de su aplicación y base de datos de SAP a través de un solo canal en el que pueda brindar respuestas automáticas en función de eventos.

Para responder ante un evento originado por el cambio de estado en sus recursos de AWS o ante eventos personalizados de SAP, puede crear [reglas de EventBridge](#) para invocar acciones en los destinos de los eventos ([por ejemplo](#) (por ejemplo, funciones de Lambda, temas de Amazon Simple Notification Service (Amazon SNS), tareas de Amazon ECS y AWS Systems Manager Automation). La automatización de AWS Systems Manager se puede utilizar para llamar el comando `sapcontrol` y realizar tareas del sistema SAP automáticamente.

Para responder a una métrica que supera un umbral de un recurso (por ejemplo, tiempo de espera), debe crear [Alarmas de CloudWatch](#) para realizar una o más acciones mediante [Acciones de Amazon EC2](#) , [acciones de Auto Scaling](#) o enviar una notificación a un [Tema Amazon SNS](#) .

Si necesita realizar acciones personalizadas en respuesta a una alarma, invoque Lambda a través de una notificación de Amazon SNS o AWS Systems Manager Automation (por ejemplo, utilizando la acción `aws:runCommand` ) consulte [Blog de AWS: Automate Start or Stop of Distributed SAP HANA systems using AWS Systems Manager \(Automatice el inicio o detención de los sistemas SAP HANA distribuidos mediante AWS Systems Manager\)](#). .

Utilice Amazon SNS para publicar notificaciones de eventos y mensajes de escalamiento a fin de mantener informadas a las personas.

AWS también admite sistemas de terceros a través de las API y los SDK del servicio de AWS. Existen una serie de herramientas de supervisión proporcionadas por socios de AWS y terceros que permiten la supervisión, las notificaciones y las respuestas. Entre algunas de estas herramientas, se incluyen New Relic, Splunk, Loggly, SumoLogic y Datadog.

Considere enviar eventos e interacciones a herramientas ITIL de terceros cuando sea necesario para su organización, como [la integración de AWS con ServiceNow](#).

Los procedimientos manuales esenciales deben mantenerse siempre a disposición de los usuarios en caso de que los procedimientos automatizados fallen.

## 2. Reduzca los defectos, facilite la corrección y mejore el flujo de trabajo de cambio de SAP

¿Cómo reduce los defectos, facilita la corrección y mejora el flujo en la producción? Adopte enfoques que mejoren el flujo de cambios que se integran en producción, lo que permitirá la refactorización, la retroalimentación rápida sobre la calidad y la corrección de errores. Estos enfoques aceleran los cambios beneficiosos que se aplican a la fase de producción, limitan los problemas implementados y permiten una rápida identificación y solución de los problemas que acarrearán las actividades de implementación.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomenda da 2.1	Obligatorio	Utilice el control de versiones y la administración de configuración
<input type="checkbox"/> Práctica recomenda da 2.2	Obligatorio	Implemente prácticas para mejorar la calidad del código
<input type="checkbox"/> Práctica	Obligatorio	Utilizar sistemas de administración de implementaciones y creaciones

ID	Prioridad	Práctica recomendada
recomendada 2.3		
<input type="checkbox"/> Práctica recomendada 2.4	Obligatorio	Utilizar varios entornos
<input type="checkbox"/> Práctica recomendada 2.5	Obligatorio	Probar y validar los cambios
<input type="checkbox"/> Práctica recomendada 2.6	Altamente recomendado	Realice cambios pequeños, reversibles y frecuentes
<input type="checkbox"/> Práctica recomendada 2.7	Recomendado	Automatice las pruebas, la integración y la implementación de cambios

Para obtener más detalles, consulte los siguientes enlaces y la siguiente información:

- Video de AWS: [Design with Ops in Mind \(Diseñar con las operaciones en mente\)](#)
- Documentación de AWS: [Herramientas para desarrolladores de AWS](#)
- Documentación de AWS: [AWS Launch Wizard para SAP](#)
- Blog de SAP on AWS: [DevOps for SAP – Driving Innovation and Lowering Costs](#)

## Práctica recomendada 2.1: utilice el control de versiones y la administración de configuración

Los sistemas de administración de configuraciones reducen los errores causados por los procesos manuales y el nivel de esfuerzo necesario para implementar cambios. De esta manera, se puede

rastrear cambios, implementar nuevas versiones, detectar cambios en versiones existentes y revertir a versiones anteriores (por ejemplo, restaurar a un estado correcto conocido en caso de error). Integre las capacidades de control de versiones de sus sistemas de administración de configuraciones en todos sus procedimientos de SAP: infraestructura, base de datos, aplicación y código y desarrollos personalizados de SAP (por ejemplo, ABAP, Java y UI5/JavaScript).

Considere los diferentes sistemas de control de versiones para cada tipo de configuración, pero consolide las métricas en una herramienta de planificación de lanzamiento central. Analice cómo se administran la configuración no transportable y el control de versiones de archivos binarios en sus entornos (por ejemplo, ¿cómo sabe que las versiones de kernel de SAP son las mismas en toda su infraestructura?)

Sugerencia 2.1.1: implemente el control de cambios de SAP u otras herramientas de terceros para administrar el control de versiones y el código de desarrollo de SAP.

Asegúrese de implementar controles de cambios para todos los enfoques de desarrollo y para el código personalizado que sean compatibles con sus aplicaciones SAP: ABAP, Java, UI5/JavaScript y cualquier otra extensión o área de scripting. Piense en todas sus aplicaciones SAP y en cómo orquestará las implementaciones de código entre los múltiples patrones de implementación de SAP (por ejemplo, cómo lanzará de manera simultánea implementaciones relacionadas entre sí alojadas en AWS y en SAP Business Technology Platform).

- Servicio de AWS: [AWS CodeCommit](#)
- Video de AWS: [Introduction to AWS CodeCommit \(Introducción a AWS CodeCommit\)](#)
- Blog de SAP on AWS: [AWS DevOps tools for SAP, Part 1: Cloud Foundry \(Herramientas de DevOps de AWS para SAP, parte 1: Cloud Foundry\)](#)
- Blog de SAP on AWS: [AWS DevOps tools for SAP, Part 2: SAP Fiori Apps \(Herramientas de DevOps de AWS para SAP, parte 2: SAP Fiori Apps\)](#)
- Documentación de SAP: [SAP Change Control Management \(Administración de control de cambios de SAP\)](#)
- Documentación de SAP: [Best Practices for SAP BTP - Lifecycle Management \(Prácticas recomendadas para SAP BTP: administración del ciclo de vida\)](#)

Sugerencia 2.1.2: implemente sistemas de administración de la configuración para sus aplicaciones SAP

Implemente herramientas de administración de configuraciones para ABAP, Java y otras tecnologías de SAP, y considere cómo se administran la configuración no transportable y el control de versiones binario en su infraestructura (por ejemplo, ¿cómo sabe que sus versiones de SAP Kernel son las mismas en todo su entorno?) Utilice SAP Solution Manager para planificar e implementar los cambios de configuración y de versión en sus aplicaciones SAP.

- Documentación de SAP: [Enhanced Change & Transport System \(CTS+\) \(Mejoras en el sistema de cambio y transporte \[CTS+\]\)](#)
- Documentación de SAP: [SAP Solution Manager: Planning Landscape Changes \(SAP Solution Manager: planificación de cambios del panorama\)](#)

Sugerencia 2.1.3: implemente sistemas de administración de configuraciones para sistemas operativos

Recurra a la generación de una AML o utilice software de administración de configuraciones previamente establecido, como Ansible, Chef o Puppet, para alinear la administración de la configuración entre sus sistemas operativos de carga de trabajo de SAP. Considere utilizar herramientas de administración de configuraciones centradas en la seguridad que emitan alertas ante vulnerabilidades y que lo insten a mantener sus sistemas operativos revisados y fortalecidos.

- Documentación de AWS: [AWS Systems Manager State Manager](#)
- Documentación de AWS: [Administración de la configuración en Amazon EC2](#)
- Documentación de AWS: [¿Qué es AWS OpsWorks?](#)
- Documentación de AWS: [¿Qué es Amazon Inspector?](#)

Sugerencia 2.1.4: implemente sistemas de administración de la configuración para sus bases de datos

Trabaje con su proveedor de software de base de datos para comprender los enfoques de administración de configuraciones para su base de datos.

- Documentación de SAP: [SAP HANA Platform Lifecycle Management \(Administración del ciclo de vida de la plataforma SAP HANA\)](#)

Sugerencia 2.1.5: implemente sistemas de administración de la configuración de la infraestructura

Emplee enfoques de infraestructura como código (IaC) para aprovisionar y administrar recursos de AWS compatibles con sus cargas de trabajo de SAP. AWS CloudFormation y AWS Cloud Development Kit son herramientas que puede usar para aprovisionar y administrar la configuración en recursos de AWS de manera programada. Considere usar herramientas de auditoría y control de configuración que le permitan crear reglas y políticas para evaluar su infraestructura de manera periódica y así dar un diagnóstico sobre la conformidad y solucionar cualquier problema.

- Documentación de AWS: [AWS Launch Wizard para SAP](#)
- Documentación de AWS: [AWS Systems Manager Inventory](#)
- Documentación de AWS: [Administrador de cambios de AWS Systems Manager](#)
- Blog de SAP on AWS: [Infrastructure as Code Example: Terraform and SAP on AWS \(Ejemplo de infraestructura como código: Terraform y SAP on AWS\)](#)
- SAP Lens [fiabilidad]: [Práctica recomendada 11.3: defina un enfoque para restaurar la disponibilidad del servicio](#)

## Práctica recomendada 2.2: implemente prácticas para mejorar la calidad del código

Implemente prácticas para mejorar la calidad del código y minimizar los defectos. Por ejemplo, el desarrollo basado en pruebas, las revisiones de códigos y la adopción de estándares. Utilice lo mínimo posible las herramientas de SAP Code Inspector.

### Sugerencia 2.2.1: implemente prácticas para mejorar la calidad del código

Por ejemplo, el desarrollo basado en pruebas, la programación en pares, las revisiones de códigos y la adopción de estándares.

Sugerencia 2.2.2: utilice herramientas de Amazon Inspector para el desarrollo de SAP e integre este proceso en sus canalizaciones de entrega e integración continuas (CI/CD)

Considere las siguientes herramientas para la inspección y depuración automatizadas de códigos en sus cargas de trabajo de SAP:

- Documentación de AWS: [Amazon CodeGuru para el desarrollo en Java y Python en AWS](#)
- Documentación de SAP: [SAP Code Inspector for ABAP and SAP-specific development \(SAP Code Inspector para el desarrollo específico en ABAP y SAP\)](#)

## Práctica recomendada 2.3: utilice sistemas de administración de implementaciones y creaciones

Utilice sistemas de administración de implementaciones y creaciones. Asegúrese de usar sistemas de implementación y creación certificados por SAP, como el Change and Transport System (CTS, sistema de cambio y transporte) de ABAP, Web IDE o herramientas de SAP. Estos sistemas reducen los errores causados por los procesos manuales y reducen el nivel de esfuerzo necesario para implementar cambios.

### Sugerencia 2.3.1: implemente sistemas de creación y desarrollo de SAP

Implemente sistemas de creación e implementación certificados por SAP, como Change and Transport System (CTS, sistema de cambio y transporte) de ABAP, Web IDE o el servicio de entrega continua de BTP de SAP u otras herramientas de SAP.

- Video de AWS: [Continuous integration best practices for software development \(Prácticas recomendadas de integración continua para el desarrollo de software\)](#)
- Blog de SAP on AWS: [AWS DevOps tools for SAP, Part 2: SAP Fiori Apps \(Herramientas de DevOps de AWS para SAP, parte 2: SAP Fiori Apps\)](#)
- Documentación de SAP: [Enhanced Change & Transport System \(CTS+\)](#)
- Documentación de SAP: [Deploying Applications to BTP \(Implementación de aplicaciones en BTP\)](#)

## Práctica recomendada 2.4: utilice varios entornos

Utilice varios entornos de SAP para experimentar, desarrollar y probar la carga de trabajo. Utilice niveles de control en crecimiento a medida que los entornos se acercan a la producción con el fin de adquirir confianza en que las cargas de trabajo funcionarán como se previó al momento de la implementación. Por lo general, en las infraestructuras SAP, se emplea como mínimo un entorno de tres niveles. Cada uno de ellos destinados al desarrollo, la realización de pruebas y la producción respectivamente.

### Sugerencia 2.4.1: utilice entornos temporales para experimentar

Ponga a disposición de los equipos de desarrollo y de pruebas de tecnología entornos aislados o temporales con controles mínimos para permitir la experimentación y la mitigación de riesgos.

- Documentación de AWS: [AWS Launch Wizard para SAP](#)
- Blog de SAP on AWS: [Infrastructure as Code Example: Terraform and SAP on AWS](#)

Sugerencia 2.4.2: proporcione entornos de desarrollo para permitir el trabajo en paralelo y mejorar la agilidad

Habilite entornos que no sean de producción para permitir el trabajo en paralelo, lo que aumentará la agilidad del desarrollo y de las pruebas. Implemente controles más rigurosos en los entornos de producción para permitirles a los desarrolladores contar con los medios necesarios para innovar. Por lo general, en los entornos de SAP se emplea como mínimo un entorno de tres niveles. Cada uno de ellos destinados al desarrollo, la realización de pruebas y la producción respectivamente.

- Documentación de AWS: [AWS Launch Wizard para SAP](#)

Sugerencia 2.4.3: habilite un entorno de prueba consolidado que se asemeje lo máximo posible a un entorno producción a fin de mejorar la calidad de los lanzamientos

Los entornos provisionales y de prueba deben ser lo más parecidos posible a los de producción en lo que respecta a las características de sus interfaces y a su seguridad, resiliencia y rendimiento a fin de poder identificar problemas de arquitectura e interacción de códigos antes del lanzamiento. Considere desactivar los recursos secundarios en clústeres o hacer una reducción (tanto horizontal como vertical) del rendimiento del servidor de aplicaciones de este entorno cuando no lo use a fin de mejorar la eficiencia de costos de la infraestructura.

- Blog de SAP on AWS: [Automate Start or Stop of Distributed SAP HANA systems using AWS Systems Manager](#)

Sugerencia 2.4.4: utilice los sistemas de infraestructura como código (IaC) y administración de la configuración para implementar entornos de forma coherente

Utilice infraestructura como código (IaC) y sistemas de administración de configuración para implementar entornos que estén configurados según los controles presentes en producción con el fin de garantizar que los sistemas funcionen como se previó al momento de implementarlos. Utilice grupos de etiquetado y de recursos para etiquetar y mejorar los metadatos de los entornos, de manera que se puedan usar con fines de automatización y conformidad.

- Blog de SAP on AWS: [Infrastructure as Code Example: Terraform and SAP on AWS](#)
- Blog de SAP on AWS: [Tagging Recommendations for SAP on AWS](#)
- Documentación de AWS: [AWS Launch Wizard para SAP](#)
- Documentación de AWS: [¿Qué son los AWS Resource Groups?](#)



Sugerencia 2.4.5: apague los entornos que no sean de producción cuando no se utilicen

Cuando los entornos no estén en uso, apáguelos para evitar costos asociados con recursos inactivos (por ejemplo, sistemas de desarrollo durante la noche o los fines de semana).

- Blog de SAP on AWS: [Automate Start or Stop of Distributed SAP HANA systems using AWS Systems Manager](#)

## Práctica recomendada 2.5: pruebe y valide los cambios

Se deben probar los cambios y se deben validar los resultados en todas las etapas del ciclo de vida (por ejemplo, desarrollo, prueba y producción). Utilice los resultados de las pruebas para confirmar nuevas características y mitigar los riesgos y el impacto de implementaciones fallidas. Automatice las pruebas y la validación para garantizar la coherencia de la revisión, a fin de reducir los errores causados por procesos manuales y, también, reducir el nivel de esfuerzo necesario.

Sugerencia 2.5.1: se deben probar los cambios y validar los resultados en todas las etapas del ciclo de vida (por ejemplo, desarrollo, prueba y producción)

Sugerencia 2.5.2: mantenga un estándar de referencia de los resultados de las pruebas en las pruebas funcionales, el rendimiento y la resiliencia que sirva como base de comparación cuando realice cambios y en proyectos importantes.

Sugerencia 2.5.3: comprenda cuál es el grado en que debe someter a pruebas los diferentes niveles de cambio. Por ejemplo, una gama completa de pruebas frente a pruebas de regresión destinadas a cambios menores. Convenga las definiciones de las pruebas y el alcance de las pruebas de cambios que se requieren para hacer lanzamientos a producción.

Sugerencia 2.5.4: automatice la realización de pruebas cuando sea posible con herramientas de terceros y arneses de pruebas. Céntrese primero en cambios que sean de tipo regular y en lanzamientos frecuentes.

## Práctica recomendada 2.6: realice cambios frecuentes, pequeños y reversibles

Los cambios frecuentes, pequeños y reversibles reducen el alcance y el impacto de un cambio. Si bien muchas soluciones de SAP NetWeaver solo admiten un enfoque de “revisiones hacia futuro”, considere usar alternadores de características en el desarrollo personalizado para permitir reversiones. Esto facilita la resolución de problemas, permite correcciones más rápidas y proporciona la opción de restaurar los cambios.

Sugerencia 2.6.1: divida el desarrollo y los lanzamientos en cambios frecuentes y más pequeños cuando sea posible

Sugerencia 2.6.2: dado que muchas soluciones de SAP solo admiten un enfoque de “revisiones hacia futuro” (y no permiten transportes reversibles), considere usar alternadores de características en el desarrollo personalizado para permitir la desactivación de características en lugar de las reversiones o retiros

Sugerencia 2.6.3: para cambios de SAP que no sean reversibles, considere opciones de reversión adicionales, como instantáneas del sistema completo, copias de seguridad de la base de datos y opciones de restauración.

- Documentación de AWS: [Instantáneas coherentes ante bloqueos de Amazon EBS](#)
- Documentación de AWS: [AWS Backint for SAP HANA \(AWS Backint para SAP HANA\)](#)

Práctica recomendada 2.7: automatice las pruebas, la integración y la implementación de cambios

Automatice la creación, implementación y prueba de la carga de trabajo. Esto reduce los errores causados por los procesos manuales y reduce el esfuerzo necesario para implementar los cambios.

Sugerencia 2.7.1: automatice completamente la canalización de implementación e integración del código de registro mediante la compilación, realización de pruebas, implementación y validación

Sugerencia 2.7.2: implemente SAP Solution Manager ChaRM, Focused Build o herramientas de administración de cambios y lanzamiento de terceros para orquestar la creación integral de canalizaciones de implementación para cambios en la aplicación

- Documentación de SAP: [SAP Solution Manager Change Request Management \(Administración de solicitud de cambios de SAP Solution Manager\)](#)
- Documentación de SAP: [SAP Focused Build](#)
- AWS Marketplace: [Productos y herramientas para DevOps](#)
- AWS Marketplace: [Productos y herramientas para pruebas](#)
- Blog de SAP on AWS: [AWS DevOps tools for SAP, Part 1: Cloud Foundry](#)

### 3. Comprenda cómo operará la carga de trabajo

¿Cómo sabe que está listo para dar respaldo y operar una carga de trabajo? Evalúe la disposición operativa de su [carga de trabajo](#), procesos y procedimientos y personal con el fin de comprender los riesgos operativos asociados a su [carga de trabajo](#). Cree manuales de procedimientos para operaciones comunes y manuales de estrategias ante problemas, y automatice tantas operaciones como sea posible para mejorar la resiliencia y reducir errores.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomenda da 3.1	Obligatorio	Garantizar la capacidad del personal
<input type="checkbox"/> Práctica recomenda da 3.2	Obligatorio	Asegúrese de que su modelo de operación en la nube coincida con sus problemas operativos
<input type="checkbox"/> Práctica recomenda da 3.3	Obligatorio	Comparta los estándares de diseño y capacite al nuevo personal de soporte en los procedimientos
<input type="checkbox"/> Práctica recomenda da 3.4	Obligatorio	Utilice manuales de procedimientos para realizar operaciones de la infraestructura SAP
<input type="checkbox"/> Práctica recomenda da 3.5	Obligatorio	Utilice los manuales de estrategias para investigar los problemas
<input type="checkbox"/> Práctica	Altamente recomendado	Utilice la automatización para realizar operaciones de la infraestructura SAP

ID	Prioridad	Práctica recomendada
recomendada 3.6		

Para obtener más detalles, consulte los siguientes enlaces y la siguiente información:

- Documento técnico de AWS: [AWS Cloud Operating Model](#)
- Servicio de AWS: [AWS Config](#)
- Documentación de AWS: [Características de AWS Systems Manager](#)
- Blog de SAP on AWS: [DevOps for SAP – Driving Innovation and Lowering Costs](#)

### Práctica recomendada 3.1: garantice la capacidad del personal

Cuente con un mecanismo para confirmar que dispone de la cantidad apropiada de personal capacitado para ofrecer respaldo práctico a las necesidades operativas y que dicho personal cuenta con las certificaciones adecuadas de SAP, AWS o de terceros. Entrene a su personal y ajuste su capacidad según sea necesario a fin de mantener un respaldo eficaz.

Sugerencia 3.1.1: evalúe las necesidades de aprendizaje y certificación de su equipo de operaciones de SAP

Según su entorno y dependencias, pueden aplicar diferentes certificaciones. Evalúe las necesidades de certificación de su equipo para poder respaldar su pila tecnológica:

- Documentación de AWS: [Formación de AWS](#)
- Documentación de AWS: [Certificaciones de AWS](#)
- Certificaciones de sistema operativo
  - Documentación de SUSE: [Certificaciones de SUSE Enterprise Linux](#)
  - Documentación de Red Hat: [Certificaciones de Red Hat Enterprise Linux](#)
  - Documentación de Microsoft: [Certificaciones de Microsoft Windows](#)

## Práctica recomendada 3.2: asegúrese de que su modelo de operación en la nube coincida con sus problemas operativos

Identifique cuál es el modelo de operación en la nube adecuado para sus cargas de trabajo de SAP, de manera que este se alinee con los requisitos comerciales que ha identificado en cuanto a la velocidad de implementación, la seguridad, las operaciones y la responsabilidad de la asistencia de la plataforma en la nube. Es esencial contar con un modelo adecuado de operación en la nube para adoptar con éxito la nube y aprovechar una mayor agilidad empresarial.

Sugerencia 3.2.1: adopte el modelo adecuado de operación en la nube para sus objetivos empresariales

En función de sus requisitos empresariales y de TI, asegúrese de adoptar el modelo adecuado de operación en la nube. Decida qué equipos crearán y operarán su carga de trabajo. Planifique pasarse a un modelo de propiedad compartida en el que el equipo de tecnología de SAP y de SAP Basis y el equipo de desarrollo creen y ejecuten su carga de trabajo de SAP a través de un modelo de DevOps.

- Guía de AWS: [Modernización de las operaciones en Nube de AWS](#)
- Documento técnico de AWS: [Creación del modelo operativo en la nube](#)
- Video de AWS: [Modelos de operación en la nube para una transformación acelerada](#)

## Práctica recomendada 3.3: comparta los estándares de diseño y capacite al nuevo personal de soporte en los procedimientos

Comparta las prácticas recomendadas existentes, los estándares de diseño, las listas de verificaciones, los procedimientos operativos y los requisitos de gobernanza con los equipos. Asegúrese de que todos los equipos estén al tanto de los procedimientos de respaldo de todos los componentes de su carga de trabajo de SAP.

Sugerencia 3.3.1: comparta las prácticas recomendadas existentes, los estándares de diseño, las listas de verificación, los procedimientos operativos y los requisitos de guía y gobernanza entre todos los equipos para reducir la complejidad y maximizar los beneficios de los esfuerzos de desarrollo

Sugerencia 3.3.2: asegúrese de que existan procedimientos para solicitar cambios e incorporaciones en los estándares de diseño y excepciones a estos a fin de favorecer la mejora e innovación continuas

Sugerencia 3.3.3: asegúrese de que los equipos conozcan el contenido publicado para poder aprovecharlo y limitar la repetición del trabajo y el esfuerzo desperdiciado

Sugerencia 3.3.4: asegúrese de que los equipos sepan cómo registrar llamadas de asistencia para diferentes componentes de su carga de trabajo de SAP

¿Quién proporciona asistencia técnica a su sistema operativo, base de datos y aplicación SAP? Por ejemplo, averigüe si AWS o su proveedor de sistemas operativos brinda asistencia directamente por problemas con clústeres o revisiones. En el caso de las licencias de sistemas operativos incluidos en EC2, AWS proporciona asistencia directamente.

- Documentación de AWS: [Cómo registrar un caso con AWS Support](#)
- Documentación de AWS: [AWS Support](#)
- Notas de SAP: [1656250 - SAP on AWS: Support prerequisites](#) [Se necesita acceso al portal de SAP]

Práctica recomendada 3.4: utilice manuales de procedimientos para realizar operaciones de la infraestructura SAP

Los manuales de procedimientos consisten en procedimientos documentados para lograr resultados específicos. Permita respuestas rápidas y constantes para eventos que se comprendan bien a través de la documentación de los procedimientos en los manuales. Comprenda las operaciones comunes de SAP y cree documentación específica y con control de versiones mediante un ciclo de revisión.

- AWS Well-Architected Framework [excelencia operativa]: [Disposición operativa](#)
- Documentación de AWS: [Manuales de procedimientos y automatización mediante AWS Incident Manager](#)

Sugerencia 3.4.1: cree manuales de procedimientos específicos de operaciones de seguridad de SAP

Considere crear manuales de procedimientos para operaciones de seguridad ordinarias de SAP, a saber:

- Administración del aprovisionamiento y la identidad de los usuarios
- Acceso de usuarios bombero
- Cambios de autorización

- Auditorías de seguridad y autorización
- Rotación de clave de cifrado
- Administración de certificado TLS

Sugerencia 3.4.2: cree manuales de procedimientos específicos para operaciones de escalado y rendimiento de SAP

Considere crear manuales de procedimientos para operaciones de escalado y de rendimiento comunes:

- Redimensionamiento del volumen del disco
- Escalado horizontal y vertical de los servidores de la aplicación SAP
- Redimensionamiento del servidor de base de datos
- Adición o eliminación de servidores desde el balanceador de carga

Sugerencia 3.4.3: cree manuales de procedimientos específicos para operaciones de SAP durante fallas

Considere crear manuales de procedimientos para operaciones durante fallas:

- Reinicio del sistema y orden de reiniciar sistemas
- Copias de seguridad y restauraciones de SAP
- Conmutación por error del clúster
- Error de almacenamiento
- Reinicios y reproducciones críticos de la interfaz
- Cambios en el DNS y en el enrutamiento de red
- Recuperación de ransomware

Sugerencia 3.4.4: cree manuales de procedimientos específicos para operaciones de mantenimiento de SAP

Considere crear manuales de procedimientos para operaciones de mantenimiento:

- Inicio y detención de SAP
- Actualización o copia del sistema SAP

- Comprobación diaria de estado
- Administración de errores y volcado de memoria de ABAP
- Revisión de la aplicación, el sistema operativo y la base de datos de SAP
- Rotación, limpieza y clasificación de registros

Tenga en cuenta el registro de la base de datos y de la aplicación, y haga un seguimiento de las limpiezas de los archivos en su entorno de SAP. A modo de ejemplo, consulte la siguiente nota de SAP: [2399996 - Automating SAP HANA Cleanup \(Automatización de la limpieza de SAP HANA\)](#) [Se necesita acceso al portal de SAP]

### Práctica recomendada 3.5: utilice los manuales de estrategias para investigar los problemas

Habilite respuestas constantes y rápidas para los problemas que no se comprendan correctamente mediante la documentación del proceso de investigación en los manuales de estrategias. Valide y desarrolle estos manuales de estrategias usándolos con regularidad en operaciones, pero también en entornos que no sean de producción y en sesiones de práctica designadas, como las simulaciones de fallos.

Sugerencia 3.5.1: cree manuales de estrategias ante problemas para usarlos en respuesta a incidentes

Comprenda los problemas que ocurren con frecuencia y los pasos de resolución que se siguen para cada uno de los problemas identificados y cree documentación específica y con control de versiones mediante un ciclo de revisión. Los manuales de estrategias sugeridos deberían incluir:

- Investigación de problemas de rendimiento
- Investigación de problemas de capacidad
- Investigación de problemas de autenticación e inicio de sesión
- Investigación de incidentes de seguridad
- Investigación de conectividad y redes
- Investigación de ransomware y virus
- Investigación de errores de interfaz
- Investigación de errores de trabajos por lotes
- Investigación de errores de implementación o transporte



Asegúrese de que sus manuales de estrategias incluyan pasos de integración y comunicación con funciones y equipos de asistencia relacionados. Entre algunos pasos de comunicación comunes, se incluyen el envío de notificaciones y actualizaciones de progreso a una mesa de incidentes críticos, a un equipo de incidentes de seguridad o a un equipo de administración de cambios.

Sugerencia 3.5.2: organice simulaciones regulares de fallos de SAP a fin de probar los procedimientos operativos y validar los manuales de estrategias

Considere organizar simulaciones de fallos de SAP de forma regular pensadas para su equipo operativo. Un día de prueba simula un error o un evento para probar los sistemas, los procesos y las respuestas de los equipos. El objetivo es llevar a cabo las acciones que realizaría el equipo si hubiera ocurrido un evento excepcional. Estas deben llevarse a cabo regularmente para que su equipo desarrolle una “memoria muscular” sobre cómo responder. Los días de prueba deben cubrir las áreas de operaciones, seguridad, fiabilidad, rendimiento y costos. A través de un entorno reservado exclusivamente a la experimentación, simule situaciones del mundo real para validar y poner en práctica procedimientos operativos y procesos de recuperación.

### Práctica recomendada 3.6: utilice la automatización para realizar operaciones de la infraestructura SAP

Cree canalizaciones de automatización para las compilaciones y operaciones de infraestructura dentro de entornos SAP. La automatización mediante técnicas de infraestructura como código (por ejemplo, CloudFormation o Launch Wizard para SAP) permite la creación y extensión de entornos repetibles y ágiles. Las canalizaciones y operaciones de infraestructura automáticas reducen los errores de los procesos manuales y el esfuerzo para implementar los cambios, y mejoran la velocidad de reacción en función de sus necesidades empresariales.

Cree canalizaciones operativas automatizadas en infraestructuras SAP que le permitan realizar tareas de entorno comunes de manera automatizada (por ejemplo, copias del sistema, inicio de SAP, detención de SAP, escalado de SAP). Invoque estas canalizaciones en respuesta a eventos operativos, como la detención del sistema en función del tiempo o el escalado automático debido a la carga de usuarios.

Sugerencia 3.6.1: implemente técnicas de infraestructura como código para crear canalizaciones de compilación y ejecución repetibles mediante el uso de código en su infraestructura SAP

Utilice herramientas tales como AWS CloudFormation, AWS Cloud Development Kit o AWS Launch Wizard para que SAP cree implementaciones de entornos repetibles, controladas y rápidas.

- Blog de SAP on AWS: [Infrastructure as Code Example: Terraform and SAP on AWS](#)

- Documentación de AWS: [AWS Launch Wizard para SAP](#)

Sugerencia 3.6.2: implemente operaciones comunes de la infraestructura SAP de manera automatizada

Combine el uso de herramientas de orquestación y de infraestructura como código (IaC) para realizar operaciones comunes de la infraestructura SAP de manera automatizada. Algunas herramientas, como AWS CloudFormation, AWS Systems Manager Automation, SAP Landscape Management (LaMa) y AWS Lambda, se pueden combinar para que realicen operaciones comunes de la infraestructura SAP en canalizaciones de implementación.

Considere utilizar herramientas de automatización de terceros en los casos en que sea necesaria una integración compleja o profunda entre las herramientas (por ejemplo: Terraform, Ansible, Chef).

Considere utilizar operaciones automatizadas como respuesta a eventos de carga de trabajo de SAP para permitir una infraestructura de autoreparación y automantenimiento.

- Notas de SAP: [2574820 - SAP Landscape Management Cloud Manager for Amazon Web Services \(AWS\)](#) [Se necesita acceso al portal de SAP]
- Documentación de AWS: [AWS Launch Wizard para SAP](#)
- Documentación de AWS: [AWS Systems Manager Automation](#)
- AWS Marketplace: [Productos y herramientas para DevOps](#)

## 4. Valide y mejore su carga de trabajo de SAP con regularidad

¿Cómo validará sus cargas de trabajo de SAP para que sigan operando de manera eficiente?

Apunte a mejorar su carga de trabajo de SAP con regularidad y aproveche los lanzamientos de los nuevos servicios de AWS. Dedique tiempo y recursos para mantener su carga de trabajo de SAP.

Apunte a tener mejoras progresivas y continuas para que la eficiencia de su carga de trabajo de SAP evolucione. Planifique la implementación de revisiones, cambios pequeños y revaluaciones de las decisiones de diseño anteriores con medidas correctivas que mejoren el rendimiento, la resiliencia y la rentabilidad.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica	Obligatorio	Comprenda y planifique los eventos del ciclo de vida de su carga de trabajo de SAP

ID	Prioridad	Práctica recomendada
recomendada 4.1		
<input type="checkbox"/> Práctica recomendada 4.2	Obligatorio	Lleve a cabo regularmente administraciones de revisiones para mantener vigente el software
<input type="checkbox"/> Práctica recomendada 4.3	Altamente recomendado	Pruebe periódicamente los planes de continuidad de la empresa y la recuperación de errores
<input type="checkbox"/> Práctica recomendada 4.4	Altamente recomendado	Realice revisiones regulares de las cargas de trabajo para optimizarlas en función de resiliencia, rendimiento, agilidad y costos

## Práctica recomendada 4.1: comprenda y planifique los eventos del ciclo de vida de su carga de trabajo de SAP

Las cargas de trabajo de SAP dependen en gran medida de que SAP proporcione nuevas revisiones de software y de vulnerabilidades, sistemas operativos y kernels de base de datos, así como escalado a modo de respaldo. Con frecuencia, SAP publica información sobre nuevos lanzamientos de software: tipos de lanzamiento, duración de las labores de mantenimiento, disponibilidad prevista y rutas de actualización en su [PAM](#) y en las notas de SAP. Le recomendamos consultar detalles específicos sobre cada una de sus aplicaciones SAP y hacerles un seguimiento a nivel local para saber si su software de SAP está vigente o tiene soporte y cuándo finalizará su vida útil desde el punto de vista del mantenimiento.

La PAM también ofrece información sobre la disponibilidad y la compatibilidad de la plataforma: incluida la plataforma de base de datos y los sistemas operativos compatibles que deberían guiarlo en la revisión y la actualización de estos componentes subyacentes de su carga de trabajo de SAP. Los proveedores de sistemas operativos también tienen su propio ciclo de vida de revisión y soporte, el cual también se debe tomar en consideración al momento de planificar eventos de ciclo de vida y mantenimiento de SAP tales como las actualizaciones.

Sugerencia 4.1.1: cree un plan de desarrollo operativo para sus aplicaciones SAP tomando en cuenta fechas de soporte y de ciclo de vida importantes

Haga una lista de todas las aplicaciones de software, versiones de kernels, sistemas operativos y versiones de base de datos de SAP en un registro central y agregue la información sobre las versiones admitidas y sobre las ventanas de mantenimiento que figura en la PAM. Utilice esta lista como una vista consolidada para planificar la revisión, las actualizaciones y los cambios de plataforma de todos los componentes requeridos para mantener a SAP vigente y en capacidad de recibir soporte.

- Documentación de SAP: [SAP Release & Maintenance Strategy: Product Availability Matrix \(Estrategia de lanzamiento y mantenimiento de SAP: Matriz de disponibilidad de productos\)](#) [Se necesita acceso al portal de SAP]

Sugerencia 4.1.2: lleve un calendario del vencimiento de las credenciales, los certificados y las licencias

Además de los principales eventos de ciclo de vida y revisión de SAP mencionados anteriormente, asegúrese de llevar un calendario operativo que prevea la ocurrencia de eventos menores en el sistema. Algunos ejemplos de estos eventos de mantenimiento podrían ser el vencimiento de las credenciales del sistema, el vencimiento de certificados (por ejemplo, para la integración STRUST entre los sistemas) y cualquier trabajo de renovación de licencia o actualizaciones requeridas (por ejemplo, licencias de base de datos o de SAP temporales para la migración, el desarrollo o para fines de Proof of Concept (POC, prueba de concepto).

- Documentación de AWS: [AWS Certificate Manager](#)

Sugerencia 4.1.3: planifique las actualizaciones o las alternativas antes de que el software de SAP llegue al final de su vida útil

Cree un plan de desarrollo de la infraestructura SAP en el que se prevea los eventos importantes de ciclo de vida de SAP y el mantenimiento operativo: revisión, actualizaciones de software, migraciones y redefinición de la plataforma, en caso de ser necesario. Haga llegar este calendario del ciclo de vida a las partes interesadas, tanto comerciales como técnicas. Planifique invertir para financiar estas actividades o proyectos del ciclo de vida de SAP. Planifique con las partes interesadas de su empresa dónde es posible que ocurran ventanas de mantenimiento y dónde se requerirán períodos de inactividad o reinicios.

- Documentación de SAP: [SAP Roadmap Explorer \(Explorador del plan de desarrollo de SAP\)](#)

Sugerencia 4.1.4: manténgase actualizado y suscríbase a las notas de SAP para recibir asesoramiento de soporte

Suscríbase a las notas clave de SAP y a los Knowledge Base Articles (KBA, artículos de la base de conocimientos) correspondiente a su carga de trabajo de SAP para que se le notifique de cualquier cambio o actualización de compatibilidad y asesoramiento. Utilice la funcionalidad “Favorite” (Agregar a favoritos) de las notas de SAP para llevar una lista de notas importantes y de acceso frecuente para su carga de trabajo de SAP a fin de que sean fácilmente accesibles y comparables.

- [SAP Support Portal - Favorite SAP Notes \(SAP Support Portal: Notas favoritas de SAP\)](#) [Se necesita acceso al portal de SAP]

**Práctica recomendada 4.2: lleve a cabo regularmente administraciones de revisiones para mantener vigente el software**

Lleve a cabo administraciones de revisiones de forma regular para obtener nuevas características, abordar problemas y mantener conformidad con la gobernanza. Considere aplicar revisiones en la capa del sistema operativo, la base de datos y la aplicación SAP. Comprenda si su proceso de revisiones será revisar sus servidores existentes o aprovisionar y revisar un nuevo servidor. Automatice la administración de revisiones para reducir los errores causados por procesos manuales, el nivel de esfuerzo en las revisiones y el tiempo de inactividad de las aplicaciones que se requiere en las principales revisiones de bases de datos y del kernel de SAP.

Sugerencia 4.2.1: implemente los procedimientos de administración de revisiones de SAP para repasar regularmente las notas de seguridad de SAP y las revisiones recientemente lanzadas

Considere aplicar revisiones en la capa del sistema operativo, la base de datos y la aplicación SAP

Documentación de AWS: [Boletines de seguridad de AWS](#)

Documentación de SAP: [SAP EarlyWatch Alert](#)

Documentación de SAP: [SAP Security News \(Noticias de seguridad de SAP\)](#)

Sistema operativo	Guía
SUSE Linux Enterprise Server	<a href="#">SUSE Update Advisories</a>

Sistema operativo	Guía
Red Hat Enterprise Linux	<a href="#">Red Hat Security Advisories</a>
Microsoft Windows	<a href="#">Microsoft Security Alerts</a>
Oracle Enterprise Linux	<a href="#">Oracle Security Alerts</a>

Para informarse más sobre este tema, consulte [seguridad] [Práctica recomendada 6.2: cree y proteja el sistema operativo](#).

Sugerencia 4.2.2: considere el uso de herramientas automatizadas, tales como AWS Systems Manager y AWS OpsWorks, para que lo ayuden a alinear y automatizar las revisiones en su infraestructura SAP

- Documentación de AWS: [AWS Systems Manager Patch Manager](#)
- Documentación de AWS: [AWS OpsWorks](#)
- Documentación de AWS: [¿Qué es AWS OpsWorks?](#)
- SAP Lens [seguridad]: [Práctica recomendada 6.2: cree y proteja el sistema operativo](#).

**Práctica recomendada 4.3: pruebe periódicamente los planes de continuidad de la empresa y la recuperación de errores**

Los sistemas SAP suelen ser esenciales para las empresas y se depende mucho de ellos para transacciones directas con clientes. Permitir la reanudación rápida de las operaciones de TI y minimizar la pérdida de datos durante un error o ante un desastre es esencial para lograr la excelencia operativa. Se requieren Business Continuity Plans (BCP, planes de continuidad empresariales) y procedimientos de recuperación de errores para asegurarse de que su equipo y sus sistemas de operaciones sepan qué hacer y cuándo hacerlo, y así se puede reanudar el servicio de la carga de trabajo rápidamente en caso de un error.

Para lograr una reanudación exitosa de los servicios es esencial que se prueben, se mejoren y se refinan con regularidad los procedimientos del BCP y los planes de recuperación de errores a medida que el equipo de soporte y los sistemas evolucionan. Probar su BCP y sus planes de recuperación fuera de situaciones de crisis reales garantizará que, cuando se produzca una falla o un desastre reales en el sistema, pueda confiar en su capacidad de reanudar el servicio de manera satisfactoria y

en que cumplirá con el Recovery Time Objective (RTO, objetivo de tiempo de recuperación) y con el Recovery Point Objective (RPO, objetivo de punto de recuperación).

Sugerencia 4.3.1: cree un calendario de pruebas de los procedimientos de recuperación de errores y del BCP

Cree un calendario para programar pruebas regulares (como mínimo anuales) de los procedimientos de recuperación de errores y del BCP para su carga de trabajo de SAP. Involucre a equipos operativos de tecnología, personal de soporte y partes interesadas comerciales en esta prueba, de manera que se comprendan los procedimientos y se cumplan las expectativas. Intente probar su sistema en una situación que se asemeje lo máximo posible a la realidad.

Considere probar las siguientes situaciones y validar las métricas de recuperación para cada uno de ellas:

- Error en el servicio de aplicaciones SAP  
(por ejemplo, el servicio de aplicaciones SAP no se inicia debido a un cambio en la configuración)
- Error del host de única instancia  
(por ejemplo, la instancia de EC2 del servidor de aplicaciones SAP se torna inaccesible)
- Error en el volumen de almacenamiento único  
(por ejemplo, un volumen de EBS único se torna inaccesible)
- Error en la red y conmutación a conexión redundante  
(por ejemplo, su conexión de Direct Connect en las instalaciones es inaccesible)
- Conmutación por error automatizada entre los componentes agrupados primarios y secundarios  
(por ejemplo, el clúster SUSE HAE fuerza a la base de datos principal de HANA a moverse a la base de datos secundaria en una AZ alternativa)
- Conmutación por error manual entre componentes primarios y secundarios  
(por ejemplo, invocación manual de la conmutación de Oracle DataGuard a la base de datos secundaria en una AZ alternativa)
- Balanceador de carga entre múltiples componentes redundantes  
(por ejemplo, el Web Dispatcher principal falla en un par de alta disponibilidad entre las AZ)
- Recuperación de su aplicación SAP en una región de AWS alterna (si es necesario)

- Recuperación a partir de la copia de seguridad en caso de ransomware

(por ejemplo, recuperar todo su sistema SAP ERP desde la copia de seguridad WORM de Amazon S3)

Sugerencia 4.3.2: revise y actualice regularmente el BCP y los procedimientos de recuperación de errores como parte de los cambios en la carga de trabajo

A medida que su carga de trabajo evoluciona y cambia, asegúrese de que se tomen en cuenta el BCP y los procedimientos de recuperación en estos cambios. Cuando un cambio de código o infraestructura podría afectar su RTO o RPO, asegúrese de que la documentación y la configuración estén actualizadas, y de probar el nuevo BCP y proceso de recuperación como parte del proceso de lanzamiento o calendario de prueba regular.

- Documentación de AWS: [Business Continuity Plan \(BCP\) Definition \(Definición del plan de continuidad empresarial \[BCP\]\)](#)
- Documentación de AWS: [Architecture Guidance for Availability and Reliability of SAP on AWS \(Guía de arquitectura para la disponibilidad y la fiabilidad de SAP on AWS\)](#)
- SAP Lens [fiabilidad]: [Práctica recomendada 11.4: realice pruebas periódicas de resiliencia](#)

**Práctica recomendada 4.4: realice revisiones regulares de las cargas de trabajo para optimizarlas en función de resiliencia, rendimiento, agilidad y costos**

Cuando ejecute SAP on AWS, haga planes para mejorar de forma continua y progresiva la efectividad y la eficiencia de su carga de trabajo y dedique tiempo y recursos a ello. Con regularidad, AWS lanza nuevos servicios, enfoques, y publica Service Level Agreements (SLA, acuerdos de nivel servicio) mejorados y reducciones de precios que puede aprovechar para optimizar su carga de trabajo de SAP. Cerciórese de que los lanzamientos de nuevos servicios sean aplicables a su carga de trabajo de SAP y, si corresponde, impleméntelos en su entorno de producción para mejorar su carga de trabajo.

Sugerencia 4.4.1: planifique revisiones regulares de su carga de trabajo de SAP

Trabaje con su equipo de AWS, socios de AWS o expertos internos para revisar de forma periódica su carga de trabajo de SAP sirviéndose de SAP Lens para Well-Architected Framework (este documento). Programe al menos una revisión anual de sus cargas de trabajo. Identifique, valide y priorice las actividades de mejora y la remediación de problemas, e incorpore esto en su lista de tareas.



#### Sugerencia 4.4.2: revise el tamaño y el rendimiento de la instancia de Amazon EC2

Revise el uso de CPU y el uso de memoria de su carga de trabajo de SAP validando las métricas históricas de CloudWatch. Revise cada componente de SAP para determinar si el uso de la CPU y memoria es bajo y considere utilizar instancias de EC2 del tamaño adecuado para que coincidan mejor con los requisitos de la carga de trabajo. Considere utilizar tipos de instancias de EC2 que estén certificadas por SAP y que se hayan lanzado recientemente para conseguir un rendimiento adecuado y optimizar costos. Planifique aprovechar las nuevas mejoras en su lista de tareas operativa.

Consulte [Optimización de costos](#) para el uso de Amazon EC2 en cargas de trabajo de SAP.

- Documentación de AWS: [Amazon EC2 Instance Types for SAP \(Tipos de instancia de Amazon EC2 para SAP\)](#)

#### Sugerencia 4.4.3: revise el ajuste de tamaño y el rendimiento de Amazon EBS

Revise el uso de almacenamiento de su carga de trabajo de SAP mediante la validación del consumo de volumen, el rendimiento y el uso de las IOPS de las métricas históricas de CloudWatch. Revise cada componente de SAP para detectar casos de almacenamiento sobredimensionado o de subutilización del rendimiento y de las IOPS, y considere utilizar un almacenamiento de Amazon EBS del tipo y tamaño adecuados a fin de satisfacer en mayor grado los requisitos de la carga de trabajo. Considere utilizar tipos de volúmenes de Amazon EBS que estén certificados por SAP y que se hayan lanzado recientemente para adaptarse al rendimiento y optimizar costos. Planifique aprovechar las nuevas mejoras en su lista de tareas operativa

- Documentación de AWS: [Ajuste del tamaño](#)
- SAP Lens [Optimización de costos]: [Práctica recomendada 18.4: evalúe el efecto del costo de las opciones de almacenamiento en función de las características requeridas](#) .

#### Sugerencia 4.4.4: revise los nuevos servicios que mejoran la agilidad o mejoran la eficiencia en sus operaciones de carga de trabajo de SAP

Revise los nuevos lanzamientos de servicios de soporte que podrían mejorar las operaciones de su carga de trabajo de SAP. Si tiene a su disposición un Technical Account Manager (TAM, administrador técnico de cuenta) en virtud de su acuerdo de AWS Support, este puede asistirlo con reuniones informativas sobre los servicios nuevos y charlas sobre optimización.

Tenga en cuenta nuevos lanzamientos, como servicios de almacenamiento compartido de archivos o de interfaz (por ejemplo, AWS Transfer, API Gateway), servicios de seguridad (por ejemplo, Amazon GuardDuty, AWS Firewall), herramientas de copia de seguridad (por ejemplo, AWS Backup) y herramientas de automatización (por ejemplo, Launch Wizard for SAP).

Planifique aprovechar las nuevas mejoras en su lista de tareas operativa.

- Documentación de AWS: [Fuente de novedades](#)
- Documentación de AWS: [Proactive Services from Support \(Servicios proactivos de soporte\)](#)

Sugerencia 4.4.5: supervise las publicaciones y anuncios del blog de SAP on AWS

Considere suscribirse a la fuente del blog SAP on AWS y a la fuente de novedades de AWS para mantenerse al tanto de los servicios recientemente lanzados, las innovaciones y las reducciones de precios.

- [Fuente del blog de SAP on AWS](#)

Sugerencia 4.4.6: planifique tareas de mejora periódicas para aprovechar los servicios de AWS nuevos y mejorados

Asegúrese de que su presupuesto operativo prevea un esfuerzo planificado de parte del equipo de soporte para la implementación y la realización de pruebas de nuevos servicios de AWS y la evolución de la carga de trabajo de forma periódica.

## Seguridad

El pilar de la seguridad abarca la capacidad para proteger los datos, sistemas y activos para aprovechar las tecnologías en la nube a fin de mejorar la seguridad. En este enfoque, se destacan algunos de los principios y recursos centrales de SAP. Dado que muchas de estas prácticas no son exclusivas de SAP, sugerimos que considere los principios centrales para su empresa y se centre en establecer controles en toda la infraestructura. El [Pilar de seguridad](#) se ponen de manifiesto principios y recomendaciones generales de diseño que recomendamos que lea junto con la guía de SAP que sigue a continuación.

Independientemente de su estrategia de implementación, ya sea que esté basada en AWS, en las instalaciones o sea híbrida, asegúrese de seguir las pautas recomendadas por SAP Security Notes y

News, y manténgase al tanto de las recomendaciones de seguridad más actualizadas relacionadas específicamente con las cargas de trabajo de SAP.

## 5. Comprenda los estándares de seguridad y cómo se aplican a su carga de trabajo de SAP

¿Cómo define los estándares y los controles de seguridad para alinearlos con la criticidad de su carga de trabajo de SAP? Los estándares son documentos publicados en los que se definen las políticas y los procedimientos requeridos para asegurar sus sistemas a través de una práctica recomendada para un producto, una organización, una industria o una jurisdicción. Proporcionan un marco con el que se puede evaluar su carga de trabajo de SAP. Algunos estándares son obligatorios para garantizar la conformidad con los requisitos normativos, mientras que otros son opcionales, pero ayudan a establecer roles y responsabilidades.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 5.1	Obligatorio	Defina los roles y las responsabilidades de seguridad
<input type="checkbox"/> Práctica recomendada 5.2	Altamente recomendado	Clasifique los datos dentro de las cargas de trabajo de SAP
<input type="checkbox"/> Práctica recomendada 5.3	Altamente recomendado	Determine los controles de seguridad requeridos en función de la clasificación de la aplicación y los datos
<input type="checkbox"/> Práctica recomendada 5.4	Altamente recomendado	Cree una estrategia para implementar controles de seguridad

## Práctica recomendada 5.1: defina los roles y las responsabilidades de seguridad

Al definir los requisitos para asegurar sus cargas de trabajo de SAP, puede identificar riesgos que se deben abordar y asegurarse de que se asignen debidamente los roles y las responsabilidades relacionadas con la seguridad. En las sugerencias, analizamos los estándares de AWS, SAP y cualquier proveedor de servicio para formar una base de referencia sobre la que puede crear su estrategia de seguridad.

### Sugerencia 5.1.1: comprenda el modelo de responsabilidad compartida de AWS

AWS es responsable de la seguridad de la nube y usted, como cliente, es responsable de la seguridad en la nube. Esté al tanto y comprenda los siguientes recursos:

- Documentación de AWS: [Modelo de responsabilidad compartida de AWS](#)
- Documentación de AWS: [Respuesta al abuso y compromiso de AWS](#)
- Documentación de AWS: [Política de uso aceptable de AWS](#)

Comprenda la división de responsabilidades entre usted y sus socios en el contexto del modelo de responsabilidad compartida de AWS

### Sugerencia 5.1.2: comprenda las bases de la seguridad entre SAP y AWS, incluidos los certificados de conformidad, los informes y las confirmaciones

Comprenda los estándares de seguridad y las certificaciones de conformidad que SAP y AWS admiten. Determine cuáles son pertinentes para su industria y su país (por ejemplo, PCI-DSS, GDPR, HIPAA). Estos controles pueden ayudar a fortalecer sus propios programas de conformidad y certificación, y reducir los esfuerzos necesarios para cumplir con los estándares de seguridad.

Consulte la documentación de SAP y de AWS para obtener más detalles:

- Documentación de AWS: [Conformidad de AWS](#)
- Documentación de AWS: [AWS Compliance Center \(Centro de conformidad de AWS\)](#)
- Documentación de AWS: [Programas de conformidad](#)
- Documentación de AWS: [Servicios de conformidad en el ámbito](#)
- Documentación de SAP: [Trust Center](#)

### Sugerencia 5.1.3: evalúe las bases de la seguridad de los proveedores de servicios que admiten su carga de trabajo de SAP

Si usted depende de organizaciones de terceros para administrar toda o parte de su carga de trabajo de SAP, evalúe la capacidad de ese tercero para cumplir con los controles de seguridad requeridos. Esto comprende los requisitos legales y regulatorios que su empresa debe cumplir.

## Práctica recomendada 5.2: clasifique los datos dentro de las cargas de trabajo de SAP

La sensibilidad de los datos puede afectar los controles necesarios para mitigar el riesgo. AWS sugiere consultar los marcos del estándar dentro de su industria o su organización y adoptarlos para clasificar sus cargas de trabajo de SAP y los datos que contienen.

### Sugerencia 5.2.1: determine la clasificación de los datos y los requisitos de manipulación

Identifique cualquier marco de clasificación de datos ya implementado en su organización. Estos marcos pueden ayudarle a categorizar los datos en función de la sensibilidad de la información, como, por ejemplo, los datos que deben protegerse por cuestiones de confidencialidad, integridad y disponibilidad. Existen modelos de clasificación estándar, por ejemplo, el [Esquema de categorización de información de EE. UU.](#), que se pueden personalizar en función de su industria, empresa o requisitos de TI.

Comprenda cómo se deben manipular los datos según las pautas apropiadas para la clasificación. Esto incluye los controles de seguridad específicos relacionados con los requisitos estándar o normativos (por ejemplo, PCI-DSS o GDPR) y las consideraciones de privacidad comunes (por ejemplo, el manejo de Información personal identificable [PII]). En los siguientes documentos, podrá encontrar información adicional:

- Documentación de AWS: [Data Classification: Secure Cloud Adoption Whitepaper \(Clasificación de datos: documento técnico de adopción segura de la nube\)](#)
- Documentación de AWS: [Reglamentación General de Protección de Datos \(RGPD\)](#)
- [NIST Security and Privacy Controls for Information Systems and Organizations \(Controles de seguridad y privacidad del NIST para organizaciones y sistemas de Información\)](#)
- [ISO 27001 – Annex A.8: Asset Management \(Anexo A.8: administración de activos\)](#)
- Well-Architected Framework [seguridad]: [Protección de los datos](#)

### Sugerencia 5.2.2: identifique los tipos de datos de SAP con reglas de manejo específicas

En función de los procesos empresariales que admite su sistema SAP, podrían existir requisitos para la manipulación y el almacenamiento de datos. Familiarícese con las pautas que rigen para su ubicación y su industria. Entre algunos ejemplos vinculados a SAP, se encuentran los siguientes:

- Evaluar si es necesario un complemento digital para pagos a fin de proteger los datos del titular de la tarjeta almacenados y garantizar la conformidad con la Payment Card Industry (PCI, industria de tarjetas de pagos).
- Evaluar los datos de RR. HH. para conocer los requisitos de residencia de los datos, por ejemplo, algunos países y jurisdicciones podrían requerir que los datos se almacenen dentro de una ubicación geográfica específica.
- Considere qué datos podrían tener que estar cifrados en sistemas que no sean de producción para ocultar información confidencial, pero mantener la integridad de los datos.

### Sugerencia 5.2.3: clasifique todas sus cargas de trabajo según el marco definido

Clasifique sus sistemas SAP según su uso comercial y la existencia de tipos de datos críticos. Los sistemas de transacciones, como SAP ERP, tienen más probabilidades de contener información confidencial que los sistemas analíticos, tales como SAP BW, o los sistemas de administración, como Solution Manager, aunque esto deberían validarlo expertos funcionales y de seguridad.

Además, debe evaluar si los mismos controles se aplican a cargas de trabajo que no son de producción. Por ejemplo, las cargas de trabajo que no son de producción incluyen datos de producción y, por lo tanto, ¿deben cumplir con los mismos controles de seguridad?

### Práctica recomendada 5.3: evalúe la necesidad de aplicar controles de seguridad específicos para sus cargas de trabajo de SAP

En función de la clasificación de datos, evalúe los controles que pueden ayudarlo a cumplir con los estándares y los requisitos establecidos en las prácticas recomendada anteriores. Estas prácticas incluyen ubicación, estrategia de cuenta de AWS y requisitos de aleatorización para cargas de trabajo de SAP que no sean de producción.

#### Sugerencia 5.3.1: evalúe cualquier requisito de ubicación geográfica

Sus cargas de trabajo de SAP podrían implementarse en una o varias regiones y AZ de AWS. Cada región de AWS consta de varias AZ aisladas y separadas físicamente dentro de un área geográfica. Además de evaluar la región en busca de latencia y resiliencia, debería considerar si se cumplen los requisitos de seguridad y conformidad. Entre algunos de las regiones aisladas con jurisdicciones operativas específicas, se encuentran las siguientes:

- AWS GovCloud (EE. UU.): designada para alojar información confidencial, cargas de trabajo reglamentadas, y seguir los requisitos de seguridad y conformidad más estrictos del gobierno de los EE. UU.

- Amazon Web Services en China: AWS ha colaborado con socios locales para garantizar que se cumplan los requisitos legales y normativos de China.

Algunas industrias o países tienen requisitos de residencia de datos que establecen que todo el contenido de los clientes que se procesa y se almacena en un sistema de TI debe permanecer dentro de las fronteras de un país en particular.

- Documentación de AWS: [Addressing Data Residency with AWS \(Cómo abordar la residencia de los datos con AWS\)](#)

Antes de decidir una ubicación, revise la disponibilidad de los servicios para esa región de AWS a fin de asegurarse de que los servicios que requiere estén disponibles.

- Documentación de AWS: [Servicios regionales de AWS](#)

Sugerencia 5.3.2: determine la estrategia de cuenta de AWS requerida para sus cargas de trabajo de SAP

Una importante consideración al ejecutar las cargas de trabajo de SAP en AWS es la estrategia de cuenta de AWS que adopte para cumplir con los controles de seguridad de la organización. Debería considerar separar las cargas de trabajo de SAP de las que no son de SAP y ejecutar las cargas de trabajo de producción en una cuenta distinta a la que destina para ejecutar cargas que no son de producción.

Comprenda la estrategia de administración de cuentas de AWS de su organización, incluido el uso de AWS Organizations y AWS Control Tower. Considere aislar las capacidades de seguridad y registro en una cuenta aislada. Consulte los siguientes recursos para obtener detalles adicionales:

- Well-Architected Framework [seguridad]: [Separación y administración de cuentas de AWS](#)
- Documentación de AWS: [Establecer su entorno de acuerdo con las prácticas recomendadas de AWS](#)
- Documentación de AWS: [Organizing Your AWS Environment Using Multiple Accounts \(Organizar su entorno de AWS utilizando varias cuentas\)](#)

La estrategia de cuenta que adopte también afectará la configuración de la red dentro de AWS. Al determinar la estrategia de cuenta de AWS adecuada para sus cargas de trabajo de SAP, debe considerar lo siguiente:

- Requisitos para el acceso entre cuentas, como la necesidad de configurar [Interconexión de VPC](#) o [Gateway de tránsito](#) para permitir la comunicación entre sistemas de producción y de no producción. Por ejemplo, el movimiento de transportes de SAP en su infraestructura.
- Las dependencias de servicios compartidos (como recursos de administración de directorios) y los componentes de administración de red que se implementan en diferentes cuentas de AWS desde sus cargas de trabajo de SAP.

Sugerencia 5.3.3: revise los controles para la aleatorización de datos (si corresponde)

Muchos clientes de SAP confían en las copias de datos de producción con fines de pruebas, incluidas las pruebas de rendimiento y regresión. Si crea una copia de datos de producción, decida qué controles debe añadir para asegurarse de que sus datos de producción estén protegidos contra accesos y modificaciones no deseados.

Considere las siguientes opciones:

- Mecanismos tradicionales de aleatorización de datos proporcionados por SAP o terceros
- Uso de cuentas tradicionales o controles de red para limitar el acceso durante una copia de datos de producción
- Uso de una cuenta que no es de producción con los mismos controles que la de producción

## Práctica recomendada 5.4: cree una estrategia para implementar controles de seguridad

Después de evaluar los requisitos empresariales en función de la clasificación de datos, cree una estrategia que equilibre los controles de seguridad de toda su organización con las guías de aplicación y los estándares abiertos disponibles. Tenga en cuenta el esfuerzo de implementación y reconozca el riesgo.

Sugerencia 5.4.1: identifique una matriz para evaluar el riesgo

Existen una variedad de marcos de administración de riesgos para geografías e industrias específicas. Comprenda el marco de riesgo adoptado por su organización y cómo aplica a la administración de riesgos relacionados con sus cargas de trabajo de SAP.

- Documentación de AWS: [Ejemplo de matriz de riesgo](#)
- Documentación de AWS: [Scaling a governance, risk, and compliance program for the cloud \(Escalar un programa de gobernanza, riesgo y conformidad para la nube\)](#)



- [NIST Risk Management Framework \(Marco de administración de riesgos del NIST\)](#)

Sugerencia 5.4.2: evalúe los requisitos de seguridad y conformidad exigidos por su organización

Consulte con su centro de excelencia en la nube, su equipo legal, los equipos de conformidad y con su proveedor de servicios administrados para comprender su base de referencia de seguridad y cómo se aplican los controles. Evalúe si todos estos controles se pueden aplicar fácilmente a su carga de trabajo de SAP e identifique áreas que podrían requerir una excepción, por ejemplo, listas de permitidos y denegados para servicios de AWS, flujo de tráfico entrante y saliente y restricciones de acceso.

Sugerencia 5.4.3: identifique y convenga un proceso de excepciones

En algunas situaciones, los requisitos de software, empresariales y de soporte para SAP podrían requerir que se desvíe de los patrones de seguridad estándar. Identifique un proceso para acordar y documentar cualquier excepción con un foro de asesoramiento de cambios o una autoridad de diseño de seguridad, y vuelva a evaluar el proceso periódicamente.

Documentación de AWS: [Change Management in the Cloud \(Administración de cambios en la nube\)](#)

## 6. Utilice controles de infraestructura y de software para reducir los errores de configuraciones de seguridad

¿Cómo protege su aplicación SAP y la base de datos, sistema operativo, almacenamiento y redes subyacentes? Recomendamos que se refuercen las soluciones de software de SAP y las configuraciones subyacentes asociadas, como las revisiones del sistema operativo y la base de datos, los parámetros, los servicios en la nube y la infraestructura. El fortalecimiento ayuda a garantizar la seguridad de todos los entornos de SAP, tanto de producción como de no producción, en el nivel correcto determinado por su organización.

Utilice el [Modelo de responsabilidad compartida de AWS](#) para guiar sus actividades con respecto a la seguridad de su entorno de SAP. Por ejemplo, las actualizaciones del firmware de sus instancias de EC2 son actividades de “seguridad de la nube” de las que AWS es responsable, mientras que la administración de las aplicaciones y del sistema operativo de esas mismas instancias de EC2 son actividades de “seguridad en la nube” de las que usted es responsable.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 6.1	Obligatorio	Asegúrese de que la seguridad y la auditoría estén integradas en el diseño de la red de SAP
<input type="checkbox"/> Práctica recomendada 6.2	Obligatorio	Cree y proteja el sistema operativo
<input type="checkbox"/> Práctica recomendada 6.3	Obligatorio	Proteja la base de datos y la aplicación
<input type="checkbox"/> Práctica recomendada 6.4	Obligatorio	Establezca un plan para actualizar y revisar todo el software aplicable

Para más información, consulte la siguiente información:

- Documentación de AWS: [AWS Security Whitepaper \(Documento técnico de seguridad de AWS\)](#)
- Notas de SAP: [2191528 - Third-party report showing security vulnerabilities \(informe de terceros en el que se muestran vulnerabilidades de seguridad\)](#) [Se necesita acceso al portal de SAP]
- Documentación de SAP: [ABAP Platform Security Guide \(Guía de seguridad de ABAP Platform\)](#)

**Práctica recomendada 6.1: asegúrese de que la seguridad y la auditoría estén integradas en el diseño de la red de SAP**

Proteger el acceso a la red que aloja su carga de trabajo de SAP es la primera línea de defensa contra la actividad maliciosa. Evalúe los requisitos de su empresa y la solución específica de SAP para determinar los puertos, protocolos y patrones de tráfico que deben habilitarse. Considere los

estándares de seguridad de su organización y las herramientas y los patrones disponibles para simplificar el diseño de la red. Realice auditorías periódicamente o cuando se produzcan cambios.

#### Sugerencia 6.1.1: comprenda los flujos de tráfico de red para SAP

Empiece por comprender sus flujos de tráfico. Los patrones de tráfico de red para las cargas de trabajo de SAP se pueden clasificar como tráfico entrante, tráfico saliente y tráfico interno. Debe identificar si el origen y el destino se encuentran dentro de los límites de su red de confianza para ayudar a definir sus conjuntos de reglas.

Además de los flujos de tráfico entrante y saliente conocidos, como el acceso de usuarios y las conexiones de interfaz, tenga en cuenta los requisitos específicos de SAP, incluidas las conexiones a SAP Support (a través de SAProuter) y las ofertas de SaaS de SAP que restringen el acceso en función de las direcciones IP de origen.

Para el tráfico interno, considere el tráfico entre los componentes y el sistema, así como AWS y servicios compartidos. Herramientas como [Registros de flujo de VPC](#) y [VPC Reachability Analyzer](#) pueden ayudarlo a comprender los flujos de tráfico que entran y salen de Amazon VPC.

Para más información, consulte la siguiente información:

- Documentación de SAP: [TCP/IP Ports for All SAP Products \(Puertos TCP/IP para todos los productos SAP\)](#)

#### Sugerencia 6.1.2: evalúe opciones para permitir y restringir flujos de tráfico

Primero, comprenda cómo conecta usuarios y sistemas de su red en las instalaciones a la cuenta de AWS en la que se ejecutan sus sistemas SAP. Esto se trata en [Network-to-Amazon VPC connectivity options \(Opciones de conectividad entre redes y Amazon VPC\)](#).

Dos métodos principales para controlar el flujo de tráfico de red hacia y desde su VPC consisten en el uso de [grupos de seguridad](#) y [listas de control de acceso de red](#) (ACL de red). Un grupo de seguridad actúa como un firewall virtual con estado que funciona a nivel de la instancia de EC2 para controlar el tráfico entrante y saliente. Una Access Control List (ACL, lista de control de acceso) de red es una capa opcional de seguridad para su VPC que actúa como firewall para controlar el tráfico de entrada y de salida de una o más subredes, y, a diferencia de los grupos de seguridad, un ACL de red no tiene estado.

Considere también las dependencias de los componentes de red fuera de su VPC. Esto puede incluir componentes de red externos proporcionados por AWS, como los puntos de conexión de Amazon

CloudWatch. Esto también puede incluir servicios alojados en Internet, como repositorios de software para revisiones del sistema operativo.

Además de las opciones estándar en AWS, SAP brinda opciones de seguridad de red adicionales, que incluyen el uso de [SAProuter](#) , [SAP Web Dispatcher](#) y las listas de control de acceso [basadas en la red de SAP Gateway](#) . Estas opciones trabajan en conjunto con servicios y configuraciones de AWS para permitir o restringir el acceso a la red de los sistemas SAP.

Para más información, consulte la siguiente información:

- Blog de SAP on AWS: [VPC Subnet Zoning Patterns for SAP on AWS \(Patrones de zonificación de la subred de VPC para SAP on AWS\)](#)
- Well-Architected Framework [seguridad]: [Protección de infraestructura: protección de redes](#)
- Well-Architected Framework [enfoque de administración y gobernanza]: [Conectividad a la red](#)
- Documentación de SAP: [Seguridad de comunicaciones y redes](#)

Sugerencia 6.1.3: utilice pautas de diseño y herramientas de AWS para simplificar la seguridad de la red

Los sistemas SAP con frecuencia tienen requisitos de integración complejos y la nube ofrece formas adicionales de simplificar la administración de la seguridad de la red. Considere los siguientes enfoques:

- Evite referirse a rangos IP o direcciones IP individuales cuando sea posible para simplificar la administración.
- Utilice un conjunto estándar de números del sistema SAP en todas sus cargas de trabajo de SAP para disminuir el rango de puertos de red necesarios.
- [Los puntos de conexión de VPC](#) eliminan el requisito de acceso a Internet saliente desde su VPC para acceder a servicios de AWS como Amazon S3 y Amazon CloudWatch. Cuando sea posible y no sea obligatorio por los requisitos de la empresa, puede evitar que el tráfico de SAP hacia y desde estos servicios atraviesen la Internet pública mediante el enrutamiento de todo el tráfico a través de componentes de red administrados de AWS.
- Simplifique los grupos de seguridad mediante el uso de [listas de prefijos de VPC](#) o [reglas del grupo de seguridad](#) que hacen referencia a otros grupos de seguridad en lugar de rangos de direcciones IP.
- Utilice la automatización para crear, actualizar y administrar grupos de seguridad para evitar sesgos en la configuración.

- Considere utilizar [AWS Firewall Manager](#) para brindar una administración centralizada de grupos de seguridad en VPC y cuentas de AWS.
- Considere utilizar [SAProuter](#) , [SAP Web Dispatcher](#) y AWS Elastic Load Balancing para ocultar los puntos de entrada a los sistemas de backend.
- Considere utilizar múltiples [puntos de entrada de SAP Internet Communication Manager \(ICM\)](#) para brindar un control de acceso más detallado.

Para más información, consulte la siguiente información:

- Documentación de SAP: [Network-based Access Control Lists \(Listas de control de acceso basadas en red\)](#)
- Documentación de SAP: [TCP/IP Ports for All SAP Products](#)

## Práctica recomendada 6.2: cree y proteja el sistema operativo

La protección del sistema operativo que subyace a su software de SAP disminuye la posibilidad de que un actor malicioso pueda obtener acceso no autorizado a los datos internos de la aplicación SAP, afectar la disponibilidad del software o desestabilizar las implementaciones esenciales para su empresa. Siga las recomendaciones de SAP, el proveedor del sistema operativo, el proveedor de la base de datos y AWS para proteger el sistema operativo. Según la solución y el sistema operativo de SAP que haya elegido, es posible que deba habilitar o desactivar servicios, establecer parámetros de kernel específicos y aplicar diferentes combinaciones de revisión de seguridad. Piense cómo los requisitos de SAP se alinean con los de su organización e identifique cualquier conflicto.

Sugerencia 6.2.1: determine un enfoque para el aprovisionamiento de un sistema operativo seguro

La imagen de máquina de Amazon (AMI) brinda la información requerida para lanzar una instancia de EC2. Debería estar convencido de que sus AMI son seguras a nivel del sistema operativo. De lo contrario, las brechas de seguridad podrían propagarse a cualquier cantidad de instancias a medida que las AMI se reutilizan y actualizan.

Las AMI pueden ser imágenes estándar del proveedor del sistema operativo o imágenes personalizadas que cree usted mismo. En ambos casos, necesita tener un enfoque coherente para garantizar que el sistema operativo sea seguro durante el lanzamiento y se mantenga de forma continua. Con herramientas de infraestructura como código (IaC), como [AWS CloudFormation](#), puede lograr la coherencia de la seguridad de la imagen. Para las soluciones de SAP basadas en HANA, [AWS Launch Wizard](#) para SAP simplifica el proceso de instalación, incluidos los scripts

previos y posteriores a la instalación que se pueden personalizar para automatizar la instalación de los componentes de seguridad.

Consulte la guía de AWS Well-Architected Framework [pilar de seguridad] sobre la protección de los recursos de computación, específicamente la información sobre cómo realizar la administración de vulnerabilidades y reducir la superficie expuesta a ataques, para obtener detalles adicionales.

- Well-Architected Framework [seguridad]: [Protección de recursos informáticos](#)

Sugerencia 6.2.2: determine un enfoque para mantener un sistema operativo seguro

Como se mencionó en la discusión de Well-Architected Framework [pilar de seguridad] sobre la protección de la computación, si el sistema operativo elegido es compatible con EC2 Image Builder, puede simplificar la creación, prueba e implementación de sus AMI específicas de SAP y su administración continua de revisiones. También debería controlarse que AWS Systems Manager Patch Manager mantenga la posición de seguridad de su sistema operativo mediante la automatización de la aplicación de revisiones de seguridad.

- Well-Architected Framework [seguridad]: [Protección de recursos informáticos](#)
- Documentación de AWS: [EC2 Image Builder](#)
- Documentación de AWS: [AWS Systems Manager Patch Manager](#)

Sugerencia 6.2.3: revise las recomendaciones de seguridad adicionales aplicables a su sistema operativo

Determine la lista completa de elementos que se requieren para fortalecer el sistema operativo subyacente al software de SAP. Por ejemplo, los permisos del sistema de archivos en los sistemas basados en Linux deben configurarse siguiendo las pautas de SAP. Por otro lado, limitar el acceso a grupos de administradores es una práctica recomendada en los sistemas basados en Windows.

Las siguientes recomendaciones específicas de SAP pueden ser relevantes para su entorno:

- Documentación de SAP: [SAP NetWeaver Security Guide - Operating System Security \(Guía de seguridad de SAP NetWeaver: seguridad del sistema operativo\)](#)

Sistema operativo	Guía
Todos los sistemas operativos de UNIX/Linux compatibles	<ul style="list-style-type: none"> <li>Documentación de SAP: <a href="#">SAP System Security Under UNIX/LINUX (Seguridad del sistema SAP en sistemas operativos UNIX/LINUX)</a></li> </ul>
SUSE Linux Enterprise Server	<ul style="list-style-type: none"> <li>Notas de SAP: <a href="#">2684254 - SAP HANA DB: Recommended OS settings for SLES 15 / SLES for SAP Applications 15 (SAP HANA DB: configuración recomendada del sistema operativo para SLES 15/SLES y para aplicaciones SAP 15)</a> [Se necesita acceso al portal de SAP]</li> <li>Notas de SAP: <a href="#">2578899 - SUSE Linux Enterprise Server 15: Installation Note (SUSE Linux Enterprise Server 15: indicaciones de instalación)</a> [Se necesita acceso al portal de SAP]</li> <li>Documentación específica del sistema operativo: <a href="#">SUSE Hardening Guide (Guía del fortalecimiento de seguridad de SUSE)</a></li> </ul>
Red Hat Enterprise Linux	<ul style="list-style-type: none"> <li>Notas de SAP: <a href="#">2777782 - SAP HANA DB: Recommended OS Settings for RHEL 8 (SAP HANA DB: configuración recomendada del sistema operativo para RHEL 8)</a> [Se necesita acceso al portal de SAP]</li> <li>Notas de SAP: <a href="#">2772999 - Red Hat Enterprise Linux 8.x: Installation and Configuration (Red Hat Enterprise Linux 8.x: instalación y configuración)</a> (con mención particular del soporte de SELinux) [Se necesita acceso al portal SAP]</li> </ul>
Microsoft Windows	<ul style="list-style-type: none"> <li>Documentación de SAP: <a href="#">SAP System Security on Windows (Seguridad del sistema SAP en Windows)</a></li> <li>Notas de SAP: <a href="#">1837765 - Security policies for &lt;SID&gt;adm and SAPService&lt;SID&gt; on Windows (Políticas de seguridad para &lt;SID&gt;adm y SAPService&lt;SID&gt; en Windows)</a> [Se necesita acceso al portal de SAP]</li> </ul>
Oracle Enterprise Linux	<ul style="list-style-type: none"> <li>(Consulte la documentación de SAP o del proveedor a modo de guía)</li> </ul>

Sugerencia 6.2.4: valide la posición de seguridad del sistema operativo

Una vez que el sistema operativo se haya implementado y revisado de manera segura, la validación de la posición de seguridad del sistema operativo garantizará que el sistema operativo mantenga un nivel alto y continuo de seguridad sin vulneraciones. Considere automatizar esta validación utilizando software de terceros de protección contra intrusiones en el host, de detección de intrusiones, de antivirus y de firewall del sistema operativo.

Para más información, consulte la siguiente información:

- Well-Architected Framework [seguridad]: [Operación segura](#)
- Well-Architected Framework [seguridad]: [Detección](#)
- Well-Architected Framework [seguridad]: [Protección de recursos informáticos](#)

### Práctica recomendada 6.3: proteja la base de datos y la aplicación

La vigilancia de la seguridad es imperativa en las capas de la base de datos y de la aplicación, ya que un actor malicioso que obtenga acceso incluso a un nivel donde solo se puedan hacer operaciones de lectura podría poner en riesgo la seguridad de los datos críticos de la empresa. En todos los casos, siga las prácticas recomendadas estándar de SAP para la protección del acceso a la base de datos y para garantizar la seguridad de las aplicaciones. Estas prácticas aplican tanto a las instalaciones como a la infraestructura basadas en la nube, y existen guías para cada base de datos subyacente compatible para los sistemas SAP.

Sugerencia 6.3.1: siga las pautas de SAP sobre la seguridad de la base de datos para su base de datos predilecta

Consulte los siguientes recursos para obtener las pautas apropiadas:

Base de datos	Documentación
SAP HANA	<ul style="list-style-type: none"><li>• Documentación de AWS: <a href="#">Seguridad de SAP HANA on AWS</a></li><li>• Documentación de SAP: <a href="#">SAP HANA Security Guide (Guía de seguridad de SAP HANA)</a></li><li>• Documentación de SAP: <a href="#">SAP HANA Administration Guide (Guía de administración de SAP HANA)</a></li><li>• Notas de SAP: <a href="#">2159014 - FAQ: SAP HANA Security (Preguntas frecuentes: seguridad de SAP HANA)</a> [Se necesita acceso al portal de SAP]</li></ul>



Base de datos	Documentación
SAP ASE	Documentación de SAP: <a href="#">Security Administration in SAP ASE (Administración de seguridad en SAP ASE)</a>
IBM Db2	(Consulte la documentación de SAP o del proveedor a modo de guía)
Oracle	Documentación de SAP: <a href="#">SAP Database Guide - Oracle (Guía de base de datos de SAP: Oracle)</a>
Microsoft SQL Server	Notas de SAP: <a href="#">3019299 - Security Audit Questions or Security Customization in NetWeaver and SQL Server systems (Preguntas sobre auditoría o personalización de la seguridad en sistemas de NetWeaver y de SQL Server)</a> [Se necesita acceso al portal de SAP]
SAP MaxDB	Documentación de SAP: <a href="#">SAP MaxDB Security Guide (Guía de seguridad de SAP MaxDB)</a>

Sugerencia 6.3.2: siga las guías de SAP sobre la seguridad de las aplicaciones

En el caso de las soluciones basadas en SAP NetWeaver, puede encontrar orientación prescriptiva en la Guía de seguridad de SAP NetWeaver.

- Documentación de SAP: [ABAP Platform Security Guide](#)

Práctica recomendada 6.4: establezca un plan para actualizar y revisar todo el software aplicable.

SAP y los proveedores de los sistemas operativos y las bases de datos subyacentes publican actualizaciones de seguridad estándar de acuerdo con una programación definida y brindan actualizaciones de emergencia para corregir vulnerabilidades. Manténgase al tanto de la información en materia de seguridad más reciente de cada proveedor. Recomendamos que mantenga su aplicación SAP y todos sus componentes subyacentes actualizados con las últimas correcciones de seguridad de manera planificada para evitar brechas de seguridad. También recomendamos que establezca un plan para aplicar correcciones de emergencia cuando se publiquen revisiones de seguridad fundamentales.

Sugerencia 6.4.1: suscríbase a las alertas de los proveedores de soluciones de sistemas operativos, bases de datos y software.

Si se suscribe a los portales de sus diversos proveedores para obtener actualizaciones de seguridad, podrá estar al tanto de nuevos problemas de seguridad y de sus soluciones a medida que se publican. Esto puede ayudarlo a planificar los cambios requeridos.

- Documentación de AWS: [Boletines de seguridad de AWS](#)
- Documentación de SAP: [SAP EarlyWatch Alert](#)
- Documentación de SAP: [SAP Security News](#)

Sistema operativo	Guía
SUSE Linux Enterprise Server	<a href="#">SUSE Update Advisories</a>
Red Hat Enterprise Linux	<a href="#">Red Hat Security Advisories</a>
Microsoft Windows	<a href="#">Microsoft Security Alerts</a>
Oracle Enterprise Linux	<a href="#">Oracle Security Alerts</a>

Sugerencia 6.4.2: revise los cambios recomendados, el riesgo que suponen para su empresa y el esfuerzo de implementación

Los equipos de SAP deben aprender a buscar un equilibrio entre la necesidad de maximizar los tiempos de disponibilidad (uptime) del sistema y la importancia de aplicar cambios recomendados a fin de mejorar la seguridad de SAP. No hacerlo puede dar lugar a riesgos innecesarios, como interrupciones del servicio, impacto financiero o pérdida de productividad. Revise los cambios recomendados y los pasos de implementación para reparar las vulnerabilidades de sus proveedores y planee implementarlos de inmediato. Esto se relaciona directamente con las prácticas recomendadas del pilar de excelencia operativa que se trataron en este enfoque, sobre todo, con la creación de manuales de procedimientos de seguridad.

- SAP Lens [excelencia operativa]: [Sugerencia 3.4.1: cree manuales de procedimientos específicos de operaciones de seguridad de SAP](#)

Sugerencia 6.4.3: establezca un plan para tratar vulnerabilidades de manera oportuna.

Aplicar nuevas recomendaciones de seguridad de SAP y revisiones relacionadas con la seguridad lo más rápido posible es fundamental tanto para las soluciones de SAP basadas en AWS como para aquellas que se instalan en otros lugares. Revise con regularidad [SAP Security Notes and News \(Noticias y notas de seguridad de SAP\)](#) y cree un proceso para solucionar los problemas de seguridad rápidamente con las revisiones, notas y recomendaciones que se encuentran allí. En algunos casos, es posible que los administradores de SAP también deban implementar medidas temporales de control o mitigación hasta que se puedan tratar las vulnerabilidades subyacentes. Siga también las recomendaciones del pilar de seguridad que tratan sobre la respuesta a incidentes.

- Well-Architected Framework [seguridad]: [Respuesta a incidentes](#)
- Documentación de SAP: [SAP Security Notes and News](#)

## 7. Controle el acceso a sus cargas de trabajo de SAP a través de la identidad y los permisos

¿Cómo controla el acceso a su carga de trabajo de SAP? Utilice mecanismos proporcionados por AWS, SAP y demás proveedores externos para garantizar que los usuarios finales y los sistemas de interfaz estén correctamente identificados y autenticados. ¿Cómo se controlan los permisos para garantizar el privilegio mínimo? ¿Cómo se audita e informa el acceso? Empiece por identificar sus categorías de usuario y luego defina sistemáticamente los controles y su enfoque de administración de identidad para limitar el acceso a su carga de trabajo de SAP.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 7.1	Obligatorio	Comprenda sus categorías de usuario de SAP y los mecanismos de acceso
<input type="checkbox"/> Práctica recomendada 7.2	Obligatorio	Administre el acceso privilegiado para su carga de trabajo de SAP

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 7.3	Obligatorio	Comprenda el enfoque de administración de identidad de su organización y cómo se aplica a SAP
<input type="checkbox"/> Práctica recomendada 7.4	Altamente recomendado	Implemente la creación de registros e informes cuando accedan usuarios y cuando se produzcan cambios en la autorización o eventos relacionados con esta

## Práctica recomendada 7.1: comprenda sus categorías de usuario de SAP y los mecanismos de acceso

Los tipos de usuarios que acceden a su sistema SAP determinarán los controles de seguridad que debe aplicar. Al examinar cada caso de uso, puede desarrollar una estrategia. Esto debe incluir cómo administra las identidades, la autenticación, las herramientas y los mecanismos para respaldar esos requisitos.

Sugerencia 7.1.1: comprenda los permisos de acceso a los datos y las acciones permitidas

Los sistemas SAP a menudo contienen datos empresariales altamente confidenciales. A medida que define los tipos de usuarios, comprenda los permisos de acceso a los datos. (Por ejemplo, un usuario de una base de datos administrativa no tiene los controles pormenorizados de un usuario de la aplicación y, por lo tanto, puede ser más crítico). Consulte también [seguridad] [Práctica recomendada 5.2: clasifique los datos dentro de las cargas de trabajo de SAP](#).

Considere las siguientes preguntas en relación con su acceso al sistema SAP:

- ¿Las medidas que toma un usuario administrativo o de servicio deben poder rastrearse hasta un individuo identificable de manera única?
- ¿En qué capa de la aplicación se otorgará el acceso?
- ¿Puede restringir el acceso a un subconjunto de funcionalidades con ayuda de permisos?
- ¿Puede restringir el acceso a un subconjunto de funcionalidades a través de otros controles, por ejemplo, exponiendo solo ciertos servicios?
- ¿Existe un requisito para auditar las medidas tomadas?

Sugerencia 7.1.2: comprenda la red o la ubicación desde la cual los usuarios accederán a los sistemas SAP

La red o la ubicación a menudo contribuyen al perfil de riesgo de seguridad y pueden determinar si el usuario se considera de confianza o no. Por lo general, esto se combina con los controles para evitar el acceso no autorizado (consulte [Práctica recomendada 6.1: asegúrese de que la seguridad y la auditoría estén integradas en el diseño de la red de SAP](#) ).

Esto puede repercutir en su diseño. Por ejemplo, un usuario o dispositivo de Internet que no sean de confianza pueden requerir factores de autenticación adicionales para acceder a su carga de trabajo de SAP, en comparación con un usuario de confianza de su red corporativa.

## Práctica recomendada 7.2: administre el acceso privilegiado a su carga de trabajo de SAP

Adopte un enfoque de privilegio mínimo cuando sea posible. Otorgue solo el acceso mínimo que se necesita para llevar a cabo un rol específico a un conjunto reducido de usuarios mientras administra la utilidad y la eficiencia. Existen cuentas administrativas (por ejemplo, <sid>adm) que, de manera predeterminada, tienen acceso para afectar significativamente la fiabilidad o la seguridad de los datos de su carga de trabajo de SAP. Considere cómo puede limitar este riesgo.

### Sugerencia 7.2.1: administre la autenticación y las credenciales de AWS

AWS Identity and Access Management (IAM) permite administrar el acceso a los servicios y recursos de AWS de manera segura. Con IAM, puede crear y administrar usuarios y grupos de AWS para diferentes tareas de administración de SAP y de la nube. Utilice los permisos de IAM para permitir y denegar el acceso de los usuarios a los recursos de AWS. Se debe seguir la orientación estándar, en particular, restringir y asegurar el acceso privilegiado (raíz).

- Documentación de AWS: [Prácticas recomendadas de seguridad en IAM](#)

En el caso del acceso que no está asignado a un usuario, pero que es necesario para la operación de la aplicación SAP, sea lo suficientemente precavido de conceder privilegios mínimos.

- Documentación de AWS: [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2](#)

### Sugerencia 7.2.2: administre la autenticación y las credenciales de SAP

Implemente un proceso para aprobar y otorgar permisos elevados solo cuando sea necesario, por un tiempo limitado. Utilice la funcionalidad de auditoría que se encarga de determinar a quién y por qué se concedió el acceso.

Restrinja el uso de nombres de usuario o de contraseñas a cuentas privilegiadas. Desactive el acceso directo cuando sea posible. Almacene las credenciales de forma segura, por ejemplo, con ayuda de una solución de administración de acceso privilegiado o un almacén de contraseñas.

Evalúe cómo se podría utilizar Systems Manager para restringir el acceso directo al sistema operativo a tareas específicas utilizando manuales de procedimientos, RunCommand y Secrets Manager.

- Documentación de AWS: [Restricción del acceso a los comandos de nivel raíz a través de SSM Agent](#)
- Documentación de AWS: [Referencia a los secretos de AWS Secrets Manager desde los parámetros de Parameter Store](#)

### Práctica recomendada 7.3: comprenda el enfoque de administración de identidad de su organización y cómo se aplica a SAP

Las cargas de trabajo típicas de SAP consistirán en múltiples sistemas y, por lo tanto, múltiples identidades. Un enfoque centralizado para administrar estos usuarios puede reducir el riesgo de seguridad y la complejidad operativa. El énfasis está en cómo puede utilizar los servicios de AWS y las herramientas de terceros en su enfoque, considerando la administración centralizada de usuarios, el inicio de sesión único y la autenticación multifactor.

#### Sugerencia 7.3.1: determine un proveedor de identidad para usuarios designados

Los usuarios se asociarán con un almacén de identidades, por ejemplo, Active Directory. Dicho almacén actúa como un repositorio central para administrar información de identidad, como roles, permisos e identificadores. Determine si cada conjunto de identidades se puede asociar con un proveedor de identidad. Un proveedor de identidad le permite desvincularse de la autenticación de los usuarios. Facilita el SSO y también administra el ciclo de vida de identidad de los usuarios (por ejemplo, los que ingresan, los que se trasladan y los que se van).

Considere excepciones para usuarios designados que no están asociados con un ser humano. Esto puede incluir lotes, programación de trabajos, integración y supervisión de usuarios.

- Documentación de AWS: [AWS Directory Service | Amazon Web Services \(AWS\)](#)

### Sugerencia 7.3.2: determine los mecanismos de autenticación

Comprenda los mecanismos de autenticación admitidos (por ejemplo, SAML, Kerberos, X.509, tickets de inicio de sesión único de SAP) en cada una de las capas de su carga de trabajo de SAP. Evalúe los requisitos para integrarse con su aplicación. Siempre que sea posible, utilice el inicio de sesión único para evitar el impacto administrativo y de seguridad de administrar múltiples credenciales de usuarios.

- Documentación de SAP: [User Authentication and single sign-on \(Autenticación de usuario e inicio de sesión único\)](#)
- Documentación de AWS: [Aplicaciones de la nube: AWS Single Sign-On](#)
- Blog de SAP on AWS: [Enable SAP Single Sign On with AWS SSO Part 1: Integrate SAP NetWeaver ABAP with AWS SSO \(Habilite el SSO de SAP con AWS SSO parte 1: integre SAP NetWeaver ABAP con AWS SSO\)](#)
- Blog de SAP on AWS: [Enable SAP Single Sign On with AWS SSO Part 2: Integrate SAP NetWeaver Java \(Habilite el SSO de SAP en AWS SSO Parte 2: integre SAP NetWeaver Java\)](#)
- Blog de SAP on AWS: [Enable Single Sign On for SAP Cloud Platform Foundry and SAP Cloud Platform Neo with AWS SSO \(Habilite el SSO para SAP Cloud Platform Foundry y SAP Cloud Platform Neo con AWS SSO\)](#)

### Sugerencia 7.3.3: considere utilizar la autenticación multifactor

La Multi-Factor Authentication (MFA, autenticación multifactor) es una práctica recomendada que añade una capa de protección adicional que se complementa con sus credenciales de inicio de sesión. Estos factores múltiples le brindan una mayor seguridad a su aplicación SAP. Entre los casos de uso, se encuentran el acceso a SAP desde un dispositivo que no es de confianza, acceso a AWS Management Console y actividades privilegiadas, como la eliminación de copias de seguridad o la terminación de instancias de EC2.

- Blog de SAP on AWS: [Securing SAP Fiori with MFA \(Protección de SAP Fiori con MFA\)](#)
- Documentación de AWS: [Uso de dispositivos MFA con la página de inicio de sesión de IAM:AWS Identity and Access](#)
- Documentación de AWS: [Configuración de la eliminación de MFA: Amazon Simple Storage Service](#)
- Documentación de AWS: [Amazon EC2: Requiere MFA \(GetSessionToken\) para operaciones EC2 específicas](#)

### Sugerencia 7.3.4: determine el enfoque para la administración de certificados

Los certificados basados en el cliente se pueden utilizar para la autenticación sin la necesidad de credenciales. Determine un enfoque que incluya el vencimiento basado en el tiempo para la administración de sesiones y la rotación de certificados para la comunicación entre sistemas. AWS brinda una autoridad de certificación en la que confía SAP. Los certificados se pueden emitir y administrar utilizando [AWS Certificate Manager \(ACM\)](#) .

- Notas de SAP: [2801396 - SAP Global Trust List \(Lista de confianza global de SAP\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [3040959 - How to get a CA signed server certificate in ABAP \(¿Cómo obtener un certificado de servidor firmado por CA en ABAP?\)](#) [Se necesita acceso al portal de SAP]
- SAP Lens [excelencia operativa]: [Sugerencia 3.4.1: cree manuales de procedimientos específicos de operaciones de seguridad de SAP](#)
- SAP Lens [excelencia operativa]: [Sugerencia 4.1.2: lleve un calendario del vencimiento de las credenciales, los certificados y las licencias](#)

### Práctica recomendada 7.4: implemente la creación de registros e informes cuando accedan usuarios y cuando se produzcan cambios en la autorización o eventos relacionados con esta

Los eventos de acceso y autorización de usuarios en sus sistemas SAP deben registrarse, analizarse y auditarse con regularidad. Consolide y correlacione los eventos de seguridad de sus aplicaciones y base de datos de SAP con otros componentes de su arquitectura. De esta forma, podrá permitir el seguimiento de extremo a extremo en caso de un problema de seguridad crítico o una vulneración. Automatice el análisis de eventos en un sistema central de Security Information and Event Management (SIEM, información de seguridad y administración de eventos). Así podrá permitir que su equipo de operaciones comprenda si ocurre alguna actividad inesperada o sospechosa fuera de los límites de los controles normales del sistema. Luego su equipo podrá aportar soluciones según sea necesario.

#### Sugerencia 7.4.1: registre eventos de AWS Identity and Access Management (IAM)

Considere mantener un registro histórico de los eventos de IAM en AWS. Esto se puede utilizar en la detección o auditoría de cambios de usuario y autorización dentro de las cuentas de AWS. Determine su período de retención de registros y los tipos de eventos por registrar en función de las políticas de seguridad requeridas por sus organizaciones.



Permita que su equipo de operaciones responda preguntas de auditoría relacionadas con la infraestructura de su sistema SAP:

- ¿Quién creó la nueva consola de AWS o el nuevo usuario de la CLI y cuándo se hizo?
- ¿Quién modificó el rol de IAM de AWS y cuándo se hizo?
- ¿Cuándo fue la última vez que el usuario de AWS inició sesión con éxito?
- ¿Hay una cantidad sospechosa de intentos de inicio de sesión fallidos en la cuenta de AWS?

Para obtener más información, considere consultar los siguientes recursos:

- Documentación de AWS: [Prácticas recomendadas de IAM: monitorice la actividad en su cuenta de AWS](#)
- Documentación de AWS: [Registro de llamadas a la API de AWS STS y de IAM con AWS CloudTrail](#)
- AWS Well-Architected Framework [seguridad]: [Detección](#)
- Blog de seguridad de AWS: [Visualizing Amazon GuardDuty findings \(Visualización de hallazgos de Amazon GuardDuty\)](#)

Sugerencia 7.4.2: registre los cambios de usuario y de autorización en su sistema operativo

Considere mantener un registro histórico de los eventos relacionados con los usuarios y la autorización del sistema operativo, de modo que se puedan utilizar en la detección o la auditoría. Determine su período de retención de registros y los tipos de eventos por registrar en función de las políticas de seguridad requeridas por sus organizaciones.

Permita que su equipo de operaciones responda preguntas de auditoría relacionadas con el sistema operativo de su sistema SAP:

- ¿Quién creó la nueva cuenta del sistema operativo del superusuario y cuándo se hizo?
- ¿Quién modificó los permisos de la cuenta del sistema operativo y cuándo se hizo?
- ¿Cuándo fue la última vez que el usuario del sistema operativo inició sesión con éxito?
- ¿Hay una cantidad sospechosa de intentos de inicio de sesión fallidos en la cuenta del sistema operativo?
- ¿Cuándo fue la última vez que el usuario de su sistema operativo utilizó permisos elevados?

Para obtener más información sobre la auditoría en el sistema operativo, considere consultar los siguientes recursos:

Sistema operativo	Guía
SUSE Linux Enterprise Server	<a href="#">Setting Up the Linux Audit Framework   Security Guide (Configuración del marco de auditoría de Linux   Guía de seguridad)</a>
Red Hat Enterprise Linux	<a href="#">Capítulo 14. Auditing the system Red Hat Enterprise Linux 8   Security Guide (Auditoría del sistema Red Hat Enterprise Linux 8   Guía de seguridad)</a>
Microsoft Windows	<a href="#">Recomendaciones de la directiva de auditoría</a>
Oracle Enterprise Linux	<a href="#">Oracle Linux 8 Enhancing System Security - Auditing and Monitoring (Oracle Linux 8 Mejora de la seguridad del sistema: auditoría y supervisión)</a>

Sugerencia 7.4.3: registre los eventos de autorización y de usuarios de la base de datos y de la aplicación SAP

Considere mantener un registro histórico de los eventos de autorización y de usuarios de SAP, de modo que puedan utilizarse en detección o auditoría. Considere tanto la pila de aplicaciones (por ejemplo, autorizaciones de ABAP) como su base de datos (por ejemplo, SAP HANA). Determine su período de retención de registros y los tipos de eventos por registrar en función de las políticas de seguridad requeridas por sus organizaciones.

Permita que su equipo de operaciones responda preguntas de auditoría sobre la aplicación y la base de datos de SAP en el caso de que se produzcan eventos como los que se detallan a continuación:

- ¿Quién creó la nueva cuenta de SAP o de la base de datos y cuándo se hizo?
- ¿Quién modificó los permisos de la cuenta de SAP o de la base de datos y cuándo se hizo?
- ¿Cuándo fue la última vez que el usuario de SAP o de la base de datos inició sesión con éxito?
- ¿Hay una cantidad sospechosa de intentos de inicio de sesión fallidos en la cuenta?
- ¿Qué códigos de transacción confidenciales o herramientas utilizó la cuenta por última vez?

Para obtener más información, considere consultar los siguientes recursos:

- Documentación de SAP: [SAP Access Control and Governance | User Access \(Control de acceso y gobernanza de SAP | Acceso de usuario\)](#)
- Documentación de SAP: [SAP NetWeaver ABAP: The Security Audit Log \(SAP NetWeaver ABAP: el registro de auditoría de seguridad\)](#)
- Documentación de SAP: [SAP NetWeaver JAVA: The Security Audit Log \(SAP NetWeaver JAVA: el registro de auditoría de seguridad\)](#)
- Documentación de SAP: [SAP HANA: Auditing Activity in SAP HANA \(SAP HANA: actividad de auditoría en SAP HANA\)](#)

Sugerencia 7.4.4: consolide los eventos de usuarios y de autorización en un sistema de SIEM para su análisis

Considere enviar todos los eventos relacionados con los usuarios y con la autorización que ocurren en los componentes de la carga de trabajo de SAP a una herramienta de SIEM central para permitir la correlación y el análisis. Utilice herramientas como SAP Enterprise Threat Detection o complementos de terceros, o envíe directamente sus registros de auditoría de SAP desde sus servidores de aplicaciones y bases de datos a una herramienta de análisis y procesamiento de datos.

Establezca comportamientos de referencia para su carga de trabajo y supervise las anomalías para mejorar la detección de incidentes de seguridad.

Considere utilizar [las soluciones de SIEM de AWS Marketplace](#) para supervisar su carga de trabajo en tiempo real, identificar problemas de seguridad y acelerar el análisis y la corrección de la causa raíz.

Para obtener más información, considere los siguientes recursos:

- AWS Marketplace: [Soluciones de SIEM](#)
- Documentación de AWS: [AWS Security Hub](#)
- Documentación de SAP: [SAP Enterprise Threat Detection](#)
- Well-Architected Framework [seguridad]: [Respuesta ante incidentes](#)
- Documentación de AWS: [AWS Security Incident Response Guide \(Respuesta ante incidentes de seguridad de AWS: documento técnico\)](#)

## 8. Proteja sus datos de SAP en reposo y en tránsito

¿Cómo protege sus datos de SAP? Los sistemas SAP a menudo ejecutan las funciones principales dentro de una empresa y almacenan datos empresariales privados. La práctica que se recomienda emplear es cifrar los datos en reposo y en tránsito utilizando al menos un mecanismo de cifrado para cumplir con los requisitos y controles de seguridad internos o externos. Además de los controles enumerados en el [Modelo de responsabilidad compartida de AWS](#), AWS brinda múltiples soluciones de cifrado. Muchos servicios de AWS tienen características que le permiten habilitar el cifrado con un mínimo esfuerzo e impacto en el rendimiento. Le recomendamos considerar opciones de cifrado disponibles para la base de datos y la capa de la aplicación SAP.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 8.1	Altamente recomendado	Cifre los datos en reposo
<input type="checkbox"/> Práctica recomendada 8.2	Altamente recomendado	Cifre los datos en tránsito
<input type="checkbox"/> Práctica recomendada 8.3	Altamente recomendado	Proteja sus mecanismos de recuperación de datos para resguardarse contra amenazas

### Práctica recomendada 8.1: cifre los datos en reposo

Los datos en reposo se refieren a cualquier dato almacenado digitalmente. Utilizamos el cifrado para garantizar que solo los usuarios autorizados puedan ver estos datos y para que permanezcan protegidos cuando el acceso al almacenamiento o a la base de datos se vea comprometido independientemente de la aplicación.

Sugerencia 8.1.1: defina en qué niveles se aplicará el cifrado

En general, cuanto más arriba en la pila implemente su cifrado, más seguros estarán sus datos. Este aumento de seguridad va acompañado de una complejidad adicional para la implementación y supervisión. AWS recomienda utilizar las opciones de cifrado en reposo disponibles dentro de sus servicios. Considere implementar un cifrado adicional del sistema operativo o de la base de datos cuando sea necesario, como se define en [seguridad]: [Práctica recomendada 5.3: evalúe la necesidad de aplicar controles de seguridad específicos para sus cargas de trabajo de SAP](#).

Sugerencia 8.1.2: comprenda las opciones de cifrado de AWS para los servicios y las soluciones de SAP

Los servicios fundamentales de AWS que SAP utiliza para los datos en reposo son Amazon EC2 (AMI y los volúmenes de EBS), Amazon FSx for Windows File Server o Amazon EFS para sistemas de archivos compartidos y Simple Storage Service (Amazon S3) para copias de seguridad u otros casos de uso del almacén de objetos.

- Documentación de AWS: [Cifrado con AMI respaldadas por EBS](#)
- Documentación de AWS: [Cifrado de Amazon EBS](#)
- Documentación de AWS: [Cifrado de Amazon EFS](#) / [Cifrado de Amazon FSx](#)
- Documentación de AWS: [Cifrado de Simple Storage Service \(Amazon S3\)](#)

Los datos almacenados en estos servicios se pueden cifrar en reposo mediante AWS o claves administradas por el cliente desde AWS KMS.

Las opciones de cifrado del sistema operativo incluyen BitLocker, DM-crypt y SuSE Remote Disk.

En los siguientes enlaces, podrá encontrar información sobre distintas opciones de cifrado de su base de datos:

Base de datos	Guía
SAP HANA	Documentación de SAP: <a href="#">Server-Side Data Encryption Services (Servicios de cifrado de datos del lado del servidor)</a>
SAP ASE	Documentación de SAP: <a href="#">SAP ASE Overview of Encryption (Información general de SAP ASE sobre el cifrado)</a>
IBM Db2	Documentación de IBM: <a href="#">Db2 Encryption Overview (Información general del cifrado de Db2)</a>

Base de datos	Guía
Oracle	Notas de SAP: <a href="#">2591575 - Using Oracle Transparent Data Encryption (TDE) with SAP NetWeaver (Uso del cifrado de datos transparente (TDE) de Oracle con SAP NetWeaver)</a> [Se necesita acceso al portal de SAP]
Microsoft SQL Server	Notas de SAP: <a href="#">1380493 - SQL Server Transparent Data Encryption (TDE) (Cifrado de datos transparente (TDE) de SQL Server)</a> [Se necesita acceso al portal de SAP]
SAP MaxDB	Documentación de SAP: <a href="#">SAP MaxDB Database Administration - Encryption (Administración de base de datos de SAP MaxDB: cifrado)</a>

### Sugerencia 8.1.3: defina métodos de cifrado y almacenes de administración de claves

Generalmente, la administración de claves se define a nivel empresarial y, de esta forma, se determinará qué opciones de administración de claves se pueden utilizar con sus cargas de trabajo de SAP. AWS KMS es un servicio resiliente y seguro para simplificar la administración de claves de cifrado para los servicios de AWS. Si necesita administrar sus propios módulos de seguridad del hardware (HSM), puede utilizar AWS CloudHSM.

- Documentación de AWS: [Opciones de servicio y herramientas de cifrado de AWS](#)
- Documentación de AWS: [AWS Key Management Service \(AWS KMS\)](#)
- Documentación de AWS: [AWS CloudHSM](#)

Considere también mecanismos para proteger las claves maestras. ¿Cómo restringe el acceso, administra la rotación y garantiza la capacidad de recuperación de las claves?

Debe estar al tanto de que las claves raíz de cifrado de datos en reposo de HANA solo se pueden almacenar de forma segura en el almacén seguro de la instancia dentro del sistema de archivos (Instancia SSFS) o dentro de la solución de SaaS SAP Data Custodian. Si utiliza el almacén de instancias, la clave maestra podría almacenarse en [AWS Secrets Manager](#) con una política de rotación.

- Notas de SAP: [2154997 - Migration of hdbuserstore entries to ABAP SSFS \(Migración de entradas de hdbuserstore a ABAP SSFS\)](#) [Se necesita acceso al portal de SAP]

- Notas de SAP: [2755815 - How to Ensure Recoverability of Hana's Data-At-Rest Encryption \(¿Cómo garantizar la capacidad de recuperación del cifrado de datos en reposo de Hana?\)](#) [Se necesita acceso al portal de SAP]

## Práctica recomendada 8.2: cifre los datos en tránsito

El uso del cifrado de datos en tránsito hace que sea más difícil interceptar, acceder o manipular sus datos mientras se mueven de un punto a otro. Asegúrese de que existan protocolos seguros y cifrado a nivel de red para minimizar amenazas potenciales y brindar un nivel de protección acorde con sus requisitos.

Well-Architected Framework [seguridad]: [Protección de los datos en tránsito](#)

Sugerencia 8.2.1: cifre el tráfico de aplicaciones de acuerdo con los protocolos de SAP y de base de datos

En el caso del tráfico de aplicaciones que utiliza protocolos de SAP (SAPGUI Dialog, RFC, y CPIC), utilice SAP SNC para garantizar la seguridad de la capa de transporte.

- Documentación de SAP: [SNC-Protected Communication Paths in SAP Systems \(Rutas de comunicación protegidas por SNC en sistemas SAP\)](#)

En el caso del tráfico de la base de datos, utilice una conexión segura entre el cliente y la base de datos cuando esté disponible.

Base de datos	Guía
SAP HANA	Documentación de SAP: <a href="#">SAP HANA: Securing Data Communication (SAP HANA: protección de la comunicación de datos)</a>
SAP ASE	Documentación de SAP: <a href="#">SSL in SAP ASE (SSL en SAP ASE)</a>
IBM Db2	Notas de SAP: <a href="#">2385640 - DB6: database connection using SSL encryption (DB6: conexión de base de datos mediante cifrado SSL)</a> [Se necesita acceso al portal de SAP]
Oracle	Notas de SAP: <a href="#">973450 - Oracle Database network encryption and data integrity (Cifrado de red e integridad de datos de la base de datos de Oracle)</a> [Se necesita acceso al portal de SAP]

Base de datos	Guía
Microsoft SQL Server	Notas de SAP: <a href="#">1570930 - SQL Server network encryption with SAP (Cifrado de red de SQL Server con SAP)</a> [Se necesita acceso al portal de SAP]
SAP MaxDB	Documentación de SAP: <a href="#">MaxDB Network and Communication (Comunicación y red de MaxDB)</a>

Sugerencia 8.2.2: cifre el tráfico de aplicaciones SAP según los protocolos de Internet

Para el tráfico de aplicaciones basadas en protocolos de Internet (HTTP, P4 (RMI), LDAP), utilice SSL/TLS para garantizar la seguridad de la capa de transporte (TLS).

- Documentación de SAP: [Transport Layer Security \(Seguridad de la capa de transporte\)](#)

Sugerencia 8.2.3: cifre el intercambio de datos basado en protocolos de transferencia de archivos o transferencia de mensajes

En lo que respecta a las transferencias de archivos, AWS pone a su disposición el servicio AWS Transfer Family para el intercambio seguro de archivos a través de SFTP o FTPS. AWS Transfer Family admite la transferencia de datos hacia y desde Amazon S3 y Amazon EFS.

- Documentación de AWS: [AWS Transfer Family](#)

El uso de comprobaciones de integridad de datos a nivel de mensaje ayuda a garantizar que los datos no se alteren mientras se transfieren. Considere utilizar uno o más de los estándares de seguridad de mensajes compatibles con SAP para firmar y verificar la integridad de los datos en los mensajes.

- Documentación de SAP: [SAP ABAP Web Services Message-Level Security \(Seguridad a nivel de mensaje de SAP ABAP Web Services\)](#)
- Documentación de SAP: [SAP NetWeaver Process Integration Security Guide \(Guía de seguridad de integración de procesos de SAP NetWeaver\)](#)
- Documentación de SAP: [SAP Cloud Integration Message-Level Security \(Seguridad a nivel de mensaje de SAP Cloud Integration\)](#)



En el caso de los mensajes basados en IDOC, utilice SNC para proteger la conexión RFC que utiliza ALE.

- Documentación de SAP: [Handling Sensitive Data in IDocs \(Manipulación de información confidencial en IDocs\)](#)

#### Sugerencia 8.2.4: cifre el acceso administrativo

Es frecuente utilizar herramientas basadas en Windows y SSH para la administración de SAP. Además de emplear controles de seguridad como hosts bastión, considere, en la medida de lo posible, cifrar este tráfico.

Como alternativa, [AWS Systems Manager Session Manager](#) brinda un mecanismo seguro para acceder al sistema operativo a través de AWS Management Console utilizando TLS para el cifrado.

- Documentación de AWS: [Guía de Windows de Amazon EC2: cifrado en tránsito](#)
- Documentación de AWS: [Guía de Linux para Amazon EC2: cifrado en tránsito](#)
- Documentación de AWS: [Protección de datos en AWS Systems Manager: cifrado de datos](#)

#### Sugerencia 8.2.5: evalúe las características de los servicios de AWS que permiten el cifrado en tránsito

Además del cifrado basado en aplicaciones, muchos servicios de AWS brindan capacidades de cifrado en tránsito. Evalúe sus estándares corporativos, el esfuerzo de implementación y los beneficios asociados para cada servicio. Los siguientes son algunos ejemplos que son relevantes para las cargas de trabajo de SAP.

- Documentación de AWS: [Simple Storage Service \(Amazon S3\): cifrado en tránsito](#) - Activado de forma predeterminada y recomendado para copias de seguridad de Simple Storage Service (Amazon S3).
- Documentación de AWS: [Amazon EFS: cifrado en tránsito](#) / [Amazon FSx](#) - Puede ser necesario para los sistemas de archivos compartidos.
- Documentación de AWS: [Elastic Load Balancing](#) - Revise sus requisitos de cifrado y si se requiere TLS de extremo a extremo con transferencia, ya que esta característica no esté disponible para todos los tipos de equilibradores de carga.
- Documentación de AWS: [Amazon EC2: cifrado en tránsito](#) - Solo tipos de instancias de generaciones posteriores tienen esta característica.

### Sugerencia 8.2.6: implemente cifrado a nivel de red

Los clientes de SAP normalmente utilizarán tanto Direct Connect o una combinación de Direct Connect y VPN para brindar conectividad confiable para sus recursos en AWS.

AWS Direct Connect no cifra su tráfico en tránsito. Si se requiere cifrado, se debe implementar el cifrado de nivel de transporte, por ejemplo, utilizando una VPN para Direct Connect.

AWS brinda una VPN de sitio a sitio que se puede utilizar para el cifrado de canales de red. También puede elegir implementar soluciones de VPN de terceros como OpenVPN, que podrá encontrar en AWS Marketplace, o traer su propia licencia.

- Documentación de AWS: [AWS Managed VPN \(VPN administrada por AWS\)](#)
- Documentación de AWS: [AWS Direct Connect + VPN](#)
- Documentación de AWS: [Software Site-to-Site VPN \(Software de VPN de sitio a sitio\)](#)

### Práctica recomendada 8.3: proteja sus mecanismos de recuperación de datos para resguardarse contra amenazas

Para ayudarlo a protegerse contra actividades maliciosas, siga las pautas establecidas en el marco de seguridad de su organización. El [libro electrónico Securing your AWS Cloud environment from ransomware \(Proteger su entorno de la nube de AWS contra el ransomware\)](#) brinda información general sobre los elementos claves que se deben tratar antes de un incidente y en una respuesta ante un incidente, incluidos los controles de red, la revisión y los permisos de privilegios mínimos. En el caso de los sistemas SAP, la amenaza es similar a la de otras aplicaciones, pero el impacto es potencialmente mayor. Si SAP es un sistema de registro o se requiere para transacciones esenciales, tenga en cuenta las siguientes sugerencias para proteger una copia de seguridad contra un ataque malicioso.

- Notas de SAP: [2663467 - Tips to avoid a Ransomware situation \(Consejos para evitar una situación de ransomware\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2496239 - Ransomware / malware on Windows \(Ransomware y malware en Windows\)](#) [Se necesita acceso al portal de SAP]

### Sugerencia 8.3.1: proteja las copias de seguridad en una cuenta separada con controles adicionales

Al proteger las copias de seguridad en una cuenta aislada de la copia principal de sus datos, ya sea de forma directa o mediante replicación, es posible minimizar el riesgo de que un sistema comprometido también afecte sus mecanismos de recuperación de datos.

La cuenta secundaria se puede ver como un “búnker de datos” con requisitos de acceso coherentes con el caso de uso.

Cuando se trata de copias de seguridad realizadas con Simple Storage Service (Amazon S3), los controles adicionales pueden incluir el uso de S3 Object Lock para almacenar objetos utilizando un modelo de escritura única y de lectura múltiple (WORM) o [la eliminación con autenticación multifactor](#).

Si se recurre a la replicación, comprenda las diferentes opciones disponibles, entre las que se encuentran [la replicación de marcador de eliminación](#) (De forma predeterminada, los marcadores de eliminación no se replican) y [el control de tiempo de replicación de S3](#). Para optimizar los costos, asegúrese de que la organización se realice tanto en los buckets principales como en los secundarios.

Sugerencia 8.3.2: valide su capacidad de recuperación

Las copias de seguridad son la última línea de defensa cuando protege sus datos contra actividades maliciosas, pero pueden resultar inútiles si la recuperación no es posible debido a copias de seguridad incompletas o copias de seguridad que no son válidas. Es posible que la recuperación no sea posible si no puede acceder o descifrar las copias de seguridad. Considere cómo protege las credenciales y las claves de cifrado.

Realice pruebas de recuperación en una situación maliciosa hipotética, por ejemplo, volver a crear en una cuenta alternativa.

- SAP Lens [excelencia operativa]: [Práctica recomendada 4.3: pruebe periódicamente los planes de continuidad de la empresa y la recuperación de errores](#)

## 9. Implemente una estrategia de seguridad para registrar, probar y responder a eventos de seguridad

¿Tiene un plan de seguridad estratégico respaldado por la metodología correcta de registro, prueba y respuesta documentada? Tener un plan de seguridad estratégico ayuda a dar forma a las tareas proactivas y reactivas que se deben realizar para garantizar que todos los desafíos de seguridad se cumplan con éxito. Los procesos de registro, detección y protección adicional para ayudar

a identificar y solucionar los incidentes de seguridad en cargas de trabajo de SAP on AWS son idénticos a los que se detallan en el pilar de seguridad de Well-Architected Framework. Revise las prácticas recomendadas que se encuentran en el pilar de seguridad que abarcan la detección de incidentes y las respuestas ante ellos y complemente con la guía que se presenta en esta sección.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 9.1	Obligatorio	Comprenda su estrategia de análisis de los registros de seguridad de la base de datos y de las aplicaciones SAP
<input type="checkbox"/> Práctica recomendada 9.2	Altamente recomendado	Realice pruebas periódicas para detectar errores de seguridad
<input type="checkbox"/> Práctica recomendada 9.3	Altamente recomendado	Tenga un plan documentado para responder ante eventos de seguridad

- Well-Architected Framework [seguridad]: [Detección](#)
- Well-Architected Framework [seguridad]: [Respuesta a incidentes](#)

## Práctica recomendada 9.1: comprenda su estrategia de análisis de los registros de seguridad de la base de datos y de las aplicaciones SAP

Si los registros de seguridad no se mantienen en los niveles adecuados de granularidad, se pueden perder los datos vitales necesarios para la respuesta ante incidentes, el análisis de seguridad forense y el moldeado de amenazas. El personal de seguridad de SAP debe poder evaluar los posibles incidentes de seguridad que afectan a los sistemas SAP que cumplen con los requisitos de seguridad de su empresa. En el caso de las cargas de trabajo de SAP que se ejecutan en AWS, los servicios de AWS descritos en el pilar de seguridad de Well-Architected Framework son un punto de inicio útil junto con las siguientes sugerencias.

- Well-Architected Framework [seguridad]: [Detección: configuración](#)

Sugerencia 9.1.1: determine qué registros se requieren para detectar eventos de seguridad

En el caso de software individuales de SAP y bases de datos compatibles, consulte SAP NetWeaver Guide Finder y la guía de seguridad de SAP NetWeaver para descubrir qué registros pueden ser aplicables (por ejemplo, [registros de acceso de lectura](#) ). Le recomendamos también revisar la guía de SAP [sobre registros de seguridad](#) y los temas relacionados con las prácticas recomendadas para sus actividades de desarrollo.

- Documentación de SAP: [SAP NetWeaver Guide Finder](#)
- Documentación de SAP: [ABAP Platform Security Guide](#)
- Documentación de SAP: [Security Logging \(Registro de seguridad\)](#)

Sugerencia 9.1.2: desarrolle mecanismos para almacenar y analizar registros

Es necesario tener datos relevantes sobre posibles eventos de seguridad para cualquier instalación segura de SAP, pero es igualmente importante almacenar esos datos de forma segura y tener las herramientas necesarias para buscar y analizar los datos de manera eficiente y oportuna. Una posible opción dentro de AWS es utilizar [CloudWatch Agent](#) para almacenar registros de instancias y de aplicaciones SAP con contenido pertinente para la seguridad en un [grupo de registro de Amazon CloudWatch](#) . Dichos registros también podrían [exportarse a Simple Storage Service \(Amazon S3\)](#) para llevar a cabo un análisis integral de registros y para integrarlos con [soluciones de análisis de registros de terceros](#) .

Consulte los siguientes materiales si necesita asistencia para ensamblar, combinar y analizar sus registros de seguridad de SAP on AWS:

- SAP Lens [seguridad]: [Sugerencia 7.4.4: consolide los eventos de usuarios y de autorización en un sistema de SIEM para su análisis](#)
- Blog de SAP on AWS: [SAP HANA monitoring: A serverless approach using Amazon CloudWatch \(Supervisión de SAP HANA: un enfoque sin servidor que utiliza Amazon CloudWatch\)](#)
- Blog de SAP on AWS: [SAP Monitoring: A serverless approach using Amazon CloudWatch \(Supervisión de SAP: un enfoque sin servidor que utiliza Amazon CloudWatch\)](#)

## Práctica recomendada 9.2: realice pruebas periódicas para detectar errores de seguridad

Tal como se describe en las secciones de respuesta a incidentes del pilar de seguridad de Well-Architected Framework sobre simulaciones, confección de manuales de procedimientos y organización de simulaciones de fallos, se recomienda realizar todas estas acciones con todas las cargas de trabajo, incluidas las de SAP on AWS. Este tipo de pruebas periódicas puede identificar nuevos vectores de ataque y vulnerabilidades, así como preparar sus recursos de seguridad de SAP para una respuesta rápida y efectiva en caso de que se produzca un incidente de seguridad.

Well-Architected Framework [seguridad]: [Respuesta ante incidentes: simulación](#)

Sugerencia 9.2.1: incluya aplicaciones SAP dentro de sus blancos y realice pruebas estándar de seguridad y penetración

Las pruebas de seguridad son una parte importante del mantenimiento de un entorno seguro. Además de realizar pruebas de penetración estándar en AWS, asegúrese de incluir a su solución de SAP dentro de los posibles blancos de una actividad maliciosa. Tenga en cuenta las soluciones de software específicas de SAP que a menudo se exponen públicamente en su arquitectura, como SAProuter, Web Dispatcher, Cloud Connector y SAP Fiori.

- Documentación de AWS: [Pruebas de penetración](#)

## Práctica recomendada 9.3: tenga un plan documentado para responder ante eventos de seguridad

Sin un plan documentado para tratar un evento de seguridad que involucre sus aplicaciones SAP, la respuesta del equipo de seguridad puede demorarse o ser menos integral y efectiva tanto para mitigar el evento como para comprender su causa. Documente detalladamente los patrones de respuesta de seguridad para sus aplicaciones SAP.

Sugerencia 9.3.1: prepárese para los eventos de seguridad con la ayuda de un plan de supervisión de incidentes consignado por escrito

Esto está directamente relacionado con la guía del pilar de seguridad de AWS Well-Architected Framework sobre la preparación de respuesta a incidentes. Consulte esta documentación y asegúrese de incluir sus aplicaciones SAP:

- Well-Architected Framework [seguridad]: [Respuesta ante incidentes: preparación](#)

# Fiabilidad

El pilar de la fiabilidad incluye la capacidad de una carga de trabajo para llevar a cabo la función prevista de forma correcta y consistente en el momento esperado. Esto incluye la capacidad de operar y probar la carga de trabajo a través de su ciclo de vida completo. Para muchas empresas, contar con una buena arquitectura en pos de garantizar la fiabilidad es un requisito clave para las cargas de trabajo de SAP. Esto se debe a la vital importancia de muchas de las cargas de trabajo de SAP y a la necesidad de comprender la arquitectura de SAP y las restricciones que esto impone.

Al igual que con otros pilares, le recomendamos revisar AWS Well-Architected Framework, en especial las prácticas recomendadas relacionados con los fundamentos, la administración de cambios y la administración de errores. Al considerar la fiabilidad con SAP Lens, concéntrese primero en tener una comprensión clara y equilibrada de sus requisitos no funcionales en los sistemas individuales, incluidas las prioridades empresariales que impulsan estos requisitos. Luego, diferenciamos entre la disponibilidad y la Disaster Recovery (DR, recuperación de desastres). La disponibilidad se relaciona con situaciones en las que es posible que un usuario final continúe accediendo al sistema SAP, a pesar del error de un componente. Por el contrario, en una situación en la que toda la carga de trabajo deja de estar disponible, se declararía un evento de DR.

## 10. Diseñe para tolerar errores

¿Cómo diseña su carga de trabajo de SAP para tolerar errores? Trabaje a partir de los requisitos de su empresa para definir un enfoque con el que pueda cumplir las metas de disponibilidad de sus datos e infraestructura de SAP. Por cada situación de error, los requisitos de resiliencia, la pérdida de datos aceptable y el Mean Time To Recover (MTTR, tiempo medio de recuperación) deben ser proporcionales a la criticidad del componente y las aplicaciones empresariales que admite. Los patrones arquitectónicos proporcionados para la garantizar la disponibilidad de SAP cumplen con la mayoría de los requisitos del cliente; sin embargo, se pueden adaptar de acuerdo con los criterios que defina. Estos criterios deben incluir el riesgo percibido y el impacto de cada error, además de tener en cuenta el costo y el rendimiento. En todos los casos, utilice pruebas iniciales y periódicas para validar sus decisiones.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica	Obligatorio	Convenga las metas de disponibilidad de la carga de trabajo de SAP que se alinean con sus requisitos comerciales

ID	Prioridad	Práctica recomendada
recomendada 10.1		
<input type="checkbox"/> Práctica recomendada 10.2	Altamente recomendado	Seleccione un patrón de implementación de SAP adecuado para sus requisitos de disponibilidad y capacidad
<input type="checkbox"/> Práctica recomendada 10.3	Altamente recomendado	Defina un enfoque para ayudar a garantizar la disponibilidad de datos críticos de SAP
<input type="checkbox"/> Práctica recomendada 10.4	Recomendado	Valide el diseño con base en un grupo de criterios extraídos de los requisitos empresariales

Para más información, consulte la siguiente información:

- Documentación de AWS: [Architecture Guidance for Availability and Reliability of SAP on AWS](#) incluidas [Failure Scenarios \(Situaciones de error\)](#) y patrones de arquitectura
- Documentación de AWS: [Amazon Builders' Library: estabilidad estática con AZ](#)
- Documentación de AWS: [Conectividad de red altamente disponible en varios centros de datos](#)
- Documentación de SAP: [SAP HANA System Architecture Overview \(Información general de la arquitectura del sistema SAP HANA\)](#)

**Práctica recomendada 10.1:** convenga las metas de disponibilidad de la carga de trabajo de SAP que se alinean con sus requisitos comerciales

Comprender sus metas de disponibilidad es el primer paso para concentrarse en los factores importantes para su organización. De esta forma, podrá definir los criterios que se pueden utilizar para evaluar sus patrones arquitectónicos.

**Sugerencia 10.1.1:** identifique las aplicaciones SAP dentro de su alcance y sus interdependencias



Identifique las aplicaciones SAP que implementó o implementará en AWS. Comprenda las dependencias de estas aplicaciones, sin importar su ubicación.

Sugerencia 10.1.2: clasifique los sistemas según el impacto del error

No existe un estándar general para clasificar sistemas que esté alineado con la disponibilidad planificada y el riesgo de error. Definir sistemas utilizando expresiones como “esencial” o “de gran importancia” puede ayudar a definir patrones, identificar agrupaciones de aplicaciones y justificar costos. Las aplicaciones de producción podrían verse afectadas de manera diferente por una interrupción. Entre los factores por considerar, se podrían encontrar los siguientes:

- Generación de ingresos o creación de informes de ingresos
- Orientación externa o interna
- Negocio principal frente a soporte técnico
- Alto acoplamiento frente a un bajo acoplamiento con otros sistemas

Los entornos que no son de producción también pueden jugar un rol importante en apoyar de forma indirecta a la empresa. También deben clasificarse según la fase y la escala del proyecto, teniendo en cuenta las rutas de transporte (como empresas habituales y proyectos) y el rol de apoyo (como desarrollo, prueba de unidad, copia de producción y formación).

Sugerencia 10.1.3: evalúe el impacto empresarial de una interrupción

El impacto debe ser cuantificable y debe tener en cuenta la duración de la interrupción. Algunos ejemplos de áreas de impacto son el estado y la seguridad, las finanzas, los asuntos legales y normativos y la marca.

Sugerencia 10.1.4: comprenda los requisitos normativos y de conformidad

Comprenda los requisitos normativos y de conformidad en cuanto a la residencia de datos y la distancia entre ubicaciones para ayudar a garantizar la continuidad de la empresa.

Sugerencia 10.1.5: defina el porcentaje mínimo aceptable de tiempo de disponibilidad (uptime)

Para cada sistema, o grupo de sistemas, acuerde y documente un porcentaje de disponibilidad aceptable que coincida con los requisitos de la empresa. Los siguientes términos se utilizan en este contexto

- MTTR: tiempo medio de recuperación

- RTO: objetivo de tiempo de recuperación
- RPO: objetivo de punto de recuperación

Puede encontrar una explicación completa de los términos en Well-Architected Framework [fiabilidad]: [Disponibilidad](#) . Puede encontrar información adicional sobre la fiabilidad en SAP en el siguiente documento técnico:

- Documentación de AWS: [Architecture Guidance for Availability and Reliability of SAP on AWS](#)

## Práctica recomendada 10.2: seleccione una arquitectura adecuada para sus requisitos de disponibilidad y capacidad

Hay patrones de arquitectura estándar para la disponibilidad de SAP que se ajustan a los requisitos de la mayoría de los clientes que implementan SAP on AWS. Utilice las siguientes sugerencias para determinar qué patrones se ajustan mejor a sus requisitos de disponibilidad y capacidad. Evalúe el riesgo y el impacto de cada situación de error frente a los requisitos de su empresa.

Puede encontrar información adicional sobre la disponibilidad en SAP en el siguiente documento técnico: [Architecture Guidance for Availability and Reliability of SAP on AWS](#) .

Sugerencia 10.2.1: identifique todos los componentes y servicios de AWS que son necesarios para su sistema SAP

Identifique todos los componentes técnicos que necesita su sistema SAP; empiece por los principales (base de datos, servidores de la aplicación, servicios centrales, sistemas de archivos globales) y luego identifique los componentes opcionales (por ejemplo, Web Dispatcher, SAProuter o Cloud Connector, entre otros). Determine los servicios de AWS necesarios para admitir estos componentes.

Sugerencia 10.2.2: utilice los SLA, la durabilidad, la disponibilidad y los datos históricos como una guía para la posibilidad de error

La posibilidad del error es subjetiva. Los SLA publicados y los datos de rendimiento pasado solo se pueden utilizar para guiarse ante el riesgo de posibles errores futuros. Sin embargo, la frecuencia supuesta de diversas situaciones sigue siendo una fuente de datos útiles. Algo que estadísticamente tiene la posibilidad de suceder una vez al año podría tener una mayor repercusión en las decisiones de diseño que un error que aún no ha tenido lugar.

La siguiente información se puede utilizar para comprender mejor los servicios:

- [AWS Personal Health Dashboard](#) proporciona alertas y orientación en materia de corrección cuando AWS experimenta eventos que podrían afectarlo
- [Se publican resúmenes posteriores a eventos de AWS](#) para todos los eventos de servicios importantes que afectan la disponibilidad del servicio de AWS
- [El acuerdo de nivel de servicio de computación de Amazon](#) enumera los SLA de los servicios de computación
- Documentación de AWS: [Durabilidad y disponibilidad de Amazon EBS](#)
- Documentación de AWS: [Disponibilidad y protección de datos de Amazon EFS](#)
- Documentación de AWS: [Recomendaciones sobre resiliencia de AWS Direct Connect](#)

También se debe evaluar la posibilidad de error de otros servicios de soporte, incluidos, entre otros, servicios de nombre de dominio, equilibradores de carga y funciones sin servidor.

Puede encontrar más información en el documento técnico [Architecture Guidance for Availability and Reliability of SAP on AWS](#).

Sugerencia 10.2.3: pruebe opciones de agrupación en clústeres, resiliencia y balanceadores de carga

Un sistema SAP se puede distribuir en varios hosts con mecanismos diferentes para garantizar la disponibilidad. Por ejemplo, se puede utilizar una solución de agrupación en clústeres para proteger los únicos puntos de error (por ejemplo, la base de datos de SAP y los servicios centrales de SAP). El nivel de la aplicación SAP se puede escalar horizontalmente, y se puede utilizar el balanceador de carga para hacer que el despachador web tenga una alta disponibilidad.

- Documentación de AWS: [SAP NetWeaver Deployment and Operations Guide for Windows - High Availability System Deployment \(Guía de operaciones e implementación de SAP NetWeaver para Windows: implementación del sistema de alta disponibilidad\)](#)
- Documentación de AWS: [SAP on AWS – IBM Db2 HADR with Pacemaker \(SAP on AWS: IBM Db2 HADR con Pacemaker\)](#)
- Documentación de AWS: [SQL Server Deployment for High Availability \(Implementación de SQL Server para obtener una alta disponibilidad\)](#)
- Documentación de SAP: [High Availability Partners \(Socios de alta disponibilidad\)](#)

Sugerencia 10.2.4: determine la disponibilidad de las familias de instancias de EC2 dentro de las AZ

Algunas familias de instancias de Amazon EC2 (por ejemplo, X y U) no están disponibles en todas las AZ. Consulte con su equipo de cuenta de AWS o con AWS Support para confirmar que las familias de instancias de EC2 que desea utilizar están disponibles en las AZ previstas. Tenga en cuenta que los identificadores lógicos de las AZ podrían ser diferentes en distintas cuentas. Consulte la documentación de AWS para obtener más información.

- Documentación de AWS: [ID de AZ para sus recursos de AWS](#)

#### Sugerencia 10.2.5: investigue estrategias para garantizar la capacidad

La mejor manera de ayudar a garantizar la capacidad es tener una instancia de tamaño similar disponible en caso de error. Otras estrategias incluyen opciones nativas en la nube (por ejemplo, instancias bajo demanda, recuperación de instancias de EC2) o reasignación de capacidad compartida.

Le recomendamos que establezca un compromiso de capacidad en al menos dos AZ en las que se residan instancias de Amazon EC2 que admitan únicos puntos de error de SAP, de manera que la capacidad esté disponible en el momento en que la necesite.

La capacidad de EC2 se puede reservar utilizando [las instancias reservadas zonales](#) o [reservas de capacidad bajo demanda](#). Tanto las instancias reservadas zonales como las reservas de capacidad bajo demanda se pueden compartir entre cuentas de AWS que se encuentran dentro de la misma organización de AWS, lo que posibilita utilizar capacidad de sacrificio de otro entorno en caso de un error significativo (por ejemplo, una falla total en una AZ).

En el siguiente recurso, podrá encontrar más orientación sobre las reservas de capacidad:

- Documentación de AWS: [Architecture Guidance for Availability and Reliability of SAP on AWS](#)

#### Sugerencia 10.2.6: diseñe su VPC en múltiples AZ

Diseñe su VPC y subredes de manera tal que las instancias se puedan aprovisionar en múltiples AZ, incluso si su diseño inicial solo está pensado para una o dos AZ. Esto le aporta resiliencia a su diseño y ayuda a garantizar que la conectividad y el acceso a los servicios se puedan confirmar con anticipación.

## Práctica recomendada 10.3: defina un enfoque para ayudar a garantizar la disponibilidad de datos críticos de SAP

Los datos empresariales de una aplicación SAP se almacenan principalmente dentro de la base de datos. No obstante, la base de datos también puede alojar datos basados en archivos de archivos binarios (por ejemplo, archivos ejecutables, bibliotecas y scripts, entre otros), configuraciones e interfaces. El enfoque seleccionado debe ser capaz de examinar las opciones de durabilidad, coherencia y recuperación para que coincidan con la criticidad de los datos y el nivel de pérdida de datos aceptable (RPO).

Sugerencia 10.3.1: evalúe los requisitos de MTTR e identifique cómo se pueden cumplir

En [fiabilidad] [Sugerencia 10.1.5: defina el porcentaje mínimo aceptable de tiempo de disponibilidad \(uptime\)](#) , habrá definido los requisitos de MTTR para cada una de sus aplicaciones. Después de evaluar el riesgo de errores y los mecanismos para proteger la disponibilidad del sistema, confirme que se pueden cumplir sus requisitos y documente las expectativas de MTTR frente a cada situación de error. Si es necesario hacer concesiones por costo, complejidad o coherencia consulte con los propietarios de la empresa para llegar a un acuerdo.

Sugerencia 10.3.2: determine en qué situaciones de error sería necesaria una recuperación desde la copia de seguridad

La copia de seguridad suele ser un mecanismo secundario para garantizar o recuperar la disponibilidad, pero la mayoría de las arquitecturas dependerán en cierta medida de las copias de seguridad. Los siguientes son ejemplos de situaciones de error que podrían utilizarse para orientar su análisis. La granularidad de las situaciones, la clasificación y el impacto variarán según sus requisitos y arquitectura.

	Riesgo comparativo de ocurrencia	Copia de seguridad requerida	Posible pérdida de datos	Tiempo de recuperación estimado
Mantenimiento planificado o controlado	Planificado			
Recurso agotado o comprometido (uso elevado de la CPU/sistema de archivos lleno/memoria insuficiente/problemas de almacenamiento)	Medio			

	Riesgo comparativo de ocurrencia	Copia de seguridad requerida	Posible pérdida de datos	Tiempo de recuperación estimado
Error de componente distribuido sin estado (por ejemplo, despachadores web)	Medio			
Error de componente distribuido con estado (por ejemplo, servidores de aplicaciones)	Medio			
Único punto de error (base de datos o servicios centrales de SAP)	Medio			
Error de red o de AZ	Bajo			
Error en servicio central (DNS/Amazon EFS/llamada a la API)	Bajo/medio			
Corrupción/eliminación accidental/ actividades maliciosas/implementación de código defectuoso	Bajo			
Error de región	Muy bajo			

Sugerencia 10.3.3: determine dónde si es necesario hacer una replicación de datos

La replicación de datos se utiliza para mejorar la fiabilidad, ya que se tienen copias de los mismos datos en varias ubicaciones. Suele ser un requisito para los sistemas con un RPO bajo. Al determinar si se requiere replicación para la disponibilidad o la recuperación, considere si el servicio es zonal (por ejemplo, Amazon EC2 y Amazon EBS y las bases de datos compatibles) o regional (por ejemplo, almacenamiento compartido o Simple Storage Service [Amazon S3]).

Base de datos	Tecnología de replicación	Guía
SAP HANA	HANA System Replication (Replicación del sistema de HANA)	Documentación de SAP: <a href="#">HANA System Replication</a>
SAP ASE	Servidor de replicación SAP (Servidor de replicación SAP)	Documentación de SAP: <a href="#">SAP Replication Server</a>
Oracle	Protección de datos de Oracle	Notas de SAP: <a href="#">105047 - Support for Oracle functions in the SAP environment (Soporte de funciones de Oracle en el entorno de SAP)</a> [Se necesita acceso al portal de SAP]
Microsoft SQL Server	SQL Server Always ON	<ul style="list-style-type: none"> <li>Documentación de SAP: <a href="#">Database High-Availability with SQL Server AlwaysOn (Base de datos de alta disponibilidad con SQL Server AlwaysOn)</a></li> <li>Documentación de AWS: <a href="#">SQL Server Deployment for High Availability</a></li> </ul>
SAP MaxDB	Base de datos en espera de MaxDb	Notas de SAP: <a href="#">952783 - FAQ: SAP MaxDB high availability (952783: preguntas frecuentes: alta disponibilidad de SAP MaxDB)</a> [Se necesita acceso al portal de SAP]
IBM Db2	HADR	Notas de SAP: <a href="#">1612105 - DB6: FAQ on Db2 High Availability Disaster Recovery (HADR) (DB6: preguntas frecuentes sobre la recuperación de desastres de alta disponibilidad [HADR] en Db2)</a> [Se necesita acceso al portal de SAP]

[AWS DataSync](#) se puede utilizar para proteger [Amazon EFS](#) y [Amazon FSx](#) en las diferentes regiones, si es necesario.

[CloudEndure Disaster Recovery](#) se replica continuamente a nivel de la instancia entre las AZ o las regiones de disponibilidad, incluidas las cuentas de AWS.

Replicación de Simple Storage Service (Amazon S3)

Las copias de seguridad y otros métodos de almacenamiento de objetos se pueden guardar en Simple Storage Service (Amazon S3) y replicar por medio de [la replicación de Simple Storage Service \(Amazon S3\)](#).

Sugerencia 10.3.4: cree una estrategia para garantizar la consistencia de los datos de configuración y de los archivos binarios

Es importante tener datos de configuración y archivos binarios consistentes para garantizar un comportamiento predecible y una configuración probada tras la ocurrencia de un error. Esto puede comprender paquetes de sistema operativo, parámetros de aplicación y configuración de clústeres. Determine cómo garantizar la consistencia en todas las instancias de una aplicación, incluidas aquellas cuyo propósito es aportar resiliencia (por ejemplo, servidores de aplicación adicionales y nodos de base de datos secundarias, entre otros).

Amazon EFS, Amazon FSx y Simple Storage Service (Amazon S3) brindan una ubicación duradera para archivos binarios compartidos o configuraciones administradas de forma centralizada.

Consulte [excelencia operativa] [Práctica recomendada 2.1: utilice el control de versiones y la administración de configuración](#) para los mecanismos de control de versiones y administración de la configuración.

Sugerencia 10.3.5: tenga un enfoque integral para la consistencia de los datos

El enfoque para garantizar la consistencia de los datos críticos de SAP no solo debe centrarse en un único conjunto de datos, sino que también debe tener en cuenta las dependencias dentro de los conjuntos de datos y los sistemas, así como las que existen entre ellos. Por ejemplo, si necesitara recuperar un sistema SAP BW, pero no los sistemas de origen de los que se abastece, ¿cuál sería el impacto sobre los indicadores de cambio y con qué mecanismos garantizaría una recuperación consistente?

Sugerencia 10.3.6: cree una estrategia para interfaces que permita reproducir o reenviar datos

En el caso del intercambio de datos entre sistemas, determine si la integración está débilmente acoplada y si los datos se pueden reproducir o reenviar, ya sea en el origen o en el destino. Revise si hay capacidades de cola para permitir que la situación se suspenda o se almacene en caché durante una interrupción.

Sugerencia 10.3.7: evalúe utilizar un búnker de datos

Las situaciones de error que dan como resultado que los datos en línea se vuelvan inutilizables o no estén disponibles debido a, por ejemplo, una eliminación accidental o un acto malicioso pueden



requerir un enfoque diferente para ayudar a garantizar que los datos estén protegidos o sean recuperables.

Si bien la mejor defensa es la prevención por medio de un marco de seguridad que garantice el aislamiento de la red y el control de acceso, el impacto debe considerarse en el contexto de la recuperación y la resiliencia.

Se suele utilizar una cuenta de copia de seguridad de solo escritura con un período de retención reducido en esta situación inusual, pero de repercusiones potencialmente grandes.

- SAP Lens [seguridad]: [Práctica recomendada 8.3: proteja sus mecanismos de recuperación de datos para resguardarse contra amenazas](#)

## Práctica recomendada 10.4: valide el diseño en función de un grupo de criterios basados en sus requisitos empresariales

Establezca un conjunto de criterios basados en los requisitos de su empresa, equilibrando el riesgo de error, el impacto en la empresa y las compensaciones aceptables. Utilice estos criterios para validar el diseño y hacer los ajustes necesarios.

Sugerencia 10.4.1: evalúe el costo que una interrupción supondría para su empresa

Los errores, ya sea de los servicios de AWS o de los componentes de SAP, afectarán su sistema SAP de manera diferente según las estrategias de resiliencia y recuperación que aplique. El tipo de error determinará la duración de la interrupción (RTO) y la posible pérdida de datos (RPO).

Por cada error, evalúe el riesgo de una interrupción y el costo para su empresa. Por ejemplo, ¿existen procesos de generación de ingresos que se verán afectados? Y, en tal caso, ¿cuál sería costo por hora asociado con la falta de disponibilidad del sistema?

Sugerencia 10.4.2: evalúe el costo de su arquitectura

En los entornos de SAP, los elementos más costosos de la factura mensual de AWS generalmente están relacionados con Amazon EC2 y los servicios de almacenamiento. Comprenda las implicaciones de costos, de manera que pueda seleccionar la mejor arquitectura para cumplir con sus requisitos de fiabilidad. Entre algunos colaboradores clave, se encuentran:

- Los patrones de implementación que no maximizan la utilización del hardware
- Las copias redundantes de datos

- Los costos de licencia del sistema operativo
- Los costos de licencia del software de agrupación
- Los costos asociados con el mantenimiento, las pruebas y los recursos calificados

Consulte [optimización de costos] [las prácticas recomendadas para la optimización de costos](#) para más detalles.

Sugerencia 10.4.3: evalúe su diseño en función de los otros pilares del marco

La fiabilidad no se puede diseñar de forma aislada, sino que debe evaluarse en función del resto de los pilares de AWS Well-Architected Framework. A continuación, se enumeran algunos ejemplos de preguntas que podría hacer para llevar a cabo dicha evaluación:

- Excelencia operativa: ¿tiene la experiencia y las habilidades para administrar la solución?
- Seguridad: ¿están protegidos sus datos durante la replicación, la recuperación, etc.?
- Rendimiento: ¿la replicación o la actividad de la copia de seguridad afectan el rendimiento del usuario?
- Optimización de costos: ¿el costo de la solución se alinea con el riesgo asumido?

## 11. Detecte los errores y reaccione ante ellos

¿Cómo detecta y reacciona ante errores que afectan su carga de trabajo de SAP? Diseñe cómo el software o los procedimientos operativos pueden ayudar a garantizar el estado y la resiliencia de su carga de trabajo de SAP. Supervise los errores potenciales y reales, centrándose, de ser posible, en la prevención. Considere si un componente está distribuido o es un único punto de error y diseñe una solución de resiliencia que minimice el impacto en su carga de trabajo. Además de realizar pruebas periódicamente para comprender su perfil de riesgo, examine cómo la automatización podría mejorar su resiliencia.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomenda da 11.1	Obligatorio	Supervise los errores de la aplicación SAP, de los recursos de AWS y de la conectividad

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 11.2	Altamente recomendado	Defina un enfoque para mantener la disponibilidad
<input type="checkbox"/> Práctica recomendada 11.3	Altamente recomendado	Defina un enfoque para restaurar la disponibilidad del servicio
<input type="checkbox"/> Práctica recomendada 11.4	Altamente recomendado	Realice pruebas periódicas de resiliencia
<input type="checkbox"/> Práctica recomendada 11.5	Recomendado	Automatice la reacción ante errores

Para obtener más información, consulte lo siguiente:

- Documentación de AWS: [Architecture Guidance for Availability and Reliability of SAP on AWS](#) incluido [Failure Scenarios](#) y [Architecture Patterns \(Patrones de arquitectura\)](#)

Práctica recomendada 11.1: supervise errores de la aplicación SAP, de los recursos de AWS y de la conectividad

La supervisión de errores de la aplicación SAP, de los recursos de AWS y de la conectividad ayudan a reaccionar ante errores potenciales o reales de manera oportuna.

Sugerencia 11.1.1: utilice AWS Personal Health Dashboard y las notificaciones

El [AWS Personal Health Dashboard](#) brinda una vista personalizada del estado de los servicios de AWS que potencian sus aplicaciones, lo que le permite ver rápidamente cuándo hay problemas que

afectan su carga de trabajo de SAP. Por ejemplo, en el caso que se pierda un volumen de [Amazon Elastic Block Store \(Amazon EBS\)](#) asociado con una de sus instancias de [Amazon EC2](#).

El panel también brinda notificaciones de proyecciones, y podrá configurar alertas en múltiples canales, incluido el correo electrónico, de modo que reciba información oportuna y relevante para ayudar a planificar los cambios programados. Por ejemplo, en el caso de que se lleven a cabo actividades de mantenimiento del hardware de AWS que afecten a una de sus instancias de [Amazon EC2](#), recibirá una notificación más detallada para ayudarlo a planificar y tratar de manera oportuna cualquier problema asociado con el cambio que va a ocurrir.

Sugerencia 11.1.2: evalúe los servicios de AWS para comprender el estado de su sistema SAP

AWS brinda una cantidad de [servicios de administración y de gobernanza](#) que debe evaluar. Céntrese en las métricas que indican un error potencial o real, como errores en la instancia de EC2, utilización elevada de la CPU y utilización del sistema de archivos.

Consulte el pilar de la excelencia operativa para obtener más detalles:

- SAP Lens [excelencia operativa]: [Práctica recomendada 1.1: implemente los requisitos previos para la supervisión de SAP on AWS](#)
- SAP Lens [excelencia operativa]: [Práctica recomendada 1.4: implemente la supervisión de la configuración de la carga de trabajo](#)

Sugerencia 11.1.3: evalúe la capacidad de las herramientas de SAP para supervisar errores

Las herramientas de SAP, como Solution Manager y Landscape Manager, permiten ver cualquier dato de supervisión en el contexto de la aplicación. Las siguientes soluciones de supervisión están disponibles en SAP. Revise cualquier costo de licencia adicional como parte de la evaluación de estas herramientas.

- Documentación de SAP: [SAP Focused run \(Ejecución de SAP Focused\)](#)
- Documentación de SAP: [SAP Solution Manager](#)
- Documentación de SAP: [SAP Landscape Management \(LaMa\)](#)
- Notas de SAP: [2574820 - SAP Landscape Management Cloud Manager for Amazon Web Services \(AWS\)](#) [Se necesita acceso al portal de SAP]

Sugerencia 11.1.4: evalúe herramientas de terceros para la supervisión de AWS y SAP

Las siguientes soluciones de supervisión están disponibles en AWS Marketplace. Debe evaluar estas y otras herramientas de terceros.

- Documentación de AWS: [Soluciones de supervisión en AWS Marketplace](#)

## Práctica recomendada 11.2: defina un enfoque para mantener la disponibilidad

Mantenga la disponibilidad con una arquitectura resiliente que pueda sostener el error de un solo componente técnico o servicio de AWS. Entre los mecanismos, se podrían enumerar la capacidad redundante, los balanceadores de carga y los clústeres de software, entre otros.

Sugerencia 11.2.1: evite errores por agotamiento de recursos o deterioro del servicio

Investigue el aprovisionamiento excesivo de recursos, la supervisión proactiva del crecimiento y la limitación del uso mediante la fijación de límites.

El pilar de excelencia operativa cubre las diferentes formas en que puede comprender el estado de su aplicación SAP y garantizar que se toman las medidas correctas, consulte [Excelencia operativa]: [1. Diseñe la carga de trabajo de SAP para permitir la comprensión y la reacción a su estado](#) .

El pilar de rendimiento puede ser de ayuda para orientarse sobre cómo hacer ajustes de tamaño correctos y sobre la capacidad de escalado [rendimiento]: [16. Comprenda las opciones de optimización y rendimiento en curso](#) .

Sugerencia 11.2.2: tenga una estrategia de mantenimiento programado

Si su empresa tiene la obligación de minimizar las interrupciones programadas, debe desarrollar una estrategia de mantenimiento en todos los niveles: aplicación SAP, base de datos, sistema operativo y AWS. Considere lo siguiente:

- Uso de soluciones de replicación y clúster para alternar el nodo principal y secundario
- Exceso de capacidad y mecanismos para escalar y reducir verticalmente a fin de facilitar las interrupciones consecutivas
- Uso de un enfoque de revisión en tiempo real para el sistema operativo, en caso de ser posible
  - [SUSE Linux Enterprise Live Patching](#)
  - [Documento técnico Red Hat Reducing Downtime for SAP HANA \(Reducción del tiempo de inactividad para SAP HANA\)](#)
- Documentación de AWS: [AWS Systems Manager Patch Manager Patch Groups \(Grupos de parches de AWS Systems Manager Patch Manager\)](#)

- Notas de SAP: [1913302 - HANA: Suspend DB connections for short maintenance tasks \(HANA: suspenda conexiones de base de datos para tareas de mantenimiento breves\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2077934 - Rolling kernel switch in HA environments \(2077934: Rolling Kernel Switch en entornos de alta disponibilidad\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [953653 - Rolling Kernel Switch](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2254173 - Linux: Rolling Kernel Switch in Pacemaker-based NetWeaver HA environments \(Linux: Rolling Kernel Switch en entornos de alta disponibilidad de NetWeaver basados en Pacemaker\)](#) [Se necesita acceso al portal de SAP]

También debe evaluar las capacidades elásticas de los servicios de AWS para reducir el tiempo de inactividad general del mantenimiento programado mediante el aumento temporal del rendimiento. Por ejemplo, escalar verticalmente el tamaño de la instancia de Amazon EC2 que ejecuta su base de datos para brindar más capacidad de procesamiento y rendimiento de almacenamiento para actividades de actualización, o cambiar los tipos de volúmenes de EBS de gp2 a io2 a fin de mejorar el rendimiento de almacenamiento durante una reorganización de la base de datos.

Sugerencia 11.2.3: proteja los únicos puntos de error de SAP con clústeres de software u otros mecanismos

Puede utilizar una solución de clústeres de alta disponibilidad para la conmutación por error autónoma del único punto de error de SAP (servicios centrales y base de datos) en las AZ.

Existen múltiples soluciones de agrupación en clústeres certificadas por SAP [enumeradas en el sitio web de SAP](#). Las soluciones de agrupamiento en clústeres de SAP son compatibles con los propios proveedores de software de clústeres, no con SAP. SAP solo certifica la solución. Cualquier solución personalizada no está certificada y necesitará el respaldo del creador de la solución.

Si elije no utilizar una solución de agrupamiento en clústeres para su único punto de error (SPOF), considere recurrir a la creación de scripts o a manuales de procedimientos para minimizar los errores asociados con los servicios de restauración.

Sugerencia 11.2.4: capacidad redundante o escalado automático para los componentes que la soportan

Evalúe los cambios de capacidad estáticos, dinámicos y programados para que coincidan con su uso. Examine los requisitos mínimos de capacidad y cómo se verían afectados por errores y

mantenimiento. Efectúe un sobreaprovisionamiento cuando sea adecuado para darse el tiempo de recuperarse del error.

Si necesita mantener el 100 % de la capacidad en caso de que se produzca un error en la zona de disponibilidad, debería considerar implementar la aplicación en tres AZ, cada una con el 50 % de la capacidad total requerida.

Además de implementar la capa del servidor de la aplicación SAP en varias AZ, podría considerar escalar soluciones como la que se describe en el siguiente artículo del blog de SAP on AWS, la cual se centra en aprovechar las capacidades de [Amazon EC2 Auto Scaling](#).

- Blog de SAP on AWS: [Using AWS to enable SAP Application Auto Scaling \(Uso de AWS para habilitar el escalado automático de aplicaciones SAP\)](#)
- Documentación de AWS: [Amazon EC2 Instance Types for SAP](#)
- Notas de SAP: [1656099 - SAP Applications on AWS: Supported DB/OS and Amazon EC2 products \(Aplicaciones SAP en AWS: bases de datos, sistemas operativos y productos de Amazon EC2 compatibles\)](#) [Se necesita acceso al portal de SAP]

Sugerencia 11.2.5: garantice la disponibilidad de capacidad para todos los casos de errores identificados

Los siguientes son ejemplos de situaciones de error que podrían utilizarse para orientar su análisis. La granularidad, cobertura, clasificación o impacto de las situaciones variarán según sus requisitos y arquitectura.

Ejemplos de situaciones de error	Riesgo comparativo de ocurrencia
Mantenimiento planificado o controlado	Planificado
Recurso agotado o comprometido (uso elevado de la CPU/sistema de archivos lleno/memoria insuficiente/problemas de almacenamiento)	Medio
Error de componente distribuido sin estado (por ejemplo, despachadores web)	Medio
Error de componente distribuido con estado (por ejemplo, servidores de aplicaciones)	Medio

Ejemplos de situaciones de error	Riesgo comparativo de ocurrencia
Único punto de error (base de datos o servicios centrales de SAP)	Medio
Error de red o de AZ	Bajo
Error en servicio central (DNS/Amazon EFS/llamada a la API)	Bajo/medio
Corrupción/eliminación accidental/actividades maliciosas/implementación de código defectuoso	Bajo
Error de región	Muy bajo

Puede obtener más información sobre las reservas de capacidad en [fiabilidad] [Sugerencia 10.2.5: investigue estrategias para garantizar la capacidad](#) y en el documento técnico de AWS: [Architecture Guidance for Availability and Reliability of SAP on AWS](#) .

Puede consultar las instancias reservadas disponibles en su cuenta de AWS por medio de los [informes de instancias reservadas de AWS Cost Explorer](#) .

Sugerencia 11.2.6: utilice servicios de AWS que tengan disponibilidad inherente cuando corresponda

Varios servicios de AWS tienen disponibilidad inherente como parte de su diseño y se ejecutan en varias AZ para lograr un alto grado de disponibilidad. Entre algunos de los servicios relevantes utilizados en el contexto de SAP, se incluyen los siguientes:

- Servicio de AWS: [Amazon EFS](#)
- Servicio de AWS: [Elastic Load Balancing](#)
- Servicio de AWS: [Route 53](#)
- Servicio de AWS: [Puerta de enlace de tránsito de AWS](#)
- Servicio de AWS: [Amazon S3](#)

Además, los componentes que usan servicios sin estado, como los hosts bastión o SAPRouter, pueden recurrir a grupos de Auto Scaling para lograr una alta disponibilidad.

Sugerencia 11.2.7: siga las prácticas recomendadas de AWS para garantizar la conectividad de la red



Evalúe una o más de las siguientes prácticas recomendadas de AWS para garantizar la resiliencia de la conectividad a través de la red a la región de AWS en uso:

- Documentación de AWS: [Kit de herramientas de resistencia de AWS Direct Connect](#)
- Documentación de AWS: [AWS VPN CloudHub](#)

Si su solución de clúster se basa en una IP superpuesta, considere lo siguiente para habilitar el acceso desde el exterior de la VPC:

- Documentación de AWS: [SAP on AWS High Availability with Overlay IP Address Routing \(SAP on AWS: alta disponibilidad con enrutamiento de direcciones IP superpuestas\)](#)

### Práctica recomendada 11.3: defina un enfoque para restaurar la disponibilidad del servicio

La restauración de la disponibilidad supone que, para una situación de error específica, se producirá alguna pérdida de servicio. El enfoque de restauración adoptado debe incluir examinar la cantidad de tiempo necesario para restaurar el servicio y las acciones necesarias para alcanzar el objetivo de disponibilidad.

#### Sugerencia 11.3.1: habilite la recuperación de instancias en instancias de EC2

Puede crear una alarma de Amazon CloudWatch que supervise una instancia de Amazon EC2 y recupere automáticamente la instancia si se daña debido a un error de hardware subyacente. Con esta acción, se puede eliminar la necesidad de una intervención manual, pero los tiempos de inicio, reinicio de la aplicación y de carga deben tenerse en cuenta en el Objetivo de tiempo de recuperación (RTO). Si tiene la intención de utilizar una solución de clúster para protegerse contra errores de hardware, debe evaluar si la recuperación de instancias es compatible con la solución de clúster.

- Documentación de AWS: [Recuperación de instancias de Amazon EC2](#)

#### Sugerencia 11.3.2: prepare una estrategia para reconstruir instancias de EC2 utilizando AMI e infraestructura como código

El beneficio de la infraestructura como código es la capacidad de crear y deshacer entornos enteros mediante programación. Si su arquitectura está diseñada para la resiliencia, puede implementar un entorno en cuestión de minutos con ayuda de las [plantillas de AWS CloudFormation](#) o [AWS Systems](#)

[Manager Automation](#) . La automatización es crucial para mantener una alta disponibilidad y lograr una rápida recuperación.

Deberá evaluar los siguientes servicios de AWS como parte de su estrategia:

- Servicio de AWS: [EC2 Image Builder](#)
- Servicio de AWS: [AWS Launch Wizard para SAP](#)
- Servicio de AWS: [Kit de desarrollo de la nube de AWS](#)
- Blog de SAP on AWS: [DevOps for SAP \(DevOps para SAP\)](#)

Sugerencia 11.3.3: comprenda los errores de Amazon EBS

Que se produzcan errores en uno o más volúmenes de EBS podría afectar la disponibilidad y la durabilidad de su carga de trabajo de SAP. Por lo tanto, debe comprender las tasas de error, los mecanismos de notificación y las opciones de recuperación de Amazon EBS.

- Documentación de AWS: [Duración de Amazon EBS](#)
- Documentación de AWS: [Monitorear el estado de los volúmenes](#)
- Servicio de AWS: [AWS Personal Health Dashboard](#)
- Documentación de AWS: [Recuperación de volúmenes con instantáneas de Amazon EBS](#)

Sugerencia 11.3.4: prepare una estrategia para reaccionar a las notificaciones de AWS Personal Health Dashboard

Debe tener una estrategia para recibir notificaciones de AWS Personal Health Dashboard y actuar en función de ellas. Esto podría incluir el uso de CloudWatch para iniciar Amazon SNS o la integración con sus herramientas de ITSM a través de [la API de AWS Health](#) .

Sugerencia 11.3.5: asegúrese de estar protegido contra eventos accidentales o maliciosos que afecten la disponibilidad

Debe tener en cuenta los siguientes enfoques para asegurarse de estar protegido contra eventos accidentales o maliciosos que podrían afectar la disponibilidad de su carga de trabajo de SAP.

- Implemente un [principio de privilegio mínimo](#) y aplique la separación de funciones dentro de AWS Identity and Access Management.

- Siga la guía que se detalla en el artículo del Centro de conocimientos de AWS [How do I protect my data against accidental EC2 instance termination? \(¿Cómo protejo mis datos contra la terminación de una instancia de EC2?\)](#)
- Siga las [prácticas recomendadas establecidas para Amazon EC2](#).
- También le recomendamos seguir la guía de seguridad que se detalla en [seguridad] [Práctica recomendada 8.3: proteja sus mecanismos de recuperación de datos para resguardarse contra amenazas](#).

Sugerencia 11.3.6: identifique dependencias adicionales a las de su carga de trabajo de SAP en AWS

Comprenda las dependencias subyacentes de sus procesos empresariales de SAP, incluidos los servicios compartidos y los componentes o sistemas de soporte. Entre algunos ejemplos, se incluyen Active Directory, DNS, proveedores de identidad, servicios de SaaS y sistemas locales. Evalúe el impacto del error y las mitigaciones necesarias.

### Práctica recomendada 11.4: realice pruebas periódicas de resiliencia

Pruebe periódicamente la resiliencia en situaciones de errores críticos para demostrar que el software y los procedimientos tienen un resultado predecible. Evalúe cualquier cambio en la arquitectura, software o personal de soporte para determinar si es necesario realizar pruebas adicionales.

Sugerencia 11.4.1: defina las situaciones de error críticas dentro de su alcance en función de los requisitos de su empresa

Debe definir qué situaciones de error críticas puede probar en función de sus requisitos empresariales. Los siguientes son ejemplos de situaciones de error que podrían servir de guía para su análisis. La granularidad, cobertura, clasificación o impacto de las situaciones variarán según sus requisitos y arquitectura.

Ejemplos de situaciones de error	Riesgo comparativo de ocurrencia
Mantenimiento planificado o controlado	Planificado
Recurso agotado o comprometido (uso elevado de la CPU/sistema de archivos lleno/memoria insuficiente/problemas de almacenamiento)	Medio

Ejemplos de situaciones de error	Riesgo comparativo de ocurrencia
Error de componente distribuido sin estado (por ejemplo, despachadores web)	Medio
Error de componente distribuido con estado (por ejemplo, servidores de aplicaciones)	Medio
Único punto de error (base de datos o servicios centrales de SAP)	Medio
Error de red o de AZ	Bajo
Error en servicio central (DNS/Amazon EFS/llamada a la API)	Bajo/medio
Corrupción/eliminación accidental/actividades maliciosas/implementación de código defectuoso	Bajo
Error de región	Muy bajo

Sugerencia 11.4.2: defina un conjunto de casos de prueba para simular errores críticos

Debería tener un conjunto completo de pruebas definidas para simular las situaciones de error críticas que afectarían su carga de trabajo de SAP.

Debe tener en cuenta que, para algunas situaciones de error, es posible que una simulación no represente completamente el error real que ocurriría. Por ejemplo, para simular un problema de hardware, no puede causar un error en una instancia de EC2, pero, en el caso de las instancias basadas en Nitro, puede generar un pánico del kernel para que la instancia se reinicie.

Además, [AWS Fault Injection Simulation](#) está diseñado para ayudar a simular errores dentro de sus recursos de AWS.

- Documentación de AWS: [Guía de configuración de alta disponibilidad para SAP HANA on AWS](#)
- Documentación de AWS: [Enviar una interrupción de diagnóstico](#)

Sugerencia 11.4.3: defina el comportamiento esperado para cada caso de prueba

Debería documentar una serie de resultados esperados que sirvan como estándares de referencia de sus pruebas.

Sugerencia 11.4.4: defina un enfoque para evaluar el impacto de un cambio y las pruebas posteriores requeridas

Debería definir un enfoque para evaluar el impacto de un cambio en su entorno y el número de pruebas que se deben realizar tras ese cambio con el fin de garantizar que no invalide su enfoque de disponibilidad y fiabilidad. Entre algunos ejemplos de cambios, se incluyen actualizaciones de software, revisiones y cambios de parámetros.

Sugerencia 11.4.5: defina un cronograma de pruebas

Asegúrese de contar con un cronograma de pruebas en el que se contemple la implementación inicial, las pruebas de los cambios y la validación periódica de su entorno.

Sugerencia 11.4.6: revise los resultados de las pruebas

Según los resultados de la prueba, identifique cualquier mejora en los casos de prueba, la configuración o la arquitectura.

Sugerencia 11.4.7: defina las actividades requeridas para hacer una reversión a un estado previo a la prueba

En cada prueba, debe definir las actividades necesarias para revertir el estado anterior a la prueba. Esto es para garantizar que cada caso de prueba esté aislado de otras pruebas y que la prueba no afecte la disponibilidad y fiabilidad de un sistema de producción.

## Práctica recomendada 11.5: automatice la reacción ante errores

Puede minimizar el impacto en el servicio al automatizar la respuesta ante errores. Diseñe acciones automáticas para responder ante errores y situaciones de deterioro de la capacidad o pérdida de conectividad. Asegúrese de que se definan criterios de arbitraje claros para evitar falsos positivos.

Sugerencia 11.5.1: evalúe su automatización por riesgo de corrupción

Ante la presencia de componentes en los que hay riesgo de corrupción de datos, asegúrese de que su solución de alta disponibilidad (HA) tenga en cuenta el método de replicación de datos, la estabilidad de la conectividad y el conocimiento de aplicaciones, y que evite situaciones de “cerebro dividido”.

## Sugerencia 11.5.2: evalúe los mecanismos de comprobación de estado que inician la automatización

Los controles de estado deben diseñarse con controles para ayudar a garantizar que las automatizaciones no se inicien como resultado de falsos positivos.

## 12. Haga un plan de recuperación de datos

¿Cómo planifica la recuperación lógica de datos para su carga de trabajo de SAP? Defina un enfoque a partir de los requisitos comerciales que se centre en recuperar o reconstruir sus datos comerciales. Dependiendo de cómo haya diseñado la resiliencia, diferentes situaciones pueden encajar en esta categoría. Como mínimo, su enfoque de creación de copias de seguridad o de DR debe protegerlo contra la eliminación accidental, la corrupción de datos lógicos y el malware. Sea deliberado acerca de la decisión de restaurar y tenga en cuenta el tiempo para volver al servicio y las dependencias entre los sistemas.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 12.1	Obligatorio	Establezca un método para la recuperación coherente de datos comerciales
<input type="checkbox"/> Práctica recomendada 12.2	Altamente recomendado	Establezca un método para la recuperación de datos de configuración
<input type="checkbox"/> Práctica recomendada 12.3	Altamente recomendado	Defina un enfoque de recuperación para su todo su catálogo de SAP
<input type="checkbox"/> Práctica recomendada 12.4	Recomendado	Realice pruebas periódicas para validar su procedimiento de recuperación

## Práctica recomendada 12.1: establezca un método para la recuperación coherente de datos empresariales

Defina planes de recuperación de datos que puedan ayudar a garantizar la coherencia de los datos empresariales para un sistema individual en caso de pérdida o corrupción de datos.

Sugerencia 12.1.1: asegúrese de que las copias de seguridad de la base de datos sean coherentes mediante el uso de mecanismos de copia de seguridad que conozcan el estado de la base de datos.

SAP brinda mecanismos para hacer una integración con la capacidad de creación de copias de seguridad de un proveedor de base de datos (por ejemplo, brtools) y proporciona visibilidad dentro de las consolas de administración o transacciones de SAP. Además, hay opciones para integrar proveedores de copia de seguridad de terceros o almacenar soluciones que incluyen [AWS Backint Agent para SAP HANA](#). Estas opciones admitidas tienen conocimiento del estado de la base de datos, puesto que capturan cambios continuamente o desactivan la base de datos (pausando o reduciendo la actividad) mientras se toma una copia consistente, por ejemplo, al usar instantáneas de almacenamiento.

Revise las guías de SAP para proveedores de bases de datos individuales, así como la documentación de AWS:

- Documentación de AWS: [AWS Backint Agent para SAP HANA](#)
- Documentación de SAP: [Guide Finder for SAP NetWeaver and ABAP Platform \(Buscador de guías de SAP NetWeaver y ABAP\)](#)
- Blog de SAP on AWS: [How to back up Microsoft SQL Server databases for SAP with VSS Snapshots \(Cómo realizar una copia de seguridad de las bases de datos de Microsoft SQL Server para SAP con instantáneas de VSS\)](#)
- Blog de AWS: [Taking crash-consistent snapshots across multiple Amazon EBS volumes on an Amazon EC2 instance \(Captura de instantáneas coherentes ante bloqueos en varios volúmenes de Amazon EBS en una instancia de Amazon EC2\)](#)

Sugerencia 12.1.2: evalúe la durabilidad y la capacidad de recuperación de los datos basados en archivos que son críticos para su empresa.

Los datos empresariales que no se almacenan en una base de datos pueden requerir una estrategia de copia de seguridad independiente.

En un sistema estándar de SAP NetWeaver, esto a menudo suele suponer el uso de archivos de interfaz basados en archivos, contenido del directorio de transporte de SAP y registros, entre ellos, registros de lotes, de trabajos y de directorios de procesos de trabajo. Los sistemas de soporte y los que no pertenecen a SAP NetWeaver, como las soluciones de administración de documentos, pueden tener otros datos comerciales basados en archivos que deben evaluarse. Evalúe [Amazon EFS](#) o [Amazon FSx](#) para aumentar la disponibilidad y durabilidad de dichos sistemas de archivos.

Las copias de seguridad del sistema de archivos se pueden realizar utilizando instantáneas, AWS Backup o soluciones de copias de seguridad de terceros.

Los datos empresariales deben evaluarse independientemente de los archivos binarios y los datos de configuración, que podrían volver a aprovisionarse a través de la descarga, reinstalación o la infraestructura como código de SAP. Consulte el siguiente recurso:

- SAP Lens [excelencia operativa]: [Sugerencia 12.2.1: defina un enfoque de infraestructura como código para la creación y los cambios de configuración](#)
- SAP Lens [excelencia operativa]: [Sugerencia 12.2.2: defina un enfoque para las copias de seguridad de los contenidos del sistema de archivos, incluido el volumen principal](#)

Sugerencia 12.1.3: evalúe la durabilidad y ubicación de las copias de seguridad y de los registros de la base de datos

Las copias de seguridad y los registros contienen información sobre sus datos en tiempo real, pero pueden fallar. Considere cómo minimizar el impacto de un error al evaluar la ubicación de sus copias de seguridad en relación con sus copias de datos activas. Es clave que tenga en cuenta lo siguiente:

- El tiempo que lleva asegurar las copias de seguridad afecta el punto de recuperación.
- El tiempo que lleva restaurar o recuperar las copias de seguridad afecta el tiempo de recuperación.

Puede encontrar más información en la siguiente documentación:

- Documentación de AWS: [AWS Backint Agent para HANA](#)
- Documentación de AWS: [Restauración rápida de instantáneas](#)
- Documentación de AWS: [Opciones de replicación de Amazon S3](#)

Sugerencia 12.1.4: evalúe sus requisitos para una recuperación a un momento dado



Si se le exigiera hacer una recuperación hacia un momento dado, ¿se lo permitiría su diseño de copias de seguridad? ¿El método de copia de seguridad tiene conocimiento de la base de datos y puede hacer avanzar su base de datos a un punto de recuperación coherente? ¿Ha considerado alguna recuperación basada en archivos para mantener la coherencia?

Considere lo siguiente:

- El intervalo de registro y la rapidez con la que se protegen los registros
- Copias de seguridad progresivas o diferenciales para mejorar el tiempo de recuperación
- Exigencia de un catálogo de copias de seguridad u otro mecanismo
- ¿Es posible usar la base de datos o las opciones de almacenamiento para retroceder en el tiempo?

Sugerencia 12.1.5: revise mecanismos de recuperación por pérdida de datos

Determine las implicaciones de recuperarse de una situación de pérdida de datos importante, como la corrupción o eliminación de datos o una implementación de código defectuosa que no se puede revertir. Evalúe la propagación de la pérdida de datos al usar replicaciones de bases de datos o basadas en almacenamiento, y el impacto del RTO y RPO al usar un mecanismo de restauración secundario, como las copias de seguridad.

Sugerencia 12.1.6: cree un búnker de datos

Siga la guía que se encuentra en [Sugerencia 10.3.7: determine en qué situaciones de error sería necesaria una recuperación desde la copia de seguridad](#) y cree un búnker de datos para proteger sus copias de seguridad de una eliminación accidental o actividades maliciosas.

**Práctica recomendada 12.2: establezca un método para la recuperación de datos de configuración**

Varios tipos diferentes de datos, que son necesarios para ejecutar una carga de trabajo de SAP, no residen en la base de datos de SAP. Esto incluye la configuración del sistema operativo, los metadatos para recrear los recursos de AWS requeridos y los datos requeridos por las aplicaciones SAP almacenadas en un sistema de archivos. Defina un proceso para recuperar o recrear estos datos en caso de que se pierdan.

Sugerencia 12.2.1: defina un enfoque de infraestructura como código para la creación y los cambios de configuración

Los cambios manuales realizados directamente en instancias individuales pueden provocar rápidamente inconsistencias en la configuración entre sistemas y una dependencia en las copias de seguridad para recuperar el estado. Al usar infraestructura como código, puede implementar sus sistemas SAP e implementar cambios de la misma forma que administraría el código de la aplicación. Los mecanismos de DevOps, como una canalización de código, pueden brindar control y pruebas adicionales para ayudar a garantizar la consistencia y la repetibilidad de su infraestructura.

Deberá evaluar los siguientes servicios de AWS como parte de su enfoque:

- Servicio de AWS: [AWS Launch Wizard para SAP](#)
- Servicio de AWS: [EC2 Image Builder](#)
- Servicio de AWS: [Kit de desarrollo de la nube de AWS](#)
- Blog de SAP on AWS: [DevOps for SAP \(DevOps para SAP\)](#)
- Documentación de AWS: [Introducción a DevOps en AWS](#)

Sugerencia 12.2.2: defina un enfoque para las copias de seguridad de los contenidos del sistema de archivos, incluido el volumen principal

Los paquetes y la configuración del sistema operativo, los archivos binarios de la aplicación y el contenido del sistema de archivos son parte integral de un sistema SAP en ejecución, pero no forman parte de la copia de seguridad de la base de datos central de SAP. Evalúe los mecanismos para asegurar y restaurar estos datos, lo que incluye las Amazon Machine Images (AMI, imágenes de máquina de Amazon), las instantáneas de volúmenes de EBS y otras opciones de copias de seguridad.

Debe tenerse en cuenta la frecuencia y la alineación de las AMI, las instantáneas y las copias del sistema de archivos, así como la granularidad de la recuperación y el tiempo necesario.

En ciertos escenarios, el uso de la infraestructura como código podría reducir los requisitos de copia de seguridad para datos no empresariales al centrarse en la recreación y no en la restauración.

- Documentación de SAP: [Directorios y sistemas de archivos requeridos](#)
- Documentación de AWS: [Diseño de una solución de copias de seguridad y recuperación](#)

Sugerencia 12.2.3: registre en un documento cualquier configuración manual

Cualquier actividad manual que no esté contenida en la base de datos o que pueda implementarse por código o restaurarse mediante copias de seguridad de volúmenes debe registrarse para garantizar que se pueda recrear un sistema SAP en el peor de los casos.

## Práctica recomendada 12.3: defina un enfoque de recuperación para todo su catálogo de SAP

Si su catálogo de SAP consta de varios sistemas SAP, debe crear un enfoque detallado en el que defina el orden en que se recuperará cada sistema, en función de las prioridades empresariales. Evalúe cómo la pérdida de datos podría afectar la coherencia entre los sistemas y las operaciones empresariales.

Sugerencia 12.3.1: cree un plan de continuidad empresarial en el que se contemple la prioridad de restauración y los planes para garantizar la coherencia

Tenga un BCP que fije la prioridad de restauración de cada sistema SAP en función de la clasificación de sistemas que se determina en [fiabilidad]: [Sugerencia 10.1.2: clasifique los sistemas según el impacto del error](#). El plan también debe considerar el impacto de los requisitos de consistencia entre sistemas y el uso de bases de datos de multiinquilinos en la prioridad de restauración.

Sugerencia 12.3.2: evalúe todas las dependencias de servicios compartidos

Al definir su enfoque de recuperación, considere qué servicios compartidos son parte de la base para ejecutar su carga de trabajo de SAP (por ejemplo, DNS, Active Directory) o son necesarios para realizar la restauración en sí (por ejemplo, herramientas de copia de seguridad). Evalúe los riesgos y los prerrequisitos de restauración vinculados a estas dependencias.

Sugerencia 12.3.3: cree manuales de procedimiento que sirvan como guías en situaciones de desastres

Definir de antemano un manual de procedimientos garantizará que se sigan una serie de pasos probados en situaciones de desastres, lo que ayuda a reducir el riesgo o la probabilidad de que no se lleven a cabo actividades fundamentales.

## Práctica recomendada 12.4: realice pruebas periódicas para validar su procedimiento de recuperación

Pruebe periódicamente sus estrategias de recuperación ante situaciones de errores críticos para demostrar que el software y los procedimientos generan un resultado predecible y para validar el

estado de los archivos de copia de seguridad. Debe evaluar cualquier cambio en la arquitectura, el software o el personal de soporte para determinar si es necesario realizar pruebas adicionales.

Sugerencia 12.4.1: identifique situaciones de error para las pruebas de recuperación

Deberá identificar las posibles situaciones de error en las que se necesitará una recuperación. Para ello, bájese en lo detallado en [fiabilidad]: [Sugerencia 10.3.2: determine en qué situaciones de error sería necesaria una recuperación desde la copia de seguridad](#) y decida el nivel apropiado de pruebas requeridas para validar el proceso y la herramienta.

Sugerencia 12.4.2: determine el impacto que tendrá un cambio en el sistema en su estrategia de recuperación.

Defina un enfoque para evaluar el impacto de un cambio y las pruebas de recuperación posteriores necesarias para garantizar que no invalide su estrategia. Entre los ejemplos de los tipos de cambios que podrían afectar la recuperación de su carga de trabajo, se incluyen actualizaciones de software, las revisiones y los cambios de parámetros.

También se debe planificar una prueba de recuperación en caso de que se produzca un cambio significativo en el modelo operativo utilizado para dar soporte a sus entornos de SAP, por ejemplo, un cambio en los socios proveedores de los servicios administrados o en el personal clave.

Sugerencia 12.4.3: defina un plan de prueba de recuperación

Debe tener un conjunto completo de pruebas definidas para simular las situaciones de errores críticos de las que necesitaría recuperarse. Las pruebas de recuperación deben planificarse durante la implementación inicial y luego periódicamente o cuando sea necesario.

- SAP Lens [excelencia operativa]: [Práctica recomendada 4.3: pruebe periódicamente los planes de continuidad de la empresa y la recuperación de errores](#) .

## Eficiencia de rendimiento

El pilar de eficiencia de rendimiento se centra en el uso eficiente de recursos informáticos para cumplir con los requisitos y la forma de mantener esa eficiencia a medida que cambian las exigencias y evolucionan las tecnologías. La optimización del rendimiento debe ser un controlado por datos que consista en supervisar y medir el rendimiento, y ajustar la infraestructura computacional para cumplir con requisitos cambiantes.

## 13. Seleccione la solución de computación óptima

¿Cómo selecciona la solución de computación óptima para su carga de trabajo de SAP? Evalúe y calcule los requisitos de rendimiento utilizando métricas de las herramientas de SAP y las cargas de trabajo existentes. Asigne los requisitos computacionales a las instancias compatibles con SAP que mejor se adapten a su carga de trabajo. Tenga en cuenta los requisitos específicos de red o de almacenamiento para los tipos de instancias, así como la disponibilidad de los tipos de instancias necesarios en la región y en las AZ de AWS que haya elegido.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 13.1	Obligatorio	Evalúe o estime los requisitos de rendimiento
<input type="checkbox"/> Práctica recomendada 13.2	Obligatorio	Seleccione instancias de EC2 adecuadas para las cargas de trabajo de SAP
<input type="checkbox"/> Práctica recomendada 13.3	Altamente recomendado	Seleccione arquitecturas que le permitan escalar de forma autónoma los sistemas o componentes
<input type="checkbox"/> Práctica recomendada 13.4	Altamente recomendado	Elija la ubicación de la instancia para el rendimiento teniendo en cuenta el rendimiento y la latencia de la red

Para más información, consulte la siguiente información:

- Documentación de AWS: [Amazon EC2 Instance Types for SAP](#)
- Documentación de SAP: [Certified and Supported SAP HANA Hardware \(Hardware de SAP HANA certificado y compatible\)](#)

- Notas de SAP: [1656099 - SAP Applications on AWS: Supported DB/OS and Amazon EC2 products](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [1656250 - SAP on AWS: Support prerequisites](#) [Se necesita acceso al portal de SAP]

## Práctica recomendada 13.1: evalúe o estime los requisitos del rendimiento

Los requisitos futuros de hardware se pueden estimar examinando la capacidad y los patrones de uso de los sistemas SAP existentes. SAP brinda varias herramientas para ajustar el tamaño del hardware en sistemas nuevos y existentes. Para validar aún más las estimaciones de ajuste de tamaño, se pueden utilizar implementaciones de POC y pruebas de rendimiento.

Sugerencia 13.1.1: consulte las métricas de rendimiento del SAPS del hardware de origen

SAP evalúa el hardware con ayuda del [SAP Application Performance Standard \(SAPS\) \(Estándar de rendimiento de la aplicación SAP \[SAPS\]\)](#), que es una unidad de medida que no depende del hardware que describe el rendimiento de la configuración de un sistema en el entorno de SAP. Consulte con su proveedor de hardware existente y con el directorio de pruebas comparativas de SAP para obtener los valores del SAPS correspondientes al hardware de su servidor en las instalaciones.

Un ajuste de tamaño basado en el SAPS es apropiado para una migración que introduce cambios mínimos en los requisitos de capacidad subyacentes, a menudo, denominada “migración mediante lift and shift”.

Sugerencia 13.1.2: consulte los informes de SAP EarlyWatch Alert y las herramientas de supervisión para obtener detalles de uso históricos

[SAP EarlyWatch Alert](#) brindan información útil sobre su aplicación SAP, como picos de memoria y uso de la CPU. Un análisis completo de estos informes en el que se traten varios eventos de pico, como el cierre de fin de mes y las cargas de lotes grandes, puede proporcionar información valiosa sobre el uso del sistema.

Además de EarlyWatch, las herramientas de supervisión a nivel de infraestructura pueden brindar más granularidad e información.

Sugerencia 13.1.3: utilice los informes de ajuste de tamaño de SAP HANA para estimar los requisitos de computación

Al migrar a SAP HANA, utilice las herramientas proporcionadas por SAP para estimar las dimensiones de la computación prevista. El resultado generado por estas herramientas detalla los requisitos de ajuste de tamaño del hardware en función de su base de datos de SAP HANA.

- Documentación de SAP: [SAP HANA Administration Guide for HANA Platform \(Guía de administración de SAP HANA para la plataforma HANA\)](#)
- Documentación de AWS: [SAP HANA Sizing \(Ajuste de tamaño de SAP HANA\)](#)
- Notas de SAP: [1793345 – Sizing for SAP Suite on HANA \(Ajuste de tamaño para SAP Suite en HANA\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [1872170 – ABAP on HANA sizing report \(S/4HANA, Suite on HANA...\) \(ABAP en el informe de ajuste de tamaño de HANA \[S/4HANA, Suite en HANA...\]\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2296290 – New Sizing Report for SAP BW/4HANA \(Nuevo informe de ajuste de tamaño de SAP BW/4HANA\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [1958910 - EarlyWatch Alert For HANA Database \(EarlyWatch Alert para la base de datos de HANA\)](#) [Se necesita acceso al portal de SAP]

Sugerencia 13.1.4: utilice SAP Quick Sizer para implementaciones nuevas y cambios funcionales

SAP Quick Sizer se puede utilizar para ajustar el tamaño de nuevas implementaciones de SAP o para aquellas que experimentan cambios (por ejemplo, un incremento en la base de usuarios, nuevas funcionalidades o módulos). La herramienta lo ayuda a trasladar los requisitos de su aplicación a las especificaciones del hardware. Para obtener mejores resultados, los equipos técnicos y funcionales deberían colaborar para aportar valores a la herramienta Quick Sizer.

Recomendamos el uso del ajuste de tamaño experto de SAP para validar el tamaño de implementaciones complejas.

Para obtener más información sobre los servicios y herramientas de SAP, consulte la siguiente documentación:

- Documentación de SAP: [SAP: Sizing Benchmarks \(SAP: referencias de ajuste de tamaño\)](#)

Sugerencia 13.1.5: utilice la implementación de prueba de concepto para obtener una exactitud en el ajuste de tamaños

Puede aprovechar la flexibilidad de los servicios de AWS para ajustar con mayor exactitud sus cargas de trabajo de SAP y escalar a medida que evolucionen las demandas empresariales. Utilice POC para probar migraciones a la nube y analizar los requisitos de rendimiento. Esto puede ayudar a ajustar con mayor exactitud las cargas de trabajo tanto en términos de costo como de rendimiento.

## Práctica recomendada 13.2: seleccione instancias de EC2 adecuadas para las cargas de trabajo de SAP

AWS trabaja con SAP para garantizar que los servicios de AWS sean aptos para implementar y operar los software de SAP en distintos tipos de instancias. Utilice a modo de guía las notas y la documentación pertinente de SAP para identificar las instancias adecuadas. Las familias de instancias de EC2 ofrecen diferentes proporciones de CPU y memoria, así como características de rendimiento de red y almacenamiento adecuadas para ejecutar cargas de trabajo de SAP. Asigne sus requisitos al tipo de instancia apropiado con ayuda de métricas de rendimiento, cifras del SAPS y estimaciones computacionales. Confirme la disponibilidad de estas instancias en su región y AZ seleccionadas.

Sugerencia 13.2.1: siga las guías de SAP sobre las bases de datos, sistemas operativos y servicios de AWS compatibles.

AWS ofrece servicios que se pueden usar para la implementación de productos de SAP. En la nota de SAP [1656099 - SAP Applications on AWS: Supported DB/OS and Amazon EC2 products](#) se describe qué productos de SAP, qué combinaciones de bases de datos y sistemas operativos y qué tipos de instancias de Amazon EC2 son actualmente compatibles.

Puede determinar la disponibilidad de tipos de instancias individuales en una AZ específica usando la AWS CLI [para describir ofertas de tipos de instancia](#).

- Documentación de AWS: [Amazon EC2 Instance Types for SAP](#)
- Documentación de SAP: [SAP NetWeaver benchmarks \(Referencias de SAP NetWeaver\)](#)

Sugerencia 13.2.2: utilice métricas de hardware y el SAPS para orientar su elección

Cada familia de instancias de Amazon EC2 compatible con SAP brinda una relación específica de vCPU sobre memoria. Debe evaluar cada familia de instancias en función de sus requisitos para comprender el perfil de rendimiento. La generación actual de instancias de Amazon EC2 (basadas en [AWS Nitro](#)) ofrece el mejor de todos los rendimientos. Estas instancias deben usarse si están disponibles y certificadas para la implementación.



Los servidores de la aplicación SAP pueden usar tanto las instancias de uso general (m\*) como las instancias optimizadas para memoria (r\*). En los casos que se requiera una relación de vCPU sobre memoria mayor, considere usar las instancias optimizadas para la computación (c\*). Para los servidores de bases de datos de AnyDB, las instancias optimizadas para memoria (r\*) son una buena opción para la relación de núcleo sobre memoria requerida, pero se debe realizar un análisis adicional para validar el tamaño, especialmente si su implementación está sujeta a licencias por CPU. Para las bases de datos de SAP HANA que se ejecutan en la memoria, su única opción es una instancia optimizada para memoria (r\*, x\*, u\*).

Sugerencia 13.2.3: utilice el directorio de hardware de SAP HANA y los requisitos de memoria para seleccionar instancias de EC2 para SAP HANA

AWS tiene la certificación de SAP HANA para un subconjunto de instancias de Amazon EC2 para ejecutar cargas de trabajo de SAP HANA. Los detalles de estas instancias y los tipos de aplicaciones de IaaS compatibles (OLAP, OLTP, SAP Business One, Scale-Out) se pueden encontrar en [Certified and Supported SAP HANA Hardware](#) y [Amazon EC2 Instance Types for SAP](#).

El tamaño de la base de datos y el uso real de la memoria de trabajo determinarán los requisitos de memoria y la selección de instancias.

Para las cargas de trabajo que no son de producción, existen opciones adicionales. Consulte el blog:

- Blog de SAP on AWS: [Smaller X1e instances for SAP HANA non-production workloads \(Instancias X1e más pequeñas para cargas de trabajo que no son de producción de SAP HANA\)](#)

Sugerencia 13.2.4: tenga en cuenta las características de la instancia de EC2 y las características de rendimiento

Las instancias de Amazon EC2 tienen diferentes funciones y características de rendimiento que deben evaluarse en función del caso de uso, especialmente para cargas de trabajo con requisitos de rendimiento y de E/S elevados. Esto incluye las capacidades de redes mejoradas mediante el [Elastic Network Adapter \(ENA, adaptador de redes elástico\)](#), el rendimiento de E/S, la optimización de Amazon EBS y la aptitud para los grupos de ubicación. Para una lista completa de las características, consulte los siguientes recursos:

- Documentación de AWS: [Instancias de uso general](#)
- Documentación de AWS: [Instancias optimizadas para memoria](#)
- Documentación de AWS: [Instancias optimizadas para computación](#)

## Práctica recomendada 13.3: seleccione arquitecturas que permitan escalar los sistemas o componentes de forma independiente

Los sistemas y componentes de SAP deberán tener la flexibilidad para escalar sin problemas. Esto se debe lograr dentro del hardware asignado o mediante el escalado horizontal de algunos componentes. Analice cuáles arquitecturas le permiten este tipo de escalado y evalúe compensaciones asociadas.

Sugerencia 13.3.1: considere el impacto en el rendimiento de los componentes o sistemas cruzados

Aísle los componentes o sistemas individuales para evitar el rendimiento negativo entre los componentes. La implementación de varias instancias de tamaño más pequeños puede brindar opciones para la reutilización de instancias, el escalado basado en la carga de trabajo y la capacidad bajo demanda. Hay excepciones cuando se trata de optimizar el uso de recursos por razones de costo. Consulte el pilar de costos para obtener más información.

Sugerencia 13.3.2: tenga en cuenta la flexibilidad de la capacidad para obtener el mayor rendimiento posible

Al seleccionar arquitecturas que permitan escalar componentes, como los servidores de aplicaciones, será posible adaptar su capacidad para que coincida con los requisitos de rendimiento y escalar para obtener una demanda excepcional, lo que incluye el procesamiento de fin de mes o los picos estacionales.

## Práctica recomendada 13.4: elija regiones y AZ para minimizar la latencia

Implemente sus instancias de SAP en regiones y AZ que minimicen la latencia de los procesos empresariales clave que afectan a los usuarios finales, las interfaces críticas y el tráfico dentro del sistema.

Sugerencia 13.4.1: seleccione la región y la conectividad en la nube para optimizar el rendimiento

Elija una región en función de la proximidad a sus usuarios finales de SAP y al centro de datos corporativo. Ajuste el tamaño de cualquier opción de conectividad en la nube (como Direct Connect y VPN) para adaptarse a sus requisitos de transferencia de datos.

Utilice las herramientas de rendimiento de SAP para comprender el desglose del tiempo de respuesta del usuario (como la red, la GUI, la aplicación y la base de datos) y evalúe el impacto de cualquier cambio en el tiempo de ida y vuelta de la red como resultado del aumento de la latencia. Le recomendamos que se concentre en interfaces de alta frecuencia y baja latencia entre sistemas en diferentes ubicaciones.

Si el aumento de la latencia afecta a ciertos grupos de usuarios finales, considere el uso de aceleradores y servicios de computación para usuarios finales.

- Documentación de AWS: [AWS Direct Connect](#)
- Documentación de AWS: [¿Qué es AWS Global Accelerator? - AWS Global Accelerator](#)
- Blog de SAP on AWS: [Deploying SAP GUI on Amazon AppStream 2.0](#)

Sugerencia 13.4.2: tenga en cuenta las pautas de SAP para la latencia dentro del sistema

SAP brinda orientación para lograr una latencia de red aceptable en el tráfico que circula de las aplicaciones a las bases de datos y para replicar el sistema SAP HANA.

- Notas de SAP: [1100926 - FAQ: Network performance \(Preguntas frecuentes: rendimiento de la red\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2543171 - Latency issue between application server and database \(Problema de latencia entre el servidor de la aplicación y la base de datos\)](#) [Se necesita acceso al portal de SAP]

En estas notas, la guía para la conectividad de la base de datos al servidor de aplicaciones se basa en sistemas que se ejecutan en un solo centro de datos, lo que no refleja los beneficios de resistencia de una implementación Multi-AZ. Una AZ es uno o más centros de datos discretos con energía, redes y conectividad redundantes en una región de AWS separados por una distancia significativa (al menos 10 km).

Las arquitecturas de SAP de alta disponibilidad (HA) en AWS generalmente implican la implementación de la infraestructura en múltiples AZ, incluidas las instancias de servidor de la aplicación SAP. Si tiene transacciones de SAP o trabajos por lotes que realizan una cantidad significativa de llamadas a la base de datos, le recomendamos que ejecute estos trabajos en servidores de aplicaciones SAP ubicados en la misma AZ que la base de datos. Además, utilice grupos de inicio de sesión de SAP (transacción SMLG) para usuarios finales y grupos de servidores por lotes (transacción SM61) para trabajos de procesamiento en segundo plano. Esto garantizará que las partes sensibles a la latencia de la carga de trabajo de SAP se ejecuten en los servidores de aplicaciones correctos. Utilice herramientas como NIPING para medir la latencia.

SAP recomienda una latencia de ~1,0 ms para admitir la replicación sincrónica de SAP HANA en modo SYNC, que se puede lograr entre AZ.

- Documentación de SAP: [SAP HANA Network Requirements \(Requisitos de red de SAP HANA\)](#)

### Sugerencia 13.4.3: utilice grupos de ubicación para el escalado horizontal de SAP HANA

Para cumplir con la certificación de SAP para la comunicación entre nodos en una implementación de escalado horizontal de SAP HANA, es necesario usar un grupo con ubicación en clúster.

- Documentación de AWS: [Grupos de ubicación - Amazon Elastic Compute Cloud](#)

## 14. Seleccione la solución de almacenamiento óptima

¿Cómo seleccionar la solución de almacenamiento óptima para su carga de trabajo de SAP? La forma en que configure este almacenamiento afectará el rendimiento de su sistema. AWS ofrece una amplia gama de servicios, incluido el almacenamiento de bloques, archivos y objetos, para satisfacer las necesidades de almacenamiento de sus bases de datos, aplicaciones y copias de seguridad de SAP. Recomendamos seguir las pautas que han sido evaluadas y certificadas por SAP. Para SAP HANA, existen pautas muy específicas. Otras bases de datos requerirán más análisis para adaptarse a su carga de trabajo.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 14.1	Obligatorio	Crear puntos de montaje y asociaciones de volumen para alinear con la función
<input type="checkbox"/> Práctica recomendada 14.2	Obligatorio	Seleccione y configure tipos de Amazon EBS que se alineen con los requisitos de rendimiento.
<input type="checkbox"/> Práctica recomendada 14.3	Recomendado	Evalúe la adecuación del rendimiento de Amazon EFS y Amazon FSx para su caso de uso de SAP
<input type="checkbox"/> Práctica recomendada 14.4	Recomendado	Considere la memoria como una alternativa al almacenamiento

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomenda da 14.5	Recomendado	Elija soluciones de copia de seguridad y programas para el rendimiento de la copia de seguridad a fin de limitar el impacto en los sistemas activos.

## Práctica recomendada 14.1: cree puntos de montaje y asociaciones de volumen para alinear con la función

Los sistemas de archivos de SAP tienen requisitos de compartición y rendimiento únicos. Por ejemplo, el perfil de rendimiento de la base de datos puede requerir que el sistema de archivos de datos admita una gran cantidad de operaciones de E/S de lectura. Por otra parte, es más probable que el sistema de archivos de registro esté limitado por el rendimiento. Sistemas de archivos como `sapmnt` y `trans` necesitan compartirse para que todos los servidores de las aplicaciones puedan acceder a los archivos de transporte y registro. Teniendo en cuenta estas diferencias, considere la asignación de sistemas de archivos a volúmenes para garantizar que no haya cuellos de botella en el rendimiento y que se cumplan los requisitos de acceso.

Sugerencia 14.1.1: identifique los requisitos tanto de los sistemas de archivos de SAP como de sus directorios para cada sistema

Los sistemas de archivos de SAP incluyen directorios del sistema (raíz, inicio), archivos ejecutables, página o intercambio y requisitos específicos de la aplicación. Se debe analizar cada uno para considerar lo siguiente:

- El impacto cuando un sistema de archivos está al máximo de su capacidad (100 % de utilización), en especial, en el directorio raíz.
- Consistencia de la compilación, incluso si está incluida en una AMI o patrones de implementación.
- Requisitos de resiliencia
- Requisitos de compartición
- Perfil de rendimiento

Los requisitos principales del sistema de archivos de SAP se enumeran en la documentación de SAP: directorios y sistemas de archivos requeridos por SAP. Utilice estos como base e incluya otros requisitos específicos de su organización.

Sugerencia 14.1.2: asigne el servicio de almacenamiento de AWS adecuado para que coincida con la función del sistema de archivos

Un sistema de archivos puede ser local o compartido (NFS/SMB). Para los sistemas de archivos compartidos, considere utilizar servicios de AWS, como Amazon EFS y Amazon FSx, que brindan beneficios de fiabilidad y disponibilidad en comparación con un servidor NFS alojado.

El almacén de instancias de Amazon EC2 es otra opción de sistema de archivos que brinda almacenamiento temporal a nivel del bloque para su instancia. No recomendamos su uso debido a la falta de persistencia y disponibilidad entre tipos de instancias y porque impide el uso de la recuperación de instancias.

Sugerencia 14.1.3: utilice tipos de sistemas de archivos admitidos

Las distribuciones de Linux compatibles con SAP recomiendan varios tipos de sistemas de archivos diferentes. Las versiones posteriores se están estandarizando en XFS, pero se debe revisar el soporte para garantizar que no haya un impacto en el rendimiento o la funcionalidad en su sistema operativo y en la versión de la base de datos.

- Notas de SAP: [405827 - Linux: Recommended file systems \(Linux: sistemas de archivos recomendados\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2972496 - SAP HANA Filesystem Types \(tipos de sistemas de archivos de SAP HANA\)](#) [Se necesita acceso al portal de SAP]

Práctica recomendada 14.2: seleccione y configure tipos de EBS alineados con los requisitos de rendimiento.

Para cada función del sistema de archivos y servicio de almacenamiento, evalúe las pautas de diseño de almacenamiento y las opciones de ajuste para garantizar que se optimicen las IOPS y el rendimiento.

Sugerencia 14.2.1: evalúe las características y opciones de almacenamiento para tipos de volumen EBS

AWS tiene una gama de tipos de volúmenes con características únicas para adaptarse a los diferentes requisitos de rendimiento de las cargas de trabajo de SAP. Utilice datos históricos o ajuste de tamaño para evaluar las IOPS y los requisitos de rendimiento. Seleccione su tipo de volumen teniendo en cuenta el rendimiento, la durabilidad, la flexibilidad y el costo.

Las IOPS y el rendimiento de los tipos de volúmenes gp3 , io1 y io2 son independientes del tamaño del volumen.

Las IOPS y el rendimiento del tipo de volumen gp2 están alineados al tamaño del volumen. Es posible que se requiera ajustar el tamaño del volumen para garantizar que las IOPS y el rendimiento necesarios estén disponibles.

- Documentación de AWS: [Tipos de volúmenes de Amazon EBS](#)

Sugerencia 14.2.2: escale linealmente utilizando mecanismos de división de LVM

Cuando el requisito de rendimiento no se puede cumplir con un solo volumen de EBS, considere la posibilidad de dividirlo por medio de la Logical Volume Management (LVM, administración de volúmenes lógicos). Por ejemplo, si un solo volumen tiene una capacidad de rendimiento de 250 MiB/s, poder dividir cuatro volúmenes puede ofrecer un rendimiento de 1000 MiB/s.

Los volúmenes deben ser del mismo tamaño y deben tener las mismas características de rendimiento.

En las pruebas comparativas de SAP HANA, se logró el mejor rendimiento aplicando una división de 256 KB en volúmenes de datos y de 64 KB en volúmenes de registro.

Tenga en cuenta los límites de las instancias para el rendimiento, la E/S y la cantidad de volúmenes adjuntos.

- Documentación de AWS: [Create an LVM Logical Volume on an EBS Volume \(Crear un volumen lógico de LVM en un volumen de EBS\)](#)
- Notas de SAP: [2931808 - Usage of Logical Volume Manager \(LVM\) with SAP HANA \(Uso de Logical Volume Manager \(LVM\) con SAP HANA\)](#) [Se necesita acceso al portal de SAP]
- Documentación de AWS: [Operating System and Storage Configuration - SAP HANA on AWS \(Sistema operativo y configuración de almacenamiento: SAP HANA on AWS\)](#)

Sugerencia 14.2.3: para garantizar el rendimiento de SAP HANA, siga las pautas de almacenamiento proporcionadas por AWS

AWS trabaja con SAP para certificar el almacenamiento de las cargas de trabajo de SAP HANA de acuerdo con los estándares de referencia de rendimiento definidos. La configuración proporcionada por AWS equilibra el rendimiento, el costo y la durabilidad en el marco de los KPI de almacenamiento

de SAP TDI 5. Un diseño de almacenamiento compatible se detalla en la documentación y se usa en Launch Wizard y en las implementaciones de inicio rápido.

- Documentación de AWS: [Storage Configuration for SAP HANA - SAP HANA on AWS \(Configuración de almacenamiento para SAP HANA: SAP HANA on AWS\)](#)

Si se desvía de la configuración de AWS, se recomienda que ejecute la herramienta de verificación de hardware.

- Notas de SAP: [1943937 - Hardware Configuration Check Tool - Central Note \(Herramienta de verificación de configuración de hardware: nota principal\)](#) [Se necesita acceso al portal de SAP]

Al decidir entre SSD de IOPS aprovisionadas y de uso general, es fundamental entender que el “uso general” cumple con los KPI de SAP. Una base de datos en memoria, como SAP HANA, debe cargar datos del disco a la memoria al iniciarse la base de datos. Una solución y un diseño de almacenamiento de alto rendimiento pueden mejorar significativamente los tiempos de inicio y también acelerar las tareas, como las copias de seguridad y las restauraciones, que dependen del rendimiento del almacenamiento.

Los sistemas grandes o aquellos con requisitos de tiempo de disponibilidad (uptime) muy altos pueden beneficiarse de las IOPS aprovisionadas. Comuníquese con su equipo de AWS para obtener más orientación sobre los mejores patrones de implementación.

Sugerencia 14.2.4: para realizar copias de seguridad locales y eficaces a bajo costo, utilice **el almacenamiento** en volúmenes **st1**

Si las soluciones de SAP necesitan almacenamiento local para guardar copias de seguridad, considere usar un tipo de instancia **st1** por su bajo costo y su alto rendimiento. **st1** es un tipo de almacenamiento en bloque de bajo costo diseñado para cargas de trabajo de alto rendimiento y de acceso frecuente.

Para SAP HANA, considere usar AWS Backint Agent for SAP HANA para evitar el impacto en el rendimiento y en los costos de una copia de seguridad de dos etapas.

**Práctica recomendada 14.3: evalúe si el rendimiento de Amazon EFS y Amazon FSx es el indicado para su caso de uso de SAP**

Amazon EFS (Linux) y Amazon FSx (Windows) brindan sistemas de archivos de larga duración y amplia disponibilidad que pueden abarcar varias AZ. Ambas soluciones están diseñadas para ofrecer



un alto rendimiento. Sin embargo, cuando decida utilizar sistemas de archivos de red, tenga en cuenta los patrones de acceso. Por ejemplo, muchos archivos pequeños, escrituras muy paralelas o proporciones altas de escritura o lectura pueden no ser adecuados. Para las cargas de trabajo de SAP, esto podría aplicarse a SAP HANA XSA, archivos ejecutables de Java o una gran cantidad de registros de trabajos y colas.

#### Sugerencia 14.3.1: evalúe opciones de escala y rendimiento

Amazon EFS tiene dos modos de rendimiento (de uso general y de E/S máxima) y dos modos de rendimiento diferentes (modo de ráfaga y de aprovisionado). Para las aplicaciones SAP, el modo de rendimiento de uso general suele proporcionar E/S suficientes. Puede haber situaciones en las que se deba considerar el rendimiento aprovisionado, como cuando la cantidad de datos en su sistema de archivos es baja en relación con las demandas de rendimiento.

- Documentación de AWS: [Amazon Elastic File System \(EFS\) | Preguntas frecuentes: escala y rendimiento](#)
- Documentación de AWS: [Amazon FSx for Windows File Server Features | Scale and Performance \(Funciones de Amazon FSx para el servidor de archivos de Windows | Escala y rendimiento\)](#)

#### Sugerencia 14.3.2: considere utilizar aprovisionamiento temporal para necesidades a corto plazo

Los casos de uso relacionados con migraciones o actividades únicas pueden beneficiarse de un sistema de archivos temporal donde las características de rendimiento se puedan ajustar durante la duración del evento.

### Práctica recomendada 14.4: considere utilizar la memoria como una alternativa al almacenamiento

Considere los beneficios en términos de rendimiento de utilizar la memoria cuando sea posible en la capa de la base de datos o de la aplicación. SAP HANA usa la memoria de forma predeterminada, pero puede beneficiarse de opciones destinadas a la optimización de la carga o descarga de datos estáticos. Las bases de datos relacionales deben aprovechar el almacenamiento en caché y los servidores de aplicaciones deben considerar si el intercambio es un requisito.

#### Sugerencia 14.4.1: optimice el uso de la memoria para SAP HANA

Busque comprender la correlación entre los requisitos de memoria de SAP HANA y los indicadores de memoria del sistema operativo para ayudar a garantizar que los cuellos de botella de la memoria no afecten el rendimiento.

- Documento de SAP: [SAP HANA Memory Usage and the Operating System \(Uso de la memoria de SAP HANA y el sistema operativo\)](#)
- Notas de SAP: [1999997 - FAQ: SAP HANA Memory \(Preguntas frecuentes: memoria de SAP HANA\)](#) [Se necesita acceso al portal de SAP]

Para mejorar el rendimiento del inicio de la base de datos en situaciones que no implican reiniciar el host, considere utilizar la opción Fast Restart de SAP HANA. La opción Fast Restart de SAP HANA dedica una parte de la RAM a un sistema de archivos temporal ( tempfs ), el cual el sistema operativo trata como memoria persistente (hasta que se reinicie el sistema operativo) y permita la colocación de la parte principal del almacén de columnas en ese tempfs , que permanece allí incluso después de un reinicio o colapso del servidor de índices. Por lo tanto, no se vuelve a cargar desde el almacenamiento (usando E/S).

- Documento de SAP: [Documentación de HANA Fast Restart](#)

Sugerencia 14.4.2: utilice el almacenamiento en caché de la base de datos para las bases de datos relacionales

Para una base de datos relacional con altos requisitos de IOP de lectura, el almacenamiento en caché de la base de datos le permite aumentar significativamente el rendimiento y reducir la latencia de recuperación de datos. El caché actúa como una capa de acceso a datos adyacente a su base de datos para mejorar el rendimiento de lectura.

La siguiente documentación proporciona información sobre casos de uso de almacenamiento en caché, pero, como la mayor parte de estos detalles son pertinentes para bases de datos de AWS, consulte las Notas de SAP para obtener información específica sobre la configuración de su base de datos relacional.

- Documentación de AWS: [Caché](#) (incluido [Database Caching \(Almacenamiento en caché de la base de datos\)](#) )

Sugerencia 14.4.3: evalúe los requisitos de espacio de intercambio para aplicaciones SAP

Cuando se agotan los recursos de la memoria física, SAP utiliza el intercambio para mover las páginas inactivas a un área de almacenamiento exclusiva en el disco. Aunque el intercambio puede evitar que la aplicación colapse debido a espacio insuficiente en la memoria, recomendamos aplicar

parámetros de configuración y ajustar el tamaño de la memoria para que el intercambio se use con poca frecuencia.

Si se espera recurrir al intercambio, evalúe las características del volumen asignado para evitar más problemas de rendimiento. El intercambio puede evitar situaciones de falta de memoria para aplicaciones SAP cuando el host se queda sin memoria física.

- Notas de SAP: [153641 - Swap space requirement for R/3 64-bit kernel \(Requisito de espacio de intercambio para kernel R/3 de 64 bits\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2999334 - SWAP Utilization \(Utilización del intercambio\)](#) (Relacionado con HANA) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2488097 - FAQ: Memory usage for the ABAP Server on Windows \(Preguntas frecuentes: uso de memoria para el servidor de ABAP en Windows\)](#) [Se necesita acceso al portal de SAP]

## Práctica recomendada 14.5: elija soluciones de copias de seguridad y esquemas apropiados

Según el método de respaldo, existe la posibilidad de aumentar drásticamente las operaciones de lectura y escritura en su almacenamiento, lo que puede afectar el rendimiento de su aplicación. Esto se da sobre todo con las copias de seguridad a nivel de base de datos que pueden ser de gran volumen y de larga duración.

Sugerencia 14.5.1: determine una franja horaria adecuada para la creación de copias de seguridad

Defina cuál es la franja horaria más apropiada para la ejecución de operaciones de copias de seguridad que se ajusten a los requerimientos de su empresa. Tenga en cuenta las dependencias clave, como la planificación de ejecución de tareas en lotes durante la noche y el tiempo de ejecución aceptable.

Sugerencia 14.5.2: considere opciones para minimizar el impacto en el rendimiento de las copias de seguridad

Analice cualquier restricción de almacenamiento o red y evalúe las opciones para minimizar el impacto de la copia de seguridad. Esto puede incluir la reducción de la duración mediante el uso de copias de seguridad de cambios delta, ya sea a nivel de base de datos o de almacenamiento. Consulte el pilar de fiabilidad para asegurarse de que esto no afecte la coherencia entre las copias de seguridad o el tiempo de restauración general.

- SAP Lens [fiabilidad]: [Práctica recomendada 12.1: establezca un método para la recuperación coherente de datos empresariales](#)

## 15. Evalúe las opciones de ajuste para el sistema operativo, la base de datos y la aplicación SAP

¿Cómo entiende y sopesa los efectos de las diferentes opciones de ajuste en el rendimiento de su sistema SAP? La gran variación en las recomendaciones de rendimiento para las diferentes combinaciones de ofertas de software de SAP y para los sistemas operativos, bases de datos y versiones compatibles imposibilita reunir en un solo documento una lista exhaustiva de recomendaciones para obtener un rendimiento excepcional. Con eso en mente, la siguiente guía debería ser aplicable a la mayoría de los casos de uso de SAP, y mencionaremos áreas de enfoque específicas cuando corresponda.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 15.1	Obligatorio	Siga las pautas del sistema operativo para el rendimiento de SAP
<input type="checkbox"/> Práctica recomendada 15.2	Altamente recomendado	Modifique los parámetros de la base de datos para alinearlos con la selección de hardware
<input type="checkbox"/> Práctica recomendada 15.3	Altamente recomendado	Modifique los parámetros de SAP para alinearlos con la selección de hardware
<input type="checkbox"/> Práctica recomendada 15.4	Recomendado	Ajuste la recuperación y disponibilidad

## Práctica recomendada 15.1: siga las pautas del sistema operativo para el rendimiento de SAP

SAP brinda orientación específica sobre la mejor manera de optimizar el rendimiento de cada uno de los sistemas operativos compatibles con el software de SAP que está implementando. Asegúrese de leer toda la documentación de SAP en la que se hable acerca del sistema operativo en el que está realizando sus implementaciones, de manera que pueda comprender los parámetros de ajuste pertinentes y aprovechar las opciones específicas del sistema operativo y hacer que el ajuste del rendimiento sea más fácil y dinámico.

Sugerencia 15.1.1: revise las notas de SAP relacionadas con el sistema operativo antes de la instalación, actualización de la versión o el cambio de infraestructura

Al crear o actualizar su sistema operativo (de manera automática o manual), confirme que se hayan aplicado las configuraciones de rendimiento adecuadas que sean específicas para su combinación de software de SAP y para la versión del sistema operativo.

Sugerencia 15.1.2: evalúe el ajuste de SAP proporcionado por el proveedor del sistema operativo

Red Hat y SUSE proporcionan imágenes y repositorios que contienen herramientas y configuraciones optimizadas para ejecutar SAP. Estos servicios están disponibles en AWS Marketplace, pero también se pueden integrar mediante el modelo de Bring Your Own Subscription (BYOS, traer su propia suscripción).

Los proveedores están comprometidos en garantizar que sus sistemas operativos estén optimizados para la aplicación SAP. Usar herramientas de ajuste proporcionadas por el proveedor, como saptune o los roles del sistema (Ansible) para Red Hat Enterprise Linux, pueden ayudar a definir un estándar de referencia conocido para el ajuste del rendimiento. Si bien esto no impide ajustar el sistema operativo para adaptarse mejor a su carga de trabajo específica de SAP, estas herramientas pueden reducir el esfuerzo asociado con la investigación, el cálculo y la aplicación de los requisitos más comunes. Las configuraciones vinculadas con el daemon `ajustado` también se pueden ajustar de forma dinámica utilizando la información que recopila del sistema, incluido el número de CPU y la memoria disponible.

Sistema operativo	Guía
SUSE Linux Enterprise Server	Notas de SAP: <a href="#">1275776 - Linux: Preparing SLES for SAP environments (Linux: preparación de SLES para entornos de SAP)</a> [Se necesita acceso al portal de SAP]

Sistema operativo	Guía
Red Hat Enterprise Linux	Notas de SAP: <a href="#">2777782 - SAP HANA DB: Recommended OS Settings for RHEL 8</a> [Se necesita acceso al portal de SAP]
Microsoft Windows	(Consulte la documentación de SAP o del proveedor a modo de guía)
Oracle Enterprise Linux	Notas de SAP: <a href="#">2478541 - Operating System Requirements for Oracle Database (Requisitos del sistema operativo para Oracle Database)</a> [Se necesita acceso al portal de SAP]

### Sugerencia 15.1.3: aplique parámetros de red pertinentes al sistema operativo

El rendimiento del sistema SAP puede verse seriamente afectado por una mala configuración de la red, en especial, cuando se trata de diseños de bases de datos escalables horizontalmente de SAP HANA y de comunicaciones entre diferentes instancias del servidor de aplicaciones y la instancia de la base de datos en un entorno del sistema. Si bien en muchos casos en AWS, el rendimiento máximo de la red de una instancia lo determina la familia y el tamaño de la instancia, el ajuste de la configuración de la red a nivel del sistema operativo y en el propio software de SAP puede tener un impacto.

Consulte las siguientes recomendaciones de SAP y de AWS:

- Documentación de AWS: [Evaluación basada en el rendimiento de la red entre instancias de Linux de Amazon EC2 en la misma VPC de Amazon](#)
- Documentación de AWS: [Elastic Network Adapter – High Performance Network Interface for Amazon EC2 \(Adaptador de red elástico: interfaz de red de alto rendimiento para Amazon EC2\)](#)
- Documentación de AWS: [Grupos de ubicación de clúster](#)
- Notas de SAP: [2198693 - Key Monitoring Metrics for SAP on Amazon Web Services \(AWS\) \(Métricas de supervisión clave para SAP en Amazon Web Services \[AWS\]\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [1612283 - Hardware Configuration Standards and Guidance \(Guía y estándares de configuración de hardware\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2081065 - Troubleshooting SAP HANA Network \(solución de problemas de red de SAP HANA\)](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [1100926 - FAQ: Network performance](#) [Se necesita acceso al portal de SAP]

## Práctica recomendada 15.2: modifique los parámetros de la base de datos para alinearlos con la selección de hardware

SAP brinda una orientación específica para optimizar el rendimiento de un sistema SAP mediante la modificación de determinados parámetros de la base de datos subyacente. Estos parámetros son específicos del tipo de base de datos y pueden variar en función de si admite una aplicación de tipo analítico o transaccional.

Sugerencia 15.2.1: revise los parámetros de ajuste específicos de SAP HANA, si corresponde

Los parámetros del sistema operativo y de la base de datos SAP HANA pueden afectar enormemente el rendimiento. Siga las recomendaciones de SAP on AWS correspondientes al sistema operativo y a la configuración de almacenamiento.

- Documentación de AWS: [SAP HANA on AWS – Operating System and Storage Configuration \(SAP HANA on AWS: sistema operativo y configuración de almacenamiento\)](#)

Consulte las notas y la documentación de SAP para obtener orientación sobre los parámetros de SAP HANA, incluida la asignación de memoria.

- Notas de SAP: [2000000 - FAQ: SAP HANA Performance Optimization \(Preguntas frecuentes: optimización del rendimiento de SAP HANA\)](#) [Se necesita acceso al portal de SAP]
- Documentación de SAP: [HANA Parameter: global\\_allocation\\_limit \(Parámetro de HANA: global\\_allocation\\_limit\)](#)
- Notas de SAP: [1999997 - FAQ: SAP HANA Memory](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [2926166 - How to limit the overall SAP HANA memory allocation \(Cómo limitar la asignación de memoria general de SAP HANA\)](#) [Se necesita acceso al portal de SAP]

Sugerencia 15.2.2: revise la guía de ajuste de bases de datos para bases de datos que no son de SAP HANA

Independientemente de la base de datos subyacente de su sistema SAP, el rendimiento del sistema depende en parte de cómo se ajuste la base de datos. Cada base de datos tiene recomendaciones específicas para el ajuste en función de la capacidad de computación, de memoria y de almacenamiento en disco disponibles. Ciertos parámetros de la base de datos dependen de su elección del tamaño de la instancia de EC2 subyacente; por ejemplo, la memoria física disponible limitará el parámetro `db_cache_size` de una base de datos Oracle.

Para obtener información pertinente para su base de datos, consulte lo siguiente:

Base de datos	Guía
SAP ASE	Notas de SAP: <a href="#">2473646 - Performance and Tuning information for ASE - SAP ASE (Información de rendimiento y ajuste para ASE -SAP ASE)</a> [Se necesita acceso al portal de SAP]
IBM Db2	Notas de SAP: <a href="#">2751102 – DB6: DB2 11.5 Standard Parameter Settings (DB6: DB2 11.5 Configuración de parámetros estándar)</a> [Se necesita acceso al portal de SAP]
Oracle	Notas de SAP: <a href="#">2470718 – Oracle Database Parameter 12.2 / 18c / 19c (Parámetro de la base de datos Oracle 12.2/18c/19c)</a> [Se necesita acceso al portal de SAP]
Microsoft SQL Server	Notas de SAP: <a href="#">2779607 – Configuration Parameters for SQL Server 2019 (Parámetros de configuración para SQL Server 2019)</a> [Se necesita acceso al portal de SAP], nota de SAP: <a href="#">2729848 – SAP Installation Media and SQL4SAP for SQL Server 2019 (Medios de instalación de SAP y SQL4SAP para SQL Server 2019)</a> [Se necesita acceso al portal de SAP]
SAP MaxDB	Notas de SAP: <a href="#">819641 – FAQ: SAP MaxDB performance (Preguntas frecuentes: rendimiento de SAP MaxDB)</a> [Se necesita acceso al portal de SAP]

## Práctica recomendada 15.3: modifique los parámetros de SAP para alinearlos con la selección de hardware

Ajustar los parámetros de la aplicación SAP puede ayudar a mejorar el rendimiento de la aplicación. Estos parámetros suelen depender de la configuración del hardware subyacente y del tipo de sistema operativo.

Sugerencia 15.3.1: permita que SAP se autoajuste en función de **PHYS\_MEMSIZE**

En las versiones recientes del software de SAP, si se usa la versión 7.40 o superior del kernel, se recomienda configurar el ajuste automático de ciertos parámetros. Por ejemplo, muchos parámetros



se derivan mediante fórmulas relacionadas con la memoria principal disponible en una instancia (PHYS\_MEMSIZE). Esto permite el ajuste automático de los parámetros de la memoria al cambiar el tamaño de una instancia de EC2 subyacente al software de SAP para cumplir con requisitos de rendimiento cambiantes.

- Documentación de SAP: [SAP Memory Management: Parameter Reference \(Gestión de memoria SAP: referencia de parámetros\)](#)
- Notas de SAP: [2085980 – New features in memory management as of Kernel Release 7.40 \(Nuevas funciones en la gestión de memoria a partir de la versión 7.40 del kernel\)](#) [Se necesita acceso al portal de SAP]

Sugerencia 15.3.2: revise el espacio de intercambio de SAP y el uso máximo de memoria

Cuando se ejecuta SAP on AWS, el espacio de intercambio sobreutilizado en el disco puede provocar el agotamiento del crédito de E/S en Amazon EBS y provocar una degradación del rendimiento. Evalúe las diferentes opciones [de almacenamiento de EBS](#) disponibles en AWS y configure el espacio de intercambio para satisfacer sus necesidades de rendimiento.

- Notas de SAP: [1597355 - Swap-space recommendation for Linux \(Recomendación de espacio de intercambio para Linux\)](#) [Se necesita acceso al portal de SAP]
- Documentación de SAP: [Swap Space Requirements \(Requisitos del espacio de intercambio\)](#)

Práctica recomendada 15.4: considere el ajuste del rendimiento para las opciones de recuperación y disponibilidad

En consonancia con los pilares de fiabilidad y excelencia operativa de Well-Architected, se debe evaluar el ajuste del sistema SAP en función de los requisitos de recuperación y resiliencia elegidos para minimizar cualquier impacto en el rendimiento. Tenga en cuenta elementos como el rendimiento del sistema durante una copia de seguridad, las opciones de agrupación en clústeres para la base de datos elegida (por ejemplo, una replicación sincrónica del sistema SAP HANA en vez de una asincrónica) y la distribución de la carga entre varias instancias del servidor de aplicaciones SAP.

Sugerencia 15.4.1: revise las recomendaciones de rendimiento para las copias de seguridad y las soluciones de recuperación

A cada base de datos compatible, le corresponden diferentes recomendaciones para la optimización del rendimiento de las operaciones de copia de seguridad y recuperación, y estas suelen funcionar

con la solución de software elegida para administrar las copias de seguridad y las restauraciones, incluidas las ofertas de terceros. Entre los ejemplos que se pueden encontrar en AWS, se incluyen la configuración de los valores máximos de las IOPS y del rendimiento para los volúmenes de EBS y la configuración de los parámetros de simultaneidad cuando se usa AWS Backint Agent para SAP HANA.

En general, si sigue las pautas para mejorar el rendimiento entre una instancia de EC2 y la ubicación de almacenamiento de destino de su copia de seguridad (como volúmenes de EBS, buckets de S3 y sistemas de archivos de EFS), podrá mejorar el rendimiento de su copia de seguridad y recuperación. Por ejemplo, cuando se utiliza Amazon S3 como repositorio para copias de seguridad, el uso de la AWS Command Line Interface (AWS CLI) para Amazon S3 puede permitir mejoras en el rendimiento mediante la realización de cambios [en parámetros de configuración](#) tales como el número máximo de solicitudes concurrentes o el tamaño de fragmentos multipartes.

Para obtener más información, consulte lo siguiente:

- Documentación de AWS: [AWS Backint Agent para SAP HANA](#)
- Documentación de AWS: [SAP NetWeaver on AWS – Backup and Recovery \(SAP NetWeaver on AWS: copia de seguridad y recuperación\)](#)
- Blog de SAP on AWS: [Build for availability and reliability \(Crear para obtener disponibilidad y fiabilidad\)](#)

Base de datos	Guía
SAP HANA	<ul style="list-style-type: none"> <li>• Documentación de AWS: <a href="#">SAP HANA on AWS – Storage Configuration for SAP HANA (SAP HANA on AWS: configuración de almacenamiento para SAP HANA)</a> [Se necesita acceso al portal de SAP]</li> <li>• Notas de SAP: <a href="#">1842096 - HANA Backup &amp; Restore Performance (Rendimiento de copia de seguridad y restauración de HANA)</a> [Se necesita acceso al portal de SAP]</li> <li>• Notas de SAP: <a href="#">2945518 - Performance issues encountered on HANA when a data backup is running (Problemas de rendimiento en HANA cuando se ejecuta una copia de seguridad de datos)</a> [Se necesita acceso al portal de SAP]</li> </ul>
SAP ASE	(Consulte la documentación de SAP o del proveedor a modo de guía)

Base de datos	Guía
IBM Db2	(Consulte la documentación de SAP o del proveedor a modo de guía)
Oracle	Notas de SAP: <a href="#">2084077 - How to plan backup cycle for Oracle database (Cómo planificar el ciclo de copia de seguridad para la base de datos de Oracle)</a> [Se necesita acceso al portal de SAP]
Microsoft SQL Server	Notas de SAP: <a href="#">1420452 - FAQ: Restore and recovery with MS SQL Server (Preguntas frecuentes: restauración y recuperación con MS SQL Server)</a> [Se necesita acceso al portal de SAP]
SAP MaxDB	Notas de SAP: <a href="#">1377148 - FAQ: SAP MaxDB backup / recovery (Preguntas frecuentes: copia de seguridad y recuperación de SAP MaxDB)</a> [Se necesita acceso al portal de SAP]

Sugerencia 15.4.2: revise la configuración de los parámetros de agrupación de clústeres

Las opciones de agrupación en clúster para SAP HANA y otras bases de datos se suelen basar en una conexión confirmada en un clúster (es decir, un latido) entre la instancia principal y la instancia de conmutación por error. Los administradores de SAP deben buscar un equilibrio entre la velocidad con la que puede ocurrir una acción en el sistema y la probabilidad de que se produzcan efectos secundarios de conmutación por error si hay una interrupción falsa en la comunicación. Siga las recomendaciones correspondientes a los parámetros de tiempo de espera y la configuración relacionada.

- Documentación de AWS: [SAP HANA on AWS: High Availability Configuration Guide for SLES and RHEL \(SAP HANA on AWS: guía de configuración de alta disponibilidad para SAP en RHEL\)](#)
- Documentación de AWS: [SAP HANA on AWS Operations Guide: Networking \(SAP HANA on AWS: guía de operaciones, redes\)](#)
- Documentación de AWS: [SAP on AWS – IBM Db2 HADR with Pacemaker](#)
- Notas de SAP: 1612105 [DB6: FAQ on Db2 High Availability Disaster Recovery \(HADR\)](#) [Se necesita acceso al portal de SAP]
- Documentación específica del sistema operativo: [SUSE Linux SAP HSR Scale-up Performance Optimized Scenario \(Caso de rendimiento optimizado del escalado horizontal de SAP HSR para SUSE Linux\)](#)

- Documentación específica del sistema operativo: [Automated SAP HANA System Replication in Scale-Up in pacemaker cluster \(Automatización de la replicación de sistema del escalado vertical de SAP HANA en clúster de marcapasos\)](#)

## 16. Comprenda las opciones de optimización y rendimiento en curso

¿Qué procesos y procedimientos implementa para medir los cambios de rendimiento y las oportunidades de optimización? Calcule el requisito de rendimiento de sus aplicaciones a partir de sus datos de supervisión históricos y establezca alertas relevantes para informar a los administradores del sistema cuando se produzcan desviaciones. Tenga procedimientos establecidos para que los administradores del sistema resuelvan tales problemas con acciones manuales o automatizadas.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 16.1	Obligatorio	Cuente con datos para evaluar el rendimiento
<input type="checkbox"/> Práctica recomendada 16.2	Obligatorio	Establezca requisitos de rendimiento básicos
<input type="checkbox"/> Práctica recomendada 16.3	Altamente recomendado	Identifique tendencias de rendimiento por medio de datos
<input type="checkbox"/> Práctica recomendada 16.4	Altamente recomendado	Identifique y clasifique problemas de rendimiento
<input type="checkbox"/> Práctica	Altamente recomendado	Escale de forma dinámica para satisfacer las demandas de rendimiento

ID	Prioridad	Práctica recomendada
recomenda da 16.5		
<input type="checkbox"/> Práctica recomenda da 16.6	Recomendado	Desarrolle mecanismos para simular la carga de producción a los fines de realizar un análisis.
<input type="checkbox"/> Práctica recomenda da 16.7	Recomendado	Optimice continuamente el ajuste de tamaño y la configuración en función de los datos de rendimiento

## Práctica recomendada 16.1: cuente con datos para evaluar el rendimiento

Para evaluar el rendimiento de un sistema SAP y tomar medidas en caso de que el rendimiento sea inferior al óptimo, se deben recopilar datos de supervisión sobre la computación, la memoria, el almacenamiento y las redes, como se describe en las Pautas de excelencia en el rendimiento de Well-Architected Framework en lo que respecta a la supervisión de sus recursos. Como se afirma en el pilar de excelencia operativa de Well-Architected Framework, entender el estado actual del sistema, establecer indicadores claves de rendimiento y recolectar métricas de manera oportuna para diagnosticar son acciones fundamentales para investigar los problemas de rendimiento.

- Well-Architected Framework [eficiencia de rendimiento]: [Monitoree los recursos para garantizar que el rendimiento es óptimo](#)
- Well-Architected Framework [excelencia operativa]: [Comprensión del estado de la carga de trabajo](#)

### Sugerencia 16.1.1: reúna y almacene datos pertinentes a las métricas de rendimiento

Para recolectar y visualizar datos de supervisión de SAP, debe instalar y configurar AWS Data Provider for SAP y establecer las métricas en las herramientas de supervisión elegidas que respaldan su carga de trabajo de SAP. Hay más detalles disponibles sobre la supervisión y las recomendaciones adicionales en el pilar de excelencia operativa.

- Documentación de AWS: [AWS Data Provider for SAP \(Proveedor de datos de AWS para SAP\)](#)

- SAP Lens [excelencia operativa]: [Práctica recomendada 1.1: implemente los requisitos previos para la supervisión de SAP on AWS](#)
- SAP Lens [excelencia operativa]: [Práctica recomendada 1.2: implemente la supervisión de infraestructura para SAP](#)
- SAP Lens [excelencia operativa]: [Práctica recomendada 1.3: implemente la supervisión de aplicaciones individuales para SAP](#)

## Práctica recomendada 16.2: establezca requisitos de rendimiento de referencia

Cada aplicación SAP tiene requisitos de rendimiento únicos. El uso de datos de supervisión históricos ayuda a los equipos administrativos de SAP a entender el rendimiento inicial de estas aplicaciones, lo que les permite identificar y entender la extensión de los cambios de rendimiento. Se pueden implementar alertas pertinentes para detectar anomalías como picos imprevistos en la CPU, diferencias en el rendimiento de almacenamiento, aumentos en el consumo de memoria y disminuciones de rendimiento más complejas. Estos datos de supervisión se pueden utilizar para optimizar aún más el rendimiento.

Sugerencia 16.2.1: recolecte y evalúe los datos que reflejan KPI específicos de SAP

Esta sugerencia tiene un alineamiento estrecho con las sugerencias adicionales contenidas en el análisis del pilar de eficiencia de rendimiento de Well-Architected Framework [sobre la supervisión de recursos](#).

Además de esta guía general, los KPI específicos de SAP incluyen el tiempo de respuesta del diálogo, los intercambios de buffers y la memoria utilizada. Estos KPI pueden diferir con base en el tipo de software de SAP y en la versión que se ejecuta. Hay más detalles disponibles sobre los KPI y las recomendaciones de supervisión en este documento, en el pilar de excelencia operativa:

- SAP Lens [excelencia operativa]: [Práctica recomendada 1.2: implemente la supervisión de infraestructura para SAP](#)
- SAP Lens [excelencia operativa]: [Práctica recomendada 1.3: implemente la supervisión de aplicaciones individuales para SAP](#)

## Práctica recomendada 16.3: identifique tendencias de rendimiento a través de datos

Una vez establecidos los valores iniciales de rendimiento, los administradores del sistema deben supervisar las tendencias a lo largo del tiempo para determinar si los KPI se mantienen estables

dentro de las normas preferidas. Si los datos de rendimiento indican una tendencia hacia valores inaceptables de los KPI, los administradores del sistema pueden seguir una serie de instrucciones para evitar o mitigar los efectos en el rendimiento.

#### Sugerencia 16.3.1: realice revisiones regulares del rendimiento del sistema SAP

Mediante las revisiones periódicas de los KPI, los administradores del sistema pueden identificar tendencias en los datos relacionados con el rendimiento, además de determinar qué alertas pueden ser más beneficiosas. A continuación, se pueden utilizar estas alertas para automatizar las notificaciones si la tendencia se mantiene e implementar medidas de autocorrección para abordar los problemas de rendimiento potenciales (por ejemplo, cambios dinámicos de los parámetros de SAP en respuesta a los indicadores de rendimiento). Los ejemplos de KPI y de las tendencias relacionadas se pueden encontrar en los informes de SAP EarlyWatch Alert, que en algunos casos se pueden personalizar con métricas útiles adicionales. Los informes de niveles de servicio de SAP también pueden resultarle útiles si sus cargas de trabajo de SAP están atadas a un SLA.

- Documentación de SAP: [Service Level Reporting \(Informes de nivel de servicio\)](#)
- Notas de SAP: [1040343 SAP EarlyWatch Alert](#) [Se necesita acceso al portal de SAP]
- Notas de SAP: [1829914 Customize EWA Reports \(Personalizar Informes de EWA\)](#) [Se necesita acceso al portal de SAP]

#### Sugerencia 16.3.2: retenga los datos históricos para identificar tendencias

Es recomendable que retenga los datos de rendimiento y sus registros asociados durante un período predeterminado para comprender las tendencias en el comportamiento del sistema. El ajuste de rendimiento de cualquier sistema SAP depende de la capacidad para repasar períodos históricos de días, semanas y meses, y descubrir qué constituye una tendencia de rendimiento o un evento de rendimiento cíclico. Entre algunos sucesos frecuentes que requieren la retención de datos para observar los efectos en el rendimiento, se incluyen los siguientes:

- Procesamiento financiero a fin de mes y a fin de año
- Aumento de los requisitos de presentación de informes en relación con los hitos comerciales (por ejemplo, después de un gran lanzamiento de ventas semestral)
- Incorporación de una gran población de usuarios nuevos de SAP dentro del negocio
- Cambios en la tecnología, como ajuste de tamaño de la infraestructura, revisiones de bases de datos, actualizaciones de la versión del sistema operativo o actualizaciones del software de SAP

## Práctica recomendada 16.4: identifique y clasifique problemas de rendimiento

Cuando las métricas clave muestran un deterioro del rendimiento, implemente un proceso para corregir la causa subyacente. Gracias a la automatización (consulte la práctica recomendada a continuación sobre el escalado dinámico), puede reducir la necesidad de intervención manual. No obstante, cuando esto no es posible, es fundamental establecer un proceso de alertas automatizado para los administradores.

Sugerencia 16.4.1: configure las alertas de rendimiento de manera apropiada

Siga las pautas mencionadas en el pilar eficiencia de rendimiento de Well-Architected Framework que versan sobre la supervisión y las alertas, y utilice las capacidades de alerta de SAP si se proveen capacidades adicionales. También puede encontrar más detalles en [excelencia operativa] [1. Diseñe la carga de trabajo de SAP para permitir la comprensión y la reacción a su estado](#) .

- Well-Architected Framework [eficiencia de rendimiento]: [Monitoreo](#)
- Documentación de SAP: [SAP NetWeaver Alert Monitor \(Monitor de alertas de SAP NetWeaver\)](#)

Sugerencia 16.4.2: corrección automática de incidentes de rendimiento

Si bien la administración de incidentes de rendimiento incluye las prácticas recomendadas en materia de operaciones detalladas en el pilar de excelencia operativa de Well-Architected Framework, la detección proactiva y la corrección automatizada del deterioro de rendimiento potencial pueden prevenir la profundización de un problema de rendimiento y mejorar la experiencia del usuario final. Cuando no es posible implementar procesos automatizados para mitigar un problema de rendimiento, tener un manual de procedimientos detallado sobre cómo deben responder los equipos operativos ante un problema de rendimiento puede acelerar la respuesta a un incidente de rendimiento.

- SAP Lens [excelencia operativa]: [Práctica recomendada 1.8: utilice técnicas de respuesta y recuperación automatizadas para reaccionar a las alertas de supervisión](#)
- Well-Architected Framework [excelencia operativa]: [Prácticas recomendadas: operar](#)

## Práctica recomendada 16.5: escale para satisfacer las demandas de rendimiento

Uno de los beneficios principales de operar cargas de trabajo en AWS es la capacidad de aumentar o disminuir la capacidad de computación y cambiar las características de rendimiento de almacenamiento para que coincidan con el rendimiento requerido para el caso de uso. En las



cargas de trabajo de SAP, utilice el escalado dinámico cuando corresponda para evitar los cuellos de botella de rendimiento. Para las situaciones en las que el escalado dinámico no es posible, como el escalado horizontal de un clúster de base de datos de SAP HANA, utilice un proceso de implementación manual.

#### Sugerencia 16.5.1: escale de forma reactiva las cargas de trabajo de SAP

En respuesta a los cambios dinámicos en los requisitos de rendimiento de las cargas de trabajo, escale sus recursos de SAP según corresponda. Cuando sea posible, utilice la automatización para reducir o aumentar el escalado horizontal. Si esta opción no es factible (por ejemplo, para el escalado vertical de una instancia de base de datos), implemente un proceso para hacerlo de forma manual. Considere lo siguiente:

- Agregar o eliminar la capacidad del servidor de la aplicación o cambiar los tamaños de la instancia según sea necesario para satisfacer la demanda
- Cambiar los parámetros de SAP para redistribuir los recursos virtuales de forma programática
- [Modificar el tipo de almacenamiento](#) (por ejemplo, Amazon EBS gp3 para io2 o viceversa en AWS), si corresponde, para optimizar el rendimiento de almacenamiento.

#### Sugerencia 16.5.2: programe el escalado de las cargas de trabajo de SAP predecibles

Independientemente de si se hace de forma automatizada o manual, se aconseja aumentar o reducir el escalado vertical de las cargas de trabajo de SAP con base en los patrones de rendimiento predecibles. Por ejemplo, cuando el procesamiento financiero a fin de mes en un sistema ECC de SAP deriva en un aumento predecible del 20 % en los requisitos de procesamiento en las instancias del servidor de la aplicación, los administradores del sistema pueden aumentar de manera proactiva la cantidad o el tamaño de los servidores de la aplicación y, luego, reducir horizontalmente la cantidad de instancias cuando el uso disminuye conforme a las predicciones.

#### Práctica recomendada 16.6: desarrolle mecanismos para simular la carga de producción a los fines de realizar un análisis

Contar con un clon de los datos de producción en un sistema de prueba permite a los administradores del sistema simular cargas de trabajo de SAP de producción y realizar pruebas de rendimiento vitales, como pruebas de estrés y volumen. Este tipo de pruebas puede ayudar a identificar cuellos de botella de rendimiento potenciales y evitar que ocurran problemas de rendimiento en un entorno de producción en tiempo real.

## Sugerencia 16.6.1: realice pruebas de estrés y volumen automatizadas en sistemas SAP

Copiar datos de producción en un entorno de prueba es relativamente fácil cuando se ejecutan en AWS (por ejemplo, a través de [instantáneas de EBS desde un entorno de producción](#) para crear una instancia de prueba nueva), aunque se debe tener cuidado de seguir correctamente los pasos posteriores a la copia, manuales o automatizados. Estos pasos posteriores a la copia pueden consistir en cambiar los nombres del sistema lógico a través del código de transacción BDLS, aleatorizar o borrar datos de producción sensibles y configurar una integración con los sistemas de prueba relacionados. Otro beneficio adicional es que los sistemas de prueba de rendimiento aislados no tienen que ser permanentes, dado que las instancias se pueden aprovisionar, configurar y apagar según sea necesario.

Existen diversas maneras de aplicar cargas al sistema de pruebas:

- En AWS, la solución [de pruebas de carga distribuidas](#) puede ser una opción útil para las pruebas de carga automatizadas.
- Se puede realizar mediante la creación y automatización de scripts en el software de SAP a través de [eCATT \(Herramienta de prueba asistida por computadora extendida\)](#).
- Se puede realizar mediante el uso de soluciones de prueba automatizadas de terceros.
- Se puede realizar mediante la creación de scripts a nivel del sistema operativo para iniciar los programas adecuados a escala dentro del sistema SAP.

## Práctica recomendada 16.7: optimice continuamente el ajuste de tamaño y la configuración en función de los datos de rendimiento

Revise las métricas de rendimiento de manera regular y externa al proceso de respuesta a incidentes. De esta manera, puede descubrir qué componentes del sistema tienen un tamaño deficiente o excesivo o ya no se usan. Se debe establecer una cadencia de optimización de rendimiento regular para las cargas de trabajo de SAP, con un enfoque en el ajuste de tamaño correcto de los componentes del sistema para la carga real del usuario. Esta actividad mejorará la experiencia del usuario, eliminará los aspectos innecesarios de la arquitectura y ayudará a mejorar la rentabilidad y la resiliencia de la carga de trabajo.

Sugerencia 16.7.1: regularmente, ajuste el tamaño correcto de la arquitectura con las métricas de rendimiento histórico como guía

Revise de manera regular su carga de trabajo de SAP en busca de oportunidades para ajustar correctamente el tamaño de sus componentes. Considere si es necesario aumentar o disminuir

el almacenamiento, la computación, las redes y los servicios de soporte para satisfacer mejor los requisitos de rendimiento de su negocio.

Para obtener más información, consulte los siguientes recursos:

- SAP Lens [optimización de costos]: [Práctica recomendada 20.5: revise el uso para detectar oportunidades de optimización](#)
- SAP Lens [excelencia operativa]: [Práctica recomendada 4.4: realice revisiones regulares de las cargas de trabajo para optimizarlas en función de resiliencia, rendimiento, agilidad y costos](#)
- Documentación de AWS: [Tamaño correcto](#)

## Optimización de costos

El pilar de optimización de costos incluye el proceso continuo de perfeccionamiento y mejora de un sistema durante todo su ciclo de vida. Esta optimización debe ocurrir desde el diseño inicial de la primera prueba de concepto hasta la operación continua de las cargas de trabajo de producción. Elija la solución y el modelo de precios correctos y cree sistemas económicos que le permitan lograr resultados comerciales y minimizar los costos. Para alcanzar la optimización de costos con el tiempo, tiene que identificar los datos, recursos de infraestructura o trabajos de análisis que se pueden eliminar o reducir.

### 17. Evalúe los patrones de arquitectura de SAP con un enfoque en la rentabilidad

¿Cómo se incorporan las consideraciones de costos en la evaluación de los patrones de arquitectura de SAP? A la hora de tomar decisiones sobre la arquitectura, verifique que se comprendan totalmente las consecuencias en los costos como parte de las consideraciones de diseño.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomenda da 17.1	Obligatorio	Evalúe su uso de las ofertas de servicios administrados por SAP
<input type="checkbox"/> Práctica	Obligatorio	Evalúe las características de costos de su patrón de arquitectura de aplicaciones SAP

ID	Prioridad	Práctica recomendada
recomendada 17.2		
<input type="checkbox"/> Práctica recomendada 17.3	Obligatorio	Comprenda los requisitos comerciales para tomar decisiones de diseño optimizadas para los costos según el entorno
<input type="checkbox"/> Práctica recomendada 17.4	Altamente recomendado	Revise el tamaño, la granularidad y las últimas opciones de instancia de EC2 disponibles para los componentes de SAP
<input type="checkbox"/> Práctica recomendada 17.5	Altamente recomendado	Considere utilizar la capacidad bajo demanda para mejorar la rentabilidad
<input type="checkbox"/> Práctica recomendada 17.6	Recomendado	Evalúe los beneficios de costos y el efecto de los servicios y soluciones compartidos
<input type="checkbox"/> Práctica recomendada 17.7	Recomendado	Evalúe los beneficios de costos de la automatización

## Práctica recomendada 17.1: evalúe su uso de las ofertas de servicios administrados por SAP

Según el modelo de responsabilidad compartida de AWS, el cliente tiene la responsabilidad de administrar sus cargas de trabajo de SAP en AWS. De manera opcional, se puede emplear un proveedor de servicio para administrar las cargas de trabajo de SAP en AWS. A la hora de evaluar a un proveedor de servicio, es preciso que la responsabilidad de la administración de costos iniciales y continuos se delegue correctamente y que se trate como un proceso continuo.

Varios socios de AWS prestan servicios para la implementación y la operación de su infraestructura SAP. El alcance y la madurez de los servicios prestados varían para cada socio. Estos tipos de servicios pueden aportar eficiencias, por ejemplo, apoyo centralizado o servicios de implementación automatizados. Pueden reducir sus costos generales y deben evaluarse según los requisitos específicos de su negocio. Evalúe las competencias en AWS de los socios, incluidos [los socios de SAP Consulting Competency](#) y de la AWS Partner Network (APN, red de socios de AWS).

Sugerencia 17.1.1: entienda los roles y responsabilidades relacionados con el control de costos

Distintas ofertas de servicios administrados poseen modelos de costos diferentes para cubrir la infraestructura, el otorgamiento de licencias y los servicios. Decida en dónde recae la responsabilidad del control de costos. Se pueden hacer las siguientes preguntas como parte de este proceso.

- Responda estas preguntas sobre los costos del proveedor:
  - ¿Dependen de un porcentaje del gasto en infraestructura?
  - ¿Dependen de un Total Cost of Ownership (TCO, costo total de propiedad) acordado?
- ¿Tienen un tamaño a medida (pequeño, mediano, grande)? ¿Se ha implementado un proceso de control de cambios adecuado para garantizar que los costos estén controlados y se comprendan?
- ¿La visibilidad y la transparencia de los costos de infraestructura son suficientes?
- ¿La administración de costos limita la innovación y flexibilidad?

Sugerencia 17.1.2: convenga un enfoque para la administración y optimización de costos con todas las partes

Al evaluar las distintas ofertas de servicios administrados disponibles, se debe comprender el enfoque del socio de los servicios administrados con respecto a la administración de costos. ¿Cómo pueden trabajar juntos para llevar adelante una optimización de costos continua para su organización?

Esta evaluación debe incluir un proceso regular de revisión. También se puede beneficiar de incentivos, como un modelo de recompensas compartido, que aliente al socio a tomar la iniciativa para que las dos partes obtengan beneficios financieros de los ahorros de costos alcanzados.

## Práctica recomendada 17.2: evalúe las características de costos de su patrón de arquitectura de aplicaciones SAP

Mientras diseña la arquitectura de su infraestructura SAP, tenga en cuenta el costo del número de componentes de infraestructura y también su tamaño y ubicación. Al establecer los requisitos empresariales de la solución y reconocer el riesgo y las oportunidades de optimización, puede obtener importantes ahorros de costos.

### Sugerencia 17.2.1: revise los patrones de instalación de SAP seleccionados

Para cada aplicación SAP, defina la naturaleza de su patrón de implementación: independiente, distribuido o de alta disponibilidad. Seleccione el modelo arquitectónico que ofrece el mejor equilibrio entre costos y características de fiabilidad para satisfacer los requisitos de su empresa. Un método útil es cuantificar el costo que significaría una interrupción de su empresa y trabajar a partir de ese punto. Compare el riesgo de un error individual que afecte la disponibilidad con el costo de reducir ese riesgo.

Además, considere si su arquitectura tiene la flexibilidad de implementar un ajuste de tamaño correcto. Se pueden ahorrar costos con la concesión de licencias de sistemas operativos y con el almacenamiento y la administración de múltiples servidores de aplicaciones en un solo host. A nivel de las aplicaciones, existen diversos tamaños de instancias con un alto grado de especificidad para la CPU y la memoria y cuyos precios son casi invariables en las familias de instancias compatibles. La implementación de instancias más pequeñas puede ofrecer más opciones para la reutilización de instancias y el escalado basado en cargas de trabajo.

Evalúe los grupos lógicos y considere el efecto de combinar componentes, sistemas (SID) o infraestructuras. ¿Estas actividades incrementarían la complejidad operativa y disminuirían la fiabilidad?

- Documentación de AWS: [Architecture Guidance for Availability and Reliability of SAP on AWS](#)
- SAP Lens [fiabilidad]: [Principios de diseño de fiabilidad](#)
- AWS Well-Architected Framework [fiabilidad]: [Pilar de fiabilidad](#)

### Sugerencia 17.2.2: evalúe las excepciones para el uso de tenencias múltiples o el alojamiento de varias bases de datos en un solo host

En la mayoría de las bases de datos, ajuste el tamaño de cada sistema de forma independiente y aproveche el ajuste flexible del tamaño de las instancias para cumplir los requisitos de los sistemas.

En algunos casos, es conveniente desviarse de esa recomendación por cuestiones de costos. Por ejemplo:

- Cuando un componente basado en HANA requiere menos memoria que la instancia de EC2 más pequeña disponible, considere utilizar [contenedores de bases de datos de multiinquilinos de SAP HANA](#). Cuando el alojamiento se lleva a cabo con otros componentes, se posibilita el uso eficiente de los recursos de computación.
- Cuando se utilizan modelos de licencias de bases de datos basadas en núcleos para bases de datos relacionales, incluidas Oracle y SQL Server.
- Cuando se tienen aplicaciones que están estrechamente acopladas o pueden acoplarse de esa manera para cumplir con requisitos de tiempo de disponibilidad (uptime) y dependencias de versiones. Esto incluye herramientas de administración (por ejemplo, Solution Manager y SAP HANA Cockpit) y algunas opciones de SAP NetWeaver Gateway Deployment (Fiori y ECC).

Sugerencia 17.2.3: evalúe el uso del patrón de instalación de un solo host para los sistemas que no requieren resiliencia y escalabilidad

Para las aplicaciones o entornos individuales, debe considerar las ventajas de un modelo de alojamiento único. Esta acción puede ayudar a ahorrar costos del sistema operativo, de la duplicación de almacenamiento, de licencias de software y de servicios administrados. Entre algunas opciones de arquitectura frecuentes, especialmente para las infraestructuras que no son de producción, se encuentran las siguientes:

- Alojamiento simultáneo de bases de datos, aplicaciones y servicios centrales de SAP
- Base de datos separada (para minimizar la concesión de licencias de bases de datos). Consulte [optimización de costos] [Práctica recomendada 18.3: evalúe el efecto de la concesión de licencias y las opciones de optimización](#).
- Aplicación combinada y servicios centrales de SAP

Sugerencia 17.2.4: elija la región más rentable que satisfaga sus requisitos

Las principales razones para seleccionar una región de SAP son la proximidad, la residencia de los datos y la disponibilidad de los servicios. Para las implementaciones donde hay una opción, tenga presente que cada región de AWS ofrece precios basados en las condiciones del mercado local, por lo que los precios de servicio de AWS son distintos en cada región. Repase las diferencias de precios y su efecto potencial.

### Sugerencia 17.2.5: aplique arquitecturas que pueden escalarse en caso de error

Los mecanismos de recuperación y la elasticidad de la nube permiten un diseño en el que los recursos redundantes no deben estar activos y al 100 % de su capacidad. Si los requisitos de su negocio permiten un RTO o RPO más flexible, considere los siguientes puntos.

En el caso de las bases de datos, tenga en cuenta lo siguiente:

- Si sus RPO lo permiten, considere un nodo de base de datos secundario o de respaldo que no requiera una capacidad de computación equivalente para aplicar cambios con respecto al nodo principal. Teniendo en cuenta el efecto del tiempo de recuperación, contemple las ventajas en los costos de implementar una instancia más pequeña o compartida para su nodo secundario y escálelo verticalmente cuando se requiera. Si se utiliza una instancia más pequeña, se mantiene una relación 1:1 entre las instancias primarias y secundarias del sistema. Una arquitectura de instancias compartidas agrupa la base de datos secundaria con una base de datos del sistema no duplicada en una sola instancia. En caso de error, el sistema no duplicado debe detenerse antes de que pueda ocurrir una adquisición. De esta manera, aumenta el RTO.
- Si utiliza una instancia más pequeña para la base de datos de SAP HANA secundaria, desactive la carga previa de memoria para permitir una huella de memoria menor en el respaldo y reducir los costos. SAP calcula los requisitos de memoria en el documento de ayuda para [el uso del sistema secundario](#).
- Documentación de SUSE: [SAP HANA System Replication Scale-Up - Cost Optimized Scenario | SUSE \(Escalado vertical de la replicación de sistemas SAP HANA: ejemplo con optimización de costos | SUSE\)](#)
- Si su RTO y sus requisitos de resiliencia lo permiten, considere enfoques de creación de copias de seguridad de datos y registros que utilicen almacenamiento Multi-AZ (como Amazon FSx, Amazon EFS o Amazon S3). Estos enfoques permiten la protección geográfica de datos sin requerir recursos secundarios redundantes. En caso de error, se pueden crear recursos secundarios bajo demanda y restaurarlos rápidamente desde las copias de seguridad de ubicaciones transversales y almacenamiento de registros.
- Blog de SAP on AWS: [How to use snapshots to create an automated recovery procedure for SAP ASE databases \(Cómo utilizar instantáneas para crear un procedimiento de recuperación automatizado para las bases de datos de SAP ASE\)](#)

En el caso de la aplicación, tenga en cuenta lo siguiente:



- [La recuperación de instancias de AWS](#) consiste en el uso de una alarma de CloudWatch para supervisar una instancia de Amazon EC2. Recupera automáticamente la instancia si queda inhabilitada debido a un error de hardware preexistente. Evalúe si las situaciones de error cubiertas proporcionan protección suficiente.
- En las situaciones en las que el servidor de una aplicación debe recrearse rápidamente, entre algunas de las opciones, se encuentran las instancias de EC2 que se aprovisionan, pero no se ejecutan, las AMI con plantillas, la replicación de almacenamiento con servidores de pruebas frecuentes o la infraestructura como código.

Sugerencia 17.2.6: considere el costo de la capacidad de computación mínima durante un error

Distribuir los componentes de SAP en varias AZ puede reducir los costos incurridos para las reservas de capacidad en caso de error. Al distribuir componentes en varias AZ, se evita la necesidad de tener capacidad de exceso porque ya tiene parte de su carga de trabajo diseminada geográficamente. Esta medida minimiza el impacto en caso de un error de la AZ.

Por ejemplo, si el 100 % de capacidad es un requisito de disponibilidad para las situaciones de error incluida la pérdida de una AZ, en vez de aprovisionar el 200 % de capacidad en dos AZ, aprovisione el 150 % de capacidad en tres.

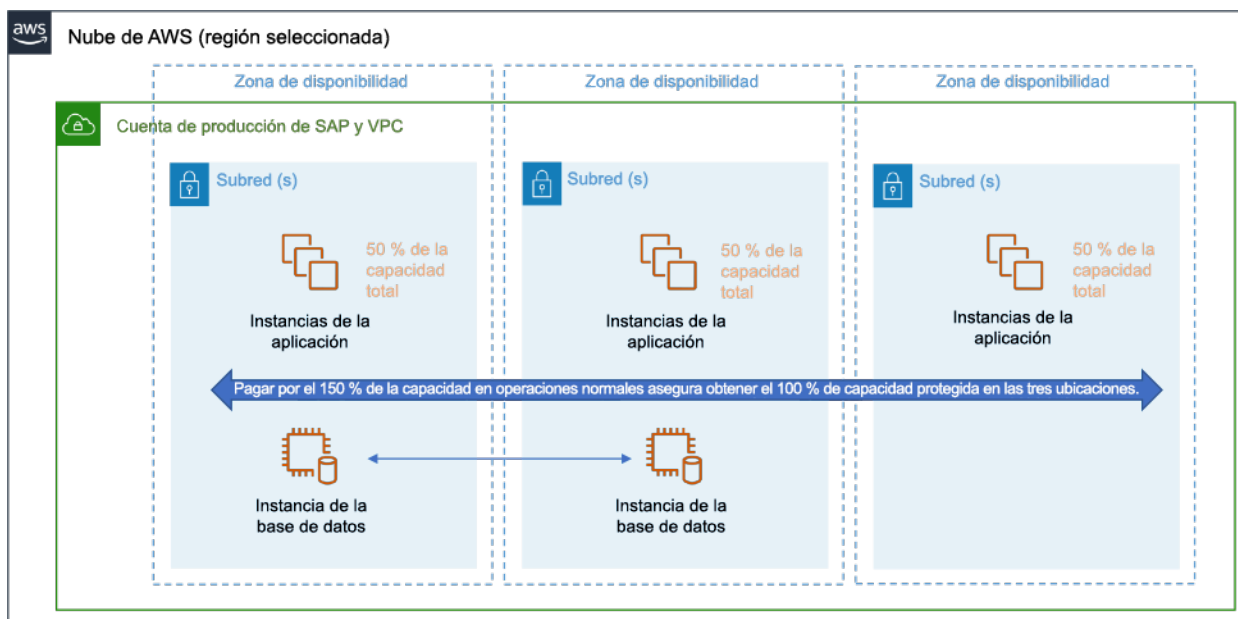


Figura: ejemplo de una arquitectura de tres AZ con el 150 % de capacidad en operaciones normales

Sugerencia 17.2.7: evalúe el uso de opciones de recuperación basadas solo en almacenamiento

En general en AWS, recomendamos la replicación de bases de datos en lugar de la replicación de almacenamiento para garantizar la protección del rango más amplio de situaciones de error. En el caso de la capa de la aplicación o de las instancias menos críticas, se puede reducir costos mediante una solución de DR que utilice replicación de almacenamiento sin computación. También minimiza la complejidad asociada con la administración de cambios.

- Documentación de AWS: [CloudEndure Disaster Recovery: Amazon Web Services](#)
- Documentación de SAP: [CloudEndure Disaster Recovery for SAP Applications \(CloudEndure Disaster Recovery para aplicaciones SAP\)](#)
- Documentación de AWS: [Replicación de las copias de seguridad automatizadas en otra región de AWS - Amazon Relational Database Service \(Amazon RDS\)](#)

Sugerencia 17.2.8: entender los costos relacionados con las redes

Los clientes de SAP suelen requerir una conexión segura entre la red en las instalaciones y Amazon VPC. Mediante el uso de una conexión de Direct Connect del tamaño adecuado o una conexión VPN o ambas, es posible cumplir los requisitos de rendimiento y fiabilidad a la par que se reducen costos.

Los costos de transferencia de datos varían según la región, la VPC y el diseño de la AZ. Evalúe de qué manera la distribución y la replicación de sus componentes de SAP se pueden optimizar sin comprometer la fiabilidad.

Por ejemplo, si dos sistemas que transfieren grandes cantidades de datos están en ubicaciones separadas, considere el efecto en los costos de transferencia de datos.

- Documentación de AWS: [Precios de las instancias bajo demanda de Amazon EC2 - Amazon Web Services](#)
- Documentación de AWS: [Architecture Patterns - General SAP Guides \(Modelos de arquitectura: guías generales de SAP\)](#)

Puede encontrar más guías en el pilar de costo del plan de revisión de Well-Architected Framework [para la transferencia de datos, en el pilar de optimización de costos](#).

**Práctica recomendada 17.3: comprenda los requisitos empresariales para tomar decisiones de diseño optimizadas en costos según el entorno**

Optimice los costos de cada sistema o entorno de manera individual según sus características distintivas. Considere la capacidad, el rendimiento, la fiabilidad y las horas de operación para cumplir

los requisitos de la empresa. En el caso de los entornos o aplicaciones que son menos críticos para la experiencia de los usuarios finales o procesos empresariales, minimice el almacenamiento, la computación y las horas de operación para reducir costos. Equilibre los ahorros de costos de una configuración reducida con los requisitos operativos para pruebas o soporte.

Sugerencia 17.3.1: evalúe si los entornos no productivos necesitan una copia completa de los datos de producción

Tener copias completas de los datos de producción en entornos distintos al de producción influirá considerablemente en los costos de almacenamiento y computación. Considere minimizar la cantidad de copias de datos de producción mientras continúa cumpliendo los requisitos de pruebas. Entre algunas de las opciones para minimizar los costos de almacenamiento de datos en entornos que no son de producción, se incluyen las siguientes:

- Utilice menos capacidad de almacenamiento para los sistemas de desarrollo y prueba.
- Utilice herramientas de segmentación de datos para escindir un subconjunto de datos de prueba más pequeño en sistemas no productivos.
- Considere utilizar copias de producción transitorias. Estas copias se pueden crear bajo demanda y sacar de servicio rápidamente o archivarse, una vez finalizada la necesidad comercial o prueba.
- Evalúe si la recomendación de SAP para las bases de datos de SAP HANA de retener el 50 % de memoria de trabajo es necesaria en sistemas que no son de producción.

Sugerencia 17.3.2: evalúe si los entornos que no son de producción siempre deben tener el mismo rendimiento que los de producción

Es probable que los sistemas que no son de producción y algunos sistemas de soporte tengan un conjunto menor de usuarios, gestionen volúmenes de transacciones menores o tengan requisitos de tiempo de respuesta flexibles. Considere lo siguiente:

- Reduzca el SAPS de su carga de trabajo mediante el uso de tipos de instancias de EC2 más pequeñas.
- Utilice menos servidores de aplicaciones.
- Utilice tipos de almacenamiento en Amazon EBS de menor costo; por ejemplo, gp3 en lugar de io2.
- Utilice características de rendimiento reducidas para los volúmenes de sistemas que no son de producción; por ejemplo, 3000 IOPS en vez de 10 000 IOPS.

- La elasticidad de la nube significa que puede escalar verticalmente los recursos de prueba que no son de producción que requieren un rendimiento similar al de producción, como pruebas de carga o de escalado.

Sugerencia 17.3.3: evalúe si los entornos que no son de producción necesitan las mismas horas de operación que los de producción

Los entornos que no son de producción, como los sistemas de prueba, formación y entornos aislados, pueden requerir menos horas de operación que los de producción. Considere las zonas horarias y las horas laborables de sus equipos de soporte para determinar si es necesario que todos los sistemas estén disponibles a toda hora, todos los días. Use esta información para seleccionar el modelo de precios más bajo.

Por ejemplo, ejecutar su sistema de formación de SAP 40 horas a la semana con un modelo de precios bajo demanda (~23 % de tiempo de disponibilidad [uptime]) será más barato que ejecutarlo siempre al 100 % con una instancia reservada de 3 años o Savings Plan.

Sugerencia 17.3.4: evalúe si los entornos que no son de producción necesitan constantemente la misma fiabilidad que los de producción

Elija la arquitectura más rentable para satisfacer los requisitos de fiabilidad individuales de cada sistema. Consulte [fiabilidad] [Práctica recomendada 10.1: convenga las metas de disponibilidad de la carga de trabajo de SAP que se alinean con sus requisitos comerciales](#) . Puede encontrar más guías en el [Pilar de fiabilidad](#) de AWS Well-Architected Framework.

Cuando se implementa una arquitectura similar a una de producción solo para fines de prueba, considere con qué frecuencia dicha arquitectura debe asemejarse a una de producción. Si se requiere una alta disponibilidad de la base de datos en un entorno que no es de producción para pruebas de fiabilidad o rendimiento, puede elegir desconectar o reducir verticalmente la instancia secundaria fuera de las ventanas de prueba para ahorrar costos.

Se pueden obtener beneficios de costos a través del uso de la automatización y de los precios bajo demanda para los entornos que no requieren un rendimiento similar al de un entorno de producción en todo momento.

Sugerencia 17.3.5: evalúe los requisitos de la empresa para los sistemas secundarios, incluidos los sistemas heredados y de apoyo

Si hay entornos que sirven solo para referencia o poseen un rol empresarial menos crítico, evalúe los requisitos de tiempo de disponibilidad (uptime), rendimiento y fiabilidad necesarios y compárelos con los de los sistemas de producción centrales.

Por ejemplo, es posible que deba mantenerse un sistema de ERP heredado para fines de referencia respecto a una conversión de la aplicación anterior o reestructura comercial. Para optimizar los costos de este sistema, se pueden ejecutar las instancias de EC2 solo cuando sea necesario, con lo que solo se paga por el almacenamiento en Amazon EBS. Una solución más rentable podría ser archivar el sistema mediante copias de seguridad en Amazon S3 y Amazon S3 Glacier.

### Práctica recomendada 17.4: revise el tamaño, la granularidad y las últimas instancias de EC2 disponibles para los componentes de SAP

Las instancias de EC2 más pequeñas proporcionan mayor flexibilidad de costos en las cargas de trabajo de SAP. Presentan opciones para el escalado horizontal que permiten deshabilitar la computación cuando no se utiliza o escalarla verticalmente solo durante los picos de carga. Adoptar un tamaño de instancia de EC2 coherente en el nivel de la aplicación lo ayudará a maximizar los beneficios de los compromisos con la instancia reservada y Savings Plans en todas las cargas de trabajo. Tenga en cuenta las instancias más recientes de AWS certificadas por SAP. También es aconsejable evaluar el impacto operativo, los costos de licencia, el soporte, el intercambio y la reutilización de cada componente.

Sugerencia 17.4.1: evalúe los beneficios de costos de varios servidores de aplicaciones más pequeños para proporcionar flexibilidad

En muchas cargas de trabajo de SAP, los servidores de aplicaciones se pueden diseñar para que sean inmutables. Tener una configuración estándar del servidor de la aplicación, que se escala en sentido horizontal replicando la unidad de base, brinda opciones para conseguir unidades repetibles uniformes. Las ventajas son la reutilización, la utilización de computación, las reservas y la automatización. En la evaluación, deben tenerse en cuenta los requisitos por unidad, como la concesión de licencias de sistemas operativos, la duplicación de almacenamiento y los costos administrativos.

Considere lo siguiente:

- Blog de SAP on AWS: [DevOps for SAP – Driving Innovation and Lowering Costs](#) .
- Blog de SAP on AWS: [Using AWS to allow SAP Application Auto Scaling \(Uso de AWS para permitir el escalado automático de aplicaciones SAP\)](#)

Sugerencia 17.4.2: evalúe los beneficios de costos de una configuración de escalado horizontal de SAP HANA si es compatible

Las cargas de trabajo de SAP OLAP se pueden implementar [tanto en configuraciones de escalado vertical como horizontal](#). SAP recomienda aplicar un escalado vertical en lugar de uno horizontal para reducir la complejidad operativa; sin embargo, las implementaciones de escalado horizontal pueden aplicarse a cargas de trabajo de SAP HANA analíticas o nativas más grandes, que requieren un poder de computación significativo (SAPS).

En ciertos casos, S/4HANA también es compatible con la configuración de escalado horizontal, pero con restricciones. Consulte la nota de SAP [2408419 SAP S/4HANA - Multi-Node Support \(SAP S/4HANA: compatibilidad multinodo\)](#) [Se necesita acceso al portal de SAP].

Para decantarse por el escalado vertical u horizontal, tenga en cuenta los siguientes aspectos:

- [Los tamaños de la instancia de EC2 certificada](#) que están disponibles para el escalado vertical u horizontal.
- El costo por GiB de memoria de una instancia de EC2 para cada familia de instancias. Las instancias de EC2 suelen tener un costo más alto por GiB que las instancias más pequeñas.
- La complejidad adicional y los costos operativos de administrar la distribución de datos en las implementaciones del escalado horizontal. Consulte la nota de SAP [2081591 FAQ: SAP HANA Table Distribution \(Preguntas frecuentes: distribución de tablas en SAP HANA\)](#) [Se necesita acceso al portal de SAP]

Práctica recomendada 17.5: considere utilizar la capacidad bajo demanda para mejorar la eficiencia de costos

El modelo de precios bajo demanda es adecuado para las cargas de trabajo de SAP que requieren menos horas de operación, proyectos de corto plazo, experimentación o capacidad ampliada durante períodos cortos (por ejemplo, en pruebas de rendimiento). Determine en qué parte puede utilizar los precios bajo demanda en su arquitectura de SAP.

Sugerencia 17.5.1: evalúe el uso de la modalidad bajo demanda para los sistemas SAP que requieren operar menos de 24 horas al día, los siete días de la semana

Con base en el punto de equilibrio entre el uso de un modelo de precios bajo demanda y de otro tipo, (Consulte [fiabilidad] [Práctica recomendada 18.1: conozca las opciones de pago y compromisos disponibles para Amazon EC2](#) ), evalúe si el modelo bajo demanda proporciona el costo más bajo. Como parte de esta evaluación, considere el compromiso general del Savings Plan.

Los casos de uso más comunes son los sistemas que no son de producción y que no se necesitan fuera de horarios comerciales extendidos o los experimentos comerciales de corto plazo, como actualizaciones de períodos de POC.

- Blog de SAP on AWS: [Automate Start or Stop of Distributed SAP HANA systems using AWS Systems Manager](#)

Sugerencia 17.5.2: evalúe las opciones de escalado programadas o dinámicas para los picos de carga

La capacidad bajo demanda generalmente se utiliza en cargas de trabajo de SAP durante los picos, cuando los requisitos de capacidad alcanzan un máximo por un tiempo breve. Considere lo siguiente:

- Utilice el escalado del servidor de la aplicación SAP en función de un cronograma para los picos conocidos de patrones de uso, como picos de fin de mes, de fin de año o estacionales.
- Utilice un escalado dinámico del nivel de la aplicación si la ocurrencia de los picos le es menos conocida y sea necesario escalar en función de la carga del usuario en tiempo real. Explore los mecanismos compatibles con SAP que proporcionan la administración y los controles requeridos.

Nota: Al evaluar el escalado dinámico del nivel de la aplicación, tenga en cuenta las repercusiones que traería a las conexiones de los usuarios y a los trabajos en lote si un servidor de la aplicación SAP se apagara en vista de que los componentes de SAP poseen estado. Las herramientas de AWS, SAP y las desarrolladas por socios de la APN pueden servir para cumplir este requisito.

- Documentación de AWS: [Referencia de acciones de Systems Manager Automation](#)
- Documentación de SAP: [SAP Landscape Management](#)
- Blog de SAP on AWS: [Using AWS to enable SAP Application Auto Scaling](#)

Práctica recomendada 17.6: evalúe los beneficios de costos y el efecto de los servicios y soluciones compartidos

Cuando varios sistemas SAP requieren la misma función, una opción rentable puede ser centralizar la administración y los costos utilizando las soluciones existentes, compartiendo los componentes o ambas alternativas. La supervisión, las copias de seguridad y la conectividad son funciones frecuentes que se pueden administrar dentro del límite de la cuenta de AWS o en una cuenta

exclusiva. La estandarización, la reducción de la duplicación y la reducción de la complejidad disminuyen los costos.

Busque maneras apropiadas de compartir recursos para reducir costos sin abandonar el aislamiento adecuado y sin presentar dependencias que podrían afectar las operaciones.

Sugerencia 17.6.1: evalúe el beneficio de costos de una configuración 1 a 1 frente a una de 1 a varios para cada servicio compartido

Un modelo estándar para las infraestructuras SAP consiste en aislar las cargas de trabajo que no son de producción y las de producción en cuentas separadas como parte de una estrategia de múltiples cuentas. Este puede ser un límite lógico para algunos servicios. Considere la complejidad y los costos operativos en cada situación, incluidos los límites de administración que refuerzan la segmentación y el impacto del costo de transferencia de datos entre las regiones, AZ, VPC o cuentas.

En un diseño de múltiples cuentas, algunos servicios de AWS se pueden alojar de manera centralizada y es posible acceder a ellos mediante varias aplicaciones y cuentas siguiendo un diseño de “ejes y radios” a fin de ahorrar costos. Estos son algunos de los servicios:

- VPC exclusiva con puerta de enlace NAT para todo el tráfico saliente de las VPC radiales
- Modelo centralizado para los equilibradores de red y los dispensadores web
- Amazon EFS o Amazon FSx compartidos para los transportes y otras necesidades de intercambio de archivos

Sugerencia 17.6.2: evalúe las situaciones en las que la reutilización de los servicios existentes puede reducir los costos

Esta sugerencia se aplica a una serie de niveles:

- Cuando AWS presta servicios, a menudo se minimizan los costos generales y se trabaja con precios basados en el consumo. Algunos ejemplos son Amazon EFS, AWS Backup for SAP HANA y AWS Backup.
- Su negocio debe contar con un estándar aplicable a toda la empresa para algunas funciones (por ejemplo, copia de seguridad de la empresa), que debe utilizarse para la uniformidad operativa y la economía de la escala.



- Las soluciones de socios de la APN pueden estar disponibles en AWS Marketplace o se pueden incorporar con un modelo Bring Your Own License (BYOL, traer licencia propia) según las demandas específicas de su negocio.
- Las imágenes de máquinas de AWS Marketplace incluidas en la licencia pueden ayudar a reducir los costos iniciales. En esta situación, deben considerarse las restricciones de licencias porque podrían afectar la flexibilidad de la solución al restringir la portabilidad en distintos tipos de instancias.

Sugerencia 17.6.3: conozca los efectos de usar enfoques de creación, de compra o de código abierto

Más allá de si la solución es de AWS o de un socio de la APN, existen diferentes grados en lo que respecta a la creación propia, el código abierto y los productos adquiridos y listos para usarse. Algunos ejemplos son soluciones de copia de seguridad, soluciones de alta disponibilidad y soluciones de almacenamiento compartido.

Para decidirse por un enfoque de creación propia o el uso de una solución de código abierto, considere los siguientes elementos:

- Acuerdos de nivel de servicio
- Habilidades requeridas para crear y mantener el producto
- Efecto comercial de un corte del servicio

Además, debe evaluar los modelos comerciales disponibles para las soluciones que desea comprar en función de los requisitos específicos de su negocio y la funcionalidad que provee cada solución. Considere los términos de los modelos comerciales; por ejemplo, los cargos por derecho de uso frente a los cargos de pago por uso y cómo se calculan dichos cargos.

## Práctica recomendada 17.7: evalúe los beneficios de costos de la automatización

Un beneficio posible de adoptar la automatización en AWS es la mejora de la eficiencia y la productividad, que puede traducirse en menores costos para su organización.

Sugerencia 17.7.1: evalúe las eficiencias de la automatización de las compilaciones

Automatizar el proceso de compilación mediante el uso de la infraestructura como código conlleva eficiencias de costos que pueden mejorar su tiempo de comercialización y productividad. Las ventajas en cuanto a la calidad, uniformidad, repetibilidad y capacidad de recuperación que aportan

las prácticas recomendadas de DevOps deben ser analizadas en contexto, ya que suponen una inversión inicial alta en el desarrollo de procesos de automatización.

Trabajar con los servicios profesionales de AWS o un socio de AWS para aprovechar su experiencia puede reducir el esfuerzo general.

AWS Launch Wizard para SAP permite acelerar las implementaciones de SAP con la automatización. Es un servicio que lo guía en los procesos de ajuste de tamaño, configuración e implementación de las aplicaciones SAP HANA en AWS de conformidad con las prácticas recomendadas de SAP. El servicio está disponible sin ningún costo adicional, con el soporte de AWS.

- Documentación de AWS: [Infraestructura como código](#)
- Documentación de AWS: [AWS CloudFormation](#)
- Blog de SAP on AWS: [AWS for SAP DevOps \(AWS para SAP DevOps\)](#)

Sugerencia 17.7.2: evalúe las eficiencias de la automatización para las operaciones

A fin de reducir el costo y el esfuerzo manual de las tareas repetitivas, investigue cómo se pueden utilizar las herramientas de AWS y de terceros para automatizar la ejecución y la supervisión de las operaciones. Considere lo siguiente:

- Servicio de AWS: [AWS Systems Manager](#)

Puede encontrar más guías en [excelencia operativa] [Práctica recomendada 3.6: utilice la automatización para realizar operaciones de la infraestructura SAP](#) .

## 18. Evalúe los recursos de computación de SAP para la eficiencia de costos

¿Cómo se evalúan las opciones de computación y almacenamiento para las cargas de trabajo de SAP? Cuando implementa o migra SAP a AWS, debe seleccionar instancias de EC2 rentables y soluciones de almacenamiento para la carga de trabajo de SAP a fin de cumplir sus metas de costos.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica	Obligatorio	Conozca las opciones de pago y compromisos disponibles para Amazon EC2

ID	Prioridad	Práctica recomendada
recomendada 18.1		
<input type="checkbox"/> Práctica recomendada 18.2	Obligatorio	Considere el costo como un elemento clave para elegir la instancia de EC2
<input type="checkbox"/> Práctica recomendada 18.3	Altamente recomendado	Evalúe el efecto de la concesión de licencias y las opciones de optimización
<input type="checkbox"/> Práctica recomendada 18.4	Altamente recomendado	Evalúe el efecto del costo de las opciones de almacenamiento en función de las características requeridas

## Práctica recomendada 18.1: conozca las opciones de pago y compromisos disponibles para Amazon EC2

Considere el uso de instancias reservadas y Savings Plans para proporcionar un descuento significativo en comparación con los precios bajo demanda. Están disponibles con términos de compromiso de 1 y 3 años y con tres opciones de pago: pago total por adelantado, pago por adelantado parcial y sin pago por adelantado.

Sugerencia 18.1.1: conozca los puntos de equilibrio entre los modelos de precios

[Las Instancias reservadas](#) se clasifican en instancias reservadas estándar (hasta un 72 % de descuento en las tarifas bajo demanda) e instancias reservadas convertibles (hasta un 54 % de descuento en las tarifas bajo demanda). [Los Savings Plans](#) se clasifican en Compute Savings Plans (hasta un 66 % de descuento en las tarifas bajo demanda) y EC2 Instance Savings Plans (hasta un 72 % de descuento en las tarifas bajo demanda).

El descuento sobre la tarifa por hora bajo demanda de Amazon EC2 que puede obtener depende de los siguientes factores:

- El término del compromiso seleccionado
- La opción de pago seleccionada
- El tipo de instancia reservada o Savings Plan seleccionado
- La familia de instancias

Las familias de instancias con memoria optimizada, como X1 y X1e , ofrecen mayores ahorros para el compromiso; por esa razón, es importante comprender las opciones de precios para SAP, especialmente para las cargas de trabajo de SAP HANA.

Utilice la opción avanzada dentro de la calculadora de precios de AWS para determinar el punto de equilibrio. Es importante que conozca las suposiciones que utiliza esta calculadora. Por ejemplo: imagine que utilizamos la siguiente fórmula para determinar el punto que ofrece un TCO más bajo utilizando una instancia reservada o Savings Plan en lugar del modelo bajo demanda para cada familia de instancias.

$(\text{Tarifa efectiva por hora de compromiso} / \text{tarifa por hora bajo demanda}) * 730 \text{ horas}$

Consulte la tarifa efectiva por hora para cada [término y tipo de compromiso de una instancia reservada](#) y para cada [período y tipo de compromiso de Savings Plan](#) . Compare y contraste los siguientes ejemplos que muestran distintos puntos de equilibrio:

Ejemplo 1: en Virginia del Norte (us-east-1), en el caso de la familia M5, el punto de equilibrio donde una instancia reservada estándar o EC2 Savings Plan de 3 años sin pago por adelantado ofrecería un TCO más bajo es 315 horas por mes (~16 horas por día, de lunes a viernes).

Ejemplo 2: en Virginia del Norte (us-east-1), en el caso de la familia de instancias X1, el punto de equilibrio donde una instancia reservada estándar o EC2 Savings Plan de 3 años sin pago por adelantado ofrecería un TCO más bajo es 235 horas por mes (~12 horas por día, de lunes a viernes).

Utilice las guías integrales sobre [la administración de costos](#) y el pilar de optimización de costos de Well-Architected Framework [Pilar de optimización de costos](#) . La siguiente guía de precios de [SAP on AWS](#) también ofrece una guía específica para las cargas de trabajo de SAP que se ejecutan en AWS. Cuando se analizan los costos, tenga presente que todos los precios de AWS (salvo en las regiones de AWS de China) están expresados en dólares estadounidenses (USD). No obstante, se puede seleccionar otra moneda para el pago: [monedas que actualmente se aceptan en AWS](#) .

- Documentación de AWS: [Savings Plans - Compute Savings Plans and Reserved Instances \(Savings Plans: Compute Savings Plans e instancias reservadas\)](#)

- Documentación de AWS: [Savings Plans - Plan Types \(Savings Plans: tipos de planes\)](#)
- Documentación de AWS: [Tipos de Instancias reservadas](#)

Sugerencia 18.1.2: conozca las consideraciones de cada modelo de precios pertinentes para SAP

Además del descuento en la tarifa por hora, hay otros beneficios de las instancias reservadas y Savings Plans que debe considerar. La documentación de AWS [Comparing Savings Plans to RIs table \(Tabla de comparación de Savings Plans con instancias reservadas\)](#) ofrece una comparación entre las instancias reservadas y los Savings Plans.

[Las instancias reservadas zonales](#) se pueden utilizar para proporcionar reservas de capacidad dentro de una AZ específica. Los Savings Plans no ofrecen una reserva de capacidad, pero puede combinarlos con [reservas de capacidad bajo demanda](#) para obtener las mismas características de una instancia reservada zonal. Consulte [fiabilidad] [Práctica recomendada 10.2: seleccione una arquitectura adecuada para sus requisitos de disponibilidad y capacidad](#) para obtener más información sobre las estrategias de capacidad.

[Las instancias de spot de Amazon EC2](#) le permiten aprovechar la capacidad de EC2 ociosa en la nube de AWS. Las instancias de spot están disponibles hasta con un 90 % de descuento en comparación con los precios de las instancias bajo demanda. AWS puede reclamar las instancias de spot con dos minutos de aviso cuando AWS requiere la capacidad. Por tanto, en general las instancias de spot no son adecuadas para ejecutar cargas de trabajo de SAP.

Cuando se utilizan instancias [bajo demanda](#), debe considerar el efecto operativo adicional de detener e iniciar los sistemas SAP y las instancias de EC2 preexistentes en función de las horas de operación requerida y el efecto del rendimiento de la aplicación cada vez que el sistema se inicia.

Sugerencia 18.1.3: evalúe la estrategia de su empresa para la facturación unificada y el intercambio de compromisos de las instancias reservadas y Savings Plans

Con [Facturación unificada](#), las instancias reservadas y los Savings Plans se aplican al uso en todas las cuentas dentro de una organización de AWS. En la cuenta de administración de una organización, se puede desactivar el intercambio de descuentos de instancias reservadas y Savings Plans para cualquier cuenta en esa organización, incluida la cuenta de administración. Esto significa que los descuentos de instancias reservadas y Savings Plans no se comparten entre las cuentas que tienen el intercambio desactivado. Para compartir un descuento de instancias reservadas o Savings Plans con una cuenta, ambas cuentas deben tener habilitada la función de intercambio. Esta preferencia no es permanente y se puede cambiar en cualquier momento.

- Documentación de AWS: [Facturación unificada de AWS Organizations](#)
- Documentación de AWS: [Desactivar descuentos compartidos de instancias reservadas y de Savings Plans](#)

Un factor clave para determinar su estrategia de intercambio de compromisos es la estrategia de cuentas [de AWS general](#) que haya adoptado su organización. También debe considerar si las cargas de trabajo de SAP se ejecutan en sus propias cuentas de AWS exclusivas o junto con otras cargas de trabajo alojadas en AWS. Para entender cómo se aplican los descuentos a las instancias reservadas y los Savings Plans en la facturación unificada de su organización, consulte las siguientes referencias:

- Documentación de AWS: [Facturas consolidadas](#)

Como se detalla en la nota de SAP [1656250 - SAP on AWS: Support prerequisites](#) [se necesita acceso al portal de SAP], SAP on AWS solo es compatible si existe [un acuerdo de soporte de AWS basado en tarifas](#) (como Business Support o Enterprise Support). Determine el plan de soporte adecuado según los costos y requisitos.

- Documentación de AWS: [Compare los planes de AWS Support](#)

Cabe destacar que AWS calcula las tarifas de soporte de forma independiente para cada cuenta de un miembro de una organización.

**Práctica recomendada 18.2:** utilice el costo como una consideración clave para elegir la instancia de EC2

Si selecciona instancias de EC2 certificadas por SAP que sean apropiadas para su carga de trabajo, puede optimizar los costos. Realice un análisis exhaustivo de cada sistema a fin de garantizar que las decisiones estén, en la medida de lo posible, controladas por datos. Puede encontrar más guías generales en el pilar de optimización de costos de Well-Architected Framework, [en la sección Recursos rentables.](#)

**Sugerencia 18.2.1:** seleccione las instancias de última generación disponibles dentro de su región

Las instancias de Amazon EC2 de última generación suelen ofrecer los costos más bajos y un mejor rendimiento y deben utilizarse si están disponibles y certificadas para la implementación.

- Documentación de AWS: [Amazon EC2 Instance Types for SAP](#)

- Documentación de AWS: [Instance type availability by Region \(Disponibilidad del tipo de instancia por región\)](#)

#### Note

Es posible que algunas familias de instancias de Amazon EC2 (por ejemplo, X1 e instancias de alta memoria) no estén disponibles en todas las AZ dentro de una región. Durante la planificación, confirme que los tipos de instancias que requiere para su carga de trabajo de SAP están disponibles en sus AZ objetivo.

### Sugerencia 18.2.2: equilibre el costo con los requisitos de rendimiento

Cada familia de instancias de Amazon EC2 compatible con SAP provee un rendimiento específico que se mide en [SAPS](#). Debe evaluar cada familia de instancias en función de sus requisitos de rendimiento. Le recomendamos que comprenda los coeficientes de costo por SAPS y de costo por GiB.

Computación optimizada (C*)	De uso general (M*)	Memoria optimizada (R*)
1 vCPU: 2 GiB	1 vCPU: 4 GiB	1 vCPU: 8 GiB

Si un componente de la carga de trabajo requiere más memoria que [SAPS](#) (CPU), debe seleccionar la familia de instancias que proporcione el menor costo por GiB de memoria. Si el componente requiere más SAPS (CPU) que memoria, debe seleccionar la familia de instancias que proporcione el menor costo por SAPS.

Las familias de instancias certificadas por SAP que funcionan con un procesador de AMD suelen suponer un 10 % de ahorro en costos en comparación con las instancias de EC2 equivalentes que funcionan con procesadores de Intel. Por ejemplo, los tipos de instancia de EC2 C5a son un 10 % menor que los de la familia C5 y poseen los mismos KPI de rendimiento.

Para las cargas de trabajo de SAP HANA que no son de producción, considere utilizar una de las familias de instancias que reúne los requisitos detallados en la Nota de SAP [2271345 Cost-Optimized SAP HANA Hardware for Non-Production Usage \(Hardware de SAP HANA con optimización de costos para usos en entornos que no son de producción\)](#) [Se necesita acceso al portal de SAP].

Sugerencia 18.2.3: revise la predictibilidad de su perfil de crecimiento y los requisitos de la capacidad máxima

Es probable que una infraestructura SAP existente en AWS o una migración homogénea tengan un crecimiento y modelos de uso más predecibles que una implementación totalmente nueva o una migración heterogénea.

En los sistemas que carecen de datos sobre el crecimiento histórico, debe considerar los beneficios de costos de seleccionar una instancia de EC2 cuyo tamaño pueda permitir un crecimiento de corto o mediano plazo. Planifique escalar el tamaño de la instancia a medida que sus requisitos cambian. Debe garantizar que su diseño de arquitectura proporcione la flexibilidad para alternar entre distintas familias de instancias de EC2 a medida que su consumo de recursos cambie.

De manera similar, debe evaluar si se tuvieron en cuenta los cambios en la capacidad máxima.

Para ajustar el tamaño de un entorno de SAP HANA, considere no solo el tamaño de la base de datos, sino también el requisito de la memoria de trabajo. Consulte los informes y herramientas de ajuste de tamaño de SAP HANA para calcular el tamaño y el uso.

Sugerencia 18.2.4: considere la flexibilidad del compromiso de la instancia

Cuando un componente (por ejemplo, base de datos de SAP HANA) debe escalarse verticalmente durante el período de compromiso, evalúe si esto implicará optar por una familia de instancias distinta. Esta situación afectará la selección de su modelo de precios.

- Documentación de AWS: [Tipos de instancias de Amazon EC2](#)

Práctica recomendada 18.3: evalúe el efecto de la concesión de licencias y las opciones de optimización

Cuando traslada cargas de trabajo de SAP a AWS, puede haber consecuencias a nivel empresarial con las licencias de software que requieren sus cargas de trabajo de SAP. Debe entender estas consecuencias y las opciones a su disposición.

Sugerencia 18.3.1: entienda cómo influye la CPU y la memoria en la licencia de software

Evalúe los distintos coeficientes de vCPU y memoria disponibles con los [tipos de instancias de Amazon EC2](#) disponibles para SAP a fin de optimizar los costos de las licencias.

- Documentación de SAP: [SAP Components licensed by vCPU or Memory \(Componentes de SAP con licencia para vCPU o memoria\)](#)



- Documentación de SAP: [SAP HANA Allocated Memory Pools and Allocation Limits \(Grupos de memoria asignados a SAP HANA y límites de asignación\)](#)

Para los entornos basados en Oracle, revise el siguiente recurso:

- [Consideraciones de la licencia de Oracle, concesión de licencias de Oracle Software en el entorno de computación en la nube](#)
- Requisitos de Oracle Premium Support detallados en la Nota de SAP: [2069760 Oracle Linux 7.x SAP Installation and Upgrade \(Instalación y actualización de Oracle Linux 7.x SAP\)](#) [Se necesita acceso al portal de SAP]

Para los entornos de Microsoft Windows y SQL Server, revise lo siguiente:

- Documentación de AWS: [Licencias de Microsoft en AWS](#)
- Notas de SAP: [2139358 Effect of changes in licensing terms of SQL Server \(Efectos de los cambios en los términos de licencia de SQL Server\)](#) [Se necesita acceso al portal de SAP]

Para los entornos de IBM Db2, revise lo siguiente:

- [Eligible Public Cloud BYOSL Policy \(Política BYOSL para nubes públicas elegibles\)](#)
- Documentación de AWS: [Track IBM license usage with AWS License Manager \(Seguimiento del uso de licencias de IBM con AWS License Manager\)](#)

Entienda el efecto de productos de ISV y terceros con licencia para CPU o memoria:

- Considere utilizar la característica [Optimizar CPU](#) a fin de optimizar los costos de licencia.
- Considere utilizar [AWS License Manager](#) para gestionar las licencias de software y los costos asociados.
- Documentación de AWS: [Núcleos físicos por tipo de instancia de Amazon EC2](#)

Sugerencia 18.3.2: entienda las opciones de compra de sistemas operativos

Para cada uno de los sistemas operativos compatibles con SAP, hay un conjunto de opciones de compra disponibles.

### 1. Licencia provista por Amazon EC2

2. Licencia provista por AWS Marketplace
3. Modelo Bring-Your-Own-Licenses (BYOL)

No todas las opciones están disponibles para cada sistema operativo. Debe evaluar sus requisitos y acuerdos de licencia para determinar qué opción es la más rentable. Puede incluir los costos de los siguientes sistemas operativos como parte del costo de Amazon EC2:

- Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server

Puede comprar los siguientes sistemas operativos a través de AWS Marketplace:

- Red Hat Enterprise Linux for SAP (con base en el costo de EC2 básico de Red Hat Enterprise Linux)
- SUSE Linux Enterprise Server for SAP (con base en el costo de EC2 básico de Amazon Linux)

Puede utilizar un modelo Bring-Your-Own-Licenses (BYOL) para los siguientes sistemas operativos:

- Windows Server
- Red Hat Enterprise Linux<sup>1</sup>
- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux for SAP<sup>2</sup>
- SUSE Linux Enterprise Server for SAP<sup>2</sup>
- Oracle Enterprise Linux (los requisitos de Oracle Premium Support están detallados en la Nota de SAP [2069760 - Oracle Linux 7.x SAP Installation and Upgrade](#) ) [Se necesita acceso al portal de SAP]

<sup>1</sup> Considere consultar la nota de SAP [2871484 SAP supported variants of Red Hat Enterprise Linux \(Variantes de Red Hat Enterprise Linux compatibles con SAP\)](#) [Se necesita acceso al portal de SAP], dado que SAP ya no es compatible con Red Hat Enterprise Linux estándar para ninguna de las cargas de trabajo de SAP como RHEL 8.

<sup>2</sup> Estos productos tienen un soporte de plazo más largo, que puede reducir sus costos operativos para las actualizaciones. Consulte la documentación de SUSE [SUSE Enterprise Support Policy](#)

([Política de SUSE Enterprise Support](#)) y la documentación de Red Hat [Red Hat Enterprise Support Policy \(Política de Red Hat Enterprise Support\)](#) para obtener más detalles.

Sugerencia 18.3.3: considere el uso de hosts dedicados de Amazon EC2 para mitigar las restricciones de concesión de licencias

Amazon EC2 ofrece hosts individuales que le permiten acceder a hardware exclusivamente destinado para usted. Puede utilizar [su propio software con licencia](#) en una infraestructura exclusiva. Los hosts dedicados de Amazon EC2 se integran con [AWS License Manager](#), un servicio que lo ayuda a administrar sus licencias de software, incluidas las licencias de Windows Server y SQL Server.

Sugerencia 18.3.4: evalúe los beneficios de costos de abandonar el modelo de licencias por gigabyte o por núcleo

Como parte de su migración a la nube, considere utilizar el modelo de licencias de bases de datos de tiempo de ejecución de SAP.

SAP permite a los clientes obtener licencias de bases de datos SAP HANA, SAP ASE y de terceros conforme a su modelo de licencias de bases de datos de tiempo de ejecución. Las bases de datos de tiempo de ejecución con licencia de SAP sirven solo para dar soporte de software y a los usuarios con nomenclatura de SAP que recibieron licencias de SAP. Las licencias de bases de datos de tiempo de ejecución de SAP se otorgan como un porcentaje de la tarifa del software de SAP, normalmente conocida como SAP Application Value (SAV, Valor de la aplicación SAP).

Las licencias de tiempo de ejecución no se basan en la cantidad de gigabytes de memoria o núcleos de CPU y, por tanto, pueden proveer un beneficio de costo superior a los modelos de licencias por gigabyte o por núcleo, especialmente en casos de varios sistemas que no son de producción, dado que la licencia de base de datos de tiempo de ejecución de SAP aplica a todos los entornos cubiertos en su acuerdo de licencia de SAP.

Si ya tiene derecho a usar la licencia de tiempo de ejecución para bases de datos de SAP HANA dentro de su acuerdo de licencias de SAP, debe determinar si también tiene derecho a usar la licencia de tiempo de ejecución destinada a bases de datos de SAP ASE para los componentes de SAP que no pueden utilizar SAP HANA como la base de datos preexistente o para reducir los costos de infraestructura asociados con el uso de SAP HANA para ese componente.

- Consulte la documentación de SAP [SAP Licensing Guide \(Guía de licencias de SAP\)](#). También puede comunicarse con su equipo de cuentas de SAP.

## Práctica recomendada 18.4: evalúe el efecto del costo de las opciones de almacenamiento en función de las características requeridas

Seleccione servicios de almacenamiento de objetos, de archivos y de bloques para alojar, archivar y proteger su sistema SAP. Diseñe su almacenamiento para reducir el costo y aumentar la agilidad.

Sugerencia 18.4.1: evalúe la manera más rentable de diseñar en función de los requisitos de E/S y rendimiento de su carga de trabajo

Para la mayoría de los requisitos de SAP, se recomiendan solid state disks (SSD, discos de estado sólido) para los volúmenes de EBS. Para garantizar una selección rentable, recomendamos comenzar con el volumen de Amazon EBS de uso general, que es adecuado para la mayoría de las cargas de trabajo de SAP. Con el tiempo, revise el uso utilizando métricas de CloudWatch y la supervisión de aplicaciones y bases de datos. Si necesita un nivel de E/S o de rendimiento más altos, lo puede lograr con los volúmenes de Amazon EBS de IOPS aprovisionadas.

- Documentación de AWS: [Tipos de volúmenes de Amazon EBS](#)

Para equilibrar las consideraciones de costo y rendimiento, la configuración de almacenamiento utilizada para los datos y volúmenes de registro de SAP HANA debe cumplir los KPI de almacenamiento de SAP. Los modelos de almacenamiento descritos en el siguiente documento se probaron conforme a las pautas de SAP TDI: [SAP HANA Tailored Data Center Integration \(Integración de centros de datos personalizados para SAP HANA\)](#)

- Documentación de AWS: [Storage Configuration for SAP HANA \(Configuración de almacenamiento para SAP HANA\)](#)

Sugerencia 18.4.2: planifique cambios dinámicos del tamaño y configuración del almacenamiento

A fin de optimizar los costos de almacenamiento, ajuste el tamaño correcto de este según el uso de datos o los requisitos de IOPS.

Amplíe el tamaño de volumen de manera dinámica según corresponda. Evalúe la opción de cambiar los tipos de volumen durante las actividades que requieren un aumento de rendimiento como las actualizaciones de la aplicación.

- Documentación de AWS: [Solicitar modificaciones de los volúmenes de EBS](#)

Garantice que todos los volúmenes huérfanos o sin utilizar se revisan de manera regular para garantizar el control de costos.

- Documentación de AWS: [List Amazon EBS volume or snapshot information \(Cómo enumerar información de volúmenes o instantáneas de Amazon EBS\)](#)

Sugerencia 18.4.3: evalúe los beneficios de costos para el almacenamiento de objetos

Los datos centrales para un sistema SAP están contenidos dentro de la base de datos y residen en Amazon EBS. Amazon S3 puede proveer almacenamiento de objetos de bajo costo para datos auxiliares, como copias de seguridad o archivos y objetos grandes como imágenes o documentos. El costo se puede optimizar más si se selecciona el tipo [de almacenamiento adecuado](#) para sus necesidades de retención y durabilidad.

Sugerencia 18.4.4: evalúe los beneficios de costos para los sistemas de archivos compartidos

Amazon Elastic File System (Amazon EFS) proporciona un sistema de archivos elástico, sin servidor y que no requiere supervisión que le permite compartir datos de archivos sin aprovisionar ni administrar almacenamiento. El costo se puede optimizar más si selecciona la clase de almacenamiento adecuado según su requisito de rendimiento y disponibilidad.

Amazon FSx proporciona una solución completamente administrada de almacenamiento de archivos de alta disponibilidad y duradera diseñada en Windows Server. La duplicación de datos permite optimizar todavía más los costos a través de la eliminación de datos redundantes.

Algunos casos de uso comunes de SAP para Amazon EFS o Amazon FSx son sapmnt, transportes, archivos de interfaz, copias de seguridad de almacenamiento y software. Usar Amazon EFS o Amazon FSx puede proporcionar más beneficios de costos que implementar su propia solución NFS de alta disponibilidad.

- Documentación de AWS: [Amazon EFS](#)
- Documentación de AWS: [Amazon FSx](#)

## 19. Optimice el uso de datos de SAP para la eficiencia de costos de almacenamiento

¿Cómo se optimiza el uso de datos de SAP para minimizar los costos de almacenamiento y de memoria? Diseñe el almacenamiento de su base de datos, las copias de seguridad y los sistemas de

archivos de respaldo teniendo en cuenta el costo, y evalúe periódicamente la ubicación, la retención y las estrategias de mantenimiento.

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 19.1	Obligatorio	Conozca los requisitos de acceso y retención
<input type="checkbox"/> Práctica recomendada 19.2	Altamente recomendado	Borre los datos innecesarios a través de la limpieza regular
<input type="checkbox"/> Práctica recomendada 19.3	Recomendado	Implemente estrategias de compresión, reorganización y reclamo
<input type="checkbox"/> Práctica recomendada 19.4	Altamente recomendado	Revise las estrategias de copias de seguridad para implementar mejoras
<input type="checkbox"/> Práctica recomendada 19.5	Recomendado	Considere opciones de categorización para datos en tiempo real
<input type="checkbox"/> Práctica recomendada 19.6	Recomendado	Evalúe las opciones de archivado y descarga

## Práctica recomendada 19.1: conozca los requisitos de acceso y retención

Conozca las maneras de acceder a datos y retenerlos. Considere los datos activos, los sistemas de administración de documentos y las copias de seguridad.

Sugerencia 19.1.1: categorice los distintos tipos de datos comerciales en el sistema SAP

A partir de la categorización de distintos tipos de datos y la frecuencia con la que se accede a estos (temperatura de datos) desde una perspectiva comercial, es posible identificar oportunidades para archivar o descargar datos de su sistema SAP para optimizar costos.

Los siguientes son algunos de los tipos de datos frecuentes que se encuentran en un sistema SAP:

- Referencia: datos con valores que cambian poco; por ejemplo, ciudades, países y tipos de cambio
- Datos maestros de SAP: datos con valores que no cambian casi nunca; por ejemplo, datos maestros del cliente de SAP o productos
- Auditoría: datos que se guardan por motivos de auditoría; por ejemplo, registros de cambio
- Transacción: datos creados como parte de las operaciones comerciales diarias; por ejemplo, órdenes de ventas
- Analíticos: datos creados para apoyar el análisis y la toma de decisiones; por ejemplo, presentación de informes de ventas mensuales

Clasifique la temperatura de los datos de la siguiente manera:

- Calientes: datos con acceso frecuente
- Cálidos: datos sin acceso frecuente
- Fríos: datos solo con acceso esporádico

Clasifique los requisitos de retención de la siguiente manera:

- Retención para fines de DR
- Retención para fines de referencia
- Retención para fines de conformidad o auditoría

## Práctica recomendada 19.2: borre los datos innecesarios a través de la limpieza regular

Para reducir su huella de datos y ahorrar costos, minimice el tamaño de la base de datos y el uso de otros sistemas de archivos a través de actividades regulares de limpieza y reorganización.

Sugerencia 19.2.1: revise el ajuste de tamaño y realice una limpieza regular en las tablas técnicas de SAP

SAP proporciona una guía integral sobre la administración de datos de tablas técnicas. Mediante la identificación y el tratamiento del incremento de estas tablas, se pueden reducir los costos de almacenamiento y computación. Esta acción es especialmente pertinente para las instancias de SAP HANA debido a la relación directa entre el tamaño de la base de datos y los requisitos de memoria.

- Notas de SAP: [2388483 How-To: Data Management for Technical Tables \(Cómo administrar datos para las tablas técnicas\)](#) [Se necesita acceso al portal de SAP]

Utilice las declaraciones de SQL “de la tabla más grande” para obtener tamaños de tablas comparativos, en particular, de aquellas que han sido marcadas como tablas de base. Un ejemplo frecuente en los clientes de SAP establecidos es la gran cantidad de elementos de flujo de trabajo de SAP completados que se pueden borrar o archivar. La limpieza previa a una migración también puede mejorar los plazos y el rendimiento. Si utiliza SAP HANA, el informe ‘/SDF/HDB\_SIZING’ puede proporcionar detalles de limpieza y requisitos de disco anticipados.

Sugerencia 19.2.2: controle el incremento del sistema de archivo a través de la limpieza automática o regular de registros, trazos, archivos de interfaz y copias de seguridad

Como los costos de almacenamiento están impulsados por el uso, hay oportunidades para optimizar el uso inicial, además del efecto multiplicador de las copias y copias de seguridad de los archivos que ya no se usan para el análisis de errores.

- Notas de SAP: [2399996 How-To: Configuring automatic SAP HANA Cleanup with SAP HANACleaner \(Cómo configurar la limpieza automática de SAP HANA con SAP HANACleaner\)](#) [Se necesita acceso al portal de SAP]



## Práctica recomendada 19.3: implemente estrategias de compresión, reorganización y reclamo

Todas las bases de datos compatibles con SAP proporcionan mecanismos para reclamar espacio. Estos mecanismos deben ser parte de las actividades de mantenimiento regulares para minimizar los aumentos de costos asociados con la extensión de memorias o volúmenes de EBS.

Sugerencia 19.3.1: utilice la compresión de base de datos

La compresión es una característica predeterminada en SAP HANA. Utilizar la compresión en otras bases de datos puede requerir licencias adicionales, pero es necesario explorar los beneficios en costos y rendimiento. Las siguientes notas proveen un punto de inicio para las distintas bases de datos, pero consulte la documentación de SAP y bases de datos para obtener información adicional.

Base de datos	Documentación de SAP o Notas de SAP
SAP HANA	Notas de SAP: <a href="#">2112604 FAQ: SAP HANA Compression (Preguntas frecuentes sobre la compresión de SAP HANA)</a> [Se necesita acceso al portal de SAP]
SAP ASE	(Consulte la documentación de SAP o del proveedor a modo de guía)
IBM Db2	Notas de SAP: <a href="#">1555903 DB6: Supported IBM Db2 Database Features (DB6: Características de bases de datos de IBM Db2 compatibles)</a> [Se necesita acceso al portal de SAP]
Oracle	Notas de SAP: <a href="#">1289494 FAQ: Oracle compression (Preguntas frecuentes: compresión de Oracle)</a> [Se necesita acceso al portal de SAP]
Microsoft SQL Server	Notas de SAP: <a href="#">1488135 Database compression for SQL Server (Compresión de bases de datos para SQL Server)</a> [Se necesita acceso al portal de SAP]

Base de datos	Documentación de SAP o Notas de SAP
SAP MaxDB	(Consulte la documentación de SAP o del proveedor a modo de guía)

### Sugerencia 19.3.2: utilice operaciones de reorganización y reclamo de bases de datos

El espacio que no se utiliza dentro de la base de datos, debido al uso orgánico o las actividades de archivo y limpieza dirigidas, puede requerir una operación de reorganización o reclamo para lograr los ahorros de espacio. Si reclama espacio de forma regular, reducirá el incremento general y el requisito de almacenamiento o memoria adicional. En las siguientes notas, se brinda una introducción para las distintas bases de datos, pero consulte la siguiente documentación de SAP y sobre bases de datos:

Base de datos	Documentación de SAP o notas de SAP
SAP HANA	Notas de SAP: <a href="#">2499913 How to shrink SAP HANA Data Volume size (Cómo comprimir el tamaño del volumen de datos de SAP HANA)</a> [Se necesita acceso al portal de SAP]
SAP ASE	Notas de SAP: <a href="#">2543407 reorg rebuild with online - SAP ASE for Business Suite (Reorganización y recreación en línea: SAP ASE para Business Suite)</a> [Se necesita acceso al portal de SAP]
IBM Db2	Notas de SAP: <a href="#">1942183 DB6: When to consider a table or index reorganization (DB6: Cuándo considerar una reorganización de tablas o índices)</a> [Se necesita acceso al portal de SAP]
Oracle	Notas de SAP: <a href="#">541538 FAQ: Reorganization (Preguntas frecuentes sobre reorganización)</a> [Se necesita acceso al portal de SAP]

Base de datos	Documentación de SAP o notas de SAP
Microsoft SQL Server	Notas de SAP: <a href="#">1721843 MSSQL: Post-step s after archiving, deleting or compression (MSSQL: Pasos posteriores después de archivar, borrar o comprimir)</a> [Se necesita acceso al portal de SAP]
SAP MaxDB	(Consulte la documentación de SAP o del proveedor a modo de guía)

## Práctica recomendada 19.4: revise la estrategia de copias de seguridad para aplicar mejoras

Cuando ejecuta SAP on AWS, debe evaluar su enfoque con respecto a las copias de seguridad y retención para optimizar los costos asociados con la ubicación, retención y recuperación.

### Sugerencia 19.4.1: evalúe las ubicaciones de sus copias de seguridad

Amazon S3 es la solución de almacenamiento de largo plazo sugerida para las copias de seguridad del sistema SAP por sus opciones de bajo costo, durabilidad y clase de almacenamiento. Para copiar los datos de sus volúmenes de Amazon EBS en Amazon S3, puede usar instantáneas de un punto temporal, herramientas de bases de datos integradas o llamadas a la API directas para transferir datos.

Las instantáneas son copias de seguridad progresivas, es decir, solo se guardan en el dispositivo los bloques que se han modificado después de la instantánea más reciente. De esta manera, se minimiza el tiempo requerido para crear la instantánea y se ahorran costos de almacenamiento sin duplicar datos.

Las soluciones de copias de seguridad de bases de datos requieren un conocimiento del estado de la base de datos para garantizar la consistencia. AWS ofrece una solución de copia de seguridad de SAP HANA (AWS Backint for SAP HANA) sin costo adicional, que se integra directamente con Amazon S3. Para otras bases de datos compatibles con SAP, hay proveedores de bases de datos o herramientas de copias de seguridad provistas por terceros disponibles que respaldan la copia de seguridad directa a Amazon S3.

- Documentación de SAP: [Featured backup solutions \(Soluciones de copia de seguridad destacadas\)](#)

Para los requisitos ad hoc o para las áreas de almacenamiento provisional, es posible que primero sea necesario hacer una copia de seguridad en Amazon EBS. Para estos casos de uso, un volumen ST1 constituiría un volumen de HDD de bajo costo que proporciona características de rendimiento y producción aptas para las copias de seguridad. Seleccionar un volumen ST1 puede reducir los costos de almacenamiento generales cuando se requiere hacer una copia de seguridad de la base de datos de SAP en el disco.

- Documentación de AWS: [Tipos de volúmenes de Amazon EBS](#)

Si utiliza Amazon EFS para hacer copias de seguridad, considere el acceso poco frecuente de EFS. Esta clase de almacenamiento reduce los costos de almacenamiento para los archivos a los que no se accede todos los días. El acceso poco frecuente de una zona de Amazon EFS no se recomienda para las copias de seguridad, debido a que los datos solo residen en una AZ.

Sugerencia 19.4.2: revise e implemente una política de retención para las copias de seguridad estándar

Para controlar los costos, tiene que implementar una política de retención alineada con sus requisitos comerciales. Amazon S3 ofrece una gama de clases de almacenamiento diseñadas para casos de uso distintos con características como costo por GB, cargo de duración de almacenamiento mínimo y tarifa de recuperación (cuando corresponde). Entender los requisitos de retención y acceso para las copias de seguridad ayudará a determinar qué clase de almacenamiento es más adecuado para cumplir sus requisitos.

Las políticas de ciclo de vida de S3 se pueden usar para hacer transferencias de forma automática a una clase de almacenamiento diferente sin ningún cambio en su aplicación. Por ejemplo, las copias de seguridad con períodos de retención más cortos pueden ser más aptos para S3 Standard que S3-IA o Amazon S3 Glacier debido a los costos de duración de almacenamiento mínimos y las tarifas de recuperación asociadas con estas clases. Las copias de seguridad con períodos de retención más largos, como copias de seguridad mensuales para fines de auditoría, son más aptas para S3-IA o Amazon S3 Glacier dependiendo del período de retención requerido.

- Documentación de AWS: [Clases de almacenamiento de Amazon S3](#)
- Servicio de AWS: [Amazon Data Lifecycle Manager](#)

- Documentación de AWS: [Administración del ciclo de vida de Amazon EFS](#)
- Servicio de AWS: [AWS Backup](#)

Sugerencia 19.4.3: cree una estrategia para la creación de copias de seguridad ad hoc

Las copias de seguridad ad hoc de un sistema o sistema de archivos asociado puede ser un requisito. Estas copias de seguridad pueden requerirse antes de un cambio o como referencia para el estado del sistema en un punto temporal particular. Es posible que estas copias de seguridad no estén alineadas con períodos de retención estándar, por lo que deberá adoptar un cronograma o proceso aparte para garantizar que las políticas del uso y del ciclo de vida del almacenamiento, lo que incluye la eliminación, sean las más rentables para los requisitos individuales de esa copia de seguridad.

Sugerencia 19.4.4: revise la configuración de la copia de seguridad con respecto al enfoque de recuperación

Las copias de seguridad se utilizan para restaurar el sistema a un punto temporal anterior y protegerlo contra situaciones de error. Para garantizar la rentabilidad de un almacenamiento robusto pero no excesivo de copias de seguridad, es necesario revisar el enfoque de recuperación. Ponga a prueba las suposiciones sobre los requisitos para las copias de seguridad más antiguas y granulares. Determine si estas copias de seguridad anteriores serían necesarias en caso de una recuperación.

Por ejemplo, es una estrategia válida usar la base de datos y copias de seguridad del sistema de archivos. Sin embargo, si en el mecanismo principal para la recuperación se utilizan herramientas de restauración de bases de datos, puede haber oportunidades para optimizar costos al reducir la retención o la eliminación de copias de seguridad de instantáneas para algunos volúmenes.

- Documentación de AWS: [Instantáneas de Amazon EBS](#)
- Documentación de AWS: [Lista de verificación de prácticas recomendadas de AWS Trusted Advisor](#)

Práctica recomendada 19.5: considere opciones de categorización para los datos en tiempo real

El impulsor principal del costo de computación con SAP HANA es la cantidad de memoria requerida. En consecuencia, el uso de opciones de descarga y categorización de datos puede reducir los costos de computación. Si bien otras bases de datos pueden incluir opciones de categorización, no se mencionan aquí. Consulte con su proveedor de bases de datos cuáles son las opciones disponibles.

Sugerencia 19.5.1: evalúe la categorización dinámica, los nodos de extensión y el almacenamiento casi lineal (NLS) para las cargas de trabajo basadas en SAP HANA OLAP

La categorización dinámica de SAP HANA es un complemento opcional de la base de datos de SAP HANA para administrar datos históricos. El propósito de la categorización dinámica es ampliar la memoria de SAP HANA con un almacén columnar centrado en el disco (en oposición al almacén en la memoria de SAP HANA) para administrar los datos a los que se accede con poca frecuencia. La categorización dinámica solo se puede usar para casos de uso de SAP HANA nativos y no para Business Warehouse (BW) en casos de uso de HANA o BW/4 HANA.

Un nodo de extensión de SAP HANA es un nodo de trabajo de SAP HANA de uso especial que se configura y reserva específicamente para almacenar datos tibios. Un nodo de extensión de SAP HANA permite almacenar datos tibios para los casos de uso de análisis de SAP Business Warehouse (BW) o SAP HANA nativos. La cantidad total de datos que se pueden almacenar en el nodo de extensión de SAP HANA varía de 1 a 2 veces la cantidad total de memoria de su nodo de extensión.

El Near-Line Storage (NLS, almacenamiento casi lineal) de SAP BW con SAP IQ permite almacenar datos fríos afuera de BW en una base de datos de HANA o BW/4 HANA. NLS permite mover los datos fríos de la base de datos HANA para almacenarlos en el servidor de SAP IQ.

- Documentación de AWS: [SAP Data Tiering \(Categorización de datos de SAP\)](#)

Sugerencia 19.5.2: evalúe el envejecimiento de datos y la Native Storage Extension (NSE, extensión de almacenamiento nativa) de SAP HANA para las cargas de trabajo basadas en OLTP

El envejecimiento de datos ayuda a liberar memoria de SAP HANA a través del almacenamiento de datos a los que se accede con menos frecuencia en la zona del disco.

- Documentación de AWS: [SAP Data Tiering](#)

Sugerencia 19.5.3: considere utilizar lagos de datos para los grandes volúmenes de datos analíticos

Cuando se analizan datos de SAP y datos que no pertenecen a SAP, los lagos de datos basados en S3 representan una opción rentable para el almacenamiento de datos.

- Blog de SAP on AWS: [Building data lakes with SAP on AWS \(Cómo crear lagos de datos con SAP on AWS\)](#)

## Práctica recomendada 19.6: evalúe las opciones de archivado y descarga

Si recurre a opciones para archivar datos a los que se accede con poca frecuencia o descargar objetos grandes en un almacenamiento casi lineal, puede reducir los costos de infraestructura y de respaldo.

Sugerencia 19.6.1: implemente el archivado de tablas grandes con datos de acceso poco frecuente

Especialmente en las bases de datos de SAP HANA, podrá obtener beneficios de costos si recurre a estrategias de archivado para gestionar el incremento de las bases de datos.

- Documentación de SAP: [Data Archiving \(Archivado de datos\)](#)

Sugerencia 19.6.2: evalúe las herramientas de archivado que respaldan Amazon S3 como destino

Amazon S3 está diseñado para tener una alta disponibilidad y durabilidad, y ofrece una amplia gama de clases de almacenamiento rentables. Por este motivo, es ideal para almacenar datos de archivos de SAP con el menor TCO.

- Documentación de AWS: [Clases de almacenamiento de Amazon S3](#)
- Documentación de SAP: [SAP Certified Archiving Solutions \(Soluciones de archivado con certificación de SAP\)](#)

Sugerencia 19.6.3: utilice un sistema de administración de datos para objetos grandes

Conozca las diferentes opciones, y sus beneficios de costos, para realizar descargas y administrar datos afuera de la base de datos de SAP cuando se trata de objetos grandes, como facturas e imágenes. Considere los requisitos comerciales para acceder a los datos, el esfuerzo de implementación y la complejidad de la administración continua.

Los objetos grandes aumentan el tamaño de la base de datos, lo que infla los costos de recursos y de copias de seguridad. Las opciones del sistema de administración de datos pueden proporcionar una solución de almacenamiento de menor costo.

- Documentación de SAP: [SAP Document Management \(Administración de documentos de SAP\)](#)
- Documentación de SAP: [Search for Certified ILM Solutions \(Búsqueda de soluciones de ILM certificadas\)](#)

## 20. Administre los costos con visibilidad, planificación y administración

¿Cómo se pone en práctica la Cloud Financial Management (CFM, administración financiera en la nube) para garantizar la optimización y reconocimiento de costos? Partiendo desde la concepción hasta la operación, ¿cómo se establecen controles sobre el presupuesto de la infraestructura en la nube de SAP y cómo se continúa optimizando su uso de acuerdo con los requisitos empresariales?

ID	Prioridad	Práctica recomendada
<input type="checkbox"/> Práctica recomendada 20.1	Obligatorio	Planifique el modelo de consumo y el uso del entorno durante las fases del proyecto
<input type="checkbox"/> Práctica recomendada 20.2	Obligatorio	Establezca un modelo de costos planificado de varios años aprovechando distintos enfoques de precios
<input type="checkbox"/> Práctica recomendada 20.3	Altamente recomendado	Establezca un presupuesto y mecanismos de asignación de costos y seguimiento, incluida la detección de anomalías
<input type="checkbox"/> Práctica recomendada 20.4	Recomendado	Establezca procedimientos de aprobación y controles relacionados con costos
<input type="checkbox"/> Práctica recomendada 20.5	Recomendado	Revise el uso para detectar oportunidades de optimización



## Práctica recomendada 20.1: planifique el modelo de consumo y el uso del entorno durante las fases del proyecto

Durante los proyectos, dentro de los que se incluyen proyectos de migración o implementación, entre otros, suele haber un enfoque por fases para implementar los sistemas. También hay un período de estabilización en el que se establece el ajuste de tamaño y el perfil de uso. Aproveche la flexibilidad y las capacidades de instancias bajo demanda para minimizar los costos durante este período.

### Sugerencia 20.1.1: planifique implementar sistemas solo cuando se requiera

La reducción de los plazos de entrega debería darle opciones para implementar sistemas solo cuando se requiere. En el caso de los sistemas de proyectos de corto plazo, utilice instancias bajo demanda para crear sistemas de proyectos mientras dure el requisito.

### Sugerencia 20.1.2: evalúe las opciones de precios según la duración esperada y el perfil de uso

La duración del proyecto y los horarios de trabajo influyen en el modelo de precios. Un modelo de precios bajo demanda suele ser la opción predeterminada al comienzo de un proyecto. Garantice que se defina y evalúe un presupuesto para adaptarlo a las opciones más económicas, si corresponde.

### Sugerencia 20.1.3: planifique suspender o sacar de servicio los sistemas que no se utilizan

Cuando los proyectos ya no están activos o han alcanzado sus objetivos, tenga en cuenta el ahorro de costos que conseguiría por desactivar instancias y el ahorro de almacenamiento por el desmantelamiento. Por lo general, en un proyecto se realizan copias múltiples de un sistema durante la migración. Recuerde apagar los sistemas cuando no se utilizan.

## Práctica recomendada 20.2: establezca un modelo de costos planificado de varios años aprovechando distintos enfoques de precios

Establezca un plan de varios años de sus requisitos de capacidad para garantizar que está aprovechando al máximo los modelos de precios a fin de maximizar los descuentos disponibles de AWS. Evalúe sus costos como referencia y hágalos un seguimiento. Los modelos de precios en la nube proporcionan flexibilidad que le permite adaptar elásticamente la infraestructura a los requisitos cambiantes del negocio. Antes de pactar compromisos con Savings Plans o instancias reservadas de largo plazo, conozca y planifique el uso esperado del sistema SAP como mínimo en un horizonte de 3 años. Aplique pruebas, datos de SAP Quick Sizer y pronósticos de crecimiento para fundamentar el plan de compromiso y aproveche los descuentos máximos para su carga de trabajo.

Sugerencia 20.2.1: establezca un valor estimado de capacidad y comprenda los eventos clave de su empresa

En general, las cargas de trabajo de SAP son estables, con modelos de uso y horas de operación conocidos. Establezca como valor de referencia una capacidad de estado regular bien comprendida para sus sistemas SAP. Para ello, realice pruebas de rendimiento y supervise su entorno de producción durante las semanas iniciales de su implementación.

Amplíe el cálculo de la capacidad de estado regular hasta un horizonte de tres años como mínimo teniendo en cuenta los siguientes parámetros:

- Eventos comerciales importantes, como fusiones, adquisiciones y desinversiones
- Cambios de las normativas que pueden afectar los requisitos de almacenamiento de datos o frecuencia del proceso comercial
- Aumento de los datos debido a las operaciones comerciales normales (especialmente importante para las bases de datos en memoria como SAP HANA, ya que los datos afectan el ajuste de tamaño de la computación, además del ajuste de tamaño del almacenamiento)
- Actualizaciones importantes del sistema, reemplazo del sistema o desmantelamiento

Sugerencia 20.2.2: evalúe si los compromisos a uno o tres años son adecuados

Evalúe en qué medida sus cargas de trabajo de SAP podrían aprovechar el compromiso de computación de tres años y maximizar los descuentos disponibles mediante el uso de su cálculo de capacidad. Considere lo siguiente:

- ¿Puede contemplar pactar un compromiso de tres años para todas las necesidades de computación de su carga de trabajo de SAP?
- ¿Puede considerar un compromiso de tres años para un subconjunto de sus necesidades que confía que no cambiarán? Por ejemplo, los servidores de la aplicación principal de SAP o bases de datos primarias.
- ¿Su carga de trabajo de SAP forma parte de una organización de AWS más amplia que podría utilizar compromisos de computación en exceso cuando los cambios en sus requisitos de capacidad de SAP reducen la necesidad de computación en un punto temporal futuro?
- ¿Su carga de trabajo de SAP forma parte de una organización de AWS más amplia y podría compartir compromisos de computación para entornos que no son de producción y que no tienen que funcionar las 24 horas del día, los 7 días de la semana?

- En caso de cambios de capacidad de mediano plazo, ¿el beneficio de comprometerse a un plan de computación de 3 años supera el desperdicio de capacidad de exceso o sin utilizar (por ejemplo, el punto de equilibrio frente a un compromiso de plazo más corto está en el mes 20)?
- ¿Puede contemplar un compromiso de plazo más corto (un año) para las aplicaciones que probablemente estarían afectadas por cambios empresariales importantes o reemplazos en el corto plazo?
- ¿Las fluctuaciones cambiarias son un factor que debería tener en cuenta? Los precios de AWS (a excepción de AWS China) están expresados en dólares estadounidenses (USD). Si desea un tipo de cambio fijo, tal vez pueda considerar modelos de precios de pago total por adelantado, si ello es posible.

Establezca un plan para emparejar los requisitos de capacidad de la carga de trabajo con la duración del compromiso a fin de maximizar los descuentos.

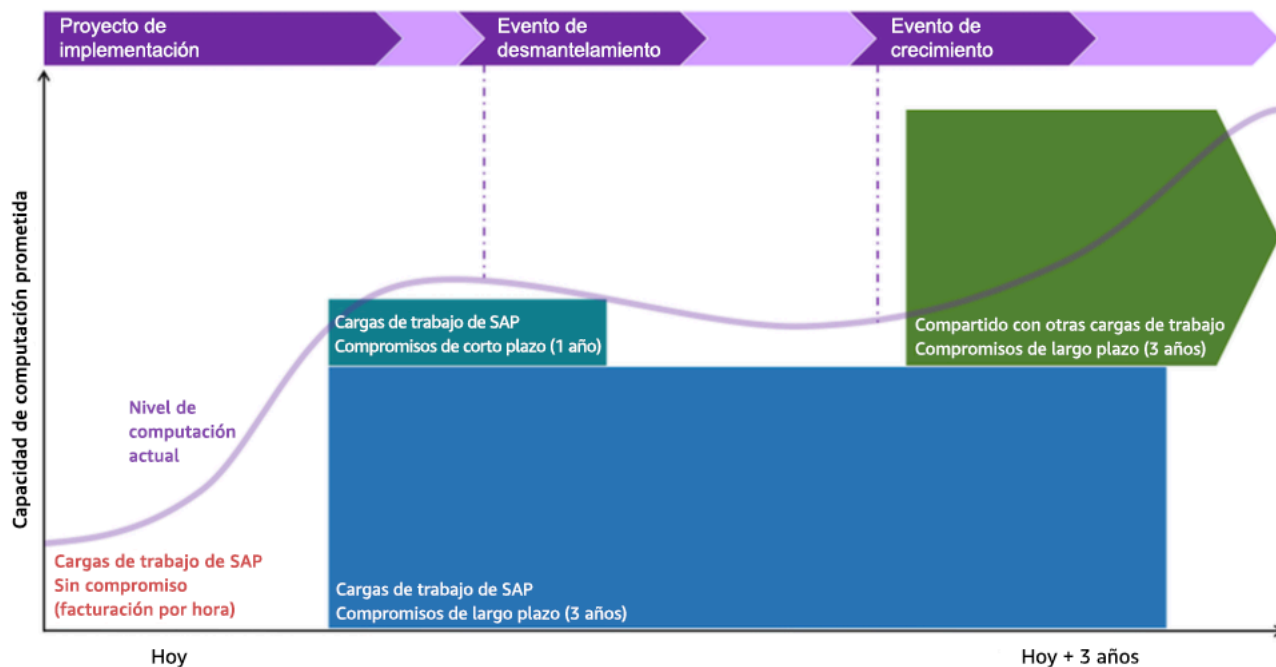


Figura: plazo de ejemplo para planificar los compromisos de computación de SAP on AWS

Sugerencia 20.2.3: evalúe si es adecuado fijar tipos de computación para obtener mayores descuentos

En general, las cargas de trabajo de SAP utilizan un conjunto limitado de tipos de computación de AWS y, por tanto, debe considerar si comprometerse con familias de computación específicas o tipos de instancias específicas es apropiado para su carga de trabajo a fin de maximizar el descuento.

Los dos enfoques de precios con mayores descuentos en materia de computación son EC2 Instance Savings Plans y las instancias reservadas estándar.

Considere lo siguiente:

- Identifique los tipos de computación que más se utilizan en su infraestructura y considere adquirir instancias reservadas estándar o un EC2 Instance Savings Plans específico para dicho tipo de computación. Por ejemplo, si utiliza `m5.xlarge` para los servidores de su aplicación en varias aplicaciones SAP, dicho tipo de instancia sería un buen candidato para un Savings Plan específico de EC2 o una instancia reservada estándar, puesto que es muy probable que siempre utilice este compromiso.
- Identifique los componentes de computación que tienen una alta probabilidad de cambiar las familias de EC2 debido al aumento de las cargas de trabajo o los eventos comerciales. Considere adquirir Compute Savings Plans o instancias reservadas convertibles más genéricos para estos elementos. Por ejemplo, si tiene una base de datos de SAP HANA que debe trasladarse entre una familia de computación de EC2 `r5` y `x1e` debido a un aumento de su tamaño después de solo 6 meses, esta sería una buena candidata para una instancia reservada convertible de corto plazo o un Compute Savings Plan.
- Identifique los puntos de equilibrio para los precios de computación generales frente a los específicos y téngalos presente cuando elige el tipo de compromiso. Por ejemplo, puede ser más barato comprar una instancia reservada estándar durante tres años en vez de elegir una instancia reservada convertible de tres años si el cambio de ajuste de tamaño ocurre en el tercer año. También puede considerar vender el valor de la instancia reservada residual en el Marketplace de la instancia reservada de AWS.
- Antes de cambiar los tipos de instancia, identifique el uso de la oferta privada del vendedor de AWS Marketplace o el software de suscripción anual. Esto evitará incurrir en costos de software adicionales. Los dos planes supondrían un ahorro, ya que le permiten comprometerse a ejecutar productos de software en una instancia de Amazon EC2 durante un tiempo específico. Por ejemplo, la adquisición de una suscripción anual de software para ejecutarlo en una instancia `r4.xlarge` instancia en ejecución. Decidió cambiar el tipo de instancia a `r5.xlarge`. La suscripción anual ya no está vinculada con la instancia, pero sigue activa. Esto genera precios bajo demanda adicionales para el software en `r5.xlarge`. Considere esperar al vencimiento de la suscripción anual antes de cambiar el tipo de instancia.

Sugerencia 20.2.4: evalúe si los Savings Plans, las instancias reservadas o ambos son más adecuados

Elija una combinación de Savings Plans con instancias reservadas para obtener beneficios de distintos modelos, si es adecuado para su carga de trabajo de SAP. Determine sus períodos de compromiso y requisitos de computación de forma completa y luego seleccione su modelo de precios.

Puede encontrar más información sobre las diferencias entre Savings Plans y las instancias reservadas en [Optimización de costos]: [Práctica recomendada 18.1: conozca las opciones de pago y compromisos disponibles para Amazon EC2](#) y para [Compute Savings Plans y las instancias reservadas](#).

Tenga en cuenta [fiabilidad] [Práctica recomendada 10.2: seleccione una arquitectura adecuada para sus requisitos de disponibilidad y capacidad](#). Se explican las diferencias de reserva de capacidad e intercambios entre Savings Plans y las instancias reservadas.

Sugerencia 20.2.5: convierta su plan de capacidad en un modelo de costos para fines de presupuesto y seguimiento

Convierta sus Savings Plans, elecciones de instancias reservadas y presupuesto bajo demanda en un plan de costo que estime su gasto de AWS para la infraestructura SAP en un plazo mínimo de tres años. Combine su cálculo de computación con otros costos de AWS para finalizar el modelo de costos de su carga de trabajo de SAP para fines de presupuesto y seguimiento.

Cuando calcule los costos de SAP, recuerde incluir lo siguiente:

- Costos de almacenamiento con computación adjunta (como volúmenes de Amazon EBS)
- Costos de almacenamiento de archivos compartidos (como Amazon EFS y Amazon FSx)
- Costos de almacenamiento de copia de seguridad (como Amazon S3 y Amazon S3 Glacier)
- Costos de red y de VPC (como Elastic Load Balancers, puertas de enlace de NAT, puertas de enlace de tránsito, costos de salida de la red, conexión directa y VPN)
- Costos de administración y servicio de gobernanza (como métricas detalladas de CloudWatch, AWS CloudTrail y AWS Config)
- Costos de servicio de seguridad (como AWS WAF, Amazon GuardDuty y AWS Shield)
- Costos de AWS Support (Business o Enterprise)
- Considere los programas de descuento para empresas o los descuentos por volumen para los que sea elegible (hable con su gerente de cuenta de AWS para obtener más detalles)
- Moneda: es importante que sepa que los precios de AWS están expresados en dólares estadounidenses (USD). Puede elegir una moneda de facturación y sus facturas se computarán en USD y se convertirán a su moneda de preferencia a un tipo de cambio competitivo.

## Práctica recomendada 20.3: establezca un presupuesto y mecanismos de asignación de costos y seguimiento, incluida la detección de anomalías

Hay [pautas](#) en Well-Architected Framework para implementar la administración financiera. Fije las expectativas sobre costos en la nube con presupuestos anuales, trimestrales, mensuales o incluso diarios, dependiendo de sus necesidades empresariales. Ajuste los pronósticos de forma regular para alinearlos con el uso e identificar tendencias y anomalías. Defina mecanismos para la asignación de costos a través de estrategias de contabilidad y etiquetado.

Sugerencia 20.3.1: utilice las herramientas de costos y facturación para aumentar la visibilidad de los gastos

Los sistemas SAP suelen ser estáticos en sus modelos de uso una vez establecidos. Si utiliza un modelo de precios bajo demanda, ya sea de forma permanente o durante fases del proyecto, puede ver una fluctuación en los costos de Amazon EC2. Si no se implementaron estrategias para administrar volúmenes de datos, puede esperarse que los costos de Amazon EBS y Amazon S3 sean más altos de lo esperado.

Una buena herramienta para visibilizar sus gastos con un bajo esfuerzo de configuración es la [Detección de anomalías de costos de AWS](#). Esta herramienta utiliza tecnologías de machine learning (ML) avanzadas para identificar los gastos anómalos y las causas principales, de manera que usted pueda tomar cartas en el asunto. Utilice [AWS Budgets](#) para definir presupuestos personalizados según sus costos y uso esperados. Configure las alertas de presupuesto para que se le notifique cuándo se supera un umbral.

[AWS Cost Explorer](#) y [AWS Billing and Cost Management](#) proveen herramientas para la visibilidad y el análisis.

Puede encontrar más guías en la sección de Well-Architected Framework [Optimización de costos] [Conocimiento de los gastos y el uso](#).

Sugerencia 20.3.2: analice y asigne gastos con etiquetas

Puede crear [etiquetas de asignación de costos](#) que lo ayuden a identificar los precios de los recursos de AWS con base en las cuentas individuales, los recursos, las unidades comerciales y los entornos de SAP. Estas etiquetas se hacen visibles en los informes de facturación de AWS y se pueden analizar usando Cost Explorer. Puede utilizar las etiquetas de asignación de costos para determinar los costos asociados con entornos de SAP individuales. Ellas ayudan a conocer si se debe implementar una acción para reducir o eliminar los costos asociados con los entornos

específicos, como entornos transitorios o entornos de proyecto que ya no se requieren. Debe tener implementado un proceso para identificar los recursos que no tienen etiquetas de asignación de costos adjuntas. Implemente las acciones requeridas para agregar etiquetas de asignación de costos a esos recursos.

- Blog de SAP on AWS: [Tagging Recommendations for SAP on AWS](#)

## Práctica recomendada 20.4: establezca procedimientos de aprobación y controles relacionados con costos

Puede ser necesario adaptar procesos de evaluación de costos tradicionales para la nube. Aprenda cómo implementar las prácticas y políticas financieras correctas en la guía [de administración financiera en la nube de AWS](#).

Sugerencia 20.4.1: eduque a los administradores sobre las consecuencias de los costos

Introduzca mecanismos para asignar responsabilidad y provea incentivos para optimizar los costos.

Sugerencia 20.4.2: solo concédale a ciertos usuarios la capacidad de aprovisionar instancias usando controles de IAM

Utilice políticas de IAM alineadas con el tipo de recurso y función laboral dentro de los límites de la cuenta para garantizar el control de costos. Por ejemplo, puede permitir el control de sistemas adicionales a escala pequeña en una cuenta de entorno aislado dentro de un equipo de proyecto, pero contar con un proceso de aprobación adicional y de acceso restringido para las instancias más grandes en una cuenta de producción.

## Práctica recomendada 20.5: revise el uso para detectar oportunidades de optimización

Revise de forma periódica la carga de trabajo de SAP para identificar las oportunidades de optimizar costos. Las revisiones regulares deben centrarse en minimizar las diferencias y anomalías halladas entre su factura de AWS y su presupuesto de carga de trabajo de SAP; verificar que todos sus recursos en la nube de SAP tengan el tamaño apropiado y no se hayan aprovisionado en exceso y entender los lanzamientos de servicios de AWS nuevos o reducciones de costos que podrían mejorar la eficacia de costos de su carga de trabajo de SAP.

Sugerencia 20.5.1: minimice el costo adicional si el uso fue más alto de lo planificado inicialmente

Es posible que su uso en la nube haya superado el modelo de costos calculado debido a eventos comerciales imprevistos o la necesidad de un rendimiento adicional. Analice estos cambios con



vistas a optimizar el costo nuevo. Considere apuntarse a compromisos de Savings Plan adicionales o solicitar nuevas instancias reservadas si se trata de un cambio sostenido.

Cuando se requiere una capacidad adicional solo durante períodos cortos, considere mecanismos de escalado horizontal (por ejemplo, servidores de aplicaciones SAP adicionales) usando el escalado automático o la capacidad de instancia bajo demanda programada para minimizar aún más el costo.

Sugerencia 20.5.2: revise las métricas de uso de la carga de trabajo de SAP y ajuste el tamaño correcto cuando sea posible

Revise de forma regular los componentes que respaldan su sistema SAP para garantizar que tengan el tamaño correcto. Use las métricas de CloudWatch para considerar lo siguiente:

- ¿La computación SAP EC2 tiene el tamaño correcto? ¿El uso de CPU o memoria es bajo? ¿Podría pasarse a un tamaño de instancia de EC2 más pequeño?
- ¿El almacenamiento de SAP tiene el tamaño correcto? ¿Hay espacio extra aprovisionado, pero sin utilizar? ¿Puede reducir los tamaños de los volúmenes?
- ¿El almacenamiento de SAP tiene el rendimiento apropiado? ¿Hay IOPS o MBps aprovisionados en exceso que podrían reducirse?
- ¿Las copias de seguridad e instantáneas se administran de manera correcta? ¿Tiene demasiadas copias de seguridad en S3 Standard que podrían archivar en Amazon S3 Standard-IA o Amazon S3 Glacier?
- Utilice herramientas como [AWS Compute Optimizer](#) y [AWS Trusted Advisor](#) para identificar las áreas adicionales de optimización. Tenga presente las restricciones de computación y almacenamiento específicas de SAP según la nota de SAP [1656099 - SAP Applications on AWS: Supported DB/OS and Amazon EC2 products](#) [Se necesita acceso al portal de SAP].

Utilice los hallazgos para ajustar continuamente el tamaño correcto de sus componentes de carga de trabajo de SAP con regularidad y maximice su uso de Savings Plans e instancias reservadas.

Sugerencia 20.5.3: conozca los servicios de AWS nuevos y planifique implementarlos si se puede lograr una optimización de costo mayor

De manera periódica, AWS lanza servicios nuevos y reduce precios. Revise los anuncios de servicios nuevos de SAP on AWS y planifique incorporarlos en su arquitectura cada 12 meses como mínimo. Si tiene un technical account manager (TAM, administrador técnico de cuenta) como parte de su acuerdo de Enterprise Support con AWS, este puede asistirlo con reuniones informativas regulares sobre los servicios nuevos y charlas sobre optimización.



Suscríbase al blog [SAP on AWS](#) y al [boletín de novedades](#) para enterarse de los anuncios y las noticias más recientes.

Consulte [excelencia operativa] [Práctica recomendada 4.4: realice revisiones regulares de las cargas de trabajo para optimizarlas en función de resiliencia, rendimiento, agilidad y costos](#) para obtener más información sobre la optimización continua de su carga de trabajo de SAP.

# Conclusión

Este enfoque le brinda orientación en materia de arquitectura para diseñar, crear y operar cargas de trabajo de SAP fiables, seguras, eficientes y rentables en AWS. Cubrimos patrones frecuentes, lecciones aprendidas y recomendaciones generales de diseño para SAP.

Aplicar el marco a su carga de trabajo lo ayuda a crear sistemas sólidos, estables y eficientes. Además, le permite enfocarse en tareas operativas de alto valor en sus cargas de trabajo de SAP y ampliar los límites del campo con el cual está comprometido.

El ecosistema de SAP continúa su evolución a medida que las aplicaciones, herramientas y procesos crecen y maduran. En la medida que ocurra esta evolución, continuaremos actualizando este documento para que pueda garantizar que sus aplicaciones SAP tengan una arquitectura adecuada.

# Colaboradores

Las siguientes personas y organizaciones colaboraron a la hora de crear este documento:

- John Studdert: gerente para EMEA, arquitecto de soluciones especializado en SAP, Amazon Web Services
- Peter Perbellini: gerente sénior para APJ, arquitecto de soluciones especializado en SAP, Amazon Web Services
- Adam Hill: arquitecto de soluciones principal especializado en SAP, Amazon Web Services
- Nerys Olver: consultor de SAP sénior, Amazon Web Services
- Wilson Puvvula: arquitecto de soluciones sénior de las cuentas globales, Amazon Web Services
- Christopher Spruell: arquitecto de soluciones sénior de las cuentas globales, Amazon Web Services
- Eneko Bilbao: arquitecto de soluciones principal especializado en SAP, Amazon Web Services
- Sabari Radhakrishnan: arquitecto de soluciones principal especializado en SAP, Amazon Web Services
- Somckit Khemmanivanh: ingeniero de desarrollo de sistemas sénior de EC2 Enterprise, Amazon Web Services
- Sander Bleijenbergh: arquitecto de soluciones sénior de ISV, Amazon Web Services
- Harpreet Singh: gerente sénior de arquitectura de soluciones de socios, Amazon Web Services
- Manoj Muthukrishnan: arquitecto de soluciones sénior especializado en SAP, Amazon Web Services
- Jongnam Lee: arquitecto de soluciones principal de Data Analytics Lens, Well-Architected, Amazon Web Services
- Ben Potter: arquitecto de soluciones principal del pilar de seguridad, Well-Architected, Amazon Web Services

# Historial del documento

Para recibir notificaciones acerca de las actualizaciones a este documento técnico, suscríbase a la fuente de RSS.

Cambio	Descripción	Fecha
<a href="#">Actualización menor</a>	Se corrigieron los enlaces rotos.	January 20, 2022
<a href="#">Publicación inicial</a>	Primera publicación de SAP Lens.	October 28, 2021

## Note

Para suscribirse a las actualizaciones de RSS, debe tener el complemento de RSS habilitado en su navegador.

# Principios de diseño organizados por pilar

Estos son los principios de diseño descritos en este artículo organizados según los pilares de AWS Well-Architected Framework.

## Excelencia operativa

- [1. Diseñe la carga de trabajo de SAP para permitir la comprensión y la reacción a su estado](#)
- [2. Reduzca los defectos, facilite la corrección y mejore el flujo de trabajo de cambio de SAP](#)
- [3. Comprenda cómo operará la carga de trabajo](#)
- [4. Valide y mejore su carga de trabajo de SAP con regularidad](#)

## Seguridad

- [5. Comprenda los estándares de seguridad y cómo se aplican a su carga de trabajo de SAP](#)
- [6. Utilice controles de infraestructura y de software para reducir los errores de configuraciones de seguridad](#)
- [7. Controle el acceso a sus cargas de trabajo de SAP a través de la identidad y los permisos](#)
- [8. Proteja sus datos de SAP en reposo y en tránsito](#)
- [9. Implemente una estrategia de seguridad para registrar, probar y responder a eventos de seguridad](#)

## Fiabilidad

- [10. Diseñe para tolerar errores](#)
- [11. Detecte los errores y reaccione ante ellos](#)
- [12. Haga un plan de recuperación de datos](#)

## Eficiencia de rendimiento

- [13. Seleccione la solución de computación óptima](#)
- [14. Seleccione la solución de almacenamiento óptima](#)

- [15. Evalúe las opciones de ajuste para el sistema operativo, la base de datos y la aplicación SAP](#)
- [16. Comprenda las opciones de optimización y rendimiento en curso](#)

## [Optimización de costos](#)

- [17. Evalúe los patrones de arquitectura de SAP con un enfoque en la rentabilidad](#)
- [18. Evalúe los recursos de computación de SAP para la eficiencia de costos](#)
- [19. Optimice el uso de datos de SAP para la eficiencia de costos de almacenamiento](#)
- [20. Administre los costos con visibilidad, planificación y administración](#)

# Avisos

Los clientes son responsables de hacer su propia evaluación independiente de la información en este documento. Este documento: (a) solo tiene fines informativos, (b) representa las prácticas y las ofertas de productos de AWS actuales, las cuales están sujetas a cambios sin aviso previo, y (c) no crea compromisos ni promesas de parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “en su estado existente” sin garantías, representaciones ni condiciones de ningún tipo, ya sean explícitas o implícitas. Las responsabilidades y obligaciones de AWS frente a sus clientes se rigen por los acuerdos celebrados con AWS, y este documento no forma parte de ningún acuerdo entre AWS y sus clientes, ni lo modifica.

© 2022 Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

# AWS Glossary

For the latest AWS terminology, see the [AWS glossary](#) in the Glosario de AWS Reference.