Estructura de unidades organizativas en zonas de AWS aterrizaje reguladas: un ejemplo de la industria farmacéutica

AWS Orientación prescriptiva

AWS Orientación prescriptiva: Estructura de unidades organizativas en zonas de AWS aterrizaje reguladas: un ejemplo de la industria farmacéutica

Table of Contents

Estructura de unidades organizativas en zonas de AWS aterrizaje reguladas: un ejemplo de la industria farmacéutica

Katja Mueller, Petar Forai y Keval Sheth, Amazon Web Services (AWS)

Marzo de 2023 (historial de documentos)

AWS proporciona varias configuraciones de Landing Zone Accelerator que son compatibles con sectores específicos, incluida la sanidad. El Landing Zone Accelerator for Healthcare se utiliza conjuntamente AWS Control Tower para facilitar la administración y el gobierno de un entorno de múltiples cuentas que se ajusta a las AWS mejores prácticas y a varios marcos de cumplimiento globales. Un aspecto importante de la organización de la gobernanza es Cuentas de AWS agruparse mediante unidades organizativas (OUs), de forma que se puedan administrar como una sola unidad.

En esta guía se analizan las prácticas recomendadas y algunas consideraciones para rediseñar las estructuras de UO actuales a medida que crece la madurez de la empresa en la nube. Presenta un ejemplo práctico basado en la AWS Control Tower implementación para una gran empresa farmacéutica y analiza las lecciones aprendidas de esa implementación. AWS el diseño de la zona de landing zone no es un esfuerzo de una sola vez. Se puede y se debe permitir que evolucione. Esta evolución se puede lograr de manera exitosa y eficiente mediante la aplicación de las AWS mejores prácticas y consejos destacados en esta guía.

Descripción general

Trabajamos con una farmacéutica multinacional para llevar a cabo actividades de prueba de concepto (PoC) en AWS a fin de explorar cómo podían migrar sus aplicaciones desde su entorno en las instalaciones a la Nube de AWS. A medida que empezaron a escalar y acelerar su flujo de trabajo de migración para incluir cargas de trabajo de producción, se hizo evidente que, para lograr su objetivo, necesitaban una zona de aterrizaje de AWS regulada y que cumpliera con las normas. Usamos AWS Control Tower para diseñar e implementar una nueva zona de aterrizaje de AWS.

Un aspecto importante de una nueva zona de aterrizaje de AWS y de su organización es la estructura de sus unidades organizativas (UO). Una UO es una agrupación lógica de Cuentas de AWS que se ha creado con AWS Organizations. Puede utilizar las UO para organizar las Cuentas de AWS en una jerarquía y aplicar los controles de administración y gobernanza de forma coherente y sencilla.

Puede asociar controles basados en políticas a una UO y a las Cuentas de AWS. Las UO secundarias de una UO heredan esos controles de forma automática. Por lo tanto, las UO desempeñan un papel fundamental en la administración de la seguridad y la gobernanza en AWS Organizations.

Una política es un documento JSON que incluye una o más instrucciones que definen los controles que se desean aplicar a un grupo de Cuentas de AWS. En este momento, AWS Organizations admite cuatro tipos de políticas, también llamadas políticas de control de servicio (SCP). Una SCP define los Servicios de AWS y las acciones que están disponibles para su uso en diferentes Cuentas de AWS. Por ejemplo, puede usar una SCP para exigir que las inicializaciones de instancias de Amazon Elastic Compute Cloud (Amazon EC2) usen un tipo de instancia específico.

Tipos de políticas

A continuación, se indican los tipos de políticas SCP:

- Las listas de permitidos y las listas de denegación son estrategias complementarias para cuando se aplican políticas SCP para filtrar los permisos que están disponibles para las cuentas.
- Las políticas de etiquetas lo ayudan a mantener la coherencia de las etiquetas, incluido el tratamiento de casos preferentes de valores y claves de etiquetas entre cuentas.

- Las políticas de copia de seguridad configuran las copias de seguridad de los tipos de recursos compatibles, como la ventana de tiempo de los almacenes de copia de seguridad y de destino para las copias de seguridad de todas las Regiones de AWS.
- Las políticas de exclusión de los servicios de IA activan o desactivan la mejora continua de los servicios de inteligencia artificial (IA) de AWS a nivel mundial.

Comportamiento de herencia de políticas: cuando asocia una política a una UO específica, las cuentas que pertenecen directamente a esa UO o a cualquier UO secundaria heredan la política. Cuando se asocia una política a una cuenta específica, solo afecta a esa cuenta. Para sobrescribir las políticas heredadas, introduzca políticas de excepción. La herencia permite explícitamente que todos los permisos fluyan desde el elemento raíz (UO) a cada Cuenta de AWS de esa UO y UO secundaria, a menos que deniegue un permiso explícitamente. Para denegar un permiso, debe crear una política adicional y asociarla a la UO o a la Cuenta de AWS correspondiente. Para obtener más información sobre la herencia y las excepciones de las políticas, consulte la documentación de AWS Organizations.

AWS Control Tower también proporciona su propio conjunto de controles de prevención y detección (también llamados barreras de protección) mediante la estructura de UO. Los controles de prevención de AWS Control Tower previenen las acciones mediante las SCP de AWS Organizations. Los controles de detección informan sobre las desviaciones en las configuraciones respecto al control mediante AWS Config. Para obtener más información sobre estos controles, consulte la documentación de AWS Control Tower.

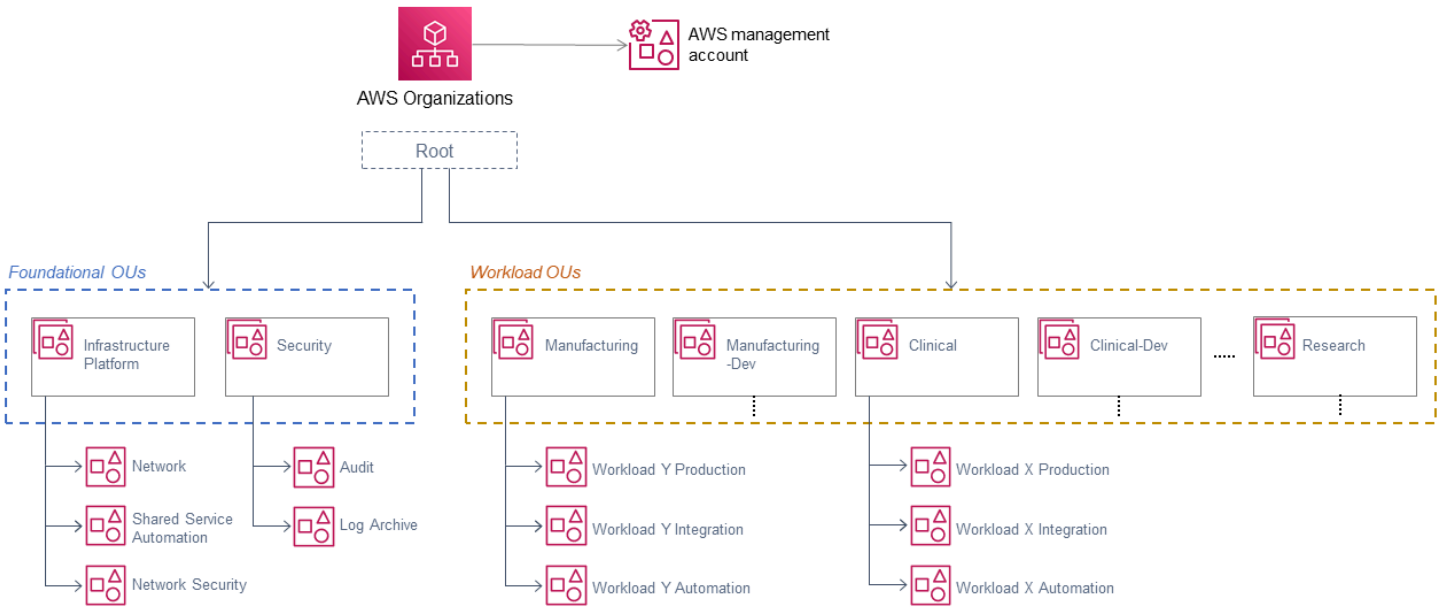
También puede activar AWS Security Hub CSPM para automatizar las comprobaciones según las prácticas recomendadas en materia de seguridad, agrupar las alertas de seguridad en un único lugar y formato y comprender la postura general de seguridad en todas las Cuentas de AWS.

Diseño de UO: fase 1

Para la empresa farmacéutica multinacional de nuestro ejemplo, el diseño inicial de las organizaciones y unidades organizativas siguió de AWS Organizations cerca AWS las recomendaciones de creación AWS Control Tower. Para ver un ejemplo, consulte Landing Zone Accelerator en AWS Healthcare. AWS Control Tower inicialmente, aprovisionó una estructura de unidad organizativa simple con unidades organizativas fundamentales comunes, tal como se describe en la entrada del blog Mejores prácticas para las unidades organizativas, e incluía la unidad organizativa de seguridad AWS Organizations, la unidad organizativa de infraestructura de plataforma y las unidades organizativas específicas de la empresa.

Diseño de arquitectura

En el siguiente diagrama se muestra la arquitectura de UO inicial.



UO de seguridad

La OU de seguridad agrupa ampliamente las funciones Cuentas de AWS relacionadas con la seguridad y utiliza dos cuentas (de auditoría y de archivo de registros) para almacenar los datos operativos de seguridad con el fin de registrar y auditar de forma centralizada el acceso al entorno. AWS servicios de seguridad básicos, como Amazon, GuardDuty y AWS Security Hub CSPM residen en la cuenta de auditoría.

UO de plataformas de infraestructura

La plataforma de infraestructura OU agrupa los grupos Cuentas de AWS que proporcionan la base de la infraestructura. Inicialmente, en esta OU se implementan Cuentas de AWS los componentes de red centrales (puertas de enlace, firewalls, concentradores de red central y servicios similares).

UO adicionales

Las demás UO específicas de la empresa (como una UO clínica) amplían las UO básicas dentro de una jerarquía de bajo nivel. Las cargas de trabajo se implementan con una estructura de varias cuentas y con entornos separados dentro de esas UO.

Este diseño inicial se basó en varias consideraciones:

- Las unidades organizativas anidadas no estaban disponibles en ese momento AWS Control Tower y requerían una amplia personalización.
- Las cargas de trabajo iniciales que se designaron para la nube se centraban en aspectos específicos de la empresa, como los ensayos clínicos o los análisis de los equipos de fabricación (vistas funcionales).
- La empresa diferencia entre cinco entornos de carga de trabajo (desarrollo, validación, integración, entrenamiento y producción). La empresa necesitaba un terreno de juego para desarrollar aplicaciones sin la estricta regulación mediante AWS controles que exigían las cargas de trabajo de producción. Las unidades organizativas de desarrollo, como la Manufacturing-Dev unidad organizativa, se asignaron con este fin.
- La automatización de las cargas de trabajo formaba parte del ecosistema de cada aplicación y no se tenía que separar.
- Los procesos de calificación de la infraestructura (IQ) y cumplimiento de las normas GxP no requerían una distinción de AWS controles a nivel de la unidad organizativa.

Diseño de UO: fase 2

En nuestro ejemplo, la farmacéutica pasó rápidamente a una nueva fase de madurez en la nube al implementar cargas de trabajo de producción calificadas en las UO que ya tenían. Esto dio inicio a una revisión del diseño inicial, y la estructura de la fase 1 se vio desafiada a medida que más cargas de trabajo migraban a la AWS landing zone regulada.

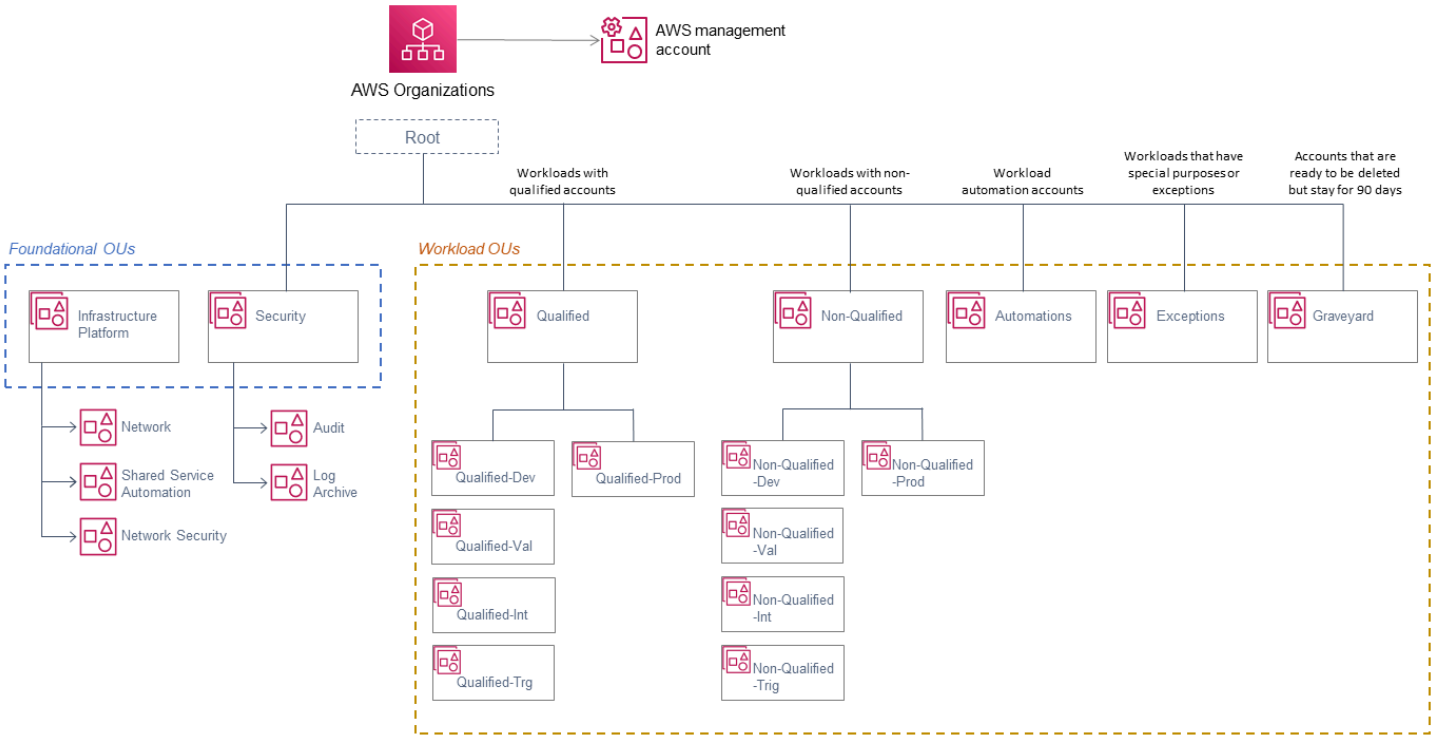
Los siguientes nuevos requisitos e información ganaron importancia:

- La empresa implementó cargas de trabajo basadas en modelos de uso compartido de datos, por lo que las aplicaciones adquirieron un carácter polivalente que ya no podía asignarse a UO independientes, como la clínica o la de fabricación.
- La cualificación (en concreto, la cualificación continua) se convirtió en un aspecto vital de muchas cargas de trabajo. Estas cargas de trabajo se tenían que integrar en los procesos operativos para que pudieran seguir las prácticas recomendadas en materia de seguridad con mayor facilidad. Las cargas de trabajo cualificadas requerían AWS controles más estrictos, que se establecieron a nivel de unidad organizativa en la fase 1.
- La funcionalidad de unidad organizativa anidada estuvo disponible en. AWS Control Tower
- La mejora de las habilidades y la experiencia permitieron comprender mejor qué políticas específicas eran relevantes para las cargas de trabajo.
- La empresa definió y acordó un modelo operativo que se basaba en la alineación de las responsabilidades.
- Los esquemas de segmentación y estructuración de las cargas de trabajo maduraron y se adoptaron para migrar las cargas de trabajo.

Como resultado, en la fase 2 se implementó un nuevo diseño y las Cuentas de AWS se migraron a esa nueva estructura. Esta nueva estructura incluye las UO que se describen en las siguientes secciones.

Diseño de arquitectura

En el siguiente diagrama se muestra la arquitectura de UO de la fase 2.



UO de seguridad

La unidad organizativa de seguridad contiene una amplia gama de funciones Cuentas de AWS relacionadas con la seguridad y utiliza dos cuentas (de auditoría y de archivo de registros) para almacenar los datos operativos de seguridad con el fin de registrar y auditar de forma centralizada el acceso al entorno. AWS servicios de seguridad básicos, como Amazon, GuardDuty y AWS Security Hub CSPM residen en la cuenta de auditoría. Esta UO permanece inalterada con respecto al diseño original.

UO de plataformas de infraestructura

La OU de Infrastructure Platform contiene cuentas de infraestructura fundamentales, como las redes y la automatización compartida en toda la AWS landing zone. Esta UO permanece inalterada con respecto al diseño original.

UO cualificada

La UO cualificada contiene las cargas de trabajo que necesitan una infraestructura cualificada, como una administración de cambios, una cualificación y una validación estrictas.

Non-qualified OU

La Non-Qualified OU contiene cargas de trabajo que no tienen requisitos de GxP o que no son fundamentales para la empresa.

UO de automatización

La OU Automations contiene recursos compartidos para la automatización de las cargas de trabajo, como las canalizaciones de integración y entrega continuas (CI/CD) para la administración de la infraestructura. Según los requisitos, la automatización puede dividirse en varios entornos o alojarse en una sola Cuenta de AWS.

UO de excepciones

La UO de excepciones contiene las cargas de trabajo que necesitan un tratamiento especial que, de otro modo, las políticas impedirían. Por ejemplo, los buckets de Amazon Simple Storage Service (Amazon S3) de fácil acceso y lectura pertenecerían a la UO de excepciones.

UO de cargas de trabajo inactivas

La OU Graveyard contiene Cuentas de AWS cuatro cargas de trabajo que se eliminarán. Las políticas de estas cuentas se tienen que eliminar para permitir un acceso administrativo sencillo y efectivo hasta que la cuenta caduque o se elimine.

Migración y verificación de UO

En el caso de la multinacional farmacéutica de nuestro ejemplo, los equipos de ingeniería de plataformas en la nube y de administración de cambios acordaron un plan y una programación para la migración. Las Cuentas de AWS se revisaron y clasificaron de acuerdo con el impacto para la empresa y la criticidad como parte de la planificación.

La nueva estructura de UO se implementó junto con la estructura de UO actual para permitir realizar pruebas en las nuevas políticas y la migración gradual. Creamos nuevas UO vacías con UO secundarias y asignamos políticas de AWS Organizations y controles de AWS Control Tower a esas UO secundarias.

Las políticas de AWS Organizations se migraron manualmente aplicando las políticas deseadas en la nueva estructura. Utilizamos controles puntuales manuales para verificar las políticas de AWS Organizations y mecanismos automatizados para verificar los controles de AWS Control Tower. Las Cuentas de AWS no se trasladaron a las nuevas UO hasta que estas comprobaciones se realizaron correctamente.

La migración de cuentas fue semiautomática y se realizó de forma escalonada o por lotes. La migración inicial se centró en las Cuentas de AWS que se consideraban menos críticas y utilizó un lote de cinco Cuentas de AWS por ejecución de migración. Los lotes de migración no superaron las 10 cuentas. Cuando se migraron las cuentas, los revisores y evaluadores utilizaron la consola de AWS Control Tower para comprobar que estas cuentas se habían trasladado a la UO correcta y supervisaron los registros de AWS CloudTrail para comprobar que no hubiera errores. Los revisores también comprobaron las consolas de AWS Service Catalog y AWS Control Tower en busca de desviaciones o cuentas con estados defectuosos o desconocidos.

Los cambios en la ubicación de las cuentas en las UO no afectaron a la conectividad ni a la accesibilidad de los recursos. No se informó de ninguna interrupción en las aplicaciones de producción.

Lecciones aprendidas y prácticas recomendadas

- El diseño de la estructura de UO no es un esfuerzo de una sola vez. A medida que una empresa aumenta la adopción de la nube y migra más cargas de trabajo a la zona de aterrizaje de AWS, su diseño de UO (e implícitamente su concepto de las políticas) también evolucionará de forma natural.
- No confunda las UO con carpetas; considérelas un destino para las políticas. Las UO y su jerarquía proporcionan el elemento estructurador de las Cuentas de AWS y siempre deben tratarse como contenedores de dichas políticas. Le recomendamos que coloque todas las Cuentas de AWS que requieran el mismo conjunto de políticas en la misma UO. Esta directriz también se aplica a las UO anidadas (las UO que están dentro de UO).

  Los entornos de AWS que necesitan una funcionalidad compartida de forma centralizada y capacidades de uso compartido de datos entre cargas de trabajo (que suelen encontrarse en las plataformas de datos empresariales) son más fáciles de acomodar en una estructura de UO que no se base en la clasificación de funciones según las líneas de negocio (LOB). Por ejemplo, en términos de políticas, en AWS Organizations no hay ninguna diferencia entre un entorno de producción para una aplicación de fabricación y un entorno de producción para una aplicación de análisis de ensayos clínicos.
- Respete y use la herencia. Cuando asocia una política a una UO específica, las Cuentas de AWS que están directamente en esa UO o cualquier UO secundaria heredan la política. Cuando se asocia una política a una Cuenta de AWS específica, la política solo afecta a esa Cuenta de AWS.

  El esfuerzo de migración de una estructura de UO a otra depende de la complejidad de configuración de las políticas actuales a nivel de UO o Cuenta de AWS. Otro factor importante es el grado de herencia de políticas que se utilizó en la jerarquía de UO actual o si se infringió la herencia. La complejidad de la migración aumenta con la implementación de rutas de herencia irregulares o que se desvían. Por ejemplo, si aplica políticas a cada Cuenta de AWS o hace excepciones frecuentes a las políticas (lo que pone interrumpe la herencia), migrar esas políticas a una nueva estructura requerirá un esfuerzo considerablemente mayor. En estos casos de alta complejidad, le recomendamos que dedique tiempo a revisar y rediseñar la herencia de políticas cuando planifique la migración.
- Preste atención tanto a las políticas de AWS Organizations como a los controles de AWS Control Tower. La estructura de UO se comparte entre AWS Control Tower y AWS Organizations. AWS Control Tower proporciona su propio conjunto de controles de prevención y detección. Estos

controles se aplican a nivel de Cuenta de AWS o de UO. AWS Organizations organiza las políticas a nivel de UO. En una migración de UO, se recomienda migrar primero las políticas de AWS Organizations, ya que estas tienen más peso para el cumplimiento. Se recomienda que aplique los controles de AWS Control Tower a la nueva estructura de UO en el segundo paso de la migración.

- La actualización de Cuentas de AWS lleva tiempo. Debe volver a inscribir las Cuentas de AWS existentes de forma individual en la nueva estructura de UO mediante AWS Control Tower. Esto lleva tiempo. Si tiene una gran cantidad de cuentas, le recomendamos que agilice este trabajo mediante la automatización para controlar y automatizar la ubicación de las Cuentas de AWS en las UO. A continuación, se muestran dos situaciones de ejemplo:
  - Cambio manual para una migración pequeña: el responsable de la migración reasigna cada Cuenta de AWS de la UO antigua a la nueva en la Consola de administración de AWS. Cuando se haya completado la reasignación de todas las Cuentas de AWS, el proceso de migración abrirá AWS Control Tower para cada Cuenta de AWS por separado o para todas las UO. Para volver a inscribir Cuentas de AWS en AWS Control Tower, se necesitan entre 10 y 15 minutos para cada Cuenta de AWS en función del número de Regiones de AWS que se usen en la cuenta. AWS Control Towerpermite ejecutar hasta cinco operaciones simultáneas de este tipo en paralelo.
  - Automatización de cambios personalizada: la automatización simplifica las tareas y ahorra esfuerzos. Por ejemplo, puede automatizar la administración del ciclo de vida de una Cuenta de AWS desde su creación hasta su migración y finalización. Puede usar el Generador de cuentas de AWS Control Tower para cambiar la asignación de una Cuenta de AWS a las UO y ejecutar el proceso de reinscripción. Esta automatización permite migrar cientos de Cuentas de AWS a gran escala.

Recursos

- AWS Organizations User Guide (documentación de AWS)
- AWS Organizations terminology and concepts (documentación de AWS)
- Service control policies (SCPs) (documentación de AWS)
- AWS Organizations API reference (documentación de AWS)
- AWS Control Tower User Guide (documentación de AWS)
- Introducing Landing Zone Accelerator for Healthcare (entrada en el blog de AWS)
- Managing the multi-account environment using AWS Organizations and AWS Control Tower (entrada en el blog de AWS)
- Best Practices for Organizational Units with AWS Organizations (entrada en el blog de AWS)
- AWS Security Reference Architecture (AWS SRA) (Recomendaciones de AWS)
- Establishing Your Cloud Foundation on AWS (documento técnico de AWS)
- Organizing Your AWS Environment Using Multiple Accounts (documento técnico de AWS)

Historial de documentos

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

Cambio	Descripción	Fecha
Publicación inicial	—	28 de marzo de 2023

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