Guía del usuario

AWS Control Tower

AWS Control Tower: Guía del usuario

Table of Contents

¿Qué es AWS Control Tower?

AWS Control Tower ofrece una forma sencilla de configurar y gobernar un entorno de AWS varias cuentas, siguiendo las prácticas recomendadas prescriptivas. AWS Control Tower organiza las capacidades de varios otros AWS servicios, como AWS Organizations AWS Service Catalog, y AWS IAM Identity Center, crear una landing zone en menos de una hora. Los recursos se configuran y administran en su nombre.

La orquestación de AWS Control Tower amplía las capacidades de AWS Organizations. Para evitar que sus organizaciones y sus cuentas se desvíen, lo que supone una divergencia con respecto a las prácticas recomendadas, AWS Control Tower aplica controles (a veces denominados barreras). Por ejemplo, puede utilizar los controles para garantizar que los registros de seguridad y los permisos de acceso entre cuentas necesarios se creen y no se modifiquen.

Si alojas más de un puñado de cuentas, es beneficioso contar con una capa de organización que facilite el despliegue y el gobierno de las cuentas. Puede adoptar AWS Control Tower como su principal forma de aprovisionar cuentas e infraestructura. Con AWS Control Tower, puede cumplir con mayor facilidad los estándares corporativos, cumplir los requisitos reglamentarios y seguir las prácticas recomendadas.

AWS Control Tower permite a los usuarios finales de sus equipos distribuidos aprovisionar nuevas AWS cuentas rápidamente mediante plantillas de cuentas configurables en Account Factory. Mientras tanto, los administradores centrales de la nube pueden supervisar que todas las cuentas estén alineadas con las políticas de conformidad establecidas en toda la empresa.

En resumen, AWS Control Tower ofrece la forma más sencilla de configurar y gestionar un AWS entorno seguro, compatible y con múltiples cuentas, basándose en las prácticas recomendadas establecidas al trabajar con miles de empresas. Para obtener más información sobre cómo trabajar con AWS Control Tower y las prácticas recomendadas descritas en la estrategia de AWS cuentas múltiples, consulteAWS estrategia multicuenta: guía de mejores prácticas.

Características

AWS Control Tower cuenta con las siguientes características:

- Zona de aterrizaje: una zona de aterrizaje es un entorno de múltiples cuentas bien diseñado que se basa en las mejores prácticas de seguridad y cumplimiento. Es el contenedor para toda la empresa que contiene todas tus unidades organizativas (OU), cuentas, usuarios y otros recursos

que deseas que estén sujetos a la normativa de conformidad. Una zona de inicio puede escalarse para adaptarse a las necesidades de una empresa de cualquier tamaño.

- Controles: un control (a veces denominado barrera) es una regla de alto nivel que proporciona un control continuo del entorno general. AWS Se expresa en lenguaje normal. Existen tres tipos de controles: preventivos, de detección y proactivos. Se aplican tres categorías de orientación a los controles: obligatorias, muy recomendables o optativas. Para obtener más información sobre controles, consulte Cómo funcionan los controles.
- Account Factory: An Account Factory es una plantilla de cuenta configurable que ayuda a estandarizar el aprovisionamiento de cuentas nuevas con configuraciones de cuentas previamente aprobadas. AWS Control Tower ofrece una Account Factory integrada que ayuda a automatizar el flujo de trabajo de aprovisionamiento de cuentas en su organización. Para obtener más información, consulte Aprovisione y administre cuentas con Account Factory.
- Panel de control: el panel ofrece una supervisión continua de tu landing zone a tu equipo de administradores de nube centrales. Utilice el panel de control para ver las cuentas aprovisionadas en toda la empresa, los controles habilitados para la aplicación de las políticas, los controles habilitados para la detección continua del incumplimiento de las políticas y los recursos no conformes organizados por cuentas y unidades organizativas.

Cómo interactúa AWS Control Tower con otros servicios AWS

AWS Control Tower se basa en AWS servicios confiables y confiables que incluyen AWS Service Catalog AWS IAM Identity Center, y AWS Organizations. Para obtener más información, consulte Servicios integrados.

Puede incorporar AWS Control Tower con otros AWS servicios en una solución que le ayude a migrar sus cargas de trabajo existentes a AWS. Para obtener más información, consulte Cómo aprovechar AWS Control Tower y CloudEndure migrar las cargas de trabajo a AWS.

Configuración, gobierno y extensibilidad

- Configuración automatizada de cuentas: AWS Control Tower automatiza la implementación y el registro de cuentas mediante una Account Factory (o «máquina expendedora»), que se crea como una abstracción sobre los productos aprovisionados. AWS Service CatalogAccount Factory puede crear e inscribir AWS cuentas, y automatiza el proceso de aplicar controles y políticas a esas cuentas.
- Gobierno centralizado: al emplear las capacidades de AWS Organizations, AWS Control Tower establece un marco que garantiza el cumplimiento y la gobernanza coherentes en todo su entorno

de múltiples cuentas. El AWS Organizations servicio proporciona capacidades esenciales para administrar un entorno de múltiples cuentas, incluidas la gobernanza y la administración centrales de las cuentas, la creación de cuentas a partir de AWS Organizations las API y las políticas de control de servicios (SCP).

- Extensibilidad: puede crear o ampliar su propio entorno de AWS Control Tower trabajando directamente en AWS Organizationsla consola de la Torre de Control de AWS o en ella. Puede ver los cambios reflejados en la Torre de Control de AWS después de registrar sus organizaciones actuales e inscribir sus cuentas existentes en la Torre de Control de AWS. Puede actualizar la zona de aterrizaje de AWS Control Tower para que refleje los cambios. Si sus cargas de trabajo requieren capacidades más avanzadas, puede aprovechar las soluciones de otros AWS socios junto con AWS Control Tower.

¿Es la primera vez que utiliza AWS Control Tower?

Si es un usuario nuevo de este servicio, le recomendamos que lea las siguientes secciones:

1. Si necesitas más información sobre cómo planificar y organizar tu landing zone, consulta Planifique la zona de aterrizaje de su AWS Control Tower yAWS estrategia de múltiples cuentas para su zona de aterrizaje de AWS Control Tower.
2. Si esta listo para crear su primer zona de inicio, consulte Introducción a AWS Control Tower.
3. Para obtener información acerca de la detección y prevención de desviaciones, consulte Detecte y resuelva desviaciones en la Torre de Control de AWS.
4. Para obtener más información sobre seguridad, consulte Seguridad en AWS Control Tower.
5. Para obtener información sobre cómo actualizar tu landing zone y tus cuentas de miembro, consultaAdministración de actualizaciones de configuración en AWS Control Tower.

Cómo funciona la Torre de Control de AWS

En esta sección se describe en detalle cómo funciona la Torre de Control de AWS. Tu landing zone es un entorno multicuenta bien diseñado para todos tus recursos. AWS Puede utilizar este entorno para hacer cumplir las normas de conformidad en todas sus cuentas. AWS

Estructura de una zona de aterrizaje de la Torre de Control de AWS

La estructura de una landing zone en la Torre de Control de AWS es la siguiente:

- Raíz: la matriz que contiene todas las demás unidades organizativas de tu landing zone.
- OU de seguridad: esta OU contiene el archivo de registros y las cuentas de auditoría. Estas cuentas suelen denominarse cuentas compartidas. Cuando lance su landing zone, podrá elegir nombres personalizados para estas cuentas compartidas y tendrá la opción de incorporar las AWS cuentas existentes a AWS Control Tower para garantizar la seguridad y el registro. Sin embargo, no se les puede cambiar el nombre más adelante y las cuentas existentes no se pueden añadir por motivos de seguridad y registro tras el lanzamiento inicial.
- Unidad organizativa Sandbox: la unidad organizativa Sandbox se crea cuando lanzas tu landing zone, si la activas. Esta y otras OU registradas contienen las cuentas inscritas con las que trabajan sus usuarios para realizar sus cargas de trabajo de AWS.
- Directorio del centro de identidad de IAM: en este directorio se encuentran los usuarios del centro de identidad de IAM. Define el alcance de los permisos de cada usuario del IAM Identity Center.
- Usuarios del IAM Identity Center: estas son las identidades que sus usuarios pueden asumir para realizar sus AWS cargas de trabajo en su landing zone.

Qué ocurre cuando configuras una landing zone

Cuando configura una landing zone, AWS Control Tower realiza las siguientes acciones en su cuenta de administración en su nombre:

- Crea dos unidades AWS Organizations organizativas (OU): Seguridad y Sandbox (opcional), incluidas en la estructura raíz de la organización.
- Crea o agrega dos cuentas compartidas en la unidad organizativa de seguridad: la cuenta Log Archive y la cuenta Audit.
- Crea un directorio nativo de la nube en el Centro de Identidad de IAM, con grupos preconfigurados y acceso de inicio de sesión único, si elige la configuración predeterminada de la Torre de Control de AWS, o si le permite administrar automáticamente su proveedor de identidades.
- Aplica todos los controles preventivos obligatorios para hacer cumplir las políticas.
- Aplica todos los controles de detección obligatorios para detectar infracciones de configuración.
- Los controles preventivos no se aplican a la cuenta de administración.

- A excepción de la cuenta de administración, los controles se aplican a la organización en su conjunto.

Gestión segura de los recursos dentro de la zona de aterrizaje y las cuentas de la Torre de Control de AWS

- Cuando creas tu landing zone, se crean varios AWS recursos. Para utilizar la Torre de Control de AWS, no debe modificar ni eliminar estos recursos gestionados por la Torre de Control de AWS fuera de los métodos compatibles que se describen en esta guía. Si eliminas o modificas estos recursos, tu landing zone pasará a un estado desconocido. Para obtener más información, consulte Guía para crear y modificar los recursos de la Torre de Control de AWS
- Cuando habilita los controles opcionales (aquellos con orientación altamente recomendada o electiva), AWS Control Tower crea AWS recursos que administra en sus cuentas. No modifique ni elimine los recursos creados por AWS Control Tower. Si lo hace, puede provocar que los controles pasen a un estado desconocido.

¿Qué son las cuentas compartidas?

En AWS Control Tower, las cuentas compartidas de su landing zone se aprovisionan durante la configuración: la cuenta de administración, la cuenta de archivo de registros y la cuenta de auditoría.

¿Qué es la cuenta de administración?

Esta es la cuenta que has creado específicamente para tu landing zone. Esta cuenta se utiliza para facturar todo lo que hay en tu landing zone. También se utiliza para el aprovisionamiento de cuentas en Account Factory, así como para gestionar las unidades organizativas y los controles.

> **Note**
>
> No se recomienda ejecutar ningún tipo de carga de trabajo de producción desde una cuenta de administración de AWS Control Tower. Cree una cuenta de AWS Control Tower independiente para ejecutar sus cargas de trabajo.

Para obtener más información, consulte Cuenta de administración.

¿Qué es la cuenta de archivo de registros?

Esta cuenta funciona como un repositorio de los registros de las actividades de la API y las configuraciones de recursos de todas las cuentas de la landing zone.

Para obtener más información, consulte Cuenta del archivo de registro.

¿Qué es la cuenta de auditoría?

La cuenta de auditoría es una cuenta restringida diseñada para que tus equipos de seguridad y cumplimiento tengan acceso de lectura y escritura a todas las cuentas de tu landing zone. Desde la cuenta de auditoría, tiene acceso mediante programación para revisar las cuentas, por medio de un rol que solo se concede a las funciones Lambda. La cuenta de auditoría no le permite iniciar sesión en otras cuentas manualmente. Para obtener más información sobre las funciones y roles de Lambda, consulte Configurar una función de Lambda para que asuma una función de otra. Cuenta de AWS

Para obtener más información, consulte Cuenta de auditoría.

Cómo funcionan los controles

Un control es una regla de alto nivel que proporciona un control continuo del AWS entorno general. Cada control aplica una sola regla y se expresa en un lenguaje sencillo. Puede cambiar los controles opcionales o muy recomendados que estén en vigor en cualquier momento desde la consola de la Torre de Control de AWS o desde las API de la Torre de Control de AWS. Los controles obligatorios se aplican siempre y no se pueden cambiar.

Los controles preventivos impiden que se lleven a cabo acciones. Por ejemplo, el control electivo denominado Disallow Changes to Bucket Policy for Amazon S3 Buckets (anteriormente denominado Disallow Policy Changes to Log Archive) impide cualquier cambio en la política de IAM en la cuenta compartida del archivo de registros. Se deniega cualquier intento de realizar una acción impedido y se inicia sesión. CloudTrail El recurso también ha iniciado sesión AWS Config.

Los controles de Detección detectan eventos específicos cuando se producen y registran la acciónCloudTrail. Por ejemplo, el control altamente recomendado denominado Detect if Enabled is Enabled for Amazon EBS Volumes Attached to Amazon EC2 Instances detecta si un volumen de Amazon EBS no cifrado está adjunto a una instancia EC2 de su landing zone.

Los controles proactivos comprueban si los recursos cumplen con las políticas y los objetivos de su empresa antes de aprovisionarlos en sus cuentas. Si los recursos no cumplen con las normas, no se

aprovisionan. Los controles proactivos supervisan los recursos que se desplegarían en sus cuentas mediante AWS CloudFormation plantillas.

Para aquellos que estén familiarizados con AWS: En AWS Control Tower, los controles preventivos se implementan mediante políticas de control de servicios (SCP). Los controles de Detective se implementan con AWS Config reglas. Los controles proactivos se implementan con AWS CloudFormation ganchos.

Temas relacionados

- Detecte y resuelva desviaciones en la Torre de Control de AWS

Cómo funciona AWS Control Tower con StackSets

AWS Control Tower se utiliza AWS CloudFormation StackSets para configurar los recursos en sus cuentas. Cada conjunto de pilas tiene StackInstances lo que corresponde a cuentas y a Regiones de AWS por cuenta. AWS Control Tower implementa una instancia de conjunto de pilas por cuenta y región.

AWS Control Tower aplica las actualizaciones a determinadas cuentas y de Regiones de AWS forma selectiva, en función de AWS CloudFormation los parámetros. Cuando las actualizaciones se aplican a algunas instancias de la pila, otras instancias de la pila pueden quedar en estado Outdated (Obsoleto). Este es el comportamiento esperado y normal.

Cuando una instancia de pila cambia al estado Outdated (Obsoleto), normalmente significa que la pila correspondiente a esa instancia de pila no está alineada con la última plantilla del conjunto de pilas. La pila permanece en la plantilla más antigua, por lo que es posible que no incluya los últimos recursos o parámetros. La pila sigue siendo completamente utilizable.

Este es un breve resumen del comportamiento que cabe esperar, en función de AWS CloudFormation los parámetros que se especifican durante una actualización:

Si la actualización del conjunto de pilas incluye cambios en la plantilla (es decir, si se especifican `TemplateURL` las propiedades `TemplateBody` o propiedades), o si se especifica la `Parameters` propiedad, AWS CloudFormation marca todas las instancias de la pila con el estado Anticuadas antes de actualizar las instancias de pila de las cuentas especificadas y Regiones de AWS. Si la actualización del conjunto de pilas no incluye cambios en la plantilla o los parámetros, AWS CloudFormation actualiza las instancias de pila de las cuentas y regiones especificadas y deja las

demás instancias de pila con el estado de instancia de pila existente. Para actualizar todas las instancias de pila asociadas a un conjunto de pilas, no especifique las propiedades `Accounts` ni `Regions`.

Para obtener más información, consulte Actualizar su conjunto de pilas en la Guía del AWS CloudFormation usuario.

Terminología

A continuación, se ofrece un breve resumen de algunos términos que aparecen en la documentación de la Torre de Control de AWS.

En primer lugar, es bueno saber que AWS Control Tower comparte gran parte de la terminología con el AWS Organizations servicio, incluidos los términos organización y unidad organizativa (OU), que aparecen en este documento.

- Para obtener más información sobre las organizaciones y las unidades organizativas, consulte AWS Organizations terminología y conceptos. Si es la primera vez que utiliza AWS Control Tower, esa terminología es un buen punto de partida.
- AWS Organizationses un AWS servicio que le ayuda a gestionar su entorno de forma centralizada a medida que crece y amplía sus cargas de AWS trabajo. AWS Control Tower se basa en la AWS Organizations creación de cuentas, la aplicación de controles preventivos a nivel de la unidad organizativa y la facturación centralizada.
- Una AWS cuenta Account Factory es una AWS cuenta aprovisionada mediante Account Factory en AWS Control Tower. A veces, Account Factory se denomina informalmente «máquina expendedora» de cuentas.
- La región de origen de la Torre de Control de AWS es la AWS región en la que se desplegó la zona de aterrizaje de la Torre de Control de AWS. Puedes ver tu región de origen en la configuración de tu landing zone.
- AWS Service Catalogle permite gestionar los servicios de TI más utilizados de forma centralizada. En el contexto de este documento, Account Factory utiliza AWS Service Catalog el aprovisionamiento de AWS cuentas nuevas, incluidas las cuentas de planos personalizados.
- AWS CloudFormation StackSetsson un tipo de recurso que amplía la funcionalidad de las pilas para que puedas crear, actualizar o eliminar pilas en varias cuentas y regiones con una sola operación y una sola plantilla. CloudFormation
- Una instancia de pila es una referencia a una pila de una cuenta de destino de una región.
- Una pila es un conjunto de AWS recursos que puedes gestionar como una sola unidad.
- Un agregador es un tipo de AWS Config recurso que recopila datos de AWS Config configuración y cumplimiento de varias cuentas y regiones de la organización, lo que le permite ver y consultar estos datos de cumplimiento en una sola cuenta.
- Un paquete de conformidad es un conjunto de AWS Config reglas y medidas correctivas que se pueden implementar como una sola entidad en una cuenta y una región, o en toda la organización.

AWS Organizations Puede usar un paquete de conformidad para ayudar a personalizar su entorno de AWS Control Tower. Para ver blogs técnicos que ofrecen más detalles, consulte la información relacionada.

- La base de AWS Control Tower es un grupo de recursos y configuraciones específicas que puede aplicar a un objetivo. El objetivo de referencia más común puede ser una unidad organizativa (OU). Por ejemplo, la línea base denominada `AWSControlTowerBaseline` está disponible para ayudarle a registrar sus unidades organizativas en AWS Control Tower. Durante la configuración y actualización de la zona de aterrizaje, el objetivo de referencia puede ser una cuenta compartida o una configuración específica para la zona de aterrizaje en su conjunto.
- Plano: un plano es un artefacto que encapsula algunos metadatos, que describen los componentes de la infraestructura que se implementan en una cuenta. Por ejemplo, una AWS CloudFormation plantilla puede servir como modelo para una cuenta de AWS Control Tower.
- Drift: cambio en un recurso instalado y configurado por AWS Control Tower. Los recursos sin desviaciones permiten que AWS Control Tower funcione correctamente.
- Recurso no conforme: recurso que infringe una AWS Config regla que define un control de detección concreto.
- Cuenta compartida: una de las tres cuentas que AWS Control Tower crea automáticamente al configurar la landing zone: la cuenta de administración, la cuenta de archivo de registros y la cuenta de auditoría. Durante la configuración, puede elegir nombres personalizados para la cuenta de archivo de registros y la cuenta de auditoría.
- Cuenta de miembro: una cuenta de miembro pertenece a la organización AWS Control Tower. La cuenta de miembro se puede inscribir o anular en AWS Control Tower. Cuando una unidad organizativa registrada contiene una combinación de cuentas inscritas y no inscritas:
  - Los controles preventivos habilitados en la OU se aplican a todas las cuentas incluidas en ella, incluidas las no inscritas. Esto es cierto porque los controles preventivos se aplican con los SCP a nivel de la unidad organizativa, no a nivel de la cuenta. Para obtener más información, consulte Herencia para conocer las políticas de control de servicios en la AWS Organizations documentación.
  - Los controles de Detective habilitados en la OU no se aplican a las cuentas no inscritas.

  Una cuenta solo puede ser miembro de una organización a la vez, y sus cargos se facturan a la cuenta de administración de esa organización. La cuenta de un miembro se puede mover al contenedor raíz de una organización.
- AWS cuenta: una AWS cuenta actúa como contenedor de recursos y límite de aislamiento de recursos. Se puede asociar una AWS cuenta a la facturación y al pago. Una AWS cuenta es

diferente de una cuenta de usuario (a veces denominada cuenta de usuario de IAM) en AWS Control Tower. Las cuentas creadas mediante el proceso de aprovisionamiento de Account Factory son AWS cuentas. AWS las cuentas también se pueden añadir a AWS Control Tower mediante el proceso de inscripción de cuentas o registro de unidades organizativas.

- Control: un control (también conocido como barandilla) es una regla de alto nivel que proporciona una gobernanza continua para el entorno general de la Torre de Control de AWS. Cada control aplica una única regla. Los controles preventivos se implementan con los SCP. Los controles de Detective se implementan con AWS Config reglas. Los controles proactivos se implementan con AWS CloudFormation ganchos. Para obtener más información, consulte Cómo funcionan los controles.
- Zona de aterrizaje: una zona de aterrizaje es un entorno de nube que ofrece un punto de partida recomendado, que incluye cuentas predeterminadas, estructura de cuentas, diseños de red y seguridad, etc. Desde una landing zone, puede implementar cargas de trabajo que utilicen sus soluciones y aplicaciones.
- OU anidada: una OU anidada en AWS Control Tower es una OU contenida dentro de otra OU. Una unidad organizativa anidada puede tener exactamente una unidad organizativa principal y cada cuenta puede ser miembro de exactamente una unidad organizativa. Las OU anidadas crean una jerarquía. Al adjuntar una política a una de las unidades organizativas de la jerarquía, esta fluye hacia abajo y afecta a todas las unidades organizativas y cuentas que se encuentran debajo de ella. Una jerarquía de unidades organizativas anidada en AWS Control Tower puede tener una profundidad máxima de cinco niveles.
- OU principal: la OU inmediatamente superior a la OU actual en la jerarquía. Cada unidad organizativa puede tener exactamente una unidad organizativa principal.
- OU secundaria: cualquier unidad organizativa inferior a la unidad organizativa actual en la jerarquía. Una unidad organizativa puede tener muchas unidades organizativas secundarias.
- Jerarquía de unidades organizativas: en AWS Control Tower, la jerarquía de las unidades organizativas anidadas puede tener hasta cinco niveles. El orden de anidación se denomina niveles. La parte superior de la jerarquía se designa como Nivel 1.
- OU de nivel superior: una OU de nivel superior es cualquier OU que se encuentre directamente debajo de la raíz, no de la raíz en sí. La raíz no se considera una OU.

Precios

No se aplica ningún cargo adicional por el uso de AWS Control Tower. Solo pagas por los AWS servicios habilitados por AWS Control Tower y los servicios que utilices en tu landing zone. Por ejemplo, pagas por Service Catalog por el aprovisionamiento de cuentas con Account Factory y AWS CloudTrail por los eventos rastreados en tu landing zone. Para obtener información sobre los precios y las tarifas asociados a la Torre de Control de AWS, consulte los precios de la Torre de Control de AWS.

Si ejecuta cargas de trabajo efímeras desde cuentas de AWS Control Tower, es posible que vea un aumento en los costos asociados a ellas. AWS ConfigConsulte Precios deAWS Config para obtener más información. Póngase en contacto con su representante de AWS cuentas para obtener información más específica sobre la administración de estos costos. Para obtener más información sobre cómo AWS Config funciona con AWS Control Tower, consulteSupervise los cambios en los recursos con AWS Config.

Si implementa AWS CloudTrail rutas fuera de la Torre de Control de AWS, puede utilizarlas con la Torre de Control de AWS. Sin embargo, puede incurrir en cargos duplicados si también opta por las rutas gestionadas por AWS Control Tower. No recomendamos instalar senderos externos, a menos que tenga un requisito específico. Si decide suscribirse durante la configuración o actualización de la zona de aterrizaje, AWS Control Tower configurará y activará un registro a nivel de organización para CloudTrail usted en la cuenta de administración. Para obtener información sobre la administración de CloudTrail los costos, consulte Administración CloudTrail de costos.

Configuración

Antes de usarla AWS Control Tower por primera vez, siga los pasos de esta sección para crear una AWS cuenta y proteger su cuenta AWS Control Tower de administración. Para obtener información sobre tareas de configuración adicionales específicas para AWS Control Tower, consulteIntroducción a AWS Control Tower.

Inscríbase en AWS

Cuando te registras en Amazon Web Services (AWS), tu AWS cuenta se registra automáticamente para todos los servicios de AWS, incluidos AWS Control Tower. Si ya tienes una AWS cuenta, pasa a la siguiente tarea. Si no tiene una AWS cuenta, utilice el siguiente procedimiento para crear una.

Anote su número de AWS cuenta, ya que lo necesitará para otras tareas.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

> **Seguridad para sus cuentas**
>
> Puedes encontrar orientación adicional sobre cómo configurar las mejores prácticas para proteger la seguridad de tus AWS Control Tower cuentas en la AWS Organizations documentación.
>
> - Prácticas recomendadas para la cuenta de administración
> - Mejores prácticas para las cuentas de los miembros

Siguiente paso

Introducción a AWS Control Tower

Introducción a AWS Control Tower

Este procedimiento de introducción está destinado a los administradores de la Torre de Control de AWS. Siga este procedimiento cuando esté listo para configurar su landing zone mediante la consola o las API de AWS Control Tower.

Si ya es AWS cliente de AWS Control Tower, pero es nuevo, le recomendamos que consulte la sección denominada Planifique la zona de aterrizaje de su AWS Control Tower antes de continuar.

Temas

Guía de inicio rápido de AWS Control Tower

Si es la primera vez que AWSutiliza AWS Control Tower, puede seguir los pasos de esta sección para empezar rápidamente a utilizar AWS Control Tower. Si prefiere personalizar su entorno de AWS Control Tower de forma inmediata, consulte Paso 2. Configura y lanza tu landing zone .

> **Note**
>
> AWS Control Tower configura servicios de pago AWS CloudTrail, como Amazon AWS ConfigCloudWatch, Amazon S3 y Amazon VPC. Cuando se utilizan, estos servicios pueden conllevar costes, tal y como se muestra en la página de precios. La consola AWS de administración muestra el uso de los servicios de pago y los costes incurridos. La propia Torre de Control de AWS no crea costes adicionales.

Antes de empezar

La decisión más importante que debe tomar antes de comenzar el proceso de configuración es elegir su región de origen. Su región de origen es la AWS región en la que ejecutará la mayoría de

sus cargas de trabajo o almacenará la mayoría de sus datos. No se puede cambiar después de configurar la zona de aterrizaje de la AWS Control Tower. Para obtener más información sobre cómo elegir una región de origen, consulte Consejos administrativos para la configuración de la landing zone .

> **Note**
>
> De forma predeterminada, AWS Control Tower elige la región en la que opera su cuenta actualmente como región de origen. Puede ver su región actual en la esquina superior derecha de la pantalla de la consola de AWS administración.

El procedimiento de inicio rápido supone que aceptará los valores predeterminados para los recursos de su entorno de AWS Control Tower. Muchas de estas opciones se pueden cambiar más adelante. En la sección denominada Expectativas para la configuración de la zona de aterrizaje .

Si ha creado una AWS cuenta nueva, cumplirá automáticamente los requisitos previos necesarios para configurar AWS Control Tower. Puede continuar con los pasos que se indican a continuación.

Pasos de inicio rápido

1. Inicie sesión en la consola AWS de administración con sus credenciales de usuario administrador.
2. Diríjase a la consola de la Torre de Control de AWS en https://console.aws.amazon.com/controltower.
3. Compruebe que trabaja en la región de origen que desee.
4. Selecciona Configurar landing zone.
5. Sigue las instrucciones de la consola y acepta todos los valores predeterminados. Deberá escribir la dirección de correo electrónico de su cuenta, una cuenta de archivo de registro y una cuenta de auditoría.
6. Confirma tus opciones y selecciona Configurar landing zone.
7. AWS Control Tower tarda unos 30 minutos en configurar todos los recursos de su landing zone.

Para obtener una versión más detallada de cómo configurar la Torre de Control de AWS, incluidas las formas de personalizar su entorno, lea y siga los procedimientos de los siguientes temas.

> **Note**
>
> Si es la primera vez que lo compra y tiene un problema de configuración, póngase en contacto con AWS Support para obtener ayuda con el diagnóstico.

Requisito previo: comprobaciones automatizadas previas al lanzamiento de su cuenta de administración

Antes de configurar la landing zone, AWS Control Tower ejecuta automáticamente una serie de comprobaciones previas al lanzamiento en su cuenta. No es necesario que realices ninguna acción para realizar estas comprobaciones, lo que garantiza que tu cuenta de gestión esté preparada para los cambios que establezcan tu landing zone. Estas son las comprobaciones que realiza AWS Control Tower antes de configurar una landing zone:

- Los límites de servicio existentes Cuenta de AWS deben ser suficientes para que AWS Control Tower pueda lanzarse. Para obtener más información, consulte Limitaciones y cuotas en la Torre de Control de AWS.
- Cuenta de AWS Debe estar suscrito a los siguientes AWS servicios:
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Config
  - AWS Identity and Access Management (YO SOY)
  - AWS Lambda

> **Note**
>
> De forma predeterminada, todas las cuentas están suscritas a estos servicios.

Consideraciones para los AWS IAM Identity Center clientes (IAM Identity Center)

- Si AWS IAM Identity Center (IAM Identity Center) ya está configurado, la región de origen de AWS Control Tower debe ser la misma que la región del IAM Identity Center.
- El IAM Identity Center solo se puede instalar en la cuenta de administración de una organización.
- Hay tres opciones disponibles para el directorio del centro de identidad de IAM, en función de la fuente de identidad que elija:
  - Almacén de usuarios del IAM Identity Center: si AWS Control Tower está configurada con el IAM Identity Center, AWS Control Tower crea grupos en el directorio del Centro de Identidad de IAM y proporciona acceso a estos grupos, para el usuario que seleccione, para las cuentas de los miembros.
  - Active Directory: si el Centro de Identidad de IAM para la Torre de Control de AWS está configurado con Active Directory, AWS Control Tower no administra el directorio del Centro de Identidad de IAM. No asigna usuarios ni grupos a cuentas nuevas AWS .
  - Proveedor de identidad externo: si el Centro de Identidad de IAM para la Torre de Control de AWS está configurado con un proveedor de identidad (IdP) externo, AWS Control Tower crea grupos en el directorio del Centro de Identidad de IAM y proporciona acceso a estos grupos para el usuario que seleccione para las cuentas de los miembros. Puede especificar un usuario existente de su IdP externo en Account Factory durante la creación de la cuenta, y AWS Control Tower le da a este usuario acceso a la cuenta recién vendida cuando sincroniza los usuarios del mismo nombre entre el IAM Identity Center y el IdP externo. También puede crear grupos en su IdP externo para que coincidan con los nombres de los grupos predeterminados de AWS Control Tower. Al asignar usuarios a estos grupos, estos usuarios tendrán acceso a sus cuentas inscritas.

  Para obtener más información sobre cómo trabajar con IAM Identity Center y AWS Control Tower, consulte Lo que debe saber sobre las cuentas del IAM Identity Center y AWS Control Tower

Consideraciones para los AWS Config clientes AWS CloudTrail

- Cuenta de AWS No pueden tener habilitado el acceso de confianza en la cuenta de administración de la organización para AWS Config o CloudTrail. Para obtener información sobre cómo deshabilitar el acceso de confianza, consulte la AWS Organizations documentación sobre cómo habilitar o deshabilitar el acceso de confianza.

- Si tiene una configuración de AWS Config grabadora, canal de entrega o agregación existente en alguna de las cuentas existentes que planea inscribir en AWS Control Tower, debe modificar o eliminar estas configuraciones antes de empezar a inscribir las cuentas, después de configurar su landing zone. Esta comprobación previa no se aplica a la cuenta de administración de la Torre de Control Tower de AWS durante el lanzamiento de la landing zone. Para obtener más información, consulte Inscribir cuentas que cuenten con AWS Config recursos existentes.
- Si ejecuta cargas de trabajo efímeras desde cuentas de AWS Control Tower, es posible que vea un aumento en los costos asociados a Config. AWS Póngase en contacto con su representante de AWS cuentas para obtener información más específica sobre la administración de estos costos.
- Cuando inscribe una cuenta en la Torre de Control de AWS, esta se rige por el AWS CloudTrail registro de la organización de la Torre de Control de AWS. Si ya tiene una implementación de CloudTrail seguimiento en la cuenta, es posible que vea cargos duplicados a menos que elimine la ruta existente de la cuenta antes de inscribirla en AWS Control Tower. Para obtener información sobre las rutas a nivel de organización y la Torre de Control de AWS, consulte. Precios

> **Note**
>
> Al lanzarse, los puntos de enlace del AWS Security Token Service (STS) deben estar activados en la cuenta de administración en todas las regiones gobernadas por la Torre de Control de AWS. De lo contrario, el lanzamiento puede fallar a mitad del proceso de configuración.

Cómo empezar a utilizar AWS Control Tower desde la consola

Este procedimiento de introducción está destinado a los administradores de la Torre de Control de AWS. Siga este procedimiento cuando esté listo para configurar su landing zone con la consola de AWS Control Tower. De principio a fin, debería tardar alrededor de media hora. Este procedimiento requiere algunos requisitos previos y tres pasos principales.

Si ya es AWS cliente de AWS Control Tower, pero es nuevo, le recomendamos que consulte la sección denominada Planifique la zona de aterrizaje de su AWS Control Tower antes de continuar.

Temas

- Paso 1: Cree las direcciones de correo electrónico de su cuenta compartida
- Expectativas para la configuración de la zona de aterrizaje

- Paso 2. Configura y lanza tu landing zone
- Paso 3. Revisa y configura la landing zone

Paso 1: Cree las direcciones de correo electrónico de su cuenta compartida

Si estás configurando tu landing zone en una nueva Cuenta de AWS, consultaConfiguración.

- Para configurar su landing zone con nuevas cuentas compartidas, AWS Control Tower necesita dos direcciones de correo electrónico únicas que aún no estén asociadas a una Cuenta de AWS. Cada una de estas direcciones de correo electrónico servirá como bandeja de entrada colaborativa (una cuenta de correo electrónico compartida) destinada a los distintos usuarios de su empresa que realizarán trabajos específicos relacionados con AWS Control Tower.
- Si está configurando la Torre de Control de AWS por primera vez y si va a incorporar las cuentas de seguridad y de archivo de registros existentes a la Torre de Control de AWS, puede introducir las direcciones de correo electrónico actuales de las AWS cuentas existentes.

Las direcciones de correo electrónico son obligatorias para:

- Cuenta de auditoría: esta cuenta es para su equipo de usuarios que necesitan acceder a la información de auditoría que proporciona AWS Control Tower. También puede utilizar esta cuenta como punto de acceso para herramientas de terceros que realicen auditorías mediante programación de su entorno para ayudar a auditar para fines de cumplimiento.
- Cuenta de archivo de registros: esta cuenta es para tu equipo de usuarios que necesitan acceder a toda la información de registro de todas tus cuentas inscritas en las unidades organizativas registradas en tu landing zone.

Estas cuentas se configuran en la unidad organizativa de seguridad cuando creas tu landing zone. Como práctica recomendada, le recomendamos que, al realizar acciones en estas cuentas, utilice un usuario del Centro de Identidad de IAM con los permisos correspondientes.

> **Note**
>
> Si especifica AWS las cuentas existentes como cuentas de auditoría y archivo de registros, las cuentas existentes deben pasar algunas comprobaciones previas al lanzamiento para garantizar que ningún recurso entre en conflicto con los requisitos de la Torre de Control de AWS. Si estas comprobaciones no se realizan correctamente, es posible que la configuración

de tu landing zone no se realice correctamente. En particular, las cuentas no deben tener AWS Config recursos existentes. Para obtener más información, consulte Consideraciones a la hora de incorporar las cuentas de seguridad o de registro existentes.

Para mayor claridad, en esta Guía del usuario siempre se hace referencia a las cuentas compartidas por sus nombres predeterminados: archivo de registro y auditoría. Al leer este documento, recuerde sustituirlos por los nombres personalizados que haya asignado a estas cuentas inicialmente, si decide personalizarlas. Puede ver sus cuentas con sus nombres personalizados en la página de detalles de la cuenta.

> **Note**
>
> Cambiaremos la terminología relativa a los nombres predeterminados de algunas unidades organizativas (OU) de la Torre de Control Tower de AWS para adaptarla a la estrategia de AWS cuentas múltiples. Es posible que observe algunas incoherencias durante la transición para mejorar la claridad de estos nombres. La unidad organizativa de seguridad se denominaba anteriormente Core OU. La unidad organizativa Sandbox se denominaba anteriormente unidad organizativa personalizada.

Expectativas para la configuración de la zona de aterrizaje

El proceso de configuración de la zona de aterrizaje de la AWS Control Tower consta de varios pasos. Algunos aspectos de la zona de aterrizaje de la AWS Control Tower son configurables. Las demás opciones no se pueden cambiar después de la configuración.

Elementos clave que se deben configurar durante la instalación

- Puedes seleccionar los nombres de las unidades organizativas de nivel superior durante la configuración y también puedes cambiar los nombres de las unidades organizativas después de configurar tu landing zone. De forma predeterminada, las unidades organizativas de nivel superior se denominan Security y Sandbox. Para obtener más información, consulte Directrices para configurar un entorno bien diseñado.
- Durante la configuración, puede seleccionar nombres personalizados para las cuentas compartidas que crea AWS Control Tower, denominadas archivo de registros y auditoría de forma predeterminada, pero no puede cambiar estos nombres después de la configuración. (Esta selección se realiza una sola vez).

- Durante la configuración, si lo desea, puede especificar AWS las cuentas existentes para que AWS Control Tower las utilice como cuentas de auditoría y archivo de registros. Si planea especificar AWS las cuentas existentes y si esas cuentas tienen AWS Config recursos existentes, debe eliminar los AWS Config recursos existentes antes de poder inscribirlas en AWS Control Tower. (Esta selección se realiza una sola vez).
- Si es la primera vez que realiza la configuración o si va a actualizar a la versión 3.0 de la zona de aterrizaje, puede elegir entre permitir que AWS Control Tower configure una AWS CloudTrail ruta a nivel de organización para su organización o puede optar por excluirse de las rutas gestionadas por AWS Control Tower y gestionar las suyas propias CloudTrail . Puede activar o desactivar las rutas a nivel de organización gestionadas por AWS Control Tower cada vez que actualice su landing zone.
- Si lo desea, puede configurar una política de retención personalizada para su depósito de registros y su depósito de acceso a registros de Amazon S3 al configurar o actualizar su landing zone.
- Si lo desea, puede especificar un plan previamente definido para utilizarlo en el aprovisionamiento de cuentas de miembros personalizadas desde la consola de la Torre de Control de AWS. Puede personalizar las cuentas más adelante si no tiene un plan disponible. Consulte Personaliza las cuentas con Account Factory Customization (AFC).

Opciones de configuración que no se pueden deshacer

- No puedes cambiar tu región de origen después de configurar tu landing zone.
- Si aprovisiona cuentas de Account Factory con VPC, los CIDR de VPC no se pueden cambiar una vez creados.

Paso 2. Configura y lanza tu landing zone

Antes de lanzar la zona de aterrizaje de la AWS Control Tower, determine la región de origen más adecuada. Para obtener más información, consulte Consejos administrativos para la configuración de la landing zone .

> **Important**
>
> Para cambiar la región de origen después de implementar la zona de aterrizaje de la AWS Control Tower, es necesario retirarla del servicio y contar con la asistencia de AWS Support. No se recomienda esta práctica.

Aprenda a configurar y lanzar su landing zone con la tecla AWS CLI inCómo empezar a utilizar AWS Control Tower mediante las API.

Para configurar e iniciar tu landing zone en la consola, lleva a cabo la siguiente serie de pasos.

Prepárese: diríjase a la consola de la Torre de Control de AWS

1. Abra un navegador web y diríjase a la consola de la Torre de Control de AWS en https://console.aws.amazon.com/controltower.
2. En la consola, compruebe que trabaja en la región de origen que desee para AWS Control Tower. A continuación, selecciona Configurar tu landing zone.

Paso 2a. Revise y seleccione sus AWS regiones

Asegúrese de haber designado correctamente la AWS región que ha seleccionado para su región de origen. Una vez implementada la Torre de Control de AWS, no podrá cambiar la región de origen.

En esta sección del proceso de configuración, puede añadir AWS las regiones adicionales que necesite. Puede añadir más regiones más adelante, si es necesario, y puede eliminar regiones de la gobernanza.

Para seleccionar AWS regiones adicionales para gobernarlas

1. El panel muestra las selecciones de regiones actuales. Abre el menú desplegable para ver una lista de regiones adicionales disponibles para la gobernanza.
2. Marque la casilla situada junto a cada región para incorporarla a la gobernanza de AWS Control Tower. La selección de su región de origen no se puede editar.

Para denegar el acceso a determinadas regiones

Para denegar el acceso a AWS los recursos y las cargas de trabajo en determinadas AWS regiones, seleccione Activado en la sección correspondiente a la región para denegar el control. De forma predeterminada, la configuración de este control es No habilitada.

Paso 2b. Configura tus unidades organizativas (OU)

Si aceptas los nombres predeterminados de estas unidades organizativas, no tendrás que realizar ninguna acción para que la configuración continúe. Para cambiar los nombres de las unidades organizativas, introduzca los nuevos nombres directamente en el campo del formulario.

- OU fundamental: AWS Control Tower se basa en una OU fundamental que inicialmente se denomina OU de seguridad. Puede cambiar el nombre de esta unidad organizativa durante la configuración inicial y, posteriormente, desde la página de detalles de la unidad organizativa. Esta unidad organizativa de seguridad contiene sus dos cuentas compartidas, que de forma predeterminada se denominan cuenta de archivo de registro y cuenta de auditoría.
- OU adicional: AWS Control Tower puede configurar una o más OU adicionales para usted. Te recomendamos que aprovisiones al menos una unidad organizativa adicional en tu landing zone, además de la unidad organizativa de seguridad. Si esta unidad organizativa adicional está destinada a proyectos de desarrollo, le recomendamos que la nombre unidad organizativa Sandbox, tal y como se indica en laDirectrices para configurar un entorno bien diseñado. Si ya tiene una OU existente en AWS Organizations, es posible que vea la opción de omitir la configuración de una OU adicional en AWS Control Tower.

Paso 2c. Configura tus cuentas compartidas, el registro y el cifrado

En esta sección del proceso de configuración, el panel muestra las selecciones predeterminadas para los nombres de las cuentas compartidas de AWS Control Tower. Estas cuentas son una parte esencial de tu landing zone. No muevas ni elimines estas cuentas compartidas. Puede elegir nombres personalizados para las cuentas de auditoría y archivado de registros durante la configuración. Como alternativa, tiene una opción única para especificar las AWS cuentas existentes como cuentas compartidas.

Debe proporcionar direcciones de correo electrónico únicas para sus cuentas de archivo de registro y de auditoría, y puede verificar la dirección de correo electrónico que proporcionó anteriormente para su cuenta de administración. Pulse el botón Editar para cambiar los valores predeterminados editables.

Acerca de las cuentas compartidas

- La cuenta de administración: la cuenta de administración de AWS Control Tower forma parte del nivel raíz. La cuenta de administración permite la facturación de AWS Control Tower. La cuenta también tiene permisos de administrador para tu landing zone. No puede crear cuentas independientes para la facturación y para los permisos de administrador en AWS Control Tower.

  La dirección de correo electrónico que se muestra para la cuenta de administración no se puede editar durante esta fase de la configuración. Se muestra como una confirmación, para que puedas comprobar que estás editando la cuenta de gestión correcta, en caso de que tengas varias cuentas.

- Las dos cuentas compartidas: puedes elegir nombres personalizados para estas dos cuentas o usar las tuyas propias, y debes proporcionar una dirección de correo electrónico única para cada cuenta, ya sea nueva o existente. Si decide que AWS Control Tower cree nuevas cuentas compartidas para usted, las direcciones de correo electrónico no deben tener ya AWS cuentas asociadas.

Para configurar las cuentas compartidas, complete la información solicitada.

1. En la consola, introduzca un nombre para la cuenta denominada inicialmente cuenta de archivo de registro. Muchos clientes deciden conservar el nombre predeterminado de esta cuenta.
2. Proporcione una dirección de correo electrónico única para esta cuenta.
3. Introduzca un nombre para la cuenta denominada inicialmente cuenta de auditoría. Muchos clientes optan por llamarla cuenta de seguridad.
4. Proporcione una dirección de correo electrónico única para esta cuenta.

Si lo desea, configure la retención de registros

Durante esta fase de configuración, puede personalizar la política de retención de registros para los buckets de Amazon S3 que almacenan sus AWS CloudTrail registros en la Torre de Control Tower de AWS, en incrementos de días o años, hasta un máximo de 15 años. Si decide no personalizar la retención de registros, la configuración predeterminada es de un año para el registro de cuentas estándar y 10 años para el registro de acceso. Esta función también está disponible cuando actualizas o restableces tu landing zone.

Opcionalmente, autogestione Cuenta de AWS el acceso

Puede seleccionar si AWS Control Tower configura el Cuenta de AWS acceso con AWS Identity and Access Management (IAM) o si desea autogestionarlo, Cuenta de AWS ya sea con usuarios, roles y permisos del AWS IAM Identity Center que puede configurar y personalizar por su cuenta, o con otro método, como un IdP externo, ya sea para la federación directa de cuentas o la federación de varias cuentas a través del IAM Identity Center. Puede cambiar esta selección más adelante.

De forma predeterminada, AWS Control Tower configura el centro de identidad de AWS IAM para su landing zone, de acuerdo con las recomendaciones de prácticas recomendadas definidas en Organizar su AWS entorno con varias cuentas. La mayoría de los clientes eligen la opción predeterminada. A veces se requieren métodos de acceso alternativos para cumplir con la normativa

en sectores o países específicos, o en aquellos Regiones de AWS lugares donde el Centro de Identidad de AWS IAM no esté disponible.

No se admite la selección de proveedores de identidad a nivel de cuenta. Esta opción solo se aplica a la zona de landing zone en su conjunto.

Para obtener más información, consulte Guía sobre el Centro de Identidad de IAM.

Opcionalmente, configure AWS CloudTrail los senderos

Como práctica recomendada, le recomendamos que configure el registro. Si desea permitir que AWS Control Tower configure un CloudTrail registro a nivel de organización y lo administre por usted, elija Optar por participar. Si desea gestionar el registro con sus propios CloudTrail senderos o con una herramienta de registro de terceros, elija Excluirse. Confirma tu selección cuando se te solicite hacerlo en la consola. Puedes cambiar tu selección e inscribirte o excluirte de las rutas a nivel de organización al actualizar tu landing zone.

Puedes configurar y gestionar tus propios CloudTrail senderos en cualquier momento, incluidos los senderos a nivel de organización y de cuenta. Si configuras CloudTrail rutas duplicadas, puedes incurrir en costes duplicados cuando se registren los eventos. CloudTrail

Opcionalmente, configure AWS KMS keys

Si desea cifrar y descifrar sus recursos con una clave de AWS KMS cifrado, seleccione la casilla de verificación. Si ya tienes claves, podrás seleccionarlas entre los identificadores que aparecen en un menú desplegable. Para generar una clave nueva, selecciona Crear una clave. Puedes añadir o cambiar una clave KMS cada vez que actualices tu landing zone.

Al seleccionar Configurar landing zone, AWS Control Tower realiza una comprobación previa para validar la clave de KMS. La clave debe cumplir los siguientes requisitos:

- Habilitado
- Simétrica
- No es una clave multirregional
- ¿Se han agregado los permisos correctos a la política
- La clave está en la cuenta de administración

Es posible que aparezca un mensaje de error si la clave no cumple estos requisitos. En ese caso, elija otra clave o genere una clave. Asegúrese de editar la política de permisos de la clave, tal y como se describe en la siguiente sección.

Actualice la política de claves de KMS

Para poder actualizar una política de claves de KMS, debe crear una clave de KMS. Para obtener más información, consulte Creating a key policy en la Guía del desarrollador de AWS Key Management Service .

Para usar una clave de KMS con AWS Control Tower, debe actualizar la política de claves de KMS predeterminada añadiendo los permisos mínimos necesarios para AWS Config y AWS CloudTrail. Como práctica recomendada, le recomendamos que incluya los permisos mínimos necesarios en cualquier política. Al actualizar una política de claves de KMS, puede añadir permisos como un grupo en una sola declaración JSON o línea por línea.

El procedimiento describe cómo actualizar la política de claves de KMS predeterminada en la AWS KMS consola mediante la adición de declaraciones de política que permitan el cifrado AWS Config y se utilicen CloudTrail AWS KMS para ello. Las declaraciones de política requieren que incluya la siguiente información:

- **`YOUR-MANAGEMENT-ACCOUNT-ID`**— el ID de la cuenta de administración en la que se configurará AWS Control Tower.
- **`YOUR-HOME-REGION`**— la región de origen que seleccionará al configurar la Torre de Control de AWS.
- **`YOUR-KMS-KEY-ID`**— el ID de clave de KMS que se utilizará con la política.

Para actualizar la política de claves de KMS

1. Abra la AWS KMS consola en https://console.aws.amazon.com/kms
2. En el panel de navegación, elija Claves administradas por el cliente.
3. En la tabla, seleccione la clave que desee editar.
4. En la pestaña Política clave, asegúrese de que puede ver la política clave. Si no puedes ver la política clave, selecciona Cambiar a la vista de políticas.
5. Selecciona Editar y actualiza la política clave de KMS predeterminada añadiendo las siguientes declaraciones de política para AWS Config y CloudTrail.

   AWS Config declaración de política

```
{
    "Sid": "Allow Config to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "config.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID"
}
```

CloudTrail declaración de política

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
        }
    }
}
```

6. Elija Guardar cambios.

Ejemplo de política clave de KMS

El siguiente ejemplo de política muestra el aspecto que tendría su política de claves de KMS después de agregar las declaraciones de política que otorgan AWS Config y CloudTrail los permisos mínimos requeridos. La política de ejemplo no incluye la política de claves de KMS predeterminada.

```
{
    "Version": "2012-10-17",
    "Id": "CustomKMSPolicy",
    "Statement": [
        {
        ... YOUR-EXISTING-POLICIES ...
        },
        {
            "Sid": "Allow Config to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
        },
        {
            "Sid": "Allow CloudTrail to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
              ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
```

```
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

Para ver otros ejemplos de políticas, consulta las páginas siguientes:

- Conceder permisos de cifrado en la Guía del AWS CloudTrail usuario.
- Los permisos necesarios para la clave KMS cuando se utiliza RoLess3 (Bucket Delivery) vinculado a un servicio (entrega de cubos) en la guía para desarrolladores.AWS Config

> **Protéjase contra los atacantes**
>
> Al añadir determinadas condiciones a sus políticas, puede ayudar a prevenir un tipo específico de ataque, conocido como ataque de agentes confusos, que se produce cuando una entidad coacciona a una entidad con más privilegios para que lleve a cabo una acción, como la suplantación de identidad entre servicios. Para obtener información general sobre las condiciones de la política, consulte también. Especificación de las condiciones de una política

El AWS Key Management Service (AWS KMS) le permite crear claves KMS multirregionales y claves asimétricas; sin embargo, AWS Control Tower no admite claves multirregionales ni claves asimétricas. AWS Control Tower realiza una comprobación previa de las claves existentes. Es posible que aparezca un mensaje de error si selecciona una clave multirregional o una clave asimétrica. En ese caso, genere otra clave para utilizarla con los recursos de la Torre de Control de AWS.

Para obtener más información al respecto AWS KMS, consulte la Guía para AWS KMS desarrolladores.

Tenga en cuenta que los datos de los clientes en la Torre de Control de AWS se cifran en reposo, de forma predeterminada, mediante SSE-S3.

Si lo desea, configure y cree cuentas de miembros personalizadas

Si sigue el flujo de trabajo Crear cuenta para añadir sus cuentas de miembro, puede especificar, si lo desea, un plan previamente definido para utilizarlo en el aprovisionamiento de cuentas de miembros personalizadas desde la consola de la Torre de Control de AWS. Puede personalizar las cuentas más adelante si no tiene un plan disponible. Consulte Personaliza las cuentas con Account Factory Customization (AFC).

Paso 3. Revisa y configura la landing zone

En la siguiente sección de la configuración, se muestran los permisos que AWS Control Tower requiere para su landing zone. Seleccione una casilla de verificación para ampliar cada tema. Se te pedirá que aceptes estos permisos, que pueden afectar a varias cuentas, y que aceptes las condiciones generales del servicio.

Para finalizar

1. En la consola, revisa los permisos del Servicio y, cuando estés listo, selecciona Comprendo los permisos que AWS Control Tower utilizará para administrar AWS los recursos y hacer cumplir las reglas en mi nombre.
2. Para finalizar tus selecciones e inicializar el lanzamiento, selecciona Configurar landing zone.

Esta serie de pasos inicia el proceso de configuración de tu landing zone, que puede tardar unos treinta minutos en completarse. Durante la configuración, AWS Control Tower crea el nivel raíz, la unidad organizativa de seguridad y las cuentas compartidas. Se crean, modifican o eliminan otros AWS recursos.

⚠ Confirme las suscripciones a SNS

La dirección de correo electrónico que proporcionó para la cuenta de auditoría recibirá correos electrónicos de AWS notificación y confirmación de suscripción de todas las AWS regiones admitidas por AWS Control Tower. Para recibir correos electrónicos de conformidad en su cuenta de auditoría, debe elegir el enlace Confirmar suscripción en cada correo electrónico de cada AWS región compatible con AWS Control Tower.

Cómo empezar a utilizar AWS Control Tower mediante las API

Este procedimiento de introducción está destinado a los administradores de la Torre de Control de AWS. Este procedimiento requiere algunos requisitos previos e incluye dos pasos principales.

En este procedimiento, utilizará las API de la Torre de Control de AWS y otros AWS servicios para configurar y lanzar una landing zone. Estas API le permiten crear un entorno de AWS Control Tower mediante programación, ya sea a través de la AWS CloudFormation consola o a través de AWS CLI.

Antes de lanzar la zona de aterrizaje de la AWS Control Tower, lleve a cabo estas tareas previas:

- Determine la región de origen más adecuada. Para obtener más información, consulte Consejos administrativos para la configuración de la landing zone .
- Revisa Requisito previo: comprobaciones automatizadas previas al lanzamiento de su cuenta de administración para obtener más información sobre las comprobaciones automáticas previas al lanzamiento que garantizan que tu cuenta de administración esté preparada para los cambios que establezcan tu landing zone.

Temas

Expectativas para la configuración de la zona de aterrizaje con API

El proceso de configuración de la zona de aterrizaje de la AWS Control Tower consta de varios pasos. Algunos aspectos de la zona de aterrizaje de la AWS Control Tower son configurables. Las demás opciones no se pueden cambiar después de la configuración.

Elementos clave que se deben configurar durante la instalación

- Puedes seleccionar los nombres de tus unidades organizativas fundamentales durante la configuración y también puedes cambiar los nombres de las unidades organizativas después de configurar tu landing zone. De forma predeterminada, las OU fundamentales se denominan Security y Sandbox. Para obtener más información, consulte Directrices para configurar un entorno bien diseñado.
- Durante la configuración, puede seleccionar nombres personalizados para las cuentas compartidas que crea AWS Control Tower, denominadas archivo de registros y auditoría de forma predeterminada, pero no puede cambiar estos nombres después de la configuración. (Esta selección se realiza una sola vez).
- Durante la configuración con las API, debe especificar AWS las cuentas existentes para que AWS Control Tower las utilice como cuentas de auditoría y archivo de registros. Para especificar AWS las cuentas existentes, si esas cuentas tienen AWS Config recursos existentes, debe eliminar o modificar los AWS Config recursos existentes antes de poder inscribir las cuentas en AWS Control Tower. (Esta selección se realiza una sola vez).
- Si es la primera vez que realiza la configuración o si va a actualizar a la versión 3.0 de la zona de aterrizaje, puede elegir entre permitir que AWS Control Tower configure una AWS CloudTrail ruta a nivel de organización para su organización o puede optar por excluirse de las rutas gestionadas por AWS Control Tower y gestionar las suyas propias CloudTrail . Puede activar o desactivar las rutas a nivel de organización gestionadas por AWS Control Tower cada vez que actualice su landing zone.
- Si lo desea, puede configurar una política de retención personalizada para su depósito de registros y su depósito de acceso a registros de Amazon S3 al configurar o actualizar su landing zone.

Opciones de configuración que no se pueden deshacer

- No puedes cambiar tu región de origen después de configurar tu landing zone.
- Si aprovisiona cuentas con VPC, los CIDR de VPC no se pueden cambiar una vez que se hayan creado.

En las siguientes secciones se detallan los requisitos previos y los pasos de la configuración, con explicaciones y advertencias. Para ver otros ejemplos de código, consulte Ejemplos: configurar una zona de aterrizaje de la Torre de Control de AWS solo con API.

Paso 1: Configura tu landing zone

El proceso de configuración de la zona de aterrizaje de la AWS Control Tower consta de varios pasos. Algunos aspectos de la zona de aterrizaje de la AWS Control Tower son configurables, pero otras opciones no se pueden cambiar después de la configuración. Para obtener más información sobre estas importantes consideraciones antes de lanzar tu landing zone, consulta Expectativas para la configuración de la zona de aterrizaje .

Antes de usar las API de zona de landing zone de AWS Control Tower, primero debe llamar a las API de otros AWS servicios para configurar la zona de aterrizaje antes del lanzamiento. El proceso incluye tres pasos principales:

- crear una nueva AWS Organizations organización,
- configurar las direcciones de correo electrónico de sus cuentas compartidas,
- y crear un rol de IAM o un usuario del IAM Identity Center con los permisos necesarios para llamar a las API de landing zone.

Paso 1. Crea la organización que contendrá tu landing zone:

1. Llame a la AWS Organizations `CreateOrganization` API y habilite todas las funciones para crear la OU fundamental. Inicialmente, AWS Control Tower lo denominó Security OU. Esta OU de seguridad contiene sus dos cuentas compartidas, que de forma predeterminada se denominan cuenta de archivo de registros y cuenta de auditoría.

   ```
   aws organizations create-organization --feature-set ALL
   ```

   AWS Control Tower puede configurar una o más unidades organizativas adicionales. Te recomendamos que aprovisiones al menos una unidad organizativa adicional en tu landing zone, además de la unidad organizativa de seguridad. Si esta OU adicional está destinada a proyectos de desarrollo, le recomendamos que la nombre OU Sandbox, tal y como se indica en laAWS estrategia de múltiples cuentas para su zona de aterrizaje de AWS Control Tower.

Paso 2. Aprovisione cuentas compartidas si es necesario:

Para configurar su landing zone, AWS Control Tower necesita dos direcciones de correo electrónico. Si utiliza las API de landing zone para configurar AWS Control Tower por primera vez, debe utilizar las AWS cuentas de seguridad y de archivo de registros existentes. Puede utilizar las direcciones de

correo electrónico actuales de las existentes Cuentas de AWS. Cada una de estas direcciones de correo electrónico servirá como bandeja de entrada colaborativa (una cuenta de correo electrónico compartida) destinada a los distintos usuarios de su empresa que realizarán trabajos específicos relacionados con AWS Control Tower.

Para empezar a configurar una nueva landing zone, si no tienes AWS cuentas existentes, puedes aprovisionar las cuentas de seguridad y archivar registros mediante AWS las AWS Organizations API.

1. Llame a la AWS Organizations `CreateAccount` API para crear la cuenta de archivo de registros y la cuenta de auditoría en la unidad organizativa de seguridad.

```
aws organizations create-account --email mylog@example.com --account-name "Logging
 Account"
```

```
aws organizations create-account --email mysecurity@example.com --account-name
 "Security Account"
```

2. (Opcional) Compruebe el estado de la `CreateAccount` operación mediante la AWS Organizations `DescribeAccount` API.

Paso 3. Cree las funciones de servicio requeridas

Cree las siguientes funciones de servicio de IAM que permitan a AWS Control Tower realizar las llamadas a la API necesarias para configurar su landing zone:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Para obtener más información sobre estas funciones y sus políticas, consulteUso de políticas basadas en identidad (políticas de IAM) para AWS Control Tower.

Para crear un rol de IAM:

1. Crea un rol de IAM con los permisos necesarios para llamar a todas las API de landing zone. Como alternativa, puede crear un usuario del centro de identidad de IAM y asignar los permisos necesarios.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Paso 2: Lanza tu landing zone

La `CreateLandingZone` API de AWS Control Tower requiere una versión de landing zone y un archivo de manifiesto como parámetros de entrada. Puede usar el archivo de manifiesto para configurar las siguientes funciones:

- Si lo desea, configure la retención de registros
- Opcionalmente, autogestione Cuenta de AWS el acceso
- Opcionalmente, configure AWS CloudTrail las rutas
- Opcionalmente, configure AWS KMS keys

Tras compilar tu archivo de manifiesto, estarás listo para crear una nueva landing zone.

> **Note**
>
> AWS Control Tower no admite la denegación de control por región cuando se utilizan las API para configurar y lanzar una landing zone. Tras lanzar correctamente su landing zone mediante las API, puede utilizar la consola de AWS Control Tower para configurar la región y denegar el control.

1. Llame a la `CreateLandingZone` API de la Torre de Control de AWS. Esta API requiere una versión de landing zone y un archivo de manifiesto como entrada.

   ```
   aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
   LandingZoneManifest.json"
   ```

   Ejemplo de manifiesto LandingZoneManifestde.json:

   ```
   {
      "governedRegions": ["us-west-2","us-west-1"],
      "organizationStructure": {
          "security": {
              "name": "CORE"
          },
   ```

```
        "sandbox": {
            "name": "Sandbox"
        }
    },
    "centralizedLogging": {
         "accountId": "222222222222",
         "configurations": {
             "loggingBucket": {
                 "retentionDays": 60
             },
             "accessLoggingBucket": {
                 "retentionDays": 60
             },
             "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
         },
         "enabled": true
    },
    "securityRoles": {
         "accountId": "333333333333"
    },
    "accessManagement": {
         "enabled": true
    }
}
```

> **Note**
>
> Como se muestra en el ejemplo, las SecurityRoles cuentas AccountIdpara CentralizedLogging y deben ser diferentes.

Salida:

```
{
   "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

2. Llama a la `GetLandingZoneOperation` API para comprobar el estado de la `CreateLandingZone` operación. La `GetLandingZoneOperation` API devuelve un estado de`SUCCEEDED`,`FAILED`, o`IN_PROGRESS`.

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-
eXXX-4XXX-aXXX-44XXXXXXXXXX"
```

Salida:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. Cuando el estado vuelva a ser`SUCCEEDED`, puedes llamar a la `GetLandingZone` API para revisar la configuración de la landing zone.

```
aws controltower get-landing-zone --landing-zone-identifier "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Salida:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
```

```
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "CORE"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

Identifica tu landing zone

Llamar `ListLandingZones` puede ayudarle a determinar si su cuenta ya está configurada con AWS Control Tower. Esta API devuelve un identificador de zona de aterrizaje (ARN) en cualquier región comercial, independientemente de la región de origen de la zona de aterrizaje. Los ARN de las zonas de aterrizaje son únicos a nivel regional.

```
aws controltower list-landing-zones --region us-east-1
```

Para las regiones de suscripción voluntaria, la `ListLandingZones` API solo devuelve el identificador de la zona de aterrizaje si llamas a la API en la misma región que la región de origen de la API. Por ejemplo, si tu zona de aterrizaje está configurada en af-south-1 y llamas a af-south-1, la API devuelve `ListLandingZones` el identificador de la zona de aterrizaje. Si tu zona de aterrizaje está configurada en af-south-1 y llamas **`ListLandingZones`** a ap-east-1, la API no devuelve el identificador de la zona de aterrizaje.

Salida:

```
{
   "landingZones" [
        "arn": "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
   ]
}
```

Actualiza tu landing zone

Cuando haya disponible una nueva versión de landing zone o para realizar otras actualizaciones en la configuración de tu zona de aterrizaje, puedes llamar a la `UpdateLandingZone` API y hacer referencia a un archivo de manifiesto actualizado. Esta API devuelve un`OperationIdentifier`, que luego puedes usar al llamar a la `GetLandingZoneOperation` API para comprobar el estado de la operación de actualización.

Para actualizar la landing zone

1. Llame a la `UpdateLandingZone` API de AWS Control Tower y consulte la versión actualizada de landing zone o su manifiesto actualizado.

   ```
   aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
   identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
    --manifest file://LandingZoneManifest.json
   ```

LandingZoneManifest.json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
```

```
            "name": "CORE"
        },
        "sandbox": {
            "name": "Sandbox"
        }
    },
    "centralizedLogging": {
         "accountId": "222222222222",
         "configurations": {
             "loggingBucket": {
                 "retentionDays":2555
             },
             "accessLoggingBucket": {
                 "retentionDays": 2555
             },
             "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
         },
         "enabled": true
    },
    "securityRoles": {
         "accountId": "333333333333"
    },
    "accessManagement": {
         "enabled": true
    }
}
```

Salida:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

Opcionalmente, vuelva a registrar OU para actualizar las cuentas

En el caso de las unidades organizativas de AWS Control Tower registradas con menos de 300 cuentas, puede utilizar la consola de AWS Control Tower, acceder a la página de unidades organizativas en el panel de control y seleccionar Volver a registrar la unidad organizativa para actualizar las cuentas de esa unidad organizativa.

Restablece la zona de aterrizaje para resolver la deriva

Cuando creas tu landing zone, la zona de aterrizaje y todas las unidades organizativas (OU), cuentas y recursos cumplen con las normas de gobierno aplicadas por los controles que hayas elegido. A medida que tú y los miembros de tu organización uséis la landing zone, es posible que se produzcan cambios en este estado de conformidad. Estos cambios se denominan deriva.

Para identificar si tu landing zone está a la deriva, puedes llamar a la `GetLandingZone` API. Esta API devuelve el estado de deriva de la zona de aterrizaje de `DRIFTED` o`IN_SYNC`.

Para resolver la deriva dentro de tu zona de aterrizaje, puedes usar la `ResetLandingZone` API para restablecer la configuración original de la zona de aterrizaje. Por ejemplo, AWS Control Tower habilita el Centro de Identidad de IAM de forma predeterminada para ayudarlo a administrar su Cuentas de AWS, pero si configura los parámetros originales de la zona de aterrizaje con el Centro de Identidad de IAM desactivado, las llamadas `ResetLandingZone` mantienen esa configuración deshabilitada del Centro de Identidad de IAM.

Solo puedes usar la `ResetLandingZone` API si utilizas la última versión disponible de landing zone. Puedes llamar a la `GetLandingZone` API y comparar tu versión de landing zone con la última versión disponible. Si es necesario, puedes hacer Actualiza tu landing zone que tu landing zone utilice la última versión disponible. En estos ejemplos, utilizamos la versión 3.3 como última versión.

1. Llame a la API de `GetLandingZone`. Si la API devuelve un estado de deriva de`DRIFTED`, tu landing zone está a la deriva.
2. Llama a la `ResetLandingZone` API para restablecer tu landing zone a su configuración original.

```
aws controltower reset-landing-zone --landing-zone-identifier
 "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Salida:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Note**
>
> El restablecimiento de la zona de aterrizaje no actualiza la versión de la zona de aterrizaje. Consulta Actualiza tu landing zone los detalles sobre la actualización de la versión de landing zone.

Retira tu landing zone

El proceso de limpiar todos los recursos de una zona de aterrizaje se denomina desmantelamiento de una zona de aterrizaje.

> **Important**
>
> Le recomendamos encarecidamente que realice este proceso de retirada solo si tiene intención de dejar de utilizar su zona de inicio. No es posible volver a crear la zona de inicio existente después de que la haya retirado.

Para obtener más información sobre el desmantelamiento de una landing zone, incluida información importante sobre cómo AWS Control Tower gestiona sus datos y los existentes AWS Organizations, consulteTutorial: Retirar del servicio una zona de aterrizaje de una Torre de Control de AWS.

Para desmantelar una landing zone, llama a la `DeleteLandingZone` API. Esta API devuelve un`OperationIdentifier`, que luego puedes usar al llamar a la `GetLandingZoneOperation` API para comprobar el estado de la operación de eliminación.

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

Salida:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

Ejemplos: configurar una zona de aterrizaje de la Torre de Control de AWS solo con API

Este tutorial de ejemplos es un documento complementario. Para obtener explicaciones, advertencias y más información, consulte Introducción a AWS Control Tower mediante las API.

Requisitos previos

Antes de crear una zona de aterrizaje de AWS Control Tower, debe crear una organización, dos cuentas compartidas y algunas funciones de IAM. Este tutorial detallado incluye estos pasos, con ejemplos de comandos y resultados de CLI.

Paso 1. Cree la organización y las dos cuentas necesarias.

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
 archive account"
aws organizations create-account --email example+aud@example.com --account-name "Audit
 account"
```

Paso 2. Cree las funciones de IAM necesarias.

`AWSControlTowerAdmin`

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://controltower_trust.json
```

```
cat <<EOF >ct_admin_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
 AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy
```

AWSControlTowerCloudTrailRole

```
cat <<EOF >controltower_trust.json
        {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
```

```
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --
assume-role-policy-document file://cloudformation_trust.json
cat <<EOF >stackset_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
```

```
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name
 AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

Paso 3. Obtén los ID de las cuentas y genera el archivo de manifiesto de la zona de aterrizaje.

Los dos primeros comandos del siguiente ejemplo almacenan los ID de cuenta de las cuentas que creó en el paso 1 en variables. A continuación, estas variables ayudan a generar el archivo de manifiesto de la zona de aterrizaje.

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
```

```
   "governedRegions": ["us-west-1", "us-west-2"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "$log_account_id",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            }
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "$sec_account_id"
   },
   "accessManagement": {
        "enabled": true
   }
}
EOF
```

Paso 4. Crea la landing zone con la última versión.

Debes configurar la landing zone con el archivo de manifiesto y la última versión. En este ejemplo se muestra la versión 3.3.

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

El resultado contendrá un arn y un OperationIdentifier, como se muestra en el siguiente ejemplo.

```
{
    "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
```

```
}
```

Paso 5. (Opcional) Realiza un seguimiento del estado de la operación de creación de tu landing zone.

Para realizar un seguimiento del estado, utilice el OperationIdentifier del resultado del comando anterior`create-landing-zone`.

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

Ejemplo de salida de estado:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "2024-02-28T21:49:31Z",
        "status": "IN_PROGRESS"
    }
}
```

Puede usar el siguiente script de ejemplo como ayuda para configurar un bucle, que informa del estado de la operación una y otra vez, como un archivo de registro. De este modo, no es necesario que siga introduciendo el comando.

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

Para mostrar información detallada sobre tu landing zone

Paso 1. Encuentra el ARN de la landing zone

```
aws --region us-west-1 controltower list-landing-zones
```

La salida incluirá el identificador de la landing zone, como se muestra en el siguiente ejemplo de salida.

```
{
```

```
    "landingZones": [
        {
            "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

Paso 2. Obtenga la información

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
 arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX
```

Este es un ejemplo del tipo de resultado que puede ver:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "9750XXXX4444"
            },
            "governedRegions": [
                "us-west-1",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
```

```
                "accountId": "012345678901",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "ACTIVE",
        "version": "3.3"
    }
}
```

Lanzar una landing zone usando AWS CloudFormation

Puedes configurar e iniciar una landing zone a AWS CloudFormation través de la AWS CloudFormation consola o a través del AWS CLI. En esta sección se proporcionan instrucciones y ejemplos para lanzar una landing zone mediante API AWS CloudFormation.

Temas

- Requisitos previos para lanzar una landing zone utilizando AWS CloudFormation
- Crea una nueva landing zone usando AWS CloudFormation
- Gestiona una landing zone existente usando AWS CloudFormation

Requisitos previos para lanzar una landing zone utilizando AWS CloudFormation

1. Desde allí AWS CLI, utilice la AWS Organizations `CreateOrganization` API para crear una organización y habilitar todas las funciones.

   Para obtener instrucciones más detalladas, consulte Paso 1: Configura tu landing zone .
2. Desde la AWS CloudFormation consola o mediante la AWS CLI, implemente una AWS CloudFormation plantilla que cree los siguientes recursos en la cuenta de administración:
   - Cuenta Log Archive (a veces denominada cuenta «Logging»)
   - Cuenta de auditoría (a veces denominada cuenta de «Seguridad»)

- Las funciones AWSControlTowerAdminAWSControlTowerCloudTrailRole, AWSControlTowerConfigAggregatorRoleForOrganizations, y AWSControlTowerStackSetRolede servicio.

  Para obtener información sobre cómo AWS Control Tower utiliza estas funciones para realizar llamadas a la API de landing zone, consulte el paso 1: Configure your landing zone.

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
    Type: String
    Description: Name for centralized logging account
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
```

```
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudtrail.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerCloudTrailRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerCloudTrailRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action:
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
            Resource: !Sub >-
```

```
              arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerCloudTrailRole
  AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: config.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
  AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerStackSetRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerStackSetRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action: 'sts:AssumeRole'
            Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
            Effect: Allow
      Roles:
```

```
        - !Ref AWSControlTowerStackSetRole

Outputs:
  LogAccountId:
    Value:
      Fn::GetAtt: LoggingAccount.AccountId
    Export:
      Name: LogAccountId
  SecurityAccountId:
    Value:
      Fn::GetAtt: SecurityAccount.AccountId
    Export:
      Name: SecurityAccountId
```

Crea una nueva landing zone usando AWS CloudFormation

Desde la AWS CloudFormation consola o mediante el AWS CLI, despliega la siguiente AWS CloudFormation plantilla para crear una landing zone.

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
```

```
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
            name:
              Ref: SecurityOuName
          sandbox:
            name:
              Ref: SandboxOuName
        centralizedLogging:
          accountId:
            Ref: CentralizedLoggingAccountId
          configurations:
            loggingBucket:
              retentionDays:
                Ref: LoggingBucketRetentionPeriod
            accessLoggingBucket:
              retentionDays:
                Ref: AccessLoggingBucketRetentionPeriod
            kmsKeyArn:
              Ref: KMSKey
          enabled: true
        securityRoles:
          accountId:
            Ref: SecurityAccountId
        accessManagement:
```

```
          enabled: true
```

Gestiona una landing zone existente usando AWS CloudFormation

Puedes utilizarla AWS CloudFormation para gestionar una zona de aterrizaje que ya hayas lanzado importándola a una AWS CloudFormation pila nueva o existente. Consulta Cómo CloudFormation gestionar los recursos existentes para obtener más información e instrucciones.

Para detectar y resolver la desviación en una zona de aterrizaje, puede utilizar la consola de AWS Control Tower AWS CLI, la o la `ResetLandingZone`API.

Siguientes pasos

Ahora que tu landing zone está configurada, está lista para usarse.

Para obtener más información sobre cómo utilizar AWS Control Tower, consulte los siguientes temas:

- Para conocer las prácticas administrativas recomendadas, consulte Prácticas recomendadas.
- Puede configurar los usuarios y grupos del IAM Identity Center con funciones y permisos específicos. Para obtener recomendaciones, consulte Recomendaciones para configurar grupos, funciones y políticas .
- Para empezar a inscribir organizaciones y cuentas desde sus AWS Organizations despliegues, consulte Gestionar las organizaciones y cuentas existentes.
- Tus usuarios finales pueden aprovisionar sus propias AWS cuentas en tu landing zone mediante Account Factory. Para obtener más información, consulte Permisos para configurar y aprovisionar cuentas.
- Para elloValidación de conformidad para AWS Control Tower, los administradores de la nube central pueden revisar los archivos de registro de la cuenta de Log Archive, y los auditores externos designados pueden revisar la información de auditoría en la cuenta de auditoría (compartida), que forma parte de la OU de seguridad.
- Para obtener más información sobre las capacidades de AWS Control Tower, consulte la información relacionada.
- Intente visitar una lista seleccionada de YouTube vídeos que explican más sobre cómo utilizar la funcionalidad de la Torre de Control de AWS.
- De vez en cuando, es posible que tengas que actualizar tu landing zone para obtener las últimas actualizaciones de backend, los últimos controles y conservar tu landing zone up-to-date. Para

obtener más información, consulte Administración de actualizaciones de configuración en AWS Control Tower.

- Si tiene problemas al usar AWS Control Tower, consulteResolución de problemas.

> **Important**
>
> Si aún no has activado el MFA para el usuario root de tu cuenta, hazlo ahora. Para obtener más información sobre las prácticas recomendadas para el usuario root, consulte Prácticas recomendadas para proteger al usuario root de su cuenta.

Limitaciones y cuotas en la Torre de Control de AWS

En este capítulo se AWS describen las limitaciones y cuotas del servicio que debe tener en cuenta al utilizar AWS Control Tower. Si no puedes configurar tu landing zone debido a un problema de cuota de servicio, ponte en contacto con nosotros AWS Support.

Para obtener más información sobre las limitaciones específicas de los controles, consulteLimitaciones de control.

> **Una nueva guía de referencia de controles**
>
> La información sobre los controles de la Torre de Control de AWS se ha trasladado a la Guía de referencia de controles de la Torre de Control de AWS.

Limitaciones de AWS Control Tower

En esta sección se describen las limitaciones conocidas y los casos de uso no admitidos en AWS Control Tower.

- AWS Control Tower tiene limitaciones generales de simultaneidad. En general, se permite realizar una operación a la vez. Se permiten dos excepciones a esta limitación:
  - Los controles opcionales se pueden activar y desactivar simultáneamente, mediante un proceso asíncrono. Pueden estar en curso hasta cien (100) operaciones relacionadas con el control a la vez, en total, sin importar si se realizan desde la consola o desde una API. De estas 100 operaciones, hasta 20 a la vez pueden ser operaciones de control proactivo.
  - Las cuentas se pueden aprovisionar, actualizar e inscribir simultáneamente en Account Factory, mediante un proceso asíncrono, con hasta cinco (5) operaciones relacionadas con la cuenta en curso simultáneamente. La desadministración de las cuentas se debe realizar de una en una.
- Se pueden cambiar las direcciones de correo electrónico de las cuentas compartidas de la OU de seguridad, pero debe actualizar su landing zone para ver estos cambios en la consola de AWS Control Tower.
- Se aplica un límite de cinco (5) SCP por OU a las OU de su zona de aterrizaje de AWS Control Tower.
- AWS Control Tower admite hasta 10 000 cuentas en la organización de su zona de destino, divididas entre todas sus unidades organizativas.

- Las unidades organizativas existentes con más de 300 cuentas directamente anidadas no se pueden registrar ni volver a registrar en AWS Control Tower. Para obtener más información sobre las limitaciones del registro de unidades organizativas, consulte. Las regiones y la pila establecen limitaciones
- Las personalizaciones de AWS Control Tower (cFCT) no están disponibles en estos sitios Regiones de AWS porque algunas dependencias no están disponibles:
  - Asia-Pacífico (Yakarta y Osaka)
  - Israel (Tel Aviv)
  - Medio Oriente (EAU)
  - Europa (España)
  - Asia-Pacífico (Hyderabad)
  - Europa (Zúrich)
  - Oeste de Canadá (Calgary)

  Puede implementar y administrar recursos en estas regiones con cFCT si implementa cFCT en su región de origen de AWS Control Tower, pero no puede crear cFCT en estas regiones.
- AWS Control Tower Account Factory for Terraform (AFT) no está disponible en las siguientes Regiones de AWS ubicaciones porque algunas dependencias no están disponibles:
  - Israel (Tel Aviv)
  - Medio Oriente (EAU)
  - Europa (España)
  - Asia-Pacífico (Hyderabad)
  - Europa (Zúrich)
  - Oeste de Canadá (Calgary)
- Las siguientes regiones no admiten el IAM Identity Center.
  - Región de Oriente Medio (EAU), me-central-1
  - Región Asia Pacífico (Hyderabad), ap-south-2
  - Canadá oeste (Calgary), ca-west-1

  Para obtener más información Regiones de AWS y soporte para IAM Identity Center, consulte Regiones y puntos finales en la Guía del usuario de AWS Identity and Access Management.
- Las siguientes regiones no son compatibles. AWS Service Catalog
  - Canadá oeste (Calgary), ca-west-1

Para obtener más información sobre la funcionalidad de la Torre de Control de AWS en las regiones que no son compatibles AWS Service Catalog, consulteLa Torre de Control de AWS está disponible en el oeste de AWS Canadá (Calgary).

- Al llamar a una API de control para activar o desactivar un control, el límite `EnableControl` y `DisableControl` las actualizaciones en AWS Control Tower son de cien (100) operaciones simultáneas. Pueden estar en curso diez operaciones (10) de forma simultánea, con las operaciones restantes en cola. Es posible que tengas que ajustar el código para esperar a que se complete.
- Dentro del límite general de 100 operaciones de control, hasta 20 operaciones a la vez pueden ser operaciones de control proactivas.
- Cuando aprovisionas cuentas a través de Account Factory Customizations (AFC), con planos basados en Terraform, puedes implementar esos planos solo en uno. Región de AWS De forma predeterminada, AWS Control Tower se implementa en la región de origen.

Solicitud de un aumento de cuota

La consola Service Quotas proporciona información sobre las cuotas de la Torre de Control de AWS. Puede utilizar la consola Service Quotas para consultar las cuotas de servicio predeterminadas o para solicitar aumentos de cuota para las cuotas ajustables.

Las siguientes cuotas se pueden ver a través de la consola Service Quotas:

- Cuota de operaciones de cuentas simultáneas: el número máximo de operaciones de cuentas simultáneas que se pueden realizar al mismo tiempo. Predeterminado: 5, máximo: 10, ajustable
- Número de cuentas en una sola unidad organizativa: la cantidad máxima de cuentas administradas por AWS Control Tower que pueden estar presentes en una unidad organizativa. Si añade cuentas que superen este límite, no se podrá realizar el proceso de registro de la OU en AWS Control Tower. Para obtener más información sobre el número de cuentas por unidad organizativa, consulte Las regiones y la pila establecen limitaciones la documentación de AWS Control Tower. Predeterminado: 300, no ajustable.
- Operaciones simultáneas para unidades organizativas (OU): número máximo de operaciones simultáneas relacionadas con la OU que se pueden realizar al mismo tiempo. Predeterminado: 1, no ajustable.

Por ejemplo, puede solicitar un aumento de la cuota de cinco a diez operaciones simultáneas relacionadas con la cuenta. Algunas características de rendimiento de AWS Control Tower pueden cambiar tras un aumento de cuota. Por ejemplo, la actualización de una unidad organizativa puede tardar más tiempo si tiene más cuentas en ella. O bien, puede llevar más tiempo completar una acción en una OU con cinco SCP que con tres SCP.

> **Note**
>
> Es posible que una solicitud de aumento de la cuota de servicio tarde hasta dos días en surtir efecto. Asegúrese de solicitar el aumento de cuota desde su región de origen de la Torre de Control de AWS.

Como alternativa, puede ponerse en contacto con AWS Support para solicitar un aumento de la cuota de algunos recursos de AWS Control Tower. O bien, puede ver el siguiente vídeo y aprender a automatizar determinados aumentos de las cuotas de servicio.

Vídeo: Automatice las solicitudes de aumento de la cuota de servicio en los servicios relacionados con AWS Control Tower

Este vídeo (7:24) describe cómo automatizar los aumentos de las cuotas de servicio para los AWS servicios relacionados e integrados, en función de las implementaciones en la Torre de Control de AWS. También muestra cómo automatizar la inscripción de nuevas cuentas en el soporte AWS empresarial de su organización. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo sobre el aumento de las cuotas en la Torre de Control de AWS.

Al aprovisionar nuevas cuentas en este entorno, puede utilizar los eventos del ciclo de vida para activar solicitudes automatizadas de aumento de la cuota de servicio según se especifique. Regiones de AWS

Encontrará más información sobre AWS las cuotas en la Referencia AWS general.

Limitaciones de control

> **Una nueva guía de referencia de controles**
>
> La información sobre los controles de la Torre de Control de AWS se ha trasladado a la Guía de referencia de controles de la Torre de Control de AWS.

Si modifica los recursos de la Torre de Control de AWS, como un SCP, o elimina algún AWS Config recurso, como un grabador o un agregador de Config, la Torre de Control de AWS ya no puede garantizar que los controles funcionen según lo diseñado. Por lo tanto, la seguridad de su entorno de múltiples cuentas puede verse comprometida. El modelo de seguridad de responsabilidad AWS compartida se aplica a todos los cambios que realice.

> **Note**
>
> AWS Control Tower ayuda a mantener la integridad de su entorno al restablecer los SCP de los controles a su configuración estándar al actualizar su landing zone. Los cambios que haya realizado en los SCP se sustituyen por la versión estándar del control, por diseño.

Algunos controles de la Torre de Control de AWS no funcionan en algunos Regiones de AWS lugares donde está disponible la Torre de Control de AWS, porque esas regiones no admiten la funcionalidad subyacente requerida. Esta limitación afecta a determinados controles de detección, a determinados controles proactivos y a determinados controles del estándar gestionado por el Servicio Security Hub: AWS Control Tower. Para obtener más información sobre la disponibilidad regional, consulte la documentación de la lista de servicios regionales y la documentación de referencia de controles del Security Hub.

El comportamiento de control también está limitado en el caso de una gobernanza mixta. Para obtener más información, consulte Evite la gobernanza mixta al configurar las regiones.

Para obtener más información sobre cómo AWS Control Tower gestiona las limitaciones de las regiones y los controles, consulteConsideraciones a la hora de activar las regiones con AWS suscripción.

Puede ver las regiones de cada control en la consola de la Torre de Control de AWS.

Las siguientes AWS regiones no admiten controles que formen parte del estándar gestionado por el Servicio Security Hub: AWS Control Tower.

- Región de Asia Pacífico (Hong Kong), ap-east-1
- Región de Asia Pacífico (Yakarta), ap-southeast-3
- Región de Asia Pacífico (Osaka), ap-northeast-3
- Región Europa (Milán), eu-south-1
- Región de África (Ciudad del Cabo), af-south-1
- Región de Medio Oriente (Bahréin), me-south-1
- Israel (Tel Aviv), il-central-1
- Región de Oriente Medio (EAU), me-central-1
- Región Europa (España), eu-south-2
- Región Asia Pacífico (Hyderabad), ap-south-2
- Región Europa (Zúrich), eu-central-2
- Región Asia Pacífico (Melbourne), ap-southeast-4
- Canadá oeste (Calgary), ca-west-1

Lo siguiente Regiones de AWS no es compatible con los controles proactivos.

- Oeste de Canadá (Calgary)

La siguiente tabla muestra los controles proactivos que no son compatibles en algunos casos Regiones de AWS.

Identificador de control	Regiones no compatibles
`CT.REDSHIFT.PR.5`	ap-southeast-4, ap-south-2, ap-southeast-3, eu-central-2, eu-sur-2, il-central-1, me-central-1
`CT.DAX.PR.2`	us-west-1
`CT.GLUE.PR.2`	No se admite

En la siguiente tabla se muestran los controles de detección de AWS Control Tower que no son compatibles en algunos casos Regiones de AWS.

Identificador de control	Regiones no compatibles
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3, ap-southeast-3, il-central-1, ap-southeast-4, ca-west-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	ap-northeast-3, ap-southeast-3, af-south-1, eu-sur-1, il-central-1, me-central-1, eu-sur-2, ap-south-2, eu-central-2, ap-south-2, eu-central-2, ap-southeast-4 ast-4, ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3, ap-southeast-3, ap-south-2, eu-south-2, ca-west-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	ap-northeast-3, ap-southeast-3, af-south-1, eu-sur-1, il-central-1, me-central-1, eu-sur-2, ap-south-2, eu-central-2, ap-south-2, eu-central-2, ap-southeast-4 ast-4, ca-west-1
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ap-northeast-3, ap-southeast-3, af-south-1, eu-south-1, us-west-1, il-central-1, me-central-1, me-central-1, eu-sur-2, ap-south-2, eu-central-2, ap-south-2 ap-southeast-4, ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-southeast-3, il-central-1, eu-sur-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_RESTRICTED_SSH	af-south-1, ap-northeast-3, ap-sur-2, ap-southeast-3, ap-southeast-4, eu-central-2, eu-sur-1,

Identificador de control	Regiones no compatibles
	eu-sur-2, eu-sur-2, il-central-1, me-central-1 al-1
AWS-GR_DMS_REPLICATION_NOT_ PUBLIC	af-south-1, ap-south-2, ap-southeast-3, ap-southeast-4, eu-central-2, eu-sur-1, eu-sur-2, il-central-1, me-central-1, ca-west-1
AWS-GR_RDS_SNAPSHOTS_PUBLIC _PROHIBITED	af-south-1, ap-southeast-4, eu-central-2, eu-sur-1, eu-south-2, il-central-1
AWS-GR_SUBNET_AUTO_ASSIGN_P UBLIC_IP_DISABLED	ap-northeast-3
AWS-GR_ENCRYPTED_VOLUMES	af-south-1, ap-northeast-3, eu-south-1, il-central-1
AWS-GR_RESTRICTED_COMMON_PORTS	af-south-1, ap-northeast-3, eu-central-2, eu-sur-1, eu-sur-2, il-central-1, me-central-1
AWS-GR_IAM_USER_MFA_ENABLED	il-central-1, me-central-1, eu-sur-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_MFA_ENABLED_FOR_IAM_ CONSOLE_ACCESS	il-central-1, me-central-1, eu-sur-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	il-central-1, ca-west-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	il-central-1, me-central-1, ca-west-1
AWS-GR_S3_ACCOUNT_LEVEL_PUB LIC_ACCESS_BLOCKS_PERIODIC	il-central-1, eu-sur-2, eu-central-2
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-sur-2
AWS-GR_RDS_INSTANCE_PUBLIC_ ACCESS_CHECK	ap-south-2, eu-sur-2

Identificador de control	Regiones no compatibles
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, eu-south-2, ca-west-1
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1

Las regiones y la pila establecen limitaciones

Si planea extender la gobernanza a las unidades organizativas con un gran número de cuentas en un gran número de Regiones de AWS ellas, es posible que los conjuntos AWS CloudFormation apilados limiten el tamaño total de una organización. Puedes estimar la limitación con esta fórmula:

Número de cuentas administradas en la organización x número de regiones gobernadas <= 150 000

Como regla general, esperamos que la cantidad de cuentas admitidas al extender la gobernanza a una OU disminuya con la cantidad de regiones gobernadas.

Esta limitación se hace evidente si se activan más de 15 regiones en las que AWS Control Tower está disponible al extender la gobernanza a una OU. Se reduce el límite máximo de cuentas por unidad organizativa (OU).

Por ejemplo, si se activan 22 regiones, el límite es de 220 cuentas por unidad organizativa, en lugar de 300. Si necesita extender la gobernanza a las unidades organizativas con más de 220 cuentas, debe reducir el número de regiones activadas. Esta reducción se debe a las limitaciones del conjunto de pilas.

Pautas:

- Con 15 regiones activadas, se admiten unidades organizativas de hasta 300 cuentas
- Con 22 regiones activadas, se admiten unidades organizativas de hasta 220 cuentas
- Con entre 16 y 21 regiones activadas, el tamaño máximo de unidades organizativas admitidas oscila entre 220 y 300 cuentas
- Con más de 23 regiones activadas, el tamaño máximo de unidades organizativas admitidas es inferior a 220 cuentas

Diferencias regionales en cuanto a la funcionalidad de la Torre de Control de AWS

Existen ciertas diferencias en el comportamiento de la Torre de Control de AWS entre sí Regiones de AWS, ya que la Torre de Control de AWS organiza el comportamiento de otros AWS servicios. Por ejemplo:

- AWS Service Catalog no está disponible en todos los Regiones de AWS lugares donde AWS Control Tower está disponible, lo que cambia el comportamiento de Account Factory en esas regiones.
- En algunas regiones, Account Factory Customizations (AFC) no está disponible porque Service Catalog no está disponible para admitir la funcionalidad subyacente de los blueprints.
- Algunos controles no están disponibles en todos los casos Regiones de AWS debido a la falta de una funcionalidad subyacente.
- AFT y cFCT no están disponibles en todos los casos Regiones de AWS debido a la falta de funcionalidad subyacente.

Para determinar mejor el comportamiento de su entorno de la Torre de Control de AWS, determine su región de origen. A continuación, evalúe los siguientes elementos. Para obtener más información, consulte Limitaciones y cuotas en AWS Control Tower.

- ¿Está AWS Service Catalog disponible en la región de origen que desee?
- ¿Están disponibles los controles que necesita? Consulte Limitaciones de control.
- ¿El Centro de identidad de IAM está disponible en la región de origen que desee?

Nuevo: Guía de referencia de AWS Control Tower Controls

La información sobre los controles de la Torre de Control de AWS se ha trasladado a una nueva guía, la Guía de referencia de controles de la Torre de Control de AWS.

Prácticas recomendadas para los administradores de la Torre de Control de AWS

Este tema está dirigido principalmente a los administradores de cuentas de administración.

Los administradores de las cuentas de administración son responsables de explicar algunas de las tareas que los controles de la Torre de Control de AWS impiden que realicen los administradores de las cuentas de sus miembros. En este tema se describen algunas de las mejores prácticas y procedimientos para transferir este conocimiento y se ofrecen otros consejos para configurar y mantener el entorno de la Torre de Control de AWS de manera eficiente.

Explicar el acceso a los usuarios

La consola AWS Control Tower solo está disponible para los usuarios con permisos de administrador de la cuenta de administración. Solo estos usuarios pueden realizar tareas administrativas en tu landing zone. De acuerdo con las prácticas recomendadas, esto significa que la mayoría de sus usuarios y administradores de cuentas de miembros nunca verán la consola de la Torre de Control de AWS. Como miembro del grupo de administradores de cuentas de administración, es su responsabilidad explicar la siguiente información a los usuarios y administradores de las cuentas de sus miembros, según corresponda.

- Explica a qué AWS recursos tienen acceso los usuarios y administradores dentro de la landing zone.
- Enumere los controles preventivos que se aplican a cada unidad organizativa (OU) para que los demás administradores puedan planificar y ejecutar sus AWS cargas de trabajo en consecuencia.

Explicar el acceso a los recursos

Es posible que algunos administradores y otros usuarios necesiten una explicación de los AWS recursos a los que tienen acceso en tu landing zone. Este acceso puede incluir acceso mediante programación y acceso basado en consola. En términos generales, se permite el acceso de lectura y escritura a AWS los recursos. Para trabajar internamente AWS, los usuarios necesitan cierto nivel de acceso a los servicios específicos que necesitan para realizar su trabajo.

Es posible que algunos usuarios, como sus AWS desarrolladores, necesiten conocer los recursos a los que tienen acceso para poder crear soluciones de ingeniería. Otros usuarios, como los usuarios

finales de las aplicaciones que se ejecutan en AWS los servicios, no necesitan conocer AWS los recursos de tu landing zone.

AWS ofrece herramientas para identificar el alcance del acceso de un usuario a AWS los recursos. Después de identificar el ámbito del acceso de un usuario, puede compartir esa información con él, de acuerdo con las directivas de administración de la información de su organización. Para obtener más información sobre estas herramientas, consulte los enlaces siguientes.

- AWS asesor de acceso: la herramienta de asesoramiento de acceso AWS Identity and Access Management (IAM) permite determinar los permisos de los que disponen los desarrolladores mediante el análisis de la última fecha y hora en que una entidad de IAM, como un usuario, un rol o un grupo, llamó a un servicio. AWS Puede auditar el acceso al servicio y quitar los permisos innecesarios, y puede automatizar el proceso si es necesario. Para obtener más información, consulte nuestra AWS entrada del blog sobre seguridad.
- Simulador de políticas de IAM: con el simulador de políticas de IAM, puede probar y solucionar problemas de políticas basadas en IAM y basadas en recursos. Para obtener más información, consulte Probar las políticas de IAM con el simulador de políticas de IAM.
- AWS CloudTrail registros: puede revisar AWS CloudTrail los registros para ver las acciones realizadas por un usuario, rol o. Servicio de AWS Para obtener más información al respecto CloudTrail, consulte la Guía AWS CloudTrail del usuario.

  Las acciones realizadas por los administradores de las zonas de aterrizaje de AWS Control Tower se pueden ver en la cuenta de administración de la zona de aterrizaje. Las acciones realizadas por los administradores de las cuentas de los miembros y los usuarios se pueden ver en la cuenta del archivo de registros compartido.

  Puede ver una tabla resumida de los eventos de la Torre de Control de AWS en la página de actividades.

Explicación de los controles preventivos

Un control preventivo garantiza que las cuentas de su organización cumplan con las políticas corporativas. El estado de un control preventivo es obligatorio o no está activado. Un control preventivo evita las infracciones de las políticas mediante el uso de políticas de control de servicios (SCP). En cambio, un control detectivesco le informa de los diversos eventos o estados que existen, mediante AWS Config reglas definidas.

Es posible que algunos de sus usuarios, como AWS los desarrolladores, necesiten conocer los controles preventivos que se aplican a las cuentas y unidades organizativas que utilicen para poder crear soluciones de ingeniería. El siguiente procedimiento ofrece algunas instrucciones sobre cómo proporcionar esta información a los usuarios adecuados, de acuerdo con las políticas de administración de la información de su organización.

> **Note**
>
> Este procedimiento supone que ya has creado al menos una unidad organizativa secundaria en tu landing zone, así como al menos un AWS IAM Identity Center usuario.

Para mostrar los controles preventivos a los usuarios que necesiten conocerlos

1. Inicie sesión en la consola de AWS Control Tower en https://console.aws.amazon.com/controltower/.
2. En la barra de navegación de la izquierda, elija Organización.
3. En la tabla, elija el nombre de una de las unidades organizativas para las que el usuario necesite información sobre los controles aplicables.
4. Anote el nombre de la OU y los controles que se aplican a esta OU.
5. Repita los dos pasos anteriores para cada unidad organizativa de la que el usuario necesite información.

Para obtener información detallada sobre los controles y sus funciones, consulte Acerca de los controles en AWS Control Tower.

Planifique la zona de aterrizaje de su AWS Control Tower

Cuando realiza el proceso de configuración, AWS Control Tower lanza un recurso clave asociado a su cuenta, denominado landing zone, que sirve de base para sus organizaciones y sus cuentas.

> **Note**
>
> Puede tener una zona de inicio por organización.

Para obtener información sobre algunas de las prácticas recomendadas que debes seguir al planificar y configurar tu landing zone, consultaAWS estrategia de múltiples cuentas para su zona de aterrizaje de AWS Control Tower.

Formas de configurar la Torre de Control de AWS

Puede configurar una zona de aterrizaje de la Torre de Control de AWS en una organización existente o puede empezar por crear una nueva organización que contenga su zona de aterrizaje de la Torre de Control de AWS.

- Lance AWS Control Tower en una organización existente: Esta sección está destinada a los clientes que disponen de un AWS Organizations sistema operativo listo para incorporarlo a la gobernanza de AWS Control Tower.
- Lance AWS Control Tower en una nueva organización: Esta sección es para clientes que no tienen AWS Organizationsunidades organizativas ni cuentas existentes.

> **Note**
>
> Si ya tiene una zona de AWS Organizations aterrizaje, puede extender la gobernanza de AWS Control Tower desde la zona de aterrizaje existente a algunas o todas las OU y cuentas existentes dentro de una organización. Consulte Gobernar las organizaciones y cuentas existentes.

Compare la funcionalidad

He aquí una breve comparación de las diferencias entre añadir la Torre de Control de AWS a una organización existente o extender la gobernanza de la Torre de Control de AWS a las unidades organizativas y las cuentas. Además, se deben tener en cuenta algunas consideraciones especiales si se muda a AWS Control Tower desde la solución AWS Landing Zone.

Acerca de la incorporación a una organización existente: La incorporación de AWS Control Tower a una organización existente es algo que se puede lograr desde la AWS consola. En este caso, ya tiene una organización que ha creado en el AWS Organizations servicio, esa organización no está registrada actualmente en AWS Control Tower y, posteriormente, desea añadir una landing zone.

Al añadir una landing zone a una organización existente, AWS Control Tower establece una estructura paralela, a AWS Organizations nivel. No cambia las unidades organizativas ni las cuentas de su organización actual.

Acerca de la ampliación de la gobernanza: la ampliación de la gobernanza se aplica a unidades organizativas y cuentas específicas de una sola organización que ya esté registrada en AWS Control Tower, lo que significa que ya existe una landing zone para esa organización. Ampliar la gobernanza significa ampliar los controles de la Torre de Control de AWS para que sus restricciones se apliquen a las unidades organizativas y cuentas específicas de esa organización registrada. En este caso, no vas a lanzar una nueva landing zone, solo vas a expandir la landing zone actual de tu organización.

> **Important**
>
> Consideración especial: si actualmente utiliza la soluciónAWS Landing Zone (ALZ) AWS Organizations, consulte con su arquitecto de AWS soluciones antes de intentar habilitar AWS Control Tower en su organización. AWS Control Tower no puede realizar comprobaciones previas para determinar si AWS Control Tower puede interferir con su implementación actual en la zona de aterrizaje. Para obtener más información, consulte Tutorial: Cómo pasar de ALZ a la Torre de Control de AWS. Además, para obtener información sobre cómo mover cuentas de una landing zone a otra, consulta ¿Qué sucede si la cuenta no cumple los requisitos previos?

Lance AWS Control Tower en una organización existente

Al configurar una zona de aterrizaje de AWS Control Tower en una organización existente, puede empezar a trabajar inmediatamente, en paralelo con su AWS Organizations entorno actual. AWS Organizations Las demás unidades organizativas que haya creado en él permanecen inalteradas porque no están registradas en AWS Control Tower. Puede seguir utilizando tales unidades organizativas y cuentas exactamente como están.

AWS Control Tower se consolida mediante el uso de la cuenta de administración de su organización actual como cuenta de administración. No se necesita una nueva cuenta de administración. Puede lanzar su zona de aterrizaje de AWS Control Tower desde su cuenta de administración existente.

> **Note**
>
> Para configurar AWS Control Tower en una organización existente, los límites de servicio deben permitir la creación de al menos dos cuentas adicionales.

Efectos de añadir AWS Control Tower a su organización actual

AWS Control Tower crea dos cuentas en su organización: una cuenta de auditoría y una cuenta de registro. Estas cuentas mantienen un registro de las acciones realizadas por su equipo, en sus cuentas individuales de usuario final. Las cuentas de archivo de auditoría y registro aparecen en la unidad organizativa de seguridad de la zona de aterrizaje de AWS Control Tower.

Cuando configura su landing zone, las cuentas agregadas por AWS Control Tower pasan a formar parte de las que ya tiene y AWS Organizations, como tales, pasan a formar parte de la facturación de su organización actual.

Resumen de las capacidades

La habilitación de AWS Control Tower en una AWS Organizations organización existente proporciona varias mejoras importantes a la organización.

- Permite una facturación unificada en todos los grupos de su organización, ya que las cuentas añadidas por AWS Control Tower pasarán a formar parte de su organización actual.
- Le permite administrar todas las cuentas desde una sola cuenta de administración de su OU.
- Simplifica la forma de aplicar y hacer cumplir los controles que cubren la seguridad y el cumplimiento de las cuentas nuevas y existentes.

> **Important**
>
> Lanzar su zona de aterrizaje de AWS Control Tower en una AWS Organizations organización existente no le permite extender la gobernanza de la Torre de Control de AWS de esa organización a otras OU o cuentas que no estén registradas en AWS Control Tower.

Para lanzar AWS Control Tower en su organización actual, siga el proceso descrito enIntroducción a AWS Control Tower.

Para obtener más información sobre cómo la Torre de Control de AWS interactúa con AWS Organizations las organizaciones existentes, consulteControle las organizaciones y las cuentas con AWS Control Tower.

Lance AWS Control Tower en una nueva organización

Si es la primera vez que utiliza AWS Control Tower y aún no ha trabajado con AWS Organizationsél, el mejor lugar para empezar es con nuestro Configuración documento.

AWS Control Tower configura una organización automáticamente cuando no la tiene configurada.

AWS estrategia de múltiples cuentas para su zona de aterrizaje de AWS Control Tower

Los clientes de AWS Control Tower suelen buscar orientación sobre cómo configurar su AWS entorno y sus cuentas para obtener los mejores resultados.AWS ha creado un conjunto unificado de recomendaciones, denominado estrategia de cuentas múltiples, para ayudarlo a aprovechar al máximo sus AWS recursos, incluida la zona de aterrizaje de su AWS Control Tower.

Básicamente, AWS Control Tower actúa como una capa de organización que funciona con otros AWS servicios, lo que le ayuda a implementar las recomendaciones de cuentas AWS múltiples para AWS cuentas y. AWS OrganizationsUna vez configurada su landing zone, AWS Control Tower seguirá ayudándole a mantener sus políticas corporativas y prácticas de seguridad en varias cuentas y cargas de trabajo.

La mayoría de las zonas de aterrizaje se desarrollan con el tiempo. A medida que aumente el número de unidades organizativas (OU) y cuentas en la zona de aterrizaje de su AWS Control Tower, podrá ampliar su implementación de AWS Control Tower de forma que le ayude a organizar sus cargas de trabajo de forma eficaz. En este capítulo se proporciona una guía preceptiva sobre cómo planificar y configurar su zona de aterrizaje de AWS Control Tower, de acuerdo con la estrategia de AWS múltiples cuentas, y ampliarla con el tiempo.

Para obtener información general sobre las mejores prácticas para las unidades organizativas, consulte Best Practices for Organizational Units with. AWS Organizations

AWS estrategia multicuenta: guía de mejores prácticas

AWS Las mejores prácticas para un entorno bien diseñado recomiendan separar los recursos y las cargas de trabajo en varias cuentas. AWS Puede pensar en AWS las cuentas como contenedores de

recursos aislados: permiten categorizar las cargas de trabajo y reducir el radio de impacto cuando las cosas van mal.

Definición de una cuenta AWS

Una AWS cuenta actúa como contenedor de recursos y límite de aislamiento de recursos.

> **Note**
>
> Una AWS cuenta no es lo mismo que una cuenta de usuario, que se configura mediante la federación o AWS Identity and Access Management (IAM).

Más información sobre las cuentas AWS

Una AWS cuenta ofrece la posibilidad de aislar los recursos y contener las amenazas de seguridad para sus AWS cargas de trabajo. Una cuenta también proporciona un mecanismo para la facturación y la gobernanza de un entorno de carga de trabajo.

La AWS cuenta es el principal mecanismo de implementación que proporciona un contenedor de recursos para sus cargas de trabajo. Si su entorno está bien diseñado, puede administrar varias AWS cuentas de manera eficaz y, por lo tanto, administrar múltiples cargas de trabajo y entornos.

AWS Control Tower configura un entorno bien diseñado. Además, se basa en AWS las cuentas AWS Organizations, que ayudan a controlar los cambios en su entorno, que pueden extenderse a varias cuentas.

Definición de un entorno bien diseñado

AWS define un entorno bien diseñado como aquel que comienza con una landing zone.

AWS Control Tower ofrece una landing zone que se configura automáticamente. Aplica controles para garantizar el cumplimiento de las directrices corporativas en varias cuentas de su entorno.

Definición de landing zone

La landing zone es un entorno de nube que ofrece un punto de partida recomendado, que incluye cuentas predeterminadas, estructura de cuentas, diseños de red y seguridad, etc. Desde una landing zone, puede implementar cargas de trabajo que utilicen sus soluciones y aplicaciones.

Directrices para configurar un entorno bien diseñado

Los tres componentes clave de un entorno bien diseñado, que se explican en las siguientes secciones, son:

- Cuentas múltiples AWS
- Varias unidades organizativas (OU)
- Una estructura bien planificada

Utilice varias cuentas de AWS

Una cuenta no es suficiente para configurar un entorno bien diseñado. Al utilizar varias cuentas, puede respaldar mejor sus objetivos de seguridad y sus procesos empresariales. Estas son algunas de las ventajas de utilizar un enfoque de cuentas múltiples:

- Controles de seguridad: las aplicaciones tienen diferentes perfiles de seguridad, por lo que requieren políticas y mecanismos de control diferentes. Por ejemplo, es mucho más fácil hablar con un auditor y seleccionar una única cuenta que aloje la carga de trabajo del sector de las tarjetas de pago (PCI).
- Aislamiento: una cuenta es una unidad de protección de seguridad. Una cuenta puede contener los posibles riesgos y amenazas a la seguridad sin afectar a las demás. Por lo tanto, las necesidades de seguridad pueden requerir que aísles las cuentas unas de otras. Por ejemplo, puede que tengas equipos con distintos perfiles de seguridad.
- Muchos equipos: los equipos tienen diferentes responsabilidades y necesidades de recursos. Al configurar varias cuentas, los equipos no pueden interferir entre sí, como lo harían cuando usan la misma cuenta.
- Aislamiento de datos: aislar los almacenes de datos en una cuenta ayuda a limitar la cantidad de personas que tienen acceso a los datos y pueden administrarlos. Este aislamiento ayuda a evitar la exposición no autorizada de datos altamente privados. Por ejemplo, el aislamiento de datos ayuda a respaldar el cumplimiento del Reglamento General de Protección de Datos (GDPR).
- Proceso empresarial: las unidades de negocio o los productos suelen tener propósitos y procesos completamente diferentes. Se pueden establecer cuentas individuales para satisfacer las necesidades específicas de la empresa.
- Facturación: una cuenta es la única forma de separar los elementos a nivel de facturación, incluidos los gastos de transferencia, etc. La estrategia de cuentas múltiples ayuda a crear partidas

facturables independientes para todas las unidades de negocio, los equipos funcionales o los usuarios individuales.

- Asignación de AWS cuotas: las cuotas se establecen por cuenta. Al separar las cargas de trabajo en diferentes cuentas, cada cuenta (por ejemplo, un proyecto) tiene una cuota individual bien definida.

Usa varias unidades organizativas

AWS Control Tower y otros marcos de organización de cuentas pueden realizar cambios que traspasen los límites de las cuentas. Por lo tanto, las AWS mejores prácticas abordan los cambios entre cuentas, que pueden dañar un entorno o socavar su seguridad. En algunos casos, los cambios pueden afectar al entorno general, más allá de las políticas. Por ello, te recomendamos que configures al menos dos cuentas obligatorias: la de producción y la de puesta en escena.

Además, AWS las cuentas suelen agruparse en unidades organizativas (OU), con fines de gobernanza y control. Las OU están diseñadas para gestionar el cumplimiento de las políticas en varias cuentas.

Nuestra recomendación es que, como mínimo, cree un entorno de preproducción (o ensayo) que sea distinto de su entorno de producción, con controles y políticas distintos. Los entornos de producción y puesta en escena se pueden crear y gobernar como unidades organizativas independientes y facturarse como cuentas independientes. Además, es posible que desee configurar una unidad organizativa Sandbox para las pruebas de código.

Utiliza una estructura bien planificada para las unidades organizativas de tu landing zone

AWS Control Tower configura algunas unidades organizativas automáticamente. A medida que tus cargas de trabajo y requisitos se expandan con el tiempo, puedes ampliar la configuración original de landing zone para adaptarla a tus necesidades.

> **Note**
>
> Los nombres que figuran en los ejemplos siguen las convenciones de AWS nomenclatura sugeridas para configurar un entorno de cuentas múltiples AWS . Puedes cambiar el nombre de tus OU después de configurar tu landing zone seleccionando Editar en la página de detalles de la OU.

Recomendaciones

Una vez que AWS Control Tower haya configurado la primera unidad organizativa necesaria para usted (la unidad organizativa de seguridad), le recomendamos que cree algunas unidades organizativas adicionales en su landing zone.

Le recomendamos que permita a AWS Control Tower crear al menos una unidad organizativa adicional, denominada unidad organizativa Sandbox. Esta OU es para sus entornos de desarrollo de software. AWS Control Tower puede configurar la unidad organizativa Sandbox por usted durante la creación de la zona de aterrizaje, si la selecciona.

Se recomiendan otras dos unidades organizativas que puede configurar por su cuenta: la unidad organizativa de infraestructura, que contiene los servicios compartidos y las cuentas de red, y una unidad organizativa que contiene las cargas de trabajo de producción, denominada unidad organizativa de cargas de trabajo. Puede añadir unidades organizativas adicionales en su landing zone a través de la consola de AWS Control Tower en la página de unidades organizativas.

Unidades organizativas recomendadas además de las que se configuran automáticamente

- OU de infraestructura: contiene sus servicios compartidos y sus cuentas de red.

  > **Note**
  >
  > AWS Control Tower no configura la OU de infraestructura por usted.

- Sandbox OU: una unidad organizativa de desarrollo de software. Por ejemplo, puede tener un límite de gasto fijo o puede que no esté conectada a la red de producción.

  > **Note**
  >
  > AWS Control Tower recomienda configurar la unidad organizativa Sandbox, pero es opcional. Se puede configurar automáticamente como parte de la configuración de tu landing zone.

- Workloads OU: contiene las cuentas que ejecutan sus cargas de trabajo.

  > **Note**
  >
  > AWS Control Tower no configura la unidad organizativa Workloads por usted.

Para obtener más información, consulte Organización para iniciar la producción con AWS Control Tower.

Ejemplo de Torre de Control de AWS con una estructura completa de unidades organizativas de varias cuentas

AWS Control Tower admite una jerarquía de unidades organizativas anidada, lo que significa que puede crear una estructura jerárquica de unidades organizativas que cumpla con los requisitos de su organización. Puede crear un entorno de AWS Control Tower que se ajuste a la guía de estrategia de AWS cuentas múltiples.

También puede crear una estructura de unidad organizativa más simple y plana que tenga un buen rendimiento y se ajuste a las directrices sobre AWS múltiples cuentas. El hecho de que pueda crear una estructura organizativa jerárquica no significa que deba hacerlo.

- Para ver un diagrama que muestra un ejemplo de conjunto de unidades organizativas en un entorno de AWS Control Tower expandido y plano con orientación para AWS varias cuentas, consulte Ejemplo: cargas de trabajo en una estructura de unidad organizativa plana.
- Para obtener más información sobre cómo funciona AWS Control Tower con estructuras de unidades organizativas anidadas, consulteUnidades organizativas anidadas en la Torre de Control de AWS.
- Para obtener más información sobre cómo AWS Control Tower se ajusta a las AWS directrices, consulte el documento AWS técnico Organizing Your AWS Environment Using Multiple Accounts.

El diagrama de la página enlazada muestra que se han creado más unidades organizativas fundamentales y más unidades organizativas adicionales. Estas unidades organizativas satisfacen las necesidades adicionales de una implementación más grande.

En la columna de unidades organizativas fundamentales, se han agregado dos unidades organizativas a la estructura básica:

- Unidad organizativa Security_Prod: proporciona un área de solo lectura para las políticas de seguridad, así como un área de auditoría de seguridad impecable.
- OU de infraestructura: tal vez desee separar la OU de infraestructura, como se recomendaba anteriormente, en dos unidades organizativas: Infrastructure_Test (para la infraestructura de preproducción) e Infrastructure_Prod (para la infraestructura de producción).

En el área de unidades organizativas adicionales, se han agregado varias unidades organizativas más a la estructura básica. Estas son las siguientes unidades organizativas recomendadas para crear a medida que el entorno crezca:

- Unidad organizativa de cargas de trabajo: la unidad organizativa Workloads, que antes se recomendaba pero era opcional, se ha dividido en dos unidades organizativas: Workloads_Test (para cargas de trabajo de preproducción) y Workloads_Prod (para cargas de trabajo de producción).
- PolicyStaging OU: permite a los administradores del sistema probar los cambios en los controles y las políticas antes de aplicarlos por completo.
- OU suspendida: ofrece una ubicación para las cuentas que pueden haber estado inhabilitadas temporalmente.

Acerca de The Root

La raíz no es una unidad organizativa. Es un contenedor para la cuenta de administración y para todas las OU y cuentas de la organización. Conceptualmente, la raíz contiene todas las unidades organizativas. No se puede eliminar. No puede controlar las cuentas inscritas en el nivel raíz de AWS Control Tower. En su lugar, controle las cuentas inscritas dentro de sus unidades organizativas. Para ver un diagrama útil, consulte la AWS Organizations documentación.

Consejos administrativos para la configuración de la landing zone

- La AWS región en la que trabajas más debe ser tu región de origen.
- Configura tu landing zone y despliega tus cuentas de Account Factory desde tu región de origen.
- Si va a invertir en varias AWS regiones, asegúrese de que sus recursos de nube estén en la región en la que realizará la mayor parte del trabajo administrativo de la nube y en la que ejecutará sus cargas de trabajo.
- Al mantener sus cargas de trabajo y registros en la misma AWS región, reduce el costo que implicaría mover y recuperar la información de los registros entre regiones.
- La auditoría y otros buckets de Amazon S3 se crean en la misma AWS región desde la que se lanza AWS Control Tower. Le recomendamos que no mueva estos buckets.
- Puede crear sus propios cubos de registro en la cuenta de Log Archive, pero no es recomendable. Asegúrese de dejar los depósitos creados por AWS Control Tower.

- Sus registros de acceso a Amazon S3 deben estar en la misma AWS región que los buckets de origen.
- Al lanzarlo, los puntos de enlace del AWS Security Token Service (STS) deben estar activados en la cuenta de administración en todas las regiones compatibles con AWS Control Tower. De lo contrario, el lanzamiento puede fallar a mitad del proceso de configuración.
- AWS Control Tower solo admite el etiquetado de los controles habilitados. Para obtener más información, consulte AWS Control Tower admite el etiquetado de los controles habilitados.
- Recomendamos habilitar la autenticación multifactor (MFA) en todas las cuentas que administra AWS Control Tower.

Consideraciones sobre las VPC

- La VPC creada por la Torre de Control de AWS se limita a la versión Regiones de AWS en la que está disponible la Torre de Control de AWS. Es posible que algunos clientes cuyas cargas de trabajo se ejecutan en regiones no compatibles deseen deshabilitar la VPC que se crea con su cuenta de Account Factory. Es posible que prefieran crear una nueva VPC con la cartera de Service Catalog o crear una VPC personalizada que se ejecute solo en las regiones requeridas.
- La VPC creada por AWS Control Tower no es la misma que la VPC predeterminada que se crea para todos. Cuentas de AWS En las regiones en las que se admite AWS Control Tower, AWS Control Tower elimina la VPC predeterminada al crear la VPC de AWS Control Tower.
- Si eliminas tu VPC predeterminada en tu AWS región de origen, es mejor eliminarla en todas las demás AWS regiones.

Recomendaciones para configurar grupos, funciones y políticas

A medida que configura su zona de inicio, es recomendable decidir de antemano qué usuarios requerirán acceso a ciertas cuentas y por qué. Por ejemplo, solo el equipo de seguridad debe poder acceder a una cuenta de seguridad, solo el equipo de administradores de la nube debe poder acceder a la cuenta de administración, etc.

Para obtener más información sobre este tema, consulte. Administración de identidades y accesos en AWS Control Tower

Restricciones recomendadas

Puede restringir el alcance del acceso administrativo a sus organizaciones configurando un rol o una política de IAM que permita a los administradores gestionar únicamente las acciones de

la Torre de Control de AWS. El enfoque recomendado consiste en utilizar la política de IAM. `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy` Con la `AWSControlTowerServiceRolePolicy` función habilitada, un administrador solo puede administrar la Torre de Control de AWS. Asegúrese de incluir en cada cuenta el acceso adecuado AWS Organizations para administrar los controles preventivos y los SCP, así como el acceso a los controles de detección AWS Config, para administrar los controles de detección.

Cuando configure la cuenta de auditoría compartida en su zona de inicio, le recomendamos que asigne el grupo `AWSSecurityAuditors` a cualquier auditor externo de sus cuentas. Este grupo concede a sus miembros permiso de solo lectura. Una cuenta no debe tener permisos de escritura en el entorno que está auditando, porque puede infringir el cumplimiento de los requisitos de separación de funciones para los auditores.

Puede imponer condiciones en las políticas de confianza de sus funciones para restringir las cuentas y los recursos que interactúan con determinadas funciones en AWS Control Tower. Le recomendamos encarecidamente que restrinja el acceso al `AWSControlTowerAdmin` rol, ya que permite permisos de acceso amplios. Para obtener más información, consulte las condiciones opcionales de las relaciones de confianza de su puesto.

Guía para crear y modificar los recursos de la Torre de Control de AWS

Recomendamos las siguientes prácticas recomendadas a la hora de crear y modificar recursos en AWS Control Tower. Estas directrices podrían cambiar cuando se actualiza el servicio. Recuerde que el modelo de responsabilidad compartida se aplica a su entorno de AWS Control Tower.

Directrices generales

- No modifique ni elimine ningún recurso creado por AWS Control Tower, incluidos los recursos de la cuenta de administración, las cuentas compartidas y las cuentas de los miembros. Si modificas estos recursos, es posible que tengas que actualizar tu landing zone o volver a registrar una OU, y la modificación puede dar lugar a informes de conformidad inexactos.

  En particular:

  - Mantenga una AWS Config grabadora activa. Si eliminas tu grabadora Config, los controles de detección no podrán detectar ni informar de la desviación. Los recursos no conformes pueden declararse conformes debido a que no hay suficiente información.

  - No modifique ni elimine las funciones AWS Identity and Access Management (de IAM) creadas en las cuentas compartidas de la unidad organizativa (OU) de seguridad. Si lo hace, es posible que tenga que actualizar estos roles en su zona de destino.
  - No elimine el `AWSControlTowerExecution` rol de las cuentas de sus miembros, ni siquiera en las cuentas no inscritas. Si lo hace, no podrá inscribir estas cuentas en AWS Control Tower ni registrar sus unidades organizativas principales inmediatas.
- No prohíba el uso de ninguna de ellas Regiones de AWS a través de SCP o AWS Security Token Service ()AWS STS. Si lo hace, la Torre de Control de AWS pasará a un estado indefinido. Si no permite las regiones con AWS STS, su funcionalidad fallará en esas regiones, ya que la autenticación no estará disponible en esas regiones. En su lugar, utilice la capacidad de denegación regional de la Torre de Control de AWS, tal como se muestra en el control, denegar el acceso a en AWS función de lo solicitado Región de AWS, que funciona a nivel de la zona de landing, o denegar el control de la región de control aplicada a la OU, que funciona a nivel de la OU para restringir el acceso a las regiones.
- El AWS Organizations `FullAWSAccess` SCP debe aplicarse y no debe fusionarse con otros SCP. El cambio en este SCP no se considera una desviación; sin embargo, algunos cambios pueden afectar a la funcionalidad de la Torre de Control Tower de AWS de forma impredecible si se deniega el acceso a determinados recursos. Por ejemplo, si el SCP se separa o se modifica, una cuenta puede perder el acceso a una AWS Config grabadora o crear un vacío en CloudTrail el registro.
- No utilice la AWS Organizations `DisableAWSServiceAccess` API para desactivar el acceso al servicio de la Torre de Control de AWS a la organización en la que configuró su landing zone. Si lo hace, es posible que algunas funciones de detección de desviaciones de la Torre de Control de AWS no funcionen correctamente sin el soporte de mensajería de su parte AWS Organizations. Estas funciones de detección de desviaciones ayudan a garantizar que AWS Control Tower pueda informar con precisión del estado de conformidad de las unidades organizativas, las cuentas y los controles de su organización. Para obtener más información, consulte API_DisableAWSServiceAccessla referencia de la AWS Organizations API.
- En general, AWS Control Tower realiza una sola acción a la vez, que debe completarse antes de que pueda comenzar otra acción. Por ejemplo, si intenta aprovisionar una cuenta mientras el proceso de activación de un control ya está en marcha, el aprovisionamiento de la cuenta fallará.

  Excepción:

- AWS Control Tower permite realizar acciones simultáneas para implementar controles opcionales. Para obtener más información, consulte Implementación simultánea para ver los controles opcionales.
- AWS Control Tower permite crear, actualizar o inscribir hasta diez acciones simultáneas en cuentas con Account Factory.

> **Note**
>
> Para obtener más información sobre los recursos creados por AWS Control Tower, consulte¿Qué son las cuentas compartidas?.

Consejos sobre cuentas y unidades organizativas

- Le recomendamos que mantenga un máximo de 300 cuentas por unidad organizativa registrada, de modo que pueda actualizarlas con la función de volver a registrar la unidad organizativa siempre que sea necesario actualizar la cuenta, por ejemplo, al configurar nuevas regiones para su gobernanza.
- Para reducir el tiempo necesario para registrar una unidad organizativa, le recomendamos que mantenga el número de cuentas por unidad organizativa en torno a 150, aunque el límite es de 300 cuentas por unidad organizativa. Como regla general, el tiempo necesario para registrar una OU aumenta en función del número de regiones en las que opera la OU, multiplicado por el número de cuentas de la OU.
- Se calcula que una unidad organizativa con 150 cuentas necesita aproximadamente 2 horas para registrarse y activar los controles, y aproximadamente 1 hora para volver a registrarse. Además, una unidad organizativa que tiene muchos controles tarda más en registrarse que una unidad organizativa con pocos controles.
- Una de las preocupaciones que plantea la posibilidad de prolongar el período de registro de una unidad organizativa es que este proceso bloquea otras acciones. Algunos clientes prefieren disponer de más tiempo para registrar o volver a registrar una OU, ya que prefieren tener más cuentas en cada OU.

¿Cuándo iniciar sesión como usuario root

Algunas tareas administrativas requieren que inicie la sesión como usuario raíz. Puede iniciar sesión como usuario raíz en una Cuenta de AWS creada por la fábrica de cuentas en AWS Control Tower.

Debe iniciar sesión como usuario raíz para realizar las siguientes acciones:

- Cambiar determinadas opciones de configuración de la cuenta, incluido el nombre de la cuenta, la contraseña del usuario raíz o la dirección de correo electrónico. Para obtener más información, consulte Actualice y mueva cuentas de fábrica con AWS Control Tower o con AWS Service Catalog.
- Para cerrar un Cuenta de AWS.
- Para obtener más información sobre las acciones que requieren credenciales de inicio de sesión de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía de AWS Account Management referencia.

> **Note**
>
> Para cambiar o habilitar su plan AWS Support, debe iniciar sesión como usuario root o ser un usuario con los permisos de IAM adecuados. .

Para iniciar sesión como usuario raíz

1. Abre la página de AWS inicio de sesión.

   Si no tiene la dirección de correo electrónico Cuenta de AWS a la que necesita acceso, puede obtenerla en AWS Control Tower. Abra la consola de la cuenta de administración, elija Cuentas y busque la dirección de correo electrónico.
2. Introduce la dirección de correo electrónico Cuenta de AWS a la que deseas acceder y, a continuación, selecciona Siguiente.
3. Elija Forgot password? (¿Ha olvidado la contraseña?) para que se envíen las instrucciones de restablecimiento de la contraseña a la dirección de correo electrónico del usuario raíz.
4. Abra el mensaje de correo electrónico de restablecimiento de contraseña en el buzón del usuario raíz y siga las instrucciones para restablecer la contraseña.
5. Abre la página de AWS inicio de sesión y, a continuación, inicia sesión con la contraseña restablecida.

AWS Organizations orientación

- Puede encontrar orientación sobre las prácticas recomendadas para proteger la seguridad de su cuenta de administración de AWS Control Tower y las cuentas de los miembros en la AWS Organizations documentación.
  - Prácticas recomendadas para la cuenta de administración
  - Mejores prácticas para las cuentas de los miembros
- No lo utilice AWS Organizations para actualizar las políticas de control de servicios (SCP) adjuntas a una OU que esté registrada en AWS Control Tower. Si lo hace, los controles podrían pasar a un estado desconocido, por lo que tendrá que restablecer su landing zone o volver a registrar su OU en AWS Control Tower. En su lugar, puede crear nuevos SCP y adjuntarlos a las unidades organizativas en lugar de editar los SCP que AWS Control Tower ha creado.
- El traslado de cuentas individuales ya inscritas a la Torre de Control de AWS desde fuera de una unidad organizativa registrada provoca un error que debe resolverse. Consulte Tipos de desviaciones de gobernanza.
- Si AWS Organizations solía crear, invitar o mover cuentas dentro de una organización registrada en AWS Control Tower, AWS Control Tower no inscribe esas cuentas y esos cambios no se registran. Si necesita acceso a estas cuentas a través de SSO, consulte la página en la que se describe el acceso a cuentas miembro.
- Si solía trasladar una OU AWS Organizations a una organización creada por AWS Control Tower, la OU externa no está registrada por AWS Control Tower.
- AWS Control Tower gestiona el filtrado de permisos de forma diferente a como AWS Organizations lo hace. Si sus cuentas se aprovisionan con la fábrica de cuentas de la Torre de Control de AWS, los usuarios finales pueden ver los nombres y los padres de todas las unidades organizativas en la consola de la Torre de Control de AWS, incluso si no tienen permiso para recuperar esos nombres y padres directamente AWS Organizations .
- AWS Control Tower no admite permisos mixtos en las organizaciones, como el permiso para ver la unidad organizativa principal pero no para ver los nombres de la unidad organizativa. Por este motivo, se espera que los administradores de la Torre de Control de AWS dispongan de todos los permisos.
- El AWS Organizations `FullAWSAccess` SCP debe aplicarse y no debe fusionarse con otros SCP. El cambio en este SCP no se considera una desviación; sin embargo, algunos cambios pueden afectar a la funcionalidad de la Torre de Control Tower de AWS de forma impredecible si se deniega el acceso a determinados recursos. Por ejemplo, si el SCP se separa o se modifica,

una cuenta puede perder el acceso a una AWS Config grabadora o crear un vacío en CloudTrail el registro.

- No utilice la AWS Organizations `DisableAWSServiceAccess` API para desactivar el acceso al servicio de la Torre de Control de AWS a la organización en la que configuró su landing zone. Si lo hace, es posible que algunas funciones de detección de desviaciones de la Torre de Control de AWS no funcionen correctamente sin el soporte de mensajería de su parte AWS Organizations. Estas funciones de detección de desviaciones ayudan a garantizar que AWS Control Tower pueda informar con precisión del estado de conformidad de las unidades organizativas, las cuentas y los controles de su organización. Para obtener más información, consulte API_DisableAWSServiceAccessla referencia de la AWS Organizations API.

Guía sobre el Centro de Identidad de IAM

> **Note**
>
> SSO es una abreviatura que se utiliza en el sector de la tecnología para indicar el inicio de sesión único. En términos generales, el SSO es un servicio de autenticación de sesión y usuario. Permite a alguien usar un conjunto de credenciales de inicio de sesión para acceder a muchas aplicaciones. Cuando nos referimos a la función de inicio de sesión único AWS, nos referimos al AWS servicio denominado AWS Identity and Access Managementy abreviado como IAM o IAM Identity Center.

AWS Control Tower recomienda que utilice AWS Identity and Access Management (IAM) para regular el acceso a su Cuentas de AWS. Sin embargo, tiene la opción de elegir si AWS Control Tower configura el Centro de Identidad de IAM por usted, si configura el Centro de Identidad de IAM usted mismo, de la manera que cumpla con los requisitos de su empresa de la manera más eficaz, o si selecciona otro método de acceso a la cuenta.

De forma predeterminada, AWS Control Tower configura el centro de identidad de AWS IAM para su landing zone, de acuerdo con las recomendaciones de prácticas recomendadas definidas en Organizar su AWS entorno con varias cuentas. La mayoría de los clientes eligen la opción predeterminada. A veces se requieren métodos de acceso alternativos para cumplir con la normativa en sectores o países específicos, o en aquellos Regiones de AWS lugares donde el Centro de Identidad de AWS IAM no esté disponible.

Elegir una opción

Desde la consola, puede optar por gestionar automáticamente el IAM Identity Center durante el proceso de configuración de la landing zone, en lugar de permitir que AWS Control Tower lo configure por usted. En cualquier momento posterior, puedes cambiar esta selección modificando la configuración de la zona de aterrizaje y actualizando tu zona de aterrizaje en la página de configuración de la zona de aterrizaje.

Para dejar de usar el Centro de Identidad de AWS IAM en la Torre de Control de AWS o para empezar a usar el Centro de Identidad de AWS IAM

1. Ve a la página de configuración de la landing zone
2. Seleccione la pestaña Configuraciones
3. A continuación, pulse el botón de radio correspondiente para cambiar la selección de AWS IAM Identity Center.

Después de decidir autogestionar el Centro de Identidad de AWS IAM como su IdP, AWS Control Tower crea solo las funciones y políticas necesarias para gestionar la Torre de Control de AWS, como y. `AWSControlTowerAdmin` `AWSControlTowerAdminPolicy` En el caso de las zonas de aterrizaje que se autogestionan, AWS Control Tower ya no crea funciones y agrupaciones de IAM para uso específico del cliente, ni durante el proceso de configuración de la zona de aterrizaje ni durante el aprovisionamiento de cuentas con Account Factory.

> **Note**
>
> Si elimina el AWS IAM Identity Center de la zona de destino de la Torre de Control de AWS, los usuarios, grupos y conjuntos de permisos que creó la Torre de Control de AWS no se eliminarán. Le recomendamos que elimine estos recursos.

Los clientes de Account Factory con proveedores de identidad alternativos (IdPs), como Azure AD, Ping u Okta, pueden seguir el proceso del Centro de Identidad de AWS IAM para conectarse a un proveedor de identidad externo e incorporar su IdP. Puede volver a permitir que AWS Control Tower genere sus agrupaciones y funciones en cualquier momento modificando la configuración de landing zone.

- Para obtener información específica sobre cómo AWS Control Tower trabaja con el IAM Identity Center en función de su fuente de identidad, consulte Consideraciones para AWS IAM Identity

Center los clientes en la sección Comprobaciones previas al lanzamiento de la página de introducción de esta Guía del usuario.

- Para obtener información adicional sobre cómo el comportamiento de la Torre de Control de AWS interactúa con el Centro de identidad de IAM y las diferentes fuentes de identidad, consulte Consideraciones para cambiar la fuente de identidad en la Guía del usuario del Centro de identidades de IAM.
- Consulte Trabajo con el Centro de Identidad de AWS IAM y la Torre de Control de AWS para obtener más información sobre cómo trabajar con AWS Control Tower y IAM Identity Center.

Guía de Account Factory

Puede tener problemas al usar Account Factory para aprovisionar una nueva cuenta en AWS Control Tower. Para obtener información sobre cómo solucionar estos problemas, consulte la sección de Solución de problemas Error en el nuevo aprovisionamiento de cuentas de la Guía del usuario de AWS Control Tower.

Le recomendamos que cree usuarios federados o roles de IAM en lugar de usuarios de IAM. Los usuarios federados y los roles de IAM le proporcionan credenciales temporales. Los usuarios de IAM tienen credenciales de larga duración que pueden resultar difíciles de gestionar. Para obtener más información, consulte las identidades de IAM (usuarios, grupos de usuarios y roles) en la Guía del usuario de IAM.

Si se ha autenticado como usuario de IAM o usuario del IAM Identity Center al aprovisionar una nueva cuenta en Account Factory o al utilizar la función de inscripción de cuentas (AWS Control Tower), compruebe que el usuario tiene acceso a su cartera. AWS Service Catalog De lo contrario, podría recibir un mensaje de error de Service Catalog. Para obtener más información, consulte Error: no se encontraron rutas de lanzamiento la sección de solución de problemas de la Guía del usuario de AWS Control Tower.

> **Note**
>
> Se pueden aprovisionar hasta cinco cuentas a la vez.

Guía sobre la suscripción a SNS Topics

- El tema `aws-controltower-AllConfigNotifications` SNS recibe todos los eventos publicados por AWS Config, incluidas las notificaciones de conformidad y las notificaciones de CloudWatch eventos de Amazon. Por ejemplo, este tema le informa si se ha producido una infracción de control. También proporciona información sobre otros tipos de eventos. (Obtenga más información AWS Configsobre lo que publican cuando se configura este tema).
- Los eventos de datos de la `aws-controltower-BaselineCloudTrail` ruta también están configurados para publicarse en el tema de `aws-controltower-AllConfigNotifications` SNS.
- Para recibir notificaciones de conformidad detalladas, le recomendamos que se suscriba al tema `aws-controltower-AllConfigNotifications` SNS. En este tema se recopilan las notificaciones de conformidad de todas las cuentas secundarias.
- Para recibir notificaciones de desvío y otras notificaciones, así como notificaciones de conformidad, pero en general menos notificaciones, te recomendamos que te suscribas al tema de las redes `aws-controltower-AggregateSecurityNotifications` sociales.
- Para recibir notificaciones sobre errores de AWS Control Tower Account Factory for Terraform (AFT), puede suscribirse a un tema de SNS llamado aft_failure_notifications, que se muestra en el repositorio de AFT. Por ejemplo:

```
resource "aws_sns_topic" "aft_failure_notifications" {
    name = "aft-failure-notifications"
    kms_master_key_id = "alias/aws/sns"
}
```

- Todos los temas de SNS están cifrados en reposo con cifrado de disco. Para obtener más información, consulte Cifrado de datos.

Para obtener más información sobre los temas de SNS y el cumplimiento, consulte Prevención y notificación.

Guía para las claves de KMS

AWS Control Tower funciona con AWS Key Management Service (AWS KMS). Si lo desea, si desea cifrar y descifrar los recursos de la Torre de Control Tower de AWS con una clave de cifrado que administre, puede generarla y configurarla. AWS KMS keys Puedes añadir o cambiar una clave KMS

cada vez que actualices tu landing zone. Como práctica recomendada, te recomendamos que utilices tus propias claves de KMS y que las cambies de vez en cuando.

AWS KMS le permite crear claves KMS multirregionales y claves asimétricas. Sin embargo, AWS Control Tower no admite claves multirregionales ni claves asimétricas. AWS Control Tower realiza una comprobación previa de las claves existentes. Es posible que aparezca un mensaje de error si selecciona una clave multirregional o una clave asimétrica. En ese caso, genere otra clave para utilizarla con los recursos de la Torre de Control de AWS.

Para los clientes que utilizan un clúster de AWS CloudHSM: cree un almacén de claves personalizado asociado a su clúster de CloudHSM. A continuación, puede crear una clave KMS, que reside en el almacén de claves personalizadas de CloudHSM que ha creado. Puede añadir esta clave de KMS a AWS Control Tower.

Debe realizar una actualización específica en la política de permisos de una clave de KMS para que funcione con AWS Control Tower. Para obtener más información, consulte la sección denominadaActualice la política de claves de KMS.

Servicios basados en IA y AWS Control Tower

Puede crear políticas de control de servicios (SCP) que le permitan optar por que los servicios basados en la IA no almacenen sus datos. AWS Estas políticas de SCP especifican que los servicios basados en IA, como Amazon Rekognition o CodeWhisperer Amazon, no pueden almacenar ni utilizar sus datos para mejorar otros servicios basados en IA. AWS

Estas políticas de SCP de exclusión de la IA se pueden aplicar a toda la organización, a una OU o a una cuenta específica. Las políticas tienen un efecto global. Puedes encontrar más información sobre estas políticas en las políticas de exclusión de los servicios de IA, en la AWS Organizations documentación.

Para obtener una lista de AWS los servicios que utilizan la IA, junto con ejemplos de políticas, consulte la sintaxis y los ejemplos de las políticas de exclusión de los servicios de IA en la Guía del AWS Organizations usuario.

Administración de actualizaciones de configuración en AWS Control Tower

Es responsabilidad de los miembros del equipo de administradores de la nube central mantener actualizada tu landing zone. La actualización de su landing zone garantiza que AWS Control Tower esté parcheada y actualizada. Además, para proteger tu landing zone de posibles problemas de conformidad, los miembros del equipo del administrador central de la nube deberían resolver los problemas de deriva tan pronto como los detecten y notifiquen.

> **Note**
>
> La consola de AWS Control Tower indica cuándo es necesario actualizar su landing zone. Si no ves la opción de actualización, significa que tu landing zone ya está actualizada.

La siguiente tabla contiene una lista de las versiones de actualización de la zona de aterrizaje de AWS Control Tower, con enlaces a las descripciones de cada versión.

Versión	Fecha de lanzamiento	Descripción
3.3	12-12-2023	Zona de aterrizaje, versión 3.3
3.2	6-09-2023	Zona de aterrizaje, versión 3.2
3.1	2-09-2023	Zona de aterrizaje, versión 3.1
3.0	26-7-2022	Landing zone versión 3.0
2.9	22-4-2022	Zona de aterrizaje, versión 2.9
2.8	2-10-2022	Zona de aterrizaje, versión 2.8
2.7	4-8-2021	Zona de aterrizaje, versión 2.7
2.6	29-12-2020	Zona de aterrizaje, versión 2.6
2,5	18-11-2020	Zona de aterrizaje, versión 2.5

Versión	Fecha de lanzamiento	Descripción
2.4	Ninguna	Ninguna
2.3	3-5-2020	Zona de aterrizaje, versión 2.3
2.2	13-11-19	Zona de aterrizaje, versión 2.2
2.1	6-24-19	Zona de aterrizaje, versión 2.1

Cada vez que actualices tu landing zone, tendrás la oportunidad de modificar la configuración de tu landing zone.

Ventajas de la actualización

- Puede cambiar las regiones gobernadas
- Puede cambiar su política de retención de registros
- Puedes añadir o eliminar la región y denegar el control
- Puede aplicar claves de cifrado de AWS KMS
- Puede activar o desactivar la ruta a nivel de la organización. CloudTrail
- Puedes resolver la deriva de la zona de aterrizaje

Cuando actualice su landing zone, recibirá automáticamente las funciones más recientes de AWS Control Tower. Consulta la versión actual de tu zona de aterrizaje en la página de configuración de la zona de aterrizaje.

Si se produce un error en una actualización, AWS Control Tower no vuelve a una versión anterior de landing zone. Es posible que encuentres tu landing zone en un estado indeterminado. Si es así, ponte en contacto con AWS el servicio de asistencia. Para obtener más información sobre cómo solucionar un error en la actualización, consulteNo se pudo actualizar la zona de aterrizaje.

Tienes la oportunidad de borrar los mapeos del centro de AWS identidad no utilizados (antes denominados AWS SSO) al actualizar tu landing zone. Para obtener más información, consulte Notas de campo: Elimine automáticamente las asignaciones de centros de identidad de IAM no utilizadas durante las actualizaciones de la Torre de Control de AWS.

Requisito previo para la actualización y el restablecimiento: desactive Requester Pays

Antes de actualizar o restablecer tu landing zone, asegúrate de que el depósito de registro de Amazon S3 de la cuenta de Log Archive no tenga habilitada la función Requester Pays. Debe desactivar esa función antes de comenzar el proceso de actualización o restablecimiento. Cuando AWS Control Tower configura el depósito de registro, esta función no está habilitada. Por lo tanto, solo los clientes que hayan activado posteriormente la función El solicitante paga deben desactivarla. Para obtener más información, consulte la política de depósitos de Amazon S3 para los depósitos Requester Pays CloudTrail y su uso.

Acerca de las actualizaciones

Las actualizaciones son necesarias para corregir los errores de gobierno o para migrar a una nueva versión de AWS Control Tower. Para realizar una actualización completa de AWS Control Tower, primero debe actualizar su landing zone y, a continuación, actualizar las cuentas inscritas de forma individual. Es posible que tenga que realizar tres tipos de actualizaciones en diferentes momentos.

- Una actualización de la zona de aterrizaje: la mayoría de las veces, este tipo de actualización se realiza seleccionando Actualizar en la página de configuración de la zona de aterrizaje. Puede que tengas que realizar una actualización de la zona de aterrizaje para resolver ciertos tipos de deriva, y puedes elegir Restablecer cuando sea necesario.
- Una actualización de una o varias cuentas individuales: debe actualizar las cuentas si cambia la información asociada o si se ha producido cierto tipo de desviación. Si una cuenta requiere una actualización, el estado de la cuenta mostrará la opción Actualización disponible en la página Cuentas.

  Para actualizar una sola cuenta, ve a la página de detalles de la cuenta y selecciona Actualizar cuenta. Las cuentas también se pueden actualizar mediante un proceso manual, al seleccionar Volver a registrar la OU, o mediante un método de creación de scripts automatizado, como se describe en una sección posterior de esta página.
- Una actualización completa: una actualización completa incluye una actualización de su zona de inicio, seguida de una actualización de todas las cuentas inscritas en su unidad organizativa registrada. Se requieren actualizaciones completas con una nueva versión de AWS Control Tower, como 2.9, 3.0, etc.

> **Note**
>
> Tras completar una actualización de landing zone, no podrás deshacer la actualización ni bajar a una versión anterior.

Actualizar la zona de inicio

La forma más sencilla de actualizar la zona de aterrizaje de la Torre de Control de AWS es a través de la página de configuración de la zona de aterrizaje, a la que puede acceder seleccionando la configuración de la zona de aterrizaje en la barra de navegación izquierda del panel de control de AWS Control Tower.

La página de configuración de la zona de aterrizaje te muestra la versión actual de tu landing zone y muestra todas las versiones actualizadas que puedan estar disponibles. Puede elegir el botón Update (Actualizar) si necesita actualizar su versión.

> **Note**
>
> También puede actualizar su zona de inicio manualmente. La actualización tarda aproximadamente el mismo tiempo, tanto si utiliza el botón Update (Actualizar) como el proceso manual. Para realizar una actualización manual solo de la zona de inicio, consulte los pasos 1 y 2 siguientes.

Actualizaciones manuales

El siguiente procedimiento explica los pasos de una actualización completa de AWS Control Tower de forma manual. Para actualizar una cuenta individual, consulteActualiza la cuenta en la consola.

Para actualizar tu landing zone manualmente, con cualquier número de cuentas por unidad organizativa

1. Abra un navegador web y diríjase a la consola de la Torre de Control de AWS en https://console.aws.amazon.com/controltower/home/update.
2. Revise la información en el asistente y elija Update (Actualizar). Esto actualiza el backend de la landing zone, así como las cuentas compartidas. Este proceso puede tardar un poco más de media hora.

3. Actualice las cuentas de sus miembros (debe seguir este procedimiento en el caso de una OU que contenga más de 300 cuentas).
4. En el panel de navegación izquierdo, elija Organización.
5. Para actualizar cada cuenta, siga los pasos que se indican enActualiza la cuenta en la consola.

> Si lo desea, vuelva a registrar OU para actualizar las cuentas
>
> En el caso de las unidades organizativas de AWS Control Tower registradas con menos de 300 cuentas, puede ir a la página de unidades organizativas del panel de control y seleccionar Volver a registrar la unidad organizativa para actualizar las cuentas de esa unidad organizativa.

Resuelva el problema con Restablecer y volver a registrar

La deriva suele producirse cuando tú y los miembros de tu organización utilizáis la landing zone.

La detección de desviaciones es automática en AWS Control Tower. Los escaneos automatizados de sus SCP le ayudan a identificar los recursos que necesitan cambios o las actualizaciones de configuración que deben realizarse para resolver el problema.

Para reparar la mayoría de los tipos de desviación, selecciona Restablecer en la página de configuración de la zona de aterrizaje. Además, puedes resolver algunos tipos de deriva si decides volver a registrar una unidad organizativa. Para obtener más información sobre los tipos de deriva y cómo resolverlos, consulte Tipos de desviaciones de gobernanza yDetecte y resuelva desviaciones en la Torre de Control de AWS.

Un caso especial de resolución de desviaciones es el de las desviaciones de rol. Si un rol obligatorio no está disponible, la consola muestra una página de advertencia y algunas instrucciones sobre cómo restaurar el rol. Tu landing zone no estará disponible hasta que se resuelva el cambio de roles. Este restablecimiento de deriva no es lo mismo que un restablecimiento completo de la zona de landing zone. Para obtener más información, consulte No eliminar los roles obligatorios en la sección denominadaTipos de deriva que se deben resolver de inmediato.

⚠ Cuando tomas medidas para resolver la deriva en una versión de landing zone, es posible que se produzcan dos comportamientos.

- Si utiliza la versión más reciente de landing zone, al seleccionar Restablecer y, a continuación, elegir Confirmar, los recursos de la zona de aterrizaje a la deriva se restablecerán a la configuración guardada de la Torre de Control de AWS. La versión de landing zone sigue siendo la misma.
- Si no tienes la última versión, debes elegir Actualizar. La zona de aterrizaje se ha actualizado a la última versión de la zona de aterrizaje. La deriva se resuelve como parte de este proceso.

Aprovisione y actualice las cuentas mediante la automatización

Puede aprovisionar o actualizar cuentas individuales en AWS Control Tower mediante varios métodos:

- Puede aprovisionar y personalizar cuentas con AWS Control Tower Account Factory for Terraform (AFT). Para obtener más información, consulte Descripción general de AWS Control Tower Account Factory para Terraform (AFT).
- Puede actualizar las cuentas con las personalizaciones de AWS Control Tower (cFCT). Para obtener más información, consulte Descripción general de las personalizaciones de AWS Control Tower (cFCT) .
- Automatización de scripts: si prefiere utilizar un enfoque de API, puede actualizar las cuentas mediante el marco de API de Service Catalog y AWS CLI actualizar las cuentas en un proceso por lotes. Llamarías a la `UpdateProvisionedProduct`API de Service Catalog para cada cuenta. Puede escribir un script para actualizar las cuentas, una por una, con esta API. Encontrará más información sobre este enfoque al añadir regiones para la gobernanza en una entrada de blog titulada Enabling guardrails in new AWS Regions.

  Puede actualizar hasta cinco (5) cuentas a la vez. Debe esperar a que al menos una actualización de la cuenta se realice correctamente antes de iniciar la siguiente actualización de la cuenta. Por lo tanto, el proceso puede tomar mucho tiempo si tiene muchas cuentas, pero no es complicado. Para obtener más información acerca de este enfoque, consulte Tutorial: Automatice el aprovisionamiento de cuentas en AWS Control Tower mediante las API de Service Catalog.

Tutorial en vídeo

Tutorial en vídeoEstá diseñado para el aprovisionamiento automático de cuentas mediante un script, pero los pasos también se aplican a la actualización de la cuenta. Usa la `UpdateProvisionedProduct` API en lugar de la `ProvisionProduct` API.

Otro paso de la automatización mediante script consiste en comprobar si el evento del `UpdateLandingZone` ciclo de vida de la Torre de Control de AWS está exitoso. Úselo como activador para empezar a actualizar las cuentas individuales, tal y como se describe en el vídeo. Un evento del ciclo de vida marca la finalización de una secuencia de actividades, por lo que la aparición de este evento significa que se ha completado la actualización de la zona de landing zone. La actualización de la zona de inicio debe estar completa antes de que comiencen las actualizaciones de la cuenta. Para obtener más información acerca de cómo trabajar con eventos del ciclo de vida, consulte Eventos del ciclo de vida.

Consulte también:

- AWS CloudShell Utilización para trabajar con AWS Control Tower.
- Automatice las tareas en AWS Control Tower .

Automatice las tareas en AWS Control Tower

Muchos clientes prefieren automatizar las tareas en AWS Control Tower, como el aprovisionamiento de cuentas, la asignación de controles y la auditoría. Puede configurar estas acciones automatizadas con llamadas a:

- AWS Service Catalog API
- AWS Organizations API
- API de AWS Control Tower
- la AWS CLI

La Información relacionada página contiene enlaces a numerosas publicaciones de blog técnicas excelentes que pueden ayudarle a automatizar las tareas en AWS Control Tower. En las secciones siguientes se proporcionan enlaces a áreas de esta guía del usuario de AWS Control Tower que pueden ayudarle a automatizar las tareas.

Automatizar las tareas de control

Puede automatizar las tareas relacionadas con la aplicación y la eliminación de controles (también conocidos como barandas) a través de la API de AWS Control Tower. Para obtener más información, consulte la referencia de la API de AWS Control Tower.

Para obtener más información sobre cómo realizar operaciones de control con las API de AWS Control Tower, consulte la entrada del blog AWS Control Tower lanza API, controles predefinidos para sus unidades organizativas.

Automatizar las tareas de landing zone

Las API de zonas de aterrizaje de AWS Control Tower le ayudan a automatizar determinadas tareas relacionadas con su zona de aterrizaje. Para obtener más información, consulte la referencia de la API de AWS Control Tower.

Automatizar el registro de la OU

Las API de referencia de AWS Control Tower le ayudan a automatizar determinadas tareas, como el registro de una OU. Para obtener más información, consulte la referencia de la API de AWS Control Tower.

Cierre automático de cuentas

Puede automatizar el cierre de las cuentas de los miembros de la Torre de Control de AWS con una AWS Organizations API. Para obtener más información, consulte Cierre una cuenta de miembro de AWS Control Tower mediante AWS Organizations.

Aprovisionamiento y actualización automatizados de cuentas

AWS Control Tower Account Factory Customization (AFC) le ayuda a crear cuentas desde la consola de AWS Control Tower, con AWS CloudFormation plantillas personalizadas que denominamos blueprints. Este proceso está automatizado, en el sentido de que puede crear cuentas nuevas y actualizarlas repetidamente, tras configurar un único plan, sin necesidad de mantener los procesos.

AWS Control Tower Account Factory for Terraform (AFT) sigue un GitOps modelo para automatizar los procesos de aprovisionamiento y actualización de cuentas en AWS Control Tower. Para obtener más información, consulte Aprovisione cuentas con AWS Control Tower Account Factory for Terraform (AFT) .

Las personalizaciones de AWS Control Tower (cFCT) le ayudan a personalizar la zona de aterrizaje de AWS Control Tower y a seguir las prácticas AWS recomendadas. Las personalizaciones se implementan con AWS CloudFormation plantillas y políticas de control de servicios (SCP). Para obtener más información, consulte Descripción general de las personalizaciones de AWS Control Tower (cFCT) .

Para obtener más información y un vídeo sobre el aprovisionamiento automatizado de cuentas, consulte Tutorial: Aprovisionamiento automatizado de cuentas en AWS Control Tower y Aprovisionamiento automatizado con funciones de IAM.

Consulte también Actualizar cuentas mediante un script.

Auditoría programática de cuentas

Para obtener más información sobre la auditoría de cuentas mediante programación, consulte Funciones programáticas y relaciones de confianza para la cuenta de auditoría de AWS Control Tower.

Automatizar otras tareas

Para obtener información sobre cómo aumentar determinadas cuotas de servicio de la Torre de Control de AWS con un método de solicitud automatizado, consulte este vídeo: Automatice los aumentos de los límites de servicio.

Para ver blogs técnicos sobre casos de uso de automatización e integración, consulte Automatización e integración.

Hay dos ejemplos de código abierto disponibles GitHub para ayudarle con determinadas tareas de automatización relacionadas con la seguridad.

- El ejemplo denominado aws-control-tower-org-setup-sample muestra cómo automatizar la configuración de la cuenta de auditoría como administradora delegada de los servicios relacionados con la seguridad.
- El ejemplo denominado aws-control-tower-account- setup-using-step-functions muestra cómo automatizar las mejores prácticas de seguridad mediante Step Functions al aprovisionar y configurar cuentas nuevas. En este ejemplo, se incluyen la adición de directores a AWS Service Catalog carteras compartidas por la organización y la asociación automática de grupos del Centro de Identidad de IAM de toda la organización a nuevas cuentas AWS . También se muestra cómo eliminar la VPC predeterminada en cada región.

La arquitectura AWS de referencia de seguridad incluye ejemplos de código para automatizar las tareas relacionadas con AWS Control Tower. Para obtener más información, consulte las páginas de orientación AWS prescriptiva y el repositorio asociado GitHub .

Para obtener información sobre el uso de AWS Control Tower con AWS CloudShell un AWS servicio que facilita el trabajo en la AWS CLI, consulte AWS CloudShell y la AWS CLI.

Dado que AWS Control Tower es una capa de orquestación para AWS Organizations, hay muchos otros AWS servicios disponibles mediante las API y la AWS CLI. Para obtener más información, consulte AWS Servicios relacionados.

AWS CloudShell Utilización para trabajar con AWS Control Tower

AWS CloudShell es un AWS servicio que facilita el trabajo en la AWS CLI: es un shell preautenticado y basado en un navegador que se puede iniciar directamente desde. AWS Management ConsoleNo es necesario descargar ni instalar herramientas de línea de comandos. Puedes ejecutar AWS CLI comandos AWS Control Tower y otros AWS servicios desde el shell que prefieras (Bash PowerShell o Z shell).

Cuando lo AWS CloudShell ejecutas desde AWS Management Console, las AWS credenciales que utilizaste para iniciar sesión en la consola están disponibles en una nueva sesión de shell. Puedes omitir la introducción de tus credenciales de configuración cuando interactúes con AWS Control Tower otros AWS servicios y utilizarás la AWS CLI versión 2, que viene preinstalada en el entorno informático del shell. AWS CloudShell

Obtener permisos de IAM para AWS CloudShell

AWS Identity and Access Management proporciona recursos de administración de acceso que permiten a los administradores conceder permisos de acceso a los usuarios de IAM y a los usuarios del Centro de Identidad de IAM. AWS CloudShell

La forma más rápida de que un administrador conceda acceso a los usuarios es mediante una AWS política gestionada. Una política administrada deAWS es una política independiente creada y administrada por AWS. La siguiente política AWS gestionada para se CloudShell puede adjuntar a las identidades de IAM:

- `AWSCloudShellFullAccess`: Concede permiso de uso AWS CloudShell con acceso completo a todas las funciones.

Si desea limitar el alcance de las acciones con las que puede realizar un usuario de IAM o un usuario del Centro de Identidad de IAM AWS CloudShell, puede crear una política personalizada que utilice la política `AWSCloudShellFullAccess` gestionada como plantilla. Para obtener más información sobre cómo limitar las acciones que están disponibles para los usuarios CloudShell, consulte Administrar el AWS CloudShell acceso y el uso con políticas de IAM en laAWS CloudShell Guía del usuario.

> **Note**
>
> Su identidad de IAM también requiere una política que otorgue permiso para realizar llamadas a. AWS Control TowerPara obtener más información, consulte Permisos necesarios para usar la AWS Control Tower consola.

Interactuar con AWS Control Tower el uso AWS CloudShell

Después AWS CloudShell de iniciarlo desde AWS Management Console, puede empezar a interactuar inmediatamente con él AWS Control Tower desde la interfaz de línea de comandos. AWS CLI los comandos funcionan de forma estándar en CloudShell.

> **Note**
>
> AWS CLI Al usarlo AWS CloudShell, no es necesario descargar ni instalar ningún recurso adicional. Ya te has autenticado en el shell, por lo que no necesitas configurar las credenciales antes de realizar llamadas.

Lanzamiento AWS CloudShell

- Desde el AWS Management Console, puede iniciar CloudShell seleccionando las siguientes opciones disponibles en la barra de navegación:
  - Selecciona el CloudShell icono.
  - Comience a escribir «cloudshell» en el cuadro de búsqueda y, a continuación, elija la CloudShell opción.

  Ahora que ha empezado CloudShell, puede introducir cualquier AWS CLI comando con AWS Control Towerel que necesite trabajar. Por ejemplo, puedes comprobar tu AWS Config estado.

Se utiliza AWS CloudShell para ayudar a configurar AWS Control Tower

Antes de realizar estos procedimientos, a menos que se indique lo contrario, debe iniciar sesión AWS Management Console en la región de origen de su zona de aterrizaje y debe iniciar sesión como usuario del IAM Identity Center o usuario de IAM con permisos administrativos para la cuenta de administración que contiene su zona de aterrizaje.

1. A continuación, te explicamos cómo puedes usar los comandos AWS Config CLI AWS CloudShell para determinar el estado de tu grabadora de configuración y canal de entrega antes de empezar a configurar tu AWS Control Tower landing zone.

   Compruebe su AWS Config estado

   Comandos de visualización:

   - `aws configservice describe-delivery-channels`
   - `aws configservice describe-delivery-channel-status`
   - `aws configservice describe-configuration-recorders`
   - `The normal response is something like "name": "default"`

2. Si ya tienes una AWS Config grabadora o un canal de entrega que debes eliminar antes de configurar tu AWS Control Tower landing zone, puedes introducir estos comandos:

   Administra tus recursos preexistentes AWS Config

   Comandos de eliminación:

   - `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

   > **Important**
   >
   > No elimine los AWS Control Tower recursos de AWS Config. La pérdida de estos recursos puede AWS Control Tower provocar que entren en un estado incoherente.

   Para obtener más información, consulte la documentación de AWS Config.

   - Administración del grabador de configuración (CLI de AWS)
   - Administrar el canal de entrega

3. En este ejemplo, se muestran los comandos de AWS CLI que debe introducir AWS CloudShell para habilitar o deshabilitar el acceso de confianza AWS Organizations. Como AWS Control Tower no es necesario activar o desactivar el acceso de confianza AWS Organizations, este es solo un ejemplo. Sin embargo, es posible que tengas que habilitar o deshabilitar el acceso de confianza para otros AWS servicios si vas a automatizar o personalizar las acciones en ellos. AWS Control Tower

   Activa o desactiva el acceso a servicios de confianza

   - `aws organizations enable-aws-service-access`
   - `aws organizations disable-aws-service-access`

Cree un bucket de Amazon S3 con AWS CloudShell

En el siguiente ejemplo, puede utilizar AWS CloudShell para crear un bucket de Amazon S3 y, a continuación, utilizar el PutObjectmétodo para añadir un archivo de código como objeto en ese bucket.

1. Para crear un bucket en una AWS región específica, introduzca el siguiente comando en la línea de CloudShell comandos:

   ```
   aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
   ```

   Si la llamada se realiza correctamente, la línea de comandos muestra una respuesta del servicio similar a la siguiente salida:

   ```
   {
       "Location": "/insert-unique-bucket-name-here"
   }
   ```

   > **Note**
   >
   > Si no sigue las reglas para asignar nombres a los depósitos (por ejemplo, utilizando solo letras minúsculas), aparecerá el siguiente error: Se produjo un error (InvalidBucketName) al llamar a la CreateBucket operación: El depósito especificado no es válido.

2. Para cargar un archivo y añadirlo como un objeto al depósito que se acaba de crear, llama al método: PutObject

   ```
   aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
    add_prog.py
   ```

   Si el objeto se carga correctamente en el bucket de Amazon S3, la línea de comandos muestra una respuesta del servicio similar a la siguiente salida:

   ```
   {
              "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
   ```

`ETag`Es el hash del objeto que se ha almacenado. Se puede utilizar para comprobar la integridad del objeto cargado en Amazon S3.

Creación de AWS Control Tower recursos con AWS CloudFormation

AWS Control Tower está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Cree una plantilla que describa todos los AWS recursos que desee, `AWS::ControlTower::EnabledControl` por ejemplo, los controles. AWS CloudFormation aprovisiona y configura esos recursos por usted.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los AWS Control Tower recursos de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varias Cuentas de AWS regiones.

AWS Control Tower y AWS CloudFormation plantillas

Para aprovisionar y configurar recursos AWS Control Tower y servicios relacionados, debe conocer AWS CloudFormation las plantillas. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus AWS CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation ? en la Guía del usuario de AWS CloudFormation .

AWS Control Tower permite crear `AWS::ControlTower::EnabledControl` (controlar los recursos), `AWS::ControlTower::LandingZone` (zonas de aterrizaje) y `AWS::ControlTower::EnabledBaseline` (líneas base) en. AWS CloudFormationPara obtener más información, incluidos ejemplos de plantillas JSON y YAML para estos tipos de recursos, consulta la Guía del AWS Control TowerAWS CloudFormation usuario.

> **Note**
>
> El límite `EnableControl` y las `DisableControl` actualizaciones AWS Control Tower son de 100 operaciones simultáneas, y hasta 20 de esas operaciones están relacionadas con los controles proactivos.

Para ver algunos AWS Control Tower ejemplos de la CLI y la consola, consulte Habilitar los controles con AWS CloudFormation.

Obtenga más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario
- Referencia de la API de AWS CloudFormation
- AWS CloudFormation Guía del usuario de la interfaz de línea de comandos

Personalice la zona de aterrizaje de su AWS Control Tower

Algunos aspectos de la zona de aterrizaje de la AWS Control Tower se pueden configurar en la consola, como la selección de regiones y los controles opcionales. Se pueden realizar otros cambios fuera de la consola, con automatización.

Por ejemplo, puede crear personalizaciones más amplias de su zona de aterrizaje con la función Customizations for AWS Control Tower, un marco de personalización de GitOps estilo que funciona con AWS CloudFormation plantillas y eventos del ciclo de vida de AWS Control Tower.

Personalice desde la consola de AWS Control Tower

Para realizar estas personalizaciones en su landing zone, siga los pasos que se indican en la consola de AWS Control Tower.

Seleccione nombres personalizados durante la configuración

- Puede seleccionar los nombres de sus unidades organizativas de nivel superior durante la configuración. Puede cambiar el nombre de las unidades organizativas en cualquier momento mediante la AWS Organizations consola, pero si las modifica, es AWS Organizations posible que se produzcan desviaciones reparables.
- Puede seleccionar los nombres de sus cuentas compartidas de Audit y Log Archive, pero no puede cambiarlos después de la configuración. (Esta selección se realiza una sola vez).

> **Sugerencia**
>
> Recuerde que cambiar el nombre de una OU AWS Organizations no actualiza el producto aprovisionado correspondiente en Account Factory. Para actualizar automáticamente el producto aprovisionado (y evitar desviaciones), debe realizar la operación de la OU a través de AWS Control Tower, lo que incluye crear, eliminar o volver a registrar una OU.

Seleccione regiones AWS

- Puedes personalizar tu landing zone seleccionando AWS regiones específicas para su gobierno. Siga los pasos de la consola de la Torre de Control de AWS.

- Puedes seleccionar y deseleccionar AWS regiones para su gobierno al actualizar tu landing zone.
- Puede configurar el control de denegación regional como Habilitado o No habilitado, y controlar el acceso de los usuarios a la mayoría de los AWS servicios en las regiones no gobernadas AWS .

Para obtener información sobre las Regiones de AWS limitaciones de implementación de cFCT, consulte. Limitaciones de control

Personalice añadiendo controles opcionales

- Los controles opcionales y altamente recomendados son opcionales, lo que significa que puedes personalizar el nivel de cumplimiento de tu landing zone eligiendo cuáles quieres habilitar. Los controles opcionales no están activados de forma predeterminada.
- Los controles de residencia de datos opcionales le permiten personalizar las regiones en las que almacena sus datos y permitir el acceso a ellos.
- Los controles opcionales que forman parte del estándar Security Hub integrado le permiten escanear el entorno de la Torre de Control de AWS para comprobar si hay riesgos de seguridad.
- Los controles proactivos opcionales le permiten comprobar sus AWS CloudFormation recursos antes de aprovisionarlos para asegurarse de que los nuevos recursos cumplen con los objetivos de control de su entorno.

Personaliza tus rutas AWS CloudTrail

- Al actualizar su landing zone a la versión 3.0 o posterior, puede optar por participar o excluirse de las CloudTrail rutas a nivel de organización gestionadas por AWS Control Tower. Puedes cambiar esta selección cada vez que actualices tu landing zone. AWS Control Tower crea un registro a nivel de organización en su cuenta de administración y ese registro pasa al estado activo o inactivo, según su elección. La zona de aterrizaje 3.0 no admite CloudTrail senderos a nivel de cuenta; sin embargo, si los necesita, puede configurar y administrar sus propios senderos. Si se duplican los senderos, es posible que tengas que pagar un coste adicional.

Cree cuentas de miembros personalizadas en la consola

- Puede crear cuentas de miembros de la Torre de Control de AWS personalizadas y actualizar las cuentas de miembros existentes para añadir personalizaciones desde la consola de la Torre de Control de AWS. Para obtener más información, consulte Personaliza las cuentas con Account Factory Customization (AFC).

Automatice las personalizaciones fuera de la consola de la Torre de Control de AWS

Algunas personalizaciones no están disponibles a través de la consola de la Torre de Control de AWS, pero se pueden implementar de otras formas. Por ejemplo:

- Puede personalizar las cuentas durante el aprovisionamiento, siguiendo un flujo de trabajo GitOps similar, con Account Factory for Terraform (AFT).

  AFT se implementa con un módulo Terraform, disponible en el repositorio AFT.

- Puede personalizar la zona de aterrizaje de la Torre de Control de AWS con Customizations for AWS Control Tower (cFCT), un paquete de funciones que se basa en AWS CloudFormation plantillas y políticas de control de servicios (SCP). Puede implementar las plantillas y políticas personalizadas en cuentas individuales y unidades organizativas (OU) de su organización.

  El código fuente de cFCT está disponible en un GitHub repositorio.

Ventajas de las personalizaciones para AWS Control Tower (cFCT)

El paquete de funciones que denominamos Personalizaciones para la Torre de Control de AWS (cFCT) le ayuda a crear personalizaciones más amplias para su zona de aterrizaje que las que puede crear en la consola de AWS Control Tower. Ofrece un proceso automatizado y GitOps estilizado. Puedes remodelar tu landing zone para adaptarla a las necesidades de tu empresa.

Este proceso de infrastructure-as-codepersonalización integra las AWS CloudFormation plantillas con las políticas de control de AWS servicios (SCP) y los eventos del ciclo de vida de AWS Control Tower, de modo que sus despliegues de recursos permanezcan sincronizados con su landing zone. Por ejemplo, cuando crea una cuenta nueva con Account Factory, los recursos adjuntos a la cuenta y a la OU se pueden implementar automáticamente.

> **Note**
>
> A diferencia de Account Factory y AFT, cFCT no está diseñado específicamente para crear nuevas cuentas, sino para personalizar las cuentas y unidades organizativas en tu landing zone mediante el despliegue de los recursos que tú especifiques.

Ventajas

- Amplíe un AWS entorno personalizado y seguro: puede ampliar su entorno de AWS Control Tower multicuenta con mayor rapidez e incorporar las AWS mejores prácticas en un flujo de trabajo de personalización repetible.
- Cree una instancia de sus requisitos: puede personalizar la zona de aterrizaje de AWS Control Tower para adaptarla a las necesidades de su empresa, con las AWS CloudFormation plantillas y las políticas de control de servicios que expresan sus intenciones políticas.
- Automatice aún más con los eventos del ciclo de vida de AWS Control Tower: los eventos del ciclo de vida le permiten implementar recursos en función de la finalización de una serie de eventos anterior. Puede confiar en que un evento del ciclo de vida le ayudará a implementar recursos en cuentas y unidades organizativas de forma automática.
- Amplíe su arquitectura de red: puede implementar arquitecturas de red personalizadas que mejoren y protejan su conectividad, como una puerta de enlace de tránsito.

Ejemplos adicionales de cFCT

- En la entrada del blog sobre AWS arquitectura titulada Implemente un DNS coherente con las personalizaciones de Service Catalog y AWS Control Tower, se ofrece un ejemplo de uso de redes con personalizaciones para AWS Control Tower (cFCT) y AWS Control Tower.
- Un ejemplo específico relacionado con cFCT y Amazon GuardDuty está disponible GitHub en el `aws-samples`repositorio.
- Hay ejemplos de código adicionales relacionados con cFCT como parte de la arquitectura de referencia de AWS seguridad, en el `aws-samples` repositorio. Muchos de estos ejemplos contienen `manifest.yaml` archivos de muestra en un directorio denominado`customizations_for_aws_control_tower`.

Para obtener más información sobre la arquitectura AWS de referencia de seguridad, consulte las páginas de orientación AWS prescriptiva.

Descripción general de las personalizaciones de AWS Control Tower (cFCT)

Las personalizaciones de AWS Control Tower (cFCT) le ayudan a personalizar la zona de aterrizaje de AWS Control Tower y a mantenerse al día con las prácticas AWS recomendadas. Las

personalizaciones se implementan con AWS CloudFormation plantillas y políticas de control de servicios (SCP).

Esta capacidad de cFCT está integrada con los eventos del ciclo de vida de AWS Control Tower, de modo que sus despliegues de recursos permanecen sincronizados con su landing zone. Por ejemplo, cuando se crea una nueva cuenta a través de Account Factory, todos los recursos asociados a la cuenta se implementan automáticamente. Puedes implementar las plantillas y políticas personalizadas en cuentas individuales y unidades organizativas (OU) de tu organización.

En el siguiente vídeo, se describen las prácticas recomendadas para implementar una canalización de cFCT escalable y las personalizaciones de cFCT más habituales.

En la siguiente sección, se describen las consideraciones arquitectónicas y los pasos de configuración para implementar las personalizaciones de AWS Control Tower (cFCT). Incluye un enlace a la AWS CloudFormationplantilla que lanza, configura y ejecuta los AWS servicios necesarios, de acuerdo con las prácticas AWS recomendadas de seguridad y disponibilidad.

Este tema está dirigido a arquitectos y desarrolladores de infraestructuras de TI que tengan experiencia práctica en la arquitectura en la AWS nube.

Para obtener información sobre las actualizaciones y los cambios más recientes en las personalizaciones de AWS Control Tower (cFCT), consulte el archivo ChangeLog.md del repositorio. GitHub

Información general de la arquitectura

La implementación de cFCT crea el siguiente entorno en la AWS nube.

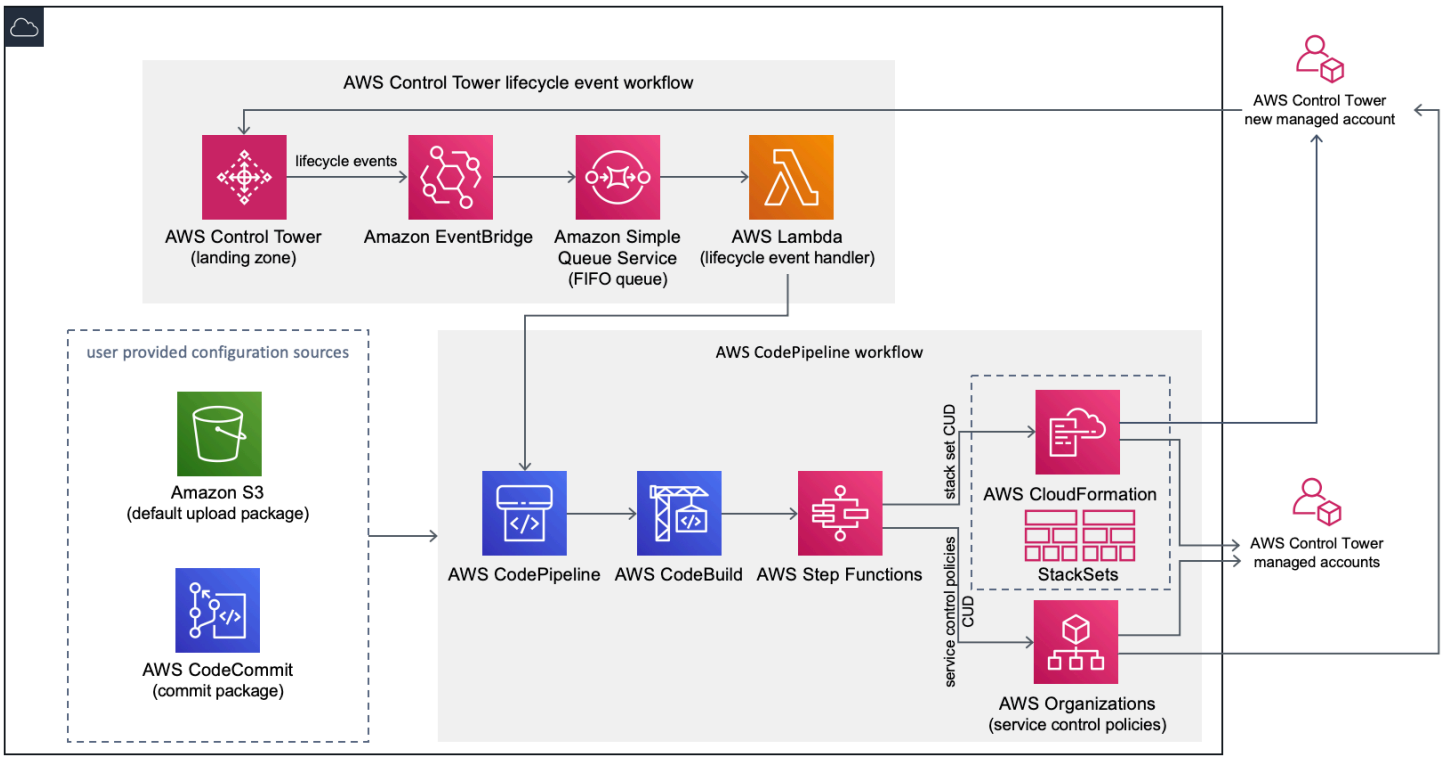


Figura 1: Personalizaciones de la arquitectura de la Torre de Control de AWS

cFCT incluye una AWS CloudFormation plantilla que puede implementar en su cuenta de administración de AWS Control Tower. La plantilla incluye todos los componentes necesarios para crear los flujos de trabajo, de forma que pueda personalizar su zona de aterrizaje de AWS Control Tower.

> **Nota**
>
> cFCT debe implementarse en la región de origen de la Torre de Control de AWS y en la cuenta de administración de la Torre de Control de AWS, ya que ahí es donde se implementa la zona de aterrizaje de la Torre de Control de AWS. Para obtener información sobre la configuración de una zona de aterrizaje de la Torre de Control de AWS, consulteIntroducción.

A medida que se implementa cFCT, este empaqueta y carga los recursos personalizados en el código fuente de la canalización, mediante Amazon Simple Storage Service (Amazon S3). El proceso de carga invoca automáticamente la máquina de estado de las políticas de control de servicios (SCP) y la máquina de AWS CloudFormation StackSetsestados para implementar las SCP a nivel de unidad organizativa o para implementar instancias apiladas a nivel de unidad organizativa o de cuenta.

> **Nota**
>
> De forma predeterminada, cFct crea un bucket de Amazon S3 para almacenar la fuente de la canalización, pero puede cambiar la ubicación a un AWS CodeCommitrepositorio. Para obtener más información, consulte Configurar Amazon S3 como fuente de configuración.

cFCT implementa dos flujos de trabajo:

- un flujo de trabajo AWS CodePipeline
- y un flujo de trabajo de eventos del ciclo de vida de AWS Control Tower.

El AWS CodePipeline flujo de trabajo

El AWS CodePipeline flujo de trabajo configura AWS CodePipeline, AWS CodeBuildproyecta y organiza AWS Step Functionsla administración y los SCP de AWS CloudFormation StackSets su organización.

Al cargar el paquete de configuración, cFCT invoca la canalización de código para ejecutar tres etapas.

- Fase de compilación: valida el contenido del paquete de configuración mediante AWS CodeBuild.
- Fase SCP: invoca la máquina de estados de la política de control de servicios, que llama a la AWS Organizations API para crear los SCP.
- AWS CloudFormation Stage: invoca la máquina de estados del conjunto de pilas para implementar los recursos especificados en la lista de cuentas u OU, que ha proporcionado en el archivo de manifiesto.

En cada etapa, la canalización de códigos invoca el conjunto de pilas y las funciones de paso de SCP, que implementan conjuntos de pilas y SCP personalizados en las cuentas individuales de destino o en toda una unidad organizativa.

> **Nota**
>
> Para obtener información detallada sobre la personalización del paquete de configuración, consulte. Guía de personalización de cFCT

El flujo de trabajo de eventos del ciclo de vida de AWS Control Tower

Cuando se crea una cuenta nueva en AWS Control Tower, un evento del ciclo de vida puede invocar el AWS CodePipeline flujo de trabajo. Puede personalizar el paquete de configuración a través de este flujo de trabajo, que consiste en una regla de EventBridge eventos de Amazon, una cola de primera entrada, primera salida (FIFO) de Amazon Simple Queue Service (Amazon SQS) y una función. AWS Lambda

Cuando la regla de EventBridge eventos de Amazon detecta un evento del ciclo de vida coincidente, pasa el evento a la cola FIFO de Amazon SQS, invoca la AWS Lambda función e invoca la canalización de código para realizar un despliegue descendente de conjuntos de pilas y SCP.

Costo

El coste de ejecutar cFCT depende del número de AWS CodePipeline ejecuciones, la duración de las AWS CodeBuild ejecuciones, el número y la duración de AWS Lambda las funciones y el número de EventBridge eventos de Amazon publicados. Por ejemplo, si ejecuta 100 compilaciones en un mes con build.general1.small y cada compilación dura cinco minutos, el coste aproximado de ejecutar cFCT es de 3$ al mes. Para obtener todos los detalles, consulta la página web de precios de cada servicio que utilices. AWS

El depósito de Amazon Simple Storage Service (Amazon S3) y los recursos del repositorio basado en Git de CodeCommit AWS se conservan después de eliminar la plantilla para proteger la información de configuración. Según la opción que seleccione, se le cobrará en función de la cantidad de datos almacenados en el bucket de Amazon S3 y del número de solicitudes de Git (no se aplica a los recursos de Amazon S3). Consulte los CodeCommit precios de Amazon S3 y AWS para obtener más información.

Servicios de componentes

Los siguientes AWS servicios son componentes de las personalizaciones de AWS Control Tower (cFCT).

AWS CodeCommit

En función de lo que introduzcas en la AWS CloudFormation plantilla, cFct puede crear un AWS CodeCommitrepositorio con la misma configuración de ejemplo que se explica en la sección Amazon Simple Storage Service.

Para clonar el AWS CodeCommit repositorio cFCT en su ordenador local, debe crear credenciales que le den acceso temporal al repositorio, tal y como se explica en la Guía del AWS CodeCommit usuario. Para obtener información sobre la compatibilidad de las versiones, consulte Configuración para AWS CodeCommit.

AWS CodePipeline

AWS CodePipeline valida, prueba e implementa los cambios en función de las actualizaciones del paquete de configuración, que realizará en el depósito predeterminado de Amazon S3 o en el AWS CodeCommit repositorio. Para obtener más información sobre cómo cambiar el control de la fuente de configuración a AWS CodeCommit, consulte Uso de Amazon S3 como fuente de configuración. La canalización incluye etapas para validar y administrar los archivos y plantillas de configuración, las cuentas principales, las políticas de control de AWS Organizations servicios y AWS CloudFormation StackSets. Para obtener más información sobre las etapas de la canalización, consulte Guía de personalización de cFCT

AWS Key Management Service

CfCT crea una clave de `CustomControlTowerKMSKey` cifrado AWS Key Management Service(AWS KMS). Esta clave se utiliza para cifrar los objetos del bucket de configuración de Amazon S3, la cola de Amazon SQS y los parámetros confidenciales del almacén de parámetros de Systems AWS Manager. De forma predeterminada, solo las funciones aprovisionadas por cFCT tienen permiso para realizar operaciones de cifrado o descifrado con esta clave. Para acceder al archivo de configuración, a la cola FIFO o a los `SecureString` valores del almacén de parámetros, se deben añadir administradores a la política. `CustomControlTowerKMSKey` La rotación automática de claves está habilitada de forma predeterminada.

AWS Lambda

CfCT utiliza AWS Lambda funciones para invocar los componentes de la instalación durante la instalación y el despliegue iniciales de los AWS Organizations SCP durante un evento del AWS CloudFormation StackSets ciclo de vida de la Torre de Control de AWS.

Amazon Simple Notification Service

CfCT puede publicar notificaciones, como la aprobación de canalizaciones, sobre temas de Amazon Simple Notification Service (Amazon SNS) durante el flujo de trabajo. Amazon SNS solo se lanza cuando eliges recibir notificaciones de aprobación de canalización.

Amazon Simple Storage Service

Al implementar cFCT, cFCT crea un bucket de Amazon Simple Storage Service (Amazon S3) con un nombre único:

Ejemplo: nombre del bucket de Amazon S3

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*

El bucket contiene un archivo de configuración de muestra llamado `_custom-control-tower-configuration.zip`

Observe el carácter de subrayado inicial en el nombre del archivo.

Este archivo zip proporciona un ejemplo de manifiesto y las plantillas de ejemplo relacionadas que describen la estructura de carpetas necesaria. Estos ejemplos le ayudan a desarrollar un paquete de configuración para personalizar la zona de aterrizaje de su AWS Control Tower. El ejemplo de manifiesto identifica las configuraciones necesarias para los conjuntos de pilas y las políticas de control de servicios (SCP) que necesitará al implementar las personalizaciones.

Puedes usar este ejemplo de paquete de configuración como modelo para desarrollar y cargar tu paquete personalizado, que activará automáticamente el proceso de configuración de cFCT.

Para obtener información sobre la personalización del archivo de configuración, consulte. Guía de personalización de cFCT

Amazon Simple Queue Service

cFCT utiliza una cola FIFO del Amazon Simple Queue Service (Amazon SQS) para capturar los eventos del ciclo de vida de Amazon. EventBridge Activa una AWS Lambda función que invoca el despliegue de los SCP AWS CodePipeline . AWS CloudFormation StackSets Para obtener más información sobre los SCP, consulte. AWS Organizations

AWS Step Functions

cFCT crea Step Functions para organizar despliegues de personalización. Estas Step Functions traducen los archivos de configuración para implementar las personalizaciones según sea necesario en todos los entornos.

AWS Almacén de parámetros de Systems Manager

AWS Systems Manager Parameter Store almacena los parámetros de configuración de cFCT. Estos parámetros le permiten integrar las plantillas de configuración relacionadas. Por ejemplo, puede configurar cada cuenta para que registre AWS CloudTrail los datos en un bucket centralizado de Amazon S3. Además, el almacén de parámetros de Systems Manager proporciona una ubicación centralizada donde los administradores pueden ver las entradas y los parámetros del cFCT.

Consideraciones sobre la implementación

Asegúrese de lanzar las personalizaciones para la Torre de Control de AWS (cFCT) en la misma cuenta y región en las que está desplegada la zona de aterrizaje de la Torre de Control de AWS; es decir, debe implementarlas en la cuenta de administración de la Torre de Control de AWS de su región de origen de la Torre de Control de AWS. De forma predeterminada, cFct crea y ejecuta el paquete de configuración de landing zone mediante la configuración de una canalización de configuración en esa cuenta y región.

Preparación para la implementación

Dispone de algunas opciones a la hora de preparar la AWS CloudFormation plantilla para la implementación inicial. Puede elegir la fuente de configuración y permitir la aprobación manual de las implementaciones en proceso. En las dos secciones siguientes se explica con más detalle estas opciones.

Elija su fuente de configuración

De forma predeterminada, la plantilla crea un depósito de Amazon Simple Storage Service (Amazon S3) para almacenar el paquete de configuración de muestra en `.zip` un archivo denominado. `_custom-control-tower-configuration.zip` El bucket de Amazon S3 está controlado por versiones y puede actualizar el paquete de configuración según sea necesario. Para obtener información sobre la actualización del paquete de configuración, consulte Uso de Amazon S3 como fuente de configuración.

> **Nota**
>
> El nombre del paquete de configuración de muestra comienza con un carácter de subrayado (_), por lo que no AWS CodePipeline se inicia automáticamente. Cuando haya terminado de personalizar el paquete de configuración, asegúrese de cargar el paquete `custom-`

`control-tower-configuration.zip` sin el carácter de subrayado (_) para poder iniciar la implementación en él. AWS CodePipeline

Puede cambiar la ubicación de almacenamiento del paquete de configuración del bucket de S3 a un repositorio de AWS CodeCommit Git seleccionando la `AWS CodeCommit` opción en el AWS CloudFormation parámetro. Esta opción te permite gestionar fácilmente el control de versiones.

> **Nota**
>
> Cuando utilice el bucket S3 predeterminado, asegúrese de que el paquete de configuración esté disponible como un `.zip` archivo. Cuando utilice el AWS CodeCommit repositorio, asegúrese de que el paquete de configuración esté colocado en el repositorio sin comprimir los archivos. Para obtener información sobre cómo crear y almacenar el paquete de configuración AWS CodeCommit, consulteGuía de personalización de cFCT.

Puede usar el paquete de configuración de ejemplo para crear su propia fuente de configuración personalizada. Cuando esté listo para implementar sus configuraciones personalizadas, cargue manualmente el paquete de configuración, ya sea en el bucket de Amazon S3 o en el AWS CodeCommit repositorio. La canalización comienza automáticamente al cargar el archivo de configuración.

> **Nota**
>
> Cuando se utiliza AWS CodeCommit para almacenar el paquete de configuración, no es necesario comprimirlo. Para obtener información sobre cómo crear y almacenar el paquete de configuración AWS CodeCommit, consulteGuía de personalización de cFCT.

Elija los parámetros de aprobación de la configuración de la canalización

La AWS CloudFormation plantilla ofrece la opción de aprobar manualmente la implementación de los cambios de configuración. De forma predeterminada, la aprobación manual no está habilitada. Para obtener más información, consulte el paso 1. Lanza la pila.

Cuando la aprobación manual está habilitada, el proceso de configuración valida las personalizaciones realizadas en el manifiesto y las plantillas del archivo de la Torre de Control

Tower de AWS y, a continuación, detiene el proceso hasta que se concede la aprobación manual. Tras la aprobación, la implementación pasa a ejecutar las etapas restantes del proceso, según sea necesario, para implementar la funcionalidad de Personalizaciones para la Torre de Control de AWS (cFCT).

Puede usar el parámetro de aprobación manual para impedir que se ejecuten las personalizaciones de la configuración de la Torre de Control de AWS, rechazando el primer intento de ejecución. Este parámetro también le permite validar manualmente las personalizaciones de los cambios de configuración de la Torre de Control de AWS, como control final antes de la implementación.

Para actualizar las personalizaciones de AWS Control Tower

Si ya implementó cFCT anteriormente, debe actualizar la AWS CloudFormation pila para obtener la versión más reciente del marco cFCT. Para obtener más información, consulte Actualizar la pila.

Plantilla y código fuente

Las personalizaciones de AWS Control Tower (cFCT) se implementan en su cuenta de administración después de lanzar la plantilla. AWS CloudFormation Puede descargar la plantilla GitHub y, a continuación, lanzarla desde. AWS CloudFormation

La plantilla customizations-for-aws-control-tower.template implementa lo siguiente:

- AWS CodeBuild Un proyecto
- ¿Un AWS CodePipeline proyecto
- Una EventBridge regla de Amazon
- AWS Lambda funciones
- Una cola de Amazon Simple Queue Service
- Un depósito de Amazon Simple Storage Service con un paquete de configuración de muestra
- AWS Step Functions

> **Note**
>
> Puede personalizar la plantilla en función de sus requisitos específicos.

Repositorio de código fuente

Puedes visitar nuestro GitHub repositorio para descargar las plantillas y los scripts de cFCT y compartir tus personalizaciones de landing zone con otras personas.

Implementación automatizada

Antes de lanzar la implementación automatizada, revise las consideraciones. Siga las step-by-step instrucciones de esta sección para configurar e implementar la solución en su cuenta de administración de AWS Control Tower.

Tiempo de implementación: aproximadamente 15 minutos

Requisitos previos

cFCT debe implementarse en su cuenta de administración de la Torre de Control de AWS y en la región de origen de la Torre de Control de AWS. Si no tiene configurada una landing zone, consulteIntroducción.

Pasos de implementación

El procedimiento para implementar el cFCT consta de dos pasos principales. Para obtener instrucciones detalladas, siga los enlaces de cada paso.

Paso 1. Lanzar la pila de

- Inicie la AWS CloudFormation plantilla en su cuenta de administración.
- Revise los parámetros de la plantilla y ajústelos si es necesario.

Paso 2. Cree un paquete personalizado

- Cree un paquete de configuración personalizado.

> **Important**
>
> Para descargar la AWS CloudFormation plantilla correcta e iniciar cFCT, siga el GitHub enlace que aparece en esta sección. No siga los enlaces anteriores a ningún depósito de S3 especificado anteriormente.

Paso 1. Lanzar la pila de

La AWS CloudFormation plantilla de esta sección implementa las personalizaciones para AWS Control Tower (cFCT) en su cuenta.

> **Nota**
>
> Usted es responsable del costo de los AWS servicios utilizados mientras ejecuta cFCT. Para obtener más información, consulte Costo.

1. Para lanzar las personalizaciones de AWS Control Tower, descargue la plantilla GitHub y ejecútela desde AWS CloudFormation.
2. La plantilla se lanza en la región Este de EE. UU. (Norte de Virginia) de forma predeterminada. Para lanzar cFCT en otra AWS región, utilice el selector de regiones de la barra de navegación de la consola.

   > **Note**
   >
   > cFCT debe lanzarse en la misma región y cuenta en las que implementó la zona de aterrizaje de AWS Control Tower, que es su región de origen.

3. En la página Crear pila, compruebe que la URL de la plantilla correcta aparezca en el cuadro de texto URL y seleccione Siguiente.
4. En la página Especificar los detalles de la pila, asigne un nombre a la pila de cFCT.
5. En Parámetros, revise los siguientes parámetros y modifíquelos en la plantilla, si es necesario.

Configuración de la canalización		
Parámetro	Predeterminado	Descripción
Etapa de aprobación de la tubería	No	Elija si desea cambiar la configuración de la canalización de la etapa de aprobación automática predeterminada a una etapa de aprobación manual. Para obtener

Configuración de la canalización		
Parámetro	Predeterminado	Descripción
		más información, consulte the section called “Guía de personalización de cFCT”.
Dirección de correo electrónico de aprobación de la tubería	<Optional Input>	La dirección de correo electrónico para las notificaciones de aprobación. Para utilizar este parámetro, debe establecer el parámetro Pipeline Approval Stage en`Yes`.
CodePipelineFuente de AWS	`Amazon S3`	La fuente de AWS para ayudarlo CodePipeline a seleccionar dónde almacenar y configurar las personalizaciones de cFCT.
CodeCommit Configuración de AWS		
Parámetro	Predeterminado	Descripción
¿ CodeCommitRepositorio existente?	`No`	Elige si quieres usar un repositorio de CodeCommit Git existente. Si lo deseas`Yes`, debes establecer el parámetro CodePipeline Source en`AWS CodeCommit` .

CodeCommit Configuración de AWS		
Parámetro	Predeterminado	Descripción
CodeCommit Nombre del repositorio	`custom-control-tower-configuration`	El nombre del repositorio de Git. Para usar este parámetro, debe establecer el parámetro AWS CodePipeline Source en`AWS CodeCommit` . Este nombre se usa para crear un nuevo repositorio de Git y debe ser único. Si proporciona el nombre de un repositorio de Git existente, ¿debe configurar el CodeCommit repositorio existente? seleccione Sí e introduzca el nombre exacto de ese repositorio.
CodeCommit Nombre de la sucursal	`main`	La rama de Git donde se guarda el paquete de personalización. Los repositorios de Git pueden tener muchas ramas. Este es el nombre predeterminado que se le da a la rama en el repositorio de Git. Para usar este parámetro, debes establecer el parámetro CodePipeline Source en`AWS CodeCommit` .

CloudFormation StackSets Configuración de AWS		
Parámetro	Predeterminado	Descripción
Tipo de simultaneidad regional	`PARALLEL`	Seleccione el tipo de simultaneidad de las StackSets operaciones de despliegue en las regiones. Esta configuración se aplica a los flujos de trabajo de creación, actualización y eliminación. Otro valor permitido es`SEQUENTIAL` .
Porcentaje máximo de concurrencia	`100`	El porcentaje máximo de cuentas en las que realizar esta operación de una vez. El valor máximo permitido es 100. Para obtener más información, consulte las opciones de operación del conjunto de pilas.
Porcentaje de tolerancia a fallos	`10`	El porcentaje de cuentas, por región, en las que esta operación de pila puede fallar antes de que AWS la CloudFormation detenga en esa región. El valor mínimo permitido es 0 y el máximo permitido es 100. Para obtener más información, consulte las opciones de operación del conjunto de pilas.

6. Elija Siguiente.
7. En la página Configurar opciones de pila, elija Siguiente.

8. En la página Revisar, revise y confirme la configuración. Asegúrese de marcar la casilla que reconoce que la plantilla puede crear recursos de AWS Identity and Access Management (IAM).
9. Elija Create stack (Crear pila) para implementar la pila.

   Puedes ver el estado de la pila en la AWS CloudFormation consola en la columna Estado. Deberás ver el estado de CREATE_COMPLETE en unos 15 minutos.

Paso 2. Cree un paquete personalizado

Con la versión lanzada, puede añadir personalizaciones a las políticas de control de servicios (SCP) y de zona de aterrizaje de la Torre de Control Control (SCP) de AWS mediante la personalización del paquete de configuración incluido. Para obtener instrucciones detalladas sobre cómo crear un paquete personalizado, consulte la. Guía de personalización de cFCT

> **Nota**
>
> La canalización no se ejecuta sin cargar el paquete de configuración personalizado.

Actualiza la pila

Si ya implementó Customizations for AWS Control Tower (cFCT), siga el procedimiento para actualizar la AWS CloudFormation pila a la versión más reciente del marco cFCT.

> **Important**
>
> Para poder completar el siguiente procedimiento, debe cargar la plantilla más reciente GitHub a un bucket de Amazon Simple Storage Service (Amazon S3). Para obtener instrucciones sobre cómo empezar a utilizar Amazon S3, consulte Introducción a Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

1. Inicie sesión en la consola deAWS CloudFormation.
2. Seleccione la CloudFormation pila de personalizaciones existentes para AWS Control Tower (cFCT) y, a continuación, seleccione Actualizar.
3. En Requisito previo: preparar la plantilla, seleccione Reemplazar la plantilla actual.

4. En Especificar plantilla, haga lo siguiente:

   a. En Fuente de plantilla, seleccione Reemplazar plantilla actual.

   b. Para la URL de Amazon S3, introduzca la URL de la plantilla desde la que cargó anteriormente GitGub a Amazon S3 y, a continuación, seleccione Siguiente.

   c. Compruebe que la URL de la plantilla sea correcta. A continuación, vuelva a seleccionar Siguiente y Siguiente.

5. En Parámetros, revise los parámetros de la plantilla y modifíquelos según sea necesario. Consulte el paso 1. Inicie la pila para obtener detalles sobre los parámetros.

6. Elija Siguiente.

7. En la página Configurar opciones de pila, elija Siguiente.

8. En la página Revisar, revise y confirme la configuración. Asegúrese de marcar la casilla para confirmar que la plantilla podría crear recursos AWS Identity and Access Management (IAM).

9. Seleccione Ver conjunto de cambios y verifique los cambios.

10. Seleccione Crear pila para implementar la pila.

    Puedes ver el estado de la pila en la AWS CloudFormation consola, en la columna Estado. Deberás ver el estado de UPDATE_COMPLETE en aproximadamente 15 minutos.

Eliminación de un conjunto de pilas

Puedes eliminar un conjunto de pilas si has habilitado la eliminación del conjunto de pilas en el archivo de manifiesto. De forma predeterminada, el parámetro `enable_stack_set_deletion` está definido como `false`. En esta configuración, no se realiza ninguna acción para eliminar el conjunto de pilas asociado cuando se elimina un recurso del archivo de manifiesto de cFCT.

Si cambias el valor de `enable_stack_set_deletion` a `true` en el archivo de manifiesto, cFct elimina el conjunto de pilas y todos sus recursos al eliminar un recurso asociado del archivo de manifiesto.

Esta capacidad se admite en la versión 2 del archivo de manifiesto.

> **Important**
>
> Si estableces inicialmente el valor de `enable_stack_set_deletion` en`true`, la próxima vez que invoques cFct, se eliminarán por etapas TODOS los recursos que comiencen por el

prefijo`CustomControlTower-`, que tengan la etiqueta `Key:AWS_Solutions, Value: CustomControlTowerStackSet` clave asociada y que no estén declarados en el archivo de manifiesto.

Este es un ejemplo de cómo configurar este parámetro en un archivo: `manifest.yaml`

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality


resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - us-west-2

  - name: demo_resource_2
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - eu-north-1
```

Configure Amazon S3 como fuente de configuración

Al configurar las personalizaciones para AWS Control Tower, esta almacena un archivo de configuración inicial, denominado `_custom-control-tower-configuration.zip` file, en un

bucket de Amazon Simple Storage Service (Amazon S3), denominado. `custom-control-tower-configuration-account-ID-region`

> **Nota**
>
> Si decide descargar y modificar este archivo, recuerde comprimir los cambios, guardarlos con un nuevo nombre ycustom-control-tower-configuration.zip, a continuación, volver a cargarlos en el mismo bucket de Amazon S3.
> El bucket de Amazon S3 es la fuente predeterminada de la canalización. Cuando se haya establecido la configuración predeterminada, al cargar un archivo zip de configuración sin el prefijo de subrayado en el nombre del archivo en el bucket de S3, se iniciará la canalización automáticamente.

El archivo zip está protegido mediante el cifrado del lado del servidor (SSE) con AWS Key Management Service (AWS KMS) y se deniega el uso de la clave KMS. Para acceder al archivo zip, debe actualizar la política de claves de KMS para especificar los roles a los que se debe conceder el acceso. El rol puede ser un rol de administrador, un rol de usuario o ambos. Siga este procedimiento:

1. Vaya a la consola deAWS Key Management Service.
2. En Claves gestionadas por el cliente, seleccione CustomControlTowerKMSKey.
3. Seleccione la pestaña Política clave. A continuación, selecciona Editar.
4. En la página Editar política clave, busca la sección Permitir el uso de la clave en el código y añade uno de los siguientes permisos:
   - Para añadir una función de administración:

     `arn:aws:iam::<account-ID>:role/<administrator-role>`
   - Para añadir un usuario:

     `arn:aws:iam::<account-ID>:user/<username>`
5. Seleccione Save Changes (Guardar cambios).
6. Navegue hasta la consola de Amazon S3, busque el bucket de S3 que contiene el archivo zip de configuración y seleccione descargar.
7. Realice los cambios de configuración necesarios en el archivo de manifiesto y en los archivos de plantilla. Para obtener información sobre la personalización de los archivos de manifiesto y plantilla, consultethe section called “Guía de personalización de cFCT”.

8. Cargue sus cambios:

   a. Comprima los archivos de configuración modificados y asigne un nombre al archivo:`custom-control-tower-configuration.zip`.

   b. Cargue el archivo en Amazon S3 mediante SSE con la AWS KMS clave maestra:. `CustomControlTowerKMSKey`

Recopilación de métricas operativas

Las personalizaciones de AWS Control Tower (cFCT) incluyen una opción para enviar métricas operativas anónimas a. AWS AWS utiliza estos datos para comprender cómo utilizan los clientes el cFCT, así como otros servicios y productos relacionados. Cuando la recopilación de datos está habilitada, se envía la siguiente información a AWS:

- ID de solución: el identificador de la AWS solución
- ID único (UUID): identificador único generado aleatoriamente para cada implementación
- Timestamp: timestamp de recopilación de datos
- Recuento de ejecuciones de la máquina de estado: cuenta de forma incremental el número de veces que se ejecuta esta máquina de estado
- Versión del manifiesto: la versión del manifiesto utilizada en la configuración

> **Note**
>
> AWS es propietario de los datos que recopila. La recopilación de datos está sujeta a la AWS Política de privacidad.

Para dejar de enviar métricas operativas anónimas a AWS, complete una de las siguientes tareas:

- Actualice la sección AWS CloudFormation de mapeo de plantillas de la siguiente manera:

  de

```
AnonymousData:
     SendAnonymousData:
        Data: Yes
```

De a

```
AnonymousData:
     SendAnonymousData:
        Data: No
```

- Una vez desplegado cFCT, busque la clave del parámetro **`/org/primary/metrics_flag`** SSM en la consola del almacén de parámetros y actualice el valor a. **`No`**

Guía de personalización de cFCT

La guía de personalizaciones para la Torre de Control de AWS (cFCT) está destinada a administradores, DevOps profesionales, proveedores de software independientes, arquitectos de infraestructuras de TI e integradores de sistemas que desean personalizar y ampliar sus entornos de torres de control de AWS para su empresa y sus clientes. Proporciona información sobre cómo personalizar y ampliar el entorno de la Torre de Control de AWS con el paquete de personalización cFCT.

> **Note**
>
> Para implementar y configurar (cFCT), debe implementar y procesar un paquete de configuración de forma completa. AWS CodePipeline En las siguientes secciones se describe el proceso en detalle.

Descripción general de la canalización de

El paquete de configuración requiere Amazon Simple Storage Service (Amazon S3 AWS CodePipeline) y. El paquete de configuración contiene los siguientes elementos:

- Un archivo de manifiesto
- Un conjunto de plantillas adjunto
- Otros archivos JSON para describir e implementar las personalizaciones del entorno de la Torre de Control de AWS

De forma predeterminada, el paquete de `_custom-control-tower-configuration.zip` configuración se carga en un bucket de Amazon S3 con la siguiente convención de nomenclatura:

`custom-control-tower-configuration-accountID-region`.

> **Note**
>
> De forma predeterminada, cFct crea un bucket de Amazon S3 para almacenar la fuente de la canalización, pero puede cambiar la ubicación de la fuente a un AWS CodeCommit repositorio. Para obtener más información, consulte Editar una canalización CodePipeline en la Guía del AWS CodePipeline usuario.

El archivo de manifiesto es un archivo de texto que describe los AWS recursos que puedes implementar para personalizar tu landing zone. CodePipeline realiza las siguientes tareas:

- extrae el archivo de manifiesto, el conjunto de plantillas adjunto y otros archivos JSON
- realiza validaciones de manifiestos y plantillas
- invoca secciones del archivo de manifiesto para ejecutar etapas de canalización específicas.

Al actualizar el paquete de configuración personalizando el archivo de manifiesto y quitando el carácter de subrayado (_) del nombre del archivo del paquete de configuración, se inicia automáticamente. AWS CodePipeline

> **Note**
>
> El nombre del archivo del paquete de configuración de ejemplo comienza con un carácter de subrayado (_) para que no AWS CodePipeline se active automáticamente. Cuando haya completado la personalización del paquete de configuración, cargue el archivo `custom-control-tower-configuration.zip` sin el carácter de subrayado (_) para activar el despliegue en él. AWS CodePipeline

AWS CodePipeline etapas

La canalización de cFCT requiere varias AWS CodePipeline etapas para implementar y actualizar su entorno de AWS Control Tower.

1. Etapa de origen

La etapa de origen es la etapa inicial. Su paquete de configuración personalizado inicia esta etapa de canalización. El origen de AWS CodePipeline puede ser un bucket de Amazon S3 o un AWS CodeCommit repositorio en el que se pueda alojar el paquete de configuración.

2. Etapa de compilación

   La etapa de compilación requiere AWS CodeBuild validar el contenido del paquete de configuración. Estas comprobaciones incluyen probar la sintaxis y el esquema del `manifest.yaml` archivo, junto con todas las AWS CloudFormation plantillas incluidas en el paquete o alojadas de forma remota, mediante AWS CloudFormation `validate-template` y`cfn_nag`. Si el archivo de manifiesto y AWS CloudFormation las plantillas superan las pruebas, la canalización pasa a la siguiente fase. Si las pruebas fallan, puedes revisar los CodeBuild registros para identificar el problema y editar el archivo fuente de configuración según sea necesario.

3. Etapa de aprobación manual (opcional)

   La etapa de aprobación manual es opcional. Si habilita esta etapa, proporciona un control adicional sobre el proceso de configuración. Hace una pausa en la canalización durante el despliegue, hasta que se dé la aprobación. Puede optar por la aprobación manual editando el parámetro Pipeline Approval Stage en Sí al lanzar la pila.

4. Etapa de política de control de servicios

   La etapa de política de control de servicios invoca la máquina de estados de la política de control de servicios para llamar a AWS Organizations las API que crean políticas de control de servicios (SCP).

5. Etapa CloudFormation de recursos de AWS

   La etapa de AWS CloudFormation recursos invoca la máquina de estados del conjunto de pilas para implementar los recursos especificados en la lista de cuentas o unidades organizativas (OU) que proporcionaste en el archivo de manifiesto. La máquina de estados crea los AWS CloudFormation recursos en el orden en que se especifican en el archivo de manifiesto, a menos que se especifique una dependencia de recursos.

Defina una configuración personalizada

Definirá la configuración personalizada de AWS Control Tower con el archivo de manifiesto, el conjunto de plantillas adjunto y otros archivos JSON. Empaquetará estos archivos en una estructura

de carpetas y los colocará en el bucket de Amazon S3 como un `.zip` archivo, como se muestra en el siguiente ejemplo de código.

Estructura de carpetas de configuración personalizada

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
   - template files for AWS CloudFormation Resources (*.template)
```

El ejemplo anterior describe la estructura de una carpeta de configuración personalizada. La estructura de carpetas permanece igual tanto si elige Amazon S3 como un AWS CodeCommit repositorio como ubicación de almacenamiento de origen. Si elige Amazon S3 como almacenamiento de origen, comprima todas las carpetas y archivos en un `custom-control-tower-configuration.zip` archivo y cargue solo el `.zip` archivo en el bucket de Amazon S3 designado.

> **Note**
>
> Si lo está utilizando AWS CodeCommit, coloque los archivos en el repositorio sin comprimirlos en zip.

El archivo de manifiesto

El `manifest.yaml` archivo es un archivo de texto que describe sus AWS recursos. En el siguiente ejemplo, se muestra la estructura del archivo de manifiesto.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP policies
...
```

Como se muestra en el ejemplo de código anterior, las dos primeras líneas del archivo de manifiesto especifican los valores de la región y las palabras clave de la versión. Estas son las definiciones de esas palabras clave.

region: cadena de texto para la región predeterminada de la Torre de Control de AWS. Este valor debe ser un nombre de AWS región válido (como `us-east-1eu-west-1`, `oap-southeast-1`). La región de origen de la Torre de Control de AWS es la predeterminada al crear recursos personalizados de la Torre de Control de AWS (como AWS CloudFormation StackSets), a menos que se especifique una región más específica de los recursos.

```
region:your-home-region
```

versión: el número de versión del esquema del manifiesto. La última versión compatible es el 15 de marzo de 2021.

```
version: 2021-03-15
```

> **Note**
>
> Le recomendamos encarecidamente que utilice la última versión. Para actualizar las propiedades del manifiesto en la última versión, consulteActualizaciones de versiones de Manifest.

La siguiente palabra clave que se muestra en el ejemplo anterior es la palabra clave resources. La sección de recursos del archivo de manifiesto está muy estructurada. Contiene una lista detallada de AWS los recursos, que la canalización de cFCT desplegará automáticamente. Estas descripciones de los recursos y sus parámetros disponibles se proporcionan en la siguiente sección.

La sección de recursos del archivo de manifiesto

En este tema se describe la sección de recursos del archivo de manifiesto, donde definirá los recursos necesarios para las personalizaciones. Esta sección del archivo de manifiesto comienza en los recursos de palabras clave y continúa hasta el final del archivo.

La sección de recursos del archivo de manifiesto especifica los AWS CloudFormation StackSets AWS Organizations SCP, que CFCT despliega automáticamente a través de la canalización de código. Puede enumerar las unidades organizativas, las cuentas y las regiones para implementar instancias apiladas.

Las instancias apiladas se implementan a nivel de cuenta en lugar de a nivel de unidad organizativa. Los SCP se implementan a nivel de la unidad organizativa. Para obtener más información, consulte Cree sus propias personalizaciones.

La siguiente plantilla de ejemplo describe las posibles entradas que están disponibles para la sección de recursos del archivo de manifiesto.

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
        - OuName1
        - OuName2
    deploy_method: scp | stack_set
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
        parameter_value: [String]
    export_outputs: # list of ssm parameters to store output values
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions: #list of strings
    - [String]
```

En el resto de este tema, se proporcionan definiciones detalladas de las palabras clave que se muestran en el ejemplo de código anterior.

nombre: el nombre que está asociado a AWS CloudFormation StackSets. La cadena que proporciones asigna un nombre más fácil de usar a un conjunto de pilas.

- Tipo: cadena
- Obligatorio: sí
- Valores válidos: a-z, A-Z, 0-9 y un guión bajo (_). Cualquier otro carácter se sustituye automáticamente por un guión bajo (_).

descripción: descripción del recurso.

- Tipo: cadena
- Obligatorio: no

resource_file: este archivo se puede especificar como la ubicación relativa al archivo de manifiesto, un URI o URL de Amazon S3 que apunta a una AWS CloudFormation plantilla o política de control de AWS Organizations servicios en JSON para crear AWS CloudFormation recursos o SCP.

- Tipo: cadena
- Obligatorio: sí

1. En el siguiente ejemplo`resource_file`, se muestra la ubicación relativa al archivo de recursos del paquete de configuración.

```
resources:
  - name: SecurityRoles
    resource_file: templates/custom-security.template
```

2. El siguiente ejemplo muestra el archivo de recursos proporcionado como URI de Amazon S3.

```
resources:
  - name: SecurityRoles
    resource_file: s3://bucket-name/[key-name]
```

3. El siguiente ejemplo muestra el archivo de recursos proporcionado como URL HTTPS de Amazon S3.

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Si proporciona una URL de Amazon S3, compruebe que la política de bucket permita el acceso de lectura a la cuenta de administración de AWS Control Tower desde la que va a implementar cFCT. Si proporciona una URL HTTPS de Amazon S3, compruebe que la ruta utilice notación de puntos. Por ejemplo, `S3.us-west-1`. cFct no admite puntos de enlace que contengan un trazo entre S3 y la región, por ejemplo. `S3-us-west-2`

4. El siguiente ejemplo muestra una política de bucket de Amazon S3 y un ARN donde se almacenan los recursos.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
         "Effect": "Allow",
         "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::my-bucket/*”
        }
    ]
}
```

Sustituirá la *AccountId*variable que se muestra en el ejemplo por el ID de AWS cuenta de la cuenta de administración que está implementando cFCT. Para ver más ejemplos, consulta los ejemplos de políticas de buckets en la Guía del usuario de Amazon Simple Storage Service.

parámetros: especifica el nombre y el valor de los AWS CloudFormation parámetros.

- Tipo: MapList
- Obligatorio: no

La sección de parámetros contiene pares de parámetros clave/valor. La siguiente pseudoplantilla describe la sección de parámetros.

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- parameter_key: la clave asociada al parámetro.
  - Tipo: cadena
  - Obligatorio: Sí (en la propiedad de parámetros)
  - Valores válidos: a-z, A-Z y 0-9
- parameter_value: el valor de entrada asociado al parámetro.
  - Tipo: cadena
  - Obligatorio: Sí (en la propiedad de parámetros)

deploy_method: el método de despliegue para implementar los recursos en la cuenta. Actualmente, deploy_method admite el despliegue de recursos mediante la `stack_set` opción de despliegue de recursos mediante AWS CloudFormation StackSets o la `scp` opción si se están implementando SCP.

- Tipo: cadena
- Valores válidos: `stack_set` | `scp`
- Obligatorio: sí

deployment_targets : lista de cuentas o unidades organizativas (OU) en las que CfCT desplegará los AWS CloudFormation recursos, especificadas como cuentas o unidades_organizativas.

> **Note**
>
> Si desea implementar un SCP, el destino debe ser una OU, no una cuenta.

- Tipo: lista de cadenas `account name` o `account number` para indicar que este recurso se implementará en la lista de cuentas determinada, o `OU names` para indicar que este recurso se implementará en la lista de unidades organizativas determinada.
- Obligatorio: al menos una de las cuentas o unidades organizativas
  - cuentas:

    Tipo: lista de cadenas `account name` o `account number` para indicar que este recurso se implementará en la lista de cuentas determinada.
  - unidades_organizativas:

    Tipo: lista de cadenas `OU names` para indicar que este recurso se implementará en una lista de unidades organizativas determinada. Si proporciona una unidad organizativa que no contiene cuentas y la propiedad de las cuentas no se agrega, cFct solo crea el conjunto de pilas.

    > **Note**
    >
    > El ID de la cuenta de administración de la organización no es un valor permitido. cFct no admite la implementación de instancias apiladas en la cuenta de administración de la organización.

export_outputs: lista de pares de nombre/valor que indican las claves de los parámetros del SSM. Estas claves de parámetros SSM permiten almacenar los resultados de la plantilla en el almacén de parámetros SSM. El resultado está pensado como referencia para otros recursos, definidos anteriormente en el archivo de manifiesto.

```
export_outputs: # List of SSM parameters
  - name: [String]
    value: [String]
```

- Tipo: lista de pares de claves de nombre y valor. El nombre contiene la `name` cadena de una clave del almacén de parámetros de SSM y el valor contiene la `value` cadena del parámetro.
- Valores válidos: cualquier cadena o `$[output_`*`CfnOutput-Logical-ID`*`]` variable en la que *`CfnOutput-Logical-ID`* corresponda a la variable de salida de la plantilla. Para obtener más información sobre la sección de salidas de una AWS CloudFormation plantilla, consulte Salidas en la Guía del usuario.AWS CloudFormation
- Obligatorio: no

Por ejemplo, el siguiente fragmento de código almacena la variable de `VPCID` salida de la plantilla en la clave de parámetro SSM que recibe su nombre. `/org/member/audit/vpc_id`

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

> **Note**
>
> El nombre de la clave export_outputs puede contener un valor distinto de. `output` Por ejemplo, si el nombre es`/org/environment-name`, el valor puede ser. `production`

regiones: lista de regiones en las que CfCT desplegará las instancias de la AWS CloudFormation pila.

- Escriba: cualquier lista de nombres de regiones AWS comerciales, para indicar que este recurso se implementará en la lista de regiones determinada. Si esta palabra clave no existe en el archivo de manifiesto, los recursos se implementan únicamente en la región de origen.
- Obligatorio: no

Unidad organizativa raíz

Según `organizational_units` la versión V2 del manifiesto (15 de marzo de 2021), cfCT admite Root como valor para una unidad organizativa (OU).

- Si elige el método de implementación `descp`, al agregar Root Under`organizational_units`, AWS Control Tower aplicará las políticas a todas las OU bajo Root. Si elige el método de implementación `destack_set`, al agregar Root under`organizational_units`, cFCT implementará los conjuntos de pilas en todas las cuentas bajo Root que estén inscritas en AWS Control Tower, excepto en la cuenta de administración.
- Según las prácticas recomendadas de AWS Control Tower, la cuenta de administración está destinada únicamente a gestionar las cuentas de los miembros y a efectos de facturación. No ejecute cargas de trabajo de producción en la cuenta de administración de AWS Control Tower.

  De acuerdo con la guía de prácticas recomendadas, la implementación de la Torre de Control de AWS coloca la cuenta de administración en la OU raíz, de modo que tiene acceso completo y no ejecuta recursos adicionales. Por este motivo, la AWSControlTowerExecutionfunción no está implementada en la cuenta de administración.
- Le recomendamos que siga estas prácticas recomendadas para la cuenta de administración. Si tienes un caso de uso específico que requiere implementar conjuntos de pilas en la cuenta de administración, incluye las cuentas como objetivo de implementación y especifica la cuenta de administración. De lo contrario, no incluyas las cuentas como objetivo de despliegue. Debe crear los recursos que faltan, incluidas las funciones de IAM requeridas, en la cuenta de administración.

Para implementar conjuntos de pilas en la cuenta de administración, inclúyalos `accounts` como destino de despliegue y especifique la cuenta de administración. De lo contrario, no incluya las cuentas como destino de despliegue.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
```

```
        - Root
```

> **Note**
>
> La función Root OU solo se admite en la versión V2 del archivo de manifiesto (15 de marzo de 2021). Si agrega Root como unidad organizativa inferior`organizational_units`, no agregue ninguna otra unidad organizativa.

OU anidada

cFct permite incluir una o más unidades organizativas anidadas bajo la `organizational_units` palabra clave en la versión V2 del manifiesto (15 de marzo de 2021).

Se requiere una ruta completa (excluida la raíz) para la OU anidada, con dos puntos como separador entre las OU. Como método de implementación`scp`, AWS Control Tower implementa los SCP en la última OU de la ruta de la OU anidada. Como método de implementación`stack_set`, AWS Control Tower implementa los conjuntos de pilas en todas las cuentas de la última OU de la ruta de la OU anidada.

Por ejemplo, considere la ruta. `OUName1:OUName2:OUName3` La última unidad organizativa de la ruta es`OUName3`. CfCT despliega los SCP `OUName3` y agrupa conjuntos únicamente en todas las cuentas directamente dependientes. `OUName3`

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> La función OU anidada solo se admite en la versión V2 del archivo de manifiesto (15 de marzo de 2021).

Cree sus propias personalizaciones

Para crear sus propias personalizaciones, puede modificar el `manifest.yaml` archivo añadiendo o actualizando políticas de control de servicios (SCP) y recursos. AWS CloudFormation En el caso de los recursos que se deben implementar, puede agregar o eliminar cuentas y unidades organizativas. Puede añadir o modificar las plantillas de las carpetas del paquete, crear sus propias carpetas y hacer referencia a las plantillas o carpetas del `manifest.yaml` archivo.

En esta sección se explican las dos partes principales de la creación de tus propias personalizaciones:

- cómo configurar su propio paquete de configuración para las políticas de control de servicios
- cómo configurar su propio paquete de configuración para conjuntos de AWS CloudFormation pilas

Configure un paquete de configuración para las políticas de control de servicios

En esta sección se explica cómo crear un paquete de configuración para las políticas de control de servicios (SCP). Las dos partes principales de este proceso son (1) preparar el archivo de manifiesto y (2) preparar la estructura de carpetas.

Paso 1: edita el archivo manifest.yaml

Usa el `manifest.yaml` archivo de ejemplo como punto de partida. Introduzca todas las configuraciones necesarias. Añada los `deployment_targets` detalles `resource_file` y.

En el siguiente fragmento se muestra el archivo de manifiesto predeterminado.

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

El valor de `region` se añade automáticamente durante la implementación. Debe coincidir con la región en la que desplegó cFCT. Esta región debe ser la misma que la región de la Torre de Control de AWS.

Para añadir un SCP personalizado en la `example-configuration` carpeta del paquete zip almacenado en el bucket de Amazon S3, abra el `example-manifest.yaml` archivo y comience a editarlo.

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

En el siguiente fragmento se muestra un ejemplo de un archivo de manifiesto personalizado. Puede añadir más de una política en un solo cambio.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

Paso 2: Crear una estructura de carpetas

Puede omitir este paso si utiliza una URL de Amazon S3 para el archivo de recursos y utiliza parámetros con pares clave/valor.

Debe incluir una política SCP en formato JSON para admitir el manifiesto, ya que el archivo de manifiesto hace referencia al archivo JSON. Asegúrese de que las rutas de los archivos coincidan con la información de ruta proporcionada en el archivo de manifiesto.

- Un archivo JSON de políticas contiene los SCP que se van a implementar en las unidades organizativas.

En el siguiente fragmento se muestra la estructura de carpetas del archivo de manifiesto de ejemplo.

```
- manifest.yaml
- policies/
   - block-s3-public.json
```

El siguiente fragmento es un ejemplo de un archivo de políticas. `block-s3-public.json`

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Configure un paquete de configuración para AWS CloudFormation StackSets

En esta sección se explica cómo configurar un paquete de configuración para AWS CloudFormation StackSets. Las dos partes principales de este proceso son: (1) preparar el archivo de manifiesto y (2) actualizar la estructura de carpetas.

Paso 1: editar el archivo de manifiesto existente

Agrega la nueva AWS CloudFormation StackSets información al archivo de manifiesto que editaste anteriormente.

A modo de resumen, el siguiente fragmento contiene el mismo archivo de manifiesto personalizado que se mostró anteriormente para configurar un paquete de configuración para los SCP. Ahora puede seguir editando este archivo para incluir los detalles sobre sus recursos.

```
---
region: us-east-1
version: 2021-03-15

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

El siguiente fragmento muestra un ejemplo de archivo de manifiesto editado que contiene los `resources` detalles. El orden de `resources` determina el orden de ejecución para crear `resources` las dependencias. Puede editar el siguiente archivo de manifiesto de ejemplo de acuerdo con los requisitos de su empresa.

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
```

```
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
regions:
  - region-name
```

En el siguiente ejemplo, se muestra que puede añadir más de un AWS CloudFormation recurso al archivo de manifiesto.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
```

```
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: $[output_TransitGatewayID]
    regions:
      - us-east-1
```

Paso 2: Actualizar la estructura de carpetas

Al actualizar la estructura de carpetas, puede incluir todos los archivos de AWS CloudFormation plantillas auxiliares y los archivos de políticas SCP que se encuentran en el archivo de manifiesto. Compruebe que las rutas de los archivos coincidan con las que se proporcionan en el archivo de manifiesto.

- Un archivo de plantilla contiene los AWS recursos que se van a implementar en las unidades organizativas y las cuentas.
- Un archivo de política contiene los parámetros de entrada utilizados en el archivo de plantilla.

En el siguiente ejemplo, se muestra la estructura de carpetas del archivo de manifiesto de ejemplo creado en el paso 1.

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

El ayudante «alfred» y los archivos de AWS CloudFormation parámetros

cFct le proporciona un mecanismo conocido como alfred helper para obtener el valor de una clave de almacén de parámetros de SSM que está definida en la plantilla. AWS CloudFormation Con el asistente alfred, puede usar valores que están almacenados en el almacén de parámetros del SSM y sin actualizar la plantilla. AWS CloudFormation Para obtener más información, consulte ¿Qué es una plantilla? AWS CloudFormation en la Guía AWS CloudFormation del usuario.

> **Important**
>
> El ayudante de Alfred tiene dos limitaciones. Los parámetros solo están disponibles en la región de origen de la cuenta de administración de la Torre de Control Tower de AWS. Como práctica recomendada, considere la posibilidad de trabajar con valores que no cambien de una instancia de pila a otra. Cuando el asistente «alfred» recupera los parámetros, elige una instancia de pila aleatoria del conjunto de pilas que exporta la variable.

Ejemplo

Suponga que tiene dos AWS CloudFormation conjuntos de pilas. El conjunto de pilas 1 tiene una instancia de pila y se despliega en una cuenta de una región. Crea una Amazon VPC y subredes en una zona de disponibilidad, `VPC ID` y `subnet ID` debe pasarse al conjunto de pilas 2 como valores de parámetros. Antes de que el `VPC ID` y se `subnet ID` pueda pasar al conjunto de pilas 2, el `VPC ID` y `subnet ID` debe almacenarse en el conjunto de pilas 1 utilizando. `AWS::SSM::Parameter` Para obtener más información, consulte `AWS::SSM::Parameter` en la Guía del usuario de AWS CloudFormation .

AWS CloudFormation conjunto de pilas 1:

En el siguiente fragmento, el ayudante de Alfred puede obtener los valores de `VPC ID` y del almacén `subnet ID` de parámetros y pasarlos como entrada a la StackSet máquina de estados.

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
      Value: !Ref MyVpc
```

```
SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
      Type: String
      Value: !Ref MySubnet
```

AWS CloudFormation conjunto de pilas 2:

El fragmento muestra los parámetros que se especifican en el archivo de la AWS CloudFormation pila 2`manifest.yaml`.

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

AWS CloudFormation conjunto de pilas 2.1:

El fragmento muestra que puede enumerar `alfred_ssm` las propiedades para admitir los parámetros de tipo. CommaDelimitedList Para obtener más información, consulte `Parameters` en la Guía del usuario de AWS CloudFormation .

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
        parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
 - "$[alfred_ssm_/availability_zone_2]"
```

Esquema JSON para el paquete de personalización

El esquema JSON del paquete de personalización de cFct se encuentra en el repositorio de código fuente de GitHub. Puedes usar el esquema con muchas de tus herramientas

de desarrollo favoritas y puede que te resulte útil para reducir los errores al crear tu propio `manifest.yaml` archivo.

Actualizaciones de versiones de Manifest

Para obtener información sobre la versión más reciente de Customizations for AWS Control Tower (cFCT), consulte el archivo ChangeLog.md en el repositorio. GitHub

Warning

La versión 2.2.0 de Customizations for AWS Control Tower (cFCT) introdujo un esquema de manifiesto (versión 2021-03-15) para alinearlo con las API de servicios relacionadas. AWS El esquema de manifiesto permite que un único archivo manifest.yaml administre los recursos compatibles (plantillas y SCP) mediante flujos de trabajo disociados.AWS CloudFormation DevOps

Te recomendamos encarecidamente que actualices el esquema del manifiesto de la versión 2020-01-01 a la versión 2021-03-15 o posterior.

cFct sigue siendo compatible con las versiones 2021-03-15 y 2020-01-01 del archivo. `manifest.yaml` No es necesario realizar cambios en la configuración actual. Sin embargo, la versión 2020-01-01 está al final del soporte. Ya no ofrecemos actualizaciones ni añadimos mejoras a la versión 2020-01-01. Las funciones de unidad organizativa raíz y unidad organizativa anidada no son compatibles con la versión 2020-01-01.

Propiedades obsoletas en la versión del manifiesto 2021-03-15:

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

Pasos de actualización obligatorios

Cuando actualices a la versión del esquema de manifiesto (15 de marzo de 2021), estos son los cambios que debes realizar para actualizar tus archivos. En las siguientes secciones, se describen los cambios obligatorios y recomendados para la transición.

Políticas de Organizations

1. Mueva los SCP de organization_policies a los recursos de nueva propiedad.
2. Cambie la propiedad policy_file por la nueva propiedad resource_file.
3. Cambie la propiedad apply_to_accounts_in_ou por la nueva propiedad deployment_targets. La lista de unidades organizativas debe definirse en la subpropiedad organizational_units. La subpropiedad accounts no es compatible con las políticas de la organización.
4. Agregue una nueva propiedad deploy_method con el valor scp.

AWS CloudFormation recursos

1. Mueva los CloudFormation recursos de cloudformation_resources a recursos de nuevas propiedades.
2. Cambie la propiedad template_file por la nueva propiedad resource_file.
3. Cambie la propiedad deploy_to_ou por la nueva propiedad deployment_targets. La lista de unidades organizativas debe definirse en la subpropiedad organizational_units.
4. Cambie la propiedad deploy_to_accounts por la nueva propiedad deployment_targets. La lista de cuentas debe definirse en las cuentas de subpropiedades.
5. Cambie la propiedad ssm_parameters por la nueva propiedad export_outputs.

Pasos de actualización muy recomendables

AWS CloudFormation parámetros

1. Cambie la propiedad parameter_file por nuevos parámetros de propiedad.
2. Elimine la ruta del archivo en el valor de la propiedad parameter_file.
3. Copie la clave y el valor del parámetro del archivo JSON de parámetros existente al nuevo formato de la propiedad de parámetros. Esto le ayudaría a administrarlos en el archivo de manifiesto.

> **Note**
>
> La propiedad parameter_file es compatible con la versión del manifiesto 2021-03-15.

Redes en la Torre de Control de AWS

AWS Control Tower proporciona soporte básico para la creación de redes a través de VPC.

Si la configuración o las capacidades predeterminadas de la VPC de la Torre de Control de AWS no satisfacen sus necesidades, puede utilizar otros AWS servicios para configurar la VPC. Para obtener más información sobre cómo trabajar con las VPC y la AWS Control Tower, consulte Creación de una infraestructura de red multiVPC AWS escalable y segura.

Temas relacionados de

- Para obtener información sobre cómo funciona AWS Control Tower al inscribir cuentas que tienen VPC existentes, consulteInscribir cuentas existentes en VPC.
- Con Account Factory, puede aprovisionar cuentas que incluyan una VPC de AWS Control Tower o puede aprovisionar cuentas sin una VPC. Para obtener información sobre cómo eliminar la VPC de la Torre de Control de AWS o configurar las cuentas de la Torre de Control de AWS sin una VPC, consulte. Tutorial: Configurar la Torre de Control de AWS sin una VPC
- Para obtener información sobre cómo cambiar la configuración de las cuentas de las VPC, consulta la documentación de Account Factory sobre la actualización de una cuenta.
- Para obtener más información sobre cómo trabajar con redes y VPC en AWS Control Tower, consulte la sección sobre redes en la página de información relacionada de esta Guía del usuario.

VPC y AWS regiones en AWS Control Tower

Como parte estándar de la creación de la cuenta, AWS crea una VPC AWS predeterminada en cada región, incluso en las regiones que no gobierna con AWS Control Tower. Esta VPC predeterminada no es la misma que una VPC que AWS Control Tower crea para una cuenta aprovisionada, pero los usuarios de IAM pueden acceder a la AWS VPC predeterminada de una región no gobernada.

Los administradores pueden permitir que la región deniegue el control, de modo que sus usuarios finales no tengan permiso para conectarse a una VPC en una región compatible con AWS Control Tower, pero fuera de las regiones gobernadas. Para configurar la región y denegar el control, vaya a la página de configuración de la zona de destino y seleccione Modificar la configuración.

El control de denegación regional bloquea las llamadas a la API a la mayoría de los servicios no regulados Regiones de AWS. Para obtener más información, consulte Denegar el acceso a en AWS función de la solicitud Región de AWS. .

> **Note**
>
> Es posible que la denegación de control por región no impida que los usuarios de IAM se conecten a una VPC AWS predeterminada en una región en la que no se admite la Torre de Control de AWS.

Si lo desea, puede eliminar las VPC AWS predeterminadas en las regiones no gobernadas. Para enumerar la VPC predeterminada en una región, puede usar un comando CLI similar al de este ejemplo:

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

Información general sobre AWS Control Tower y las VPC

Estos son algunos datos esenciales sobre las VPC de AWS Control Tower:

- La VPC creada por AWS Control Tower al aprovisionar una cuenta en Account Factory no es la misma que la AWS VPC predeterminada.
- Cuando AWS Control Tower configura una nueva cuenta en una AWS región compatible, AWS Control Tower elimina automáticamente la AWS VPC predeterminada y configura una nueva VPC configurada por AWS Control Tower.
- A cada cuenta de AWS Control Tower se le permite una VPC creada por AWS Control Tower. Una cuenta puede tener AWS VPC adicionales dentro del límite de la cuenta.
- Cada VPC de AWS Control Tower tiene tres zonas de disponibilidad en todas las regiones, excepto en la región EE.UU. Oeste (Norte de California)`us-west-1`, y dos zonas de disponibilidad en ellas. `us-west-1` De forma predeterminada, a cada zona de disponibilidad se le asigna una subred pública y dos subredes privadas. Por lo tanto, en las regiones, excepto EE. UU. Oeste (norte de California), cada VPC de la Torre de Control de AWS contiene nueve subredes de forma predeterminada, divididas en tres zonas de disponibilidad. En el oeste de EE. UU. (norte de California), seis subredes se dividen en dos zonas de disponibilidad.
- A cada una de las subredes de la VPC de la Torre de Control de AWS se le asigna un rango único, del mismo tamaño.
- El número de subredes de una VPC se puede configurar. Para obtener más información acerca de cómo cambiar la configuración de la subred de VPC, consulte el tema Account Factory.

- Como las direcciones IP no se superponen, las seis o nueve subredes de su VPC de AWS Control Tower pueden comunicarse entre sí de forma ilimitada.

Cuando se trabaja con VPC, AWS Control Tower no hace distinciones a nivel regional. Cada subred se asigna desde el rango de CIDR exacto que especifique. Las subredes de VPC pueden existir en cualquier región.

Notas

> **Gestione los costes de VPC**
>
> Si configuras la VPC de Account Factory para que las subredes públicas estén habilitadas al aprovisionar una cuenta nueva, Account Factory configura la VPC para crear una puerta de enlace NAT. Amazon VPC le facturará por su uso.

> **Configuración de control y VPC**
>
> Si aprovisiona cuentas de Account Factory con la configuración de acceso a Internet de la VPC habilitada, esa configuración de Account Factory anula el control No permitir el acceso a Internet para una instancia de Amazon VPC gestionada por un cliente. Para evitar habilitar el acceso a Internet para las cuentas recién aprovisionadas, debes cambiar la configuración en Account Factory. Para obtener más información, consulte Tutorial: Configuración de AWS Control Tower sin una VPC.

CIDR e interconexión para VPC y AWS Control Tower

Esta sección está destinada principalmente a los administradores de red. El administrador de red de su empresa suele ser la persona que selecciona el rango general de CIDR para su organización de la Torre de Control de AWS. A continuación, el administrador de red asigna subredes dentro de ese rango para fines específicos.

Cuando elige un rango de CIDR para su VPC, AWS Control Tower valida los rangos de direcciones IP de acuerdo con la especificación RFC 1918. Account Factory permite un bloque CIDR de hasta `/16` los siguientes rangos:

- `10.0.0.0/8`

- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10`(solo si su proveedor de Internet permite el uso de este rango)

El delimitador `/16` permite hasta 65 536 direcciones IP distintas.

Puede asignar cualquier dirección IP válida de los siguientes rangos:

- `10.0.x.x to 10.255.x.x`
- `172.16.x.x - 172.31.x.x`
- `192.168.0.0 - 192.168.255.255` (sin IP fuera del rango `192.168`)

Si el rango que especifica está fuera de estos, la Torre de Control de AWS mostrará un mensaje de error.

El rango de CIDR predeterminado es `172.31.0.0/16`.

Cuando AWS Control Tower crea una VPC con el rango de CIDR que seleccione, asigna el mismo rango de CIDR a cada VPC para cada cuenta que cree en la unidad organizativa (OU). Debido a la superposición predeterminada de direcciones IP, esta implementación inicialmente no permite la interconexión entre ninguna de las VPC de la Torre de Control de AWS en la OU.

Subredes

Dentro de cada VPC, la Torre de Control de AWS divide el rango de CIDR especificado de manera uniforme en nueve subredes (excepto en el oeste de EE. UU. (norte de California), donde hay seis subredes). Ninguna de las subredes de una VPC se solapan. Por lo tanto, todos pueden comunicarse entre sí, dentro de la VPC.

En resumen, de forma predeterminada, la comunicación de subred dentro de la VPC no está restringida. La práctica recomendada para controlar la comunicación entre las subredes de VPC, si es necesario, consiste en configurar listas de control de acceso con reglas que definan el flujo de tráfico permitido. Utilice grupos de seguridad para controlar el tráfico entre instancias específicas. Para obtener más información sobre la configuración de grupos de seguridad y firewalls en AWS Control Tower, consulte Tutorial: Configurar grupos de seguridad en AWS Control Tower con AWS Firewall Manager.

Intercambio de tráfico

AWS Control Tower no restringe la interconexión de VPC a VPC para la comunicación entre varias VPC. Sin embargo, de forma predeterminada, todas las VPC de AWS Control Tower tienen el mismo rango de CIDR predeterminado. Para admitir el emparejamiento, puede modificar el rango CIDR en la configuración de Account Factory para que las direcciones IP no se superpongan.

Si cambia el rango de CIDR en la configuración de Account Factory, a todas las cuentas nuevas que AWS Control Tower cree posteriormente (mediante Account Factory) se les asigna el nuevo rango de CIDR. Las cuentas antiguas no se actualizan. Por ejemplo, puede crear una cuenta y, a continuación, cambiar el rango de CIDR y crear una cuenta nueva, y las VPC asignadas a esas dos cuentas se pueden interconectar. La interconexión es posible porque sus rangos de direcciones IP no son idénticos.

Permisos y roles necesarios

AWS Control Tower utiliza las funciones de IAM para ayudar a administrar el acceso a los recursos.

Para obtener información general sobre las funciones, consulte Grupos de usuarios, funciones y conjuntos de permisos.

Acerca de los permisos

- Para obtener información sobre los grupos de IAM y sus permisos en la Torre de Control de AWS, consulte los grupos del Centro de Identidad de IAM para la Torre de Control de AWS.
- Para obtener información sobre los permisos necesarios para aprovisionar cuentas, consulte Permisos necesarios para las cuentas.
- Para obtener información sobre los permisos de consola necesarios para la Torre de Control de AWS, consulte Permisos necesarios para usar la consola de la Torre de Control de AWS.

Acerca de los roles

- Para obtener información sobre cómo crear un rol, incluidos los permisos diseñados para el acceso mediante programación, consulte Crear roles y asignar permisos y roles programáticos y relaciones de confianza para la cuenta de auditoría de AWS Control Tower.
- Para obtener información sobre otras funciones que AWS Control Tower utiliza para administrar sus cuentas, consulte Uso de políticas basadas en la identidad (políticas de IAM) para la Torre de Control de AWS y Políticas administradas para la Torre de Control de AWS.
- Para obtener información sobre la Torre de Control y AWS Config las funciones de AWS, consulte AWS Control Tower ConfigRecorderRole.
- Para obtener información sobre las funciones que AWS Control Tower utiliza para agregar AWS Config información para sus cuentas, consulte Cómo AWS Control Tower agrega AWS Config reglas en unidades organizativas y cuentas no administradas.
- Para obtener información sobre cómo proteger sus recursos al asignar funciones y permisos, consulte Condiciones opcionales para las relaciones de confianza de sus funciones, Configurar AWS KMS claves de forma opcional y Evitar la suplantación de identidad entre servicios.
- Para obtener información específica sobre el aprovisionamiento automatizado de cuentas en AWS Control Tower con funciones de IAM, consulte Aprovisionamiento automatizado de cuentas con funciones de IAM.

- Para ver la política que protege el tema AWS Config SNS, consulte La política temática SNS. AWS Config

Cómo trabaja AWS Control Tower con los roles para crear y administrar cuentas

En general, los roles forman parte de la gestión de identidades y accesos (IAM) en AWS. Para obtener información general sobre la IAM y las funciones en ella AWS, consulte el tema de las funciones de IAM en la Guía del usuario de AWS IAM.

Creación de roles y cuentas

AWS Control Tower crea la cuenta de un cliente llamando a la `CreateAccount` API de AWS Organizations. Cuando AWS Organizations crea esta cuenta, crea un rol dentro de esa cuenta, al que AWS Control Tower nombra pasando un parámetro a la API. El nombre del rol es `AWSControlTowerExecution`.

AWS Control Tower asume la `AWSControlTowerExecution` función de todas las cuentas creadas por Account Factory. Con esta función, AWS Control Tower establece una base de referencia para la cuenta y aplica los controles obligatorios (y cualquier otro control habilitado), lo que da lugar a la creación de otras funciones. Estos roles, a su vez, los utilizan otros servicios, como. AWS Config

> **Note**
>
> La base de referencia de una cuenta es configurar sus recursos, que incluyen plantillas de Account Factory, a veces denominadas planos, y controles. El proceso de referencia también establece las funciones centralizadas de registro y auditoría de seguridad de la cuenta, como parte de la implementación de las plantillas. Las bases de referencia de AWS Control Tower se incluyen en las funciones que aplica a cada cuenta inscrita.

Para obtener más información sobre las cuentas y los recursos, consulte. Acerca Cuentas de AWS de AWS Control Tower

Explicación de la AWSControlTowerExecution función

El rol `AWSControlTowerExecution` debe estar presente en todas las cuentas inscritas. Permite a AWS Control Tower gestionar sus cuentas individuales y enviar información sobre ellas a sus cuentas de Audit y Log Archive.

El `AWSControlTowerExecution` rol se puede añadir a una cuenta de varias maneras, como se indica a continuación:

- Para las cuentas de la OU de seguridad (a veces denominadas cuentas principales), AWS Control Tower crea el rol en el momento de la configuración inicial de la Torre de Control de AWS.
- En el caso de una cuenta de Account Factory creada a través de la consola de AWS Control Tower, AWS Control Tower crea este rol en el momento de la creación de la cuenta.
- Para la inscripción de una sola cuenta, pedimos a los clientes que creen el rol manualmente y, a continuación, inscriban la cuenta en AWS Control Tower.
- Al extender la gobernanza a una OU, AWS Control Tower usa el StackSet-AWSControlTowerExecutionRole para crear el rol en todas las cuentas de esa OU.

Propósito de la `AWSControlTowerExecution` función:

- `AWSControlTowerExecution`le permite crear e inscribir cuentas automáticamente con scripts y funciones Lambda.
- `AWSControlTowerExecution` le ayuda a configurar el registro de su organización, de modo que todos los registros de cada cuenta se envíen a la cuenta de registro.
- `AWSControlTowerExecution`le permite inscribir una cuenta individual en AWS Control Tower. En primer lugar, debe añadir el `AWSControlTowerExecution` rol a esa cuenta. Para ver los pasos sobre cómo agregar el rol, consulteAñada manualmente el rol de IAM requerido a uno existente Cuenta de AWS e inscríbalo.

Cómo funciona el `AWSControlTowerExecution` rol con las unidades organizativas:

El `AWSControlTowerExecution` rol garantiza que los controles de la Torre de Control de AWS que haya seleccionado se apliquen automáticamente a cada cuenta individual, en cada unidad organizativa, de su organización, así como a cada cuenta nueva que cree en la Torre de Control de AWS. Como resultado:

- Puede proporcionar informes de conformidad y seguridad con mayor facilidad, en función de las funciones de auditoría y registro incorporadas en los controles de la Torre de Control de AWS.
- Los equipos de seguridad y conformidad pueden verificar que se cumplen todos los requisitos y que no se ha producido ninguna desviación organizativa.

Para obtener más información sobre la desviación, consulte Detectar y resolver la desviación en AWS Control Tower.

En resumen, el rol `AWSControlTowerExecution` y su política asociada le brindan un control flexible de la seguridad y el conformidad en toda la organización. Por lo tanto, es menos probable que se produzcan violaciones de la seguridad o del protocolo.

Condiciones opcionales para su función: relaciones de confianza

Puede imponer condiciones en las políticas de confianza de sus funciones para restringir las cuentas y los recursos que interactúan con determinadas funciones en AWS Control Tower. Le recomendamos encarecidamente que restrinja el acceso al `AWSControlTowerAdmin` rol, ya que permite amplios permisos de acceso.

Para evitar que un atacante acceda a sus recursos, edite manualmente la política de confianza de AWS Control Tower para añadir al menos una `aws:SourceArn` `aws:SourceAccount` condición a la declaración de política. Como práctica recomendada de seguridad, recomendamos encarecidamente añadir la `aws:SourceArn` condición, ya que es más específica que `aws:SourceAccount` limitar el acceso a una cuenta y un recurso específicos.

Si no conoce el ARN completo del recurso o si está especificando varios recursos, puede usar la `aws:SourceArn` condición con caracteres comodín (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:controltower:*:123456789012:*` funciona si no desea especificar una región.

El siguiente ejemplo demuestra el uso de la condición de `aws:SourceArn` IAM con las políticas de confianza de su rol de IAM. Añada la condición a su relación de confianza para el AWSControlTowerAdminrol, ya que el director del servicio de la Torre de Control de AWS interactúa con él.

Como se muestra en el ejemplo, el ARN de origen tiene el siguiente formato: `arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:*`

Sustituya las cadenas `${HOME_REGION}` y `${CUSTOMER_AWSACCOUNT_id}` por su propia región de origen y el identificador de cuenta de la cuenta que realiza la llamada.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

En el ejemplo, el ARN de origen designado como `arn:aws:controltower:us-west-2:012345678901:*` es el único ARN permitido para realizar la acción. `sts:AssumeRole` En otras palabras, solo los usuarios que puedan iniciar sesión con el ID `012345678901` de la cuenta en la `us-west-2` región pueden realizar acciones que requieran este rol específico y una relación de confianza para el servicio de la Torre de Control de AWS, denominado como`controltower.amazonaws.com`.

El siguiente ejemplo muestra las `aws:SourceArn` condiciones `aws:SourceAccount` y condiciones que se aplican a la política de confianza del rol.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
```

```
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

El ejemplo ilustra la declaración de `aws:SourceArn` condición, con una declaración de `aws:SourceAccount` condición añadida. Para obtener más información, consulte Evite la suplantación de identidad entre servicios.

Para obtener información general sobre las políticas de permisos de la Torre de Control de AWS, consulteAdministra el acceso a los recursos.

Recomendaciones:

Le recomendamos que añada condiciones a las funciones que crea AWS Control Tower, ya que esas funciones las asumen directamente otros servicios de AWS. Para obtener más información, consulte el ejemplo AWSControlTowerAdminmostrado anteriormente en esta sección. Para la función de AWS Config grabadora, recomendamos añadir la `aws:SourceArn` condición y especificar el ARN de la grabadora Config como el ARN de origen permitido.

Para funciones como AWSControlTowerExecutionlas demás funciones programáticas que puede asumir la cuenta de auditoría de la Torre de Control Tower de AWS en todas las cuentas administradas, le recomendamos que añada la `aws:PrincipalOrgID` condición a la política de confianza de estas funciones, que valida que el principal que accede al recurso pertenece a una cuenta de la organización correcta AWS . No añada la declaración de `aws:SourceArn` condición, ya que no funcionará según lo esperado.

> **Note**
>
> En caso de desviación, es posible que se restablezca una función de la Torre de Control de AWS en determinadas circunstancias. Se recomienda volver a comprobar los roles periódicamente, si los ha personalizado.

Cómo AWS Control Tower agrega AWS Config reglas en unidades organizativas y cuentas no administradas

La cuenta de administración de AWS Control Tower crea un agregador a nivel de organización que ayuda a detectar AWS Config reglas externas, de modo que AWS Control Tower no necesite acceder a cuentas no administradas. La consola de AWS Control Tower le muestra cuántas AWS Config reglas creadas externamente tiene para una cuenta determinada. Puedes ver los detalles sobre esas reglas externas en la pestaña External Config Rule Compliance de la página de detalles de la cuenta.

Para crear el agregador, AWS Control Tower añade un rol con los permisos necesarios para describir una organización y enumerar las cuentas que contiene. El `AWSControlTowerConfigAggregatorRoleForOrganizations` rol requiere una política `AWSConfigRoleForOrganizations` gestionada y una relación de confianza con`config.amazonaws.com`.

Esta es la política de IAM (artefacto JSON) asociada a la función:

```
{
    "Version": "2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
       "Resource": "*"
      }
    ]
  }
```

Esta es la relación de `AWSControlTowerConfigAggregatorRoleForOrganizations` confianza:

```
{
    "Version": "2012-10-17",
      "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
        "Service": "config.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

Para implementar esta funcionalidad en la cuenta de administración, se agregan los siguientes permisos a la política administrada`AWSControlTowerServiceRolePolicy`, que el `AWSControlTowerAdmin` rol utiliza cuando crea el AWS Config agregador:

```
{
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
```

```
    ]
}
```

Se han creado nuevos recursos: `AWSControlTowerConfigAggregatorRoleForOrganizations` y `aws-controltower-ConfigAggregatorForOrganizations`

Cuando esté listo, puede inscribir las cuentas de forma individual o inscribirlas en grupo mediante el registro de una OU. Cuando haya inscrito una cuenta, si crea una regla en ella AWS Config, AWS Control Tower detectará la nueva regla. El agregador muestra el número de reglas externas y proporciona un enlace a la AWS Config consola donde puede ver los detalles de cada regla externa de su cuenta. Utilice la información de la AWS Config consola y de la consola de la Torre de Control Tower de AWS para determinar si tiene habilitados los controles adecuados para la cuenta.

Funciones programáticas y relaciones de confianza para la cuenta de auditoría de la Torre de Control de AWS

Puede iniciar sesión en la cuenta de auditoría y asumir la función de revisar otras cuentas mediante programación. La cuenta de auditoría no le permite iniciar sesión en otras cuentas manualmente.

La cuenta de auditoría le proporciona acceso programático a otras cuentas, mediante algunas funciones que se otorgan únicamente a las funciones de AWS Lambda. Por motivos de seguridad, estas funciones tienen relaciones de confianza con otras funciones, lo que significa que las condiciones en las que se pueden utilizar las funciones están estrictamente definidas.

El conjunto de componentes de AWS Control Tower `StackSet-AWSControlTowerBP-BASELINE-ROLES` crea estas funciones multicuenta únicamente mediante programación en la cuenta de auditoría:

- aws-controltower- AdministratorExecutionRole
- aws-torre de control- AuditAdministratorRole
- aws-torre de control- ReadOnlyExecutionRole
- aws-torre de control- AuditReadOnlyRole

`ReadOnlyExecutionRole:`Tenga en cuenta que esta función permite a la cuenta de auditoría leer los objetos de los buckets de Amazon S3 en toda la organización (a diferencia de la `SecurityAudit` política, que solo permite el acceso a los metadatos).

aws-controltower-: AdministratorExecutionRole

- Tiene permisos de administrador
- No se puede asumir desde la consola
- Solo puede asumirlo un rol en la cuenta de auditoría: el `aws-controltower-AuditAdministratorRole`

El siguiente artefacto muestra la relación de confianza de`aws-controltower-AdministratorExecutionRole`. El número de marcador de posición se `012345678901` sustituirá por el `Audit_acct_ID` número de su cuenta de auditoría.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: AuditAdministratorRole

- Solo puede asumirlo el AWS servicio Lambda
- Tiene permiso para realizar operaciones de lectura (Get) y escritura (Put) en objetos de Amazon S3 con nombres que comiencen por la cadena log

Políticas adjuntas:

1. AWSLambdaExecute— política AWS gestionada

2. AssumeRole-aws-controltower- AuditAdministratorRole — política en línea — Creada por AWS Control Tower, el artefacto sigue a continuación.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
 "Resource": [
   "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
   ],
 "Effect": "Allow"
 }
   ]
}
```

El siguiente artefacto muestra la relación de confianza de: `aws-controltower-AuditAdministratorRole`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: ReadOnlyExecutionRole

- No se puede suponer desde la consola
- Solo puede asumirlo otro rol de la cuenta de auditoría: el `AuditReadOnlyRole`

El siguiente artefacto muestra la relación de confianza de`aws-controltower-ReadOnlyExecutionRole`. El número de marcador de posición se `012345678901` sustituirá por el `Audit_acct_ID` número de su cuenta de auditoría.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: AuditReadOnlyRole

- Solo puede asumirlo el AWS servicio Lambda
- Tiene permiso para realizar operaciones de lectura (Get) y escritura (Put) en objetos de Amazon S3 con nombres que comiencen por la cadena log

Políticas adjuntas:

1. AWSLambdaExecute— política AWS gestionada

2. AssumeRole-aws-controltower- AuditReadOnlyRole — política en línea — Creada por AWS Control Tower, el artefacto sigue a continuación.

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
  "sts:AssumeRole"
 ],
 "Resource": [
  "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
 ],
 "Effect": "Allow"
   }
  ]
}
```

El siguiente artefacto muestra la relación de confianza de: `aws-controltower-AuditAdministratorRole`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Aprovisionamiento automatizado de cuentas con roles de IAM

Para configurar las cuentas de Account Factory de forma más automatizada, puede crear funciones de Lambda en la cuenta de administración de AWS Control Tower, que asume la AWSControlTowerExecutionfunción en la cuenta del miembro. A continuación, utilizando el rol, la cuenta de administración realiza los pasos de configuración deseados en cada cuenta de miembro.

Si aprovisiona cuentas mediante funciones Lambda, la identidad que realizará este trabajo debe tener la siguiente política de permisos de IAM, además de. `AWSServiceCatalogEndUserFullAccess`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetPeregrineStatus",
                "sso:GetApplicationInstance",
```

```
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Control Tower Account Factory requiere `sso:ProvisionSAMLProvide` los permisos `sso:GetPeregrineStatussso:ProvisionApplicationProfileForAWSAccountInstance`, y para interactuar con el AWS IAM Identity Center. `sso:ProvisionApplicationInstanceForAWSAccount`

Recursos en AWS Control Tower

- Para obtener información general sobre la propiedad de los recursos en AWS Control Tower, consulteInformación general sobre la administración de los permisos de acceso a los recursos de la Torre de Control de AWS.
- Para obtener información sobre los recursos que AWS Control Tower crea en las cuentas compartidas, consulteAcerca de las cuentas compartidas.
- Para obtener información sobre los recursos que AWS Control Tower crea cuando aprovisiona una cuenta a través de Account Factory, consulteConsideraciones sobre los recursos para Account Factory.
- Para ver los detalles sobre los tipos de AWS recursos que define la Torre de Control de AWS, para su uso con las API de la Torre de Control de AWS, consulte la referencia sobre los tipos de recursos de la Torre de Control de AWS en la Guía del AWS CloudFormation usuario.

Cómo funcionan AWS las regiones con AWS Control Tower

Actualmente, AWS Control Tower es compatible con las siguientes AWS regiones:

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Oregón)
- Canadá (centro)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Singapur)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europe (London)
- Europa (Estocolmo)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Tokio)
- Europa (París)
- América del Sur (São Paulo)
- Oeste de EE. UU. (Norte de California)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Osaka)
- Europa (Milán)
- África (Ciudad del Cabo)
- Medio Oriente (Baréin)
- Israel (Tel Aviv)
- Medio Oriente (EAU)
- Europa (España)
- Asia-Pacífico (Hyderabad)
- Europa (Zúrich)

- Asia-Pacífico (Melbourne)
- Oeste de Canadá (Calgary)

Acerca de su región de origen

Cuando crea una landing zone, la región que utiliza para acceder a la consola de AWS administración se convierte en su AWS región de origen para AWS Control Tower. Durante el proceso de creación, algunos recursos se aprovisionan en la región de origen. Otros recursos, como las unidades organizativas y AWS las cuentas, son globales.

Una vez que haya seleccionado una región de origen, no podrá cambiarla.

Controles y regiones

En la actualidad, todos los controles preventivos funcionan a nivel mundial. Sin embargo, los controles proactivos y de detección solo funcionan en las regiones en las que se admite AWS Control Tower. Para obtener más información sobre el comportamiento de los controles al activar la Torre de Control de AWS en una nueva región, consulteConfigure sus regiones de AWS Control Tower.

Configure sus regiones de AWS Control Tower

En esta sección se describe el comportamiento que puede esperar al extender la zona de aterrizaje de la Torre de Control de AWS a una nueva AWS región o al eliminar una región de la configuración de la zona de aterrizaje. Por lo general, esta acción se realiza mediante la función de actualización de la consola de la Torre de Control de AWS.

> **Note**
>
> Le recomendamos que evite expandir su zona de aterrizaje de AWS Control Tower a AWS regiones en las que no necesite que se ejecuten sus cargas de trabajo. La exclusión voluntaria de una región no le impide implementar recursos en esa región, pero esos recursos permanecerán fuera de la gobernanza de la Torre de Control de AWS.

Durante la configuración de una nueva región, la Torre de Control de AWS actualiza la zona de aterrizaje, lo que significa que sirve de referencia para su zona de aterrizaje:

- para operar activamente en todas las regiones recién seleccionadas, y

- dejar de gobernar los recursos en las regiones no seleccionadas.

Las cuentas individuales de sus unidades organizativas (OU) administradas por AWS Control Tower no se actualizan como parte de este proceso de actualización de landing zone. Por lo tanto, debe actualizar sus cuentas volviendo a registrar sus OU.

Al configurar las regiones de la Torre de Control de AWS, tenga en cuenta las siguientes recomendaciones y limitaciones:

- Seleccione las regiones en las que planea alojar AWS recursos o cargas de trabajo.
- La exclusión voluntaria de una región no le impide implementar recursos en esa región, pero esos recursos permanecerán fuera de la gobernanza de la Torre de Control de AWS.

Al configurar su landing zone para nuevas regiones, los controles de detección de AWS Control Tower cumplen las siguientes reglas:

- Lo que existe permanece igual. El comportamiento de las medidas de seguridad, tanto de detección como preventivas, no cambia para las cuentas existentes, en las unidades organizativas existentes, en las regiones existentes.
- No puede aplicar nuevos controles de detección a las unidades organizativas existentes que contengan cuentas que no estén actualizadas. Cuando haya configurado la zona de aterrizaje de la Torre de Control de AWS en una nueva región (actualizando la zona de aterrizaje), deberá actualizar las cuentas existentes en las OU existentes antes de poder habilitar nuevos controles de detección en esas OU y cuentas.
- Sus controles de detección actuales comenzarán a funcionar en las regiones recién configuradas en cuanto actualice las cuentas. Cuando actualice la zona de aterrizaje de AWS Control Tower para configurar nuevas regiones y, a continuación, actualice una cuenta, los controles de detección que ya están habilitados en la OU comenzarán a funcionar en esa cuenta en las regiones recién configuradas.

Configuración de las regiones de la Torre de Control de AWS

1. Inicie sesión en la consola de AWS Control Tower en https://console.aws.amazon.com/controltower
2. En el menú de navegación del panel izquierdo, seleccione Configuración de la zona de aterrizaje.

3. En la página de configuración de la zona de aterrizaje, en la sección Detalles, selecciona el botón Modificar la configuración en la esquina superior derecha. Se te redirige al flujo de trabajo de actualización de la zona de aterrizaje, ya que para gobernar nuevas regiones o eliminar regiones de la gobernanza es necesario que actualices a la versión más reciente de la zona de aterrizaje.
4. En AWS Regiones adicionales para la gobernanza, busca las regiones que quieres gobernar (o dejar de gobernar). La columna Estado indica qué regiones gobiernas actualmente y cuáles no.
5. Seleccione la casilla de verificación de cada región adicional que desee gobernar. Desactive la casilla de verificación de cada región de la que vaya a eliminar la gobernanza.

   > **Note**
   >
   > Si opta por no gobernar una región, podrá seguir desplegando recursos en esa región, pero dichos recursos permanecerán fuera de la gobernanza de la Torre de Control de AWS.

6. Completa el resto del flujo de trabajo y, a continuación, selecciona Actualizar landing zone.
7. Cuando se complete la configuración de la landing zone, vuelve a registrar las OU para actualizar las cuentas en tus nuevas regiones. Para obtener más información, consulte Cuándo actualizar las unidades organizativas y las cuentas de AWS Control Tower.

Un método alternativo para aprovisionar o actualizar cuentas individuales después de configurar nuevas regiones consiste en utilizar el marco de API de Service Catalog y AWS CLI actualizar las cuentas en un proceso por lotes. Para obtener más información, consulte Aprovisione y actualice las cuentas mediante la automatización.

Evite la gobernanza mixta al configurar las regiones

Es importante actualizar todas las cuentas de una OU después de extender la gobernanza de la Torre de Control de AWS a una nueva Región de AWS y después de eliminar la gobernanza de la Torre de Control de AWS de una región.

La gobernanza mixta es una situación indeseable que puede producirse si los controles que rigen una OU no coinciden completamente con los controles que rigen cada una de las cuentas de una OU. La gobernanza mixta se produce en una OU si las cuentas no se actualizan después de que AWS Control Tower amplíe la gobernanza a una nueva Región de AWS o la elimine.

En esta situación, determinadas cuentas de una OU pueden tener diferentes controles aplicados en distintas regiones, en comparación con otras cuentas de la OU o con respecto a la postura de gobierno general de la zona de destino.

En una OU con gobierno mixto, si aprovisionas una cuenta nueva, esa nueva cuenta recibe la misma postura de gobierno regional y de OU (actualizada) que la landing zone. Sin embargo, las cuentas existentes que aún no se han actualizado no reciben la postura de gobernanza regional actualizada.

En general, la gobernanza mixta puede crear indicadores de estado contradictorios o imprecisos en la consola de AWS Control Tower. Por ejemplo, durante la gobernanza mixta, las regiones optativas se muestran con el estado No gobernadas, en las unidades organizativas registradas, en el caso de las cuentas que aún no se han actualizado.

> **Note**
>
> AWS Control Tower no permite habilitar los controles durante un estado de gobierno mixto.

Comportamiento de los controles durante la gobernanza mixta

- Durante la gobernanza mixta, AWS Control Tower no puede implementar de manera coherente controles basados en AWS Config reglas (es decir, controles de detección) en regiones que la OU ya muestra como gobernadas, porque algunas cuentas de la OU no se han actualizado. Es posible que reciba un mensaje `FAILED_TO_ENABLE` de error.
- Durante la gobernanza mixta, si se amplía la gobernanza de la zona de destino a una región en la que se haya optado por participar y alguna cuenta de la OU aún no se ha actualizado, el funcionamiento de la `EnableControl` API en la OU no funcionará debido a los controles preventivos y proactivos. Recibirá un mensaje de `FAILED_TO_ENABLE` error porque las cuentas de miembros no actualizadas de la OU aún no se han incluido en esas regiones.
- Durante la gobernanza mixta, controles que forman parte del estándar gestionado por el servicio Security Hub: AWS Control Tower no puede informar de conformidad con precisión en las regiones en las que no hay coincidencia entre la configuración de landing zone y las cuentas que no están actualizadas.
- La gobernanza mixta no modifica el comportamiento de los controles basados en SCP (controles preventivos), que se aplican de manera uniforme a todas las cuentas de una OU y a todas las regiones gobernadas.

> **Note**
>
> La gobernanza mixta no es lo mismo que una deriva, y no se considera una desviación.

Reparar la gobernanza mixta

- Elija Actualizar cuenta para cada cuenta de la OU que muestre el estado Actualizar disponible en la página Organizations de la consola.
- Seleccione Reregistrar la OU en la página Organizations, que actualiza automáticamente todas las cuentas de la OU, para las OU con menos de 300 cuentas.

Consideraciones a la hora de activar las regiones con AWS suscripción

Aunque la mayoría Regiones de AWS están activas de forma predeterminada Cuenta de AWS, algunas regiones solo se activan cuando las seleccionas manualmente. En este documento se hace referencia a esas regiones como regiones de suscripción voluntaria. Por el contrario, las regiones que están activas de forma predeterminada, tan pronto como Cuenta de AWS se crea la suya, se denominan regiones comerciales o, simplemente, regiones.

El término suscripción voluntaria tiene una base histórica. Todas las regiones que Regiones de AWS se introduzcan después del 20 de marzo de 2019 se considerarán regiones de suscripción voluntaria. Las regiones de suscripción voluntaria tienen requisitos de seguridad más estrictos que las regiones comerciales en lo que respecta al intercambio de datos de IAM a través de cuentas que están activas en las regiones de suscripción. Todos los datos gestionados a través del servicio de IAM se consideran datos de identidad, incluidos los usuarios, los grupos, las funciones, las políticas, los proveedores de identidad, sus datos asociados (por ejemplo, los certificados de firma X.509 o las credenciales específicas del contexto) y otros ajustes a nivel de cuenta, como la política de contraseñas y el alias de la cuenta.

Puedes activar automáticamente las regiones de suscripción durante la configuración de la landing zone, seleccionándolas. Tu landing zone se activará en todas las regiones seleccionadas.

Si elige seleccionar una región de suscripción como región de origen de AWS Control Tower, actívela primero siguiendo los pasos que se indican en Habilitar una región cuando haya iniciado sesión en

la consola AWS de administración. Para crear sus propias cuentas de registro, archivado y auditoría existentes de una región que haya optado por participar, active primero esa región manualmente.

Las regiones AWS opcionales incluyen varias regiones en las que AWS Control Tower está disponible:

- Región de Asia Pacífico (Hong Kong), ap-east-1
- Región de Asia Pacífico (Yakarta), ap-southeast-3
- Región Europa (Milán), eu-south-1
- Región de África (Ciudad del Cabo), af-south-1
- Región de Medio Oriente (Bahréin), me-south-1
- Israel (Tel Aviv), il-central-1
- Región de Oriente Medio (EAU), me-central-1
- Región Europa (España), eu-south-2
- Región Asia Pacífico (Hyderabad), ap-south-2
- Región Europa (Zúrich), eu-central-2
- Región Asia Pacífico (Melbourne), ap-southeast-4
- Región Canadá Oeste (Calgary), ca-west-1

AWS Control Tower tiene algunos controles que funcionan de forma diferente en las regiones de suscripción que en las regiones comerciales. Para obtener más información, consulte Limitaciones de control. Estas son algunas consideraciones que debe tener en cuenta al implementar cargas de trabajo en las regiones en las que se ha optado por participar.

> **¿Gobernar o activar?**
>
> Recuerde que gobernar una región es una acción que puede seleccionar en la consola de AWS Control Tower para que los controles se puedan aplicar en la región. Activar o desactivar una región optativa es otra acción que puede elegir en la AWS consola, que abre la región en su cuenta para que pueda implementar recursos y cargas de trabajo en la región.

Consideraciones sobre el comportamiento

- Si decide regir las regiones de suscripción voluntaria, le recomendamos que no desactive (excluya) ninguna de las regiones de suscripción reguladas, ya que esto podría provocar fallos en sus cargas de trabajo. La Torre de Control de AWS no permite la desactivación de una región gobernada desde la consola de la Torre de Control de AWS, pero asegúrese de no desactivar las regiones gobernadas desde una fuente ajena a la Torre de Control de AWS, como la consola de AWS facturación o AWS el SDK.
- Cuando AWS Control Tower extiende la gobernanza a una región de suscripción voluntaria, se activa (opta por participar) en la región en todas las cuentas de los miembros. Al eliminar una región de la gobernanza, AWS Control Tower no desactiva (excluye) la región en las cuentas de los miembros.
- Al anular la selección de una región, AWS Control Tower omite la eliminación de recursos de una región que haya optado por participar si dicha región se desactivó manualmente para una cuenta de una fuente ajena a la Torre de Control de AWS, como la consola de AWS facturación o el SDK. AWS Le recomendamos que elimine los recursos de las regiones que ha desactivado o podría recibir cargos de facturación inesperados por esos recursos.
- Si su landing zone se retira del servicio, AWS Control Tower limpia los recursos de todas las regiones gobernadas, incluidas las regiones en las que se ha optado por participar. Sin embargo, AWS Control Tower no desactiva las regiones de suscripción. Puede desactivar las regiones opcionales como paso adicional tras el desmantelamiento.
- Si tu región de origen es una región de suscripción voluntaria y pretendes inscribir las cuentas existentes como tus cuentas de archivo de registros y auditoría, debes activar manualmente la región de suscripción antes de poder seleccionarla como región de origen para tu landing zone. Consulte Habilitar una región.
- Si AWS Control Tower está configurada con una región opcional como región de origen y si visita el servicio AWS Control Tower desde la consola de cualquier otra región, la AWS consola no lo redireccionará automáticamente a la región de origen.
- La API subyacente tiene límites de capacidad, lo que puede aumentar la latencia de unos minutos a varias horas, en función del número de regiones, cuentas y carga de servicios. Como práctica recomendada, opte solo por aquellas en las que ejecutará las Regiones de AWS cargas de trabajo y opte por una región a la vez.

Limitaciones importantes de la gobernanza y los controles

- Si actualmente ha activado un control de la Torre de Control de AWS que no es compatible en una región de suscripción voluntaria, no podrá extender la gobernanza de la Torre de Control de AWS a esa región de suscripción hasta que el control sea compatible en esa región. Para más información, consulte Limitaciones de control.
- Si extiende la gobernanza de la Torre de Control de AWS a una región opcional en la que no se admite un control específico, no podrá habilitar ese control en ninguna región hasta que el control sea compatible con todas las regiones que gobierna con AWS Control Tower. Para obtener más información, consulte Limitaciones de control
- Si se activan las 22 regiones comerciales en las que está disponible la Torre de Control de AWS, incluidas las regiones con suscripción voluntaria, se reduce el límite máximo de cuentas por unidad organizativa (OU) al extender la gobernanza a una OU. El límite es de 220 en lugar de 300 cuentas. Esta reducción se debe a StackSet limitaciones. Si necesita extender la gobernanza a las unidades organizativas con más de 220 cuentas, reduzca el número de regiones activadas.

Configure la región y deniegue el control

AWS Control Tower ofrece dos controles de denegación por región. Un control`GRREGIONDENY`, cuando está activado, se aplica a toda la landing zone. Otro control`CTMULTISERVICEPV1`, cuando está activado, se puede aplicar a las unidades organizativas específicas que especifique. Para obtener más información, consulte Denegar el acceso en AWS función del control de denegación regional solicitado Región de AWS y aplicado a la OU.

La región deniega el control `GRREGIONDENY` es única, ya que se aplica a la zona de aterrizaje en su conjunto y no a una OU específica. Para configurar el control de denegación regional, vaya a la página de configuración de la zona de aterrizaje y seleccione Modificar la configuración.

- Esta configuración se puede cambiar más adelante.
- Cuando está activado, este control se aplica a todas las unidades organizativas registradas.
- Este control no se puede configurar para unidades organizativas individuales.

> **Note**
>
> Antes de activar el control de denegación regional, asegúrese de que no dispone de recursos en esas regiones, ya que no tendrá acceso a los recursos una vez que haya aplicado el

control. Mientras el control esté activado, no podrás desplegar recursos en las regiones denegadas.

El control de denegación de región prohíbe el acceso a AWS los servicios, según la configuración regional de la Torre de Control de AWS. Denega el acceso a AWS las regiones con el estado No gobernado. La región deniega el control también deniega el acceso a las regiones en las que AWS Control Tower no está disponible. No puede denegar el acceso a su región de origen. Algunos AWS servicios globales, como IAM, están exentos de la región AWS Organizations, deniegan el control. Para obtener más información, consulte Denegar el acceso a en AWS función de la solicitud Región de AWS.

Cuando habilita el control, se aplica a todas las unidades organizativas de nivel superior registradas en su jerarquía y las unidades organizativas más bajas de la cadena lo heredan. Al eliminar el control, se elimina de todas las unidades organizativas registradas, todas las regiones no gobernadas de la Torre de Control de AWS permanecen en el estado No gobernadas y puede implementar recursos en regiones fuera de la disponibilidad de la Torre de Control de AWS.

- Nombre de control total: denegar el acceso en AWS función de la región solicitada AWS
- Descripción de la barrera: no permite el acceso a operaciones no cotizadas en servicios globales y regionales fuera de las regiones especificadas.
- Se trata de un control electivo con orientación preventiva.

Para ver la plantilla del SCP de denegación de control regional, consulte Denegar el acceso a AWS según lo solicitado Región de AWS en la referencia de AWS Control Tower Control. El SCP de la Torre de Control de AWS es similar al SCP AWS Organizations, pero no idéntico.

Puede determinar los puntos de enlace de los servicios regionales en la página de servicios regionales.

Las consideraciones para la región a nivel de la OU niegan el control

La consideración principal sobre el control de denegación de control de región a nivel de OU es determinar cómo interactuará con el control de denegación de control de la región de landing, si ambos están activados. Para obtener más información, consulte el control de denegación regional aplicado a la OU.

Aprovisione y administre cuentas en AWS Control Tower

Este capítulo incluye información general y procedimientos para aprovisionar y administrar las cuentas de los miembros en la zona de aterrizaje de AWS Control Tower.

También incluye información general y procedimientos para inscribir una AWS cuenta existente en AWS Control Tower.

Para obtener más información sobre las cuentas de AWS Control Tower, consulteAcerca Cuentas de AWS de AWS Control Tower. Para obtener información sobre cómo inscribir varias cuentas en AWS Control Tower, consulte. Registrar una unidad organizativa existente en AWS Control Tower

> **Note**
>
> Puede realizar hasta cinco (5) operaciones relacionadas con la cuenta de forma simultánea, como el aprovisionamiento, la actualización y la inscripción.

Métodos de aprovisionamiento

AWS Control Tower proporciona varios métodos para crear y actualizar las cuentas de los miembros. Algunos métodos se basan principalmente en la consola y otros están principalmente automatizados.

Información general

La forma estándar de crear cuentas de miembros es a través de Account Factory, un producto basado en consola que forma parte del Service Catalog. Si su landing zone no se encuentra en un estado de deriva, puede utilizar Crear cuenta como método para añadir nuevas cuentas desde la consola, así como Inscribir una cuenta para inscribir AWS las cuentas existentes en AWS Control Tower.

Con Account Factory, puede aprovisionar cuentas básicas basándose en la configuración predeterminada de AWS Control Tower. También puede aprovisionar cuentas personalizadas que cumplan con los requisitos de casos de uso especializados.

Account Factory Customization (AFC) es una forma de aprovisionar cuentas personalizadas desde la consola de AWS Control Tower y automatiza la personalización y el despliegue de las

cuentas. Permite el aprovisionamiento automatizado y basado en una consola, tras unos pasos de configuración únicos, lo que elimina la necesidad de escribir scripts o configurar canalizaciones. Para obtener más información, consulte Personaliza las cuentas con Account Factory Customization (AFC).

Métodos basados en consolas:

- A través de la consola Account Factory que forma parte AWS Service Catalog, para cuentas básicas o personalizadas. Revisa Aprovisione y administre cuentas con Account Factory los detalles y las instrucciones.
- A través de la función Inscribir una cuenta de AWS Control Tower, si su landing zone no se encuentra en un estado de deriva. Consulte Inscriba una cuenta existente.
- En la consola de AWS Control Tower, puede usar Account Factory para crear, actualizar o inscribir hasta cinco cuentas al mismo tiempo.

Métodos automatizados:

- Código Lambda: desde la cuenta de administración de la zona de aterrizaje de la Torre de Control Tower de AWS, con código Lambda y las funciones de IAM adecuadas. Consulte el aprovisionamiento automatizado de cuentas con funciones de IAM.
- Terraform: de la AWS Control Tower Account Factory for Terraform (AFT), que se basa en Account Factory y en un GitOps modelo que permite la automatización del aprovisionamiento y la actualización de las cuentas. Consulte Aprovisione cuentas con AWS Control Tower Account Factory for Terraform (AFT) .
- Personalización de Account Factory en la consola de AWS Control Tower: Tras los pasos de configuración, el aprovisionamiento futuro de cuentas personalizadas no requiere ninguna configuración adicional ni mantenimiento de la canalización. Las cuentas se aprovisionan mediante un AWS Service Catalog producto denominado blueprint. Un plano puede usar AWS CloudFormation plantillas o plantillas de Terraform.

> **Note**
>
> AWS CloudFormation los planos pueden desplegar recursos en varias regiones. Los planos de Terraform solo pueden desplegar recursos en una sola región. De forma predeterminada, esa es la región de origen.

Qué ocurre cuando AWS Control Tower crea una cuenta

Las nuevas cuentas en AWS Control Tower se crean y, a continuación, se aprovisionan mediante una interacción entre AWS Control Tower AWS Organizations, y AWS Service Catalog. Para ver los pasos para inscribir una empresa existente Cuenta de AWS mediante la consola de la Torre de Control de AWS, consulteInscriba una cuenta existente.

Entre bastidores de la creación de cuentas

1. La solicitud se inicia, por ejemplo, desde la página Account Factory de AWS Control Tower, directamente desde la AWS Service Catalog consola o llamando a la `ProvisionProduct` API de Service Catalog.
2. AWS Service Catalog llama a AWS Control Tower.
3. AWS Control Tower inicia un flujo de trabajo que, como primer paso, llama a la AWS Organizations `CreateAccount` API.
4. Tras AWS Organizations crear la cuenta, AWS Control Tower completa el proceso de aprovisionamiento aplicando planos y controles.
5. Service Catalog continúa sondeando a AWS Control Tower para comprobar si se ha completado el proceso de aprovisionamiento.
6. Cuando se complete el flujo de trabajo en AWS Control Tower, Service Catalog finaliza el estado de la cuenta y le informa a usted (el solicitante) del resultado.

Se requieren permisos para las cuentas

Los permisos necesarios para cada método de aprovisionamiento y actualización de cuentas se describen en cada sección, respectivamente. Con los permisos de grupo de usuarios adecuados, los aprovisionadores pueden especificar líneas base y configuraciones de red estandarizadas para cualquier cuenta de su organización.

> **Note**
>
> Al aprovisionar una cuenta, el solicitante de la cuenta siempre debe tener los permisos y los permisos. `CreateAccount` `DescribeCreateAccountStatus` Este conjunto de permisos forma parte de la función de administrador y se otorga automáticamente cuando el solicitante asume la función de administrador. Si delegas el permiso para aprovisionar cuentas, es posible que tengas que añadir estos permisos directamente a los solicitantes de la cuenta.

Al crear cuentas desde la consola de la Torre de Control de AWS con Account Factory, debe iniciar sesión en una cuenta con un usuario de IAM que tenga la `AWSServiceCatalogEndUserFullAccess` política habilitada, junto con permisos para usar la consola de la Torre de Control de AWS, y no puede iniciar sesión como usuario root.

Para obtener información general sobre los permisos necesarios en la Torre de Control de AWS, consulteUso de políticas basadas en identidad (políticas de IAM) para AWS Control Tower. Para obtener información sobre las funciones y las cuentas en AWS Control Tower, consulte Funciones y cuentas.

> **Seguridad para sus cuentas**
>
> Puede encontrar orientación sobre las prácticas recomendadas para proteger la seguridad de su cuenta de administración de AWS Control Tower y las cuentas de los miembros en la AWS Organizations documentación.
>
> - Prácticas recomendadas para la cuenta de administración
> - Mejores prácticas para las cuentas de los miembros

Acerca Cuentas de AWS de AWS Control Tower

An Cuenta de AWS es el contenedor de todos los recursos que posee. Estos recursos incluyen las identidades AWS Identity and Access Management (IAM) aceptadas por la cuenta, que determinan quién tiene acceso a esa cuenta. Las identidades de IAM pueden incluir usuarios, grupos, roles y más. Para obtener más información sobre cómo trabajar con IAM, usuarios, funciones y políticas en AWS Control Tower, consulte Administración de identidades y accesos en AWS Control Tower.

Recursos y tiempo de creación de la cuenta

Cuando AWS Control Tower crea o inscribe una cuenta, implementa la configuración de recursos mínima necesaria para la cuenta, incluidos los recursos en forma de plantillas de Account Factory y otros recursos en su landing zone. Estos recursos pueden incluir funciones de IAM, AWS CloudTrail rutas, productos aprovisionados por Service Catalog y usuarios del IAM Identity Center. AWS Control Tower también despliega recursos, según lo requiera la configuración de control, para la unidad organizativa (OU) en la que la nueva cuenta está destinada a convertirse en una cuenta de miembro.

AWS Control Tower organiza la implementación de estos recursos en su nombre. Es posible que se necesiten varios minutos por recurso para completar la implementación, así que tenga en

cuenta el tiempo total antes de crear o inscribir una cuenta. Para obtener más información sobre la administración de los recursos de sus cuentas, consulteGuía para crear y modificar los recursos de la Torre de Control de AWS.

Consideraciones a la hora de incorporar las cuentas de seguridad o de registro existentes

Antes de aceptar una cuenta Cuenta de AWS como cuenta de seguridad o de registro, AWS Control Tower comprueba si hay recursos que no cumplan con los requisitos de la Torre de Control de AWS. Por ejemplo, es posible que tenga un depósito de registro con el mismo nombre que requiere AWS Control Tower. Además, AWS Control Tower valida que la cuenta puede aprovisionar recursos; por ejemplo, garantizando que AWS Security Token Service (AWS STS) esté habilitada, que la cuenta no esté suspendida y que AWS Control Tower tenga permiso para aprovisionar recursos dentro de la cuenta.

AWS Control Tower no elimina ningún recurso existente en las cuentas de registro y seguridad que usted proporciona. Sin embargo, si decide habilitar la función de Región de AWS denegación, el control de denegación regional impide el acceso a los recursos de las regiones denegadas.

Vea sus cuentas

La página de la organización muestra todas las OU y cuentas de su organización, independientemente de la OU o del estado de inscripción en AWS Control Tower. Puede ver e inscribir las cuentas de los miembros en AWS Control Tower, individualmente o por grupos de unidades organizativas, si cada cuenta cumple los requisitos previos para la inscripción.

Para ver una cuenta específica en la página de la organización, puede seleccionar Solo cuentas en el menú desplegable de la esquina superior derecha y, a continuación, seleccionar el nombre de su cuenta en la tabla. Como alternativa, puede seleccionar el nombre de la unidad organizativa principal de la tabla y ver una lista de todas las cuentas de esa unidad organizativa en la página de detalles de esa unidad organizativa.

En la página de la organización y en la página de detalles de la cuenta, puede ver el estado de la cuenta, que es uno de los siguientes:

- No inscrita: la cuenta es miembro de la unidad organizativa principal, pero AWS Control Tower no la administra completamente. Si la OU principal está registrada, la cuenta se rige por los controles preventivos configurados para su OU principal registrada, pero los controles de detección de la OU

no se aplican a esta cuenta. Si la unidad organizativa principal no está registrada, no se aplicará ningún control a esta cuenta.

- Inscripción: AWS Control Tower pasa a ser la entidad de gobierno de la cuenta. Estamos alineando la cuenta con la configuración de control de la unidad organizativa principal. Este proceso puede requerir varios minutos por recurso de la cuenta.
- Inscrita: la cuenta se rige por los controles configurados para su unidad organizativa principal. Está totalmente gestionado por AWS Control Tower.
- Error en la inscripción: no se pudo inscribir la cuenta en AWS Control Tower. Para obtener más información, consulte Causas frecuentes de no inscripción.
- Actualización disponible: la cuenta tiene una actualización disponible. Las cuentas de este estado siguen inscritas, pero la cuenta debe actualizarse para reflejar los cambios recientes realizados en su entorno. Para actualizar una sola cuenta, vaya a la página de detalles de la cuenta y seleccione Actualizar cuenta.

  Si tiene varias cuentas en este estado en una sola unidad organizativa, puede optar por volver a registrar la unidad organizativa y actualizar esas cuentas juntas.

Recursos creados en las cuentas compartidas

En esta sección se muestran los recursos que AWS Control Tower crea en las cuentas compartidas al configurar la landing zone.

Para obtener información sobre los recursos de las cuentas de los miembros, consulteConsideraciones sobre los recursos para Account Factory.

Recursos de cuentas de administración

Cuando configuras tu landing zone, se crean los siguientes AWS recursos en tu cuenta de administración.

Servicio de AWS	Tipo de recurso	Nombre del recurso
AWS Organizations	Cuentas	audit log archive
AWS Organizations	OU	Security

Servicio de AWS	Tipo de recurso	Nombre del recurso
		Sandbox
AWS Organizations	Políticas de control de servicios	aws-guardrails-*
AWS CloudFormation	Pilas	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER(en la versión 2.6 y posteriores)

Servicio de AWS	Tipo de recurso	Nombre del recurso
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(No se implementó en la versión 3.0 y versiones posteriores) AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES AWSControlTowerBP-BASELINE-SERVICE-ROLES AWSControlTowerBP-SECURITY-TOPICS AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED AWSControlTowerLoggingResources

Servicio de AWS	Tipo de recurso	Nombre del recurso
		AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	Producto	AWS Control Tower Account Factory
AWS Config	Agregador	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Registros	aws-controltower/CloudTrailLogs
AWS Identity and Access Management	Roles	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	Políticas	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

Servicio de AWS	Tipo de recurso	Nombre del recurso
AWS IAM Identity Center	Grupos de directorios	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	Conjuntos de permisos	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

Note

No AWS CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL` está desplegado en las versiones 3.0 o posteriores de landing zone. Sin embargo, seguirá existiendo en las versiones anteriores de la landing zone, hasta que la actualices.

Registra los recursos de la cuenta

Cuando configuras tu landing zone, se crean los siguientes AWS recursos en tu cuenta de archivo de registros.

Servicio de AWS	Tipo de recurso	Nombre del recurso
AWS CloudFormation	Pilas	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later)

Servicio de AWS	Tipo de recurso	Nombre del recurso
		StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerLoggingResources-
AWS Config	Reglas de AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	Registros de seguimiento	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Reglas del evento	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Registros	/aws/lambda/aws-controltower-NotificationForwarder

Servicio de AWS	Tipo de recurso	Nombre del recurso
AWS Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Políticas	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Temas	aws-controltower-SecurityNotifications
AWS Lambda	Aplicaciones	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Funciones	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	Buckets	aws-controltower-logs-* aws-controltower-s3-access-logs-*

Audite los recursos de la cuenta

Cuando configuras tu landing zone, se crean los siguientes AWS recursos en tu cuenta de auditoría.

Servicio de AWS	Tipo de recurso	Nombre del recurso
AWS CloudFormation	Pilas	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED- StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES-

Servicio de AWS	Tipo de recurso	Nombre del recurso
		StackSet-AWSControlTowerSecurityResources-*
AWS Config	Agregador	aws-controltower-GuardrailsComplianceAggregator
AWS Config	Reglas de AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Reglas del evento	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Registros	/aws/lambda/aws-controltower-NotificationForwarder

Servicio de AWS	Tipo de recurso	Nombre del recurso
AWS Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution
AWS Identity and Access Management	Políticas	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Temas	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications
AWS Lambda	Funciones	aws-controltower-NotificationForwarder

Acerca de las cuentas compartidas

Cuentas de AWS Hay tres especiales asociadas a AWS Control Tower: la cuenta de administración, la cuenta de auditoría y la cuenta de archivo de registros. Por lo general, estas cuentas se denominan cuentas compartidas o, a veces, cuentas principales.

- Puedes seleccionar nombres personalizados para las cuentas de auditoría y archivo de registros al configurar tu landing zone. Para obtener información sobre cómo cambiar el nombre de una cuenta, consulte Cambiar externamente los nombres de los recursos de la Torre de Control de AWS.
- También puede especificar una cuenta existente Cuenta de AWS como de seguridad o de registro de AWS Control Tower durante el proceso inicial de configuración de la landing zone. Esta opción elimina la necesidad de que AWS Control Tower cree nuevas cuentas compartidas. (Esta selección se realiza una sola vez).

Para obtener más información sobre las cuentas compartidas y sus recursos asociados, consulteRecursos creados en las cuentas compartidas.

Cuenta de administración

Esto Cuenta de AWS lanza AWS Control Tower. De forma predeterminada, el usuario raíz de esta cuenta y el usuario de IAM o el usuario administrador de IAM de esta cuenta tienen acceso total a todos los recursos de tu landing zone.

> **Note**
>
> Como práctica recomendada, recomendamos iniciar sesión como usuario del Centro de Identidad de IAM con privilegios de administrador al realizar funciones administrativas en la consola de la Torre de Control de AWS, en lugar de iniciar sesión como usuario raíz o usuario administrador de IAM para esta cuenta.

Para obtener más información sobre las funciones y los recursos disponibles en la cuenta de administración, consulte. Recursos creados en las cuentas compartidas

Cuenta del archivo de registro

La cuenta compartida del archivo de registros se configura automáticamente al crear tu landing zone.

Esta cuenta contiene un bucket central de Amazon S3 para almacenar una copia de todas las cuentas AWS CloudTrail y los archivos de AWS Config registro de todas las demás cuentas de tu landing zone. Como práctica recomendada, recomendamos restringir el acceso a las cuentas del archivo de registros a los equipos responsables del cumplimiento y las investigaciones, así como a sus herramientas de seguridad o auditoría relacionadas. Esta cuenta se puede usar para auditorías de seguridad automatizadas o para alojar funciones personalizadas Reglas de AWS Config, como Lambda, para realizar acciones de corrección.

> **Política de bucket de Amazon S3**
>
> Para la versión 3.3 y posteriores de la zona de aterrizaje de AWS Control Tower, las cuentas deben cumplir una `aws:SourceOrgID` condición para cualquier permiso de escritura en su segmento de auditoría. Esta condición garantiza que CloudTrail solo pueda escribir registros en nombre de las cuentas de su organización en su bucket de S3; evita que CloudTrail los registros ajenos a su organización se escriban en su bucket de S3 de AWS Control Tower. Para obtener más información, consulte Versión 3.3 de la zona de aterrizaje de AWS Control Tower.

Para obtener más información sobre las funciones y los recursos disponibles en la cuenta de archivo de registros, consulte Registra los recursos de la cuenta

> **Note**
>
> Estos registros no se pueden cambiar. Todos los registros se almacenan con fines de auditoría e investigaciones de cumplimiento relacionadas con la actividad de la cuenta.

Cuenta de auditoría

Esta cuenta compartida se configura automáticamente al crear tu landing zone.

La cuenta de auditoría debe estar restringida a los equipos de seguridad y cumplimiento con funciones de auditor (solo lectura) y administrador (acceso completo) en todas las cuentas de la landing zone. Estas funciones están pensadas para que las utilicen los equipos de seguridad y cumplimiento para:

- Realice auditorías mediante AWS mecanismos, como el alojamiento de funciones Lambda de AWS Config reglas personalizadas.

- Realice operaciones de seguridad automatizadas, como acciones correctivas.

La cuenta de auditoría también recibe notificaciones a través del servicio Amazon Simple Notification Service (Amazon SNS). Se pueden recibir tres categorías de notificaciones:

- Todos los eventos de configuración: en este tema se agrupan todos los eventos de configuración CloudTrail y AWS Config las notificaciones de todas las cuentas de tu landing zone.
- Notificaciones de seguridad agregadas: en este tema se agrupan todas las notificaciones de seguridad de CloudWatch eventos específicos, eventos de cambios en el estado de Reglas de AWS Config cumplimiento y GuardDuty hallazgos.
- Notificaciones de deriva: en este tema se recopilan todas las advertencias de deriva descubiertas en todas las cuentas, usuarios, unidades organizativas y SCP de tu landing zone. Para obtener más información sobre la deriva, consulte. Detecte y resuelva desviaciones en la Torre de Control de AWS

Las notificaciones de auditoría que se activan en la cuenta de un miembro también pueden enviar alertas a un tema local de Amazon SNS. Esta funcionalidad permite a los administradores de cuentas suscribirse a las notificaciones de auditoría específicas de una cuenta de miembro individual. Como resultado, los administradores pueden resolver los problemas que afectan a una cuenta individual y, al mismo tiempo, agregar todas las notificaciones de la cuenta a su cuenta de auditoría centralizada. Para obtener más información, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

Para obtener más información sobre las funciones y los recursos disponibles en la cuenta de auditoría, consulteAudite los recursos de la cuenta.

Para obtener más información sobre la auditoría programática, consulte Funciones programáticas y relaciones de confianza para la cuenta de auditoría de AWS Control Tower.

> **Important**
>
> La dirección de correo electrónico que proporcione para la cuenta de auditoría recibirá los correos electrónicos de AWS notificación y confirmación de suscripción de todas las direcciones Región de AWS compatibles con AWS Control Tower. Para recibir correos electrónicos de conformidad en su cuenta de auditoría, debe elegir el enlace Confirmar

suscripción incluido en cada correo electrónico de cada correo electrónico Región de AWS compatible con AWS Control Tower.

Acerca de las cuentas de los miembros

Las cuentas de miembro son las cuentas a través de las cuales los usuarios realizan sus AWS cargas de trabajo. Estas cuentas de miembros las pueden crear en Account Factory, los usuarios del IAM Identity Center con privilegios de administrador en la consola de Service Catalog o mediante métodos automatizados. Cuando se crean, estas cuentas de miembros se encuentran en una OU que se creó en la consola de la Torre de Control de AWS o se registró en la Torre de Control de AWS. Para obtener más información, consulte estos temas relacionados:

- Aprovisione y administre cuentas con Account Factory
- Automatice las tareas en AWS Control Tower
- AWS Terminología y conceptos de las organizaciones en la guía AWS Organizations del usuario.

Consulte también Aprovisione cuentas con AWS Control Tower Account Factory for Terraform (AFT) .

Cuentas y controles

Las cuentas de los miembros se pueden inscribir en AWS Control Tower o se pueden anular. Los controles se aplican de forma diferente a las cuentas inscritas y no inscritas, y los controles pueden aplicarse a las cuentas en unidades organizativas anidadas en función de la herencia.

Para obtener información sobre los recursos de cuentas de miembros que asigna AWS Control Tower, consulte. Consideraciones sobre los recursos para Account Factory

Inscribir un ya existente Cuenta de AWS

Puede extender el gobierno de la Torre de Control de AWS a una persona, ya existente Cuenta de AWS al inscribirla en una unidad organizativa (OU) que ya esté gobernada por la Torre de Control de AWS. Las cuentas aptas existen en unidades organizativas no registradas que forman parte de la misma AWS Organizations organización que la unidad organizativa de AWS Control Tower.

> **Note**
>
> No puedes inscribir una cuenta existente para que sirva como cuenta de auditoría o archivo de registros, excepto durante la configuración inicial de landing zone.

Configure primero el acceso confiable

Antes de poder inscribir una Cuenta de AWS cuenta existente en la Torre de Control de AWS, debe dar permiso a la Torre de Control de AWS para administrar o gobernar la cuenta. En concreto, AWS Control Tower requiere permiso para establecer un acceso de confianza entre AWS CloudFormation y AWS Organizations en su nombre, de modo que AWS CloudFormation pueda implementar su pila automáticamente en las cuentas de la organización seleccionada. Con este acceso confiable, el `AWSControlTowerExecution` rol lleva a cabo las actividades necesarias para administrar cada cuenta. Por eso, debes agregar este rol a cada cuenta antes de inscribirla.

Cuando el acceso de confianza está activado, AWS CloudFormation puedes crear, actualizar o eliminar pilas en varias cuentas y Regiones de AWS con una sola operación. AWS Control Tower se basa en esta capacidad de confianza para poder aplicar funciones y permisos a las cuentas existentes antes de trasladarlas a una unidad organizativa registrada y, por lo tanto, ponerlas bajo control.

Para obtener más información sobre el acceso confiable y AWS CloudFormation StackSets, consulte AWS CloudFormationStackSetsy AWS Organizations.

¿Qué sucede durante la inscripción de la cuenta

Durante el proceso de inscripción, AWS Control Tower lleva a cabo las siguientes acciones:

- Establece la cuenta, que incluye la implementación de estos conjuntos de pilas:
  - `AWSControlTowerBP-BASELINE-CLOUDTRAIL`
  - `AWSControlTowerBP-BASELINE-CLOUDWATCH`
  - `AWSControlTowerBP-BASELINE-CONFIG`
  - `AWSControlTowerBP-BASELINE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES`
  - `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`

Es buena idea revisar las plantillas de estos conjuntos de pilas y asegurarse de que no entren en conflicto con las políticas existentes.

- Identifica la cuenta mediante AWS IAM Identity Center o AWS Organizations.
- Coloca la cuenta en la unidad organizativa que ha especificado. Asegúrese de aplicar todos los SCP que se aplican en la unidad organizativa actual, de modo que su posición de seguridad siga siendo coherente.
- Aplica los controles obligatorios a la cuenta mediante los SCP que se aplican a la OU seleccionada en su conjunto.
- Lo habilita AWS Config y configura para registrar todos los recursos de la cuenta.
- Añade a la cuenta AWS Config las reglas que aplican los controles de detective de la Torre de Control Tower de AWS.

Cuentas y registros a nivel de organización CloudTrail

Todas las cuentas de los miembros de una OU se rigen por el AWS CloudTrail registro de la OU, estén inscritas o no:

- Cuando inscribe una cuenta en AWS Control Tower, su cuenta se rige por el AWS CloudTrail registro de la nueva organización. Si ya tiene una implementación de una versión de CloudTrail seguimiento, es posible que vea cargos duplicados, a menos que elimine la versión de seguimiento existente de la cuenta antes de inscribirla en AWS Control Tower.
- Si traslada una cuenta a una unidad organizativa registrada (por ejemplo, mediante la AWS Organizations consola) y no procede a inscribirla en AWS Control Tower, es posible que desee eliminar cualquier rastro restante a nivel de cuenta de la cuenta. Si ya tiene una implementación de una versión de seguimiento, se le cobrarán cargos CloudTrail duplicados. CloudTrail

Si actualizas tu landing zone y decides excluirte de las rutas a nivel de organización, o si tu landing zone es anterior a la versión 3.0, las CloudTrail rutas a nivel de organización no se aplican a tus cuentas.

Inscribir cuentas existentes en VPC

AWS Control Tower gestiona las VPC de forma diferente cuando aprovisiona una nueva cuenta en Account Factory que cuando inscribe una cuenta existente.

- Al crear una cuenta nueva, AWS Control Tower elimina automáticamente la VPC AWS predeterminada y crea una nueva VPC para esa cuenta.
- Al inscribir una cuenta existente, AWS Control Tower no crea una nueva VPC para esa cuenta.
- Al inscribir una cuenta existente, AWS Control Tower no elimina ninguna VPC existente ni ninguna VPC predeterminada AWS asociada a la cuenta.

> **Tip**
>
> Puede cambiar el comportamiento predeterminado de las cuentas nuevas configurando Account Factory, de modo que no configure una VPC de forma predeterminada para las cuentas de su organización en AWS Control Tower. Para obtener más información, consulte Cree una cuenta en AWS Control Tower sin una VPC.

Requisitos previos para la inscripción

Estos requisitos previos son necesarios para poder inscribir a una empresa existente Cuenta de AWS en AWS Control Tower:

1. Para inscribir un puesto existente Cuenta de AWS, el `AWSControlTowerExecution` rol debe estar presente en la cuenta que vaya a inscribir. Puede revisar Inscribir una cuenta para obtener detalles e instrucciones.
2. Además del `AWSControlTowerExecution` rol, la persona a la Cuenta de AWS que desee inscribir debe contar con los siguientes permisos y relaciones de confianza. De lo contrario, la inscripción fallará.

   Permiso de rol: `AdministratorAccess` (política AWS gestionada)

   Relación de confianza del rol:

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::Management Account ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. Recomendamos que la cuenta no tenga un grabador de AWS Config configuración ni un canal de entrega. Es posible que se eliminen o modifiquen AWS CLI antes de poder registrar una cuenta. De lo contrario, consulte Inscribir cuentas que tengan AWS Config recursos existentes para obtener instrucciones sobre cómo puede modificar sus recursos existentes.
4. La cuenta que desee inscribir debe estar en la misma AWS Organizations organización que la cuenta de administración de AWS Control Tower. La cuenta existente solo se puede inscribir en la misma organización que la cuenta de administración de AWS Control Tower, en una OU que ya esté registrada en AWS Control Tower.

Para comprobar otros requisitos previos para la inscripción, consulte Introducción a AWS Control Tower.

> **Note**
>
> Cuando inscribe una cuenta en la Torre de Control de AWS, esta se rige por el AWS CloudTrail registro de la organización de la Torre de Control de AWS. Si ya tiene una implementación de una versión de CloudTrail seguimiento, es posible que vea cargos duplicados, a menos que elimine la versión de seguimiento existente de la cuenta antes de inscribirla en AWS Control Tower.

Inscriba una cuenta existente

La función Inscribir cuentas está disponible en la consola de la Torre de Control de AWS, para inscribir a las existentes de Cuentas de AWS forma que estén gobernadas por la Torre de Control de AWS. Para obtener más información, consulte Inscribir una empresa existente Cuenta de AWS.

La función Enroll account (Inscribir cuenta) está disponible cuando la zona de inicio no se encuentra en un estado de desviación. Para ver esta capacidad en la consola:

- Diríjase a la página de la organización en AWS Control Tower.
- Busque el nombre de la cuenta que desea inscribir. Para encontrarlo, selecciona Solo cuentas en el menú desplegable de la esquina superior derecha y, a continuación, busca el nombre de la cuenta en la tabla filtrada.
- Sigue los pasos para registrar una cuenta individual, tal y como se muestra en la Pasos para inscribir una cuenta sección.

> **Note**
>
> Cuando inscribas una existente Cuenta de AWS, asegúrate de verificar la dirección de correo electrónico existente. De lo contrario, es posible que se cree una cuenta nueva.

Algunos errores pueden requerir que actualice la página y lo intente de nuevo. Si su zona de inicio se encuentra en un estado de desviación, es posible que no pueda utilizar correctamente la función Enroll account (Inscribir cuenta) . Deberás aprovisionar nuevas cuentas a través de Account Factory hasta que se resuelva tu problema de zona de aterrizaje.

Al inscribir cuentas desde la consola de la Torre de Control de AWS, debe iniciar sesión en una cuenta con un usuario que tenga la `AWSServiceCatalogEndUserFullAccess` política habilitada, junto con permisos de acceso de administrador para usar la consola de la Torre de Control de AWS, y no puede iniciar sesión como usuario raíz.

Las cuentas que inscriba se pueden actualizar a través de AWS Service Catalog la fábrica de cuentas de AWS Control Tower, del mismo modo que actualizaría cualquier otra cuenta. Los procedimientos de actualización se indican en la sección Actualice y mueva cuentas de fábrica con AWS Control Tower o con AWS Service Catalog.

Pasos para inscribir una cuenta

Una vez que el AdministratorAccesspermiso (política) esté en vigor en tu cuenta actual, sigue estos pasos para inscribir la cuenta:

Para inscribir una cuenta individual en AWS Control Tower

- Diríjase a la página de organización de la Torre de Control de AWS.
- En la página de la organización, las cuentas que pueden inscribirse le permiten seleccionar Inscribirse en el menú desplegable Acciones situado en la parte superior de la sección. Estas

cuentas también muestran el botón Inscribir una cuenta cuando las ves en la página de detalles de la cuenta.

- Al seleccionar Inscribir una cuenta, verá la página Inscribir una cuenta, en la que se le solicitará que añada el `AWSControlTowerExecution` rol a la cuenta. Para obtener algunas instrucciones, consulteAñada manualmente el rol de IAM requerido a uno existente Cuenta de AWS e inscríbalo.
- A continuación, seleccione una unidad organizativa registrada de la lista desplegable. Si la cuenta ya está en una unidad organizativa registrada, esta lista mostrará la unidad organizativa.
- Seleccione Enroll account (Inscribir cuenta).
- Verás un recordatorio modal para añadir el `AWSControlTowerExecution` rol y confirmar la acción.
- Selecciona Inscribir.
- AWS Control Tower comienza el proceso de inscripción y se le redirige a la página de detalles de la cuenta.

Causas frecuentes de no inscripción

- Para inscribir una cuenta existente, el `AWSControlTowerExecution` rol debe estar presente en la cuenta que estás inscribiendo.
- La entidad principal de IAM carece de los permisos necesarios para aprovisionar una cuenta.
- AWS Security Token Service (AWS STS) está deshabilitado Cuenta de AWS en su región de origen o en cualquier región compatible con la Torre de Control de AWS.
- Es posible que haya iniciado sesión en una cuenta que deba añadirse a la cartera de Account Factory en AWS Service Catalog. La cuenta debe añadirse antes de poder acceder a Account Factory para poder crear o inscribir una cuenta en AWS Control Tower. Si el usuario o rol apropiado no se agrega a la cartera de Account Factory, recibirás un error cuando intentes agregar una cuenta. Para obtener instrucciones sobre cómo conceder acceso a las AWS Service Catalog carteras, consulta Conceder acceso a los usuarios.
- Es posible que haya iniciado sesión como usuario raíz.
- Es posible que la cuenta que estás intentando inscribir tenga una AWS Config configuración residual. En concreto, la cuenta puede tener un grabador de configuración o un canal de entrega. Deben eliminarse o modificarse AWS CLI antes de poder registrar una cuenta. Para obtener más información, consulte Inscribir cuentas que cuenten con AWS Config recursos existentes y Interactuar con AWS Control Tower el uso AWS CloudShell.

- Si la cuenta pertenece a otra OU con una cuenta de administración, incluida otra OU de AWS Control Tower, debe cancelar la cuenta en su OU actual antes de que pueda unirse a otra OU. Los recursos existentes se deben eliminar de la OU original. De lo contrario, la inscripción fallará.
- El aprovisionamiento y la inscripción de la cuenta fallan si los SCP de la OU de destino no le permiten crear todos los recursos necesarios para esa cuenta. Por ejemplo, un SCP de la unidad organizativa de destino puede bloquear la creación de recursos sin determinadas etiquetas. En este caso, se produce un error en el aprovisionamiento o la inscripción de la cuenta porque AWS Control Tower no admite el etiquetado de los recursos. Para obtener ayuda, póngase en contacto con su representante de cuentas o AWS Support

Para obtener más información sobre cómo AWS Control Tower trabaja con los roles al crear cuentas nuevas o al inscribir cuentas existentes, consulte Funciones y cuentas.

> **Tip**
>
> Si no puede confirmar que una cuenta existente Cuenta de AWS cumple con los requisitos previos de inscripción, puede configurar una OU de inscripción e inscribir la cuenta en esa OU. Una vez que la inscripción se haya realizado correctamente, puede mover la cuenta a la OU que desee. Si se produce un error en la inscripción, el error no afectará a ninguna otra cuenta o unidad organizativa.

Si tiene dudas sobre si sus cuentas actuales y sus configuraciones son compatibles con AWS Control Tower, puede seguir las prácticas recomendadas en la siguiente sección.

Recomendado: puede configurar un enfoque de dos pasos para la inscripción de cuentas

- En primer lugar, utilice un paquete de AWS Config conformidad para evaluar cómo algunos controles de la Torre de Control de AWS pueden afectar a sus cuentas. Para determinar cómo la inscripción en la Torre de Control de AWS puede afectar a sus cuentas, consulte Ampliar la gobernanza de la Torre de Control de AWS mediante paquetes de AWS Config conformidad.
- A continuación, es posible que desee inscribir la cuenta. Si los resultados de conformidad son satisfactorios, la ruta de migración es más fácil porque puede inscribir la cuenta sin consecuencias inesperadas.
- Una vez realizada la evaluación, si decide configurar una zona de aterrizaje de la AWS Control Tower, es posible que tenga que eliminar el canal de AWS Config entrega y el registrador de

configuración que se crearon para la evaluación. De este modo, podrá configurar AWS Control Tower correctamente.

> **Note**
>
> El paquete de conformidad también funciona en situaciones en las que las cuentas están ubicadas en unidades organizativas registradas por la Torre de Control de AWS, pero las cargas de trabajo se ejecutan en AWS regiones que no son compatibles con la Torre de Control de AWS. Puede usar el paquete de conformidad para administrar los recursos de las cuentas que existen en regiones en las que AWS Control Tower no está implementada.

¿Qué sucede si la cuenta no cumple los requisitos previos?

Recuerde que, como requisito previo, las cuentas que puedan inscribirse en el gobierno de la Torre de Control de AWS deben formar parte de la misma organización general. Para cumplir con este requisito previo para la inscripción de una cuenta, puede seguir estos pasos preparatorios para trasladar una cuenta a la misma organización que AWS Control Tower.

Pasos preparatorios para incorporar una cuenta a la misma organización que AWS Control Tower

1. Elimine la cuenta de su organización actual. Si utilizas este método de pago, debes proporcionar un método de pago diferente.
2. Invite a la cuenta a unirse a la organización de la Torre de Control de AWS. Para obtener más información, consulte Invitar a una AWS cuenta a unirse a su organización en la Guía del AWS Organizations usuario.
3. Acepta la invitación. La cuenta aparece en la raíz de la organización. Este paso mueve la cuenta a la misma organización que AWS Control Tower y establece los SCP y la facturación unificada.

> **Tip**
>
> Puede enviar la invitación a la nueva organización antes de que la cuenta deje de pertenecer a la antigua. La invitación estará pendiente cuando la cuenta abandone oficialmente su organización actual.

Pasos para cumplir los requisitos previos restantes:

1. Cree el `AWSControlTowerExecution` rol necesario.
2. Borre la VPC predeterminada. (Esta parte es opcional. (AWS Control Tower no cambia su VPC predeterminada actual).
3. Elimine o modifique cualquier grabadora AWS Config de configuración o canal de entrega existente a través de AWS CLI o AWS CloudShell. Para obtener más información, consulte Ejemplos de comandos AWS Config CLI para el estado de los recursos y Inscribir cuentas que cuenten con AWS Config recursos existentes.

Una vez que haya completado estos pasos preparatorios, podrá inscribir la cuenta en AWS Control Tower. Para obtener más información, consulte Pasos para inscribir una cuenta. Este paso lleva la cuenta al gobierno completo de la Torre de Control de AWS.

Pasos opcionales para anular el aprovisionamiento de una cuenta y poder inscribirla y conservar su pila

1. Para conservar la AWS CloudFormation pila aplicada, elimina la instancia de pila de los conjuntos de pilas y selecciona Conservar pilas para la instancia.
2. Finalice el producto aprovisionado para la AWS Service Catalog cuenta en Account Factory. (Este paso solo elimina el producto aprovisionado de AWS Control Tower. No elimina la cuenta).
3. Configura la cuenta con los detalles de facturación necesarios, como se requiere para cualquier cuenta que no pertenezca a una organización. A continuación, elimina la cuenta de la organización. (Si lo haces, la cuenta no se descontará del total de tu AWS Organizations cuota).
4. Limpia la cuenta si quedan recursos y, después, ciérrala siguiendo los pasos del cierre de la cuentaAnule la administración de una cuenta.
5. Si tiene una unidad organizativa suspendida con controles definidos, puede mover la cuenta allí en lugar de realizar el paso 1.

Ejemplos de comandos AWS Config CLI para el estado de los recursos

Estos son algunos ejemplos de comandos AWS Config CLI que puede usar para determinar el estado de su grabadora de configuración y canal de entrega.

Comandos de visualización:

- `aws configservice describe-delivery-channels`

- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

La respuesta normal es algo así como `"name": "default"`

Comandos de eliminación:

- `aws configservice stop-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-delivery-channel --delivery-channel-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*

Añada manualmente el rol de IAM requerido a uno existente Cuenta de AWS e inscríbalo

Si ya ha configurado la zona de aterrizaje de la Torre de Control de AWS, puede empezar a inscribir las cuentas de su organización en una OU que esté registrada en AWS Control Tower. Si no ha configurado su landing zone, siga los pasos descritos en la Guía del usuario de AWS Control Tower, en Introducción, paso 2. Cuando la landing zone esté lista, complete los siguientes pasos para que AWS Control Tower controle las cuentas existentes de forma manual.

Asegúrese de revisar lo Requisitos previos para la inscripción indicado anteriormente en este capítulo.

Antes de inscribir una cuenta en AWS Control Tower, debe conceder permiso a AWS Control Tower para administrar esa cuenta. Para ello, añadirá un rol que tenga acceso total a la cuenta, tal y como se indica en los pasos que se indican a continuación. Estos pasos se deben realizar para cada cuenta que inscriba.

Para cada cuenta:

Paso 1: inicie sesión con acceso de administrador en la cuenta de administración de la organización que contiene actualmente la cuenta que desea inscribir.

Por ejemplo, si creó esta cuenta AWS Organizations y utiliza un rol de IAM multicuenta para iniciar sesión, puede seguir estos pasos:

1. Inicia sesión en la cuenta de administración de tu organización.
2. Vaya a AWS Organizations.
3. En Cuentas, selecciona la cuenta que quieres inscribir y copia su ID de cuenta.
4. Abre el menú desplegable de la cuenta en la barra de navegación superior y selecciona Cambiar rol.
5. En el formulario Cambiar de rol, rellena los siguientes campos:
   - En Cuenta, introduce el ID de cuenta que copiaste.
   - En Función, introduzca el nombre de la función de IAM que permite el acceso entre cuentas a esta cuenta. El nombre de este rol se definió cuando se creó la cuenta. Si no especificó un nombre de rol al crear la cuenta, introduzca el nombre de rol predeterminado,`OrganizationAccountAccessRole`.
6. Elija Switch Role.
7. Ahora debería iniciar sesión en la cuenta AWS Management Console como hijo.
8. Cuando termines, permanece en la cuenta infantil durante la siguiente parte del procedimiento.
9. Anota el identificador de la cuenta de administración, ya que tendrás que introducirlo en el siguiente paso.

Paso 2: Otorgue permiso a AWS Control Tower para administrar la cuenta.

1. Vaya a IAM.
2. Ve a Funciones.
3. Elija Crear rol.
4. Cuando se te pida que selecciones el servicio al que corresponde el rol, selecciona Política de confianza personalizada.
5. Copie el ejemplo de código que se muestra aquí y péguelo en el documento de política. Sustituya la cadena *`Management Account ID`*por el ID de cuenta de administración real de su cuenta de administración. Esta es la política para pegar:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Effect":"Allow",
      "Principal":{
```

```
        "AWS": "arn:aws:iam::Management Account ID:root"
        },
        "Action": "sts:AssumeRole",
        "Condition": {}
    }
 ]
}
```

6. Cuando se le pida que adjunte políticas, elija AdministratorAccess.
7. Elija Siguiente:Etiquetas.
8. Es posible que veas una pantalla opcional titulada Añadir etiquetas. Omite esta pantalla por ahora seleccionando Next:Review
9. En la pantalla de revisión, en el campo Nombre del rol, introduzca. `AWSControlTowerExecution`
10. Introduzca una breve descripción en el cuadro Descripción, como por ejemplo Permite el acceso total a la cuenta para la inscripción.
11. Elija Crear rol.

Paso 3: Para inscribir la cuenta, muévala a una unidad organizativa registrada y verifique la inscripción.

Una vez que haya configurado los permisos necesarios mediante la creación del rol, siga estos pasos para inscribir la cuenta y verificar la inscripción.

1. Vuelva a iniciar sesión como administrador y vaya a AWS Control Tower.
2. Inscriba la cuenta.
   - En la página de la organización de AWS Control Tower, seleccione su cuenta y, a continuación, elija Inscribirse en el menú desplegable Acciones de la esquina superior derecha.
   - Siga los pasos para inscribir una cuenta individual, tal y como se muestra en la Pasos para inscribir una cuenta página.
3. Verifica la inscripción.
   - En la Torre de Control de AWS, elija Organization en el panel de navegación de la izquierda.
   - Busque la cuenta que ha inscrito recientemente. Su estado inicial mostrará el estado de Inscripción.

- Cuando el estado cambia a Inscrito, la mudanza se realizó correctamente.

Para continuar con este proceso, inicie sesión en cada cuenta de su organización que desee inscribir en AWS Control Tower. Repita los pasos previos y los pasos de inscripción para cada cuenta.

Registro automatizado de AWS Organizations cuentas

Puede usar el método de inscripción descrito en una entrada de blog titulada Inscribir AWS cuentas existentes en AWS Control Tower para inscribir sus AWS Organizations cuentas en AWS Control Tower mediante un proceso programático.

La siguiente plantilla de YAML puede ayudarle a crear el rol necesario en una cuenta para poder inscribirla mediante programación.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

Inscribir cuentas que cuenten con AWS Config recursos existentes

En este tema se proporciona un step-by-step enfoque sobre cómo inscribir cuentas que tienen AWS Config recursos existentes. Para ver ejemplos de cómo comprobar los recursos existentes, consulteEjemplos de comandos AWS Config CLI para el estado de los recursos.

> **Note**
>
> Si planea incorporar AWS las cuentas existentes a la Torre de Control de AWS como cuentas de archivo de auditoría y registro, y si esas cuentas tienen AWS Config recursos existentes, debe eliminar los AWS Config recursos existentes por completo antes de poder inscribirlas en la Torre de Control de AWS con este fin. Para las cuentas que no están destinadas a convertirse en cuentas de archivo de auditoría y registro, puede modificar los recursos de Config existentes.

Ejemplos de AWS Config recursos

Estos son algunos tipos de AWS Config recursos que podría tener ya tu cuenta. Es posible que sea necesario modificar estos recursos para que pueda inscribir su cuenta en AWS Control Tower.

- AWS Config grabadora
- AWS Config canal de entrega
- AWS Config autorización de agregación

Supuestos

- Ha implementado una zona de aterrizaje de AWS Control Tower
- Su cuenta aún no está inscrita en AWS Control Tower.
- Su cuenta tiene al menos un AWS Config recurso preexistente en al menos una de las regiones de AWS Control Tower reguladas por la cuenta de administración.
- Su cuenta no es la cuenta de administración de AWS Control Tower.
- Su cuenta no está sujeta a la deriva de la gobernanza.

Para ver un blog que describe un enfoque automatizado para inscribir cuentas con AWS Config recursos existentes, consulte Automatizar la inscripción de cuentas con AWS Config recursos

existentes en AWS Control Tower. Podrá enviar un único ticket de soporte para todas las cuentas que desee inscribir, tal y como se describe a continuación. Paso 1: Póngase en contacto con el servicio de atención al cliente con un ticket para añadir la cuenta a la lista de usuarios permitidos de la Torre de Control de AWS

Limitaciones

- La cuenta solo se puede inscribir mediante el flujo de trabajo de la Torre de Control de AWS para ampliar la gobernanza.
- Si los recursos se modifican y se produce una desviación en la cuenta, AWS Control Tower no actualiza los recursos.
- AWS Config los recursos de las regiones que no están gobernadas por la Torre de Control de AWS no se modifican.

> **Note**
>
> Si intentas inscribir una cuenta que tiene recursos de Config existentes sin añadir la cuenta a la lista de permitidos, la inscripción fallará. A partir de entonces, si posteriormente intenta añadir la misma cuenta a la lista de permitidos, AWS Control Tower no podrá validar que la cuenta se haya aprovisionado correctamente. Debe retirar el aprovisionamiento de la cuenta de AWS Control Tower antes de poder solicitar la lista de permitidos e inscribirla. Si solo mueve la cuenta a una unidad organizativa de la Torre de Control de AWS diferente, se produce un error de gobierno, lo que también impide que la cuenta se añada a la lista de permitidos.

Este proceso consta de 5 pasos principales.

1. Añada la cuenta a la lista de usuarios permitidos de la Torre de Control de AWS.
2. Cree un nuevo rol de IAM en la cuenta.
3. Modifique los recursos preexistentes AWS Config .
4. Crea AWS Config recursos en AWS regiones donde no existan.
5. Inscriba la cuenta en AWS Control Tower.

Antes de continuar, tenga en cuenta las siguientes expectativas con respecto a este proceso.

- AWS Control Tower no crea ningún AWS Config recurso en esta cuenta.
- Tras la inscripción, los controles de la Torre de Control de AWS protegen automáticamente los AWS Config recursos que ha creado, incluida la nueva función de IAM.
- Si se realiza algún cambio en AWS Config los recursos después de la inscripción, dichos recursos deben actualizarse para que se ajusten a la configuración de AWS Control Tower antes de volver a inscribir la cuenta.

Paso 1: Póngase en contacto con el servicio de atención al cliente con un ticket para añadir la cuenta a la lista de usuarios permitidos de la Torre de Control de AWS

Incluya esta frase en el asunto de su ticket:

Inscriba cuentas que cuenten con AWS Config recursos existentes en AWS Control Tower

Incluya los siguientes detalles en el cuerpo de su ticket:

- Número de cuenta de administración
- Números de cuenta de las cuentas de los miembros que tienen AWS Config recursos existentes
- La región de origen seleccionada para la configuración de la Torre de Control de AWS

> **Note**
>
> El tiempo necesario para añadir su cuenta a la lista de usuarios permitidos es de 2 días laborables.

Paso 2: Crea un nuevo rol de IAM en la cuenta del miembro

1. Abre la AWS CloudFormation consola de la cuenta de miembro.
2. Crea una pila nueva con la siguiente plantilla

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
```

```
Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. Proporcione el nombre de la pila como CustomerCreatedConfigRecorderRoleForControlTorre
4. Cree la pila.

> **Note**
>
> Cualquier SCP que cree debe excluir un `aws-controltower-ConfigRecorderRole*` rol. No modifique los permisos que restringen la capacidad de AWS Config las reglas para realizar evaluaciones.
> Siga estas pautas para no recibir una `AccessDeniedException` cuando tenga SCP que le impidan llamar `aws-controltower-ConfigRecorderRole*` a Config.

Paso 3: Identifique las AWS regiones con recursos preexistentes

Para cada región gobernada (gobernada por la Torre de Control de AWS) de la cuenta, identifique y anote las regiones que tienen al menos uno de los tipos de ejemplos de AWS Config recursos existentes que se muestran anteriormente.

Paso 4: Identifique las AWS regiones sin AWS Config recursos

Para cada región gobernada (gobernada por la Torre de Control de AWS) de la cuenta, identifique y anote las regiones en las que no hay AWS Config recursos del tipo de ejemplo mostrado anteriormente.

Paso 5: Modifique los recursos existentes en cada AWS región

Para este paso, se necesita la siguiente información sobre la configuración de la Torre de Control de AWS.

- `LOGGING_ACCOUNT`- el ID de la cuenta de registro
- `AUDIT_ACCOUNT`- el ID de la cuenta de auditoría
- `IAM_ROLE_ARN`- el ARN del rol de IAM creado en el paso 1
- `ORGANIZATION_ID`- el identificador de la organización de la cuenta de administración
- `MEMBER_ACCOUNT_NUMBER`- la cuenta de miembro que se está modificando
- `HOME_REGION`- la región de origen para la configuración de la Torre de Control de AWS.

Modifique cada recurso existente siguiendo las instrucciones que figuran en las secciones 5a a 5c, que aparecen a continuación.

Paso 5a. AWS Config recursos de grabadora

Solo puede existir una AWS Config grabadora por AWS región. Si existe una, modifique la configuración como se muestra. Sustituya el artículo `GLOBAL_RESOURCE_RECORDING` por true en su región de origen. Sustituya el elemento por falso en otras regiones en las que haya una AWS Config grabadora.

- Nombre: DON'T CHANGE
- RoLearn: `IAM_ROLE_ARN`
  - RecordingGroup:
  - AllSupported: cierto
  - IncludeGlobalResourceTypes: `GLOBAL_RESOURCE_RECORDING`
  - ResourceTypes: Vacío

Esta modificación se puede realizar a través de la AWS CLI mediante el siguiente comando. Sustituya la cadena RECORDER_NAME por el nombre de la AWS Config grabadora existente.

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

Paso 5b. Modificar los AWS Config recursos del canal de entrega

Solo puede existir un canal de AWS Config entrega por región. Si existe otro, modifique la configuración como se muestra.

- Nombre: DON'T CHANGE
- ConfigSnapshotDeliveryProperties: TwentyFour _Horas
- S3BucketName: El nombre del depósito de registro de la cuenta de registro de la Torre de Control de AWS

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3KeyPrefix: ***ORGANIZATION_ID***
- SnsTopicARN: El ARN del tema de SNS de la cuenta de auditoría, con el siguiente formato:

  `arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-AllConfigNotifications`

Esta modificación se puede realizar a través de la AWS CLI mediante el siguiente comando. Sustituya la cadena *DELIVERY_CHANNEL_NAME* por el nombre de la AWS Config grabadora existente.

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

Paso 5c. Modificar los recursos AWS Config de autorización de agregación

Pueden existir varias autorizaciones de agregación por región. AWS Control Tower requiere una autorización de agregación que especifique la cuenta de auditoría como la cuenta autorizada y que tenga la región de origen de AWS Control Tower como región autorizada. Si no existe, cree una nueva con la siguiente configuración:

- AuthorizedAccountId: El ID de la cuenta de auditoría
- AuthorizedAwsRegion: La región de origen de la configuración de la Torre de Control de AWS

Esta modificación se puede realizar a través de la AWS CLI mediante el siguiente comando:

```
aws configservice put-aggregation-authorization --authorized-account-
id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region
CURRENT_REGION
```

Paso 6: Cree recursos donde no existan, en las regiones gobernadas por la Torre de Control de AWS

Revise la AWS CloudFormation plantilla para que en su región de origen el IncludeGlobalResourcesTypesparámetro tenga el valorGLOBAL_RESOURCE_RECORDING, como se muestra en el siguiente ejemplo. Actualice también los campos obligatorios de la plantilla, tal y como se especifica en esta sección.

Sustituya el artículo GLOBAL_RESOURCE_RECORDING por true en su región de origen. Sustituya el elemento por falso en otras regiones en las que haya una AWS Config grabadora.

1. Navegue hasta la AWS CloudFormation consola de la cuenta de administración.
2. Crea una nueva StackSet con el nombre CustomerCreatedConfigResourcesForControlTower.
3. Copia y actualiza la siguiente plantilla:

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
```

```
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

Actualice la plantilla con los campos obligatorios:

a. *En el BucketName campo **S3**, sustituya los campos LOGGING_ACCOUNT_ID y HOME_REGION*

b. En el KeyPrefix campo S3, sustituya el *ORGANIZATION_ID*

c. *En el campo **SnsTopicARN**, sustituya la AUDIT_ACCOUNT*

d. *En el **AuthorizedAccountId**campo, sustituya la AUDIT_ACCOUNT*

e. *En el **AuthorizedAwsRegion**campo, sustituya HOME_REGION*

4. Durante el despliegue en la AWS CloudFormation consola, añada el número de cuenta del miembro.
5. Agregue las AWS regiones que se identificaron en el paso 4.
6. Implemente el conjunto de pilas.

Paso 7: Registrar la unidad organizativa en AWS Control Tower

En el panel de control de AWS Control Tower, registre la OU.

> **Note**
>
> El flujo de trabajo de inscripción de la cuenta no se realizará correctamente para esta tarea. Debe elegir Registrar OU o Volver a registrar OU.

Aprovisione y administre cuentas con Account Factory

Este capítulo incluye información general y procedimientos para aprovisionar nuevas cuentas de miembros en una zona de aterrizaje de AWS Control Tower con Account Factory.

Permisos para configurar y aprovisionar cuentas

AWS Control Tower Account Factory permite a los administradores y usuarios de la nube AWS IAM Identity Center aprovisionar cuentas en su landing zone. De forma predeterminada, los usuarios del IAM Identity Center que aprovisionan cuentas deben estar en el `AWSAccountFactory` grupo o en el grupo de administración.

> **Note**
>
> Tenga cuidado al trabajar desde la cuenta de administración, como lo haría cuando utilice cualquier cuenta que tenga permisos en toda la organización.

La cuenta de administración de AWS Control Tower tiene una relación de confianza con el `AWSControlTowerExecution` rol, lo que permite configurar la cuenta desde la cuenta de administración, incluida la configuración automática de la cuenta. Para obtener más información sobre el `AWSControlTowerExecution` rol, consulte Funciones y cuentas.

> **Note**
>
> Para inscribir una Cuenta de AWS cuenta existente en AWS Control Tower, esa cuenta debe tener el `AWSControlTowerExecution` rol habilitado. Para obtener más información acerca de cómo inscribir una cuenta existente, consulte Inscribir un ya existente Cuenta de AWS.

Para obtener más información sobre los permisos, consulte Se requieren permisos para las cuentas.

Aprovisione cuentas con AWS Service Catalog Account Factory

El siguiente procedimiento describe cómo crear y aprovisionar cuentas como usuario en el Centro de Identidad de IAM mediante AWS Service Catalog. Este procedimiento también se denomina aprovisionamiento avanzado de cuentas o aprovisionamiento manual de cuentas. Si lo desea, puede aprovisionar cuentas mediante programación, con la AWS CLI o con AWS Control Tower Account Factory for Terraform (AFT). Es posible que pueda aprovisionar cuentas personalizadas en la consola si ha configurado previamente planes personalizados. Para obtener más información sobre la personalización, consultePersonaliza las cuentas con Account Factory Customization (AFC).

Para aprovisionar cuentas individualmente en Account Factory, como usuario

1. Inicie sesión en la URL del portal de usuarios.
2. En Tus aplicaciones, selecciona AWS Cuenta.
3. En la lista de cuentas, elige el ID de cuenta de tu cuenta de administración. Este ID también puede tener una etiqueta, por ejemplo, (Administración).
4. Desde AWSServiceCatalogEndUserAccess, elija Consola de administración. Esto abre la AWS Management Console para este usuario en esta cuenta.
5. Asegúrese de haber seleccionado la correcta Región de AWS para el aprovisionamiento de cuentas, que debe ser su región de AWS Control Tower.
6. Busque y elija Service Catalog para abrir la consola de Service Catalog.
7. En el panel de navegación, elija Productos.
8. Seleccione AWS Control Tower Account Factory y, a continuación, pulse el botón Iniciar producto. Esta selección inicia el asistente para aprovisionar una nueva cuenta.
9. Rellene la información y tenga en cuenta lo siguiente:

   - El SSO UserEmail puede ser una nueva dirección de correo electrónico o la dirección de correo electrónico asociada a un usuario existente del IAM Identity Center. Independientemente de lo que elija, este usuario tendrá acceso administrativo a la cuenta que va a aprovisionar.
   - AccountEmailDebe ser una dirección de correo electrónico que aún no esté asociada a un. Cuenta de AWS Si usaste una dirección de correo electrónico nueva en el SSO UserEmail, puedes usar esa dirección de correo electrónico aquí.

10. No definas ni TagOptionshabilites las notificaciones; de lo contrario, es posible que no se pueda aprovisionar la cuenta. Cuando hayas terminado, selecciona Lanzar producto.

11. Revise la configuración de la cuenta y, a continuación, elija Launch (Lanzar). No cree un plan de recursos; de lo contrario, no se podrá aprovisionar la cuenta.
12. Su cuenta está siendo aprovisionada. Esto puede tardar varios minutos en completarse. Puede renovar la página para actualizar la información de estado mostrada.

> **Note**
>
> Se pueden aprovisionar hasta cinco cuentas a la vez.

Consideraciones para administrar cuentas en Account Factory

Puede actualizar, anular la administración y cerrar las cuentas que cree y aprovisione a través de Account Factory. Puede reciclar las cuentas actualizando los parámetros de usuario de las cuentas que desee reutilizar. También puedes cambiar la unidad organizativa (OU) de una cuenta.

> **Note**
>
> Al actualizar un producto aprovisionado que está asociado a una cuenta que vende Account Factory, si especifica una nueva dirección de correo electrónico de usuario AWS IAM Identity Center, AWS Control Tower crea un nuevo usuario en el IAM Identity Center. La cuenta creada anteriormente no se elimina. Para obtener información sobre cómo eliminar la dirección de correo electrónico del usuario anterior del Centro de Identidad de IAM del Centro de Identidad de IAM, consulte Desactivación de un usuario.

Actualice y mueva cuentas de fábrica con AWS Control Tower o con AWS Service Catalog

La forma más sencilla de actualizar una cuenta inscrita es a través de la consola de AWS Control Tower. Las actualizaciones de cuentas individuales son útiles para resolver problemas, por ejemploCuenta de miembro trasladada. Las actualizaciones de la cuenta también son obligatorias como parte de una actualización completa de landing zone.

Si mueves una cuenta de una unidad organizativa (OU) a otra, recuerda que los controles aplicados por la nueva OU pueden ser diferentes a los controles de la antigua OU. Asegúrese de que los controles de la nueva OU cumplen los requisitos de la política para la cuenta.

Controle el comportamiento cuando las cuentas se transfieran de una cuenta a otra Unidades organizativas

Al mover una cuenta entre unidades organizativas, los controles de la unidad organizativa de destino se aplican a cuenta. Sin embargo, los controles que se aplicaban a la cuenta desde la antigua OU no lo son eliminado. El comportamiento exacto de los controles es específico de la implementación del controles que están activos en la unidad organizativa anterior y en la unidad organizativa de destino.

- Para los controles implementados con AWS Config reglas: los controles de la OU anterior no se eliminan. Estos controles se deben quitar manualmente.
- Para los controles implementados con los SCP: los controles basados en SCP de la OU anterior son eliminado. Los controles basados en SCP para la unidad organizativa de destino entran en vigor en esta cuenta.
- Para los controles implementados con AWS CloudFormation ganchos: este comportamiento depende del estado de los controles de la nueva unidad organizativa.
  - Si la unidad organizativa de destino no tiene ningún control basado en ganchos activo: el anterior Los controles permanecen activos para la cuenta trasladada, a menos que los elimines manualmente.
  - Si la unidad organizativa de destino tiene los controles de gancho activos: los controles antiguos son se quitan y los controles de la unidad organizativa de destino se aplican a cuenta.

Actualiza la cuenta en la consola

Para actualizar una cuenta en la consola de AWS Control Tower

1. Cuando haya iniciado sesión en la Torre de Control de AWS, vaya a la página de la organización.
2. En la lista de unidades organizativas y cuentas, seleccione el nombre de la cuenta que desee actualizar. Las cuentas que están disponibles para su actualización muestran el estado de Actualización disponible.
3. A continuación, verás la página de detalles de la cuenta seleccionada.
4. En la esquina superior derecha, selecciona Actualizar cuenta.

Actualiza el producto aprovisionado

El siguiente procedimiento le guía sobre cómo actualizar su cuenta en Account Factory o moverla a una nueva OU mediante la actualización del producto aprovisionado de la cuenta en Service Catalog.

Para actualizar una cuenta de Account Factory o cambiar su OU a través de Service Catalog

1. Inicie sesión en la consola AWS de administración y abra la AWS Service Catalog consola en https://console.aws.amazon.com/servicecatalog/.

   > **Note**
   >
   > Debe iniciar sesión como usuario con permisos para aprovisionar nuevos productos en Service Catalog (por ejemplo, un usuario `AWSAccountFactory` o `AWSServiceCatalogAdmins` grupos del Centro de Identidad de IAM).

2. En el panel de navegación, seleccione Aprovisionamiento y, a continuación, elija Productos aprovisionados.
3. Para cada una de las cuentas de miembros de la lista, lleve a cabo los siguientes pasos para actualizar todas las cuentas de miembros:

   a. Seleccione una cuenta de miembro. Se le redirigirá a la página de detalles del producto aprovisionado de esa cuenta.

   b. En la página de detalles del producto aprovisionado, selecciona la pestaña Eventos.

   c. Anote los siguientes parámetros:

      - SSO UserEmail (disponible en los detalles del producto aprovisionado)
      - AccountEmail(Disponible en los detalles del producto aprovisionado)
      - SSO UserFirstName (disponible en el Centro de identidades de IAM)
      - SSOU SerLastName (disponible en el Centro de identidad de IAM)
      - AccountName(Disponible en el Centro de identidades de IAM)

   d. En Actions (Acciones), seleccione Update (Actualizar).

   e. Seleccione el botón situado al lado de la versión del producto que desea actualizar y, a continuación, seleccione Next (Siguiente).

   f. Facilite los valores de los parámetros mencionados anteriormente.

- Si desea conservar la unidad organizativa existente ManagedOrganizationalUnit, elija la unidad organizativa en la que ya estaba la cuenta.
- Si desea migrar la cuenta a una nueva unidad organizativa ManagedOrganizationalUnit, elija la nueva unidad organizativa para la cuenta.

Un administrador central de la nube puede encontrar esta información en la consola de la Torre de Control de AWS, en la página de la organización.

g. Elija Siguiente.

h. Revise los cambios y, a continuación, seleccione Update (Actualizar). Este proceso puede tardar unos minutos por cuenta.

Cambie la dirección de correo electrónico de una cuenta inscrita

Para cambiar la dirección de correo electrónico de una cuenta de miembro inscrita en AWS Control Tower, siga el procedimiento de esta sección.

> **Note**
>
> El siguiente procedimiento no le permite cambiar la dirección de correo electrónico de una cuenta de administración, una cuenta de archivo de registros o una cuenta de auditoría. Para obtener más información al respecto, consulte ¿Cómo cambio la dirección de correo electrónico asociada a mi AWS cuenta? o ponte en contacto con AWS Support.

Para cambiar la dirección de correo electrónico de una cuenta que crea AWS Control Tower

1. Recupere la contraseña del usuario raíz de la cuenta. Puedes seguir los pasos del artículo ¿Cómo recupero una AWS contraseña perdida u olvidada?
2. Inicie sesión en la cuenta con la contraseña del usuario root.
3. Cambia la dirección de correo electrónico como lo harías con cualquier otra Cuenta de AWS y espera a que el cambio se refleje AWS Organizations. Es posible que se produzca un retraso mientras se termina de actualizar el cambio de dirección de correo electrónico.
4. Actualice el producto aprovisionado en Service Catalog con la dirección de correo electrónico que anteriormente pertenecía a la cuenta. El proceso de actualización del producto aprovisionado incluye asociar la nueva dirección de correo electrónico al producto

aprovisionado. De esta forma, el cambio de dirección de correo electrónico se efectuará en AWS Control Tower. Utilice la nueva dirección de correo electrónico para actualizar los productos aprovisionados posteriormente.

Para cambiar la contraseña o la dirección de correo electrónico de una cuenta de miembro con la que creó AWS Organizations, consulte Acceder a una cuenta de miembro como usuario root en la Guía del AWS Organizations usuario.

Cambie el nombre de una cuenta inscrita

Siga el procedimiento de esta sección para cambiar el nombre de una cuenta de AWS Control Tower inscrita.

> **Note**
>
> Para cambiar el nombre de una cuenta de AWS administrador, debe tener permisos de administrador y haber iniciado sesión como usuario raíz de la cuenta.

Para cambiar el nombre de una cuenta creada por AWS Control Tower

1. Recupera la contraseña raíz de la cuenta. Puedes seguir los pasos descritos en este artículo, ¿Cómo recupero una AWS contraseña perdida u olvidada?
2. Inicia sesión en la cuenta con la contraseña raíz.
3. En la AWS Billing consola, dirígete a la página de configuración de la cuenta.
4. Cambia el nombre en la configuración de la cuenta como lo harías con cualquier otro Cuenta de AWS.
5. AWS Control Tower se actualiza automáticamente para reflejar el cambio de nombre. Esta actualización no se reflejará en el producto aprovisionado en AWS Service Catalog.

Configurar Account Factory con los ajustes de Amazon Virtual Private Cloud

Account Factory le permite crear líneas base y opciones de configuración previamente aprobadas para las cuentas de su organización. Puede configurar y aprovisionar nuevas cuentas a través de AWS Service Catalog.

En la página Account Factory, puedes ver una lista de unidades organizativas (OU) y su estado en la lista de permitidos. De forma predeterminada, todas las unidades organizativas están en la lista de direcciones permitidas, lo que significa que las cuentas se pueden aprovisionar bajo ellas. Puedes inhabilitar determinadas unidades organizativas para el aprovisionamiento de cuentas. AWS Service Catalog

Puede ver las opciones de configuración de Amazon VPC disponibles para sus usuarios finales cuando aprovisionan cuentas nuevas.

Para configurar los ajustes de Amazon VPC en Account Factory

1. Como administrador central de la nube, inicie sesión en la consola de la Torre de Control de AWS con permisos de administrador en la cuenta de administración.
2. En el lado izquierdo del panel de control, selecciona Account Factory para ir a la página de configuración de red de Account Factory. Aquí puede ver la configuración de red predeterminada. Para editarlo, selecciona Editar y consulta la versión editable de los ajustes de configuración de red de Account Factory.
3. Puede modificar cada campo de la configuración predeterminada según sea necesario. Elija las opciones de configuración de VPC que desee establecer para todas las cuentas nuevas de Account Factory que puedan crear sus usuarios finales e introduzca sus ajustes en los campos.

- Elija deshabilitada o habilitada para crear una subred pública en Amazon VPC. De forma predeterminada, la subred accesible a través de Internet está inhabilitada.

  > **Note**
  >
  > Si establece la configuración de VPC de Account Factory para que las subredes públicas estén habilitadas al aprovisionar una cuenta nueva, Account Factory configura Amazon VPC para crear una gateway NAT. Amazon VPC le facturará por su uso. Para obtener más información, consulte Precios de VPC.

- Elija el número máximo de subredes privadas en Amazon VPC de la lista. De forma predeterminada, se selecciona 1. El número máximo de subredes privadas permitido es de 2 por zona de disponibilidad.
- Escriba el rango de direcciones IP para crear sus VPC de la cuenta. El valor debe tener la forma de bloque de enrutamiento entre dominios sin clase (CIDR) (por ejemplo, `172.31.0.0/16` es el predeterminado). Este bloque CIDR proporciona el rango general de direcciones IP de

subred para la VPC que Account Factory crea para su cuenta. Dentro de su VPC, las subredes se asignan automáticamente desde el rango que especifique y tienen el mismo tamaño. De forma predeterminada, las subredes de la VPC no se solapan. Sin embargo, los rangos de direcciones IP de subredes de las VPC de todas las cuentas aprovisionadas podrían solaparse.

- Elija una región o todas las regiones para crear una VPC cuando se aprovisione una cuenta. De forma predeterminada, se seleccionan todas las regiones disponibles.
- En la lista, seleccione el número de zonas de disponibilidad para las que configurar subredes en cada VPC. El número predeterminado y recomendado es 3.
- Seleccione Guardar.

Puede establecer estas opciones de configuración para crear nuevas cuentas que no incluyan una VPC. Consulte la explicación.

Anule la administración de una cuenta

Si creó una cuenta en Account Factory o inscribió una Cuenta de AWS y ya no desea que AWS Control Tower administre la cuenta en una zona de aterrizaje, puede anular la administración de la cuenta desde la consola de AWS Control Tower.

Al anular la administración de una cuenta de la Torre de Control de AWS, se eliminan todos los recursos aprovisionados por la Torre de Control de AWS, incluidos los planos. La cuenta se traslada de cualquier unidad organizativa de la Torre de Control de AWS al área raíz. La cuenta ya no forma parte de una unidad organizativa registrada y ya no está sujeta a los SCP de AWS Control Tower. Puede cerrar la cuenta a través AWS Organizations de.

Un usuario del `AWSAccountFactory` grupo del Centro de Identidad de IAM también puede anular la administración de una cuenta en la consola de Service Catalog, cancelando el producto aprovisionado. Para obtener más información sobre los usuarios o grupos del Centro de Identidad de IAM, consulte Administrar los usuarios y el acceso a través de ellos. AWS IAM Identity Center El siguiente procedimiento describe cómo anular la administración de una cuenta de miembro en Service Catalog.

Para anular la administración de una cuenta inscrita

1. Abra la consola de Service Catalog en su navegador web enhttps://console.aws.amazon.com/servicecatalog.
2. En el panel de navegación izquierdo, elija la lista de productos aprovisionados.

3. En la lista de cuentas aprovisionadas, elija el nombre de la cuenta que desee que AWS Control Tower deje de administrar.
4. En la página Provisioned product details (Detalles de producto aprovisionado), en el menú Actions (Acciones), seleccione Terminate (Terminar).
5. En el cuadro de diálogo que aparece, elija Terminate (Terminar).

> **Important**
>
> La palabra terminar es específica de Service Catalog. Al cancelar una cuenta en Service Catalog Account Factory, la cuenta no se cierra. Esta acción elimina la cuenta de su OU y de tu landing zone.

6. Cuando la cuenta no está administrada, su estado cambia a No inscrita.
7. Si ya no necesitas la cuenta, ciérrala. Para obtener más información sobre el cierre de AWS cuentas, consulte Cerrar una cuenta en la Guía del AWS Billing usuario

Al anular la administración de una cuenta personalizada, AWS Control Tower elimina los recursos que el blueprint ha implementado, así como cualquier otro recurso que AWS Control Tower haya creado en la cuenta. Una vez que haya dejado de administrar la cuenta, podrá cerrarla de forma automática. AWS Organizations

> **Note**
>
> Las cuentas no administradas no se cierran ni se eliminan. Si la cuenta no está gestionada, el usuario del Centro de Identidad de IAM que seleccionó al crear la cuenta en Account Factory sigue teniendo acceso administrativo a la cuenta. Si no desea que este usuario tenga acceso administrativo, debe cambiar esta configuración en IAM Identity Center actualizando la cuenta en Account Factory y cambiando la dirección de correo electrónico del usuario de IAM Identity Center para la cuenta. Para obtener más información, consulte Actualice y mueva cuentas de fábrica con AWS Control Tower o con AWS Service Catalog.

Tutorial en vídeo

En este vídeo (3:25) se describe cómo eliminar una cuenta de AWS Control Tower, obtener acceso root a la cuenta y, finalmente, cerrar la Cuenta de AWS. También puede cerrar una cuenta con una

AWS Organizations API. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo sobre el cierre de una cuenta en AWS Control Tower.

Puede ver una lista de AWS YouTube vídeos en los que se explican las tareas habituales en AWS Control Tower.

Cerrar una cuenta creada en Account Factory

Las cuentas creadas en Account Factory son Cuentas de AWS. Para obtener información sobre el cierre Cuentas de AWS, consulte Cerrar una cuenta en la Guía de referencia de administración de AWS cuentas.

> **Note**
>
> Cerrar una cuenta no Cuenta de AWS es lo mismo que anular la administración de una cuenta de AWS Control Tower; se trata de acciones independientes. Debe anular la administración de la cuenta antes de cerrarla.

Cierre una cuenta de miembro de AWS Control Tower mediante AWS Organizations

Puede cerrar sus cuentas de miembro de AWS Control Tower desde la cuenta de administración de su organización sin necesidad de iniciar sesión en cada cuenta de miembro de forma individual con credenciales raíz, mediante AWS Organizations. Sin embargo, no puede cerrar su cuenta de administración de esta manera.

Cuando llamas a la AWS Organizations CloseAccountAPI o cierras una cuenta en la AWS Organizations consola, la cuenta del miembro permanece aislada durante 90 días, como lo Cuenta de AWS haría cualquier otro día. La cuenta muestra un estado Suspendido en la Torre de Control de AWS y AWS Organizations. Si intenta trabajar con la cuenta durante esos 90 días, AWS Control Tower mostrará un mensaje de error.

Antes de que venzan los 90 días, puede restaurar la cuenta del miembro, como puede hacer con cualquier otra Cuenta de AWS. Después de ese período de 90 días, se eliminan los registros de la cuenta.

Se recomienda, como práctica recomendada, dejar de administrar la cuenta de un miembro antes de cerrarla. Si cierra la cuenta de un miembro sin desadministrarla primero, AWS Control Tower

mostrará el estado de la cuenta como Suspendida, pero también como Inscrita. Como resultado, si intenta volver a registrar la unidad organizativa de la cuenta durante ese período de 90 días, AWS Control Tower mostrará un mensaje de error. Básicamente, la cuenta suspendida bloquea las acciones de volver a registrarse debido a un error de comprobación previa. Si eliminas la cuenta de la OU, puedes volver a registrarla, pero es AWS posible que se produzca un error relacionado con la falta de un método de pago para la cuenta. Para evitar esta limitación, cree otra unidad organizativa y mueva la cuenta a esa unidad organizativa antes de intentar volver a registrarla. Se recomienda denominar a esta OU como OU suspendida.

> **Note**
>
> Si no anula la administración de la cuenta antes de cerrarla, debe eliminar el producto aprovisionado de la cuenta una AWS Service Catalog vez transcurridos esos 90 días.

Para obtener más información, consulta la AWS Organizations documentación sobre la CloseAccount API.

Consideraciones sobre los recursos para Account Factory

Cuando se aprovisiona una cuenta con Account Factory, se crean los siguientes AWS recursos dentro de la cuenta.

AWS servicio	Tipo de recurso	Nombre del recurso
AWS CloudFormation	Pilas	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-*

AWS servicio	Tipo de recurso	Nombre del recurso
		StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Reglas del evento	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Registros	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Roles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution

AWS servicio	Tipo de recurso	Nombre del recurso
AWS Identity and Access Management	Políticas	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Temas	aws-controltower-SecurityNotifications
AWS Lambda	Aplicaciones	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Funciones	aws-controltower-NotificationForwarder

Personaliza las cuentas con Account Factory Customization (AFC)

AWS Control Tower le permite personalizar los nuevos y los existentes Cuentas de AWS al aprovisionar sus recursos desde la consola de AWS Control Tower. Tras configurar la personalización de fábrica de la cuenta, AWS Control Tower automatiza este proceso para el aprovisionamiento futuro, de modo que no tendrá que mantener ningún proceso. Las cuentas personalizadas están disponibles para su uso inmediatamente después de aprovisionar los recursos.

Sus cuentas personalizadas se aprovisionan en la fábrica de cuentas, mediante AWS CloudFormation plantillas o con Terraform. Definirás una plantilla que sirva como modelo de cuenta personalizado. Su plan describe los recursos y las configuraciones específicos que necesita cuando se aprovisiona una cuenta. También están disponibles planes predefinidos, creados y gestionados por AWS los socios. Para obtener más información sobre los planes gestionados por los socios, consulte la biblioteca de introducción.AWS Service Catalog

> **Note**
>
> La Torre de Control de AWS contiene controles proactivos que supervisan AWS CloudFormation los recursos de la Torre de Control de AWS. Si lo desea, puede activar estos controles en su landing zone. Cuando aplicas controles proactivos, se aseguran de que los recursos que vas a implementar en tus cuentas cumplan con las políticas y

los procedimientos de tu organización. Para obtener más información sobre los controles proactivos, consulte Controles proactivos.

Los planos de su cuenta se almacenan en una cuenta que Cuenta de AWS, para nuestros fines, se denomina cuenta central. Los planos se almacenan en forma de un producto de Service Catalog. A este producto lo denominamos plano para distinguirlo de cualquier otro producto de Service Catalog. Para obtener más información sobre cómo crear productos de Service Catalog, consulte Creación de productos en la Guía AWS Service Catalog del administrador.

Aplique esquemas a las cuentas existentes

También puede aplicar planos personalizados a las cuentas existentes siguiendo los pasos de actualización de la cuenta en la consola de AWS Control Tower. Para obtener más detalles, consulte Actualiza la cuenta en la consola.

Antes de empezar

Antes de empezar a crear cuentas personalizadas en AWS Control Tower Account Factory, debe tener implementado un entorno de zona de aterrizaje de AWS Control Tower y debe tener una unidad organizativa (OU) registrada en AWS Control Tower, donde se colocarán las cuentas recién creadas.

Para obtener más información sobre cómo trabajar con AFC, consulte Automatizar la personalización de cuentas mediante Account Factory Customization en AWS Control Tower.

Preparación para la personalización

- Puede crear una cuenta nueva para que sirva como cuenta central o puede utilizar una existente Cuenta de AWS. Le recomendamos encarecidamente que no utilice la cuenta de administración de AWS Control Tower como cuenta de blueprint hub.
- Si planea inscribirse Cuentas de AWS en la Torre de Control de AWS y personalizarlas, primero debe añadir el `AWSControlTowerExecution` rol a esas cuentas, como lo haría con cualquier otra cuenta que esté inscribiendo en la Torre de Control de AWS.
- Si tiene pensado utilizar planos de socios que tengan requisitos de suscripción a Marketplace, debe configurarlos desde su cuenta de administración de la Torre de Control Tower de AWS antes de implementar los planos de socios como planos de personalización de fábrica de cuentas.

Temas

Prepárese para la personalización

En las siguientes secciones se explican los pasos para configurar Account Factory para el proceso de personalización. Te recomendamos que configures la administración delegada para la cuenta hub antes de comenzar con estos pasos.

Resumen

- Paso 1. Crea el rol necesario. Cree un rol de IAM que conceda permiso para que AWS Control Tower tenga acceso a la cuenta (hub), donde se almacenan los productos de Service Catalog, también denominados blueprints.
- Paso 2. Cree el producto. AWS Service Catalog Crea el AWS Service Catalog producto (también denominado «producto modelo») que necesitarás para crear una cuenta personalizada como base.
- Paso 3. Revisa tu plan personalizado. Inspecciona el AWS Service Catalog producto (plano) que has creado.
- Paso 4. Llama a tu plan para crear una cuenta personalizada. Introduzca la información del producto del plan y la información del rol en los campos correspondientes de Account Factory, en la consola de AWS Control Tower, al crear la cuenta.

Paso 1. Cree el rol requerido

Antes de empezar a personalizar las cuentas, debe configurar un rol que contenga una relación de confianza entre AWS Control Tower y su cuenta central. Cuando se asume, el rol otorga a AWS Control Tower acceso para administrar la cuenta hub. El rol debe tener un nombre AWSControlTowerBlueprintAccess.

AWS Control Tower asume esta función para crear un recurso de cartera en su nombre y, a continuación AWS Service Catalog, añadir su plan como producto de Service Catalog a esta cartera y, a continuación, compartir esta cartera y su plan con su cuenta de miembro durante el aprovisionamiento de la cuenta.

Creará el `AWSControlTowerBlueprintAccess` rol, tal y como se explica en las siguientes secciones.

Navegue hasta la consola de IAM para configurar el rol requerido.

Para configurar el rol en una cuenta de AWS Control Tower inscrita

1. Federe o inicie sesión como principal en la cuenta de administración de la Torre de Control Tower de AWS.
2. Desde el director federado de la cuenta de administración, asuma o cambie las funciones a la `AWSControlTowerExecution` función de la cuenta de AWS Control Tower inscrita que seleccione para que sirva como cuenta de blueprint hub.
3. A partir del `AWSControlTowerExecution` rol de la cuenta de AWS Control Tower inscrita, cree el `AWSControlTowerBlueprintAccess` rol con los permisos y las relaciones de confianza adecuados.

Note

Para cumplir con la guía de prácticas AWS recomendadas, es importante que cierre sesión en el `AWSControlTowerExecution` puesto inmediatamente después de `AWSControlTowerBlueprintAccess` crearlo.
Para evitar cambios involuntarios en los recursos, la `AWSControlTowerExecution` función está destinada únicamente a AWS Control Tower.

Si su cuenta de blueprint hub no está inscrita en AWS Control Tower, el `AWSControlTowerExecution` rol no existirá en la cuenta y no es necesario que lo asuma antes de continuar configurándolo. `AWSControlTowerBlueprintAccess`

Para configurar el rol en una cuenta de miembro no inscrita

1. Federe o inicie sesión como principal en la cuenta que desee designar como cuenta central, mediante el método que prefiera.
2. Cuando hayas iniciado sesión como principal en la cuenta, crea el `AWSControlTowerBlueprintAccess` rol con los permisos y las relaciones de confianza adecuados.

El AWSControlTowerBlueprintAccessrol debe configurarse para otorgar confianza a dos directores:

- El principal (usuario) que ejecuta la Torre de Control de AWS en la cuenta de administración de la Torre de Control de AWS.
- El rol nombrado `AWSControlTowerAdmin` en la cuenta de administración de la Torre de Control de AWS.

A continuación, se muestra un ejemplo de política de confianza, similar a la que tendrá que incluir en su puesto. Esta política demuestra la mejor práctica de conceder el acceso con los privilegios mínimos. Cuando cree su propia política, sustituya el término *`YourManagementAccountId`*por el ID de cuenta real de su cuenta de administración de AWS Control Tower y sustituya el término *`YourControlTowerUserRole`*por el identificador de la función de IAM de su cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
                "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
```

```
        }
    ]
}
```

Política de permisos obligatoria

AWS Control Tower requiere que la política administrada nombrada `AWSServiceCatalogAdminFullAccess` esté asociada a la `AWSControlTowerBlueprintAccess` función. Esta política proporciona los permisos que AWS Service Catalog busca cuándo permite a AWS Control Tower administrar su cartera y los recursos de sus AWS Service Catalog productos. Puede adjuntar esta política al crear el rol en la consola de IAM.

Es posible que se necesiten permisos adicionales

- Si almacena sus planos en Amazon S3, AWS Control Tower también requiere la política de `AmazonS3ReadOnlyAccess` permisos para el `AWSControlTowerBlueprintAccess` rol.
- El tipo de producto AWS Service Catalog Terraform requiere que añada algunos permisos adicionales a la política de IAM personalizada de AFC si no utiliza la política de administración predeterminada. Los requiere además de los permisos necesarios para crear los recursos que defina en su plantilla de terraform.

Paso 2. Crea el producto AWS Service Catalog

Para crear un AWS Service Catalog producto, siga los pasos que se indican en la sección Creación de productos de la Guía AWS Service Catalog del administrador. Cuando crees el AWS Service Catalog producto, añadirás el esquema de tu cuenta como plantilla.

Important

Como resultado de la actualización de las licencias HashiCorp de Terraform, se AWS Service Catalog cambió el soporte para los productos de código abierto de Terraform y se aprovisionaron los productos a un nuevo tipo de producto, denominado Externo. Para obtener más información sobre cómo afecta este cambio a AFC, incluida la forma de actualizar los esquemas de sus cuentas actuales al tipo de producto externo, consulte Transición al tipo de producto externo.

Resumen de los pasos para crear un plan

- Cree o descargue una AWS CloudFormation plantilla o un archivo de configuración tar.gz de Terraform que se convertirá en el plano de su cuenta. Más adelante en esta sección se ofrecen algunos ejemplos de plantillas.
- Inicia sesión en el Cuenta de AWS lugar donde guardas los planos de Account Factory (a veces denominada cuenta hub).
- Navega hasta la AWS Service Catalog consola. Selecciona Lista de productos y, a continuación, selecciona Cargar nuevo producto.
- En el panel de detalles del producto, introduce los detalles de tu producto modelo, como el nombre y la descripción.
- Selecciona Usar un archivo de plantilla y, a continuación, selecciona Elegir archivo. Seleccione o pegue la plantilla o el archivo de configuración que ha desarrollado o descargado para usarlo como modelo.
- Selecciona Crear producto en la parte inferior de la página de la consola.

Puede descargar una AWS CloudFormation plantilla del repositorio de arquitectura de AWS Service Catalog referencia. Un ejemplo de ese repositorio ayuda a configurar un plan de respaldo para sus recursos.

Aquí tienes una plantilla de ejemplo para una empresa ficticia llamada Best Pets. Ayuda a establecer una conexión con su base de datos de mascotas.

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
    Properties:
```

```
     FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
     Description: Retrieves the connection string for this account to access the Pet
Database
     Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
     Runtime: nodejs16.x
     Handler: index.handler
     Timeout: 5
     Code:
       ZipFile: >
         const response = require("cfn-response");
         exports.handler = function (event, context) {
           const awsAccountId = context.invokedFunctionArn.split(":")[4]
           const connectionString= "fake connection string that's specific to account
" + awsAccountId;
           const responseData = {
             Value: connectionString,
           }
           response.send(event, context, response.SUCCESS, responseData);
           return connectionString;
         };

 ConnectionString:
   Type: Custom::ConnectionStringGenerator
   Properties:
     ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn

 PetDatabaseConnectionString:
   DependsOn: ConnectionString
   # For example purposes we're using SSM parameter store.
   # In your template, use secure alternatives to store
   # sensitive values such as connection strings.
   Type: AWS::SSM::Parameter
   Properties:
     Name: pet-database-connection-string
     Description: Connection information for the BestPets pet database
     Type: String
     Value: !GetAtt ConnectionString.Value
```

Paso 3. Revisa tu plan personalizado

Puede ver su plano en la AWS Service Catalog consola. Para obtener más información, consulte Administración de productos en la Guía del administrador de Service Catalog.

Paso 4. Llame a su plan para crear una cuenta personalizada

Cuando siga el flujo de trabajo Crear una cuenta en la consola de AWS Control Tower, verá una sección opcional en la que puede introducir información sobre el plan que desea utilizar para personalizar las cuentas.

> **Note**
>
> Debe configurar su cuenta de centro de personalización y añadir al menos un blueprint (producto de Service Catalog) antes de poder introducir esa información en la consola de AWS Control Tower y empezar a aprovisionar cuentas personalizadas.

Cree o actualice una cuenta personalizada en la consola de AWS Control Tower.

1. Introduzca el ID de cuenta de la cuenta que contiene sus planos.
2. Desde esa cuenta, seleccione un producto de Service Catalog existente (blueprint existente).
3. Seleccione la versión adecuada del blueprint (producto Service Catalog), si tiene más de una versión.
4. (Opcional) Puede añadir o cambiar una política de aprovisionamiento de planos en este punto del proceso. La política de aprovisionamiento del blueprint está escrita en JSON y se adjunta a una función de IAM, por lo que puede aprovisionar los recursos que se especifican en la plantilla del blueprint. AWS Control Tower crea este rol en la cuenta del miembro para que Service Catalog pueda implementar recursos mediante conjuntos de AWS CloudFormation pilas. El rol se denomina `AWSControlTower-BlueprintExecution-bp-`*`xxxx`*. La `AdministratorAccess` política se aplica aquí de forma predeterminada.
5. Elija la Región de AWS o las regiones en las que desee implementar las cuentas según este plan.
6. Si su blueprint contiene parámetros, puede introducir los valores de los parámetros en campos adicionales del flujo de trabajo de la Torre de Control de AWS. Los valores adicionales pueden incluir: un nombre de GitHub repositorio, una GitHub rama, un nombre de clúster de Amazon ECS y una GitHub identidad del propietario del repositorio.
7. Puedes personalizar las cuentas más adelante siguiendo el proceso de actualización de la cuenta, si tu cuenta central o tus planos aún no están listos.

Para obtener más información, consulte Crea una cuenta personalizada a partir de un plano.

Crea una cuenta personalizada a partir de un plano

Una vez que haya creado los blueprints personalizados, puede empezar a crear cuentas personalizadas en la fábrica de cuentas de AWS Control Tower.

Siga estos pasos para implementar un plan personalizado cuando cree una cuenta nueva AWS :

1. Diríjase a la Torre de Control de AWS en AWS Management Console.
2. Seleccione Account Factory y cree una cuenta.
3. Introduce los detalles de la cuenta, como el nombre de la cuenta y la dirección de correo electrónico.
4. Configure los detalles del centro de identidad de IAM con la dirección de correo electrónico y el nombre de usuario.
5. Seleccione una unidad organizativa registrada a la que se añadirá su cuenta.
6. Amplíe la sección de personalización de la cuenta de fábrica.
7. Introduzca el ID de cuenta de la cuenta de blueprint hub que contiene sus productos de Service Catalog y seleccione Validar. Para obtener más información sobre una cuenta de blueprint hub, consulte. Personaliza las cuentas con Account Factory Customization (AFC)
8. Seleccione el menú desplegable que contiene todos los planos de la lista de productos de Service Catalog (todos los planos personalizados y de socios). Elija un plano y la versión correspondiente para implementarlo.
9. Si el blueprint contiene parámetros, se muestran estos campos para que los rellene. Los valores predeterminados se rellenan previamente.
10. Por último, seleccione dónde va a implementar su plan, ya sea en la región de origen o en todas las regiones gobernadas. Es posible que los recursos globales, como Route 53 o IAM, deban implementarse solo en una sola región. Los recursos regionales, como las instancias de Amazon EC2 o los buckets de Amazon S3, podrían implementarse en todas las regiones gobernadas
11. Una vez completados todos los campos, seleccione Crear cuenta.

> **Note**
>
> Los planos creados con Terraform se pueden implementar solo en una región, no en varias regiones.

Puedes ver el progreso del aprovisionamiento de tu cuenta en la página de la organización. Cuando se complete el aprovisionamiento de su cuenta, los recursos especificados en su plan ya estarán desplegados en ella. Para ver los detalles de la cuenta y el plan, vaya a la página de detalles de la cuenta.

Inscriba y personalice las cuentas

Para inscribir y personalizar cuentas en la consola de AWS Control Tower.

1. Diríjase a la consola de la Torre de Control de AWS y seleccione Organización en el panel de navegación de la izquierda.
2. Verá una lista de las cuentas disponibles. Identifique la cuenta que desea inscribir con un plan personalizado. La columna Estado de esa cuenta debe reflejar la cuenta en estado No inscrito.
3. Selecciona el botón de radio situado a la izquierda de la cuenta y selecciona el menú desplegable Acciones, en la parte superior derecha de la pantalla. Aquí seleccionará la opción de inscripción.
4. Complete la sección de configuración de acceso con la información del centro de identidad de IAM de la cuenta.
5. Seleccione la OU registrada de la que su cuenta pasará a ser miembro.
6. Complete la sección de personalización de la cuenta de fábrica siguiendo los mismos pasos que los pasos 7 a 12 del procedimiento de creación de una cuenta. Para obtener más información, consulte Aprovisionar cuentas de Account Factory con AWS Service Catalog.

Puedes ver el estado del progreso de tu cuenta en la página de la organización. Cuando se complete la inscripción de su cuenta, los recursos especificados en el plan ya estarán desplegados en ella.

Añadir un plano a una cuenta de AWS Control Tower

Para añadir un blueprint a una cuenta de miembro de la Torre de Control de AWS existente, siga el flujo de trabajo Actualizar la cuenta en la consola de la Torre de Control de AWS y elija un nuevo blueprint para añadirlo a la cuenta. Para obtener más información, consulte Actualizar y mover cuentas de Account Factory con AWS Control Tower o con AWS Service Catalog.

> **Note**
>
> Si agrega un plan nuevo a una cuenta, se sobrescribe el plan existente.

> **Note**
>
> Se puede implementar un blueprint por cada cuenta de AWS Control Tower.

Actualice un plano

Los siguientes procedimientos describen cómo actualizar los blueprints personalizados y cómo implementarlos.

Para actualizar sus blueprints personalizados

1. Actualice su AWS CloudFormation plantilla o el archivo tar.gz (plano) de Terraform con sus nuevas configuraciones.
2. Guarde el plano actualizado como una versión nueva en. AWS Service Catalog

Para implementar su blueprint actualizado

1. Diríjase a la página de la organización en la consola de AWS Control Tower.
2. Filtre la página de la organización por nombre y versión del plano.
3. Siga el proceso de actualización de la cuenta e implemente la última versión del blueprint en su cuenta.

Si la actualización del plano no se realiza correctamente

AWS Control Tower permite actualizar los planos cuando el producto aprovisionado se encuentra en ese estado. `AVAILABLE` Si el producto aprovisionado está en un `TAINTED` estado, la actualización fallará. Se recomienda la siguiente solución alternativa:

1. En la AWS Service Catalog consola, actualice manualmente el producto `TAINTED` aprovisionado para cambiar el estado a. `AVAILABLE` Para obtener más información, consulte Actualización de los productos aprovisionados.
2. A continuación, siga el proceso de actualización de la cuenta desde la Torre de Control de AWS para corregir el error de implementación del blueprint.

Recomendamos este paso manual porque: al eliminar un blueprint, es posible que se eliminen los recursos de la cuenta del miembro. La eliminación de recursos puede afectar a las cargas de

trabajo existentes. Por este motivo, recomendamos este método en lugar de la forma alternativa de actualizar un blueprint, que consiste en eliminar y reemplazar el blueprint original, especialmente si está ejecutando cargas de trabajo de producción.

Eliminar un blueprint de una cuenta

Para eliminar un blueprint de una cuenta, siga el flujo de trabajo Actualizar cuenta para eliminar el blueprint y devolver la cuenta a las configuraciones predeterminadas de la Torre de Control de AWS.

Al introducir el flujo de trabajo de actualización de la cuenta en la consola, verá que se rellenan todos los detalles de la cuenta y no se rellenan los detalles de personalización. Si deja estos detalles de AFC en blanco, AWS Control Tower eliminará el plano de la cuenta. Verá un mensaje de advertencia antes de que comience la acción.

> **Note**
>
> AWS Control Tower añade un blueprint a una cuenta solo si selecciona un blueprint durante el proceso de creación de cuenta o actualización de cuenta.

Planos de socios

AWS Control Tower Account Factory Customization (AFC) proporciona acceso a planos de personalización predefinidos que crean y administran los socios. AWS Estos planes de socios le ayudan a personalizar sus cuentas para casos de uso específicos. Los planes de cada socio le ayudan a crear cuentas personalizadas, que están preconfiguradas para que funcionen con las ofertas de productos de ese socio en particular.

Para ver una lista completa de los planos de socios de AWS Control Tower, vaya a la biblioteca de introducción de Service Catalog en su consola. Busque el tipo de fuente AWS Control Tower Blueprints.

Consideraciones para las personalizaciones de Account Factory (AFC)

- AFC admite la personalización mediante un único producto de AWS Service Catalog diseño.
- Los productos AWS Service Catalog blueprint deben crearse en la cuenta hub y en la misma región que la región de origen de la zona de aterrizaje de AWS Control Tower.
- El rol de `AWSControlTowerBlueprintAccess` IAM debe crearse con el nombre correcto, los permisos y la política de confianza.

- AWS Control Tower admite dos opciones de implementación para los planos: implementarla solo en la región de origen o implementarla en todas las regiones gobernadas por la Torre de Control de AWS. La selección de regiones no está disponible.
- Al actualizar un plan en una cuenta de miembro, el identificador de cuenta de Blueprint Hub y el producto del AWS Service Catalog blueprint no se pueden cambiar.
- AWS Control Tower no admite la eliminación de un blueprint existente ni la adición de un blueprint nuevo en una sola operación de actualización del blueprint. Puede eliminar un plano y, a continuación, añadir uno nuevo en operaciones independientes.
- AWS Control Tower cambia el comportamiento en función de si crea o inscribe cuentas personalizadas o no personalizadas. Si no va a crear o inscribir cuentas personalizadas con planos, AWS Control Tower crea un producto aprovisionado por Account Factory (a través del catálogo de servicios) en la cuenta de administración de AWS Control Tower. Si especifica la personalización al crear o inscribir cuentas con blueprints, AWS Control Tower no crea un producto aprovisionado por Account Factory en la cuenta de administración de AWS Control Tower.

En caso de que se produzca un error en el plano

Error al aplicar un blueprint

Si se produce un error durante el proceso de aplicación de un blueprint a una cuenta (ya sea una cuenta nueva o una cuenta existente que esté inscribiendo en AWS Control Tower), el procedimiento de recuperación es el mismo. La cuenta existirá, pero no está personalizada ni está inscrita en AWS Control Tower. Para continuar, siga los pasos para inscribir la cuenta en AWS Control Tower y añada el plano al momento de la inscripción.

Error al crear el **`AWSControlTowerBlueprintAccess`** rol y soluciones

Al crear el `AWSControlTowerBlueprintAccess` rol desde una cuenta de AWS Control Tower, debe iniciar sesión como principal con el `AWSControlTowerExecution` rol. Si ha iniciado sesión con cualquier otro usuario, un SCP impide la `CreateRole` operación, como se muestra en el siguiente artefacto:

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWSControlTowerExecution",
```

```
                    "arn:aws:iam::*:role/stacksets-exec-*"
                ]
            }
        },
        "Action": [
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateAssumeRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription"
        ],
        "Resource": [
            "arn:aws:iam::*:role/aws-controltower-*",
            "arn:aws:iam::*:role/*AWSControlTower*",
            "arn:aws:iam::*:role/stacksets-exec-*"
        ],
        "Effect": "Deny",
        "Sid": "GRIAMROLEPOLICY"
    }
```

Están disponibles las siguientes soluciones alternativas:

- (Lo más recomendable) Asuma el `AWSControlTowerExecution` rol y cree el `AWSControlTowerBlueprintAccess` rol. Si elige esta solución alternativa, asegúrese de cerrar sesión en el `AWSControlTowerExecution` rol inmediatamente después para evitar cambios involuntarios en los recursos.
- Inicie sesión en una cuenta que no esté inscrita en AWS Control Tower y, por lo tanto, no esté sujeta a este SCP.
- Edite temporalmente este SCP para permitir la operación.
- (No se recomienda encarecidamente) Utilice su cuenta de administración de la Torre de Control Tower de AWS como cuenta central, de modo que no esté sujeta a la SCP.

Personalice su documento de política para los planos de AFC en función de CloudFormation

Cuando habilita un blueprint a través de la fábrica de cuentas, AWS Control Tower le indica AWS CloudFormation que cree uno StackSet en su nombre. AWS CloudFormation requiere acceso a su cuenta gestionada para crear AWS CloudFormation pilas en. StackSet Aunque AWS CloudFormation ya tiene privilegios de administrador en la cuenta gestionada a través del `AWSControlTowerExecution` rol, este rol no lo puede asumir. AWS CloudFormation

Como parte de la habilitación de un plan, AWS Control Tower crea un rol en la cuenta del miembro, que AWS CloudFormation puede asumir que debe completar las tareas StackSet de administración. La forma más sencilla de habilitar un plan personalizado de fábrica de cuentas es utilizar una política que lo permita todo, ya que esas políticas son compatibles con cualquier plantilla de plan.

Sin embargo, las prácticas recomendadas sugieren que debes restringir los permisos AWS CloudFormation en la cuenta de destino. Puede proporcionar una política personalizada, que AWS Control Tower aplicará al rol que cree AWS CloudFormation para su uso. Por ejemplo, si su plan crea un parámetro SSM denominado something-important, puede proporcionar la siguiente política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
                 "ssm:GetParameter",
                 "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
```

```
}
```

La `AllowCloudFormationActionsOnStacks` declaración es obligatoria para todas las políticas personalizadas de AFC; AWS CloudFormation utiliza esta función para crear instancias de pila, por lo que requiere permiso para realizar acciones en las pilas. AWS CloudFormation La `AllowSsmParameterActions` sección es específica de la plantilla que se va a habilitar.

Resolver problemas de permisos

Al habilitar un blueprint con una política restringida, es posible que no haya suficientes permisos para habilitar el blueprint. Para resolver estos problemas, revise el documento de la política y actualice las preferencias del plan de la cuenta del miembro para utilizar la política corregida. Para comprobar que la política es suficiente para habilitar el plan, asegúrate de que se concedan los AWS CloudFormation permisos y de que puedes crear una pila directamente utilizando esa función.

Se requieren permisos adicionales para crear un producto Service Catalog basado en Terraform

Al crear un producto AWS Service Catalog externo con un archivo de configuración de Terraform para AFC, es AWS Service Catalog necesario añadir ciertos permisos a la política de IAM personalizada de AFC, además de los permisos necesarios para crear los recursos definidos en la plantilla. Si eliges la política de administración completa predeterminada, no necesitas añadir estos permisos adicionales.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
```

```
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

Para obtener más información sobre la creación de productos Terraform mediante el tipo de producto externo en AWS Service Catalog, consulte el paso 5: Crear funciones de lanzamiento en la Guía del administrador de Service Catalog.

Aprovisione cuentas con AWS Control Tower Account Factory for Terraform (AFT)

AWS Control Tower Account Factory for Terraform (AFT) adopta un GitOps modelo que automatiza el proceso de aprovisionamiento y actualización de cuentas en AWS Control Tower.

> **Note**
>
> La AFT no afecta al rendimiento del flujo de trabajo en AWS Control Tower. Si aprovisiona una cuenta a través de AFT o Account Factory, se produce el mismo flujo de trabajo de back-end.

Con AFT, se crea un archivo Terraform de solicitud de cuenta, que contiene la entrada que invoca el flujo de trabajo de AFT. Una vez finalizados el aprovisionamiento y la actualización de la cuenta, el

flujo de trabajo de AFT continúa ejecutando el marco de aprovisionamiento de cuentas de AFT y los pasos de personalización de la cuenta.

Requisitos previos

Antes de empezar con AFT, debe crear lo siguiente:

- Un entorno AFT completamente implementado. Para obtener más información, consulte Descripción general de AWS Control Tower Account Factory for Terraform (AFT) e Implementación de AWS Control Tower Account Factory for Terraform (AFT)
- Uno o más `git` repositorios de AFT en su entorno de AFT completamente implementado. Para obtener más información, consulte los pasos posteriores a la implementación de AFT.

> **Tip**
>
> Si lo desea, puede crear una carpeta de plantillas de cuentas en el aft-account-customizationsrepositorio.

Para obtener información sobre los Regiones de AWS aspectos en los que AFT tiene limitaciones de implementación, consulte Limitaciones y cuotas en la Torre de Control de AWS yLimitaciones de control.

Aprovisione una nueva cuenta con AFT

Para aprovisionar una nueva cuenta con AFT, cree un archivo Terraform de solicitud de cuenta. Este archivo contiene la entrada de los parámetros del aft-account-requestrepositorio. Después de crear un archivo Terraform de solicitud de cuenta, comience a procesar su solicitud de cuenta `git push` ejecutándolo. Este comando invoca la `ct-aft-account-request` operación en la AWS CodePipeline, que se crea en la cuenta de administración de AFT una vez finalizado el aprovisionamiento de la cuenta. Para obtener más información, consulte Canalización de aprovisionamiento de cuentas AFT.

Solicitud de cuenta: parámetros del archivo Terraform

Debe incluir los siguientes parámetros en el archivo de solicitud de cuenta de Terraform. Puedes ver un ejemplo del archivo Terraform de solicitud de cuenta en. GitHub

- El valor de `module name` debe ser único según la Cuenta de AWS solicitud.
- El valor de `module source` es la ruta al módulo Terraform de solicitud de cuenta que proporciona AFT.
- El valor de `control_tower_parameters` captura los datos necesarios para crear una cuenta de AWS Control Tower. El valor incluye los siguientes campos de entrada:
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> La entrada que proporciones no se `control_tower_parameters` puede cambiar durante el aprovisionamiento de la cuenta.
> Los formatos admitidos para `ManagedOrganizationalUnit` especificarlos en el aft-account-requestrepositorio incluyen `OUName` y`OUName (OU-ID)`.

- `account_tags`captura claves y valores definidos por el usuario, que se pueden etiquetar de Cuentas de AWS acuerdo con criterios empresariales. Para obtener más información, consulte Etiquetado de AWS Organizations recursos en la Guía del AWS Organizations usuario.
- El valor de `change_management_parameters` captura información adicional, como el motivo por el que se creó una solicitud de cuenta y quién inició la solicitud de cuenta. El valor incluye los siguientes campos de entrada:
  - `change_reason`
  - `change_requested_by`
- `custom_fields`captura metadatos adicionales con claves y valores que se despliegan como parámetros SSM en la cuenta vendida en /aft/account-request/custom-fields/. Puede hacer referencia a estos metadatos durante las personalizaciones de la cuenta para implementar los controles adecuados. Por ejemplo, una cuenta que esté sujeta a la conformidad normativa podría implementar más. Reglas de AWS Config Los metadatos que recopiles `custom_fields` pueden requerir un procesamiento adicional durante el aprovisionamiento y la actualización de la cuenta.

Si se elimina un campo personalizado de la solicitud de cuenta, el campo personalizado se elimina del almacén de parámetros de SSM de la cuenta vendida.

- (Opcional) `account_customizations_name` captura la carpeta de plantillas de la cuenta en el aft-account-customizationsrepositorio. Para obtener más información, consulte Personalizaciones de cuentas.

Envíe varias solicitudes de cuentas

La AFT procesa las solicitudes de cuentas de una en una, pero puede enviar varias solicitudes de cuentas a la AFT. Cuando envía varias solicitudes de cuentas a la cartera de AFT, AFT pone en cola y procesa las solicitudes de cuentas siguiendo el orden de entrada y salida.

> **Note**
>
> Puede crear un archivo Terraform de solicitud de cuenta para cada cuenta que desee que AFT aprovisione o agrupar en cascada varias solicitudes de cuentas en un único archivo Terraform de solicitud de cuenta.

Actualizar una cuenta existente

Puede actualizar las cuentas que AFT aprovisiona editando las solicitudes de cuenta enviadas anteriormente y ejecutándolas`git push`. Este comando invoca el flujo de trabajo de aprovisionamiento de cuentas y puede procesar las solicitudes de actualización de cuentas. Puede actualizar la entrada`ManagedOrganizationalUnit`, que forma parte del valor requerido`control_tower_parameters`, y otros parámetros del archivo Terraform de solicitud de cuenta. Para obtener más información, consulte Aprovisionar una nueva cuenta con AFT.

> **Note**
>
> La entrada que proporciona no se `control_tower_parameters` puede cambiar durante el aprovisionamiento de la cuenta.
> Los formatos admitidos para `ManagedOrganizationalUnit` especificarlos en el aft-account-requestrepositorio incluyen `OUName` y`OUName (OU-ID)`.

Actualice una cuenta que AFT no aprovisione

Puede actualizar las cuentas de AWS Control Tower creadas fuera de AFT especificando la cuenta en el aft-account-requestrepositorio.

> **Note**
>
> Asegúrese de que todos los detalles de la cuenta sean correctos y coherentes con la organización de AWS Control Tower y el producto AWS Service Catalog aprovisionado correspondiente.

Requisitos previos para actualizar una existente con AFT Cuenta de AWS

- Cuenta de AWS Deben estar inscritos en AWS Control Tower.
- Cuenta de AWS Deben formar parte de la organización de la Torre de Control de AWS.

Implemente AWS Control Tower Account Factory para Terraform (AFT)

Esta sección está destinada a los administradores de los entornos de la Torre de Control de AWS que deseen configurar Account Factory for Terraform (AFT) en su entorno actual. Describe cómo configurar un entorno Account Factory para Terraform (AFT) con una nueva cuenta de administración de AFT dedicada.

> **Note**
>
> Un módulo de Terraform implementa AFT. Este módulo está disponible en el repositorio AFT y GitHub se considera módulo todo el repositorio AFT.
> Le recomendamos que consulte los módulos AFT en GitHub lugar de clonar el repositorio AFT. De esta forma, puede controlar y consumir las actualizaciones de los módulos a medida que estén disponibles.

Para obtener más información sobre las versiones más recientes de la funcionalidad AWS Control Tower Account Factory for Terraform (AFT), consulte el archivo de versiones de este GitHub repositorio.

Requisitos previos de implementación

Antes de configurar e iniciar su entorno AFT, debe disponer de lo siguiente:

- Una zona de aterrizaje de la AWS Control Tower. Para obtener más información, consulte Planificar la zona de aterrizaje de la AWS Control Tower.
- Una región de origen para la zona de aterrizaje de su AWS Control Tower. Para obtener más información, consulte Cómo Regiones de AWS trabajar con AWS Control Tower.
- Una versión y distribución de Terraform. Para obtener más información, consulte las versiones Terraform y AFT.
- Un proveedor de VCS para rastrear y administrar los cambios en el código y otros archivos. De forma predeterminada, AFT usa AWS CodeCommit. Para obtener más información, consulte ¿Qué es AWS CodeCommit? en la Guía AWS CodeCommit del usuario. Si desea elegir un proveedor de VCS diferente, consulte Alternativas para el control de versiones del código fuente en AFT.
- Un entorno de ejecución en el que puede ejecutar el módulo Terraform que instala AFT.
- Opciones de funciones de AFT. Para obtener más información, consulte Habilitar las opciones de funciones.

Configure y lance su AWS Control Tower Account Factory para Terraform

En los siguientes pasos se supone que está familiarizado con el flujo de trabajo de Terraform. También puede obtener más información sobre la implementación de la AFT siguiendo el laboratorio de introducción a la AFT en el sitio web de AWS Workshop Studio.

Paso 1: Lance su zona de aterrizaje de AWS Control Tower

Complete los pasos de Introducción a AWS Control Tower. Aquí es donde se crea la cuenta de administración de la Torre de Control de AWS y se configura la zona de aterrizaje de la Torre de Control de AWS.

> **Note**
>
> Asegúrese de crear un rol para la cuenta de administración de la Torre de Control de AWS que tenga AdministratorAccesscredenciales. Para más información, consulte los siguientes temas:
>
> - Identidades de IAM (usuarios, grupos de usuarios y roles) en la Guía del AWS Identity and Access Management usuario
> - AdministratorAccessen la Guía de referencia de políticas AWS gestionadas

Paso 2: Crear una nueva unidad organizativa para la AFT (recomendado)

Le recomendamos que cree una unidad organizativa independiente en su AWS organización. Aquí es donde se implementa la cuenta de administración de AFT. Cree la nueva unidad organizativa con su cuenta de administración de AWS Control Tower. Para obtener más información, consulte Crear una nueva unidad organizativa.

Paso 3: Aprovisione la cuenta de administración de AFT

AFT requiere que proporcione una AWS cuenta dedicada a las operaciones de administración de AFT. La cuenta de administración de AWS Control Tower, que está asociada a su zona de aterrizaje de AWS Control Tower, vende la cuenta de administración de AFT. Para obtener más información, consulte Aprovisionar cuentas con AWS Service Catalog Account Factory.

> **Note**
>
> Si creó una OU independiente para AFT, asegúrese de seleccionar esta OU al crear la cuenta de administración de AFT.

El aprovisionamiento completo de la cuenta de administración de AFT puede demorar hasta 30 minutos.

Paso 4: Verifique que el entorno Terraform esté disponible para su implementación

En este paso se supone que tiene experiencia con Terraform y que cuenta con procedimientos para ejecutar Terraform. Para obtener más información, consulte Command: init en el sitio web del HashiCorp desarrollador.

> **Note**
>
> AFT es compatible con la versión Terraform `1.2.0` o posterior.

Paso 5: Llame al módulo Account Factory for Terraform para implementar AFT

Llame al módulo AFT con el rol que creó para la cuenta de administración de la Torre de Control Tower de AWS que tiene AdministratorAccesscredenciales. AWS Control Tower aprovisiona un módulo Terraform a través de la cuenta de administración de AWS Control Tower, que establece

toda la infraestructura necesaria para organizar las solicitudes de AWS Control Tower Account Factory.

Puede ver el módulo AFT en el repositorio de AFT en. GitHub Todo el GitHub repositorio se considera el módulo AFT. Consulte el archivo README para obtener información sobre las entradas necesarias para ejecutar el módulo AFT e implementar AFT. Como alternativa, puede ver el módulo AFT en el registro de Terraform.

El módulo AFT incluye un `aft_enable_vpc` parámetro que especifica si AWS Control Tower aprovisiona los recursos de la cuenta dentro de una nube privada virtual (VPC) en la cuenta de administración central de AFT. De forma predeterminada, el parámetro está establecido en. `true` Si establece este parámetro en`false`, AWS Control Tower implementa AFT sin usar una VPC ni recursos de redes privadas, como puertas de enlace NAT o puntos de enlace de VPC. La desactivación *`aft_enable_vpc`* puede ayudar a reducir el costo operativo de la AFT en algunos patrones de uso.

> **Note**
>
> Para volver a activar el `aft_enable_vpc` parámetro (cambiar el valor de `false` `atrue`), es posible que tenga que ejecutar el `terraform apply` comando dos veces seguidas.

Si tiene canalizaciones en su entorno establecidas para administrar Terraform, puede integrar el módulo AFT en su flujo de trabajo actual. De lo contrario, ejecute el módulo AFT desde cualquier entorno que esté autenticado con las credenciales requeridas.

El tiempo de espera provoca un error en la implementación. Se recomienda utilizar credenciales AWS Security Token Service (STS) para garantizar que el tiempo de espera es suficiente para una implementación completa. El tiempo de espera mínimo para las AWS STS credenciales es de 60 minutos. Para obtener más información, consulte Credenciales de seguridad temporales en IAM en la Guía del AWS Identity and Access Management usuario.

> **Note**
>
> Puede esperar hasta 30 minutos para que AFT termine de implementarse a través del módulo Terraform.

Paso 6: Administre el archivo de estado de Terraform

Al implementar AFT, se genera un archivo de estado de Terraform. Este artefacto describe el estado de los recursos que creó Terraform. Si planea actualizar la versión AFT, asegúrese de conservar el archivo de estado de Terraform o configure un backend de Terraform con Amazon S3 y DynamoDB. El módulo AFT no administra un estado de Terraform del backend.

> **Note**
>
> Eres responsable de proteger el archivo de estado de Terraform. Algunas variables de entrada pueden contener valores confidenciales, como una `ssh` clave privada o un token de Terraform. Según el método de implementación, estos valores se pueden ver como texto sin formato en el archivo de estado de Terraform. Para obtener más información, consulte Datos confidenciales del estado en el HashiCorp sitio web.

Pasos posteriores a la implementación

Una vez que se complete el despliegue de la infraestructura AFT, siga estos pasos adicionales para completar el proceso de configuración y prepararse para aprovisionar las cuentas.

Paso 1: (opcional) Complete CodeConnections con el proveedor de VCS que desee

Si elige un proveedor de VCS externo, AFT lo establece CodeConnections y usted lo confirma. Consulte para Alternativas para el control de versiones del código fuente en AFT obtener información sobre cómo configurar AFT con su VCS preferido.

El paso inicial para establecer la AWS CodeStar conexión lo realiza AFT. Debe confirmar la conexión.

Paso 2: (obligatorio) Rellene cada repositorio

AFT requiere que administres cuatro repositorios:

1. Solicitudes de cuentas: este repositorio se encarga de realizar o actualizar las solicitudes de cuentas. Ejemplos disponibles. Para obtener más información sobre las solicitudes de cuentas AFT, consulteAprovisione una nueva cuenta con AFT.
2. Personalizaciones de aprovisionamiento de cuentas AFT: este repositorio administra las personalizaciones que se aplican a todas las cuentas creadas y administradas por AFT, antes de comenzar la etapa de personalización global. Ejemplos disponibles. Para crear personalizaciones de aprovisionamiento de cuentas AFT, consulte. Cree su máquina de estado, personalizaciones, personalizaciones y aprovisionamiento de cuentas AFT.

3. Personalizaciones globales: este repositorio administra las personalizaciones que se aplican a todas las cuentas creadas y administradas por AFT. Ejemplos disponibles. Para crear personalizaciones globales de AFT, consulteAplica personalizaciones globales.
4. Personalizaciones de cuentas: este repositorio administra las personalizaciones que se aplican solo a cuentas específicas creadas y administradas por AFT. Ejemplos disponibles. Para crear personalizaciones de cuentas AFT, consulteAplica personalizaciones de cuentas.

AFT espera que cada uno de estos repositorios siga una estructura de directorios específica. Las plantillas que se utilizan para rellenar tus repositorios y las instrucciones que describen cómo rellenar las plantillas están disponibles en el módulo Account Factory for Terraform del repositorio de GitHub de AFT.

Descripción general de AWS Control Tower Account Factory para Terraform (AFT)

Account Factory for Terraform (AFT) configura una canalización de Terraform para ayudarlo a aprovisionar y personalizar cuentas en AWS Control Tower. AFT le ofrece la ventaja del aprovisionamiento de cuentas basado en Terraform y, al mismo tiempo, le permite gestionar sus cuentas con AWS Control Tower.

Con AFT, puede crear un archivo Terraform de solicitud de cuenta para obtener la información que desencadena el flujo de trabajo de AFT para el aprovisionamiento de cuentas. Una vez completada la etapa de aprovisionamiento de la cuenta, AFT ejecuta automáticamente una serie de pasos antes de que comience la etapa de personalización de la cuenta. Para obtener más información, consulte el proceso de aprovisionamiento de cuentas de AFT.

AFT es compatible con Terraform Cloud, Terraform Enterprise y Terraform Community Edition. Con AFT, puede iniciar la creación de una cuenta mediante un archivo de entrada y un `git push` comando simple y personalizar las cuentas nuevas o existentes. La creación de cuentas incluye todos los beneficios de gobierno de AWS Control Tower y las personalizaciones de la cuenta que le ayudan a cumplir con los procedimientos de seguridad y las directrices de conformidad estándar de su organización.

AFT admite el seguimiento de las solicitudes de personalización de cuentas. Cada vez que envía una solicitud de personalización de una cuenta, AFT genera un token de rastreo único que pasa por una máquina de AWS Step Functions estados de personalizaciones de AFT, que registra el token como parte de su ejecución. A continuación, puede utilizar las consultas de estadísticas de Amazon CloudWatch Logs para buscar intervalos de marcas de tiempo y recuperar el token de solicitud.

Como resultado, puede ver las cargas útiles que acompañan al token, de modo que puede rastrear la solicitud de personalización de su cuenta a lo largo de todo el flujo de trabajo de AFT. Para obtener información sobre CloudWatch Logs y Step Functions, consulte lo siguiente:

- ¿Qué es Amazon CloudWatch Logs? en la Guía del usuario CloudWatch de Amazon Logs
- ¿Qué es AWS Step Functions? en la Guía AWS Step Functions para desarrolladores

AFT combina las capacidades de otros AWS serviciosServicios de componentes, para crear un marco, con las canalizaciones que implementan Terraform Infrastructure as Code (IaC). AFT le permite:

- Enviar solicitudes de aprovisionamiento y actualización de cuentas en un modelo GitOps
- Almacene los metadatos de la cuenta y el historial de auditorías
- Aplica etiquetas a nivel de cuenta
- Añada personalizaciones a todas las cuentas, a un conjunto de cuentas o a cuentas individuales
- Habilite las opciones de funciones

AFT crea una cuenta separada, llamada cuenta de administración de AFT, para implementar las capacidades de AFT. Para poder configurar AFT, debe disponer de una zona de aterrizaje de AWS Control Tower. La cuenta de administración de AFT no es la misma que la cuenta de administración de AWS Control Tower.

AFT ofrece flexibilidad

- Flexibilidad para su plataforma: AFT es compatible con cualquier distribución de Terraform para el despliegue inicial y el funcionamiento continuo: Community Edition, Cloud y Enterprise.
- Flexibilidad para su sistema de control de versiones: AFT se basa en fuentes alternativas de forma nativa AWS CodeCommit, pero las admite. CodeConnections

AFT ofrece opciones de funciones

Puede habilitar varias opciones de funciones, según las mejores prácticas:

- Crear un nivel de organización CloudTrail para registrar eventos de datos
- Eliminar la VPC AWS predeterminada de las cuentas
- Inscripción de cuentas aprovisionadas en el plan Enterprise AWS Support

> **Note**
>
> La canalización AFT no está diseñada para su uso en la implementación de recursos, como las instancias de Amazon EC2, que sus cuentas necesitan para ejecutar sus aplicaciones. Está diseñado únicamente para el aprovisionamiento y la personalización automatizados de las cuentas de AWS Control Tower.

Tutorial en vídeo

Este vídeo (7:33) describe cómo implementar cuentas con AWS Control Tower Account Factory for Terraform. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo del aprovisionamiento automatizado de cuentas en AWS Control Tower.

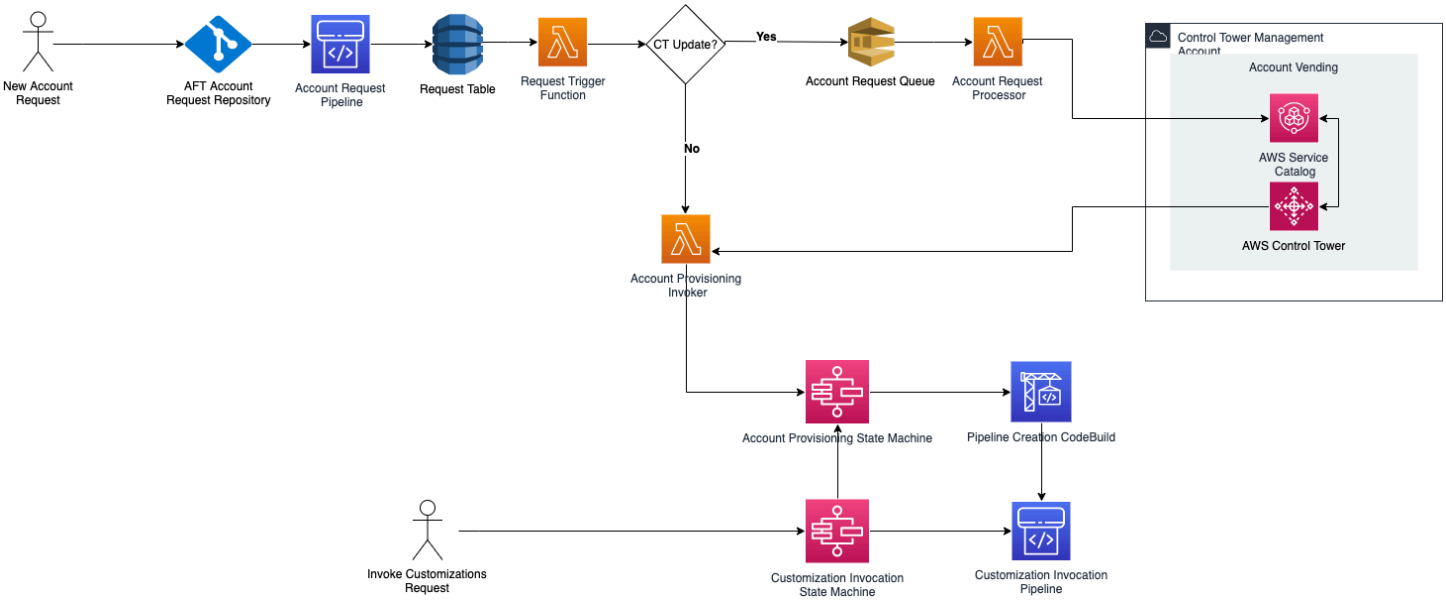
Arquitectura AFT

Orden de operaciones

Las operaciones de AFT se ejecutan en la cuenta de administración de AFT. Para un flujo de trabajo completo de aprovisionamiento de cuentas, el orden de las etapas del diagrama, de izquierda a derecha, es el siguiente:

1. Las solicitudes de cuentas se crean y se envían a la canalización. Puedes crear y enviar más de una solicitud de cuenta a la vez. Account Factory procesa las solicitudes de un first-in-first-out pedido. Para obtener más información, consulte Enviar solicitudes de varias cuentas.
2. Cada cuenta está aprovisionada. Esta etapa se ejecuta en la cuenta de administración de la Torre de Control de AWS.
3. Las personalizaciones globales se ejecutan en las canalizaciones que se crean para cada cuenta vendida.
4. Si las personalizaciones se especifican en las solicitudes iniciales de aprovisionamiento de cuentas, las personalizaciones se ejecutan solo en las cuentas de destino. Si tienes una cuenta que ya está aprovisionada, debes iniciar las personalizaciones adicionales de forma manual en el proceso de creación de la cuenta.

AWS Control Tower Account Factory para Terraform: flujo de trabajo de aprovisionamiento de cuentas



Costo

No existe ningún cargo adicional por la AFT. Solo paga por los recursos desplegados por AFT, los AWS servicios habilitados por AFT y los recursos que implementa en su entorno de AFT.

La configuración predeterminada de AFT incluye la asignación de AWS PrivateLink puntos finales, para mejorar la protección y la seguridad de los datos, y una puerta de enlace NAT necesaria para su compatibilidad AWS CodeBuild. Para obtener más información sobre los precios de esta infraestructura, consulte los AWS PrivateLink precios y los precios de Amazon VPC para NAT Gateway. Póngase en contacto con su representante de AWS cuentas para obtener información más específica sobre la administración de estos costos. Puede cambiar esta configuración predeterminada para AFT.

Versiones Terraform y AFT

Account Factory for Terraform (AFT) es compatible con la versión Terraform `1.2.0` o posterior. Debe proporcionar una versión de Terraform como parámetro de entrada para el proceso de implementación de AFT, como se muestra en el siguiente ejemplo.

```
terraform_version = "1.2.0"
```

Distribuciones de Terraform

AFT admite tres distribuciones de Terraform:

- Edición comunitaria de Terraform
- Nube Terraform
- Terraform Enterprise

Estas distribuciones se explican en las secciones siguientes. Proporcione la distribución de Terraform de su elección como parámetro de entrada durante el proceso de arranque de AFT. Para obtener más información sobre los parámetros de entrada y despliegue de AFT, consulte. Implemente AWS Control Tower Account Factory para Terraform (AFT)

Si elige las distribuciones Terraform Cloud o Terraform Enterprise, el token de API que especifique `terraform_token` debe ser un token de API de usuario o de equipo. No todas las API requeridas admiten un token de organización. Por motivos de seguridad, debes evitar registrar el valor de este token en tu sistema de control de versiones (VCS) asignando una variable de terraformación, como se muestra en el siguiente ejemplo.

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

Edición comunitaria de Terraform

Cuando selecciona Terraform Community Edition como su distribución, AFT administra el backend de Terraform por usted en la cuenta de administración de AFT. AFT descarga la versión `terraform-cli` de Terraform que especificó para ejecutarla durante las fases de despliegue y canalización de AFT. La configuración de estado de Terraform resultante se almacena en un bucket de Amazon S3, denominado con el siguiente formato:

```
aft-backend-[account_id]-primary-region
```

AFT también crea un bucket de Amazon S3 que replica su configuración de estado de Terraform en otro Región de AWS, con fines de recuperación ante desastres, denominado con el siguiente formulario:

```
aft-backend-[account_id]-secondary-region
```

Le recomendamos que habilite la autenticación multifactorial (MFA) para las funciones de eliminación en estos buckets Amazon S3 de Terraform State. Para obtener más información sobre Terraform Community Edition, consulte la documentación de Terraform.

Para seleccionar Terraform OSS como su distribución, proporcione el siguiente parámetro de entrada:

```
terraform_distribution = "oss"
```

Terraform Cloud

Cuando selecciona Terraform Cloud como su distribución, AFT crea espacios de trabajo para los siguientes componentes de su organización de Terraform Cloud, lo que inicia un flujo de trabajo basado en API.

- Solicitud de cuenta
- Personalizaciones de AFT para cuentas que AFT aprovisiona
- Personalizaciones de cuentas para cuentas que proporciona AFT
- Personalizaciones globales para las cuentas que proporciona AFT

Terraform Cloud administra la configuración de estado de Terraform resultante.

Cuando seleccione Terraform Cloud como su distribución, proporcione los siguientes parámetros de entrada:

- `terraform_distribution = "tfc"`
- `terraform_token`— Este parámetro contiene el valor del token de Terraform Cloud. AFT marca el valor como confidencial y almacena el valor como una cadena segura en el almacén de parámetros SSM de la cuenta de administración de AFT. Le recomendamos que modifique periódicamente el valor del token de Terraform de acuerdo con las políticas de seguridad y las directrices de cumplimiento de su empresa. El token de Terraform debe ser un token de API a nivel de usuario o equipo. No se admiten los tokens de organización.
- `terraform_org_name`— Este parámetro contiene el nombre de su organización de Terraform Cloud.

> **Note**
>
> No se admiten múltiples despliegues de AFT en una sola organización de Terraform Cloud.

Para obtener información sobre cómo configurar Terraform Cloud, consulte la documentación de Terraform.

Terraform Enterprise

Cuando selecciona Terraform Enterprise como su distribución, AFT crea espacios de trabajo para los siguientes componentes de su organización de Terraform Enterprise y activa un flujo de trabajo basado en API para las ejecuciones de Terraform resultantes.

- Solicitud de cuenta
- Personalizaciones de aprovisionamiento de cuentas AFT para cuentas aprovisionadas por AFT
- Personalizaciones de cuentas para cuentas aprovisionadas por AFT
- Personalizaciones globales para cuentas aprovisionadas por AFT

La configuración de estado de Terraform resultante la administra su configuración de Terraform Enterprise.

Para seleccionar Terraform Enterprise como su distribución, proporcione los siguientes parámetros de entrada:

- `terraform_distribution = "tfe"`
- `terraform_token`— Este parámetro contiene el valor de su token de Terraform Enterprise. AFT marca su valor como confidencial y lo almacena como una cadena segura en el almacén de parámetros de SSM, en la cuenta de administración de AFT. Le recomendamos que rote periódicamente el valor del token de Terraform, de acuerdo con las políticas de seguridad y las pautas de cumplimiento de su empresa.
- `terraform_org_name`— Este parámetro contiene el nombre de su organización de Terraform Enterprise.
- `terraform_api_endpoint`— Este parámetro contiene la URL de su entorno de Terraform Enterprise. El valor de este parámetro debe tener el siguiente formato:

```
https://{fqdn}/api/v2/
```

Consulte la documentación de Terraform para obtener más información sobre cómo configurar Terraform Enterprise.

Consulte la versión AFT

Puede comprobar la versión AFT implementada consultando la clave del almacén de parámetros del AWS SSM:

```
/aft/config/aft/version
```

Si utiliza el método de registro, puede fijar la versión.

```
module "control_tower_account_factory" {
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
}
```

Puede ver más información sobre las versiones de AFT en el repositorio de AFT.

Actualice la versión AFT

Puede actualizar la versión AFT implementada extrayéndola de la rama del `main` repositorio:

```
terraform get -update
```

Una vez finalizada la extracción, puedes volver a ejecutar el plan Terraform o ejecutar apply para actualizar la infraestructura AFT con los cambios más recientes.

Habilitar opciones de funciones

AFT ofrece opciones de funciones basadas en las mejores prácticas. Puede optar por utilizar estas funciones, mediante indicadores de funciones, durante la implementación de AFT. Consulte Aprovisione una nueva cuenta con AFT para obtener más información sobre los parámetros de configuración de entrada de AFT.

Estas funciones no están habilitadas de forma predeterminada. Debe habilitar cada una de ellas de forma explícita en su entorno.

Temas

- AWS CloudTrail eventos de datos

- AWS Plan Enterprise Support
- Eliminar la AWS VPC predeterminada

AWS CloudTrail eventos de datos

Cuando está habilitada, la opción de eventos de AWS CloudTrail datos configura estas capacidades.

- Crea un registro de la organización en la cuenta de administración de la Torre de Control Tower de AWS, para CloudTrail
- Activa el registro de eventos de datos de Amazon S3 y Lambda
- Cifra y exporta todos los eventos de CloudTrail datos a un bucket de `aws-aft-logs-*` S3 en la cuenta de AWS Control Tower Log Archive, con AWS KMS cifrado
- Activa la configuración de validación del archivo de registro

Para habilitar esta opción, defina el siguiente indicador de función en True en la configuración de entrada de la implementación de AFT.

```
aft_feature_cloudtrail_data_events
```

Requisito previo

Antes de activar esta opción de función, asegúrese de que el acceso confiable para AWS CloudTrail esté habilitado en su organización.

Para comprobar el estado del acceso de confianza para CloudTrail :

1. Navega hasta la AWS Organizations consola.
2. Seleccione Servicios > CloudTrail.
3. A continuación, selecciona Habilitar el acceso de confianza en la esquina superior derecha, si es necesario.

Es posible que recibas un mensaje de advertencia en el que se te pida que utilices la AWS CloudTrail consola, pero en ese caso, ignora la advertencia. AFT crea el rastro como parte de la activación de esta opción de función, después de permitir el acceso confiable. Si el acceso confiable no está habilitado, recibirá un mensaje de error cuando AFT intente crear su registro para los eventos de datos.

> **Note**
>
> Esta configuración funciona a nivel de la organización. La activación de esta configuración afecta a todas las cuentas AWS Organizations, estén administradas por AFT o no. Todos los depósitos de la cuenta de AWS Control Tower Log Archive en el momento de la activación se excluyen de los eventos de datos de Amazon S3. Consulte la Guía del AWS CloudTrail usuario para obtener más información al respecto CloudTrail.

AWS Plan Enterprise Support

Cuando esta opción está habilitada, la canalización de AFT activa el plan AWS Enterprise Support para las cuentas aprovisionadas por AFT.

AWS las cuentas vienen con el plan AWS Basic Support activado de forma predeterminada. AFT proporciona la inscripción automática en el nivel de soporte empresarial, para las cuentas que AFT aprovisiona. El proceso de aprovisionamiento abre un ticket de soporte para la cuenta, en el que se solicita que se añada al plan AWS Enterprise Support.

Para habilitar la opción Enterprise Support, defina el siguiente indicador de función en True en la configuración de entrada de implementación de AFT.

```
aft_feature_enterprise_support=false
```

Consulte Compare AWS Support Plans para obtener más información sobre los planes de AWS Support.

> **Note**
>
> Para permitir que esta función funcione, debe inscribir la cuenta del pagador en el plan Enterprise Support.

Eliminar la AWS VPC predeterminada

Al habilitar esta opción, AFT elimina todas las VPC AWS predeterminadas de la cuenta de administración y de todas Regiones de AWS, incluso si no ha implementado los recursos de AWS Control Tower en ellas. Regiones de AWS

AFT no elimina automáticamente las VPC AWS predeterminadas de las cuentas de la Torre de Control de AWS que AFT aprovisione ni de las AWS cuentas existentes que usted inscriba en la Torre de Control de AWS a través de AFT.

Las AWS cuentas nuevas se crean con una VPC configurada en cada una de ellas Región de AWS, de forma predeterminada. Es posible que su empresa tenga prácticas estándar para crear VPC, que requieren que elimine la VPC AWS predeterminada y evite habilitarla, especialmente para la cuenta de administración de AFT.

Para habilitar esta opción, defina el siguiente indicador de función en True en la configuración de entrada de despliegue de AFT.

```
aft_feature_delete_default_vpcs_enabled
```

Consulte la VPC predeterminada y las subredes predeterminadas para obtener más información sobre las VPC predeterminadas.

Consideraciones sobre los recursos de AWS Control Tower Account Factory for Terraform

Cuando configura su landing zone con AWS Control Tower Account Factory for Terraform, se crean varios tipos de AWS recursos en sus AWS cuentas.

Busque recursos

- Puede usar etiquetas para buscar la lista más actualizada de recursos de la AFT. El par clave-valor para su búsqueda es:

  ```
  Key: managed_by | Value: AFT
  ```

- En el caso de los servicios de componentes que no admiten etiquetas, puede buscar los recursos buscando `aft` en los nombres de los recursos.

Tablas de recursos creadas inicialmente, por cuenta

Cuenta de administración de AWS Control Tower Account Factory para Terraform

AWS service	Tipo de recurso	Nombre del recurso
AWS Identity and Access Management	Roles	AWSAFTAdministrator AWSAFTExecution AWSAFTService aws-ct-aft-*
AWS Identity and Access Management	Políticas	aws-ct-aft-*
CodeCommit	Repositorios	aws-ct-aft-*
CodeBuild	Proyectos de compilación	aws-ct-aft-*
Code Pipeline	Canalizaciones	*-baseline-*
Amazon S3	Buckets	*-aws-ct-aft-* aws-ct-aft-*
Lambda	Funciones	aws-ct-aft-*
Lambda	Capas	aws-ct-aft-common-layer
DynamoDB	Tablas	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	Máquinas estatales	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline

AWS service	Tipo de recurso	Nombre del recurso
		aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	Temas	aws-ct-aft-notifications aws-ct-aft-failure-notifications
Amazon EventBridge	Buses de eventos	aws-ct-aft-events-from-ct-management
Amazon EventBridge	Reglas del evento	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor
Servicio de administración de claves (KMS)	Claves administradas por el cliente	*-aws-ct-aft-* aws-ct-aft-*
AWS Systems Manager	Almacén de parámetros	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	Queues	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	Grupos de registro	/aws/*/aws-ct-aft-* aws-ct-aft-*
AWS Support Center (opcional)	Planes Support	Enterprise

AWS cuentas aprovisionadas a través de AWS Control Tower Account Factory para Terraform

AWS service	Tipo de recurso	Nombre del recurso
AWS Identity and Access Management	Roles	AWSAFTExecution
AWS Support Center (opcional)	Planes Support	Enterprise

Cuenta de administración de AWS Control Tower

AWS service	Tipo de recurso	Nombre del recurso
AWS Identity and Access Management	Roles	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-controltower-events-rule
AWS Systems Manager	Almacén de parámetros	/aws-ct-aft/account/aws-ct-aft-management/account-id
AWS Organizations (Opcional)	Políticas de control de servicios	aws-ct-aft-protect-resources
CloudTrail (Opcional)	Registros de seguimiento	aws-ct-aft-BaselineCloudTrail
AWS Support Center (opcional)	Planes Support	Enterprise

Cuenta de archivo de registros de AWS Control Tower

AWS service	Tipo de recurso	Nombre del recurso
AWS Identity and Access Management	Roles	AWSAFTExecutionRole AWSAFTExecution

AWS service	Tipo de recurso	Nombre del recurso
		aws-ct-aft-cloudtrail-data-events-role
Servicio de administración de claves (KMS)	Claves administradas por el cliente	*-aws-ct-aft-kms-gd-findings
Amazon S3	Buckets	*-aws-ct-aft-logs* aws-ct-aft-s3-access-logs*
AWS Support Center (opcional)	Planes Support	Enterprise

Cuenta de auditoría de AWS Control Tower

AWS service	Tipo de recurso	Nombre del recurso
AWS Identity and Access Management	Roles	AWSAFTExecutionRole AWSAFTExecution
AWS Support Center (opcional)	Planes Support	Enterprise

Funciones obligatorias

En general, las funciones y las políticas forman parte de la gestión de identidad y acceso (IAM) en AWS. Consulte la Guía del usuarioAWS de IAM para obtener más información.

AFT crea múltiples funciones y políticas de IAM en las cuentas de administración de AFT y de administración de la Torre de Control Tower de AWS para respaldar las operaciones del oleoducto de AFT. Estas funciones se crean en función del modelo de acceso con privilegios mínimos, que restringe el permiso a los conjuntos de acciones y recursos mínimos necesarios para cada función y política. A estos roles y políticas se les asigna un `key:value` par de AWS etiquetas `managed_by:AFT` para su identificación.

Además de estas funciones de IAM, AFT crea tres funciones esenciales:

- el `AWSAFTAdmin` rol
- el `AWSAFTExecution` papel
- el `AWSAFTService` papel

Estas funciones se explican en las siguientes secciones.

La AWSAFTAdmin función, explicada

Al implementar AFT, el `AWSAFTAdmin` rol se crea en la cuenta de administración de AFT. Esta función permite a la canalización de AFT asumir la `AWSAFTExecution` función en las cuentas aprovisionadas de AWS Control Tower y AFT y, por lo tanto, realizar acciones relacionadas con el aprovisionamiento y la personalización de las cuentas.

Esta es la política en línea (artefacto JSON) asociada a la función: `AWSAFTAdmin`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
        }
    ]
}
```

El siguiente artefacto de JSON muestra la relación de confianza del rol. `AWSAFTAdmin` El número de marcador de posición `012345678901` se sustituye por el número de identificación de la cuenta de administración de la AFT.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

El AWSAFTExecution rol, explicado

Al implementar AFT, el `AWSAFTExecution` rol se crea en las cuentas de administración de AFT y de administración de AWS Control Tower. Más adelante, la canalización de AFT crea el `AWSAFTExecution` rol en cada cuenta aprovisionada de AFT durante la etapa de aprovisionamiento de la cuenta de AFT.

AFT utiliza el `AWSControlTowerExecution` rol inicialmente para crear el `AWSAFTExecution` rol en cuentas específicas. El `AWSAFTExecution` rol permite a la canalización de AFT ejecutar los pasos que se llevan a cabo durante las etapas de aprovisionamiento y personalización del aprovisionamiento del marco AFT, para las cuentas aprovisionadas por AFT y para las cuentas compartidas.

> **Los roles distintos le ayudan a limitar el alcance**
>
> Como práctica recomendada, mantenga los permisos de personalización separados de los permisos permitidos durante el despliegue inicial de los recursos. Recuerde que el `AWSAFTService` rol está diseñado para el aprovisionamiento de cuentas y el `AWSAFTExecution` rol está destinado a la personalización de cuentas. Esta separación limita el alcance de los permisos que se permiten durante cada fase de la canalización. Esta distinción es especialmente importante si va a personalizar las cuentas compartidas de AWS Control Tower, ya que las cuentas compartidas pueden contener información confidencial, como detalles de facturación o información de usuario.

Permisos para `AWSAFTExecution` el rol: AdministratorAccess— una política administrada por AWS

El siguiente artefacto de JSON muestra la política de IAM (relación de confianza) asociada al `AWSAFTExecution` rol. El número de marcador de posición `012345678901` se sustituye por el número de identificación de la cuenta de administración de la AFT.

Política de confianza para `AWSAFTExecution`

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

El AWSAFTService rol, explicado

El `AWSAFTService` rol despliega los recursos de AFT en todas las cuentas inscritas y administradas, incluidas las cuentas compartidas y la cuenta de administración. Anteriormente, los recursos los desplegaba únicamente el `AWSAFTExecution` rol.

El `AWSAFTService` rol está diseñado para que lo utilice la infraestructura de servicios para implementar recursos durante la `AWSAFTExecution` etapa de aprovisionamiento y solo para implementar personalizaciones. Al asumir las funciones de esta manera, puede mantener un control de acceso más detallado durante cada etapa.

Permisos para `AWSAFTService` el rol: AdministratorAccess— una política administrada por AWS

El siguiente artefacto de JSON muestra la política de IAM (relación de confianza) asociada al `AWSAFTService` rol. El número de marcador de posición `012345678901` se sustituye por el número de identificación de la cuenta de administración de la AFT.

Política de confianza para `AWSAFTService`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Servicios de componentes

Al implementar AFT, se agregan componentes a su AWS entorno desde cada uno de estos AWS servicios.

- AWS Control Tower: AFT utiliza AWS Control Tower Account Factory en la cuenta de administración de AWS Control Tower para aprovisionar cuentas.
- Amazon DynamoDB: AFT crea tablas de Amazon DynamoDB en la cuenta de administración de AFT, que almacenan las solicitudes de cuentas, el historial de auditorías de las actualizaciones de las cuentas, los metadatos de las cuentas y los eventos del ciclo de vida de AWS Control Tower. AFT también crea activadores Lambda de DynamoDB para iniciar procesos posteriores, como iniciar el flujo de trabajo de aprovisionamiento de cuentas AFT.
- Amazon Simple Storage Service: AFT crea depósitos de Amazon Simple Storage Service (S3) en la cuenta de administración de AFT y en la cuenta de archivo de registros de la Torre de Control de AWS, que almacenan los registros generados por los servicios de AWS que requiere la canalización de AFT. AFT también crea un depósito S3 del backend de Terraform, en las regiones de AWS principales y secundarias, para almacenar los estados de Terraform generados durante los flujos de trabajo de AFT.
- Amazon Simple Notification Service: AFT crea temas del Amazon Simple Notification Service (SNS) en la cuenta de administración de AFT, que almacena las notificaciones de éxito y fracaso después de procesar cada solicitud de cuenta AFT. Puede recibir estos mensajes utilizando el protocolo que elija.
- Amazon Simple Queuing Service: AFT crea una cola FIFO de Amazon Simple Queuing Service (Amazon SQS) en la cuenta de administración de AFT. La cola le permite enviar varias solicitudes de cuentas en paralelo, pero envía una solicitud a la vez a AWS Control Tower Account Factory para su procesamiento secuencial.
- AWS CodeBuild: AFT crea proyectos de CodeBuild compilación de AWS en la cuenta de administración de AFT para inicializar, compilar, probar y aplicar los planes de Terraform para el código fuente de AFT en varias etapas de compilación.
- AWS CodePipeline: AFT crea CodePipeline canalizaciones de AWS en la cuenta de administración de AFT para integrarlas con el proveedor de CodeStar conexiones de AWS que haya seleccionado y compatible para el código fuente de AFT y activar trabajos de creación en AWS CodeBuild.
- AWS Lambda: AFT crea funciones y capas de AWS Lambda en la cuenta de administración de AFT para realizar los pasos durante los procesos de solicitud de cuenta, aprovisionamiento de cuentas AFT y personalización de cuentas.

- AWS Systems Manager Parameter Store: AFT configura el AWS Systems Manager Parameter Store en la cuenta de administración de AFT para almacenar los parámetros de configuración necesarios para los procesos de canalización de AFT.
- Amazon CloudWatch: AFT crea grupos de CloudWatch registros de Amazon en la cuenta de administración de AFT para almacenar los registros generados por los servicios de AWS empleados por la canalización de AFT. El período de retención de CloudWatch los registros está establecido en`Never Expire`.
- Amazon VPC: AFT crea una Amazon Virtual Private Cloud (VPC) para aislar los servicios y recursos de la cuenta de administración de AFT en un entorno de red independiente, a fin de mejorar la seguridad.
- AWS KMS: AFT utiliza el AWS Key Management Service (KMS) en la cuenta de administración de AFT y en la cuenta de archivo de registros de AWS Control Tower. AFT crea claves para cifrar los estados de Terraform, los datos almacenados en las tablas de DynamoDB y los temas de SNS. Estos registros y artefactos se generan cuando AFT implementa los recursos y servicios de AWS. Las claves de KMS creadas por AFT tienen habilitada la rotación anual de forma predeterminada.
- AWS Identity and Access Management (IAM): AFT sigue el modelo de privilegios mínimos recomendado. Crea funciones y políticas de AWS Identity and Access Management (IAM) en la cuenta de administración de la AFT, en las cuentas de la Torre de Control de AWS y en las cuentas aprovisionadas por la AFT, según sea necesario, para realizar las acciones necesarias durante el flujo de trabajo de la canalización de AFT.
- AWS Step Functions: AFT crea máquinas de estado de AWS Step Functions en la cuenta de administración de AFT. Estas máquinas de estado organizan y automatizan el proceso y los pasos del marco de aprovisionamiento y las personalizaciones de las cuentas AFT.
- Amazon EventBridge: AFT crea un bus de EventBridge eventos de Amazon en la cuenta de administración de AFT y AWS Control Tower para capturar y almacenar los eventos del ciclo de vida de la Torre de Control de AWS a largo plazo en la tabla DynamoDB de la cuenta de administración de AFT. AFT crea reglas de CloudWatch eventos de AWS en las cuentas de administración de AFT y de administración de AWS Control Tower, que activan varios pasos necesarios durante la ejecución del flujo de trabajo de la canalización de AFT
- AWS CloudTrail (opcional): cuando esta función está habilitada, AFT crea un registro de la CloudTrail organización de AWS en la cuenta de administración de la Torre de Control Tower de AWS para registrar los eventos de datos de los buckets de Amazon S3 y las funciones de AWS Lambda. AFT envía estos registros a un depósito S3 central en la cuenta de archivo de registros de AWS Control Tower.

- AWS Support (opcional): cuando esta función está habilitada, AFT activa el plan AWS Enterprise Support para las cuentas aprovisionadas por AFT. De forma predeterminada, las cuentas de AWS se crean con el plan AWS Basic Support activado.

Canalización de aprovisionamiento de cuentas AFT

Una vez completada la etapa de aprovisionamiento de cuentas de la canalización, el marco AFT continúa. Ejecuta automáticamente una serie de pasos para garantizar que las cuentas recién aprovisionadas cuenten con todos los detalles antes de que comience la Personalizaciones de cuentas etapa.

Estos son los siguientes pasos que sigue el oleoducto AFT.

1. Valida la entrada de la solicitud de cuenta.
2. Recupera información sobre la cuenta aprovisionada, por ejemplo, el ID de la cuenta.
3. Almacena los metadatos de la cuenta en una tabla de DynamoDB en la cuenta de administración de AFT.
4. Crea el rol de AWSAFTExecutionIAM en la cuenta recién aprovisionada. AFT asume esta función para realizar la fase de personalización de la cuenta, ya que esta función otorga acceso a la cartera de la fábrica de cuentas.
5. Aplica las etiquetas de cuenta que proporcionó como parte de los parámetros de entrada de la solicitud de cuenta.
6. Aplica las opciones de funciones de AFT que eligió en el momento de la implementación de AFT.
7. Aplica las personalizaciones de aprovisionamiento de cuentas AFT que proporcionó. La siguiente sección ofrece más información sobre cómo configurar estas personalizaciones con una máquina de estados de AWS Step Functions, en un `git` repositorio. Esta etapa a veces se denomina etapa del marco de aprovisionamiento de cuentas. Forma parte del proceso principal de aprovisionamiento, pero anteriormente has configurado un marco que ofrece integraciones personalizadas como parte del flujo de trabajo de aprovisionamiento de cuentas, antes de añadir personalizaciones adicionales a las cuentas en la siguiente etapa.
8. Para cada cuenta aprovisionada, crea una cuenta de administración AWS CodePipeline en la AFT, que se ejecutará en la siguiente fase (global). Personalizaciones de cuentas
9. Invoca el proceso de personalización de cuentas para cada cuenta aprovisionada (y destinada).
10. Envía una notificación de éxito o error al tema de SNS, desde donde puedes recuperar los mensajes.

Configure las personalizaciones del marco de aprovisionamiento de cuentas con una máquina de estados

Si configura integraciones personalizadas que no son de Terraform antes de aprovisionar sus cuentas, estas personalizaciones se incluyen en el flujo de trabajo de aprovisionamiento de cuentas de AFT. Por ejemplo, es posible que necesite ciertas personalizaciones para garantizar que todas las cuentas creadas por AFT cumplan con los estándares y políticas de su organización, como los estándares de seguridad, y estos estándares pueden agregarse a las cuentas antes de realizar una personalización adicional. Estas personalizaciones del marco de aprovisionamiento de cuentas se implementan en cada cuenta aprovisionada, antes de que comience la siguiente etapa de personalización de la cuenta global.

> **Note**
>
> La función AFT que se describe en esta sección está destinada a usuarios avanzados que entienden el funcionamiento de AWS Step Functions. Como alternativa, le recomendamos que trabaje con los ayudantes globales en la fase de personalización de la cuenta.

El marco de aprovisionamiento de cuentas AFT llama a una máquina de estados AWS Step Functions, que usted define, para implementar sus personalizaciones. Consulte la documentación de AWS Step Functions para obtener más información sobre las posibles integraciones de máquinas de estado.

Estas son algunas de las integraciones más comunes.

- AWS Lambda funciona en el idioma que prefiera
- Tareas de AWS ECS o AWS Fargate, mediante contenedores Docker
- Actividades de AWS Step Functions con trabajadores personalizados, alojadas en AWS o en las instalaciones
- Integraciones de Amazon SNS o SQS

Si no se ha definido ninguna máquina de estados de AWS Step Functions, la etapa pasa sin operación. Para crear una máquina de estados con personalizaciones y aprovisionamiento de cuentas AFT, siga las instrucciones que se indican en. Cree su máquina de estado, personalizaciones, personalizaciones y aprovisionamiento de cuentas AFT. Antes de añadir personalizaciones, asegúrese de cumplir los requisitos previos.

Estos tipos de integraciones no forman parte de la Torre de Control de AWS y no se pueden añadir durante la fase global previa a la API de la personalización de la cuenta AFT. En cambio, la canalización AFT le permite configurar estas personalizaciones como parte del proceso de aprovisionamiento y se ejecutan en el flujo de trabajo de aprovisionamiento. Debe implementar estas personalizaciones creando su máquina de estados con antelación, antes de iniciar la etapa de aprovisionamiento de cuentas AFT, tal y como se describe en las siguientes secciones.

Requisitos previos para crear una máquina de estados

- Una AFT completamente desplegada. Consulte Implemente AWS Control Tower Account Factory para Terraform (AFT) para obtener más información sobre el despliegue de la AFT.
- Configure un `git` repositorio en su entorno para las personalizaciones del aprovisionamiento de cuentas AFT. Para obtener más información, consulte Pasos posteriores a la implementación.

Cree su máquina de estado, personalizaciones, personalizaciones y aprovisionamiento de cuentas AFT.

Paso 1: Modifique la definición de la máquina de estados

Modifique la definición de máquina de `customizations.asl.json` estados del ejemplo. El ejemplo está disponible en el `git` repositorio que configuró para almacenar las personalizaciones de aprovisionamiento de cuentas AFT, en los pasos posteriores a la implementación. Consulte la Guía para desarrolladores de AWS Step Functions para obtener más información sobre las definiciones de máquinas de estado.

Paso 2: Incluya la configuración de Terraform correspondiente

Incluya los archivos de Terraform con la `.tf` extensión en el mismo `git` repositorio con la definición de la máquina de estados para su integración personalizada. Por ejemplo, si decide llamar a una función Lambda en la definición de tarea de la máquina de estados, debe incluir el `lambda.tf` archivo en el mismo directorio. Asegúrese de incluir las funciones y los permisos de IAM necesarios para sus configuraciones personalizadas.

Cuando proporcionas la entrada adecuada, la canalización de AFT invoca automáticamente tu máquina de estados y despliega tus personalizaciones como parte de la fase del marco de aprovisionamiento de cuentas de AFT.

Para reiniciar el marco de aprovisionamiento de cuentas y las personalizaciones de AFT

AFT ejecuta el marco de aprovisionamiento de cuentas y los pasos de personalización para cada cuenta vendida a través de la AFT. Para volver a iniciar las personalizaciones de aprovisionamiento de cuentas, puede utilizar uno de estos dos métodos:

1. Realiza cualquier cambio en una cuenta existente en el repositorio de solicitudes de cuentas.
2. Aprovisione una nueva cuenta con AFT.

Personalizaciones de cuentas

AFT puede implementar configuraciones estándar o personalizadas en las cuentas aprovisionadas. En la cuenta de administración de AFT, AFT proporciona una canalización para cada cuenta. Con esta canalización, puede implementar sus personalizaciones en todas las cuentas, en un conjunto de cuentas o en cuentas individuales. Puede ejecutar scripts de Python, scripts de bash y configuraciones de Terraform, o puede interactuar con la AWS CLI como parte de la etapa de personalización de su cuenta.

Información general

Una vez especificadas las personalizaciones en los `git` repositorios elegidos, ya sea en el repositorio en el que almacene las personalizaciones globales o en el que almacene las personalizaciones de la cuenta, la fase de personalización de la cuenta se completa automáticamente en la fase de personalización de la cuenta. Para personalizar las cuentas de forma retroactiva, consulte. Vuelva a invocar las personalizaciones

Personalizaciones globales (opcional)

Puede optar por aplicar determinadas personalizaciones a todas las cuentas aprovisionadas por AFT. Por ejemplo, si necesita crear un rol de IAM concreto o implementar un control personalizado en cada cuenta, la fase de personalización global de AFT le permitirá hacerlo automáticamente.

Personalizaciones de la cuenta (opcional)

Para personalizar una cuenta individual, o un conjunto de cuentas, de manera diferente a otras cuentas aprovisionadas por AFT, puede aprovechar la parte de personalización de cuentas del proceso de AFT para implementar configuraciones específicas de la cuenta. Por ejemplo, es posible que solo una cuenta determinada requiera acceso a una puerta de enlace de Internet.

Requisitos previos de personalización

Antes de empezar a personalizar las cuentas, asegúrese de que se cumplen estos requisitos previos.

- Una AFT completamente desplegada. Para obtener información sobre cómo realizar la implementación, consulteConfigure y lance su AWS Control Tower Account Factory para Terraform.
- `git`Repositorios prepoblados para personalizaciones globales y personalizaciones de cuentas en su entorno. Consulte el paso 3: Rellenar cada repositorio para obtener más información. Pasos posteriores a la implementación

Aplica personalizaciones globales

Para aplicar las personalizaciones globales, debe insertar una estructura de carpetas específica en el repositorio que elija.

- Si tus configuraciones personalizadas están en forma de programas o scripts de Python, colócalas en la carpeta api_helpers/python de tu repositorio.
- Si tus configuraciones personalizadas están en forma de scripts de Bash, colócalas en la carpeta api_helpers de tu repositorio.
- Si tus configuraciones personalizadas tienen el formato de Terraform, colócalas en la carpeta terraform de tu repositorio.
- Consulta el archivo README de personalizaciones globales para obtener más información sobre la creación de configuraciones personalizadas.

> **Note**
>
> Las personalizaciones globales se aplican automáticamente, una vez finalizada la fase de creación del marco de aprovisionamiento de cuentas AFT.

Aplica personalizaciones de cuentas

Puede aplicar las personalizaciones de la cuenta insertando una estructura de carpetas específica en el repositorio que elija. Las personalizaciones de las cuentas se aplican automáticamente

en el proceso de AFT y después de la fase de personalización global. También puede crear varias carpetas que contengan diferentes personalizaciones de cuentas en su repositorio de personalizaciones de cuentas. Para cada personalización de cuenta que necesites, sigue estos pasos.

Para aplicar las personalizaciones de la cuenta

1. Paso 1: Crea una carpeta para personalizar una cuenta

   En el repositorio que elija, copie la `ACCOUNT_TEMPLATE` carpeta que proporciona AFT en una nueva carpeta. El nombre de su nueva carpeta debe coincidir con el `account_customizations_name` que proporcionó en su solicitud de cuenta.

2. Agrega las configuraciones a la carpeta de personalizaciones de tu cuenta específica

   Puede añadir configuraciones a la carpeta de personalizaciones de su cuenta en función del formato de las configuraciones.

   - Si tus configuraciones personalizadas están en forma de programas o scripts de Python, colócalas en la carpeta ***[account_customizations_name] /api_helpers/python*** que se encuentra en tu repositorio.
   - ***Si tus configuraciones personalizadas están en forma de scripts de Bash, colócalas en la carpeta [account_customizations_name] / api_helpers de tu repositorio.***
   - ***Si tus configuraciones personalizadas tienen el formato de Terraform, colócalas en la carpeta [account_customizations_name] /terraform que se encuentra en tu repositorio.***

   Para obtener más información sobre la creación de configuraciones personalizadas, consulta el archivo README de personalizaciones de cuentas.

3. Consulte el **`account_customizations_name`** parámetro específico en el archivo de solicitud de cuenta

   El archivo de solicitud de cuenta AFT incluye el parámetro de entrada`account_customizations_name`. Introduzca el nombre de la personalización de su cuenta como valor para este parámetro.

> **Note**
>
> Puede enviar varias solicitudes de cuentas para las cuentas de su entorno. Si desea aplicar personalizaciones de cuenta diferentes o similares, especifique las personalizaciones de la cuenta mediante el parámetro de `account_customizations_name` entrada de las solicitudes de cuenta. Para obtener más información, consulta Enviar solicitudes de varias cuentas.

Vuelva a invocar las personalizaciones

AFT proporciona una forma de volver a invocar las personalizaciones en la cartera de AFT. Este método es útil cuando ha agregado un nuevo paso de personalización o cuando está realizando cambios en una personalización existente. Al volver a invocar, AFT inicia el proceso de personalizaciones para realizar cambios en la cuenta aprovisionada por AFT. Al event-source-based volver a invocar, puede aplicar personalizaciones a cuentas individuales, a todas las cuentas, a las cuentas según su OU o a las cuentas seleccionadas según las etiquetas.

Siga estos tres pasos para volver a invocar las personalizaciones de las cuentas aprovisionadas por AFT.

Paso 1: Envía los cambios a los repositorios de personalizaciones globales o de cuentas **`git`**

Puedes actualizar tus personalizaciones globales y de cuenta según sea necesario y devolver los cambios a tus repositorios. `git` En este momento, no pasa nada. Una fuente de eventos debe invocar la canalización de personalizaciones, tal y como se explica en los dos pasos siguientes.

Paso 2: iniciar una ejecución de AWS Step Function para volver a invocar las personalizaciones

AFT proporciona una función AWS Step llamada `aft-invoke-customizations` en la cuenta de administración de AFT. El propósito de esa función es volver a invocar el proceso de personalización de las cuentas aprovisionadas por AFT.

Este es un ejemplo de un esquema de eventos (formato JSON) que puede crear para pasar la entrada a la `aft-invoke-customizations` AWS Step Function.

```
{
  "include": [
    {
      "type": "all"
```

```
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],

  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

El ejemplo de esquema de eventos muestra que puede elegir cuentas para incluirlas o excluirlas del proceso de reinvocación. Puedes filtrar por unidad organizativa (OU), etiquetas de cuenta e ID de cuenta. Si no aplicas ningún filtro e incluyes la declaración`"type":"all"`, se volverá a invocar la personalización de todas las cuentas aprovisionadas por AFT.

> **Note**
>
> Si su versión de AWS Control Tower es la 1.6.5 o posterior, puede segmentar las unidades organizativas anidadas (con la sintaxis`OU Name (ou-id-1234)`. Para obtener más información, consulte el siguiente tema sobre. GitHub

Tras rellenar los parámetros del evento, Step Functions ejecuta e invoca las personalizaciones correspondientes. AFT puede invocar un máximo de 5 personalizaciones a la vez. Step Functions espera y se repite hasta que se completen todas las cuentas que cumplen los criterios del evento.

Paso 3: Supervise el resultado de AWS Step Function y observe cómo CodePipeline funciona AWS

- El resultado de Step Function contiene identificadores de cuenta que coinciden con la fuente del evento de entrada de Step Function.
- Diríjase a AWS CodePipeline en Herramientas para desarrolladores y consulte las canalizaciones de personalización correspondientes al ID de la cuenta.

Solución de problemas con el seguimiento de las solicitudes de personalización de la cuenta AFT

Flujos de trabajo de personalización de cuentas que se basan en registros de AWS Lambda emisiones que contienen los ID de la cuenta de destino y de las solicitudes de personalización. AFT le permite rastrear las solicitudes de personalización y solucionar problemas con Amazon CloudWatch Logs al proporcionarle consultas de CloudWatch Logs Insights que puede usar para filtrar CloudWatch los registros relacionados con su solicitud de personalización por su cuenta de destino o ID de solicitud de personalización. Para obtener más información, consulte Análisis de datos de registro con Amazon CloudWatch Logs en la Guía del usuario de Amazon CloudWatch Logs.

Para utilizar CloudWatch Logs Insights para AFT

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, selecciona Registros y, a continuación, selecciona Logs insights.
3. Elija Consultas.
4. En Consultas de muestra, elige Account Factory for Terraform y, a continuación, selecciona una de las siguientes consultas:

   - Registros de personalización por ID de cuenta

   > **Note**
   >
   > Asegúrate de reemplazar *«YOUR-ACCOUNT-ID» por tu ID* de cuenta objetivo.

```
fields @timestamp, log_message.account_id as target_account_id,
 log_message.customization_request_id as customization_request_id,
 log_message.detail as detail, @logStream
| sort @timestamp desc
| filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
customization_request_id/
```

- Registros de personalización por ID de solicitud de personalización

> **Note**
>
> Asegúrese de reemplazar *«YOUR-CUSTOMIZATION-REQUEST-ID» por el ID de su solicitud de personalización*. Puede encontrar el ID de su solicitud de personalización en la salida de la máquina de estados del marco de aprovisionamiento de cuentas AFT. AWS Step Functions Para obtener más información sobre el marco de aprovisionamiento de cuentas AFT, consulte Canalización de aprovisionamiento de cuentas AFT

```
fields @timestamp, log_message.account_id as target_account_id,
 log_message.customization_request_id as customization_request_id,
 log_message.detail as detail, @logStream
| sort @timestamp desc
| filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
```

5. Después de seleccionar una consulta, asegúrese de seleccionar un intervalo de tiempo y, a continuación, elija Ejecutar consulta.

Alternativas para el control de versiones del código fuente en AFT

AFT utiliza AWS CodeCommit de forma nativa un sistema de control de versiones de código fuente (VCS), pero permite otros CodeConnectionsque cumplan con los requisitos de su negocio o con la arquitectura existente. Puede especificar un VCS de terceros como parte de los requisitos previos de implementación de AFT.

AFT admite las siguientes alternativas de control del código fuente:

- GitHub

- GitHub Servidor empresarial
- BitBucket

Si lo selecciona AWS CodeCommit como su VCS, no es necesario realizar ningún paso adicional. De forma predeterminada, AFT crea los `git` repositorios necesarios en su entorno, con los nombres predeterminados. Sin embargo, puede anular los nombres de los repositorios predeterminados CodeCommit, según sea necesario, para cumplir con los estándares de su organización.

Configure un sistema de control de versiones de código fuente alternativo (VCS personalizado) con AFT

Para configurar un sistema de control de versiones de código fuente alternativo para su implementación de AFT, siga estos pasos.

Paso 1: Cree **`git`** repositorios en un sistema de control de versiones (VCS) de terceros compatible.

Si no los utiliza AWS CodeCommit, debe crear `git` repositorios en su entorno de proveedor de VCS externo compatible con AFT para los siguientes elementos.

- Solicitudes de cuentas AFT. Código de muestra disponible. Para obtener más información sobre las solicitudes de cuentas AFT, consulteAprovisione una nueva cuenta con AFT.
- Personalizaciones de aprovisionamiento de cuentas AFT. Código de muestra disponible. Para obtener más información sobre las personalizaciones del aprovisionamiento de cuentas AFT, consulte. Cree su máquina de estado, personalizaciones, personalizaciones y aprovisionamiento de cuentas AFT.
- Personalizaciones globales de AFT. Código de muestra disponible. Para obtener más información sobre las personalizaciones globales de AFT, consultePersonalizaciones de cuentas.
- Personalizaciones de cuentas AFT. Código de muestra disponible. Para obtener más información sobre las personalizaciones de las cuentas AFT, consultePersonalizaciones de cuentas.

Paso 2: Especifique los parámetros de configuración del VCS necesarios para el despliegue de AFT

Los siguientes parámetros de entrada son necesarios para configurar su proveedor de VCS como parte del despliegue de AFT.

- vcs_provider: Si no lo está utilizando AWS CodeCommit, especifique el proveedor de VCS como`"bitbucket"`, o `"github""githubenterprise"`, según su caso de uso.

- github_enterprise_url: solo para clientes empresariales, especifique la URL. GitHub GitHub
- account_request_repo_name: de forma predeterminada, este valor está establecido en para los usuarios. `aft-account-request` AWS CodeCommit Si ha creado el repositorio con un nombre nuevo en CodeCommit o dentro de un entorno de proveedores de VCS de terceros compatible con AFT, actualice este valor de entrada con el nombre real de su repositorio. BitBucketEn Github y GitHub Enterprise, el nombre del repositorio debe tener ese formato. `[Org]/[Repo]`
- account_customizations_repo_name: de forma predeterminada, este valor está establecido en para los usuarios. `aft-account-customizations` AWS CodeCommit Si ha creado un repositorio con un nombre nuevo en CodeCommit o dentro de un entorno de proveedores de VCS de terceros compatible con AFT, actualice este valor de entrada con el nombre de su repositorio. BitBucketEn Github y GitHub Enterprise, el nombre del repositorio debe tener ese formato. `[Org]/[Repo]`
- account_provisioning_customizations_repo_name: de forma predeterminada, este valor está establecido en para los usuarios. `aft-account-provisioning-customizations` AWS CodeCommit Si ha creado un repositorio con un nombre nuevo en AWS CodeCommit o dentro de un entorno de proveedores de VCS de terceros compatible con AFT, actualice este valor de entrada con el nombre de su repositorio. BitBucketEn Github y GitHub Enterprise, el nombre del repositorio debe tener ese formato`[Org]/[Repo]`.
- global_customizations_repo_name: de forma predeterminada, este valor se establece en para los usuarios. `aft-global-customizations` AWS CodeCommit Si creó el repositorio con un nombre nuevo en CodeCommit o en un entorno de proveedores de VCS de terceros compatible con AFT, actualice este valor de entrada con el nombre de su repositorio. BitBucketEn Github y GitHub Enterprise, el nombre del repositorio debe tener ese formato. `[Org]/[Repo]`
- account_request_repo_branch: La rama es la `main` predeterminada, pero el valor se puede anular.

De forma predeterminada, AFT se extrae de la rama de cada repositorio. `main` `git` Puede anular el valor del nombre de la sucursal con un parámetro de entrada adicional. Para obtener más información sobre los parámetros de entrada, consulte el archivo README del módulo AFT Terraform.

Paso 3: Complete la AWS CodeStar conexión para los proveedores de VCS de terceros

Cuando se ejecuta su implementación, AFT crea los AWS CodeCommit repositorios necesarios o crea una AWS CodeStar conexión para el proveedor de VCS externo que elija. En este último caso, debe iniciar sesión manualmente en la consola de la cuenta de administración de AFT para completar la conexión pendiente AWS CodeStar . Consulte la AWS CodeStar documentación para obtener más instrucciones sobre cómo completar la AWS CodeStar conexión.

Protección de datos

El modelo de responsabilidadAWS compartida se aplica a la protección de datos en AFT. Para fines de protección de datos, recomendamos las siguientes mejores prácticas de seguridad.

- Siga las directrices de protección de datos proporcionadas por AWS Control Tower. Para obtener más detalles, consulte Protección de datos en AWS Control Tower.
- Conserve la configuración de estado de Terraform generada en el momento de la implementación de AFT. Para obtener más detalles, consulte Implemente AWS Control Tower Account Factory para Terraform (AFT).
- Cambie periódicamente las credenciales confidenciales según lo indique la política de seguridad de su organización. Algunos ejemplos de secretos son las fichas de Terraform, las `git` fichas, etc.

Cifrado en reposo

AFT crea depósitos de Amazon S3, temas de Amazon SNS, colas de Amazon SQS y bases de datos de Amazon DynamoDB que se cifran en reposo con claves del Servicio de administración de claves. AWS Las claves KMS creadas por AFT tienen habilitada la rotación anual de forma predeterminada. Si elige las distribuciones Terraform Cloud o Terraform Enterprise de Terraform, AFT incluye un SecureString parámetro de AWS Systems Manager para almacenar los valores de los tokens de Terraform que son confidenciales.

AFT utiliza AWS los servicios descritos en Servicios de componentes que, de forma predeterminada, están cifrados en reposo. Para obtener más información, consulte la AWS documentación de cada AWS servicio componente de AFT y conozca las prácticas de protección de datos que sigue cada servicio.

Cifrado en tránsito

AFT se basa en AWS los servicios descritos en Servicios de componentes que emplean el cifrado en tránsito, de forma predeterminada. Para obtener más información, consulte la AWS documentación de cada AWS servicio componente de AFT y conozca las prácticas de protección de datos que sigue cada servicio.

En el caso de las distribuciones de Terraform Cloud o Terraform Enterprise, AFT utiliza una API de punto final HTTPS para acceder a su organización de Terraform. Si elige un proveedor de VCS externo compatible con AWS CodeStar conexiones, AFT llama a una API de punto final HTTPS para acceder a su organización proveedora de VCS.

Eliminar una cuenta de AFT

En este tema se describe cómo eliminar una cuenta de AFT para que la canalización de AFT deje de implementar y actualizar la cuenta.

> **Important**
>
> Eliminar una cuenta de la cartera de AFT es irreversible y puede provocar la pérdida de estado.

Puede eliminar una cuenta de AFT cuando desee cerrar una cuenta para una solicitud retirada, aislar una cuenta comprometida o mover una cuenta de una organización a otra.

> **Note**
>
> Eliminar una cuenta de AFT es diferente a eliminar una cuenta de AWS Control Tower o Cuenta de AWS. Al eliminar una cuenta de AFT, AWS Control Tower sigue administrándola. Para eliminar una cuenta de AWS Control Tower o Cuenta de AWS, consulte lo siguiente:
>
> - Elimine la administración de una cuenta en la Guía del usuario de AWS Control Tower.
> - Cerrar una cuenta en la Guía delAWS Billing usuario.

Para eliminar una cuenta de los oleoductos de la AFT

El siguiente procedimiento describe cómo eliminar una cuenta de AFT.

1. Elimine la cuenta del **`git`** repositorio que almacena las solicitudes de cuenta

   En el `git` repositorio donde almacena las solicitudes de cuenta, elimine la solicitud de cuenta de la cuenta que desee eliminar de AFT.

   Al eliminar una solicitud de cuenta del repositorio de solicitudes de cuenta, AFT elimina la canalización de personalización y los metadatos de la cuenta. Para obtener más información, consulte las notas de la versión 1.8.0 de AFT on. GitHub
2. Eliminar el espacio de trabajo de Terraform (solo para clientes de Terraform Cloud y Terraform Enterprise)

Elimine las personalizaciones globales y los espacios de trabajo de personalización de cuentas de la cuenta que desee eliminar de AFT.

3. Eliminar el estado de Terraform del backend de Amazon S3

   En la cuenta de administración de AFT, elimine todas las carpetas relevantes dentro de los buckets de Amazon S3 de la cuenta que desee eliminar de AFT.

   > **Tip**
   >
   > En los siguientes ejemplos, sustitúyalo por *012345678901* el número de identificación de la cuenta de administración de AFT.

   Ejemplo: Terraform OSS

   Al elegir Terraform OSS, encontrará 3 carpetas para cada cuenta en los buckets `aft-backend-`*012345678901*`-primary-region` y `aft-backend-`*012345678901*`-secondary-region` Amazon S3. Estas carpetas están relacionadas con el estado de las personalizaciones de la cuenta, el estado de la canalización de las personalizaciones y el estado de las personalizaciones globales

   Ejemplo: Terraform Cloud o Terraform Enterprise

   Al elegir Terraform Cloud o Terraform Enterprise, encontrará una carpeta para cada cuenta en los buckets `aft-backend-`*012345678901*`-primary-region` y `aft-backend-`*012345678901*`-secondary-region` Amazon S3. Estas carpetas están relacionadas con el estado del proceso de personalización.

Métricas operativas

De forma predeterminada, Account Factory for Terraform (AFT) envía métricas operativas anónimas a AWS. Usamos estos datos para entender cómo los clientes utilizan AFT y así poder mejorar la calidad y las características de la solución. Puede optar por no participar en la recopilación de datos cambiando un parámetro durante la implementación de AFT. Cuando la recopilación está habilitada, se envían los siguientes datos a AWS:

- Solución: el identificador específico de AFT

- Versión: La versión de AFT
- Identificador único universal (UUID): identificador único generado aleatoriamente para cada implementación de AFT
- Timestamp: timestamp de recopilación de datos
- Datos: configuración de AFT y medidas adoptadas por el cliente

AWS es propietario de los datos recopilados. La recopilación de datos está sujeta a la AWS Política de privacidad.

> **Note**
>
> Las versiones de AFT anteriores a la 1.6.0 no informan sobre las métricas de uso. AWS

Para excluirse de la presentación de informes sobre las métricas:

- Defina el valor de `aft_metrics_reporting` entrada `false` en su archivo de configuración de entradas de Terraform, como se muestra en el siguiente ejemplo, y vuelva a implementar AFT. Este valor se establece en forma `true` predeterminada, si no lo establece de forma explícita.

Si copia el ejemplo, recuerde sustituir los valores reales de ID y región por los elementos que aparecen en las cadenas por`x`.

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
ct_home_region              = "xx-xxxx-x"
tf_backend_secondary_region = "xx-xxxx-x"

# Optional Vars
aft_metrics_reporting = false    # to opt out, set this value to false
}
```

Guía de solución de problemas de Account Factory for Terraform (AFT)

Esta sección puede ayudarlo a solucionar problemas comunes que pueden surgir al usar Account Factory for Terraform (AFT).

Temas

Problemas generales

- Se superaron las cuotas AWS de recursos

  Si sus grupos de registros indican que ha superado las cuotas de AWS recursos, póngase en contacto con AWS Support. Account Factory utiliza Servicios de AWS cuotas de recursos que incluyen AWS CodeBuild AWS Organizations, y AWS Systems Manager. Para más información, consulte los siguientes temas:

  - ¿Qué es AWS CodeBuild? en la Guía CodeBuild del usuario.
  - ¿Qué es AWS Organizations? en la Guía del usuario de Organizations.
  - ¿Qué es AWS Systems Manager? en la Guía del usuario de Systems Manager.
- Versión desactualizada de Account Factory

  Si encuentras un problema y crees que se trata de un error, asegúrate de tener la última versión de Account Factory. Para obtener más información, consulta Actualización de la versión Account Factory.
- Se realizaron cambios locales en el código fuente de Account Factory

  Account Factory es un proyecto de código abierto. AWS Control Tower es compatible con el código principal de Account Factory. Si realiza un cambio local en el código principal de Account Factory, AWS Control Tower solo admite su implementación de Account Factory si hace todo lo posible.
- Permisos de rol de Account Factory insuficientes

  Account Factory crea funciones y políticas de IAM para gestionar las implementaciones y personalizaciones de cuentas vendidas. Si cambias estas funciones o políticas, es posible que

la canalización de Account Factory no pueda realizar determinadas acciones. Para obtener más información, consulta Funciones obligatorias.

- Los repositorios de cuentas no se rellenan correctamente

  Asegúrese de seguir los pasos posteriores a la implementación antes de aprovisionar las cuentas.

- No se detecta una desviación después de cambiar la unidad organizativa manualmente

  > **Note**
  >
  > AWS Control Tower detecta la desviación automáticamente. Para obtener información sobre la resolución de desviaciones, consulte Detectar y resolver desviaciones en AWS Control Tower.

  La desviación no se detecta cuando la unidad organizativa (OU) se cambia manualmente. Esto se debe a la naturaleza de Account Factory basada en eventos. Cuando se envía una solicitud de cuenta, el recurso que Terraform administra es un elemento de Amazon DynamoDB, no una cuenta directa. Cuando se cambia un elemento, la solicitud pasa a una cola, donde AWS Control Tower la procesa a través de Service Catalog (el servicio que administra los detalles de la cuenta). Si cambia la OU manualmente, no se detectará ningún cambio porque la solicitud de cuenta no ha cambiado.

Problemas relacionados con el aprovisionamiento o el registro de cuentas

- La solicitud de cuenta (dirección de correo electrónico/nombre) ya existe

  El problema suele provocar un error en el producto de Service Catalog durante el aprovisionamiento o durante el aprovisionamiento. `ConditionalCheckFailedException`

  Para obtener más información sobre el problema, realice una de las siguientes acciones:

  - Revisa tus grupos de registros de Terraform o CloudWatch Logs.
  - Revise los errores que se emiten en el tema Amazon SNS. `aft-failure-notifications`

- Solicitud de cuenta con un formato incorrecto

  Asegúrese de que la solicitud de su cuenta siga el esquema esperado. Para ver ejemplos, consulta terraform-aws-control_tower_account_factory en. GitHub

- Se superaron AWS las cuotas de recursos de Organizations

Asegúrese de que la solicitud de su cuenta no supere las cuotas AWS Organizations de recursos. Para obtener más información, consulte Quotas for AWS Organizations.

Problemas relacionados con la invocación de personalizaciones

- La cuenta de destino no está incorporada a Account Factory

  Asegúrese de que todas las cuentas incluidas en una solicitud de personalización se hayan incorporado a Account Factory. Para obtener más información, consulta Actualizar una cuenta existente.
- La cuenta a la que se dirige la solicitud de personalización existe en la **`aft-request-metadata`** tabla de DynamoDB, pero no en el repositorio de solicitudes de cuenta

  Formatee la solicitud de invocación de personalización para excluir la cuenta infractora mediante una de las siguientes acciones:
  - En la `aft-request-metadata` tabla de DynamoDB, elimine la entrada que hace referencia a la cuenta que ya no está en el repositorio de solicitudes de cuentas.
  - No usar «todos» como objetivo.
  - No segmentar la unidad organizativa a la que pertenece la cuenta.
  - No se dirige directamente a la cuenta.
- Se utilizó un token incorrecto para Terraform Cloud

  Asegúrese de configurar el token correcto. Terraform Cloud solo admite fichas basadas en equipos, no en fichas basadas en organizaciones.
- No se pudo crear la cuenta antes de crear la canalización de personalizaciones de la cuenta; no se puede personalizar la cuenta

  Realiza un cambio en la especificación de la cuenta en el repositorio de solicitudes de cuentas. Cuando realizas un cambio, como cambiar el valor de una etiqueta para una cuenta, Account Factory sigue la ruta que intenta crear la canalización, incluso si la canalización no existe.

Problemas relacionados con el flujo de trabajo de personalización de la cuenta

Si tiene problemas relacionados con el flujo de trabajo de personalización de cuentas, asegúrese de que su versión de AFT sea la 1.8.0 o superior y de eliminar todas las instancias de metadatos relacionados con la cuenta de la tabla de solicitudes de DynamoDB.

Para obtener información sobre la versión 1.8.0 de AFT, consulte la versión 1.8.0 en adelante.
GitHub

Para obtener información sobre cómo comprobar y actualizar su versión de AFT, consulte lo siguiente:

- Compruebe la versión AFT
- Actualice la versión AFT

También puede rastrear las solicitudes de personalización y solucionar sus problemas mediante consultas de Amazon CloudWatch Logs Insights para filtrar los registros que contienen su cuenta de destino y los ID de solicitud de personalización. Para obtener más información, consulte Solución de problemas relacionados con el seguimiento de las solicitudes de personalización de la cuenta AFT.

Detecte y resuelva desviaciones en la Torre de Control de AWS

Identificar y resolver las desviaciones es una tarea operativa habitual de los administradores de cuentas de administración de la Torre de Control Tower de AWS. Resolver los errores ayuda a garantizar el cumplimiento de los requisitos de gobierno.

Cuando creas tu landing zone, la zona de aterrizaje y todas las unidades organizativas (OU), cuentas y recursos cumplen con las normas de gobierno aplicadas por los controles que hayas elegido. A medida que tú y los miembros de tu organización uséis la landing zone, es posible que se produzcan cambios en este estado de conformidad. Algunos cambios pueden ser accidentales, mientras que otros pueden realizarse a propósito para dar respuesta a eventos operativos en los que el tiempo es crucial.

La detección de la desviación ayuda a identificar recursos que necesitan cambios o actualizaciones de configuración para resolver la desviación.

Detectando la deriva

AWS Control Tower detecta la desviación automáticamente. Para detectar desviaciones, el `AWSControlTowerAdmin` rol requiere un acceso permanente a su cuenta de administración para que AWS Control Tower pueda realizar llamadas a la API de solo lectura. AWS Organizations Estas llamadas a la API se muestran como AWS CloudTrail eventos.

La desviación aparece en las notificaciones del Amazon Simple Notification Service (Amazon SNS) que se agregan a la cuenta de auditoría. Las notificaciones de cada cuenta de miembro envían alertas a un tema local de Amazon SNS y a una función de Lambda.

En el caso de los controles que forman parte del AWS Security Hub estándar gestionado por servicios: AWS Control Tower, los cambios se muestran en las páginas Cuenta y Detalles de la cuenta de la consola de AWS Control Tower, así como mediante una notificación de Amazon SNS.

Los administradores de cuentas de miembro pueden (y, como práctica recomendada, deben) suscribirse a las notificaciones de desviación de SNS para cuentas específicas. Por ejemplo, en el tema `aws-controltower-AggregateSecurityNotifications` SNS se proporcionan notificaciones de desviaciones. La consola de AWS Control Tower indica a los administradores de cuentas de administración cuándo se ha producido un desvío. Para obtener más información

sobre los temas de las redes sociales relacionados con la detección y notificación de desviaciones, consulte Prevención y notificación de desviaciones.

Deduplicación de notificaciones de deriva

Si se produce el mismo tipo de desviación en el mismo conjunto de recursos varias veces, AWS Control Tower envía una notificación de SNS solo para la instancia inicial de desviación. Si AWS Control Tower detecta que se ha corregido este caso de desviación, envía otra notificación solo si la desviación se repite en el caso de esos recursos idénticos.

Ejemplos: la desviación de cuentas y la desviación de SCP se gestionan de la siguiente manera

- Si modifica el mismo SCP gestionado varias veces, recibirá una notificación la primera vez que lo modifique.
- Si modifica un SCP gestionado, corrige la desviación y, a continuación, lo modifica de nuevo, recibirá dos notificaciones.
- Si una cuenta se mueve entre las mismas unidades organizativas de origen y destino varias veces, sin reparar primero la desviación, se envía una única notificación, aunque la cuenta se haya trasladado de una unidad organizativa a otra más de una vez.

Tipos de desviaciones de cuentas

- La cuenta se trasladó entre unidades organizativas
- Cuenta eliminada de la organización

> **Note**
>
> Al mover una cuenta de una OU a otra, no se eliminan los controles de la OU anterior. Si habilita cualquier control nuevo basado en ganchos en la unidad organizativa de destino, la antigua El control basado en ganchos se elimina de la cuenta y el nuevo control lo reemplaza. Los controles implementados con los SCP y AWS Config las reglas siempre deben eliminarse manualmente cuando una cuenta cambia de unidad organizativa.

Tipos de desviaciones políticas

- SCP actualizado

- SCP adjunto a la OU
- SCP separado de la OU
- SCP adjunto a la cuenta

Para obtener más información, consulte Types of Governance Drift.

Resolver la deriva

Aunque la detección es automática, los pasos para resolver la desviación deben realizarse a través de la consola.

- Se pueden resolver muchos tipos de deriva a través de la página de configuración de la zona de aterrizaje. Puedes pulsar el botón Restablecer en la sección de versiones para resolver estos tipos de deriva.
- Si su OU tiene menos de 300 cuentas, puede resolver el problema de las cuentas aprovisionadas por Account Factory (SCP) seleccionando Volver a registrar la OU en la página de la organización o en la página de detalles de la OU.
- Es posible que pueda resolver el cambio de cuenta, por ejemplo, actualizando una cuenta individual. Cuenta de miembro trasladada Para obtener más información, consulte Actualiza la cuenta en la consola.

⚠ Cuando tomas medidas para resolver la deriva en una versión de landing zone, es posible que se produzcan dos comportamientos.

- Si utiliza la versión más reciente de landing zone, al seleccionar Restablecer y, a continuación, elegir Confirmar, los recursos de la zona de aterrizaje a la deriva se restablecerán a la configuración guardada de la Torre de Control de AWS. La versión de landing zone sigue siendo la misma.
- Si no tienes la última versión, debes elegir Actualizar. La zona de aterrizaje se ha actualizado a la última versión de la zona de aterrizaje. La deriva se resuelve como parte de este proceso.

Consideraciones sobre la deriva y los escaneos SCP

AWS Control Tower escanea los SCP gestionados a diario para comprobar que los controles correspondientes se aplican correctamente y que no se han desviado. Para recuperar los SCP y comprobarlos, AWS Control Tower llama AWS Organizations en su nombre utilizando un rol en su cuenta de administración.

Si un escaneo de la Torre de Control de AWS detecta una desviación, recibirá una notificación. AWS Control Tower envía solo una notificación por cada problema de deriva, por lo que si su zona de aterrizaje ya se encuentra en un estado de deriva, no recibirá notificaciones adicionales a menos que encuentre un nuevo elemento de deriva.

AWS Organizations limita la frecuencia con la que se puede llamar a cada una de sus API. Este límite se expresa en transacciones por segundo (TPS) y se conoce como límite de TPS, tasa de aceleración o tasa de solicitudes de API. Cuando AWS Control Tower audita sus SCP mediante una llamada AWS Organizations, las llamadas a la API que realiza AWS Control Tower se tienen en cuenta para su límite de TPS, ya que AWS Control Tower utiliza la cuenta de administración para realizar las llamadas.

En raras ocasiones, este límite se puede alcanzar si llama repetidamente a las mismas API, ya sea a través de una solución de terceros o de un script personalizado que haya creado. Por ejemplo, si usted y AWS Control Tower llaman a las mismas AWS Organizations API en el mismo momento (en menos de 1 segundo) y se alcanzan los límites de TPS, las llamadas posteriores se limitan. Es decir, estas llamadas devuelven un error como: `Rate exceeded`

Si se supera una tasa de solicitudes de API

- Si AWS Control Tower alcanza el límite y se ralentiza, pausaremos la ejecución de la auditoría y la reanudaremos más adelante.
- Si su carga de trabajo alcanza el límite y se reduce, el resultado puede variar desde una latencia leve hasta un error grave en la carga de trabajo, en función de cómo esté configurada la carga de trabajo. Este caso extremo es algo que hay que tener en cuenta.

Un escaneo SCP diario consiste en

1. Recuperar sus unidades organizativas activas recientemente.

2. Para cada unidad organizativa registrada, se recuperan todos los SCP administrados por AWS Control Tower que están conectados a la unidad organizativa. Los SCP administrados tienen identificadores que comienzan por. `aws-guardrails`
3. Para cada control preventivo habilitado en la OU, verificar que la declaración de política del control esté presente en los SCP gestionados por la OU.

Una OU puede tener uno o más SCP administrados.

Tipos de deriva que se deben resolver de inmediato

Los administradores pueden resolver la mayoría de los tipos de desviación. Hay algunos tipos de errores que deben resolverse de inmediato, incluida la eliminación de una unidad organizativa que requiera la zona de aterrizaje de AWS Control Tower. Estos son algunos ejemplos de desviaciones importantes que tal vez desee evitar:

- No elimine la unidad organizativa de seguridad: no se debe eliminar la unidad organizativa denominada originalmente Security during landing zone setup por AWS Control Tower. Si la eliminas, verás un mensaje de error en el que se te indica que debes restablecer la landing zone inmediatamente. No podrá realizar ninguna otra acción en AWS Control Tower hasta que se complete el restablecimiento.
- No elimine las funciones obligatorias: AWS Control Tower comprueba determinadas funciones AWS Identity and Access Management (de IAM) al iniciar sesión en la consola para detectar la desviación de funciones de IAM. Si estas funciones faltan o son inaccesibles, verás una página de error en la que se te indica que restablezcas tu landing zone. Estos roles son. `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRole` `AWSControlTowerStackSetRole`

  Para obtener más información sobre estas funciones, consultePermisos necesarios para usar la consola de la Torre de Control de AWS.
- No elimine todas las unidades organizativas adicionales: si elimina la unidad organizativa originalmente denominada Sandbox durante la configuración de la zona de aterrizaje por parte de AWS Control Tower, su zona de aterrizaje estará en un estado de deriva, pero podrá seguir utilizando AWS Control Tower. Se necesita al menos una OU adicional para que la Torre de Control de AWS funcione, pero no tiene que ser la OU Sandbox.
- No elimines las cuentas compartidas: si eliminas las cuentas compartidas de las unidades organizativas fundamentales, por ejemplo, si eliminas la cuenta de registro de la unidad

organizativa de seguridad, tu landing zone estará en un estado de deriva. Debe restablecer la zona de aterrizaje para poder seguir utilizando la consola de AWS Control Tower.

Cambios reparables en los recursos

Esta es una lista de los cambios en los recursos de la Torre de Control Tower de AWS que están permitidos, aunque generan desviaciones solucionables. Los resultados de estas operaciones permitidas se pueden ver en la consola de la Torre de Control Tower de AWS, aunque puede ser necesaria una actualización.

Para obtener más información sobre cómo resolver el problema resultante, consulte Administrar recursos fuera de la Torre de Control de AWS.

Se permiten cambios fuera de la consola de la Torre de Control de AWS

- Cambie el nombre de una unidad organizativa registrada.
- Cambie el nombre de la unidad organizativa de seguridad.
- Cambie el nombre de las cuentas de los miembros en las unidades organizativas no fundamentales.
- Cambie el nombre de las cuentas compartidas de AWS Control Tower en la unidad organizativa de seguridad.
- Elimine una unidad organizativa que no sea fundamental.
- Elimine una cuenta inscrita de una OU no fundacional.
- Cambie la dirección de correo electrónico de una cuenta compartida en la OU de seguridad.
- Cambie la dirección de correo electrónico de una cuenta de miembro en una OU registrada.

> **Note**
>
> Mover cuentas entre unidades organizativas se considera un error y debe resolverse.

Desviación y aprovisionamiento de nuevas cuentas

Si su landing zone se encuentra en un estado de deriva, la función Inscribir una cuenta de AWS Control Tower no funcionará. En ese caso, debe aprovisionar nuevas cuentas a través de AWS

Service Catalog. Para ver instrucciones, consulte Aprovisione cuentas con AWS Service Catalog Account Factory .

En concreto, si ha realizado algunos cambios en sus cuentas a través de Service Catalog, como cambiar el nombre de su cartera, la función de inscripción de cuentas no funcionará.

Tipos de desviaciones de gobernanza

Los cambios en la gobernanza, también denominados cambios organizativos, se producen cuando se modifican o actualizan las OU, los SCP y las cuentas de los miembros. Los tipos de desviaciones en la gobernanza que se pueden detectar en la Torre de Control de AWS son los siguientes:

- Cuenta de miembro trasladada
- Cuenta de miembro eliminada
- Actualización no programada para SCP administrada
- SCP asociada a cuenta de miembro
- SCP asociada a OU administrada
- SCP desvinculada de OU administrada
- Se ha eliminado la unidad organizativa fundamental
- Desviación de control de Security Hub
- Acceso de confianza desactivado

Otro tipo de deriva es la deriva de la zona de aterrizaje, que se puede encontrar en la cuenta de administración. La desviación de la zona de destino consiste en la desviación de las funciones de IAM o cualquier tipo de desviación organizacional que afecte específicamente a las unidades organizativas fundamentales y a las cuentas compartidas.

Un caso especial de desviación en la zona de landing zone es la desviación de roles, que se detecta cuando no hay disponible un rol requerido. Si se produce este tipo de desviación, la consola muestra una página de advertencia y algunas instrucciones sobre cómo restablecer el rol. Tu landing zone no estará disponible hasta que se resuelva el cambio de roles. Para obtener más información sobre la deriva, consulta No eliminar los roles obligatorios en la sección denominadaTipos de deriva que se deben resolver de inmediato.

AWS Control Tower no busca desviaciones con respecto a otros servicios que funcionan con la cuenta de administración CloudTrail CloudWatch, como el IAM Identity Center AWS CloudFormation

AWS Config, etc. No se permite la detección de desviaciones en las cuentas secundarias, ya que estas cuentas están protegidas por controles preventivos obligatorios.

Sin embargo, sí informa de desviaciones con respecto a los controles que forman parte del estándar de AWS Security Hub administración de servicios: AWS Control Tower.

Cuenta de miembro trasladada

Este tipo de desviación se produce en la cuenta y no en la OU. Este tipo de desviación puede producirse cuando la cuenta de un miembro de la Torre de Control de AWS, la cuenta de auditoría o la cuenta del archivo de registros se traslada de una unidad organizativa de la Torre de Control de AWS registrada a cualquier otra unidad organizativa. El siguiente es un ejemplo de la notificación de Amazon SNS cuando se detecta este tipo de desviación.

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 300 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

Soluciones

Cuando se produce este tipo de desviación en una cuenta aprovisionada por Account Factory en una OU con hasta 300 cuentas, puede resolverlo de la siguiente manera:

- Vaya a la página de la organización en la consola de la Torre de Control de AWS, seleccione la cuenta y elija Actualizar cuenta en la parte superior derecha (la opción más rápida para cuentas individuales).

- Vaya a la página de la organización en la consola de la Torre de Control de AWS y, a continuación, seleccione Volver a registrarse en la OU que contiene la cuenta (la opción más rápida para varias cuentas). Para obtener más información, consulte Registrar una unidad organizativa existente en AWS Control Tower.
- Actualización del producto aprovisionado en Account Factory. Para obtener más información, consulte Actualice y mueva cuentas de fábrica con AWS Control Tower o con AWS Service Catalog.

  > **Note**
  >
  > Si tiene varias cuentas individuales que actualizar, consulte también este método para realizar actualizaciones con un script:Aprovisione y actualice las cuentas mediante la automatización.

- Cuando este tipo de desviación se produce en una OU con más de 300 cuentas, la resolución puede depender del tipo de cuenta que se haya trasladado, como se explica en los párrafos siguientes. Para obtener más información, consulte Actualizar la zona de inicio.
  - Si se traslada una cuenta aprovisionada por Account Factory: en una OU con menos de 300 cuentas, puedes resolver el problema actualizando el producto aprovisionado en Account Factory, volviendo a registrar la OU o actualizando tu landing zone.

    En una OU con más de 300 cuentas, debe resolver el problema realizando una actualización en cada cuenta trasladada, ya sea a través de la consola de AWS Control Tower o del producto aprovisionado, ya que volver a registrar la OU no realizará la actualización. Para obtener más información, consulte Actualice y mueva cuentas de fábrica con AWS Control Tower o con AWS Service Catalog.
  - Si se traslada una cuenta compartida: actualiza tu landing zone para resolver el problema que supone el traslado de la cuenta de auditoría o del archivo de registros. Para obtener más información, consulte Actualizar la zona de inicio.

> **Nombre de campo obsoleto**
>
> Se `MasterAccountID` ha cambiado el nombre del campo para `ManagementAccountID` cumplir con las AWS directrices. El nombre anterior está obsoleto. A partir de 2022, los scripts que contengan el nombre de campo obsoleto dejarán de funcionar.

Cuenta de miembro eliminada

Este tipo de desviación puede producirse cuando se elimina la cuenta de un miembro de una unidad organizativa de AWS Control Tower registrada. El siguiente ejemplo muestra la notificación de Amazon SNS cuando se detecta este tipo de desviación.

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
}
```

Resolución

- Cuando se produce este tipo de error en la cuenta de un miembro, puede resolverlo actualizando la cuenta en la consola de AWS Control Tower o en Account Factory. Por ejemplo, puede añadir la cuenta a otra unidad organizativa registrada desde el asistente de actualización de Account Factory. Para obtener más información, consulte Actualice y mueva cuentas de fábrica con AWS Control Tower o con AWS Service Catalog.
- Si se elimina una cuenta compartida de una OU fundamental, debes resolver el problema restableciendo tu landing zone. Hasta que no se resuelva este inconveniente, no podrá utilizar la consola de la Torre de Control de AWS.
- Para obtener más información acerca de la resolución de desviaciones para cuentas y unidades organizativas, consulte Si administra recursos fuera de la Torre de Control de AWS.

> **Note**
>
> En Service Catalog, el producto aprovisionado por Account Factory que representa la cuenta no se actualiza para eliminarla. En su lugar, el producto aprovisionado se muestra como

TAINTED y en un estado de error. Para limpiar, vaya al Service Catalog, elija el producto aprovisionado y, a continuación, elija Finalizar.

Actualización no programada para SCP administrada

Este tipo de desviación puede producirse cuando el SCP de un control se actualiza en la AWS Organizations consola o mediante programación mediante el SDK de AWS AWS CLI o uno de ellos. El siguiente es un ejemplo de la notificación de Amazon SNS cuando se detecta este tipo de desviación.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Resolución

Cuando se produce este tipo de desviación en una unidad organizativa con hasta 300 cuentas, puede resolverla de la siguiente manera:

- Ir a la página de la organización en la consola de la Torre de Control de AWS para volver a registrar la OU (la opción más rápida). Para obtener más información, consulte Registrar una unidad organizativa existente en AWS Control Tower.
- Actualización de tu landing zone (opción más lenta). Para obtener más información, consulte Actualizar la zona de inicio.

Cuando se produzca este tipo de desviación en una OU con más de 300 cuentas, resuélvala actualizando su landing zone. Para obtener más información, consulte Actualizar la zona de inicio.

SCP asociada a OU administrada

Este tipo de desviación puede producirse cuando un SCP de un control está conectado a cualquier otra OU. Esto es especialmente común cuando trabaja en sus unidades organizativas desde fuera de la consola de la Torre de Control Tower de AWS. El siguiente es un ejemplo de la notificación de Amazon SNS cuando se detecta este tipo de desviación.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Resolución

Cuando se produce este tipo de desviación en una unidad organizativa con hasta 300 cuentas, puede resolverla de la siguiente manera:

- Ir a la página de la organización en la consola de la Torre de Control de AWS para volver a registrar la OU (la opción más rápida). Para obtener más información, consulte Registrar una unidad organizativa existente en AWS Control Tower.
- Actualización de tu landing zone (opción más lenta). Para obtener más información, consulte Actualizar la zona de inicio.

Cuando se produzca este tipo de desviación en una OU con más de 300 cuentas, resuélvala actualizando su landing zone. Para obtener más información, consulte Actualizar la zona de inicio.

SCP desvinculada de OU administrada

Este tipo de desviación puede producirse cuando el SCP de un control se separa de una unidad organizativa gestionada por AWS Control Tower. Esto es especialmente común cuando se trabaja

desde fuera de la consola de AWS Control Tower. El siguiente es un ejemplo de la notificación de Amazon SNS cuando se detecta este tipo de desviación.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Resolución

Cuando se produce este tipo de desviación en una unidad organizativa con hasta 300 cuentas, puede resolverla de la siguiente manera:

- Navegar hasta la OU en la consola de la Torre de Control Tower de AWS para volver a registrar la OU (la opción más rápida). Para obtener más información, consulte Registrar una unidad organizativa existente en AWS Control Tower.
- Actualización de tu landing zone (opción más lenta). Si la desviación afecta a un control obligatorio, el proceso de actualización crea una nueva política de control de servicios (SCP) y la adjunta a la OU para resolver la desviación. Para obtener más información sobre cómo actualizar tu landing zone, consultaActualizar la zona de inicio.

Cuando se produzca este tipo de desviación en una OU con más de 300 cuentas, resuélvala actualizando su landing zone. Si la desviación afecta a un control obligatorio, el proceso de actualización crea una nueva política de control de servicios (SCP) y la adjunta a la OU para resolver la desviación. Para obtener más información sobre cómo actualizar tu landing zone, consultaActualizar la zona de inicio.

SCP asociada a cuenta de miembro

Este tipo de desviación puede producirse cuando se adjunta un SCP de un control a una cuenta en la consola de Organizations. Las barandillas y sus SCP se pueden habilitar en las unidades organizativas (y, por lo tanto, se pueden aplicar a todas las cuentas inscritas de una unidad organizativa) a través de la consola de la Torre de Control de AWS. El siguiente es un ejemplo de la notificación de Amazon SNS cuando se detecta este tipo de desviación.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

Resolución

Este tipo de desviación se produce en la cuenta y no en la OU.

Cuando se produce este tipo de desviación en las cuentas de una unidad organizativa fundamental, como la unidad organizativa de seguridad, la solución es actualizar la landing zone. Para obtener más información, consulte Actualizar la zona de inicio.

Cuando este tipo de desviación se produce en una unidad organizativa no básica con hasta 300 cuentas, puede resolverla de la siguiente manera:

- Separar el SCP de la AWS Control Tower de la cuenta de fábrica de la cuenta.
- Navegar hasta la OU en la consola de la Torre de Control Tower de AWS para volver a registrar la OU (la opción más rápida). Para obtener más información, consulte Registrar una unidad organizativa existente en AWS Control Tower.

Cuando este tipo de error se produce en una unidad organizativa con más de 300 cuentas, puede intentar resolverlo actualizando la configuración de fábrica de la cuenta. Es posible que no sea

posible resolverlo correctamente. Para obtener más información, consulte Actualizar la zona de inicio.

Se ha eliminado la unidad organizativa fundamental

Este tipo de desviación solo se aplica a las unidades organizativas fundamentales de AWS Control Tower, como la unidad organizativa de seguridad. Puede ocurrir si se elimina una unidad organizativa fundamental fuera de la consola de AWS Control Tower. Las unidades organizativas fundamentales no se pueden mover sin provocar este tipo de desviación, ya que mover una unidad organizativa equivale a eliminarla y, a continuación, añadirla a otro lugar. Cuando resuelva el problema actualizando su landing zone, AWS Control Tower sustituirá a la unidad organizativa fundamental de la ubicación original. El siguiente ejemplo muestra una notificación de Amazon SNS que puede recibir cuando se detecta este tipo de desviación.

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

Resolución

Como esta desviación se produce únicamente en las unidades organizativas fundamentales, la resolución es actualizar la zona de aterrizaje. Cuando se eliminan otros tipos de unidades organizativas, AWS Control Tower se actualiza automáticamente.

Para obtener más información acerca de la resolución de desviaciones para cuentas y unidades organizativas, consulte Si administra recursos fuera de la Torre de Control de AWS.

Desviación de control de Security Hub

Este tipo de desviación se produce cuando un control que forma parte del estándar AWS Security Hub gestionado por servicios: AWS Control Tower informa de un estado de desviación. El propio

AWS Security Hub servicio no informa de un estado de desviación de estos controles. En su lugar, el servicio envía sus conclusiones a la Torre de Control de AWS.

La desviación de control del Security Hub también se puede detectar si AWS Control Tower no ha recibido una actualización de estado del Security Hub en más de 24 horas. Si esos resultados no se reciben como se esperaba, AWS Control Tower verifica que el control está a la deriva. El siguiente ejemplo muestra una notificación de Amazon SNS que puede recibir cuando se detecta este tipo de desviación.

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

Resolución

En el caso de las unidades organizativas con menos de 300 cuentas, la solución es volver a registrar la unidad organizativa, lo que restablece el control al estado original. Para cualquier unidad organizativa, puede eliminar y volver a activar el control a través de la consola o las API de la Torre de Control de AWS, que también restablecen el control.

Para obtener más información acerca de la resolución de desviaciones para cuentas y unidades organizativas, consulte Si administra recursos fuera de la Torre de Control de AWS.

Acceso de confianza desactivado

Este tipo de desviación se aplica a las zonas de aterrizaje de la Torre de Control de AWS. Se produce cuando inhabilita el acceso de confianza a la Torre de Control de AWS AWS Organizations después de configurar la zona de aterrizaje de la Torre de Control de AWS.

Cuando el acceso de confianza está deshabilitado, la Torre de Control de AWS ya no recibe eventos de cambio de AWS Organizations. AWS Control Tower se basa en estos eventos de cambio para mantenerse sincronizado. AWS Organizations Como resultado, es posible que AWS Control Tower no realice cambios organizativos en las cuentas y las unidades organizativas. Por eso es importante volver a registrar cada OU cada vez que actualice su landing zone.

Ejemplo: notificación de Amazon SNS

El siguiente es un ejemplo de la notificación de Amazon SNS que recibe cuando se produce este tipo de desviación.

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
}
```

Resolución

La Torre de Control de AWS le notifica cuando se produce este tipo de desviación en la consola de la Torre de Control de AWS. La solución es restablecer la zona de aterrizaje de la AWS Control Tower. Para obtener más información, consulte Resolver la desviación.

Si administra recursos fuera de la Torre de Control de AWS

AWS Control Tower configura cuentas, unidades organizativas y otros recursos en su nombre, pero usted es el propietario de estos recursos. Puede cambiar estos recursos dentro o fuera de la Torre de Control de AWS. El lugar más común para cambiar los recursos fuera de la Torre de Control de

AWS es la AWS Organizations consola. En este tema se describe cómo conciliar los cambios en los recursos de la Torre de Control de AWS cuando los realiza fuera de la Torre de Control de AWS.

Si se cambia el nombre, se eliminan y se mueven recursos fuera de la consola de la Torre de Control Tower de AWS, la consola deja de estar sincronizada. Muchos cambios se pueden conciliar automáticamente. Algunos cambios requieren restablecer la zona de aterrizaje para actualizar la información que se muestra en la consola de la Torre de Control de AWS.

En general, los cambios que realice fuera de la consola de la Torre de Control de AWS en los recursos de la Torre de Control de AWS crean un estado de deriva solucionable en su landing zone. Para obtener más información sobre estos cambios, consulte Cambios reparables en los recursos.

Tareas que requieren restablecer la zona de aterrizaje

- Eliminar la unidad organizativa de seguridad (un caso especial, que no debe hacerse a la ligera).
- Eliminar una cuenta compartida de la unidad organizativa de seguridad (no se recomienda).
- Actualizar, adjuntar o separar un SCP asociado a la OU de seguridad.

Cambios que AWS Control Tower actualiza automáticamente

- Cambiar la dirección de correo electrónico de una cuenta inscrita
- Cambiar el nombre de una cuenta registrada
- Crear una nueva unidad organizativa (OU) de nivel superior
- Cambiar el nombre de una OU registrada
- Eliminar una unidad organizativa registrada (excepto la unidad organizativa de seguridad, que requiere una actualización).
- Eliminar una cuenta inscrita (excepto una cuenta compartida en la OU de seguridad)

> **Note**
>
> AWS Service Catalog gestiona los cambios de forma diferente a AWS Control Tower. AWS Service Catalog puede provocar un cambio en la postura de gobierno al conciliar sus cambios. Para obtener más información sobre la actualización de un producto aprovisionado, consulte Actualización de productos aprovisionados en la documentación. AWS Service Catalog

Hacer referencia a recursos ajenos a la Torre de Control de AWS

Cuando crea nuevas unidades organizativas y cuentas fuera de la Torre de Control de AWS, no se rigen por la Torre de Control de AWS, aunque se muestren.

Crear una unidad organizativa

Las unidades organizativas (OU) creadas fuera de la Torre de Control de AWS se denominan No registradas. Se muestran en la página de la organización, pero no se rigen por los controles de la Torre de Control de AWS.

Creación de una cuenta

Las cuentas creadas fuera de la Torre de Control de AWS se denominan no inscritas. Las cuentas inscritas y no inscritas que pertenecen a una OU registrada en AWS Control Tower se muestran en la página de la organización. Se puede invitar a las cuentas que no pertenezcan a una OU registrada desde la AWS Organizations consola. Esta invitación a unirse no inscribe la cuenta en la Torre de Control de AWS ni extiende la gobernanza de la Torre de Control de AWS a la cuenta. Para ampliar la gobernanza mediante la inscripción de la cuenta, vaya a la página de la organización o a la página de detalles de la cuenta en AWS Control Tower y seleccione Inscribir cuenta.

Cambiar externamente los nombres de los recursos de la Torre de Control de AWS

Puede cambiar los nombres de sus unidades organizativas (OU) y cuentas fuera de la consola de AWS Control Tower, y la consola se actualizará automáticamente para reflejar esos cambios.

Cambiar el nombre de una unidad organizativa

En AWS Organizations, puede cambiar el nombre de una OU mediante la AWS Organizations API o la consola. Cuando cambia el nombre de una unidad organizativa fuera de la Torre de Control de AWS, la consola de la Torre de Control de AWS refleja automáticamente el cambio de nombre. Sin embargo, si aprovisiona sus cuentas mediante AWS Service Catalog, también debe restablecer su landing zone para garantizar que AWS Control Tower mantenga la coherencia AWS Organizations. El flujo de trabajo Reset garantiza la coherencia entre los servicios de las unidades organizativas fundamentales y adicionales. Puedes resolver este tipo de desviación desde la página de configuración de la zona de aterrizaje. Consulta la sección llamada «Resolver la deriva» enDetecte y resuelva desviaciones en la Torre de Control de AWS.

AWS Control Tower muestra los nombres de las unidades organizativas en la página de la organización del panel de control de AWS Control Tower. Puedes ver si la operación de restablecimiento de tu zona de landing zone se ha realizado correctamente.

Cambiar el nombre de una cuenta registrada

Cada AWS cuenta tiene un nombre para mostrar que el usuario raíz de la cuenta puede cambiar en la AWS Billing and Cost Management consola. Al cambiar el nombre de una cuenta que está inscrita en AWS Control Tower, el cambio de nombre se refleja automáticamente en AWS Control Tower. Para obtener más información sobre cómo cambiar el nombre de una cuenta, consulte Administrar una AWS cuenta en la Guía del usuario de AWS facturación.

Eliminar la unidad organizativa de seguridad

Este tipo de desviación es un caso especial. Si eliminas la unidad organizativa de seguridad, verás una página con un mensaje de error que te pedirá que restablezcas tu landing zone. Debe restablecer su landing zone antes de poder realizar cualquier otra acción en AWS Control Tower.

- No podrá realizar ninguna acción en la consola de AWS Control Tower ni podrá crear cuentas nuevas AWS Service Catalog hasta que se haya restablecido.
- No podrá ver la página de configuración de la zona de destino para ver allí el botón de restablecimiento.

En esta situación, el proceso de restablecimiento de la zona de landing zone crea una nueva unidad organizativa de seguridad y mueve las dos cuentas compartidas a la nueva unidad organizativa de seguridad. AWS Control Tower marca las cuentas de archivo de registros y auditoría como desviadas. El mismo proceso resuelve la desviación de estas cuentas.

Si decide que debe eliminar la unidad organizativa de seguridad, debe saber lo siguiente:

Antes de poder eliminar la unidad organizativa de seguridad, debe asegurarse de que no contiene cuentas. En concreto, debe eliminar el archivo de registro y las cuentas de auditoría de la OU. Le recomendamos que mueva estas cuentas a otra unidad organizativa.

> **Note**
>
> La acción de eliminar su unidad organizativa de seguridad no debe realizarse sin la debida consideración. La acción podría generar problemas de conformidad si el registro se suspende temporalmente y porque es posible que algunos controles no se apliquen.

Para obtener información general acerca de la desviación, consulte «Resolving Drift (Resolver desviación)» en Detecte y resuelva desviaciones en la Torre de Control de AWS.

Eliminar una cuenta de la OU de seguridad

No se recomienda eliminar ninguna de las cuentas compartidas de su organización ni sacarlas de la OU de seguridad. Si ha eliminado una cuenta compartida de forma accidental, puede seguir los pasos de corrección de esta sección para restaurarla.

- Desde la consola de AWS Control Tower: para iniciar el proceso de corrección, siga los pasos de corrección semimanuales. Asegúrese de que el usuario o el rol que utiliza para acceder a la consola de la Torre de Control de AWS tenga permisos de ejecución`organizations:InviteAccountToOrganization`. Si no dispone de dichos permisos, siga los pasos de corrección manuales, que utilizan tanto la consola de la Torre de Control de AWS como la AWS Organizations consola.
- Empezar desde la AWS Organizations consola: este proceso de corrección es un procedimiento un poco más largo y totalmente manual. Cuando siga los pasos de corrección manuales, cambiará entre la AWS Organizations consola y la consola de la Torre de Control de AWS. Cuando trabaje en AWS Organizations ella, necesitará un usuario o un rol con la política `AWSOrganizationsFullAccess` administrada o equivalente. Cuando trabaje en la consola de la Torre de Control de AWS, necesitará un usuario o rol con la política `AWSControlTowerServiceRolePolicy` administrada o equivalente, y permiso para ejecutar todas las acciones de la Torre de Control de AWS (controltower: *).
- Si las medidas correctivas no restauran la cuenta, póngase en contacto con nosotros. AWS Support

Los resultados de eliminar una cuenta compartida mediante AWS Organizations:

- La cuenta ya no está protegida por los controles obligatorios de la Torre de Control de AWS con políticas de control de servicios (SCP). Resultado: es posible que los recursos creados por AWS Control Tower en la cuenta se modifiquen o eliminen.
- La cuenta ya no forma parte de la cuenta AWS Organizations de administración. Resultado: el administrador de la cuenta de AWS Organizations administración ya no puede ver los gastos de la cuenta.
- Ya no se garantiza que la cuenta esté supervisada por AWS Config. Resultado: es posible que el administrador de la cuenta de AWS Organizations administración no pueda detectar los cambios en los recursos.

- La cuenta ya no está en la organización. Resultado: las actualizaciones y el restablecimiento de AWS Control Tower fallarán.

Para restaurar una cuenta compartida mediante la consola de la Torre de Control de AWS (procedimiento semimanual)

1. Inicie sesión en la consola de AWS Control Tower en https://console.aws.amazon.com/controltower. Debe iniciar sesión como usuario de IAM, usuario del Centro de Identidad de IAM o con un rol con permisos para poder ejecutarse. `organizations:InviteAccountToOrganization` Si no dispone de dichos permisos, utilice el procedimiento de corrección manual que se describe más adelante en este tema.
2. En la página detectada por un desvío en la zona de destino, selecciona Volver a invitar para corregir la eliminación de la cuenta compartida y volver a invitar a la cuenta compartida a la organización. Se envía un correo electrónico generado automáticamente a la dirección de correo electrónico de la cuenta.
3. Acepta la invitación para volver a incorporar la cuenta compartida a la organización. Realice una de las acciones siguientes:
   - Inicia sesión en la cuenta compartida que se eliminó y, a continuación, ve a https://console.aws.amazon.com/organizations/home#/invites
   - Si tienes acceso al mensaje de correo electrónico enviado al volver a invitar a la cuenta, inicia sesión en la cuenta eliminada y, a continuación, haz clic en el enlace del mensaje para ir directamente a la invitación a la cuenta.
   - Si la cuenta compartida que se ha eliminado no pertenece a otra organización, inicia sesión en la cuenta, abre la AWS Organizations consola y ve a Invitaciones.
4. Vuelva a iniciar sesión en la cuenta de administración o vuelva a cargar la consola de AWS Control Tower si ya está abierta. Verá la página de distribución de la zona de destino. Selecciona Restablecer para reparar la landing zone.
5. Espere a que se complete el proceso de restablecimiento.

Si la corrección se realiza correctamente, la cuenta compartida aparecerá en un estado normal y en conformidad con las normas.

Si los pasos de corrección no restauran la cuenta, ponte en contacto con nosotros. AWS Support

Para restaurar una cuenta compartida mediante la Torre de Control Tower y AWS Organizations las consolas de AWS (corrección manual)

1. Inicie sesión en la AWS Organizations consola enhttps://console.aws.amazon.com/organizations/. Debe iniciar sesión como usuario de IAM, usuario del Centro de Identidad de IAM o con un rol con la política `AWSOrganizationsFullAccess` gestionada o equivalente.
2. Vuelva a invitar a la cuenta compartida a la organización. Para obtener información sobre los requisitos, los requisitos previos y el procedimiento para invitar una cuenta a una organización AWS Organizations, consulte Invitar una AWS cuenta a su organización en la Guía del AWS Organizations usuario.
3. Inicie sesión en la cuenta compartida que se eliminó y, a continuación, vaya a https://console.aws.amazon.com/organizations/home#/invites para aceptar la invitación.
4. Vuelva a iniciar sesión en la cuenta de administración.
5. Inicie sesión en la consola de la Torre de Control de AWS como usuario o rol con la política `AWSControlTowerServiceRolePolicy` administrada o equivalente y permisos para ejecutar todas las acciones de la Torre de Control de AWS (controltower: *).
6. Verás la página de deriva de la zona de aterrizaje con una opción para restablecer la zona de aterrizaje. Selecciona Restablecer para reparar la landing zone.
7. Espere a que se complete el proceso de restablecimiento.

Si la corrección se realiza correctamente, la cuenta compartida aparecerá en un estado normal y en conformidad con las normas.

Si los pasos de corrección no restauran la cuenta, ponte en contacto con nosotros. AWS Support

Cambios externos que se actualizan automáticamente

AWS Control Tower actualiza automáticamente los cambios que realice en las direcciones de correo electrónico de su cuenta, pero Account Factory no los actualiza automáticamente.

Cambiar la dirección de correo electrónico de una cuenta gobernada

AWS Control Tower recupera y muestra las direcciones de correo electrónico según lo requiera la experiencia de la consola. Por lo tanto, las direcciones de correo electrónico compartidas y de otras cuentas se actualizan y se muestran de forma coherente en AWS Control Tower después de cambiarlas.

> **Note**
>
> En AWS Service Catalog, Account Factory muestra los parámetros que se especificaron en la consola al crear un producto aprovisionado. Sin embargo, la dirección de correo electrónico de la cuenta original no se actualiza automáticamente cuando cambia la dirección de correo electrónico de la cuenta. Esto se debe a que la cuenta está conceptualmente contenida en el producto aprovisionado; no es la misma que el producto aprovisionado. Para actualizar este valor, debe actualizar el producto aprovisionado, lo que puede provocar un cambio en la gestión.

Aplicar reglas externas AWS Config

La Torre de Control de AWS muestra el estado de conformidad de todas AWS Config las reglas implementadas en las unidades organizativas registradas en la Torre de Control de AWS, incluidas las reglas que se activaron fuera de la consola de la Torre de Control de AWS.

Eliminar recursos de la Torre de Control de AWS fuera de la Torre de Control de AWS

Puede eliminar unidades organizativas y cuentas en AWS Control Tower y no necesita realizar ninguna otra acción para ver las actualizaciones. Account Factory se actualiza automáticamente al eliminar una OU, pero no al eliminar una cuenta.

Eliminar una unidad organizativa registrada (excepto la unidad organizativa de seguridad)

En AWS Organizations ella, puedes eliminar las unidades organizativas (OU) vacías mediante la API o la consola. Las unidades organizativas que contienen cuentas no se pueden eliminar.

AWS Control Tower recibe una notificación AWS Organizations cuando se elimina una unidad organizativa. Actualiza la lista de unidades organizativas en Account Factory para que la lista de unidades organizativas registradas siga siendo coherente.

> **Note**
>
> En AWS Service Catalog, Account Factory se actualiza para eliminar la OU eliminada de la lista de OU disponibles en las que puede aprovisionar una cuenta.

Eliminación de una cuenta inscrita de una unidad organizativa

Al eliminar una cuenta inscrita, AWS Control Tower recibe una notificación y realiza actualizaciones para que la información siga siendo coherente.

> **Note**
>
> En AWS Service Catalog, el producto aprovisionado por Account Factory que representa la cuenta gobernada no se actualiza para eliminar la cuenta. En su lugar, el producto aprovisionado se muestra como `TAINTED` y en un estado de error. Para limpiar, vaya a AWS Service Catalog, elija el producto aprovisionado y, a continuación, elija Terminate (Terminar).

Controle las organizaciones y las cuentas con AWS Control Tower

Todas las unidades organizativas (OU) y las cuentas que cree en la Torre de Control de AWS se rigen automáticamente por la Torre de Control de AWS. Además, si tiene unidades organizativas y cuentas existentes que se crearon fuera de la Torre de Control de AWS, puede incorporarlas al gobierno de la Torre de Control de AWS.

En el caso de AWS las cuentas AWS Organizations AND existentes, la mayoría de los clientes prefieren inscribir grupos de cuentas registrando toda la unidad organizativa (OU) que contiene las cuentas. También puede inscribir las cuentas de forma individual. Para obtener más información sobre cómo inscribir cuentas individuales, consulteInscribir un ya existente Cuenta de AWS.

Terminología

- Cuando incorporas una organización existente a la Torre de Control de AWS, se denomina registrar la organización o extender la gobernanza a la organización.
- Cuando incorporas una AWS cuenta a AWS Control Tower, se denomina inscribir la cuenta.

Vea sus unidades organizativas y sus cuentas

En la página de organización de la Torre de Control de AWS, puede ver todas las unidades organizativas de su empresa AWS Organizations, incluidas las que están registradas en la Torre de Control de AWS y las que no lo están. Puede ver las unidades organizativas anidadas como parte de la jerarquía. Una forma sencilla de ver las unidades organizativas en la página de la organización consiste en seleccionar las unidades organizativas únicamente en el menú desplegable de la parte superior derecha.

La página de la organización muestra todas las cuentas de su organización, independientemente de la OU o del estado de inscripción en AWS Control Tower. Una forma sencilla de ver sus cuentas en la página de la organización es seleccionar Cuentas únicamente en el menú desplegable de la parte superior derecha. Puede ver, actualizar e inscribir cuentas de forma individual en las OU, si las cuentas cumplen los requisitos previos para la inscripción.

Si no selecciona ningún filtro, la página de la organización mostrará sus cuentas y unidades organizativas jerárquicamente. Es una ubicación central para monitorear y tomar medidas en todos

los recursos de la Torre de Control de AWS. Para obtener más información sobre la página de la organización, puede ver el tutorial en vídeo.

Tutorial en vídeo

En este vídeo (4:01) se describe cómo trabajar con la página de organización de AWS Control Tower. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo sobre cómo trabajar con la página de la organización en AWS Control Tower.

Temas

- Registrar una unidad organizativa existente en AWS Control Tower
- Inscribir un ya existente Cuenta de AWS

Amplíe la gobernanza a una organización existente

Puede añadir la gobernanza de la Torre de Control de AWS a una organización existente configurando una zona de aterrizaje (LZ), tal y como se describe en la Guía del usuario de la Torre de Control de AWS, en la sección Introducción, paso 2.

Esto es lo que puede esperar al configurar su zona de aterrizaje de AWS Control Tower en una organización existente.

- Puedes tener una landing zone por AWS Organizations organización.
- AWS Control Tower utiliza la cuenta de administración de su AWS Organizations organización actual como cuenta de administración. No se necesita una cuenta de administración nueva.
- AWS Control Tower configura dos cuentas nuevas en una unidad organizativa registrada: una cuenta de auditoría y una cuenta de registro.
- Los límites de servicio de su organización deben permitir la creación de estas dos cuentas adicionales.
- Una vez que haya lanzado su landing zone o registrado una OU, los controles de AWS Control Tower se aplicarán automáticamente a todas las cuentas inscritas en esa OU.
- Puede inscribir AWS cuentas existentes adicionales en una OU que esté gobernada por AWS Control Tower para que los controles se apliquen a esas cuentas.

- Puede añadir más unidades organizativas en la Torre de Control de AWS y registrar las unidades organizativas existentes.

Para comprobar otros requisitos previos para el registro y la inscripción, consulte Introducción a AWS Control Tower.

Aquí encontrará más información sobre cómo los controles de la Torre de Control de AWS no se aplican a las unidades organizativas de las organizaciones de AWS que no tienen configuradas las zonas de aterrizaje de la Torre de Control de AWS:

- Las cuentas nuevas creadas fuera de AWS Control Tower Account Factory no están sujetas a los controles de la OU registrada.
- Las cuentas nuevas creadas en unidades organizativas que no estén registradas en la Torre de Control de AWS no están sujetas a controles, a menos que inscriba específicamente esas cuentas en la Torre de Control de AWS. Consulte Inscribir un ya existente Cuenta de AWS para obtener más información sobre cómo inscribir cuentas.
- Las organizaciones existentes adicionales, las cuentas existentes y las unidades organizativas nuevas o las cuentas que cree fuera de la Torre de Control de AWS no están sujetas a los controles de la Torre de Control de AWS, a menos que registre la OU por separado o inscriba la cuenta.

Para obtener más información sobre cómo aplicar AWS Control Tower a las unidades organizativas y cuentas existentes, consulteRegistrar una unidad organizativa existente en AWS Control Tower.

Para obtener información general sobre el proceso de configuración de una zona de aterrizaje de AWS Control Tower en su organización actual, consulte el vídeo de la siguiente sección.

> **Note**
>
> Durante la configuración, AWS Control Tower realiza comprobaciones previas para evitar problemas habituales. Sin embargo, si actualmente utiliza la solución AWS Landing Zone AWS Organizations, consulte con su arquitecto de AWS soluciones antes de intentar habilitar AWS Control Tower en su organización para determinar si la Torre de Control de AWS puede interferir con su implementación actual en la zona de aterrizaje. Consulte también ¿Qué sucede si la cuenta no cumple los requisitos previos? para obtener información sobre cómo mover cuentas de una landing zone a otra.

Vídeo: Habilita una zona de aterrizaje en la existente AWS Organizations

En este vídeo (7:48), se describe cómo configurar y habilitar una zona de aterrizaje de la AWS Control Tower en AWS Organizations estructuras existentes. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Habilite AWS Control Tower para las organizaciones existentes

Consideraciones para el centro de identidad de IAM y las organizaciones existentes

- Si AWS IAM Identity Center (IAM Identity Center) ya está configurado, la región de origen de AWS Control Tower debe ser la misma que la región del IAM Identity Center.
- AWS Control Tower no elimina una configuración existente.
- Si el Centro de identidades de IAM ya está activado y utiliza el directorio de centros de identidad de IAM, AWS Control Tower añade recursos como conjuntos de permisos, grupos, etc., y continúa como de costumbre.
- Si se configura otro directorio (externo, AD, AD administrado), AWS Control Tower no cambia la configuración existente. Para obtener más información, consulte Consideraciones para los AWS IAM Identity Center clientes (IAM Identity Center).

Acceso a otros AWS servicios

Una vez que haya incorporado su organización al gobierno de la Torre de Control de AWS, seguirá teniendo acceso a todos los AWS servicios que estén disponibles a través AWS Organizationsde la AWS Organizations consola y las API. Para obtener más información, consulte Servicios de AWS relacionados.

Unidades organizativas anidadas en la Torre de Control de AWS

En este capítulo se enumeran las expectativas y consideraciones que debe tener en cuenta al trabajar con unidades organizativas anidadas en AWS Control Tower. En la mayoría de los casos, trabajar con unidades organizativas anidadas es lo mismo que trabajar con una estructura de unidad organizativa plana. Las funciones de registro y reregistro funcionan con unidades organizativas anidadas, excepto en lo que respecta a los cambios de comportamiento que se indican en este capítulo.

Tutorial en vídeo

Este vídeo (4:46) describe cómo administrar las implementaciones de unidades organizativas anidadas en AWS Control Tower. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo sobre la administración de unidades organizativas anidadas en AWS Control Tower.

Para obtener orientación sobre las prácticas recomendadas para las unidades organizativas anidadas y su zona de aterrizaje, consulte la entrada del blog Cómo organizar la zona de aterrizaje de la Torre de Control Tower de AWS con unidades organizativas anidadas.

Pase de una estructura de unidad organizativa plana a una estructura de unidad organizativa anidada

Si creó la zona de aterrizaje de la Torre de Control Tower de AWS con una estructura de unidad organizativa plana, puede ampliarla para convertirla en una estructura de unidad organizativa anidada.

Este proceso consta de cuatro pasos principales:

1. Cree la estructura de unidades organizativas anidada que desee en AWS Control Tower.
2. Vaya a la AWS Organizations consola y utilice su función de movimiento masivo para mover las cuentas de la unidad organizativa de origen (plana) a la unidad organizativa de destino (anidada). A continuación se explica cómo:
   a. Diríjase a la OU desde la que desea transferir las cuentas.
   b. Seleccione todas las cuentas de la OU.
   c. Seleccione Mover.

   > **Note**
   >
   > Este paso debe realizarse en la AWS Organizations consola, ya que AWS Control Tower no tiene la función Move.

3. Vaya a la unidad organizativa anidada en la Torre de Control de AWS y regístrela o vuelva a registrarla. Se inscribirán todas las cuentas de la OU anidada.
   - Si creó la OU en AWS Control Tower, vuelva a registrarla.

- Si creó la unidad organizativa en AWS Organizations, regístrela por primera vez.

4. Una vez que sus cuentas se hayan trasladado e inscrito, elimine la unidad organizativa de nivel superior vacía de la AWS Organizations consola o de la consola de la Torre de Control de AWS.

Verificaciones previas del registro de la OU anidada

Para respaldar el registro correcto de sus unidades organizativas anidadas y sus cuentas de miembros, AWS Control Tower realiza una serie de comprobaciones previas. Estas mismas comprobaciones previas se realizan al registrar cualquier OU anidada o unidad organizativa de nivel superior. Para obtener más información, consulte Causas comunes de error durante el registro o la reinscripción.

- Si se aprueban todas las comprobaciones previas, AWS Control Tower empezará a registrar su OU automáticamente.
- Si alguna de las comprobaciones previas falla, AWS Control Tower detiene el proceso de registro y le proporciona una lista de los elementos que deben corregirse antes de que pueda registrar su OU.

Funciones y unidades organizativas anidadas

AWS Control Tower implementa la `AWSControlTowerExecution` función en las cuentas de la OU de destino y en las cuentas de todas las OU anidadas en la OU de destino, incluso cuando su intención es registrar únicamente la OU de destino. Esta función otorga a cualquier usuario de la cuenta de administración permisos de administrador en cualquier cuenta que tenga esa función. `AWSControlTowerExecution` El rol se puede usar para realizar acciones que normalmente no estarían permitidas por los controles de la Torre de Control de AWS.

Puede eliminar este rol de las cuentas no inscritas que no tenga previsto inscribir. Si elimina esta función, no podrá inscribir la cuenta en AWS Control Tower ni registrar las unidades organizativas principales inmediatas, a menos que restablezca la función en la cuenta. Para eliminar el `AWSControlTowerExecution` rol de una cuenta, debe iniciar sesión con el `AWSControlTowerExecution` rol, ya que ningún otro responsable de IAM puede eliminar los roles administrados por AWS Control Tower.

Para obtener información sobre cómo restringir el acceso a los roles, consulte las condiciones opcionales de las relaciones de confianza de sus roles.

¿Qué ocurre durante el registro y la reinscripción de unidades organizativas y cuentas anidadas

Al registrar o volver a registrar una unidad organizativa anidada, AWS Control Tower inscribe todas las cuentas no inscritas de la unidad organizativa de destino y actualiza todas las cuentas inscritas. Esto es lo que puede esperar.

AWS Control Tower realiza las siguientes tareas

- Añade la `AWSControlTowerExecution` función a todas las cuentas no inscritas en esta OU y a todas las cuentas no inscritas en sus OU anidadas.
- Inscribe las cuentas de los miembros que no están inscritas.
- Vuelve a inscribir las cuentas de los miembros inscritos.
- Crea un inicio de sesión en el IAM Identity Center para las cuentas de los miembros recién inscritos.
- Actualiza las cuentas de los miembros inscritos existentes para reflejar tus cambios de landing zone.
- Actualiza los controles configurados para esta OU y sus cuentas de miembros.

Consideraciones para el registro de unidades organizativas anidadas

- No puede registrar una unidad organizativa en la unidad organizativa principal (unidad organizativa de seguridad).
- Las unidades organizativas anidadas deben registrarse por separado.
- No puede registrar una unidad organizativa a menos que su unidad organizativa principal esté registrada.
- No puede registrar una unidad organizativa a menos que todas las unidades organizativas situadas más arriba en el árbol se hayan registrado correctamente en algún momento (es posible que algunas se hayan eliminado).
- Puede registrar una unidad organizativa que esté por debajo de una unidad organizativa superior que esté a la deriva, pero esa acción no reparará la desviación.

Limitaciones de la OU anidada

- Las unidades organizativas pueden estar anidadas a un máximo de 5 niveles de profundidad por debajo de la raíz.
- Las unidades organizativas anidadas en la unidad organizativa de destino se deben registrar o volver a registrar por separado.
- Si la unidad organizativa de destino se encuentra en el nivel 2 o inferior de la jerarquía, es decir, si no es una unidad organizativa de nivel superior, los controles preventivos activados en las unidades organizativas superiores se aplican automáticamente a esta unidad organizativa y a todas las unidades organizativas inferiores.
- Los errores de registro de la OU no se propagan hacia arriba en el árbol jerárquico. Puede ver los detalles sobre los estados de las unidades organizativas anidadas en la página de detalles de la unidad organizativa principal.
- Los errores de registro de la OU no se propagan hacia abajo en el árbol jerárquico.
- AWS Control Tower no modifica la configuración de la VPC de ninguna cuenta nueva o existente.

Unidades organizativas anidadas y conformidad

Desde la consola de AWS Control Tower, puede ver las unidades organizativas y las cuentas que no cumplen con las normas en la página de la organización, de forma que pueda comprender el cumplimiento a mayor escala.

Consideraciones sobre la conformidad de las unidades organizativas y las cuentas anidadas

- La conformidad de una unidad organizativa no se determina en función de la conformidad de las unidades organizativas integradas en ella.
- El estado de conformidad de un control se calcula en todas las unidades organizativas en las que está activado el control, incluidas las unidades organizativas anidadas. Consulte el estado de conformidad de AWS Control Tower para las unidades organizativas y las cuentas w.
- Una OU se muestra como no conforme solo si tiene cuentas que no lo son, independientemente del lugar en que se encuentre la OU en la jerarquía de la OU.
- Si una unidad organizativa anidada no es compatible, su unidad organizativa principal no se considera automáticamente no conforme.

- En la página de detalles de la unidad organizativa o de detalles de la cuenta, puede ver una lista de los recursos no conformes que pueden estar provocando que sus unidades organizativas o cuentas muestren un estado no conforme.

Unidades organizativas anidadas y derivas

En determinadas situaciones, la desviación puede impedir el registro de unidades organizativas anidadas.

Expectativas en cuanto a la deriva y las unidades organizativas anidadas

- Puede activar los controles en las unidades organizativas con padres desviados, pero no directamente en las unidades organizativas desviadas.
- Puede activar los controles de detección en una unidad organizativa desviada, siempre que no sea una unidad organizativa desviada de nivel superior.
- Los controles obligatorios solo están activados en las unidades organizativas de nivel superior. Los controles obligatorios se omiten al registrar una unidad organizativa anidada.
- Un control obligatorio protege AWS Config los recursos; por lo tanto, ese control debe estar en un estado no variable para registrar las unidades organizativas anidadas. Si se desvía, la Torre de Control de AWS bloquea el registro de las unidades organizativas anidadas.
- Si la unidad organizativa de nivel superior está a la deriva, es posible que el control que protege AWS Config los recursos lo esté haciendo. En esta situación, AWS Control Tower bloquea cualquier acción que requiera la creación o actualización de AWS Config recursos, incluida la aplicación de controles de detección.

Controles y unidades organizativas anidados

Cuando se activa un control en una unidad organizativa registrada, los controles preventivos y de detección se comportan de forma diferente. En el caso de las unidades organizativas anidadas, los controles proactivos se comportan de forma similar a los controles de detección.

Controles preventivos

- Los controles preventivos se aplican en las unidades organizativas anidadas.
- Los controles preventivos obligatorios se aplican a todas las cuentas incluidas en la OU y sus OU anidadas.

- Los controles preventivos afectan a todas las cuentas y unidades organizativas incluidas en la unidad organizativa de destino, incluso si esas cuentas y unidades organizativas no están registradas.

Controles proactivos y de detección

- Las unidades organizativas anidadas no heredan automáticamente los controles de detección o proactivos; estos deben habilitarse por separado.
- Los controles proactivos y de detección se implementan solo en las cuentas registradas en las regiones operativas de su zona de aterrizaje.

Se habilitan los estados de control y la herencia

Puede ver los controles heredados de cada unidad organizativa en la página de detalles de la unidad organizativa.

> **Tip**
>
> Puede utilizar la herencia de controles para mantenerse dentro de la cuota de SCP de una OU. Por ejemplo, puede habilitar un control en la unidad organizativa de nivel superior de una jerarquía de unidades organizativas, en lugar de habilitarlo directamente para una unidad organizativa anidada.

Estado heredado

- El estado Heredado indica que el control está habilitado únicamente por herencia y no se ha aplicado directamente a la unidad organizativa.
- El estado Activado significa que el control se aplica a esta unidad organizativa, independientemente del estado en que se encuentre en otras unidades organizativas.
- El estado Fallido significa que el control no se aplica a esta unidad organizativa, independientemente del estado en que se encuentre en otras unidades organizativas.

> **Note**
>
> El estado Heredado indica que el control se aplicó a una unidad organizativa situada más arriba en el árbol y se aplica a esta unidad organizativa, pero no se agregó directamente a esta unidad organizativa.

> **Si tu landing zone no es la versión actual**
>
> Cada fila de la tabla de controles habilitados representa un control habilitado en una unidad organizativa individual.

Las unidades organizativas anidadas y la raíz

La raíz no es una unidad organizativa y no se puede registrar ni volver a registrar. Tampoco puedes crear cuentas directamente en la raíz. La raíz no puede ser no compatible ni tener un estado de ciclo de vida, como registrado o desplazado.

Sin embargo, la raíz es el contenedor de nivel superior de todas las cuentas y unidades organizativas. En el contexto de las unidades organizativas anidadas, es el nodo en el que se anidan todas las demás unidades organizativas.

Registrar una unidad organizativa existente en AWS Control Tower

Una forma eficaz de incorporar varias AWS cuentas existentes a la Torre de Control de AWS consiste en extender la gobernanza de la Torre de Control de AWS a toda una unidad organizativa (OU).

Para permitir el gobierno de la Torre de Control de AWS sobre una unidad organizativa existente que se creó con AWS Organizations ella y sus cuentas, registre la unidad organizativa en su zona de aterrizaje de AWS Control Tower. Puede registrar unidades organizativas que contengan hasta 300 cuentas. Si una OU contiene más de 300 cuentas, no podrá registrarla en AWS Control Tower.

Al registrar una OU, las cuentas de sus miembros se inscriben en la zona de aterrizaje de AWS Control Tower. Se rigen por los controles que se aplican a su OU.

> **Note**
>
> Si aún no tiene una zona de aterrizaje de la Torre de Control de AWS, comience por configurar una zona de aterrizaje, ya sea en una nueva organización creada por AWS Control Tower o en una AWS Organizations organización existente. Para obtener más información sobre cómo configurar una landing zone, consulteIntroducción a AWS Control Tower.

¿Qué ocurre con mis cuentas cuando registro mi OU?

AWS Control Tower requiere permiso para establecer un acceso de confianza entre AWS CloudFormation y AWS Organizations en su nombre, de modo que AWS CloudFormation pueda implementar su pila en las cuentas de su organización de forma automática.

- El `AWSControlTowerExecution` rol se añade a todas las cuentas con el estado No inscritas.
- Los controles obligatorios se activan de forma predeterminada en la OU y en todas sus cuentas al registrar la OU.

Inscripción parcial de las cuentas después de registrar una OU

Es posible registrar una OU correctamente, pero es posible que algunas cuentas permanezcan sin inscribir. Si es así, estas cuentas no cumplen con algunos de los requisitos previos para la inscripción. Si la inscripción de una cuenta como parte del proceso de Register OU no se realiza correctamente, el estado de la cuenta en la página de cuentas indica que la inscripción ha fallado. También puede ver la información de la cuenta en la página de la OU, por ejemplo, 4 de 5, en el campo de cuentas.

Por ejemplo, si ve 4 de 5, significa que su OU tiene 5 cuentas en total y 4 de ellas se inscribieron correctamente, pero una cuenta no se pudo inscribir durante el proceso de registro de la OU. Puede optar por volver a registrar la OU para incluir las cuentas en la inscripción, después de asegurarse de que cumplen los requisitos de inscripción.

Requisitos previos de usuario de IAM para registrar una OU

Su identidad AWS Identity and Access Management (de IAM) (usuario o rol) o de usuario del Centro de Identidad de IAM debe incluirse en la cartera de Account Factory correspondiente al realizar la operación de registro de unidades organizativas, incluso si ya tiene `Admin` permisos. De lo contrario, la creación de los productos aprovisionados fallará durante el registro. El error se produce porque

AWS Control Tower se basa en las credenciales del usuario de IAM o en la identidad del usuario del IAM Identity Center al registrar una OU.

La cartera correspondiente es una creada por AWS Control Tower, denominada AWS Control Tower Account Factory Portfolio. Para llegar a él, elija Service Catalog > Account Factory > AWS Control Tower Account Factory Portfolio. A continuación, seleccione la pestaña denominada Grupos, roles y usuarios para ver su identidad de IAM o del IAM Identity Center. Para obtener más información sobre cómo conceder el acceso, consulte la documentación de. AWS Service Catalog

Registre una unidad organizativa existente

En la consola de AWS Control Tower, en la página de la organización, puede ver todas las OU y cuentas de su organización en una jerarquía, incluidas las OU que están registradas en AWS Control Tower y las que no lo están.

En general, las unidades organizativas no registradas se crearon en AWS Organizations ninguna otra zona de landing zone y no se rigen por ella. Puede registrar las OU existentes que contengan hasta 300 cuentas. Si una OU contiene más de 300 cuentas, no podrá registrarla en AWS Control Tower.

Para registrar una OU existente

1. Inicie sesión en la consola de la Torre de Control de AWS en https://console.aws.amazon.com/controltower.
2. En el menú de navegación del panel izquierdo, elija Organización.
3. En la página de la organización, seleccione el botón de opción situado junto a la OU que desee registrar y, a continuación, seleccione Registrar la unidad organizativa en el menú desplegable Acciones de la esquina superior derecha o, si lo prefiere, seleccione el nombre de la OU para poder ver la página de detalles de la OU correspondiente.
4. En la página de detalles de la unidad organizativa, en la parte superior derecha, puede seleccionar Registrar la unidad organizativa en el menú desplegable Acciones.

El proceso de registro tarda un mínimo de 10 minutos para extender la gobernanza a la OU y hasta 2 minutos adicionales por cada cuenta adicional.

Resultados del registro de una OU existente

Tras registrar una OU existente, el `AWSControlTowerExecution` rol permite a AWS Control Tower extender la gobernanza a sus cuentas individuales. Se aplican medidas cautelares y la información sobre las actividades de la cuenta se envía a sus cuentas de auditoría y registro.

Otros resultados incluyen los siguientes:

- `AWSControlTowerExecution` permite realizar auditorías mediante la cuenta de auditoría de AWS Control Tower.
- `AWSControlTowerExecution`le ayuda a configurar el registro de su organización, de modo que todos los registros de cada cuenta se envíen a la cuenta de registro.
- `AWSControlTowerExecution`garantiza que los controles de la Torre de Control de AWS que haya seleccionado se apliquen automáticamente a todas las cuentas individuales de sus unidades organizativas, así como a todas las cuentas nuevas que cree en la Torre de Control de AWS.

En el caso de una OU registrada, puede proporcionar informes de conformidad y seguridad basados en las funciones de auditoría y registro incorporadas en los controles de la Torre de Control de AWS. Los equipos de seguridad y conformidad pueden verificar que se cumplen todos los requisitos y que no se ha producido ninguna desviación organizativa. Para obtener más información sobre la deriva, consulte[Detecte y resuelva desviaciones en la Torre de Control de AWS](#).

> **Note**
>
> Puede producirse una situación inusual cuando la Torre de Control de AWS muestra las unidades organizativas y sus cuentas. Si ha creado una cuenta en una OU registrada y, posteriormente, mueve esa cuenta inscrita a otra OU que no está registrada, especialmente si AWS Organizations solía mover la cuenta, verá el resultado «1 de 0» cuentas en la página de detalles de la OU. Además, es posible que haya creado otra cuenta no inscrita en esa OU no registrada. Si hay una cuenta no registrada, es posible que la consola diga «1 de 1» en la OU. Parece que la cuenta única (recién creada) está inscrita, pero en realidad no lo está. Debe inscribir la nueva cuenta.

Cree una nueva unidad organizativa

Para crear una nueva unidad organizativa en AWS Control Tower

1. Navegue a la página de la organización.
2. Selecciona Crear unidad organizativa en el menú desplegable Crear recursos en la esquina superior derecha.
3. Especifique un nombre en el campo de nombre de la unidad organizativa.

4. En el menú desplegable de la unidad organizativa principal, puede ver la jerarquía de las unidades organizativas registradas. Seleccione una unidad organizativa principal para la nueva unidad organizativa que va a crear.
5. Elija Añadir.

> **Tip**
>
> Para añadir una unidad organizativa anidada en menos pasos, seleccione el nombre de la unidad organizativa principal que se muestra en la tabla de la página de la organización, consulte la página de la unidad organizativa principal y, a continuación, seleccione Añadir una unidad organizativa en el menú desplegable Acciones de la esquina superior derecha. La nueva unidad organizativa se crea automáticamente como una unidad organizativa anidada debajo de la unidad organizativa seleccionada.

> **Note**
>
> Si tu landing zone no está actualizada, verás una lista plana en lugar de una jerarquía en el menú desplegable. Incluso si tu zona de aterrizaje incluye unidades organizativas anidadas, no verás unidades organizativas de nivel 5 en el menú desplegable, ya que no puedes crear una nueva unidad organizativa debajo de una unidad organizativa de nivel 5. Para obtener más información sobre las unidades organizativas anidadas en la Torre de Control de AWS, consulteUnidades organizativas anidadas en la Torre de Control de AWS.

Causas frecuentes de error durante el registro o la reinscripción

Si el registro (o la reinscripción) de una OU o de cualquiera de sus cuentas de miembros no se aprueba, puede descargar un archivo con un informe detallado en el que se muestran las comprobaciones previas que no se han superado. Para completar la descarga, pulse el botón Descargar, que aparece en la parte superior derecha del área de registro.

En esta sección se enumeran los tipos de errores que se pueden producir si las comprobaciones previas fallan y cómo corregirlos.

En general, al registrar o volver a registrar una OU, todas las cuentas de esa OU se inscriben en AWS Control Tower. Sin embargo, es posible que algunas cuentas no se inscriban, incluso si la OU

en su conjunto se ha registrado correctamente. En estos casos, debe resolver el error de verificación previa relacionado con la cuenta y, a continuación, intentar volver a inscribir esa cuenta o unidad organizativa.

Error en la zona de aterrizaje

- La zona de aterrizaje no está lista

  Restablece tu landing zone actual o actualízala a la última versión.

Errores de OU

- Supera el número máximo de SCP

  Es posible que haya superado el límite de políticas de control de servicios (SCP) por unidad organizativa o que haya alcanzado otra cuota. Se aplica un límite de 5 SCP por OU a todas las OU de la zona de aterrizaje de AWS Control Tower. Si tiene más SCP de los que permite la cuota, debe eliminar o combinar los SCP.
- SCP conflictivos

  Los SCP existentes se pueden aplicar a la OU o a la cuenta, lo que impide que AWS Control Tower inscriba la cuenta. Compruebe los SCP aplicados para ver si hay alguna política que pueda impedir el funcionamiento de AWS Control Tower. Asegúrese de comprobar los SCP que se heredan de las unidades organizativas que ocupan un lugar superior en la jerarquía.
- Supera la cuota del conjunto de pilas

  Es posible que se haya superado la cuota del conjunto de pilas. Si tienes más instancias de las que permite la cuota, debes eliminar algunas instancias de la pila. Para obtener más información, consulte las cuotas de AWS CloudFormation en la Guía del usuario de AWS CloudFormation .
- Supera el límite de la cuenta

  AWS Control Tower limita cada OU a 300 cuentas durante el registro.

Errores en la cuenta

- Se han impedido las comprobaciones previas de las cuentas

Un SCP existente en la OU impide que AWS Control Tower realice verificaciones previas de las cuentas de los miembros de la OU. Para resolver este error de verificación previa, actualice o elimine el SCP de la OU.

- Error en la dirección de correo electrónico

  La dirección de correo electrónico que especificó para la cuenta no cumple con los estándares de nomenclatura. Esta es la expresión regular (regex) que especifica qué caracteres están permitidos: `[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- Config: grabador o canal de entrega activado

  La cuenta puede tener un grabador de AWS Config configuración o un canal de entrega existente. Deben eliminarse o modificarse AWS CLI en todas AWS las regiones en las que la cuenta de administración de AWS Control Tower haya gobernado los recursos antes de poder inscribir una cuenta.

- STS deshabilitado

  AWS Security Token Service (AWS STS) puede estar deshabilitado en la cuenta. AWS Los puntos de enlace STS deben estar activados en las cuentas de todas las regiones compatibles con AWS Control Tower.

- Conflicto en el centro de identidad de IAM

  La región de origen de AWS Control Tower no es la misma que la región AWS IAM Identity Center (IAM Identity Center). Si el Centro de identidad de IAM ya está configurado, la región de origen de la Torre de Control de AWS debe ser la misma que la región del Centro de Identidad de IAM.

- Tema de SNS conflictivo

  La cuenta tiene un nombre de tema de Amazon Simple Notification Service (Amazon SNS) que AWS Control Tower debe usar. AWS Control Tower crea recursos (como temas de SNS) con nombres específicos. Si estos nombres ya están en uso, se produce un error en la configuración de la Torre de Control de AWS. Esta situación podría producirse si está reutilizando una cuenta previamente inscrita en AWS Control Tower.

- Se detectó una cuenta suspendida

  Esta cuenta ha sido suspendida. No se puede inscribir en AWS Control Tower. Elimine la cuenta de esta OU e inténtelo de nuevo.

- El usuario de IAM no está en la cartera

Agregue el usuario AWS Identity and Access Management (IAM) a la cartera de Service Catalog antes de registrar su OU. Este error afecta únicamente a la cuenta de administración.

- La cuenta no cumple los requisitos previos

  La cuenta no cumple los requisitos previos para la inscripción de la cuenta. Por ejemplo, es posible que a la cuenta le falten las funciones y los permisos necesarios para inscribirla en AWS Control Tower. Las instrucciones para añadir un rol están disponibles enAñada manualmente el rol de IAM requerido a uno existente Cuenta de AWS e inscríbalo.

Le recordamos que AWS CloudTrail se activa automáticamente en todas sus AWS cuentas al inscribirlas en AWS Control Tower. Si CloudTrail está habilitada en una cuenta antes de la inscripción, podría producirse una doble facturación, a menos que la desactive CloudTrail antes de comenzar el proceso de inscripción.

Actualizar organizaciones

La forma más rápida de actualizar una unidad organizativa (OU) o de actualizar varias cuentas dentro de una OU es volver a registrar la OU.

Cuándo actualizar las unidades organizativas y las cuentas de AWS Control Tower

Cuando realizas una actualización de landing zone, debes actualizar tus cuentas inscritas para aplicar nuevos controles a esas cuentas.

- Puede realizar una actualización en todas las cuentas de una OU mediante la opción de volver a registrarse.
- Si tienes más de una OU registrada en tu landing zone, vuelve a registrar todas tus OU para actualizar todas tus cuentas.
- Para actualizar una sola cuenta, puede hacerlo desde la consola de AWS Control Tower o puede seleccionar la opción Actualizar producto aprovisionado en AWS Service Catalog. Consulte Actualiza la cuenta en la consola.

Actualice varias cuentas en la misma unidad organizativa

Para actualizar varias cuentas en una unidad organizativa, con una sola acción

1. Inicie sesión en la consola de la Torre de Control de AWS en https://console.aws.amazon.com/controltower.
2. En el menú de navegación del panel izquierdo, elija Organización.
3. En la página Organización, elija cualquier OU para ver la página de detalles de la OU.
4. En Acciones, en la parte superior derecha, seleccione Volver a registrar la OU.

Repita estos pasos para cada unidad organizativa de su organización de AWS Control Tower si necesita actualizar todas sus cuentas y unidades organizativas.

Como alternativa, puede seleccionar cualquier cuenta que muestre el estado de Actualización disponible y, a continuación, elegir Actualizar cuenta para todas las cuentas que necesite.

¿Qué ocurre durante la reinscripción

Al volver a registrar una OU:

- El campo Estado indica si la cuenta está actualmente inscrita en AWS Control Tower (inscrita), si la cuenta nunca se inscribió (No se inscribió) o si la inscripción falló anteriormente (no se pudo inscribir).
- Al volver a registrar la OU, la `AWSControlTowerExecution` función se añade a todas las cuentas con el estado No inscrita o Inhabilitación fallida.
- AWS Control Tower crea un inicio de sesión único (IAM Identity Center) para las nuevas cuentas inscritas.
- Las cuentas inscritas se vuelven a inscribir en AWS Control Tower.
- Se ha corregido un error en los controles preventivos aplicados a la OU, ya que los SCP vuelven a sus definiciones predeterminadas.
- Todas las cuentas se actualizan para reflejar los cambios más recientes en las zonas de landing zone.

Para obtener más información, consulte Inscribir un ya existente Cuenta de AWS.

> **Tip**
>
> Al volver a registrar una OU o al actualizar la versión de tu landing zone y las cuentas de varios miembros, es posible que veas un mensaje de error en el que se menciona el signo StackSet- AWSControlTowerExecutionRole. Esto StackSet en la cuenta de administración puede fallar porque la función de AWSControlTowerExecutionIAM ya existe en todas las cuentas de los miembros inscritos. Este mensaje de error es un comportamiento esperado y puede ignorarse.

Actualiza una sola cuenta

Puede actualizar las cuentas individuales de AWS Control Tower en la consola de AWS Control Tower o en la consola de Service Catalog.

Para actualizar una sola cuenta en la consola de la Torre de Control de AWS, consulteActualiza la cuenta en la consola.

Para actualizar una sola cuenta en AWS Service Catalog

1. Vaya a AWS Service Catalog.
2. En el menú de navegación del panel izquierdo, selecciona Productos aprovisionados.
3. En la página de productos aprovisionados, selecciona el botón de opción situado junto al producto aprovisionado que deseas actualizar.
4. En la esquina superior derecha, selecciona el menú desplegable Acciones para actualizar.

Para obtener más información sobre la actualización AWS Service Catalog, consulte Actualiza el producto aprovisionado y Actualización de productos en la Guía del administrador de Service Catalog.

Servicios integrados

AWS Control Tower es un servicio que se basa en otros AWS servicios para ayudarlo a configurar un entorno bien diseñado. En este capítulo se ofrece una breve descripción general de estos servicios, incluida información de configuración sobre los servicios subyacentes y su funcionamiento en la Torre de Control de AWS.

Para obtener más información sobre cómo medir un entorno bien diseñado, conozca la herramienta Well-Architected Tool AWS . Consulte también la Guía del entorno de nube de gestión y gobierno.

Temas

Implemente entornos con AWS CloudFormation

AWS CloudFormation le permite crear y aprovisionar despliegues de AWS infraestructura de forma predecible y repetitiva. Le ayuda a aprovechar AWS los productos para crear aplicaciones altamente confiables, altamente escalables y rentables en la nube sin preocuparse por crear y configurar la infraestructura subyacente AWS . AWS CloudFormation le permite utilizar un archivo de plantilla para crear y eliminar un conjunto de recursos juntos como una sola unidad (una pila). Si quiere obtener más información, consulte la Guía del usuario de AWS CloudFormation.

AWS Control Tower utiliza AWS CloudFormation conjuntos de pilas para aplicar controles a las cuentas. Para obtener más información sobre cómo AWS CloudFormation funcionan juntas la Torre de Control de AWS, consulte Creación de AWS Control Tower recursos con AWS CloudFormation.

Supervise los eventos con CloudTrail

AWS Control Tower se configura AWS CloudTrail para permitir el registro y la auditoría centralizados. Con ella CloudTrail, la cuenta de administración puede revisar las acciones administrativas y los eventos del ciclo de vida de las cuentas de los miembros.

CloudTrail le ayuda a supervisar su AWS entorno en la nube al mantener un historial de las llamadas a la AWS API de sus cuentas. Por ejemplo, puede identificar los usuarios y las cuentas que llamaron a AWS las API de los servicios compatibles CloudTrail, la dirección IP de origen desde la que se realizaron las llamadas y la hora en que se produjeron las llamadas. Puede CloudTrail integrarse en las aplicaciones mediante la API, automatizar la creación de rutas para su organización, comprobar el estado de las rutas y controlar la forma en que los administradores activan y desactivan el CloudTrail inicio de sesión. Si quiere obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Supervise los recursos y servicios con CloudWatch

Amazon CloudWatch proporciona una solución de monitorización fiable, escalable y flexible que puede empezar a utilizar en cuestión de minutos. Ya no tendrá que configurar, administrar ni escalar sus propios sistemas de monitorización ni su propia infraestructura. Para obtener más información, consulta la Guía CloudWatch del usuario de Amazon.

Para obtener más información sobre cómo Amazon CloudWatch trabaja con AWS Control Tower, consulte Monitorización.

Controle las configuraciones de los recursos con AWS Config

AWS Config proporciona una vista detallada de los recursos asociados a su AWS cuenta, incluida la forma en que están configurados, cómo se relacionan entre sí y cómo han cambiado las configuraciones y sus relaciones a lo largo del tiempo. Para obtener información, consulte la Guía para desarrolladores de AWS Config.

AWS Config los recursos aprovisionados por AWS Control Tower se etiquetan automáticamente con `aws-control-tower` un valor de`managed-by-control-tower`.

Para obtener más información sobre cómo AWS Config monitorea y registra los recursos en AWS Control Tower y cómo se facturan por ellos, consulteSupervise los cambios en los recursos con AWS Config.

AWS Control Tower se utiliza Reglas de AWS Config para implementar controles de detección. Para obtener más información, consulte Acerca de los controles de AWS Control Tower.

Administre los permisos de las entidades con IAM

AWS Identity and Access Management (IAM) es un AWS servicio para controlar el acceso a otros AWS servicios. Con IAM, puede gestionar de forma centralizada los usuarios y las credenciales de seguridad (como las claves de acceso y los permisos) que designan los AWS recursos a los que tienen acceso sus usuarios y aplicaciones.

Cuando configuras tu landing zone, puedes crear varios grupos AWS IAM Identity Center automáticamente si seleccionas IAM como tu proveedor de identidad. Estos grupos tienen conjuntos de permisos que son políticas de permisos predefinidas de IAM. Los usuarios finales también pueden usar IAM para definir el alcance de los permisos para los usuarios de IAM y otras entidades de las cuentas de los miembros.

AWS Identity and Access Management (IAM) simplifica la forma de gestionar el acceso a las cuentas y las aplicaciones empresariales. AWS Puede controlar el acceso al IAM Identity Center y los permisos de usuario en todas sus AWS cuentas de AWS Control Tower.

Si quiere obtener más información, consulte la Guía del usuario de AWS IAM Identity Center.

Si reside en una empresa Región de AWS que no admite la IAM, puede contratar otro proveedor de identidades para configurar y mantener sus propios usuarios y grupos de forma manual.

AWS Key Management Service

AWS Key Management Service (AWS KMS) le permite crear y controlar claves que protegen sus datos. De forma opcional, AWS Control Tower le permite cifrar sus datos con claves de AWS KMS cifrado. Para obtener más información AWS KMS, consulte la Guía para desarrolladores de AWS KMS.

Para obtener información sobre cómo configurar AWS KMS claves con AWS Control Tower, consulte Configuración opcional de AWS KMS claves.

Ejecute funciones informáticas sin servidor con Lambda

Con AWS Lambda, puede ejecutar código sin aprovisionar ni administrar servidores. Puede ejecutar código para muchos tipos de aplicaciones o servicios de backend, sin necesidad de sobrecargas de administración adicionales. Al cargar el código, Lambda puede ejecutar y escalar el código con alta disponibilidad. Puede configurar su código para que se active automáticamente desde otros AWS servicios, o puede llamarlo directamente desde cualquier aplicación web o móvil.

Por ejemplo, determinadas funciones de la cuenta de auditoría de la Torre de Control Tower de AWS se pueden asumir mediante programación, de modo que puede revisar otras cuentas con Lambda. Además, puede utilizar los eventos del ciclo de vida de AWS Control Tower para activar las funciones de Lambda.

Administre las cuentas mediante AWS Organizations

AWS Organizations es un servicio de administración de cuentas que le permite consolidar varias AWS cuentas en una organización que usted crea y administra de forma centralizada. Con Organizations, puede crear cuentas de miembros e invitar a las cuentas existentes a unirse a su organización. Puede organizar las cuentas en grupos y adjuntar controles basados en políticas. Si quiere obtener más información, consulte la Guía del usuario de AWS Organizations.

En AWS Control Tower, Organizations ayuda a gestionar la facturación de forma centralizada, a controlar el acceso, la conformidad y la seguridad, y a compartir los recursos entre AWS las cuentas de los miembros. Las cuentas se agrupan en grupos lógicos, denominados unidades organizativas (OU). Para obtener más información sobre Organizations, consulte la Guía AWS Organizations del usuario.

AWS Control Tower utiliza las siguientes unidades organizativas:

- Raíz: el contenedor principal de todas las cuentas y demás unidades organizativas de tu landing zone.
- Seguridad: esta unidad organizativa contiene la cuenta de archivo de registros, la cuenta de auditoría y los recursos que poseen.
- Sandbox: esta OU se crea cuando configuras tu landing zone. Esta unidad organizativa y otras unidades organizativas secundarias de tu landing zone contienen tus cuentas de miembro. Estas son las cuentas a las que acceden sus usuarios finales para trabajar con los AWS recursos.

> **Note**
>
> Puede añadir unidades organizativas adicionales en su landing zone a través de la consola de AWS Control Tower en la página de unidades organizativas.

Consideraciones

A las unidades organizativas creadas mediante la Torre de Control de AWS se les pueden aplicar controles. De forma predeterminada, las unidades organizativas creadas fuera de la Torre de Control de AWS no pueden hacerlo. Sin embargo, puede registrar dichas unidades organizativas. Una vez que haya registrado una OU, podrá aplicar controles a la unidad organizativa y a sus cuentas. Para obtener información sobre el registro de una OU, consulte Registrar una unidad organizativa existente en AWS Control Tower.

Almacene objetos con Amazon S3

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento para Internet. Puede utilizar Amazon S3 para almacenar y recuperar cualquier cantidad de datos en cualquier momento y desde cualquier parte de la web. Puede realizar estas tareas usando la interfaz web sencilla e intuitiva de la AWS Management Console. Para obtener más información, consulte la Guía del usuario de Amazon Simple Storage Service.

Cuando configuras tu landing zone, se crea un bucket de Amazon S3 en tu cuenta de archivo de registros para contener todos los registros de todas las cuentas de tu landing zone.

Supervise su entorno con Security Hub

AWS Control Tower se integra con AWS Security Hub mediante el estándar Security Hub denominado Service-Managed Standard: AWS Control Tower. Para obtener más información, consulte el estándar Security Hub.

Aprovisione cuentas mediante AWS Service Catalog

AWS Service Catalog permite a los administradores de TI crear, administrar y distribuir carteras de productos aprobados a los usuarios finales, quienes, a su vez, tienen acceso a los productos que necesitan en un portal personalizado. Los productos típicos incluyen servidores, bases de datos, sitios web o aplicaciones que se implementan mediante AWS recursos.

Puede controlar los usuarios que tienen acceso a productos específicos, lo que le permite garantizar el cumplimiento de los estándares empresariales de la organización, gestionar los ciclos de vida de los productos y ayudar a los usuarios a encontrar y lanzar productos con confianza. Para obtener más información, consulte la Guía del administrador de Service Catalog.

En AWS Control Tower, los administradores de la nube central y los usuarios finales pueden aprovisionar cuentas personalizadas en su landing zone mediante AWS Service Catalog productos, denominados «planos personalizados». Para obtener más información, consulte el paso 2. Cree el AWS Service Catalog producto.

AWS Control Tower también puede utilizar las API de Service Catalog para automatizar aún más el aprovisionamiento y la actualización de las cuentas. Para obtener más información, consulte la Guía AWS Service Catalog para desarrolladores.

Transición al tipo de producto AWS Service Catalog externo

AWS Service Catalog cambió el soporte para los productos de código abierto de Terraform y los productos aprovisionados por un nuevo tipo de producto, denominado Externo. Para obtener más información sobre esta transición, consulte Actualización de los productos de código abierto y aprovisionados de Terraform existentes al tipo de producto externo en la guía del administrador.AWS Service Catalog

Este cambio afecta a las cuentas existentes que creó o inscribió con la personalización de fábrica de cuentas de AWS Control Tower. Para realizar la transición de estas cuentas al tipo de producto externo, debe realizar cambios tanto AWS Service Catalog en AWS Control Tower como en AWS Control Tower.

Para realizar la transición al tipo de producto externo

1. Actualice su motor de referencia de Terraform actual AWS Service Catalog para incluir soporte para los tipos de productos externos y de código abierto de Terraform. Para obtener instrucciones sobre cómo actualizar su motor de referencia de Terraform, consulte el repositorio.AWS Service Catalog GitHub
2. En AWS Service Catalog, duplique todos los productos de código abierto de Terraform (planos) existentes y utilice el nuevo tipo de producto externo para los duplicados. No cancele los planos de código abierto de Terraform existentes.
3. En AWS Control Tower, actualice cada cuenta con un plan de código abierto de Terraform para usar el nuevo plan externo.

a. Para actualizar un plano, primero debe eliminar por completo el plano de código abierto de Terraform. Para obtener más información, consulta Eliminar un plano de una cuenta.

b. Añada el nuevo plano externo a la misma cuenta. Para obtener más información, consulte Añadir un plano a una cuenta de AWS Control Tower.

4. Una vez que todas las cuentas que utilizan planes de código abierto de Terraform se hayan actualizado a modelos externos, devuelva AWS Service Catalog y cancele cualquier producto que utilice Terraform Open Source como tipo de producto.

5. De ahora en adelante, todas las cuentas creadas o inscritas mediante la personalización de fábrica de cuentas de la Torre de Control Tower de AWS deberán hacer referencia a los planos que utilicen el tipo de producto AWS CloudFormationo el tipo de producto externo.

   En el caso de los planos creados con el tipo de producto externo, AWS Control Tower solo admite personalizaciones de cuentas que utilicen plantillas de Terraform y el motor de referencia de Terraform. Para obtener más información, consulte Configurar para la personalización.

> **Note**
>
> AWS Control Tower no admite el código abierto de Terraform como tipo de producto al crear cuentas nuevas. Para obtener más información sobre estos cambios, consulte Actualización de los productos de código abierto y aprovisionados de Terraform existentes al tipo de producto externo en la guía del AWS Service Catalog administrador. AWS Service Catalog apoyará a los clientes durante la transición de este tipo de producto, según sea necesario. Póngase en contacto con su representante de cuentas para solicitar asistencia.

Realice un seguimiento de las alertas a través del servicio Amazon Simple Notification

Amazon Simple Notification Service (Amazon SNS) es un servicio web que permite a las aplicaciones, los usuarios finales y los dispositivos enviar y recibir notificaciones al instante desde la nube. Para obtener más información, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

AWS Control Tower utiliza Amazon SNS para enviar alertas programáticas a las direcciones de correo electrónico de su cuenta de administración y de auditoría. Estas alertas te ayudan a evitar

la deriva dentro de tu landing zone. Para obtener más información, consulte Detecte y resuelva desviaciones en la Torre de Control de AWS.

También utilizamos Amazon Simple Notification Service para enviar notificaciones de conformidad desde AWS Config.

> **Tip**
>
> Una de las mejores formas de recibir notificaciones de conformidad con el control de la Torre de Control de AWS (en su cuenta de auditoría) es suscribirse a`AggregateConfigurationNotifications`. Es un servicio que le ayuda a inspeccionar la conformidad. Le proporciona datos reales sobre AWS Config las normas que no cumplen con las normas. AWS Config mantiene automáticamente la lista de cuentas de su OU. Debe suscribirse manualmente, mediante correo electrónico o cualquier tipo de suscripción que permita el SNS. La declaración `arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications` lleva a su cuenta de auditoría.

Cree aplicaciones distribuidas con AWS Step Functions

AWS Step Functions facilita la coordinación de los componentes de las aplicaciones distribuidas como una serie de pasos en un flujo de trabajo visual. Puede crear y ejecutar rápidamente máquinas de estado para implementar los pasos en su aplicación de una manera fiable y de escala ajustable. Para obtener más información, consulte la Guía para desarrolladores de AWS Step Functions.

Administración de identidades y accesos en AWS Control Tower

Para realizar cualquier operación en su landing zone, como el aprovisionamiento de cuentas en Account Factory o la creación de nuevas unidades organizativas (OU) en la consola de AWS Control Tower, ya sea AWS Identity and Access Management (IAM) o AWS IAM Identity Center solicite que autentique que es un usuario aprobado. AWS Por ejemplo, si utiliza la consola de la Torre de Control Tower de AWS, autentica su identidad proporcionando sus AWS credenciales, tal como las ha proporcionado su administrador.

Tras autenticar su identidad, IAM controla su acceso AWS con un conjunto definido de permisos a un conjunto específico de operaciones y recursos. Si es administrador de una cuenta, puede usar IAM para controlar el acceso de otros usuarios de IAM a los recursos asociados a su cuenta.

Temas

Autenticación

Tiene acceso a cualquiera AWS de los siguientes tipos de identidades:

- AWS usuario raíz de la cuenta: cuando crea una AWS cuenta por primera vez, comienza con una identidad que tiene acceso completo a todos los AWS servicios y recursos de la cuenta. Esta identidad se denomina usuario raíz de la AWS cuenta. Obtiene acceso a esta identidad cuando inicia sesión con la dirección de correo electrónico y la contraseña que usó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En su lugar, siga la práctica recomendada de utilizar el usuario raíz únicamente para crear su primer usuario del Centro de Identidad de IAM

(recomendado) o usuario de IAM (no es una práctica recomendada en la mayoría de los casos de uso). A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios. Para obtener más información, consulte ¿Cuándo iniciar sesión como usuario root.

- Usuario de IAM: un usuario de IAM es una identidad de tu AWS cuenta que tiene permisos específicos y personalizados. Puede usar las credenciales de usuario de IAM para iniciar sesión en AWS páginas web seguras, como la consola de AWS administración, los foros de AWS debate o el AWS Support Center. AWS Las prácticas recomendadas recomiendan crear un usuario del Centro de identidades de IAM en lugar de un usuario de IAM, ya que se corre un mayor riesgo de seguridad cuando se crea un usuario de IAM con credenciales de larga duración.

  Si debe crear un usuario de IAM para un fin determinado, además de las credenciales de inicio de sesión, puede generar claves de acceso para cada usuario de IAM. Puede usar estas teclas cuando llama a AWS los servicios mediante programación, ya sea a través de uno de los diversos SDK o mediante la interfaz de línea de AWS comandos (CLI). El SDK y las herramientas de CLI utilizan claves de acceso para firmar criptográficamente una solicitud. Si no utilizas AWS herramientas, debes firmar la solicitud tú mismo. AWS Control Tower admite la versión 4 de Signature, un protocolo para autenticar las solicitudes de API entrantes. Para obtener más información sobre la autenticación de las solicitudes, consulte el proceso de firma de la versión 4 en la AWS referencia general.

- Rol de IAM: un rol de IAM es una identidad de IAM que puede crear en su cuenta con permisos específicos. Una función de IAM es similar a la de un usuario de IAM en el sentido de que es una AWS identidad y tiene políticas de permisos que determinan lo que la identidad puede y no puede hacer en ella. AWS No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo estándar, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

  - Acceso de usuario federado: en lugar de crear un usuario de IAM, puede utilizar las identidades existentes del directorio de usuarios de AWS Directory Service su empresa o de un proveedor de identidades web. Se conocen como usuarios federados. AWS asigna un rol a un usuario federado cuando se solicita el acceso a través de un proveedor de identidad. Para obtener más información acerca de los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.
  - AWS acceso al servicio: un rol de servicio es un rol de IAM que un servicio asume para realizar acciones en tu cuenta en tu nombre. Al configurar algunos entornos de AWS servicio, debe

definir una función que deba asumir el servicio. Esta función de servicio debe incluir todos los permisos necesarios para que el servicio acceda a los AWS recursos que necesita. Los roles de servicio varían de servicio a servicio, pero muchos le permiten elegir sus permisos, siempre y cuando se cumplan los requisitos documentados para dicho servicio. Las funciones del servicio ofrecen acceso solo dentro de su cuenta y no se pueden utilizar para otorgar acceso a servicios en otras cuentas. Puede crear, modificar y eliminar un rol de servicio desde IAM. Por ejemplo, puede crear una función que permita a Amazon Redshift obtener acceso a un bucket de Amazon S3 en su nombre y, a continuación, cargar los datos de ese bucket en un clúster de Amazon Redshift. Para obtener más información, consulte Creación de un rol para delegar permisos a un AWS servicio en la Guía del usuario de IAM.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia de Amazon EC2 y que realizan solicitudes de CLI AWS o API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de Amazon EC2. Para asignar un AWS rol a una instancia de Amazon EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se encuentran en ejecución en la instancia de Amazon EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de IAM.

- La autenticación de los usuarios del Centro de Identidad de IAM en el portal de usuarios del Centro de Identidad de IAM se controla mediante el directorio que se ha conectado al Centro de identidades de IAM. Sin embargo, la autorización de las AWS cuentas que están disponibles para los usuarios finales desde el portal de usuarios viene determinada por dos factores:
  - A quién se le ha asignado el acceso a esas AWS cuentas en la consola del AWS IAM Identity Center. Para obtener más información, consulte el acceso mediante inicio de sesión único en la Guía del AWS IAM Identity Center usuario.
  - Qué nivel de permisos se han concedido a los usuarios finales en la consola de AWS IAM Identity Center para permitirles el acceso adecuado a esas cuentas. AWS Para obtener más información, consulte los conjuntos de permisos en la Guía del AWS IAM Identity Center usuario.

Control de acceso

Para crear, actualizar, eliminar o incluir en una lista los recursos de AWS Control Tower u otros AWS recursos de su landing zone, necesita permisos para realizar la operación y necesita permisos

para acceder a los recursos correspondientes. Además, para realizar la operación mediante programación, necesita claves de acceso válidas.

En las siguientes secciones se describe cómo administrar los permisos de AWS Control Tower:

Temas

- Información general sobre la administración de los permisos de acceso a los recursos de la Torre de Control de AWS
- Uso de políticas basadas en identidad (políticas de IAM) para AWS Control Tower

Trabajo con el Centro de Identidad de AWS IAM y la Torre de Control de AWS

En AWS Control Tower, el Centro de Identidad de IAM permite a los administradores de la nube central y a los usuarios finales gestionar el acceso a varias AWS cuentas y aplicaciones empresariales. De forma predeterminada, AWS Control Tower usa este servicio para configurar y administrar el acceso a las cuentas creadas a través de Account Factory, a menos que haya seleccionado la opción de autoadministrar su identidad y control de acceso.

Para obtener más información sobre cómo seleccionar un proveedor de identidad, consulte. Guía sobre el Centro de Identidad de IAM

Para ver un breve tutorial sobre cómo configurar los usuarios y los permisos del IAM Identity Center en AWS Control Tower, puede ver este vídeo (6:23). Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo sobre la configuración del centro de identidad de AWS IAM en la Torre de Control de AWS.

Acerca de la configuración de la Torre de Control de AWS con el Centro de Identidad de IAM

Cuando configuró AWS Control Tower por primera vez, solo el usuario raíz y los usuarios de IAM con los permisos correctos podían añadir usuarios del IAM Identity Center. Sin embargo, una vez agregados los usuarios finales al AWSAccountFactorygrupo, pueden crear nuevos usuarios del IAM Identity Center desde el asistente Account Factory. Para obtener más información, consulte Aprovisione y administre cuentas con Account Factory.

Si elige la opción predeterminada recomendada, AWS Control Tower configura su landing zone con un directorio preconfigurado que le ayuda a administrar las identidades de los usuarios y el inicio de sesión único, de modo que sus usuarios tengan acceso federado a todas las cuentas. Cuando configuras tu landing zone, este directorio predeterminado se crea para contener grupos de usuarios y conjuntos de permisos.

> **Note**
>
> Puede delegar la administración de AWS IAM Identity Center su organización a una cuenta que no sea la cuenta de administración mediante la función de administrador delegado de IAM Identity Center. Si decide utilizar esta función, tenga en cuenta que los administradores con acceso para gestionar la pertenencia a un grupo también pueden gestionar los grupos asignados a la cuenta de gestión. Para obtener más información, consulte esta entrada del blog, titulada Introducción a la administración delegada AWS del SSO

Grupos de usuarios, funciones y conjuntos de permisos

Los grupos de usuarios administran roles especializados que se definen en las cuentas compartidas. Los roles establecen conjuntos de permisos que deben estar juntos. Todos los miembros de un grupo heredan los conjuntos de permisos o roles asociados al grupo. Puede crear nuevos grupos para los usuarios finales de sus cuentas de miembro, de modo que pueda personalizar solo los roles necesarios para las tareas específicas que realiza un grupo.

Los conjuntos de permisos disponibles cubren una amplia gama de requisitos de permisos de usuario distintos, como el acceso de solo lectura, el acceso administrativo a la Torre de Control de AWS y el acceso al Service Catalog. Estos conjuntos de permisos permiten a tus usuarios finales aprovisionar sus propias AWS cuentas en tu landing zone rápidamente y de conformidad con las directrices de tu empresa.

Para obtener sugerencias sobre cómo planificar las asignaciones de usuarios, grupos y permisos, consulte Recomendaciones para configurar grupos, funciones y políticas

Para obtener más información sobre cómo utilizar este servicio en el contexto de AWS Control Tower, consulte los siguientes temas de la Guía delAWS IAM Identity Center usuario.

- Para añadir usuarios, consulte Añadir usuarios.
- Para agregar los usuarios a los grupos, consulte Añadir usuarios a grupos.
- Para editar las propiedades del usuario, consulte Editar propiedades de usuarios.

- Para añadir un grupo, consulte Añadir grupos.

> **Warning**
>
> AWS Control Tower configura el directorio del centro de identidad de IAM en su región de origen. Si configuras tu landing zone en otra región y, a continuación, accedes a la consola del IAM Identity Center, debes cambiar la región a tu región de origen. No elimine la configuración del centro de identidad de IAM en su región de origen.

Lo que debe saber sobre las cuentas del IAM Identity Center y AWS Control Tower

Estas son algunas cosas útiles que debe tener en cuenta al trabajar con las cuentas de usuario del IAM Identity Center en AWS Control Tower.

- Si su cuenta de usuario de AWS IAM Identity Center está deshabilitada, recibirá un mensaje de error al intentar aprovisionar cuentas nuevas en Account Factory. Puede volver a activar su usuario del IAM Identity Center en la consola del IAM Identity Center.
- Si especifica una nueva dirección de correo electrónico de usuario del IAM Identity Center al actualizar el producto aprovisionado asociado a una cuenta vendida por Account Factory, AWS Control Tower crea una nueva cuenta de usuario del IAM Identity Center. No se elimina la cuenta de usuario creada anteriormente. Si prefiere eliminar la dirección de correo electrónico del usuario anterior del Centro de Identidad de IAM del Centro de Identidad de AWS IAM, consulte Desactivación de un usuario.
- AWS El IAM Identity Center se ha integrado con Azure Active Directory y puede conectar su Azure Active Directory existente a la Torre de Control de AWS.
- Para obtener más información sobre cómo el comportamiento de la Torre de Control de AWS interactúa con el Centro de identidad de AWS IAM y las diferentes fuentes de identidad, consulte las consideraciones para cambiar la fuente de identidad en la documentación del Centro de identidades de AWS IAM.

Grupos de centros de identidad de IAM para AWS Control Tower

AWS Control Tower ofrece grupos preconfigurados para organizar a los usuarios que realizan tareas específicas en sus cuentas. Puede añadir usuarios y asignarlos a estos grupos directamente en

el Centro de identidades de IAM. Si lo hace, se asignan los mismos conjuntos de permisos a los usuarios de los grupos dentro de sus cuentas. Los siguientes grupos se crean al configurar tu landing zone.

AWSAccountFactory

Cuenta	Conjuntos de permisos	Descripción
Cuenta de administración	AWSServiceCatalogEndUserAccess	Este grupo solo se usa en esta cuenta para aprovisionar nuevas cuentas mediante Account Factory.

AWSServiceCatalogAdmins

Cuenta	Conjuntos de permisos	Descripción
Cuenta de administración	AWSServiceCatalogAdminFullAccess	Este grupo solo se usa en esta cuenta para realizar cambios administrativos en Account Factory. Los usuarios de este grupo no pueden aprovisionar cuentas nuevas a menos que también estén en el AWSAccountFactorygrupo.

AWSControlTowerAdmins

Cuenta	Conjuntos de permisos	Descripción
Cuenta de administración	AWSAdministratorAccess	Los usuarios de este grupo de esta cuenta son los únicos que tienen acceso a la consola de AWS Control Tower.

Cuenta	Conjuntos de permisos	Descripción
Cuenta del archivo de registro	AWSAdministratorAccess	Los usuarios tendrán acceso de administrador en esta cuenta.
Cuenta de auditoría	AWSAdministratorAccess	Los usuarios tendrán acceso de administrador en esta cuenta.
Cuentas de miembros	AWSOrganizationsFullAccess	Los usuarios tienen acceso completo a Organizations en esta cuenta.

AWSSecurityAuditPowerUsers

Cuenta	Conjuntos de permisos	Descripción
Cuenta de administración	AWSPowerUserAccess	Los usuarios pueden realizar tareas de desarrollo de aplicaciones y pueden crear y configurar recursos y servicios que respalden AWS el desarrollo de aplicaciones inteligentes.
Cuenta del archivo de registro	AWSPowerUserAccess	Los usuarios pueden realizar tareas de desarrollo de aplicaciones y crear y configurar recursos y servicios que respalden AWS el desarrollo de aplicaciones inteligentes.
Cuenta de auditoría	AWSPowerUserAccess	Los usuarios pueden realizar tareas de desarrollo de aplicaciones y crear y configurar recursos y servicios

Cuenta	Conjuntos de permisos	Descripción
		que respalden AWS el desarrollo de aplicaciones inteligentes.
Cuentas de miembros	AWSPowerUserAccess	Los usuarios pueden realizar tareas de desarrollo de aplicaciones y crear y configurar recursos y servicios que respalden AWS el desarrollo de aplicaciones inteligentes.

AWSSecurityAuditors

Cuenta	Conjuntos de permisos	Descripción
Cuenta de administración	AWSReadOnlyAccess	Los usuarios tienen acceso de solo lectura a todos los AWS servicios y recursos de esta cuenta.
Cuenta del archivo de registro	AWSReadOnlyAccess	Los usuarios tienen acceso de solo lectura a todos los AWS servicios y recursos de esta cuenta.
Cuenta de auditoría	AWSReadOnlyAccess	Los usuarios tienen acceso de solo lectura a todos los AWS servicios y recursos de esta cuenta.
Cuentas de miembros	AWSReadOnlyAccess	Los usuarios tienen acceso de solo lectura a todos los AWS servicios y recursos de esta cuenta.

AWSLogArchiveAdmins

Cuenta	Conjuntos de permisos	Descripción
Cuenta del archivo de registro	AWSAdministratorAccess	Los usuarios tendrán acceso de administrador en esta cuenta.

AWSLogArchiveViewers

Cuenta	Conjuntos de permisos	Descripción
Cuenta del archivo de registro	AWSReadOnlyAccess	Los usuarios tienen acceso de solo lectura a todos los AWS servicios y recursos de esta cuenta.

AWSAuditAccountAdmins

Cuenta	Conjuntos de permisos	Descripción
Cuenta de auditoría	AWSAdministratorAccess	Los usuarios tendrán acceso de administrador en esta cuenta.

Información general sobre la administración de los permisos de acceso a los recursos de la Torre de Control de AWS

Cada AWS recurso es propiedad de un Cuenta de AWS, y los permisos para crear u obtener acceso a un recurso se rigen por las políticas de permisos. Un administrador de cuentas puede asociar políticas de permisos a identidades de IAM (es decir, usuarios, grupos y funciones). Algunos servicios (como AWS Lambda) también permiten adjuntar políticas de permisos a los recursos.

> **Note**
>
> Un administrador de la cuenta (o administrador) es un usuario con privilegios de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Cuando sea responsable de conceder permisos a un usuario o rol, debe conocer y realizar un seguimiento de los usuarios y roles que requieren permisos, los recursos para los que cada usuario o rol requiere permisos y las acciones específicas que deben permitirse para operar esos recursos.

Temas

- Recursos y operaciones de AWS Control Tower
- Acerca de la propiedad de los recursos
- Administra el acceso a los recursos
- Especifique los elementos de la política: acciones, efectos y principios
- Especificación de las condiciones de una política

Recursos y operaciones de AWS Control Tower

En AWS Control Tower, el recurso principal es una landing zone. AWS Control Tower también admite un tipo de recurso adicional, los controles, que a veces se denominan barandas. Sin embargo, en el caso de AWS Control Tower, solo puede administrar los controles en el contexto de una landing zone existente. Los controles pueden denominarse subrecursos.

Los recursos y subrecursos de Amazon AWS tienen nombres de recursos de Amazon (ARN) exclusivos asociados a ellos, como se muestra en el siguiente ejemplo.

AWS Control Tower proporciona un conjunto de operaciones de API para que funcionen con los recursos de la Torre de Control de AWS. Para obtener una lista de las operaciones disponibles, consulte AWS Control Tower, la referencia de la API de AWS Control Tower.

Para obtener más información sobre los AWS CloudFormation recursos de AWS Control Tower, consulte la Guía del AWS CloudFormation usuario.

Acerca de la propiedad de los recursos

La AWS cuenta es propietaria de los recursos que se crean en la cuenta, independientemente de quién los haya creado. En concreto, el propietario del recurso es la AWS cuenta de la entidad principal (es decir, el usuario Cuenta de AWS raíz, un usuario del Centro de Identidad de IAM, un usuario de IAM o un rol de IAM) que autentica la solicitud de creación de recursos. Los siguientes ejemplos ilustran cómo funciona:

- Si utilizas las AWS credenciales de usuario raíz de tu AWS cuenta para configurar una landing zone, tu AWS cuenta es la propietaria del recurso.
- Si creas un usuario de IAM en tu AWS cuenta y le concedes permisos para configurar una landing zone, el usuario podrá configurar una landing zone siempre que su cuenta cumpla los requisitos previos. Sin embargo, su AWS cuenta, a la que pertenece el usuario, es propietaria del recurso landing zone.
- Si creas un rol de IAM en tu AWS cuenta con permisos para configurar una landing zone, cualquiera que pueda asumir el rol podrá configurar una landing zone. Tu AWS cuenta, a la que pertenece el rol, es propietaria del recurso landing zone.

Administra el acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

> **Note**
>
> En esta sección se analiza el uso de IAM en el contexto de AWS Control Tower. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte ¿Qué es IAM? en la Guía del usuario de IAM. Para obtener más información acerca de la sintaxis y las descripciones de las políticas de IAM, consulte Referencia de políticas de IAM de AWS en la Guía del usuario de IAM.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM). Las políticas que se adjuntan a un recurso se denominan políticas basadas en recursos.

> **Note**
>
> AWS Control Tower solo admite políticas basadas en identidad (políticas de IAM).

Temas

Acerca de las políticas basadas en la identidad (políticas de IAM)

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Adjunte una política de permisos a un usuario o grupo de su cuenta: para conceder a un usuario permisos para crear un recurso de la Torre de Control Tower de AWS, como la configuración de una landing zone, puede adjuntar una política de permisos a un usuario o grupo al que pertenezca el usuario.
- Adjuntar una política de permisos a un rol (conceder permisos para cuentas cruzadas): puede adjuntar una política de permisos basada en identidades a un rol de IAM para conceder permisos para cuentas cruzadas. Por ejemplo, el administrador de una AWS cuenta (cuenta A) puede crear un rol que conceda permisos entre cuentas a otra AWS cuenta (cuenta B), o el administrador puede crear un rol que conceda permisos a otro AWS servicio.
  1. El administrador de la cuenta A crea una función de IAM y adjunta una política de permisos a la función que concede permisos para gestionar los recursos de la cuenta A.
  2. El administrador de la cuenta A adjunta una política de confianza al rol. La política identifica la cuenta B como la entidad principal, que puede asumir el rol.
  3. Como principal, el administrador de la cuenta B puede conceder permiso a cualquier usuario de la cuenta B para que asuma la función. Al asumir esa función, los usuarios de la cuenta B pueden crear recursos de la cuenta A u obtener acceso a ellos.
  4. Para conceder a un AWS servicio la capacidad (permisos) de asumir el rol, el principal que especifiques en la política de confianza puede ser un AWS servicio.

Cree funciones y asigne permisos

Los roles y permisos le dan acceso a los recursos, en la Torre de Control Tower de AWS y en otros AWS servicios, incluido el acceso programático a los recursos.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones descritas en Crear un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para obtener más información sobre el uso de IAM para delegar permisos, consulte Administración de accesos en la Guía del usuario de IAM.

> **Note**
>
> Al configurar una zona de aterrizaje de AWS Control Tower, necesitará un usuario o un rol con la política AdministratorAccessadministrada. (arn:aws:iam: :aws:policy/) AdministratorAccess

Para crear un rol para una (consola de IAM) Servicio de AWS

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, elija Crear rol.

3. En Tipo de entidad de confianza, elija Servicio de AWS.
4. En Servicio o caso de uso, seleccione un servicio y, a continuación, el caso de uso. Los casos de uso son definidos por el servicio de modo tal que ya incluyen la política de confianza que el servicio mismo requiere.
5. Elija Siguiente.
6. Para las Políticas de permisos, las opciones dependen del caso de uso que haya seleccionado:
   - Si el servicio define los permisos para el rol, no puede seleccionar políticas de permisos.
   - Seleccione entre un conjunto limitado de políticas de permisos.
   - Seleccione una de todas las políticas de permisos.
   - No seleccione ninguna política de permisos en este momento. Después de crear el rol, genere las políticas y luego asócielas al rol.
7. (Opcional) Configure un límite de permisos. Se trata de una característica avanzada que está disponible para los roles de servicio, pero no para los roles vinculados a servicios.
   a. Abra la sección Configurar límite de permisos y, a continuación, elija Utilizar un límite de permisos para controlar los permisos que puede tener el rol como máximo.

      IAM incluye una lista de las políticas AWS gestionadas y gestionadas por los clientes de tu cuenta.
   b. Seleccione la política que desea utilizar para el límite de permisos.
8. Elija Siguiente.
9. Para Nombre del rol, las opciones varían según el servicio:
   - Si el servicio define el nombre del rol, no podrá editarlo.
   - Si el servicio define un prefijo para el nombre del rol, puede ingresar un sufijo opcional.
   - Si el servicio no define el nombre del rol, podrá nombrarlo usted mismo.

> **Important**
>
> Cuando asigne un nombre a un rol, tenga en cuenta lo siguiente:
>
> - Los nombres de los roles deben ser únicos dentro de tu perfil Cuenta de AWS y no se pueden hacer únicos por mayúsculas y minúsculas.
>
>   Por ejemplo, no puede crear roles denominados tanto **`PRODROLE`** como **`prodrole`**. Cuando se utiliza un nombre de rol en una política o como parte de un ARN, el

nombre de rol distingue entre mayúsculas y minúsculas, sin embargo, cuando un nombre de rol les aparece a los clientes en la consola, como por ejemplo durante el proceso de inicio de sesión, el nombre de rol no distingue entre mayúsculas y minúsculas.

- Dado que otras entidades podrían hacer referencia al rol, no es posible editar el nombre del rol una vez creado.

10. (Opcional) En Descripción, ingrese una descripción para el rol.
11. (Opcional) Para editar los casos de uso y los permisos de la función, en las secciones Paso 1: Seleccionar entidades confiables o en Paso 2: Agregar permisos, elija Editar.
12. (Opcional) Para ayudar a identificar, organizar o buscar el rol, agregue etiquetas como pares clave-valor. Para obtener más información sobre el uso de etiquetas en IAM, consulte Etiquetado de recursos de IAM en la Guía de usuario de IAM.
13. Revise el rol y, a continuación, elija Crear rol.

Para utilizar el editor de política de JSON para crear una política

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la izquierda, seleccione Políticas.

   Si es la primera vez que elige Políticas, aparecerá la página Bienvenido a políticas administradas. Elija Comenzar.
3. En la parte superior de la página, seleccione Crear política.
4. En la sección Editor de políticas, seleccione la opción JSON.
5. Introduzca o pegue un documento de política de JSON. Para obtener más información sobre el lenguaje de la política de IAM, consulte Referencia de políticas JSON de IAM.
6. Resuelva las advertencias de seguridad, errores o advertencias generales generadas durante la validación de política y luego elija Siguiente.

> **Note**
>
> Puede alternar entre las opciones Visual y JSON del editor en todo momento. No obstante, si realiza cambios o selecciona Siguiente en la opción Visual del editor, es posible que IAM reestructure la política, con el fin de optimizarla para el editor visual.

Para obtener más información, consulte Reestructuración de política en la Guía del usuario de IAM.

7. (Opcional) Al crear o editar una política en AWS Management Console, puedes generar una plantilla de política JSON o YAML que puedes usar en AWS CloudFormation las plantillas.

   Para ello, en el editor de políticas, selecciona Acciones y, a continuación, selecciona Generar CloudFormation plantilla. Para obtener más información AWS CloudFormation, consulte la referencia sobre AWS Identity and Access Management los tipos de recursos en la Guía del AWS CloudFormation usuario.
8. Cuando haya terminado de agregar permisos a la política, seleccione Siguiente.
9. En la página Revisar y crear, introduzca el Nombre de la política y la Descripción (opcional) para la política que está creando. Revise los Permisos definidos en esta política para ver los permisos que concede la política.
10. (Opcional) Agregar metadatos a la política al adjuntar las etiquetas como pares de clave-valor. Para obtener más información sobre el uso de etiquetas en IAM, consulte Etiquetado de recursos de IAM en la Guía de usuario de IAM.
11. Elija Crear política para guardar la nueva política.

Para utilizar el editor visual para crear una política

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la izquierda, seleccione Políticas.

   Si es la primera vez que elige Políticas, aparecerá la página Bienvenido a políticas administradas. Elija Get Started (Comenzar).
3. Elija Create Policy (Crear política).
4. En la sección del editor de políticas, busque la sección Seleccione un servicio y, a continuación, elija un Servicio de AWS. Puede utilizar el cuadro de búsqueda en la parte superior para limitar los resultados en la lista de servicios. Puede elegir solo un servicio dentro de un bloque de permisos de editor visual. Para conceder acceso a más de un servicio, agregue varios bloques de permisos seleccionando Agregar más permisos.
5. En Acciones permitidas, seleccione las acciones que desee agregar a la política. Puede elegir acciones de una de las siguientes formas:

- Active la casilla de verificación para todas las acciones.
- Selecciona Añadir acciones para introducir el nombre de una acción específica. Puede utilizar un carácter comodín (*) para especificar varias acciones.
- Seleccione uno de los grupos de niveles de acceso para elegir todas las acciones del nivel de acceso (por ejemplo, Leer, Escribir, o Lista).
- Amplíe cada uno de los grupos Access level (Nivel de acceso) para elegir acciones individuales.

De forma predeterminada, la política que está creando permite las acciones que usted elija. Para denegar las acciones elegidas, seleccione Switch to deny permissions (Cambiar a denegar permisos). Dado que IAM deniega de forma predeterminada, por motivos de seguridad recomendamos que permita solo aquellas acciones y recursos a los que un usuario necesita acceso. Cree una declaración JSON para denegar los permisos solo si desea anular un permiso permitido por separado por otra declaración o política. Le recomendamos que limite al mínimo el número de operaciones de denegación de permisos, ya que pueden aumentar la dificultad de solucionar problemas con los permisos.

6. Para Recursos, si el servicio y las acciones que seleccionó en los pasos anteriores no admiten la elección de recursos específicos, todos los recursos están permitidos y no puede editar esta sección.

   Si eligió una o más acciones que admiten permisos en el nivel de recursos, el editor visual enumera dichos recursos. A continuación, puede elegir Resources (Recursos) para especificar los recursos para su política.

   Puede especificar recursos de las siguientes maneras:

   - Seleccione Agregar ARN para especificar recursos por su nombre de recurso de Amazon (ARN). Puede utilizar el editor ARN visual o enumerar ARN manualmente. Para obtener más información sobre la sintaxis de los ARN, consulte Nombres de recursos de Amazon (ARN) en la Guía del usuario de IAM. Para obtener información sobre el uso de los ARN en el `Resource` elemento de una política, consulte Elementos de la política JSON de IAM: recurso en la Guía del usuario de IAM.
   - Seleccione Cualquiera de esta cuenta junto a un recurso para conceder permisos a cualquier recurso de ese tipo.
   - Seleccione Todos para seleccionar todos los recursos para el servicio.

7. (Opcional) Seleccione Solicitar condiciones: opcional para agregar condiciones a la política que está creando. Las condiciones limitan el efecto de una instrucción de política de JSON. Por ejemplo, puede especificar que a un usuario se le permite realizar las acciones en los recursos solo cuando la solicitud de dicho usuario se produce dentro de un intervalo de tiempo determinado. También puede usar las condiciones de uso común para limitar si un usuario debe autenticarse mediante un dispositivo de autenticación multifactor (MFA). O bien puede exigir que la solicitud se origine dentro de un determinado rango de direcciones IP. Para ver una lista de todas las claves de contexto que puede usar en una condición de política, consulte Acciones, recursos y claves de condición de los AWS servicios en la Referencia de autorización de servicios.

   Puede elegir las condiciones de una de las siguientes formas:

   - Utilice las casillas de verificación para seleccionar condiciones de uso común.
   - Seleccione Agregar otra condición para especificar otras condiciones. Elija la clave de condición, el calificador y el operador de la condición y, a continuación, introduzca un valor. Para agregar más de un valor, seleccione Agregar. Puede considerar que los valores están conectados por un `OR` operador lógico. Cuando haya terminado, seleccione Agregar condición.

   Para agregar más de una condición, vuelva a seleccionar Agregar condición. Repita este procedimiento según sea necesario. Cada condición se aplica únicamente a este bloque de permisos del editor visual. Todas las condiciones deben ser "true" para que el bloque de permisos se considere una coincidencia. En otras palabras, considere las condiciones que se van a conectar mediante un `AND` operador lógico.

   Para obtener más información sobre el elemento Condición, consulte Elementos de la política JSON de IAM: Condición en la Guía del usuario de IAM.

8. Para agregar más bloques de permisos, seleccione Agregar más permisos. Para cada bloque, repita los pasos 2 a 5.

   > **Note**
   >
   > Puede alternar entre las opciones Visual y JSON del editor en todo momento. No obstante, si realiza cambios o selecciona Siguiente en la opción Visual del editor, es posible que IAM reestructure la política, con el fin de optimizarla para el editor visual.

Para obtener más información, consulte Reestructuración de política en la Guía del usuario de IAM.

9. (Opcional) Al crear o editar una política en AWS Management Console, puedes generar una plantilla de política JSON o YAML que puedes usar en las plantillas. AWS CloudFormation

   Para ello, en el editor de políticas, selecciona Acciones y, a continuación, selecciona Generar CloudFormation plantilla. Para obtener más información AWS CloudFormation, consulte la referencia sobre AWS Identity and Access Management los tipos de recursos en la Guía del AWS CloudFormation usuario.
10. Cuando haya terminado de agregar permisos a la política, seleccione Siguiente.
11. En la página Revisar y crear, introduzca el Nombre de la política y la Descripción (opcional) para la política que está creando. Revise los Permisos definidos en esta política para asegurarse de que ha concedido los permisos deseados.
12. (Opcional) Agregar metadatos a la política al adjuntar las etiquetas como pares de clave-valor. Para obtener más información sobre el uso de etiquetas en IAM, consulte Etiquetado de recursos de IAM en la Guía de usuario de IAM.
13. Elija Crear política para guardar la nueva política.

Para conceder acceso programático

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. AWS Management Console La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el Centro de identidades de IAM)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del uso AWS IAM Identity Center en AWS CLI la Guía del AWS

¿Qué usuario necesita acceso programático?	Para	Mediante
		Command Line Interface usuario. • Para ver AWS los SDK, las herramientas y las AWS API, consulte la autenticación del IAM Identity Center en la Guía de referencia de AWS los SDK y las herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credencia les de usuario de IAM en la Guía del usuario.AWS Command Line Interface • Para obtener informaci ón AWS sobre los SDK y las herramientas, consulte Autenticarse con credencia les de larga duración en la Guía de referencia de los AWS SDK y las herramien tas. • Para obtener informaci ón AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Protéjase contra los atacantes

Para obtener más información sobre cómo protegerte de los atacantes cuando concedes permisos a otros directores de AWS servicio, consulta las condiciones opcionales de las relaciones de confianza en tus funciones. Si añades determinadas condiciones a tus políticas, puedes ayudar a prevenir un tipo específico de ataque, conocido como ataque de ayudante confuso, que se produce cuando una entidad coacciona a una entidad con más privilegios para que lleve a cabo una acción, como la suplantación de identidad entre servicios. Para obtener información general sobre las condiciones de la política, consulte también. Especificación de las condiciones de una política

Para obtener más información sobre el uso de políticas basadas en la identidad con AWS Control Tower, consulte. Uso de políticas basadas en identidad (políticas de IAM) para AWS Control Tower Para obtener más información sobre usuarios, grupos, roles y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede asociar una política a un bucket de S3 para administrar los permisos de acceso a dicho bucket. AWS Control Tower no admite políticas basadas en recursos.

Especifique los elementos de la política: acciones, efectos y principios

Puede configurar y administrar su zona de aterrizaje a través de la consola de AWS Control Tower o las API de landing zone. Para configurar tu landing zone, debes ser un usuario de IAM con permisos administrativos tal y como se definen en una política de IAM.

Los siguientes elementos son los más básicos que puede identificar en una política:

- Recurso: en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte Recursos y operaciones de AWS Control Tower.
- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Para obtener información sobre los tipos de acciones que se pueden realizar, consulte Acciones definidas por AWS Control Tower.
- Efecto: especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- Principal: en las políticas basadas en la identidad (políticas de IAM), el usuario al que se vincula la política es el principal implícito. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). AWS Control Tower no admite políticas basadas en recursos.

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte Referencia de la política de IAM de AWS en la Guía del usuario de IAM.

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de IAM para especificar las condiciones en la que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte Condition en la Guía del usuario de IAM.

Para expresar las condiciones, puede utilizar claves de condición predefinidas. No hay claves de condición específicas para AWS Control Tower. Sin embargo, existen claves AWS de condición muy amplias que puede utilizar según convenga. Para obtener una lista completa de las claves AWS de ancho, consulte las claves disponibles para las condiciones en la Guía del usuario de IAM.

Evite la suplantación de identidad entre servicios

En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. Cuando un servicio llama a otro servicio, la suplantación de identidad entre servicios se produce si un servicio manipula a otro servicio para que utilice sus permisos y actúe con los recursos de un cliente de una forma que de otro modo no estaría permitida. Para evitar este ataque, AWS proporciona herramientas que te ayudan a proteger tus datos, de forma que solo los servicios que cuenten con un permiso legítimo puedan acceder a los recursos de tu cuenta.

Le recomendamos que utilice las `aws:SourceAccount` condiciones `aws:SourceArn` y de sus políticas para limitar los permisos que AWS Control Tower concede a otro servicio para acceder a sus recursos.

- `aws:SourceArn`Utilícelo si desea que solo un recurso esté asociado al acceso entre servicios.
- `aws:SourceAccount`Utilícelo si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.
- Si el `aws:SourceArn` valor no contiene el ID de la cuenta, como el ARN de un bucket de Amazon S3, debe utilizar ambas condiciones para limitar los permisos.
- Si usa ambas condiciones y si el `aws:SourceArn` valor contiene el ID de cuenta, el `aws:SourceAccount` valor y la cuenta que figura en el `aws:SourceArn` valor deben mostrar el mismo ID de cuenta cuando se utilicen en la misma declaración de política

Para obtener más información y ejemplos, consulte https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html.

Uso de políticas basadas en identidad (políticas de IAM) para AWS Control Tower

En este tema se proporcionan ejemplos de políticas basadas en la identidad que demuestran cómo un administrador de cuentas puede adjuntar políticas de permisos a las identidades de IAM (es decir, usuarios, grupos y funciones) y, de ese modo, conceder permisos para realizar operaciones en los recursos de la Torre de Control Tower de AWS.

> **Important**
>
> Le recomendamos que consulte primero los temas introductorios en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a los recursos de la Torre de Control de AWS. Para obtener más información, consulte Información general sobre la administración de los permisos de acceso a los recursos de la Torre de Control de AWS.

Permisos necesarios para usar la consola de la Torre de Control de AWS

AWS Control Tower crea tres funciones automáticamente al configurar una landing zone. Los tres roles son necesarios para permitir el acceso a la consola. AWS Control Tower divide los permisos en tres funciones como práctica recomendada para restringir el acceso a un conjunto mínimo de acciones y recursos.

Tres funciones obligatorias

- AWS ControlTowerAdmin rol
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

Le recomendamos que restrinja el acceso a las políticas de confianza de sus roles para estos roles. Para obtener más información, consulte Condiciones opcionales para las relaciones de confianza de sus roles.

AWS ControlTowerAdmin rol

Esta función proporciona a AWS Control Tower acceso a la infraestructura fundamental para el mantenimiento de la landing zone. El `AWS ControlTowerAdmin` rol requiere una política

administrada adjunta y una política de confianza del rol para el rol de IAM. Una política de confianza de roles es una política basada en los recursos que especifica qué directores pueden asumir la función.

A continuación, se muestra un fragmento de ejemplo de esta política de confianza de roles:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Para crear este rol desde la AWS CLI y colocarlo en un archivo llamado`trust.json`, este es un ejemplo de comando CLI:

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

Esta función requiere dos políticas de IAM.

1. Una política en línea, por ejemplo:

   ```
   {
       "Version": "2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": "ec2:DescribeAvailabilityZones",
               "Resource": "*"
           }
       ]
   }
   ```

2. La política gestionada que sigue, que es la`AWS ControlTowerServiceRolePolicy`.

AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicySe trata de una política AWS administrada que define los permisos para crear y administrar los recursos de la Torre de Control de AWS, como AWS CloudFormation conjuntos de pilas e instancias apiladas, archivos de AWS CloudTrail registro, un agregador de configuraciones para la Torre de Control de AWS, así como AWS Organizations cuentas y unidades organizativas (OU) que se rigen por la Torre de Control de AWS.

Las actualizaciones de esta política gestionada se resumen en la tabla. Políticas administradas para AWS Control Tower

Para obtener más información, consulte `AWSControlTowerServiceRolePolicy`la Guía de referencia de políticas administradas de AWS.

Nombre de la política administrada: `AWS ControlTowerServiceRolePolicy`

El artefacto JSON para `AWS ControlTowerServiceRolePolicy` es el siguiente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
```

```
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
```

```
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeleteConfigurationAggregator",
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
                }
            }
        }
    ]
}
```

Política de confianza de roles:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

La política en línea es`AWSControlTowerAdminPolicy`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AWS ControlTowerStackSetRole

AWS CloudFormation asume esta función para implementar conjuntos de pilas en las cuentas creadas por AWS Control Tower. Política insertada:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Política de confianza

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRole

AWS Control Tower CloudTrail lo habilita como práctica recomendada y proporciona esta función a CloudTrail. CloudTrailasume esta función para crear y publicar CloudTrail registros. Política insertada:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

Política de confianza

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerBlueprintAccess requisitos de función

AWS Control Tower requiere que cree el `AWSControlTowerBlueprintAccess` rol en la cuenta de blueprint hub designada, dentro de la misma organización.

Nombre de rol

El nombre de rol debe ser `AWSControlTowerBlueprintAccess`.

Política de confianza de roles

El rol debe configurarse para confiar en los siguientes principios:

- El director que usa AWS Control Tower en la cuenta de administración.
- El `AWSControlTowerAdmin` rol en la cuenta de administración.

El siguiente ejemplo muestra una política de confianza de privilegios mínimos. Cuando cree su propia política, sustituya el término *`YourManagementAccountId`*por el ID de cuenta real de su cuenta de administración de AWS Control Tower y sustituya el término *`YourControlTowerUserRole`*por el identificador de la función de IAM de su cuenta de administración.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
```

```
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Permisos de rol

Debe adjuntar la política gestionada AWSServiceCatalogAdminFullAccessal rol.

AWSServiceRoleForAWSControlTower

Esta función proporciona a AWS Control Tower acceso a la cuenta de Log Archive, la cuenta de auditoría y las cuentas de los miembros para operaciones fundamentales para el mantenimiento de la landing zone, como la notificación de la desviación de recursos.

El `AWSServiceRoleForAWSControlTower` rol requiere una política administrada adjunta y una política de confianza de roles para el rol de IAM.

Política gestionada para este rol: `AWSControlTowerAccountServiceRolePolicy`

Política de confianza de roles:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerAccountServiceRolePolicy

Esta política AWS gestionada permite a AWS Control Tower llamar en su nombre a AWS los servicios que proporcionan una configuración de cuentas automatizada y un gobierno centralizado.

La política contiene los permisos mínimos para que la Torre de Control de AWS implemente el reenvío de AWS Security Hub hallazgos para los recursos administrados por los controles de Security Hub que forman parte del estándar administrado por el servicio Security Hub: AWS Control Tower, e impide cambios que restrinjan la capacidad de administrar las cuentas de los clientes. Forma parte de un proceso de detección de AWS Security Hub desviaciones en segundo plano y no lo inicia directamente el cliente.

La política otorga permisos para crear EventBridge reglas de Amazon, específicamente para los controles de Security Hub, en cada cuenta de miembro, y estas reglas deben especificar una exacta EventPattern. Además, una regla solo puede funcionar en las reglas administradas por nuestro director de servicio.

Director de servicio: `controltower.amazonaws.com`

El artefacto JSON para `AWSControlTowerAccountServiceRolePolicy` es el siguiente:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
     "events:detail-type": "false"
    },
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com",
     "events:detail-type": "Security Hub Findings - Imported"
    }
   }
  },
  // Other operations to manage the managed rule
  {
   "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
```

```
    "Action": [
     "events:DeleteRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "controltower.amazonaws.com"
     }
    }
   },
   // More managed rule permissions
   {
    "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
   },
   // Add permission to publish the security notifications to SNS
   {
    "Sid": "AllowControlTowerToPublishSecurityNotifications",
    "Effect": "Allow",
    "Action": "sns:publish",
    "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
    "Condition": {
     "StringEquals": {
      "aws:PrincipalAccount": "${aws:ResourceAccount}"
     }
    }
   },
   // For drift verification
   {
    "Sid": "AllowActionsForSecurityHubIntegration",
    "Effect": "Allow",
    "Action": [
     "securityhub:DescribeStandardsControls",
     "securityhub:GetEnabledStandards"
    ],
```

```
    "Resource": "arn:aws:securityhub:*:*:hub/default"
   }
  ]
}
```

Las actualizaciones de esta política gestionada se resumen en la tabla,Políticas administradas para AWS Control Tower.

Políticas administradas para AWS Control Tower

AWS aborda muchos casos de uso comunes al proporcionar políticas de IAM independientes que son creadas y administradas por. AWS Las políticas administradas conceden los permisos necesarios para casos de uso comunes, lo que le evita tener que investigar los permisos que se necesitan. Para más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Cambio	Descripción	Fecha
AWSControlTowerAccountServiceRolePolicy— Una nueva política	AWS Control Tower agregó una nueva función vinculada a un servicio que permite a AWS Control Tower crear y administrar reglas de eventos y, en función de esas reglas, administrar la detección de desviaciones para los controles relacionados con Security Hub. Este cambio es necesario para que los clientes puedan ver los recursos desviados en la consola, cuando esos recursos están relacionados con los controles de Security Hub que forman parte del estándar gestionado por el	22 de mayo de 2023

Cambio	Descripción	Fecha
	servicio Security Hub: AWS Control Tower.	
AWS ControlTowerServiceRolePolicy: actualización de una política actual	AWS Control Tower agregó nuevos permisos que permiten a AWS Control Tower realizar llamadas al servicio de administración de cuentas y a las `EnableRegion` `GetRegionOptStatus` API implementadas por el servicio de administración de AWS cuentas, para que la suscripción Regiones de AWS esté disponible para las cuentas de los clientes en la zona de aterrizaje (cuenta de administración, cuenta de archivo de registros, cuenta de auditoría, cuentas de miembros de la OU). `ListRegions` Este cambio es necesario para que los clientes puedan tener la opción de ampliar la gobernanza regional de AWS Control Tower a las regiones que opten por participar.	6 de abril de 2023

Cambio	Descripción	Fecha
AWS ControlTowerServiceRolePolicy: actualización de una política actual	AWS Control Tower agregó nuevos permisos que permiten a AWS Control Tower asumir el `AWSControlTowerBlueprintAccess` rol en la cuenta blueprint (hub), que es una cuenta dedicada en una organización que contiene planos predefinidos almacenados en uno o más productos de Service Catalog. AWS Control Tower asume la `AWSControlTowerBlueprintAccess` función de realizar tres tareas: crear una cartera de Service Catalog, añadir el producto plano solicitado y compartir la cartera con la cuenta de un miembro solicitado en el momento del aprovisionamiento de la cuenta. Este cambio es necesario para que los clientes puedan aprovisionar cuentas personalizadas a través de AWS Control Tower Account Factory.	28 de octubre de 2022

Cambio	Descripción	Fecha
AWS ControlTowerServiceRolePolicy: actualización de una política actual	AWS Control Tower agregó nuevos permisos que permiten a los clientes configurar AWS CloudTrail rutas a nivel de organización, a partir de la versión 3.0 de landing zone. La CloudTrail función basada en la organización requiere que los clientes tengan habilitado el acceso de confianza al CloudTrail servicio y que el usuario o rol de IAM tenga permiso para crear un registro a nivel de organización en la cuenta de administración.	20 de junio de 2022

Cambio	Descripción	Fecha
AWS ControlTowerServiceRolePolicy: actualización de una política actual	AWS Control Tower agregó nuevos permisos que permiten a los clientes usar el cifrado de claves KMS. La función KMS permite a los clientes proporcionar su propia clave KMS para cifrar sus CloudTrail registros. Los clientes también pueden cambiar la clave KMS durante la actualización o reparación de la zona de aterrizaje. Al actualizar la clave KMS, AWS CloudFormation necesita permisos para llamar a la AWS CloudTrail `PutEventSelector` API. El cambio en la política consiste en permitir que el AWS ControlTowerAdminrol llame a la AWS CloudTrail `PutEventSelector` API.	28 de julio de 2021
AWS Control Tower comenzó a rastrear los cambios	AWS Control Tower comenzó a realizar un seguimiento de los cambios en sus políticas AWS administradas.	27 de mayo de 2021

Seguridad en AWS Control Tower

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a la Torre de Control de AWS, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por los AWS servicios que utilice. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar AWS Control Tower. En los siguientes temas, se muestra cómo configurar la Torre de Control de AWS para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de la Torre de Control de AWS.

Protección de datos en AWS Control Tower

El modelo de se aplica a protección de datos en la Torre de Control de AWS. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access

Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS Control Tower u otro dispositivo Servicios de AWS mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

> **Note**
>
> El registro de la actividad de los usuarios AWS CloudTrail se gestiona automáticamente en AWS Control Tower al configurar la landing zone.

Para obtener más información sobre la protección de datos, consulte la entrada de blog relativa al modelo de responsabilidad compartida de AWS y GDPR en el blog de seguridad de AWS . AWS Control Tower ofrece las siguientes opciones que puede utilizar para proteger el contenido que existe en su landing zone:

Temas

Cifrado en reposo

AWS Control Tower utiliza depósitos de Amazon S3 y bases de datos de Amazon DynamoDB que se cifran en reposo mediante claves gestionadas por Amazon S3 (SSE-S3) como soporte para su landing zone. Este cifrado se configura de forma predeterminada cuando configuras tu landing zone. Si lo desea, puede configurar su landing zone para cifrar los recursos con claves de cifrado de KMS. También puedes establecer el cifrado en reposo para los servicios que utilizas en tu landing zone para los servicios que lo admiten. Para obtener más información, consulta el capítulo de seguridad de la documentación en línea de ese servicio.

Cifrado en tránsito

AWS Control Tower utiliza Transport Layer Security (TLS) y el cifrado del lado del cliente para el cifrado en tránsito en apoyo de su landing zone. Además, para acceder a la Torre de Control de AWS es necesario utilizar la consola, a la que solo se puede acceder a través de un punto de conexión HTTPS. Este cifrado se configura de forma predeterminada cuando configuras tu landing zone.

Restricción del acceso a contenido

Como práctica recomendada, debería restringir el acceso al subconjunto de usuarios adecuado. Con AWS Control Tower, puede hacerlo asegurándose de que los administradores de la nube central y los usuarios finales tengan los permisos de IAM correctos o, en el caso de los usuarios del IAM Identity Center, de que estén en los grupos correctos.

- Para obtener más información sobre los roles y las políticas para entidades de IAM, consulte la Guía del usuario de IAM.
- Para obtener más información sobre los grupos del Centro de identidad de IAM que se crean al configurar la landing zone, consulteGrupos de centros de identidad de IAM para AWS Control Tower.

Validación de conformidad para AWS Control Tower

AWS Control Tower es un servicio bien diseñado que puede ayudar a su organización a cumplir sus necesidades de conformidad con controles y prácticas recomendadas. Además, auditores externos evalúan la seguridad y el cumplimiento de varios servicios que puedes usar en tu landing zone como parte de varios programas de AWS cumplimiento. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de cumplimiento. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact en la Guía del AWS Artifact usuario.

Su responsabilidad de conformidad al utilizar AWS Control Tower viene determinada por la confidencialidad de sus datos, los objetivos de conformidad de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudarlo a cumplir con los requisitos:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- Diseño de arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: este documento técnico describe cómo las empresas pueden utilizar AWS para crear aplicaciones compatibles con la HIPAA.
- AWS Recursos de conformidad: esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- AWS Config— Este AWS servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Control Tower

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad.

AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que se conectan mediante redes de baja latencia, alto rendimiento y alta redundancia. Las zonas de disponibilidad permiten diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener una lista de los Regiones de AWS lugares en los que AWS Control Tower está disponible, consulteCómo funcionan AWS las regiones con AWS Control Tower.

Tu región de origen se define como la AWS región en la que se configuró tu landing zone.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura AWS global.

Seguridad de la infraestructura en AWS Control Tower

AWS Control Tower está protegida por los procedimientos de seguridad de la red AWS global que se describen en el documento técnico Amazon Web Services: Overview of Security Processes.

Utilizas las llamadas a la API AWS publicadas para acceder a AWS los servicios y recursos de tu landing zone a través de la red. Necesitamos Transport Layer Security (TLS) 1.2 y recomendamos Transport Layer Security (TLS) 1.3 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede configurar grupos de seguridad para proporcionar seguridad adicional a la infraestructura de red para las cargas de trabajo de las zonas de aterrizaje de AWS Control Tower. Para obtener más información, consulte Tutorial: Configurar grupos de seguridad en la Torre de Control de AWS con AWS Firewall Manager.

Registro y supervisión en la Torre de Control de AWS

La monitorización le permite planificar y responder a posibles incidentes. Los resultados de las actividades de monitoreo se almacenan en archivos de registro. Por lo tanto, el registro y la supervisión son conceptos estrechamente relacionados y son una parte importante de la naturaleza bien diseñada de AWS Control Tower.

Cuando configuras tu landing zone, una de las cuentas compartidas que se crean es la cuenta de archivo de registros. Se dedica a recopilar todos los registros de forma centralizada, incluidos los registros de todas tus cuentas compartidas y de miembros. Los archivos de registro se almacenan en un bucket de Amazon S3. Estos archivos de registro permiten a los administradores y auditores revisar las acciones y los eventos que se han producido.

Como práctica recomendada, debería recopilar los datos de monitoreo de todas las partes de su AWS configuración en sus registros, de modo que pueda depurar más fácilmente un error multipunto en caso de que se produzca. AWS proporciona varias herramientas para monitorizar tus recursos y actividad en tu landing zone.

Por ejemplo, el estado de los controles se supervisa constantemente. Puede ver su estado de un vistazo en la consola de la Torre de Control de AWS o mediante programación mediante las API de la Torre de Control de AWS. El estado y el estado de las cuentas que has aprovisionado en Account Factory también se supervisan constantemente.

Consulta las acciones registradas desde la página de Actividades

En la consola de AWS Control Tower, la página Actividades ofrece una descripción general de las acciones de las cuentas de administración de AWS Control Tower. Para ir a la página de actividades de la Torre de Control de AWS, seleccione Actividades en la barra de navegación de la izquierda.

Las actividades que se muestran en la página Actividades son las mismas que se muestran en el registro de AWS CloudTrail eventos de AWS Control Tower, pero se muestran en formato de tabla. Para obtener más información sobre una actividad específica, selecciónela en la tabla y, a continuación, elija View details (Ver detalles).

Puede ver las acciones y los eventos de las cuentas de los miembros en los archivos de registro.

En las siguientes secciones se describe con más detalle la supervisión y el registro en AWS Control Tower:

Temas

Acerca del inicio de sesión en AWS Control Tower

AWS Control Tower registra las acciones y los eventos automáticamente, mediante su integración con AWS CloudTrail y AWS Config, y los registra en CloudWatch ella. Se registran todas las acciones, incluidas las acciones de la cuenta de administración de la Torre de Control Tower de AWS y de las cuentas de los miembros de su organización. Las acciones y los eventos de la cuenta de administración se pueden ver en la página de actividades de la consola. Puede ver las acciones y los eventos de las cuentas de los miembros en los archivos de registro.

Rutas a nivel de organización

AWS Control Tower establece una nueva CloudTrail ruta al configurar una landing zone. Se trata de un registro a nivel de organización, lo que significa que registra todos los eventos de la cuenta de administración y de todas las cuentas de los miembros de la organización. Esta función se basa en un acceso confiable para otorgar a la cuenta de administración permisos para crear un registro en cada cuenta de miembro.

Para obtener más información sobre la Torre de Control de AWS y las rutas CloudTrail organizativas, consulte Crear una ruta para una organización.

> **Note**
>
> En las versiones de AWS Control Tower anteriores a la versión 3.0 de landing zone, AWS Control Tower creó un registro de cuentas de miembros en cada cuenta. Cuando actualiza a la versión 3.0, su CloudTrail registro se convierte en un registro de la organización. Para conocer las mejores prácticas a la hora de moverse entre senderos, consulta las prácticas recomendadas para cambiar de sendero en la Guía del CloudTrail usuario.

Cuando inscribe una cuenta en la Torre de Control de AWS, esta se rige por el AWS CloudTrail registro de la organización de la Torre de Control de AWS. Si ya tiene una implementación de una

versión de CloudTrail seguimiento en esa cuenta, es posible que vea cargos duplicados, a menos que elimine la versión de seguimiento existente de la cuenta antes de inscribirla en AWS Control Tower.

> **Note**
>
> Cuando actualiza a la versión 3.0 de la zona de aterrizaje, AWS Control Tower elimina en su nombre las rutas a nivel de cuenta (que AWS Control Tower ha creado) de las cuentas inscritas. Los archivos de registro existentes a nivel de cuenta se conservan en su bucket de Amazon S3.

Política de bucket de Amazon S3 en la cuenta de auditoría

En AWS Control Tower, AWS los servicios tienen acceso a sus recursos solo cuando la solicitud proviene de su organización o unidad organizativa (OU). Todos los permisos de escritura deben cumplirse con una `aws:SourceOrgID` condición.

Puedes usar la clave de `aws:SourceOrgID` condición y establecer el valor del ID de tu organización en el elemento de condición de tu política de bucket de Amazon S3. Esta condición garantiza que CloudTrail solo pueda escribir registros en nombre de las cuentas de su organización en su bucket de S3; evita que CloudTrail los registros ajenos a su organización se escriban en su bucket de S3 de AWS Control Tower.

Esta política no afecta a la funcionalidad de sus cargas de trabajo actuales. La política se muestra en el siguiente ejemplo.

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
```

```
        - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
      Condition:
        Bool:
          aws:SecureTransport: false
    - Sid: AWSBucketPermissionsCheck
      Effect: Allow
      Principal:
        Service:
          - cloudtrail.amazonaws.com
          - config.amazonaws.com
      Action: s3:GetBucketAcl
      Resource:
        - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
    - Sid: AWSConfigBucketExistenceCheck
      Effect: Allow
      Principal:
        Service:
          - cloudtrail.amazonaws.com
          - config.amazonaws.com
      Action: s3:ListBucket
      Resource:
        - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
    - Sid: AWSBucketDeliveryForConfig
      Effect: Allow
      Principal:
        Service:
          - config.amazonaws.com
      Action: s3:PutObject
      Resource:
        - Fn::Join:
            - ""
            -
              - !Sub "arn:${AWS::Partition}:s3:::"
              - !Ref "S3AuditBucket"
              - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
      Condition:
        StringEquals:
          aws:SourceOrgID: !Ref OrganizationId
    - Sid: AWSBucketDeliveryForOrganizationTrail
      Effect: Allow
      Principal:
        Service:
          - cloudtrail.amazonaws.com
      Action: s3:PutObject
```

```
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
            aws:SourceOrgID: !Ref OrganizationId
```

Para obtener más información sobre esta clave de condición, consulte la documentación de IAM y la entrada del blog de IAM titulada «Use controles escalables para los AWS servicios que acceden a sus recursos».

Herramientas integradas para la supervisión

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Control Tower y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar la Torre de Control de AWS, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Events ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. CloudWatch Events permite la computación automatizada basada en eventos, ya que puede escribir reglas que vigilen ciertos eventos y activen acciones automatizadas en otros AWS servicios cuando estos eventos ocurren. Para obtener más información, consulta la Guía del usuario de Amazon CloudWatch Events.
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde instancias de Amazon EC2 y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcancen ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga

duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.

- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron.

Consejo: Puedes ver y consultar la CloudTrail actividad de una cuenta a través de CloudWatch Logs and CloudWatch Logs Insights. Esta actividad incluye los eventos del ciclo de vida de AWS Control Tower. CloudWatchLas capacidades de los registros le permiten realizar consultas más detalladas y precisas de las que normalmente podría realizar con CloudTrail ellas.

Para obtener más información, consulte Registro de las acciones de AWS Control Tower con AWS CloudTrail.

Registro de las acciones de AWS Control Tower con AWS CloudTrail

AWS Control Tower está integrada con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en la Torre de Control de AWS. CloudTrail captura las acciones de AWS Control Tower como eventos. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de AWS Control Tower.

Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a la Torre de Control de AWS, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, incluido cómo configurarlo y habilitarlo, consulte la Guía delAWS CloudTrail usuario.

Información sobre la Torre de Control de AWS en CloudTrail

CloudTrail está activado en su AWS cuenta al crearla. Cuando se produce una actividad de eventos admitidos en la Torre de Control de AWS, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos

recientes en su AWS cuenta. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

> **Note**
>
> En las versiones de AWS Control Tower anteriores a la versión 3.0 de landing zone, AWS Control Tower creó un registro de cuentas de miembros. Cuando actualiza a la versión 3.0, su CloudTrail registro se actualiza para convertirse en un registro de la organización. Para conocer las mejores prácticas a la hora de moverse de un sendero a otro, consulta Cómo crear un sendero organizativo en la Guía del CloudTrail usuario.

Recomendado: Crea un sendero

Para obtener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de AWS Control Tower, cree una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS . La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Prepárese para crear una ruta
- Administrar CloudTrail los costos
- CloudTrail Integraciones y servicios compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

AWS Control Tower registra las siguientes acciones como eventos en los archivos de CloudTrail registro:

API públicas

- `DisableControl`

- EnableControl
- GetControlOperation
- ListEnabledControls

Otras API

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- EnableGuardrail
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups
- DescribeSingleSignOn
- DescribeCoreService

- `GetAvailableUpdates`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.
- Si la solicitud se rechazó por denegación de acceso o si se procesó correctamente.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail .

Ejemplo: entradas del archivo de registro de AWS Control Tower

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail los eventos no aparecen en ningún orden específico en los archivos de registro.

El siguiente ejemplo muestra una entrada de CloudTrail registro que muestra la estructura de una entrada de archivo de registro típica para un evento de la Torre de Control de `SetupLandingZone` AWS, incluido un registro de la identidad del usuario que inició la acción.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
```

```
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```

Supervise los cambios en los recursos con AWS Config

AWS Control Tower habilita todas AWS Config las cuentas inscritas, de modo que puede supervisar el cumplimiento mediante controles de detección, registrar los cambios en los recursos y entregar los registros de cambios de los recursos a la cuenta de archivo de registros.

Si tu versión de landing zone es anterior a la 3.0: en el caso de las cuentas inscritas, AWS Config registra todos los cambios en los recursos de todas las regiones en las que opera la cuenta. Cada cambio se modela como un elemento de configuración (IC), que contiene información como el

identificador del recurso, la región, la fecha en que se registró cada cambio y si el cambio se refiere a un recurso conocido o a uno descubierto recientemente.

Si su versión de landing zone es 3.0 o posterior: AWS Control Tower limita el registro de los recursos globales, como los usuarios de IAM, los grupos, las funciones y las políticas administradas por los clientes, únicamente a su región de origen. No se almacenan copias de los cambios en los recursos globales en todas las regiones. Esta limitación del registro de recursos se ajusta a las AWS Config mejores prácticas. La lista completa de los recursos globales está disponible en la AWS Config documentación.

- Para obtener más información AWS Config, consulte Cómo AWS Config funciona.
- Para ver una lista de los recursos compatibles AWS Config , consulta Tipos de recursos compatibles.
- Para obtener información sobre cómo personalizar el seguimiento de recursos en el entorno de la Torre de Control de AWS, consulte la entrada del blog titulada Personalizar el seguimiento de AWS Config recursos en la Torre de Control de AWS.

AWS Control Tower configura un canal de AWS Config entrega en todas las cuentas inscritas. A través de este canal de entrega, registra todos los cambios registrados AWS Config en la cuenta del archivo de registros, donde se almacenan en una carpeta de un depósito de Amazon Simple Storage Service.

Administre AWS Config los costos en AWS Control Tower

En esta sección se describe cómo se AWS Config registran y facturan los cambios en los recursos de sus cuentas de AWS Control Tower. Esta información puede ayudarlo a comprender cómo administrar los costos asociados AWS Configa la utilización de AWS Control Tower. AWS Control Tower no añade ningún coste adicional.

> **Note**
>
> Si su versión de landing zone es 3.0 o posterior: AWS Control Tower limita el AWS Config registro de los recursos globales, como los usuarios de IAM, los grupos, las funciones y las políticas administradas por los clientes, únicamente a su región de origen. Por lo tanto, es posible que parte de la información de esta sección no se aplique a tu landing zone.

AWS Config está diseñado para registrar cada cambio en cada recurso, en cada región en la que opera una cuenta, como un elemento de configuración (CI). AWS Config le factura por cada elemento de configuración que genere.

¿Cómo AWS Config funciona

AWS Config registra los recursos de cada región, por separado. Algunos recursos globales, como las funciones de IAM, se registran una vez por región. Por ejemplo, si crea un nuevo rol de IAM en una cuenta inscrita que opera en cinco regiones, AWS Config generará cinco IC, uno para cada región. Otros recursos globales, como las zonas alojadas en Route 53, se registran solo una vez en todas las regiones. Por ejemplo, si crea una nueva zona alojada de Route 53 en una cuenta inscrita, AWS Config genera un CI, independientemente del número de regiones seleccionadas para esa cuenta. Para obtener una lista que le ayude a distinguir estos tipos de recursos, consulteEl mismo recurso se graba varias veces.

> **Note**
>
> Cuando AWS Control Tower trabaja con AWS Config, una región puede estar gobernada por AWS Control Tower o no estar gobernada y, AWS Config aun así, registra los cambios si la cuenta opera en esa región.

AWS Config detecta dos tipos de relaciones en los recursos

AWS Config hace una distinción entre las relaciones directas e indirectas entre los recursos. Si se devuelve un recurso en la llamada a la API Describe de otro recurso, esos recursos se registran como una relación directa. Cuando cambias un recurso en relación directa con otro recurso, AWS Config no se crea un CI para ambos recursos.

Por ejemplo, si crea una instancia de Amazon EC2 y la API requiere que cree una interfaz de red, AWS Config considera que la instancia de Amazon EC2 tiene una relación directa con la interfaz de red. Como resultado, AWS Config genera solo un CI.

AWS Config registra los cambios separados para las relaciones de recursos que son relaciones indirectas. Por ejemplo, AWS Config genera dos CI si crea un grupo de seguridad y agrega una instancia de Amazon EC2 asociada que forma parte del grupo de seguridad.

Para obtener más información sobre las relaciones directas e indirectas, consulte ¿Qué es una relación directa e indirecta con respecto a un recurso?

Puede encontrar una lista de relaciones de recursos en la AWS Config documentación.

Vea los datos del AWS Config registrador de las cuentas inscritas

AWS Config está integrado CloudWatch para que pueda ver los AWS Config CI en un panel de control. Para obtener más información, consulta la entrada del blog titulada AWS Config Compatible con CloudWatch las métricas de Amazon.

Mediante programación, para ver AWS Config los datos, puede trabajar con la AWS CLI o utilizar otras AWS herramientas.

Consulte los datos de la AWS Config grabadora en un recurso específico

Puede usar la AWS CLI para recuperar una lista de los cambios más recientes de un recurso.

Comando de historial de recursos:

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

Para obtener más información, consulte la documentación de la API de `get-config-history`.

Visualice AWS Config los datos con Amazon QuickSight

Puede visualizar y consultar los recursos registrados AWS Config en toda su organización. Para obtener más información, consulte Visualización de AWS Config datos con Amazon Athena y Amazon. QuickSight

Solución de problemas AWS Config en AWS Control Tower

En esta sección se proporciona información sobre algunos problemas que pueden surgir AWS Config al utilizar AWS Control Tower.

AWS Config Costos elevados

Si su flujo de trabajo incluye procesos que crean, actualizan o eliminan recursos con frecuencia, o si gestiona los recursos en grandes cantidades, ese flujo de trabajo puede generar un gran número de elementos de configuración. Si ejecuta estos procesos en una cuenta que no es de producción, considere la posibilidad de anular la inscripción de la cuenta. Es posible que tengas que desactivar la AWS Config grabadora de esa cuenta manualmente.

> **Note**
>
> Tras anular la inscripción de la cuenta, AWS Control Tower no podrá aplicar controles de detección ni registrar los eventos de la cuenta, como AWS Config las actividades, para los recursos de esa cuenta.

Para obtener más información, consulte Anular la administración de una cuenta inscrita. Para obtener información sobre cómo desactivar la AWS Config grabadora, consulte Administrar la grabadora de configuración.

El mismo recurso se graba varias veces

Compruebe si el recurso es un recurso global. En el caso de las zonas de aterrizaje de la Torre de Control de AWS anteriores a la versión 3.0, AWS Config es AWS Config posible que se registren determinados recursos globales una vez por cada región en la que opere. Por ejemplo, si AWS Config está habilitado en ocho regiones, cada rol se graba ocho veces.

Los siguientes recursos se registran una vez para cada región en la que AWS Config se opera:

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Los demás recursos globales se registran solo una vez. Estos son algunos ejemplos de recursos que se registran una vez:

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config no registró un recurso

Algunos recursos tienen relaciones de dependencia con otros recursos. Estas relaciones pueden ser directas o indirectas. Puedes encontrar una lista de relaciones indirectas obsoletas en las AWS Config Preguntas frecuentes.

Eventos del ciclo de vida en AWS Control Tower

Algunos eventos registrados por AWS Control Tower son eventos del ciclo de vida. El propósito de un evento del ciclo de vida es marcar la finalización de determinadas acciones de la Torre de Control de AWS que cambian el estado de los recursos. Los eventos del ciclo de vida se aplican a los recursos que AWS Control Tower crea o administra, como las unidades organizativas (OU), las cuentas y los controles.

Características de los eventos del ciclo de vida de AWS Control Tower

- En cada evento del ciclo de vida, el registro de eventos muestra si la acción de Control Tower de origen se completó correctamente o falló.
- AWS CloudTrail registra automáticamente cada evento del ciclo de vida como un evento de AWS servicio ajeno a la API. Para obtener más información, consulte la Guía del AWS CloudTrail usuario.
- Cada evento del ciclo de vida también se envía a los servicios Amazon EventBridge y Amazon CloudWatch Events.

Los eventos del ciclo de vida en AWS Control Tower ofrecen dos ventajas principales:

- Como un evento del ciclo de vida registra la finalización de una acción de la Torre de Control de AWS, puede crear una EventBridge regla de Amazon o una regla de Amazon CloudWatch Events que pueda activar los siguientes pasos de su flujo de trabajo de automatización, en función del estado del evento del ciclo de vida.
- Los registros proporcionan detalles adicionales para ayudar a los administradores y auditores a revisar ciertos tipos de actividad en las organizaciones.

Cómo funcionan los eventos del ciclo de vida

AWS Control Tower se basa en varios servicios para implementar sus acciones. Por lo tanto, cada evento del ciclo de vida se registra solo después de completar una serie de acciones. Por ejemplo,

cuando habilita un control en una unidad organizativa, AWS Control Tower lanza una serie de subpasos que implementan la solicitud. El resultado final de toda la serie de pasos secundarios se registra en el registro como el estado del evento del ciclo de vida.

- Si todos los pasos secundarios subyacentes se han completado correctamente, el estado del evento del ciclo de vida se registra como Succeeded (Correcto).
- Si alguno de los pasos secundarios subyacentes no se ha completado correctamente, el estado del evento del ciclo de vida se registra como Failed (Error).

Cada evento del ciclo de vida incluye una marca de tiempo registrada que muestra cuándo se inició la acción de AWS Control Tower y otra marca de tiempo que muestra cuándo se completó el evento del ciclo de vida, lo que marca el éxito o el fracaso.

Visualización de eventos del ciclo de vida en Control Tower

Puede ver los eventos del ciclo de vida en la página Actividades del panel de control de AWS Control Tower.

- Para navegar a la página Activities (Actividades), seleccione Activities (Actividades) en el panel de navegación izquierdo.
- Para obtener más detalles acerca de un evento específico, seleccione el evento y, a continuación, haga clic en el botón View details (Ver detalles) en la parte superior derecha.

Para obtener más información sobre cómo integrar los eventos del ciclo de vida de la Torre de Control de AWS en sus flujos de trabajo, consulte esta entrada del blog, Uso de los eventos del ciclo de vida para realizar un seguimiento de las acciones de la Torre de Control de AWS y activar flujos de trabajo automatizados.

Comportamiento esperado CreateManagedAccount y eventos UpdateManagedAccount del ciclo de vida

Cuando crea una cuenta o inscribe una cuenta en AWS Control Tower, esas dos acciones utilizan la misma API interna. Si se produce un error durante el proceso, suele producirse después de crear la cuenta, pero no está completamente aprovisionada. Cuando vuelva a intentar crear la cuenta después del error o cuando intente actualizar el producto aprovisionado, AWS Control Tower comprobará que la cuenta ya existe.

Como la cuenta existe, AWS Control Tower registra el evento del `UpdateManagedAccount` ciclo de vida en lugar del evento del `CreateManagedAccount` ciclo de vida al final de la solicitud de reintento. Es posible que esperara ver otro `CreateManagedAccount` evento debido al error. Sin embargo, el evento `UpdateManagedAccount` del ciclo de vida es el comportamiento esperado y deseado.

Si planea crear o inscribir cuentas en AWS Control Tower mediante métodos automatizados, programe la función Lambda para que busque eventos del ciclo de vida y eventos UpdateManagedAccountdel ciclo de CreateManagedAccountvida.

Nombres de eventos del ciclo de vida

Cada evento del ciclo de vida recibe un nombre que corresponde a la acción originaria de la Torre de Control de AWS, que también registra AWS CloudTrail. Así, por ejemplo, se denomina un evento del ciclo de vida originado por el `CreateManagedAccount` CloudTrail evento de la Torre de Control de AWS`CreateManagedAccount`.

Cada nombre de la lista siguiente es un enlace a un ejemplo del detalle registrado en formato `JSON`. Los detalles adicionales que se muestran en estos ejemplos provienen de los registros de CloudWatch eventos de Amazon.

Aunque `JSON` no admite comentarios, se han añadido algunos comentarios a los ejemplos con fines explicativos. Los comentarios van precedidos por "//" y aparecen en el lado derecho de los ejemplos.

En estos ejemplos, se ocultan algunos nombres de cuentas y de organizaciones. Un `accountId` es siempre una secuencia de 12 números, que se ha sustituido por "xxxxxxxxxxxx" en los ejemplos. Un `organizationalUnitID` es una cadena única de letras y números. Su forma se conserva en los ejemplos.

- `CreateManagedAccount`: El registro registra si AWS Control Tower completó correctamente todas las acciones para crear y aprovisionar una nueva cuenta mediante Account Factory.
- `UpdateManagedAccount`: El registro registra si AWS Control Tower completó correctamente todas las acciones para actualizar un producto aprovisionado que está asociado a una cuenta que usted creó anteriormente mediante Account Factory.
- `EnableGuardrail`: El registro registra si la Torre de Control de AWS ha completado correctamente todas las acciones para permitir el control de una unidad organizativa creada por la Torre de Control de AWS.

- `DisableGuardrail`: El registro registra si la Torre de Control de AWS completó correctamente todas las acciones para deshabilitar un control en una unidad organizativa creada por la Torre de Control de AWS.
- `SetupLandingZone`: El registro registra si AWS Control Tower completó correctamente todas las acciones para configurar una landing zone.
- `UpdateLandingZone`: El registro registra si AWS Control Tower completó correctamente todas las acciones para actualizar su landing zone actual.
- `RegisterOrganizationalUnit`: El registro registra si AWS Control Tower completó correctamente todas las acciones para habilitar sus funciones de gobierno en una unidad organizativa.
- `DeregisterOrganizationalUnit`: El registro registra si AWS Control Tower completó correctamente todas las acciones para deshabilitar sus funciones de gobierno en una unidad organizativa.
- `PrecheckOrganizationalUnit`: El registro registra si la Torre de Control de AWS detectó algún recurso que pudiera impedir que la operación de gobierno de Extend se completara correctamente.

En las siguientes secciones se proporciona una lista de los eventos del ciclo de vida de la Torre de Control de AWS, con ejemplos de los detalles registrados para cada tipo de evento del ciclo de vida.

`CreateManagedAccount`

Este evento del ciclo de vida registra si AWS Control Tower creó y aprovisionó correctamente una nueva cuenta mediante Account Factory. Este evento corresponde al evento de la Torre `CreateManagedAccount` CloudTrail de Control de AWS. El registro de eventos del ciclo de vida incluye el `accountName` y `accountId` de la cuenta recién creada y el `organizationalUnitName` y `organizationalUnitId` de la OU en la que se ha colocado la cuenta.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                  // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                             // Format: yyyy-MM-
dd'T'hh:mm:ssZ
```

```
    "region": "us-east-1",                                          // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                        // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

UpdateManagedAccount

Este evento del ciclo de vida registra si AWS Control Tower actualizó correctamente el producto aprovisionado asociado a una cuenta que se creó anteriormente mediante Account Factory. Este evento corresponde al evento de la Torre `UpdateManagedAccount` CloudTrail de Control de AWS.

El registro de eventos del ciclo de vida incluye el `accountName` y `accountId` de la cuenta asociada y el `organizationalUnitName` y `organizationalUnitId` de la OU en la que se ha colocado la cuenta actualizada.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"624281831893"
                    },
                "state":"SUCCEEDED",
```

```
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

EnableGuardrail

Este evento del ciclo de vida registra si la Torre de Control de AWS habilitó correctamente un control en una unidad organizativa gestionada por la Torre de Control de AWS. Este evento corresponde al evento de la Torre `EnableGuardrail` CloudTrail de Control de AWS. El registro de eventos del ciclo `guardrailBehavior` de vida incluye las direcciones y direcciones del control `organizationalUnitName` y `organizationalUnitId` de la unidad organizativa en las que está activado el control. `guardrailId`

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                    // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                             // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
```

```
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
        }
    }
}
```

DisableGuardrail

Este evento del ciclo de vida registra si la Torre de Control de AWS ha desactivado correctamente un control en una unidad organizativa gestionada por la Torre de Control de AWS. Este evento corresponde al evento de la Torre `DisableGuardrail` CloudTrail de Control de AWS. El registro de eventos del ciclo `guardrailBehavior` de vida incluye las direcciones `guardrailId` y direcciones del control `organizationalUnitName` y `organizationalUnitId` de la unidad organizativa en las que el control está desactivado.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
```

```
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully disabled a guardrail on an
organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
               }
            }
        }
    }
```

SetupLandingZone

Este evento del ciclo de vida registra si AWS Control Tower configuró correctamente una landing zone. Este evento corresponde al evento de la Torre `SetupLandingZone` CloudTrail de Control

de AWS. El registro de eventos del ciclo de vida incluye el`rootOrganizationalId`, que es el ID de la organización que AWS Control Tower crea a partir de la cuenta de administración. La entrada del registro también incluye la `organizationalUnitName` y `organizationalUnitId` para cada una de las unidades organizativas `accountName` y la y `accountId` para cada cuenta que se crean cuando AWS Control Tower configura la landing zone.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                         // Management-account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "SetupLandingZone",
        "awsRegion": "us-east-1",                                // AWS Control Tower
 home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                        // This value is
 generated by CloudTrail.
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "setupLandingZoneStatus": {
                "state": "SUCCEEDED",                             // Status of entire
 lifecycle operation.
                "message": "AWS Control Tower successfully set up a new landing zone.",
```

```
                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                          // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
 name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",           // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Custom OU ID.
                  },
                ],
               "accounts": [                                      // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

UpdateLandingZone

Este evento del ciclo de vida registra si AWS Control Tower actualizó correctamente su landing zone actual. Este evento corresponde al evento de la Torre `UpdateLandingZone` CloudTrail de Control de AWS. El registro de eventos del ciclo de vida incluye el`rootOrganizationalId`, que es el ID de la organización (actualizada) gobernada por AWS Control Tower. La entrada del registro también incluye la `organizationalUnitName` y `organizationalUnitId` para cada una de las unidades organizativas `accountName` y la y `accountId` para cada cuenta que se creó anteriormente, cuando AWS Control Tower configuró originalmente la landing zone.

```
{
```

```
   "version": "0",
   "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
   "detail-type": "AWS Service Event via CloudTrail",
   "source": "aws.controltower",
   "account": "XXXXXXXXXXXX",                                   // Management account
ID.
   "time": "2018-08-30T21:42:18Z",                              // Event time from
CloudTrail.
   "region": "us-east-1",                                       // Management account
CloudTrail region.
   "resources": [ ],
   "detail": {
       "eventVersion": "1.05",
       "userIdentity": {
           "accountId": "XXXXXXXXXXXX",                         // Management account
ID.
           "invokedBy": "AWS Internal"
       },
       "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
       "eventSource": "controltower.amazonaws.com",
       "eventName": "UpdateLandingZone",
       "awsRegion": "us-east-1",                                // AWS Control Tower
home region.
       "sourceIPAddress": "AWS Internal",
       "userAgent": "AWS Internal",
       "eventID": "CloudTrail_event_ID",                        // This value is
generated by CloudTrail.

       "readOnly": false,
       "eventType": "AwsServiceEvent",
       "serviceEventDetails": {
           "updateLandingZoneStatus": {
               "state": "SUCCEEDED",                            // Status of entire
operation.
               "message": "AWS Control Tower successfully updated a landing zone.",


               "rootOrganizationalId" : "r-1234",
               "organizationalUnits" : [                         // Use a list.
                 {
                   "organizationalUnitName": "Security",             // Security OU
name.
                   "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
```

```
                },
                {
                  "organizationalUnitName": "Custom",            // Custom OU name.
                  "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                },
              ],
             "accounts": [                                       // All created
 accounts are here. Use a list of "account" objects.

                {
                  "accountName": "Audit",
                  "accountId": "XXXXXXXXXXXX"
                },
                {
                  "accountName": "Log archive",
                  "accountId": "XXXXXXXXXX"
                }
            ],
            "requestedTimestamp": "2018-08-30T21:42:18Z",
            "completedTimestamp": "2018-08-30T21:42:18Z"
          }
        }
    }
}
```

RegisterOrganizationalUnit

Este evento del ciclo de vida registra si AWS Control Tower habilitó correctamente sus funciones de gobierno en una unidad organizativa. Este evento corresponde al evento de la Torre `RegisterOrganizationalUnit` CloudTrail de Control de AWS. El registro de eventos del ciclo de vida incluye la `organizationalUnitName` `organizationalUnitId` parte final de la unidad organizativa que AWS Control Tower ha incorporado bajo su control.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
```

```
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

DeregisterOrganizationalUnit

Este evento del ciclo de vida registra si AWS Control Tower ha desactivado correctamente sus funciones de gobierno en una unidad organizativa. Este evento corresponde al evento de la Torre `DeregisterOrganizationalUnit` CloudTrail de Control de AWS. El registro de eventos del ciclo `organizationalUnitId` de vida incluye la dirección `organizationalUnitName` y la unidad organizativa en la que AWS Control Tower ha desactivado sus funciones de gobierno.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully deregistered an
organizational unit, and enabled mandatory guardrails on the new organizational
unit.",
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",                   // Foundational
OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"          // Foundational
OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
        }
    }
```

PrecheckOrganizationalUnit

Este evento del ciclo de vida registra si AWS Control Tower realizó correctamente las comprobaciones previas en una OU. Este evento corresponde al evento de la Torre `PrecheckOrganizationalUnit` CloudTrail de Control de AWS. El registro de eventos del ciclo de vida contiene un campo para `IdName`, y `failedPrechecks` valores para cada recurso en el que AWS Control Tower haya realizado comprobaciones previas durante el proceso de registro de la OU.

El registro de eventos también contiene información sobre las cuentas anidadas en las que se realizaron las comprobaciones previas, incluidos los campos `accountNameaccountId`, y. `failedPrechecks`

Si el `failedPrechecks` valor está vacío, significa que todas las comprobaciones previas de ese recurso se han realizado correctamente.

- Este evento se emite solo si se produce un error en la comprobación previa.
- Este evento no se emite si se registra una unidad organizativa vacía.

Ejemplo de evento:


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
```

```
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
        },
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
 pre-check failures. Go to the OU details page to download a list of failed pre-checks
 for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
  },
  "eventCategory": "Management"
```

```
}
```

Uso de las notificaciones de AWS usuario con AWS Control Tower

Puedes usar las notificacionesAWS de usuario para configurar canales de entrega para recibir notificaciones sobre AWS Control Tower eventos. Recibirá una notificación cuando un evento coincida con una regla que especifique. Puedes recibir notificaciones de eventos a través de varios canales, como el correo electrónico, las notificaciones de AWS Chatbotchat o las notificaciones push de la aplicación móvil de laAWS consola. También puede ver las notificaciones en el Centro de notificaciones de la consola.

AWS Las notificaciones de usuario admiten la agregación, lo que puede reducir la cantidad de notificaciones que recibes durante eventos específicos. Las notificaciones también están visibles en el Centro de notificaciones de la consola.

Entre las ventajas de suscribirse a las notificaciones a través de las notificaciones de AWS usuario, en lugar de las notificaciones, se EventBridge incluyen las siguientes:

- Una interfaz de usuario (UI) más amigable.
- Integración con la AWS consola, en el área de campana/notificaciones de la barra de navegación global.
- Soporte nativo para notificaciones por correo electrónico, no es necesario configurar Amazon SNS.
- En particular, la compatibilidad con las notificaciones push móviles, exclusiva de las notificaciones AWS de usuario.

Por ejemplo, un tipo de notificación que quizás desee recibir es en caso de que el Security Hub detecte una situación crítica y de alta gravedad. Un fragmento de código en JSON para configurar la suscripción a las notificaciones puede tener el siguiente aspecto:

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
```

```
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

Filtrado de eventos

- Puede filtrar los eventos por servicio y nombre mediante los filtros disponibles en la consola AWS de notificaciones de usuario.
- Puedes filtrar los eventos por propiedades específicas si creas tu propio EventBridge filtro a partir del código JSON.

Ejemplo de AWS Control Tower evento

A continuación se muestra un ejemplo generalizado de un evento para AWS Control Tower.

- Es un EventBridge evento.
- Puedes suscribirte a EventBridge eventos (como este) mediante las notificaciones AWS de usuario.

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
```

```
        "eventSource": "controltower.amazonaws.com",
        "eventName": "<event name>", // one of the 9 event names in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

Explicaciones

Este capítulo contiene procedimientos explicativos que pueden ayudarle a utilizar AWS Control Tower.

Temas

Tutorial: Cómo pasar de ALZ a la Torre de Control de AWS

Muchos AWS clientes han adoptado la solución AWS Landing Zone (ALZ) para configurar un entorno seguro, compatible y con múltiples cuentas AWS . Para reducir la carga que supone gestionar una landing zone, AWS creó el servicio gestionado denominado AWS Control Tower.

No se han programado funciones adicionales para ALZ; solo se trata de un soporte a largo plazo. Por lo tanto, le recomendamos que se traslade al servicio AWS Control Tower desde ALZ. En el blog que se incluye en este capítulo, se explican las diferentes consideraciones que se deben tener en cuenta a este respecto y se explica cómo planificar una migración exitosa de ALZ a AWS Control Tower.

Blog: Migrar la solución AWS Landing Zone a AWS Control Tower

AWS La guía prescriptiva ofrece una documentación más amplia, que incluye los pasos para la transición de ALZ a AWS Control Tower. Básicamente, habilitará la gobernanza de la Torre de Control de AWS en su organización actual que ejecute ALZ, en función de una serie de requisitos previos. Para obtener más información, consulte Transición de la zona de AWS aterrizaje a la Torre de Control de AWS.

Tutorial: Automatice el aprovisionamiento de cuentas en AWS Control Tower mediante las API de Service Catalog

AWS Control Tower está integrada con varios otros AWS servicios, como AWS Service Catalog. Puede usar las API para crear y aprovisionar sus cuentas de miembros en AWS Control Tower.

El vídeo muestra cómo aprovisionar cuentas de forma automática y por lotes, mediante el uso de las AWS Service Catalog API. Para el aprovisionamiento, llamará a la `ProvisionProduct`API desde la interfaz de línea de AWS comandos (CLI) y especificará un archivo JSON que contenga los parámetros de cada cuenta que desee configurar. El vídeo ilustra la instalación y el uso del entorno de desarrollo AWS Cloud9 para realizar este trabajo. Los comandos CLI serían los mismos si usas AWS Cloudshell en lugar de AWS Cloud9.

> **Note**
>
> También puedes adaptar este enfoque para automatizar las actualizaciones de las cuentas, llamando a la `UpdateProvisionedProduct`API de AWS Service Catalog cada cuenta. Puede escribir un script para actualizar las cuentas, una por una.

Como método de automatización completamente diferente, si está familiarizado con Terraform, puede aprovisionar cuentas con AWS Control Tower Account Factory for Terraform (AFT).

Ejemplo de función de administración de automatización

A continuación, se muestra un ejemplo de plantilla que puede utilizar para configurar su función de administración de automatización en la cuenta de administración. Debería configurar este rol en su cuenta de administración para que pueda realizar la automatización con acceso de administrador en las cuentas de destino.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
```

```
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

Ejemplo de función de ejecución de la automatización

Esta es una plantilla de ejemplo que puede usar para configurar su rol de ejecución de automatización. Debería configurar este rol en las cuentas de destino.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
    Type: "Number"
    Description: "Maximum session duration in seconds."
```

```
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

Tras configurar estas funciones, debe llamar a las AWS Service Catalog API para que realicen las tareas automatizadas. Los comandos de la CLI se muestran en el vídeo.

Ejemplo de entrada de aprovisionamiento para la API de Service Catalog

A continuación, se muestra un ejemplo de la información que puede proporcionar a la `ProvisionProduct` API de Service Catalog si la utiliza para aprovisionar cuentas de AWS Control Tower:

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
```

```
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

Para obtener más información, consulte la referencia de API de Service Catalog.

> **Note**
>
> Observe que el formato de la cadena de entrada para el valor de `ManagedOrganizationalUnit` ha cambiado de `OU_NAME` a`OU_NAME (OU_ID)`. En el siguiente vídeo no se menciona este cambio.

Tutorial en vídeo

En este vídeo (6:58) se describe cómo automatizar las implementaciones de cuentas en AWS Control Tower. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo del aprovisionamiento automatizado de cuentas en AWS Control Tower.

Tutorial: Configurar la Torre de Control de AWS sin una VPC

En este tema se explica cómo configurar las cuentas de la Torre de Control de AWS sin una VPC.

Si la carga de trabajo no requiere una VPC, puede hacer lo siguiente:

- Puede eliminar la nube privada virtual (VPC) de la Torre de Control de AWS. Esta VPC se creó al configurar la zona de inicio.
- Puede cambiar la configuración de Account Factory para crear nuevas cuentas de AWS Control Tower sin una VPC asociada.

> **Important**
>
> Si aprovisiona cuentas de Account Factory con la configuración de acceso a Internet de la VPC habilitada, esa configuración de Account Factory anula el control No permitir el acceso a Internet para una instancia de Amazon VPC gestionada por un cliente. Para evitar habilitar el acceso a Internet para las cuentas recién aprovisionadas, debes cambiar la configuración en Account Factory.

Eliminar la VPC de AWS Control Tower

Fuera de la Torre de Control de AWS, cada AWS cliente tiene una VPC predeterminada, que puede ver en la consola Amazon Virtual Private Cloud (Amazon VPC) en https://console.aws.amazon.com/vpc/. Reconocerá la VPC predeterminada, ya que su nombre siempre incluye la palabra (default) al final del nombre.

Al configurar una zona de aterrizaje de AWS Control Tower, AWS Control Tower elimina la VPC AWS predeterminada y crea una nueva VPC predeterminada de AWS Control Tower. La nueva VPC está asociada a su cuenta de administración de AWS Control Tower. En este tema se hace referencia a esa nueva VPC como Control Tower VPC.

Cuando visualice su VPC de la Torre de Control de AWS en la consola de Amazon VPC, no verá la palabra (predeterminada) al final del nombre. Si tiene más de una VPC, debe usar el rango de CIDR asignado para identificar la VPC de AWS Control Tower correcta.

Puede eliminar la VPC de la Torre de Control de AWS, pero si más adelante necesita una VPC en la Torre de Control de AWS, debe crearla usted mismo.

Para eliminar la VPC de AWS Control Tower

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Busque **VPC** o seleccione VPC en las opciones de Service Catalog. A continuación, verá el panel de VPC.
3. En el menú de la izquierda, elija Your VPCs (Sus VPC). A continuación, verá una lista de todas las VPC.
4. Identifique la VPC de la Torre de Control de AWS por su rango de CIDR.
5. Seleccione la VPC; elija Actions (Acciones) y luego elija Delete VPC (Eliminar VPC).

Ya existe una VPC AWS (predeterminada) en cada región para la cuenta de administración de AWS Control Tower. Para seguir las prácticas recomendadas de seguridad, si decide eliminar la VPC de AWS Control Tower, también es mejor eliminar la AWS VPC predeterminada asociada a la cuenta de administración de todas las regiones. AWS Por lo tanto, para proteger la cuenta de administración, elimine la VPC predeterminada de cada región y elimine la VPC creada por Control Tower en su región de origen de AWS Control Tower.

Cree una cuenta en AWS Control Tower sin una VPC

Si sus cargas de trabajo de usuario final no requieren VPC, puede usar este método para configurar cuentas de usuario final en las que no se creen VPC automáticamente.

Desde el panel de control de AWS Control Tower, puede ver y editar los ajustes de configuración de la red. Tras cambiar la configuración para que las cuentas de la Torre de Control de AWS se creen sin una VPC asociada, todas las cuentas nuevas se crean sin una VPC hasta que vuelva a cambiar la configuración.

Para configurar Account Factory para crear cuentas sin VPC

1. Abra un navegador web y diríjase a la consola de la Torre de Control de AWS en https://console.aws.amazon.com/controltower.
2. Selecciona Account Factory en el menú de la izquierda.
3. A continuación, verá la página Account Factory con la sección Configuración de red.
4. Tenga en cuenta la configuración actual si va a restaurarla más adelante.
5. Elija el botón Edit (Editar) en la sección Network Configuration (Configuración de red).

6. En la página Edit account factory network configuration (Editar configuración de red de fábrica de cuentas), vaya a la sección VPC Configuration options for new accounts (Opciones de configuración de VPC para cuentas nuevas).

   Puede seguir la opción 1 o la opción 2, o ambas, para asegurarse de que AWS Control Tower no cree una VPC al aprovisionar una cuenta.

   a. Opción 1: Eliminar las subredes

      - Desactive el conmutador de conmutación de subred accesible a Internet.
      - Establezca el valor Maximum number of private subnets (Número máximo de subredes privadas) en 0.

   b. Opción 2: Eliminar regiones AWS

      - Desactive cada casilla de verificación de la columna Regions for VPC creation (Regiones para la creación de VPC).

7. Seleccione Guardar.

Posibles errores

Tenga en cuenta estos posibles errores que pueden producirse al eliminar su VPC de AWS Control Tower o al volver a configurar Account Factory para crear cuentas sin VPC.

- Es posible que su cuenta de administración actual tenga dependencias o recursos en la VPC de AWS Control Tower, lo que puede provocar un error de eliminación.
- Si deja el CIDR predeterminado en vigor al configurar para lanzar cuentas nuevas sin una VPC, la solicitud produce un error que indica que el CIDR no es válido.

Tutorial: Configurar grupos de seguridad en la Torre de Control de AWS con AWS Firewall Manager

El vídeo muestra cómo utilizar el servicio AWS Firewall Manager para mejorar la seguridad de la red para AWS Control Tower. Puede designar una cuenta de administrador de seguridad habilitada para configurar grupos de seguridad. Verá cómo puede configurar las políticas de seguridad y hacer cumplir las reglas de seguridad para sus organizaciones de la Torre de Control de AWS, y cómo puede corregir los recursos no conformes mediante la aplicación automática de las políticas. Puede

ver los grupos de seguridad que están en vigor para cada cuenta y recurso (como una instancia de Amazon EC2) de su organización.

Puede crear sus propias políticas de firewall o suscribirse a reglas de proveedores de confianza.

Configurar grupos de seguridad con AWS Firewall Manager

Este vídeo (8:02) describe cómo configurar una mejor seguridad de la infraestructura de red para sus recursos y cargas de trabajo en la Torre de Control de AWS. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo de la configuración del firewall en AWS Control Tower.

Para obtener más información, consulte la documentación sobre cómo configurar el AWS WAF.

Tutorial: Retirar del servicio una zona de aterrizaje de una Torre de Control de AWS

AWS Control Tower le permite configurar y gobernar AWS entornos seguros de múltiples cuentas, conocidos como zonas de aterrizaje. El proceso de limpieza de todos los recursos asignados por la Torre de Control de AWS se denomina desmantelamiento de una landing zone.

Si ya no desea utilizar la Torre de Control de AWS, la herramienta de desmantelamiento automatizada limpia los recursos asignados por la Torre de Control de AWS. Para iniciar el proceso de desmantelamiento automatizado, vaya a la página de configuración de la zona de aterrizaje, seleccione la pestaña de desmantelamiento y elija Desmantelar zona de aterrizaje.

Para obtener una lista de las acciones realizadas durante el desmantelamiento, consulte. Descripción general del proceso de desmantelamiento

> **Warning**
>
> Eliminar manualmente todos los recursos de la Torre de Control de AWS no es lo mismo que retirarlos. No te permitirá configurar una nueva landing zone.

El proceso de desmantelamiento AWS Organizations no modifica sus datos ni los existentes de las siguientes maneras.

- AWS Control Tower no elimina los datos, solo elimina partes de la zona de inicio que creó.
- Una vez finalizado el proceso de desmantelamiento, quedan algunos artefactos de recursos, como los buckets de Amazon S3 y los grupos de CloudWatch registros de Amazon Logs. Estos recursos se deben eliminar manualmente antes de configurar otra zona de inicio y para evitar posibles costos asociados al mantenimiento de determinados recursos.
- No puede utilizar el desmantelamiento automático para eliminar una zona de aterrizaje parcialmente configurada. Si el proceso de configuración de la zona de aterrizaje falla, debe resolver el estado de error y configurarlo todo el camino para que sea posible el desmantelamiento automático, o debe eliminar manualmente los recursos individualmente.

La retirada de una zona de inicio es un proceso con consecuencias importantes y no se puede deshacer. En las siguientes secciones se describen las medidas de desmantelamiento adoptadas por la Torre de Control de AWS y los artefactos que quedan tras el desmantelamiento.

> **Important**
>
> Le recomendamos encarecidamente que realice este proceso de retirada solo si tiene intención de dejar de utilizar su zona de inicio. No es posible volver a crear la zona de inicio existente después de que la haya retirado.

Descripción general del proceso de desmantelamiento

Cuando solicita el desmantelamiento de su landing zone, AWS Control Tower realiza las siguientes acciones.

- Desactiva todos los controles de detección activados en la landing zone. AWS Control Tower elimina los AWS CloudFormation recursos que respaldan el control.
- Desactiva cada control preventivo al eliminar las políticas de control de servicios (SCP). AWS Organizations Si una política está vacía (lo que debería ocurrir después de eliminar todos los SCP gestionados por AWS Control Tower), AWS Control Tower desconecta y elimina la política por completo.
- Elimina todos los planos implementados como. AWS CloudFormation StackSets
- Elimina todos los planos desplegados como CloudFormation pilas en todas las regiones.
- Para cada cuenta aprovisionada, AWS Control Tower realiza las siguientes acciones durante el proceso de desmantelamiento.

  - Elimina los registros de cada cuenta de Account Factory.
  - Revoca los permisos de AWS Control Tower para la cuenta eliminando el rol de IAM que creó AWS Control Tower (a menos que se le hayan agregado políticas adicionales) y vuelve a crear el rol de IAM estándar`OrganizationsFullAccessRole`.
  - Elimina los registros de la cuenta de. AWS Service Catalog
  - Elimina el producto de Account Factory y la cartera de AWS Service Catalog.
- Elimina los planos de las cuentas compartidas (archivo de auditoría y registro).
- Revoca los permisos de la Torre de Control de AWS de las cuentas compartidas eliminando la función de IAM que creó la Torre de Control de AWS (a menos que se le hayan agregado políticas adicionales) y vuelve a crear la `OrganizationsFullAccessRole` función de IAM.
- Elimina los registros relacionados con las cuentas compartidas.
- Elimina los registros relacionados con las unidades organizativas creadas por el cliente.
- Elimina los registros internos que identifican la región de origen.

> **Note**
>
> Después de la retirada, es posible que desee quitar el proyecto de la VPC de Account Factory (`BP_ACCOUNT_FACTORY_VPC`) para limpiar las rutas y las gateways NAT, si la VPC no estaba vacía.

Los recursos no se eliminaron durante el desmantelamiento

El desmantelamiento de una landing zone no anula por completo el proceso de configuración de la AWS Control Tower. Quedan algunos recursos, que pueden eliminarse manualmente.

AWS Organizations

Para los clientes sin AWS Organizations organizaciones existentes, AWS Control Tower configura una organización con dos unidades organizativas (OU), denominadas Security y Sandbox. Cuando se retira la zona de inicio, se mantiene la jerarquía de la organización, de la siguiente manera:

- Las unidades organizativas (OU) que creó desde la consola de AWS Control Tower no se eliminan.
- Las unidades organizativas de seguridad y Sandbox no se eliminan.
- La organización no se elimina de AWS Organizations.

- No se mueve ni elimina ninguna cuenta AWS Organizations (compartida, aprovisionada o de gestión).

AWS IAM Identity Center (SSO)

Para los clientes que no tienen un directorio de centros de identidad de IAM existente, AWS Control Tower configura el centro de identidades de IAM y configura un directorio inicial. Al desmantelar su landing zone, AWS Control Tower no realiza cambios en el IAM Identity Center. Si es necesario, puede eliminar manualmente la información del centro de identidad de IAM almacenada en su cuenta de administración. En particular, estas zonas no se modifican mediante la retirada:

- Los usuarios creados con Account Factory no se quitan.
- Los grupos creados mediante la configuración de la Torre de Control de AWS no se eliminan.
- Los conjuntos de permisos creados por AWS Control Tower no se eliminan.
- No se eliminan las asociaciones entre las cuentas de AWS y los conjuntos de permisos del IAM Identity Center.
- Los directorios del IAM Identity Center no se modifican.

Roles

Durante la configuración, AWS Control Tower le crea determinadas funciones si utiliza la consola, o le pide que las cree si configura su landing zone a través de las API. Al desmantelar tu landing zone, no se eliminan las siguientes funciones:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Buckets de Amazon S3

Durante la configuración, AWS Control Tower crea depósitos en la cuenta de registro para el registro y para el acceso al registro. Al retirar la zona de inicio, no se quitan los siguientes recursos:

- No se quitan los buckets de S3 de registro y acceso de registro en la cuenta de registro.
- El contenido de los buckets de acceso de registro y registro no se elimina.

Cuentas compartidas

Durante la configuración de la Torre de Control de AWS, se crean dos cuentas compartidas (Audit y Log Archive) en la unidad organizativa de seguridad. Al retirar la zona de inicio:

- Las cuentas compartidas que se crearon durante la configuración de la Torre de Control de AWS no se cierran.
- La función `OrganizationAccountAccessRole` de IAM se recrea para alinearla con la configuración estándar AWS Organizations .
- Se quita el rol de `AWSControlTowerExecution`.

Cuentas aprovisionadas

Los clientes de AWS Control Tower pueden usar la fábrica de cuentas para crear nuevas cuentas de AWS. Al retirar la zona de inicio:

- Las cuentas aprovisionadas que creó con Account Factory no están cerradas.
- Los productos aprovisionados no AWS Service Catalog se eliminan. Si los eliminas cancelándolos, sus cuentas se trasladarán a la unidad organizativa raíz.
- La VPC que creó AWS Control Tower no se elimina y el conjunto de AWS CloudFormation pilas asociado (`BP_ACCOUNT_FACTORY_VPC`) no se elimina.
- La función de `OrganizationAccountAccessRole` IAM se recrea para alinearla con la configuración estándar. AWS Organizations
- Se quita el rol de `AWSControlTowerExecution`.

CloudWatch Registros: Grupo de registros

Se crea un grupo de CloudWatch registros`aws-controltower/CloudTrailLogs`,, como parte del esquema denominado`AWSControlTowerBP-BASELINE-CLOUDTRAIL-MANAGEMENT`. Este grupo de registro no se quita. En su lugar, se elimina el proyecto y se conservan los recursos.

- Este grupo de registro debe eliminarse manualmente antes de configurar otra zona de inicio.

> **Note**
>
> Los clientes de landing zone 3.0 y versiones posteriores no necesitan eliminar los CloudTrail CloudTrail registros y las funciones de registro de sus cuentas individuales inscritas, ya que

estos se crean únicamente en la cuenta de administración, para el seguimiento a nivel de la organización.
A partir de la versión 3.2 de landing zone, AWS Control Tower crea una EventBridge regla de Amazon llamada`AWSControlTowerManagedRule`. Esta regla se crea en la cuenta de cada miembro, para todas las regiones gobernadas. La regla no se elimina automáticamente durante el desmantelamiento, por lo que debes eliminarla manualmente de las cuentas compartidas y de los miembros de todas las regiones gobernadas antes de poder configurar una landing zone en una nueva región.

Los procedimientos para eliminar los recursos de la Torre de Control de AWS se detallan enAdministre los recursos de AWS Control Tower.

Administre los recursos de AWS Control Tower

Este documento proporciona instrucciones sobre cómo eliminar los recursos de la Torre de Control de AWS de forma individual, como parte de las tareas administrativas y de mantenimiento habituales. Los procedimientos descritos en este capítulo están destinados únicamente a eliminar recursos individuales, o algunos recursos, cuando sea necesario. No es lo mismo que desmantelar tu landing zone.

Hay dos tipos de tareas que pueden requerir la eliminación de recursos:

- Para eliminar recursos a medida que administra su zona de inicio en situaciones normales.
- Para limpiar los recursos que quedan tras el desmantelamiento automatizado.

Warning

Eliminar recursos manualmente no te permitirá configurar una nueva landing zone. No es lo mismo que desmantelar. Si tiene intención de desmantelar su zona de aterrizaje de la AWS Control Tower, siga las instrucciones que se indican Tutorial: Retirar del servicio una zona de aterrizaje de una Torre de Control de AWS antes de realizar cualquier acción que se describe en este capítulo. Las instrucciones de este capítulo pueden ayudarle a limpiar los recursos que quedan una vez finalizado el desmantelamiento automatizado. Incluso si eliminas todos los recursos de la zona de aterrizaje manualmente, no es lo mismo que desmantelar la zona de aterrizaje y puedes incurrir en cargos inesperados.

Si necesita eliminar una cuenta de AWS Control Tower, consulte las siguientes secciones para cerrar una cuenta:

- Anule la administración de una cuenta
- Cerrar una cuenta creada en Account Factory

¿Necesito retirarme del servicio en lugar de eliminarlo?

Si ya no tiene intención de utilizar AWS Control Tower para su empresa o si necesita una redistribución importante de los recursos de su organización, puede que desee retirar los recursos creados al configurar inicialmente su landing zone.

- Una vez finalizado el proceso de desmantelamiento, quedan algunos artefactos de recursos, como los buckets de Amazon S3 y los grupos de CloudWatch registros de Amazon Logs.
- Debes limpiar los recursos restantes de tus cuentas manualmente antes de configurar otra landing zone y evitar la posibilidad de cargos inesperados. Para obtener más información, consulte Los recursos no se eliminaron durante el desmantelamiento.

> **Warning**
>
> Te recomendamos encarecidamente que realices un proceso de desmantelamiento solo si pretendes dejar de usar tu landing zone. Este proceso no se puede deshacer.

Acerca de la eliminación de los recursos de AWS Control Tower

Los procedimientos individuales de este capítulo lo guían por los métodos manuales para eliminar los recursos de la Torre de Control de AWS. Puedes seguir estos procedimientos cuando necesites eliminar un recurso específico de tu landing zone.

Antes de realizar estos procedimientos, a menos que se indique lo contrario, debe iniciar sesión AWS Management Console en la región de origen de su zona de aterrizaje y debe iniciar sesión como usuario de IAM o usuario en el Centro de identidades de IAM con permisos administrativos para la cuenta de administración que contiene su zona de aterrizaje.

> **Warning**
>
> Se trata de acciones destructivas que pueden provocar una desviación de la gobernanza en la configuración de la Torre de Control de AWS. No se pueden deshacer.

Temas

Eliminación de SCP

AWS Control Tower utiliza políticas de control de servicios (SCP) para sus controles. Este procedimiento explica cómo eliminar los SCP relacionados específicamente con AWS Control Tower.

Para eliminar los SCP AWS Organizations

1. Abra la consola de Organizations en https://console.aws.amazon.com/organizations/.
2. Abra la pestaña Policies (Políticas), busque las políticas de control de servicios (SCP) que tengan el prefijo aws-guardrails- y realice lo siguiente para cada SCP.
    a. Separe la SCP de la OU asociada.
    b. Elimine la SCP.

Eliminar StackSets y apilar

AWS Control Tower utiliza StackSets y apila para implementar controles Reglas de AWS Config relacionados con los de su landing zone. Los siguientes procedimientos explican cómo eliminar estos recursos específicos.

Para eliminar AWS CloudFormation StackSets

1. Abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.

2. En el menú de navegación de la izquierda, selecciona StackSets.
3. Para cada uno StackSet con el prefijo AWSControlTower, haga lo siguiente. Si tienes varias cuentas en una StackSet, esto puede llevar algún tiempo.

    a. Elige la específica StackSet de la tabla del panel de control. Esto abre la página de propiedades correspondiente StackSet.

    b. En la parte inferior de la página, en la tabla Stacks, haz un registro de los AWS identificadores de todas las cuentas de la tabla. Copie la lista de todas las cuentas.

    c. En Acciones, selecciona Eliminar pilas de. StackSet

    d. En Establecer opciones de despliegue, en Ubicaciones de despliegue, selecciona Implementar pilas en cuentas.

    e. En el campo de texto, introduce los ID de AWS cuenta que registraste en el paso 3.b, separados por comas. Por ejemplo: *123456789012*, *098765431098*, etc.

    f. En Specify regions (Especificar regiones), elija Add all (Añadir todo), deje el resto de los parámetros de la página establecidos en sus valores predeterminados y elija Next (Siguiente).

    g. En la página Review (Revisar), revise las opciones y seleccione Delete stacks (Eliminar pilas).

    h. En la página de StackSet propiedades, puede volver a iniciar este procedimiento para la otra. StackSets

4. El proceso finaliza cuando los registros de la tabla Stacks de las distintas páginas de StackSets propiedades están vacíos.
5. Cuando los registros de la tabla Stacks estén vacíos, seleccione Eliminar. StackSet

Para eliminar pilas AWS CloudFormation

1. Abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. En el panel de control de Stacks, busca todas las pilas con el prefijo. AWSControlTower
3. Para cada pila de la tabla, realice lo siguiente:

    a. Active la casilla situada junto al nombre de la pila.

    b. En el menú Actions (Acciones), elija Delete Stack (Eliminar la pila).

    c. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa y elija Yes, Delete (Sí, eliminar).

Eliminar buckets de Amazon S3 de la cuenta de Log Archive

Los siguientes procedimientos le explican cómo iniciar sesión en la cuenta del archivo de registros como usuario del IAM Identity Center del AWSControlTowerExecutiongrupo y, a continuación, eliminar los buckets de Amazon S3 de su cuenta de archivo de registros.

Para iniciar sesión en su cuenta del archivo de registro con los permisos adecuados

1. Abra la consola de Organizations en https://console.aws.amazon.com/organizations/.
2. En la pestaña Accounts (Cuentas), busque la cuenta Log archive (Archivo de registro).
3. En el panel derecho que se abre, realice un registro del número de la cuenta del archivo de registro.
4. En la barra de navegación, elija el nombre de la cuenta para abrir el menú de la misma.
5. Elija Switch Role.
6. En la página que se abre, proporcione el número de la cuenta del archivo de registro en Account (Cuenta).
7. En Rol, introduzca. AWSControlTowerExecution
8. Display Name (Nombre de visualización) se rellena con texto.
9. Elija su Color favorito.
10. Elija Switch Role.

Para eliminar buckets de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Busque nombres que contengan aws-controltower.
3. Para cada bucket de la tabla, realice lo siguiente:
    a. Active la casilla del bucket de la tabla.
    b. Elija Eliminar.
    c. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa, escriba el nombre del bucket que desea confirmar y, a continuación, elija Confirm (Confirmar).

Eliminar una cartera y un producto de Account Factory

El siguiente procedimiento le explica cómo iniciar sesión como usuario del IAM Identity Center en el AWSServiceCatalogAdminsgrupo y, a continuación, limpiar su cartera y sus productos de Account Factory.

Para iniciar sesión en su cuenta de administración con los permisos adecuados

1. Vaya a la URL del portal de usuarios en *directory-id*.awsapps.com/start
2. En AWS Cuenta, busca la cuenta de administración.
3. Desde AWSServiceCatalogAdminFullAccess, selecciona la consola de administración para iniciar sesión con este rol. AWS Management Console

Para limpiar Account Factory

1. Abra la consola de Service Catalog en https://console.aws.amazon.com/servicecatalog/.
2. En el panel de navegación izquierdo, elija Portfolios list (Lista de carteras).
3. En la tabla Portafolios locales, busque un portafolio denominado AWS Control Tower Account Factory Portfolio.
4. Elija el nombre de esa cartera para ir a su página de detalles.
5. Amplíe la sección Restricciones de la página y elija el botón de radio para la restricción con el nombre del producto AWS Control Tower Account Factory.
6. Elija REMOVE CONSTRAINTS (QUITAR RESTRICCIONES).
7. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa y, a continuación, elija CONTINUE (CONTINUAR).
8. En la sección Productos de la página, selecciona el botón de radio del producto denominado AWS Control Tower Account Factory.
9. Elija REMOVE PRODUCT (QUITAR PRODUCTO).
10. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa y, a continuación, elija CONTINUE (CONTINUAR).
11. Amplíe la sección Users, Groups, and Roles (Usuarios, grupos y roles) de la página y active las casillas de todos los registros en esta tabla.
12. Elija REMOVE USERS, GROUP OR ROLE (QUITAR USUARIOS, GRUPO O ROL).
13. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa y, a continuación, elija CONTINUE (CONTINUAR).

14. En el panel de navegación izquierdo, elija Portfolios list (Lista de carteras).
15. En la tabla Portafolios locales, busque un portafolio denominado AWS Control Tower Account Factory Portfolio.
16. Elija el botón de opción para esa cartera y, a continuación, elija DELETE PORTFOLIO (ELIMINAR CARTERA).
17. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa y, a continuación, elija CONTINUE (CONTINUAR).
18. En el menú de navegación izquierdo, elija Product list (Lista de productos).
19. En la página de productos de administración, busque el producto denominado AWS Control Tower Account Factory.
20. Elija el producto para abrir la página Admin product details (Detalles del producto de administrador).
21. En Actions (Acciones), elija Delete product (Eliminar producto).
22. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa y, a continuación, elija CONTINUE (CONTINUAR).

Elimine las funciones y políticas de AWS Control Tower

Estos procedimientos le explican cómo limpiar las funciones y políticas que AWS Control Tower creó cuando se creó su landing zone o posteriormente.

Para eliminar el rol del Centro AWSServiceCatalogEndUserAccess de Identidad de IAM

1. Abra la AWS IAM Identity Center consola en https://console.aws.amazon.com/singlesignon/.
2. Cambie su AWS región a su región de origen, que es la región en la que configuró inicialmente la Torre de Control de AWS.
3. En el menú de navegación de la izquierda, seleccione AWS cuentas.
4. Elige el enlace de tu cuenta de administración.
5. Elige el menú desplegable de conjuntos de permisos, selecciona y AWSServiceCatalogEndUserAccess, a continuación, selecciona Eliminar.
6. Selecciona AWS las cuentas en el panel izquierdo.
7. Abra la pestaña Permission sets (Conjuntos de permisos).
8. AWSServiceCatalogEndUserAccessSelecciónala y elimínala.

Para eliminar funciones de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el menú de navegación izquierdo, elija Roles.
3. En la tabla, busque los roles con el nombre AWSControlTower.
4. Para cada rol de la tabla, realice lo siguiente:
    a. Active la casilla del rol.
    b. Elija Eliminar rol.
    c. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa y, a continuación, elija Yes, delete (Sí, eliminar).

Para eliminar las políticas de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el menú de navegación izquierdo, elija Policies (Políticas).
3. En la tabla, busque las políticas con el nombre AWSControlTower.
4. Para cada política de la tabla, realice lo siguiente:
    a. Active la casilla de la política.
    b. Elija Policy actions (Acciones de política) y Delete (Eliminar) en el menú desplegable.
    c. En el cuadro de diálogo que se abre, revise la información para asegurarse de que sea precisa y, a continuación, elija Delete (Eliminar).

Ayuda con los recursos de AWS Control Tower

Si encuentra algún problema que no pueda resolver al eliminar los recursos de AWS Control Tower, póngase en contacto con AWS Support.

Cómo desmantelar una landing zone

Para desmantelar su zona de aterrizaje de la AWS Control Tower, siga el procedimiento que se indica aquí.

> **Note**
>
> Le recomendamos que desgestione sus cuentas inscritas antes de retirarlas del servicio.

1. Diríjase a la página de configuración de la zona de aterrizaje en la consola de AWS Control Tower.
2. Elija Decommission your landing zone (Retirada de la zona de inicio) en la sección Decommission your landing zone (Retirada de la zona de inicio).
3. Aparece un cuadro de diálogo en el que se explica la acción que está a punto de realizar, con un proceso de confirmación requerido. Para confirmar su intención de retirada, debe seleccionar todas las casillas y escribir la confirmación según lo solicitado.

   > **Important**
   >
   > El proceso de retirada no se puede deshacer.

4. Si confirma su intención de desmantelar su landing zone, se le redirigirá a la página de inicio de AWS Control Tower mientras el desmantelamiento está en curso. El proceso puede requerir hasta dos horas.
5. Si el desmantelamiento se ha realizado correctamente, debe eliminar los recursos restantes manualmente antes de configurar una nueva landing zone desde la consola de la Torre de Control de AWS. Estos recursos restantes incluyen algunos buckets, organizaciones y grupos de CloudWatch registros de Amazon S3 específicos.

   > **Note**
   >
   > Estas acciones pueden tener consecuencias importantes para sus actividades de facturación y cumplimiento. Por ejemplo, si no se eliminan estos recursos, se pueden producir cargos inesperados.

   Para obtener más información acerca de cómo eliminar recursos manualmente, consulte Acerca de la eliminación de los recursos de AWS Control Tower.
6. Si pretendes configurar una nueva landing zone en una nueva AWS región, sigue este paso adicional. Introduzca el siguiente comando a través de la CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

Tras el desmantelamiento, es necesario realizar tareas de limpieza manuales

- Debe especificar direcciones de correo electrónico diferentes para las cuentas de archivo de registro y de auditoría si crea una nueva landing zone después de desmantelar una, o sigue el procedimiento para incorporar sus propias cuentas de archivo de registro o de auditoría existentes.
- El grupo de CloudWatch registros`aws-controltower/CloudTrailLogs`,, debe eliminarse manualmente antes de configurar otra landing zone.
- Los dos buckets de Amazon S3 con nombres reservados para los registros se deben eliminar o cambiar de nombre manualmente.
- Debe eliminar o cambiar el nombre de las unidades organizativas de Security y Sandbox existentes manualmente.

> **Note**
>
> Antes de poder eliminar la organización OU de AWS Control Tower Security, primero debe eliminar las cuentas de registro y auditoría, pero no la cuenta de administración. Para eliminar estas cuentas, debe ¿Cuándo iniciar sesión como usuario root en la cuenta de auditoría y en la cuenta de registro y eliminarlas individualmente.

- Es posible que desee eliminar manualmente la configuración AWS IAM Identity Center (del Centro de identidad de IAM) de la Torre de Control de AWS, pero puede continuar con la configuración del Centro de identidad de IAM existente.
- Es posible que desee eliminar la VPC creada por AWS Control Tower y eliminar el conjunto de CloudFormation pilas de AWS asociado.
- Para poder configurar una nueva landing zone en una nueva AWS región, debes seguir estos pasos adicionales.
  - Introduzca el siguiente comando a través de la CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- Elimine la regla gestionada restante, denominada`AWSControlTowerManagedRule`, de las cuentas compartidas y de los miembros de todas las regiones gobernadas. `AWSControlTowerManagedRule`es una EventBridge regla de Amazon.

Configuración después del desmantelamiento de una landing zone

Después de retirar la zona de inicio, no podrá ejecutar correctamente la configuración de nuevo hasta que haya finalizado la limpieza manual. Además, sin la limpieza manual de estos recursos restantes, puede incurrir en cargos de facturación inesperados. Debe atender estas cuestiones:

- La cuenta de administración de la Torre de Control de AWS forma parte de la unidad organizativa raíz de la Torre de Control de AWS. Asegúrese de eliminar estas funciones y políticas de IAM de la cuenta de administración:
  - Roles:
    - `AWSControlTowerAdmin`
    - `AWSControlTowerCloudTrailRole`
    - `AWSControlTowerStackSetRole`
  - Políticas:
    - `AWSControlTowerAdminPolicy`
    - `AWSControlTowerCloudTrailRolePolicy`
    - `AWSControlTowerStackSetRolePolicy`
- Es posible que desee eliminar o actualizar la configuración del centro de identidad de IAM existente para AWS Control Tower antes de volver a subir a una landing zone, pero no es obligatorio que la elimine.
- Es posible que desee eliminar la VPC creada por AWS Control Tower.
- La configuración falla si las direcciones de correo electrónico especificadas para las cuentas de registro o auditoría están asociadas a una AWS cuenta existente. Puedes cerrar las AWS cuentas o usar direcciones de correo electrónico diferentes para volver a configurar una landing zone. Como alternativa, puedes reutilizar estas cuentas compartidas existentes, con la función que te permite crear tus propias cuentas de registro y auditoría. Para obtener más información, consulte Consideraciones a la hora de incorporar las cuentas de seguridad o de registro existentes.

- La configuración falla si ya existen buckets de Amazon S3 con los siguientes nombres reservados en la cuenta de registro:
  - `aws-controltower-logs-{accountId}-{region}` (utilizado para el bucket de registro).
  - `aws-controltower-s3-access-logs-{accountId}-{region}` (utilizado para el bucket de acceso de registro).

  Debe cambiar el nombre o quitar estos buckets o usar una cuenta diferente para la cuenta de registro.
- La configuración falla si la cuenta de administración tiene el grupo de CloudWatch registros existente`aws-controltower/CloudTrailLogs`, en Logs. Debe cambiar el nombre o quitar el grupo de registro.

Antes de configurarlo en un nuevo Región de AWS

Si quieres configurar una nueva landing zone en una nueva AWS región, sigue estos pasos adicionales.

- Introduzca el siguiente comando a través de la CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- Elimine la regla gestionada restante, denominada`AWSControlTowerManagedRule`, de las cuentas compartidas y de los miembros de todas las regiones gobernadas.

> **Note**
>
> No puedes configurar una nueva landing zone en una organización con unidades organizativas de nivel superior denominadas Security o Sandbox. Debe cambiar el nombre o quitar estas unidades organizativas para volver a configurar una zona de inicio.

Resolución de problemas

Si tiene problemas al utilizar AWS Control Tower, puede utilizar la siguiente información para resolverlos de acuerdo con nuestras prácticas recomendadas. Si los problemas que encuentra están fuera del alcance de la siguiente información o si persisten después de haber intentado resolverlos, póngase en contacto con AWS Support.

Error de lanzamiento de Landing Zone

Causas comunes de fallo en el lanzamiento de la zona de inicio:

- Falta de respuesta a un mensaje de email de confirmación.
- AWS CloudFormation StackSet fallo.

Mensajes de correo electrónico de confirmación: si tu cuenta de administración tiene menos de una hora de antigüedad, es posible que surjan problemas al crear las cuentas adicionales.

Acción que debe ejecutarse

Si se produce este problema, compruebe su correo electrónico. Es posible que se le haya enviado un correo electrónico de confirmación que está a la espera de respuesta. También le recomendamos que espere una hora y, a continuación, vuelva a intentarlo. Si el problema persiste, ponte en contacto con AWS Support.

Fallado StackSets: otra posible causa del fallo en el lanzamiento de la zona de landing zone es un AWS CloudFormation StackSet fallo. AWS Las regiones del Security Token Service (STS) deben estar habilitadas en la cuenta de administración de todas AWS las regiones que controla AWS Control Tower para que el aprovisionamiento se realice correctamente; de lo contrario, los conjuntos de pilas no se lanzarán.

Acción que debe ejecutarse

Asegúrese de habilitar todas las regiones de punto final del AWS Security Token Service (STS) requeridas antes de lanzar AWS Control Tower.

Para ver una lista de los Regiones de AWS elementos compatibles con AWS Control Tower, consulteCómo funcionan AWS las regiones con AWS Control Tower.

Error en la zona de aterrizaje no actualizada

Si no ha actualizado su landing zone recientemente, es posible que reciba un mensaje de error al intentar recuperar el acceso a AWS Control Tower. Es posible que aparezca un mensaje de error similar a este:

```
Unable to access Control Tower
```

Tu cuenta ha estado inactiva durante demasiado tiempo. Debido a la inactividad, debe actualizar su landing zone para poder acceder a AWS Control Tower.

Sin embargo, la actualización de tu landing zone puede fallar.

Pasos a seguir

Inicie sesión en la cuenta de administración de su organización e inicie sesión como usuario root. Su usuario de IAM o usuario del Centro de Identidad de IAM debe tener permisos de administrador de AWS Control Tower y formar parte del AWSControlTowerAdminsgrupo. A continuación, vuelva a intentar la actualización.

Error en el nuevo aprovisionamiento de cuentas

Si se produce este problema, compruebe estas causas comunes.

Al completar el formulario de aprovisionamiento de cuentas, es posible que haya:

- especificado tagOptions,
- activado las notificaciones de SNS,
- habilitado las notificaciones de productos aprovisionados.

Vuelva a intentar el aprovisionamiento de su cuenta, sin especificar ninguna de esas opciones. Para obtener más información, consulte Aprovisione cuentas con AWS Service Catalog Account Factory .

Otras causas comunes de falla:

- Si ha creado un plan de productos aprovisionados (para ver los cambios en los recursos), es posible que el aprovisionamiento de cuentas permanezca en estado In progress (En curso) indefinidamente.

- La creación de una cuenta nueva en Account Factory fallará mientras se estén realizando otros cambios en la configuración de AWS Control Tower. Por ejemplo, mientras se ejecuta un proceso para añadir un control a una OU, Account Factory mostrará un mensaje de error si intenta aprovisionar una cuenta.

Para comprobar el estado de una acción anterior en la Torre de Control de AWS

- Navegue hasta AWS CloudFormation > StackSets
- Compruebe cada conjunto de pilas relacionado con AWS Control Tower (prefijo: "AWSControlTower«)
- Busque AWS CloudFormation StackSets operaciones que aún estén ejecutándose.

Si el aprovisionamiento de cuentas tarda más de una hora, lo mejor es finalizar el proceso de aprovisionamiento e intentarlo de nuevo.

Error al inscribir una cuenta existente

Si intentas inscribir una AWS cuenta existente una vez y no lo consigues, al intentarlo por segunda vez, el mensaje de error podría indicarte que el conjunto de pilas existe. Para continuar, debe quitar el producto aprovisionado en Account Factory.

Si el motivo del primer error de inscripción fue que olvidó crear el rol `AWSControlTowerExecution` en la cuenta de antemano, el mensaje de error que recibirá correctamente le indicará que cree el rol. Sin embargo, cuando intenta crear el rol, es probable que reciba otro mensaje de error que indica que AWS Control Tower no ha podido crear el rol. Este error se produce porque el proceso se ha completado parcialmente.

En este caso, debe realizar dos pasos de recuperación antes de poder continuar con la inscripción de su cuenta existente. En primer lugar, debe cancelar el producto aprovisionado por Account Factory a través de la AWS Service Catalog consola. A continuación, debe usar la AWS Organizations consola para mover manualmente la cuenta fuera de la unidad organizativa y volver a la raíz. Una vez hecho esto, cree el rol `AWSControlTowerExecution` en la cuenta y, a continuación, rellene de nuevo el formulario Enroll account (Inscribir cuenta).

Otra posible causa del error de inscripción es que la cuenta tiene recursos de AWS Config existentes. En ese caso, consulta Inscribir cuentas que tengan AWS Config recursos existentes para obtener instrucciones sobre cómo puedes modificar tus recursos existentes.

No se puede actualizar una cuenta de Account Factory

Cuando una cuenta se encuentra en un estado incoherente, no se puede actualizar correctamente desde Account Factory o AWS Service Catalog.

Caso 1: Es posible que aparezca un mensaje de error similar a este:

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

Causa común: AWS Control Tower siempre elimina la VPC AWS predeterminada durante el aprovisionamiento inicial. Para tener una VPC AWS predeterminada en una cuenta, debe añadirla después de crear la cuenta. AWS Control Tower tiene su propia VPC predeterminada que reemplaza a la AWS VPC predeterminada, a menos que configure Account Factory como se muestra en el tutorial, de modo que AWS Control Tower no aprovisione ninguna VPC en absoluto. Entonces la cuenta no tiene VPC. Tendrías que volver a añadir la VPC AWS predeterminada si quieres usarla.

Sin embargo, AWS Control Tower no admite la AWS VPC predeterminada. La implementación de una hace que la cuenta entre en estado `Tainted`. Cuando se encuentra en ese estado, no puede actualizar la cuenta de forma automática. AWS Service Catalog

Medida a seguir: debe eliminar la VPC predeterminada que agregó y, a continuación, podrá actualizar la cuenta.

> **Note**
>
> El `Tainted` estado provoca un problema posterior: una cuenta que no esté actualizada puede impedir la activación de los controles en la unidad organizativa de la que forma parte.

Caso 2: Es posible que veas un mensaje de error similar a este:

```
AWS Control Tower detects that your enrolled account has been moved to a new organizational unit.
```

Causa común: intentó mover una cuenta de una OU registrada a otra, pero las antiguas reglas de AWS Config permanecen. La cuenta está en un estado incoherente.

Acción a tomar:

Si el traslado de la cuenta estaba previsto:

- Cierre la cuenta en Service Catalog.
- Inscríbala de nuevo.
- Contexto/impacto: las reglas de AWS Config implementadas no coinciden con la configuración dictada por la OU de destino.
- AWS Es posible que las reglas de configuración sigan siendo las de la OU anterior, lo que provocará gastos imprevistos.
- Los intentos de volver a inscribir o actualizar la cuenta fallarán debido a conflictos en los nombres de los recursos.

Si el traslado de la cuenta no fue intencionado:

- Devuelva la cuenta a su OU original.
- Actualice la cuenta desde Service Catalog.
- En los parámetros de lanzamiento, introduzca la unidad organizativa en la que estaba originalmente la cuenta.
- Contexto o impacto: si la cuenta no vuelve a su OU original, su estado será incompatible con los controles dictados por la nueva OU en la que se encuentra.
- Actualizar una cuenta no es una solución válida, ya que no elimina AWS Config las reglas asociadas a su unidad organizativa anterior.

No se pudo actualizar la zona de aterrizaje

AWS Control Tower no revierte a una versión anterior de landing zone si se produce un error en una actualización. Es posible que encuentres tu landing zone en un estado indeterminado. Si es así, ponte en contacto con AWS el servicio de asistencia.

Las actualizaciones de la zona de aterrizaje pueden fallar por varios motivos.

- No se cumplen los requisitos previos
- AWS Config existen recursos en determinadas cuentas
- Existen cuentas cerradas

No se cumplen los requisitos previos

La actualización de una zona de aterrizaje debe cumplir los mismos requisitos previos que la configuración de una zona de aterrizaje. Antes de realizar la actualización, revisa las comprobaciones previas al lanzamiento.

AWS Config los recursos existen en las cuentas de Security OU

No añada AWS Config recursos a sus cuentas de archivo de auditoría y registro. El proceso de actualización de la zona de aterrizaje no puede completarse con estos recursos presentes. Estas restricciones son similares a las de registrar una cuenta o configurar una landing zone por primera vez. Para obtener más información, consulte Inscribir cuentas que cuenten con AWS Config recursos existentes.

Existen cuentas cerradas

Cuando una cuenta está cerrada o suspendida, es posible que se produzca un problema al intentar actualizar tu landing zone. Debes eliminar el producto aprovisionado en todas las cuentas cerradas antes de realizar una actualización en la landing zone.

En la página del producto AWS Service Catalog aprovisionado, es posible que veas un mensaje de error similar a este:

```
AWSControlTowerExecution role can't be assumed on the account.
```

Causa común: has suspendido una cuenta sin eliminar el producto aprovisionado.

Acción a realizar: si aparece este error, tiene dos opciones:

1. Póngase en contacto con AWS Support y vuelva a abrir la cuenta, elimine el producto aprovisionado y vuelva a cerrar la cuenta.
2. Elimine los recursos de los StackSets que quedaron huérfanos debido al cierre de la cuenta. (Esta opción solo está disponible si StackSets tienen instancias en el estado Actual que no va a eliminar).

Para eliminar los recursos de StackSets, haga lo siguiente para cada cuenta cerrada:

- Vaya a cada una de las Torres de Control StackInstances de AWS StackSets y elimine la cuenta que se haya cerrado de todas las regiones.
- IMPORTANTE: Elija la opción Retain Stack para StackSet eliminar solo las instancias de la pila. StackSet no puede asumir un rol desde la cuenta cerrada, por lo que fallará si intenta asumir el `AWSControlTowerExecution` rol, lo que generará el mensaje de error que has recibido.

Error: error que menciona AWS Config

Si AWS Config está habilitada en alguna AWS región compatible con la Torre de Control de AWS, es posible que reciba un mensaje de error porque no se pudo realizar una comprobación previa. Es posible que el mensaje no explique el problema de manera adecuada, debido a algún comportamiento subyacente de AWS Config.

Puede recibir un mensaje de error similar a uno de los siguientes:

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

Causa común: cuando el AWS Config servicio está habilitado en una AWS cuenta, crea un registrador de configuración y un canal de entrega con un nombre predeterminado. Si deshabilita el AWS Config servicio a través de la consola, no se elimina el grabador de configuración ni el canal de entrega. Debe eliminarlos mediante la CLI o modificarlos para usarlos en AWS Control Tower. Si el AWS Config servicio está habilitado en alguna de las regiones admitidas por AWS Control Tower, se puede producir un error.

Si la cuenta tiene recursos de AWS Config existentes, consulta Inscribir cuentas que tengan AWS Config recursos existentes para obtener instrucciones sobre cómo puedes modificar tus recursos existentes.

Acción: elimine el grabador de configuración y el canal de entrega en todas las regiones compatibles. No basta con deshabilitar AWS Config, la grabadora de configuración y el canal de entrega deben eliminarse mediante la CLI. Tras eliminar el grabador de configuración y el canal de entrega de la CLI, puede volver a intentar iniciar AWS Control Tower e inscribir la cuenta.

Si se encuentra en el proceso de implementar un producto aprovisionado, debe eliminarlo antes de volver a intentarlo. De lo contrario, es posible que aparezca un mensaje de error similar a este:

- `An error occurred (InvalidParametersException) when calling the ProvisionProduct operation: A stack named Stackname already exists.`

En el mensaje, *Stackname*especifica el nombre de la pila.

Estos son algunos ejemplos de comandos AWS Config CLI que puede usar para determinar el estado de su grabadora de configuración y canal de entrega.

Comandos de visualización:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

Comandos de eliminación:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

Para obtener más información, consulte la AWS Config documentación

- Administración de la grabadora de configuración (AWS CLI)
- Administración del canal de entrega

Error: no se encontraron rutas de lanzamiento

Cuando intente crear una cuenta nueva, es posible que aparezca un mensaje de error similar al siguiente:

```
No launch paths found for resource: prod-dpqqfywxxxx
```

Este mensaje de error lo genera AWS Service Catalog, que es el servicio integrado que ayuda a aprovisionar cuentas en AWS Control Tower.

Causas comunes:

- Puede que haya iniciado sesión como root. AWS Control Tower no admite la creación de cuentas si ha iniciado sesión como usuario root.
- Su usuario del Centro de Identidad de IAM no se ha añadido al grupo de permisos correspondiente. Es posible que deba añadir su usuario del Centro de Identidad de IAM a uno de estos grupos de permisos: AWSAccountFactory(para el acceso de los usuarios finales) o AWSServiceCatalogAdmins(para el acceso de administrador).
- Si está autenticado como usuario de IAM, debe añadirlo a la AWS Service Catalog cartera para que tenga los permisos correctos.
- Este problema también se produce si tiene los permisos correctos, pero se detecta una desviación en la Torre de Control de AWS y es necesario repararla. Para reparar la mayoría de los tipos de desviación, seleccione Restablecer en la página de configuración de la zona de aterrizaje.

Se ha recibido un error de permisos insuficientes

Es posible que tu cuenta no tenga los permisos necesarios para realizar determinadas tareas en determinadas áreas AWS Organizations. Si se produce el siguiente tipo de error, compruebe todas las áreas de permisos, como los permisos de IAM o del Centro de Identidad de IAM, para asegurarse de que no se le deniegue el permiso desde esos lugares:

```
You have insufficient permissions to perform AWS Organizations API actions.
```

Si cree que su trabajo requiere la acción que está intentando realizar y no encuentra ninguna restricción relevante, póngase en contacto con el administrador del sistema o con AWS Support.

Los controles de Detectives no entran en vigor en las cuentas

Si ha ampliado recientemente su implementación de la Torre de Control de AWS a una nueva AWS región, los controles de detección recién aplicados no se aplicarán a las cuentas nuevas que cree en ninguna región hasta que se actualicen las cuentas individuales de las unidades organizativas gobernadas por la Torre de Control de AWS. Los controles de detección existentes en las cuentas existentes siguen en vigor.

Si intentas activar un control policial antes de actualizar tus cuentas, es posible que aparezca un mensaje de error similar al siguiente:

```
AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child accounts have dependencies that are missing. Update all child accounts under the OU, then try again.
```

Acción que se debe ejecutar: actualizar cuentas.

Para actualizar sus cuentas desde la consola de AWS Control Tower, consulteCuándo actualizar las unidades organizativas y las cuentas de AWS Control Tower.

Para actualizar varias cuentas individuales mediante programación, puede utilizar las API AWS Service Catalog y la AWS CLI para automatizar las actualizaciones. Para obtener más información acerca de cómo abordar el proceso de actualización, consulte esto Tutorial en vídeo. Puede sustituir la UpdateProvisionedProductAPI que se muestra en el ProvisionProductvídeo por la API.

Si tiene más dificultades para activar los controles de detección en sus cuentas, póngase en contacto con AWS Support.

Error de tasa superada devuelto por la AWS Organizations API

Causa posible

Su carga de trabajo se estaba ejecutando mientras la Torre de Control de AWS realizaba un análisis diario para comprobar si sus SCP se habían desviado.

Pasos a seguir

Si encuentras una limitación o un `rate exceeded` error en la API, sigue estos pasos:

- Ejecute sus cargas de trabajo en otro momento. (Consulte el programa de escaneos de invariancia SCP de AWS Control Tower por región para saber cuándo AWS Control Tower ejecuta sus escaneos de auditoría).
- Si llama a las API directamente a través de HTTP: utilice el AWS SDK, que reintenta automáticamente las acciones fallidas
- Solicita un aumento del límite a través de Service Quotas and AWS Support

Puede encontrar un ejemplo de instrucciones de solución de problemas para la limitación de API en Elastic Beanstalk aquí: `https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

No se pudo mover una cuenta de Account Factory directamente de una zona de aterrizaje de la Torre de Control de AWS a otra zona de aterrizaje de la Torre de Control de AWS

> **Warning**
>
> Esta práctica no cumple con el requisito previo para la inscripción de cuentas aptas, ya que las cuentas aptas deben formar parte de la misma organización general de AWS y cada organización puede tener solo una landing zone. Si ha intentado realizar esta acción y recibe varios mensajes de error, aquí encontrará información que puede resultarle útil.

Para mover una cuenta que ha aprovisionado a través de Account Factory a otra landing zone gestionada por AWS Control Tower, a otra cuenta de administración, debe eliminar todas las funciones de IAM y las pilas asociadas a esa cuenta de la OU original. Elimine estos recursos de todas las regiones en las que esté desplegada la cuenta.

> **Note**
>
> La mejor forma de eliminar los recursos es desaprovisionar la cuenta en su unidad organizativa original antes de intentar moverla.

Si no se eliminan los recursos, la inscripción en la nueva unidad organizativa no se podrá realizar de forma espectacular. Es posible que reciba uno o más mensajes de error y seguirá recibiendo mensajes de error similares hasta que se eliminen las funciones y grupos restantes de todas las regiones en las que se desplegó la cuenta.

Cada vez que reciba un mensaje de error, deberá eliminar la cuenta de la nueva unidad organizativa, eliminar el recurso anterior objeto del mensaje de error y, a continuación, intentar volver a mover la cuenta a la nueva unidad organizativa. Este proceso removing-and-deleting debe repetirse para todos los recursos restantes, para cada región en la que se implementó la cuenta, posiblemente 10 o 20 veces. Estos errores recurrentes se producen porque la cuenta se aprovisionó en una unidad

organizativa con un SCP que impide la eliminación de la función de IAM. Puede acortar el proceso de recuperación eliminando todos los recursos de la cuenta antes de volver a intentarlo.

Los ejemplos que aparecen a continuación representan los tipos de mensajes de error que puede recibir si permanecen funciones y pilas sin eliminar. Lo más probable es que veas uno de estos mensajes a la vez cada vez que intentes inscribir la cuenta, siempre y cuando queden recursos antiguos.

Los valores de las cadenas de ID de recurso se han modificado para los ejemplos. Sus valores no serán los mismos en un mensaje de error que pueda recibir. Es posible que veas un mensaje similar a los siguientes ejemplos:

- `AWS Control Tower cannot create the IAM role aws-controltower-AdministratorExecutionRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ConfigRecorderRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ForwardSnsNotificationRole because the role already exists. To continue, delete the existing IAM role and try again.`

O puede que veas un mensaje de error sobre un error en un conjunto de pilas, similar a este:

```
"Error\":\"StackSetFailState\",
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
```

```
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

Una vez que se hayan eliminado todos los recursos restantes de la primera OU, podrá invitar, aprovisionar o inscribir la cuenta en la nueva OU correctamente.

AWS Support

Si desea trasladar sus cuentas de miembro existentes a otro plan de soporte, puede iniciar sesión en cada cuenta con credenciales de cuenta raíz, comparar planes y establecer el nivel de soporte que prefiera.

Le recomendamos que actualice la MFA y los contactos de seguridad de la cuenta cuando realice cambios en el plan de soporte.

Tipos de líneas de base

La base de AWS Control Tower es un grupo de recursos y configuraciones específicas que puede aplicar a un objetivo. El objetivo de referencia más común puede ser una unidad organizativa (OU). Por ejemplo, puede habilitar una línea base con una unidad organizativa seleccionada como objetivo para registrar esa unidad organizativa en AWS Control Tower.

Durante la configuración de la zona de aterrizaje, el objetivo de referencia puede ser una cuenta compartida o la zona de aterrizaje en su conjunto. Es posible que determinadas líneas base se habiliten y actualicen en función de los ajustes y configuraciones de tu zona de landing zone. AWS Control Tower crea e implementa los recursos en el objetivo de la manera que especifica la línea base.

Cuando habilita una línea base para un objetivo, la línea base se representa como un AWS CloudFormation recurso, denominado `EnabledBaseline` recurso.

AWS Control Tower incluye cuatro tipos esenciales de líneas de base:

- Un tipo puede aplicarse a una unidad organizativa registrada en AWS Control Tower o a una unidad organizativa que desee registrar aplicando la línea base.
- Se pueden aplicar tres tipos de líneas base a una zona de aterrizaje o a una cuenta compartida, durante la configuración inicial o durante una actualización de la zona de aterrizaje.

Tipo de línea base que se aplica a nivel de unidad organizativa, para registrar y actualizar las unidades organizativas

- Nombre: `AWSControlTowerBaseline`

  Descripción: Configura los recursos y los controles obligatorios para las cuentas de los miembros dentro de la OU de destino, necesarios para la gobernanza de la Torre de Control de AWS.

  Consideración: Esta línea base conserva la configuración de la zona de landing zone (la región deniega el control). En otras palabras, si una región no está permitida en el nivel de landing zone, esa región no estará permitida para esa OU cuando llames a la `EnableBaseline` API para registrar una OU.

> **Note**
>
> La región a nivel de OU que deniega el control no tiene forma de permitir regiones que la región de landing zone deniegue el control no permita.

Para obtener más información, consulte Cómo funcionan los SCP con la denegación en la documentación. AWS Organizations

Recomendación: Le recomendamos que confirme las regiones en las que la OU de destino puede estar ejecutando cargas de trabajo y que compruebe los resultados con la zona de landing zone (la región deniega el control) antes de llamar a la `EnableBaseline` API de la OU o podría perder el acceso a los recursos de determinadas regiones.

> **Note**
>
> Las líneas base de la zona de aterrizaje se comportan de forma diferente a las líneas base de la OU.

AWS Control Tower habilita automáticamente las líneas base que se aplican a nivel de zona de aterrizaje, como parte del proceso de configuración y actualización de la zona de aterrizaje. Las líneas base de tu zona de aterrizaje pueden cambiar a medida que cambies la configuración de la zona de aterrizaje. Por ejemplo, si opta por el IAM Identity Center, AWS Control Tower puede habilitar la última versión de la `IdentityCenterBaseline` línea base en su landing zone.

Puedes ver las líneas base habilitadas para tu landing zone con la llamada a la `ListEnabledBaselines` API.

Tipos de referencia que pueden aplicarse a tu landing zone o a tus cuentas compartidas

- Nombre: `AuditBaseline`

  Descripción: Configura recursos para supervisar la seguridad y el cumplimiento de las cuentas de su organización. No puede cambiar esta línea base, la implementa AWS Control Tower.
- Nombre: `LogArchiveBaseline`

Descripción: Configura un repositorio central para los registros de las actividades de las API y las configuraciones de recursos de las cuentas de su organización. No puede cambiar esta línea base, la implementa AWS Control Tower.

- Nombre: `IdentityCenterBaseline`

  Descripción: Configura los recursos compartidos para el Centro de Identidad de IAM, que preparan el acceso `AWSControlTowerBaseline` al Centro de Identidad para las cuentas.

  Consideración: Esta línea base solo funciona si seleccionó IAM Identity Center como su proveedor de identidad en el momento de configurar su zona de aterrizaje inicialmente, o si posteriormente cambia la configuración de la zona de aterrizaje para habilitar el IAM Identity Center para su zona de aterrizaje. Si utilizas un proveedor de identidad diferente, no podrás habilitar esta línea base.

Inscripción parcial de cuentas

Cuando se trabaja con valores de referencia, se puede colocar una cuenta en un estado denominado Inscrita parcialmente.

Este estado puede producirse si vuelve a registrar una OU mediante una llamada a la `ResetEnabledBaseline` API, ya que AWS Control Tower aplica solo los recursos obligatorios a las cuentas de la OU de destino. Una cuenta a la que le faltan los recursos opcionales (controles) de su unidad organizativa principal se marca como Inscrita parcialmente.

Si traslada una cuenta no inscrita a una OU registrada y, a continuación, llama a la `ResetEnabledBaseline` API de la OU para inscribirla, AWS Control Tower aplica los recursos asociados `AWSControlTowerBaseline` a la cuenta recién inscrita. Sin embargo, los controles opcionales habilitados para esta OU no se aplican a la cuenta. La cuenta permanece en un estado de inscripción parcial.

Para inscribir la cuenta por completo, selecciona Volver a registrar o Actualizar cuenta en la consola. Al seleccionar estas operaciones desde la consola, AWS Control Tower aplica todos los recursos de esa OU a la cuenta recién inscrita, incluidos los controles opcionales que se activan para esa OU.

Variación en las operaciones entre la consola de la Torre de Control de AWS y las API para las líneas base

Cuando cambia el estado de gobierno de una OU, la consola de AWS Control Tower realiza más operaciones automáticamente, en comparación con el cambio de gobierno mediante las API para las líneas base.

Diferencias

- Registrar y aprovisionar productos

  Al registrar una OU a través de la consola, AWS Control Tower crea productos de Service Catalog para las cuentas de los miembros de la OU, como parte de la inscripción de cada cuenta. Cuando registra una OU mediante la `EnableBaseline` API y la OU`AWSControlTowerBaseline`, AWS Control Tower no crea productos aprovisionados para las cuentas de los miembros de la OU.
- Anule el registro de una OU

  Cada vez que cancele el registro de una OU, primero debe eliminar todas las cuentas de los miembros y las OU anidadas. A continuación, AWS Control Tower elimina todos los controles que se aplican a la OU.
  - Si selecciona Eliminar la OU de la consola, AWS Control Tower procederá a anular el registro y, a continuación, a eliminar la OU de su organización.
  - Sin embargo, si anula el registro de la OU llamando a la `DisableBaseline` API para eliminarla `AWSControlTowerBaseline` de la OU, AWS Control Tower no elimina la OU de su organización, sino que la OU sigue presente en la organización sin estar registrada.

Líneas base y valores predeterminados de control de versiones

Si la zona de aterrizaje de su torre de control de AWS ya está configurada y decide habilitar una línea base de zona de aterrizaje, AWS Control Tower habilita la última versión de la línea base que sea compatible con la versión de su zona de aterrizaje. Si decide habilitar una línea base para una OU que aún no esté registrada en AWS Control Tower, AWS Control Tower proporcionará automáticamente la última versión compatible de la línea base para esa OU.

Compatibilidad de las versiones de las líneas base y de las zonas de aterrizaje de la OU

Las líneas base de AWS Control Tower le permiten establecer un estándar de gobierno a nivel de unidad organizativa, en lugar de a nivel de landing zone, si su empresa lo requiere. La línea base denominada `AWSControlTowerBaseline` está disponible para ayudarle a registrar sus unidades organizativas en AWS Control Tower.

> **Note**
>
> Una línea base es un grupo de controles y recursos que trabajan juntos para establecer un entorno de gobierno estable dentro de tu landing zone.

Cuando habilita una línea de base en una OU, al llamar a la `EnableBaseline` API de AWS Control Tower, debe especificar una versión de referencia que sea compatible con su versión actual de zona de aterrizaje de AWS Control Tower. Tras especificar una línea base, todas las cuentas de los miembros de una OU siguen la línea base establecida para la OU. En otras palabras, las cuentas nuevas se aprovisionan con la línea base actualizada y las cuentas de los miembros existentes se rigen de acuerdo con la nueva línea base.

Si no seleccionas una línea base para tus unidades organizativas y cuentas existentes, la versión de landing zone determina toda la postura de gobierno de forma predeterminada. Sin embargo, a cada OU registrada en la zona de aterrizaje se le asigna una versión de referencia, que es la última versión de referencia compatible con la versión de la zona de aterrizaje actual. Por lo tanto, cada unidad organizativa y cuenta de miembro inscrito tiene una línea base asociada, incluso si nunca se asigna una línea base específica.

Para la línea base a nivel de OU`AWSControlTowerBaseline`, en la siguiente tabla se muestra la compatibilidad de las líneas base con las versiones de zonas de landing zone de AWS Control Tower.

Versión de referencia	Versiones de zonas de aterrizaje	Planos incluidos	Controles incluidos	Cambio con respecto a la línea base anterior	
1.0	2.0 a 2.7	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Recursos de IAM	Todos los controles obligatorios	Ninguna	
2.0	2.8 a 2.9	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR,	Todos los controles obligatorios	Se agregó el rol AWS Config vinculado a servicios (SLR) y un nuevo esquema de Config para usar el SLR	

Versión de referencia	Versiones de zonas de aterrizaje	Planos incluidos	Controles incluidos	Cambio con respecto a la línea base anterior	
		recursos de IAM			
3.0	3.0 a 3.1	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, recursos de IAM	Todos los controles obligatorios	Nuevo AWS Config plano. Cámbielo para registrar los recursos globales solo en la región de origen. Se ha eliminado el CloudTrail plano	

Versión de referencia	Versiones de zonas de aterrizaje	Planos incluidos	Controles incluidos	Cambio con respecto a la línea base anterior	
4.0	3.2 a 3.3	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, recursos de IAM	Todos los controles obligatorios	Nuevo plano de SLR	

Para obtener más información sobre los recursos específicos que se crean en las cuentas al configurar tu landing zone, consulta Recursos creados en las cuentas compartidas.

Si actualizas la zona de aterrizaje a una versión que admite una versión de `AWSControlTowerBaseline` referencia más reciente y la nueva versión de la zona de aterrizaje es compatible con la versión de referencia existente, el estado de la unidad organizativa cambia a Actualizar disponible.

- Puedes seguir utilizando la fábrica de cuentas y otras funciones sin actualizar inmediatamente la base de la OU, excepto en el caso de una actualización de landing zone de la versión 2.x a la 3.x.
- Las cuentas nuevas inscritas en esta OU reciben recursos en función de la versión básica existente hasta que se actualice la versión básica (con la función de ampliación de la gobernanza de la consola o mediante la `UpdateEnabledBaseline` API).

- Tras actualizar la versión de referencia, todas las cuentas de esa OU reciben los recursos en función de la nueva versión de referencia.

> **Note**
>
> Si actualiza la zona de aterrizaje de la AWS Control Tower de una versión 2.X a una versión 3.X, también debe actualizar la versión básica de sus unidades organizativas, debido al cambio de las rutas a nivel de cuenta a las de organización. AWS CloudTrail En la consola, su OU mostrará el estado de Actualización requerida.

Consideraciones sobre las líneas de base

- Si su OU requiere una actualización de referencia, no puede aprovisionar cuentas nuevas ni inscribir cuentas existentes en esa OU.
- Tras una actualización de la zona de aterrizaje, si también planea actualizar una línea base de la OU, debe volver a registrar la OU o actualizar la versión de la línea base de la OU mediante programación.
- Te recomendamos que actualices a la línea base más alta compatible para la versión de zona de aterrizaje que utilices, de modo que disfrutes de todas las ventajas de la zona de aterrizaje y la línea base combinadas. Por ejemplo, si actualizas a la versión 3.3 de landing zone, puedes seguir usando la línea base 3.0, pero no obtendrás todos los beneficios de la versión 3.3 de landing zone a menos que también actualices a la línea base 4.0.
- Las actualizaciones de referencia no se pueden revertir.
- La activación de referencia se dirige a una unidad organizativa a la vez. Por lo tanto, las OU anidadas no se actualizan automáticamente cuando se actualiza la OU principal. Se recomienda actualizar la unidad organizativa principal antes de actualizar las unidades organizativas anidadas.
- Al llamar a la `UpdateEnabledBaseline` API o volver a registrar una OU desde la consola, la OU conserva todos los controles que estaban habilitados antes de la actualización de referencia.
- Cuando varias versiones de referencia son compatibles con su versión de zona de aterrizaje, debe utilizar la última versión de referencia si habilita una línea de base en una OU no administrada,.

Ejemplos: Registrar una unidad organizativa de AWS Control Tower solo con API

Este tutorial de ejemplos es un documento complementario. Para obtener explicaciones, advertencias y más información, consulte. Tipos de líneas de base

Requisitos previos

Debe tener una unidad organizativa existente que no esté registrada en AWS Control Tower y que desee registrar. O bien, debe tener una unidad organizativa registrada que desee volver a registrar para actualizarla.

Registre una OU

1. Comprueba si `IdentityCenterBaseline` está activado para la landing zone. Si es así, obtenga el identificador de referencia habilitado para Identity Center.

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. Obtenga el ARN de la unidad organizativa objetivo.

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. Obtenga el ARN de la línea base. `AWSControlTowerBaseline`

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. Cree la `AWSControlTowerBaseline` línea base en la unidad organizativa de destino.

   Si la línea base de Identity Center está habilitada:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
```

```
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

Si la línea base de Identity Center no está habilitada, omita la *parameters* marca de la siguiente manera:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Vuelva a registrar una unidad organizativa

Tras actualizar la configuración de la zona de aterrizaje o actualizar la versión de la zona de aterrizaje, debes volver a registrar las unidades organizativas para proporcionarles los cambios más recientes. Siga estos pasos para volver a registrar una unidad organizativa mediante programación, restableciendo el recurso asociado. `EnabledBaseline`

1. Obtenga el ARN de la unidad organizativa de destino para volver a registrarla.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. Obtenga el ARN del `EnabledBaseline` recurso para la unidad organizativa de destino.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. Restablezca la línea base habilitada.

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

Ejemplos de uso básico de la API

Esta sección contiene ejemplos de parámetros de entrada y salida para las API de referencia de AWS Control Tower.

DisableBaseline

Para obtener más información sobre el funcionamiento de esta API, consulte DisableBaseline.

`DisableBaseline`entrada:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

`DisableBaseline`salida:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`DisableBaseline`Ejemplo de CLI:

```
aws controltower disable-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
    --region us-west-2
```

EnableBaseline

Para obtener más información sobre esta operación de API, consulte EnableBaseline.

`EnableBaseline`entrada:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
```

```
        }
    ]
}
```

`EnableBaseline`salida:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
}
```

`EnableBaseline`Ejemplo de CLI:

En este ejemplo, se muestra cómo habilitar una línea base para una AWS Organizations organización que tiene la zona de aterrizaje habilitada para acceder al AWS IAM Identity Center, gestionado por AWS Control Tower. Para recuperar el `EnabledBaseline` identificador del centro de identidad, puede llamar a la `ListEnabledBaselines` API y filtrar según la línea base del centro de identidad: (`arn:aws:controltower:`*`Region`*`::baseline/LN25R72TTG6IGPTQ`)

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

La respuesta mostrará el `EnabledBaseline` detalle, que muestra su identificador.

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
```

```
}
```

> **Note**
>
> Anote el valor del ARN de la respuesta y pase este valor como parámetro para habilitar la línea base predeterminada.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

En el caso de una organización con la zona de aterrizaje excluida de la administración de AWS Control Tower del IAM Identity Center, habilite la línea base sin el parámetro.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --region us-west-2
```

`GetBaseline`

Para obtener más información sobre el funcionamiento de esta API, consulte. GetBaseline

`GetBaseline`entrada:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

`GetBaseline`salida:

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

`GetBaseline`Ejemplo de CLI:

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

`GetBaselineOperation`

Para obtener más información sobre esta operación de API, consulte GetBaselineOperation.

`GetBaselineOperation`entrada:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`GetBaselineOperation`salida:

```
{
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

`GetBaselineOperation`Ejemplo de CLI:

```
aws controltower get-baseline-operation \
```

```
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

GetEnabledBaseline

Para obtener más información sobre esta operación de API, consulte GetEnabledBaseline.

`GetEnabledBaseline`entrada:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

`GetEnabledBaseline`salida:

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
            }
        ]
    }
}
```

`GetEnabledBaseline`Ejemplo de CLI:

```
aws controltower get-enabled-baseline \
```

```
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

ListBaselines

Para obtener más información sobre esta operación de API, consulte ListBaselines.

`ListBaselines`entrada (mediante entradas opcionales):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

`ListBaselines`salida:

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/J8HX46AHS5MIKQPD",
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/17BSJV3IGJ2QSGA2",
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
```

```
        }
    ]
}
```

`ListBaselines`Ejemplo de CLI:

```
aws controltower list-baselines \
    --region us-west-2
```

`ListEnabledBaselines`

Para obtener más información sobre esta operación de API, consulte ListEnabledBaselines.

`ListEnabledBaselines`entrada (sin filtros):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`entrada (solo `baselineIdentifiers` filtro):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`entrada (solo `targetIdentifiers` filtro):

```
{
    "filter": {
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
```

```
}
```

`ListEnabledBaselines`entrada (`baselineIdentifiers`y `targetIdentifiers` filtros):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`salida:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
```

```
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

Ejemplo de CLI con un tipo de filtro (`baselineIdentifiers`filtro):

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

Ejemplo de CLI con varios filtros (`baselineIdentifiers`y `targetIdentifiers` filtros):

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

`ResetEnabledBaseline`

Para obtener más información sobre esta operación de API, consulte ResetEnabledBaseline.

`ResetEnabledbaseline`entrada:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

`ResetEnabledBaseline`salida:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`ResetEnabledBaseline`Ejemplo de CLI:

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

UpdateEnabledBaseline

Para obtener más información sobre esta operación de API, consulte UpdateEnabledBaseline.

`UpdateEnabledBaseline`entrada:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`UpdateEnabledBaseline`salida:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`UpdateEnabledBaseline`Ejemplo de CLI:

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --baseline-version 4.0
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

Información relacionada

En este tema se enumeran los casos de uso habituales y las prácticas recomendadas para las capacidades de la Torre de Control de AWS y las mejoras adicionales. Este tema también incluye enlaces a publicaciones de blog relevantes, documentación técnica y recursos relacionados que pueden ayudarle a trabajar con AWS Control Tower.

Tutoriales y laboratorios

- Laboratorio de la Torre de Control de AWS: estos laboratorios ofrecen una visión general de alto nivel de las tareas habituales relacionadas con la Torre de Control de AWS.
- En el panel de control de AWS Control Tower, elija Obtener orientación personalizada si tiene en mente un caso de uso pero no sabe por dónde empezar.
- Intente visitar una lista seleccionada de YouTube vídeos en los que se explica más sobre cómo utilizar la funcionalidad de la Torre de Control de AWS.

Red

Configure patrones repetibles y administrables para las redes de. AWS Obtenga más información sobre el diseño, la automatización y los dispositivos que utilizan habitualmente los clientes.

- AWS Arquitectura de VPC de inicio rápido: esta guía de inicio rápido proporciona una base de redes basada en las AWS mejores prácticas para su infraestructura de AWS nube. Crea un AWS Virtual Private Network entorno con subredes públicas y privadas en el que puede lanzar AWS servicios y otros recursos.
- VPC de autoservicio en AWS Control Tower mediante AWS Service Catalog: en esta entrada de blog se describe una forma de configurar Account Factory para poder aprovisionar cuentas con VPC personalizadas.
- Implementación de Serverless Transit Network Orchestrator (STNO) en AWS Control Tower: esta entrada de blog demuestra cómo automatizar el acceso a la conectividad de red en todas las cuentas. Este blog está dirigido a los administradores de la Torre de Control de AWS o a los responsables de administrar las redes de su AWS entorno.

Seguridad, identidad y registro

Amplíe su postura de seguridad, intégrela con proveedores de identidad externos o existentes y centralice los sistemas de registro.

Seguridad

- Automatización de AWS Security Hub alertas con eventos del ciclo de vida de la Torre de Control de AWS: esta entrada de blog describe cómo automatizar la activación y la configuración de Security Hub en un entorno de múltiples cuentas de la Torre de Control de AWS en cuentas nuevas y existentes.
- Habilitación AWS Identity and Access Management: esta entrada de blog describe cómo mejorar la visibilidad de la seguridad de su organización mediante la activación y la centralización de los hallazgos de IAM Access Analyzer.
- El Almacén de parámetros de AWS Systems Manager proporciona un almacenamiento seguro y jerárquico para administrar los datos de configuración y los secretos. Puede usarla para compartir información de configuración en una ubicación segura, para que la usen AWS Systems Manager y AWS CloudFormation. Por ejemplo, puede almacenar una lista de regiones en las que desee implementar paquetes de conformidad.

Identidad

- Vincule la identidad de usuario de Azure AD a AWS cuentas y aplicaciones para el inicio de sesión único: esta entrada de blog describe cómo usar Azure AD con IAM Identity Center y AWS Control Tower.
- Gestione el acceso a AWS de forma centralizada para los usuarios de Okta con AWS IAM Identity Center: esta entrada de blog describe cómo utilizar Okta con IAM Identity Center y AWS Control Tower.

Registro

- AWS Solución de registro centralizado: esta publicación de soluciones describe la solución de registro centralizado que permite a las organizaciones recopilar, analizar y mostrar los registros de varias cuentas y AWS regiones. AWS

Implementación de recursos y administración de cargas de trabajo

Implemente y gestione los recursos y las cargas de trabajo.

- Introducción a la integración de bibliotecas: esta entrada de blog describe las carteras de introducción que puede utilizar.
- Implementación continua de Cloud Custodian en AWS Control Tower

Trabajar con organizaciones y cuentas existentes

Trabaje con AWS las organizaciones y cuentas existentes.

- Inscribir una cuenta: en este tema de la guía del usuario se describe cómo inscribir una AWS cuenta existente en AWS Control Tower.
- Cree una cuenta en AWS Control Tower: en esta entrada de blog se describe cómo implementar AWS Control Tower en sus AWS organizaciones actuales.
- Amplíe la gobernanza de la Torre de Control de AWS mediante los paquetes de conformidad de AWS Config: en esta entrada de blog se describe cómo implementar paquetes de AWS Config conformidad para ayudar a que las cuentas y organizaciones existentes pasen a ser gobernadas por la Torre de Control de AWS.
- Cómo detectar y mitigar las infracciones de protección con AWS Control Tower: en esta entrada de blog se describe cómo añadir controles y cómo suscribirse a las notificaciones de las redes sociales para que pueda recibir notificaciones por correo electrónico de las infracciones de conformidad con los controles.

Automatización e integración

Automatice la creación de cuentas e integre los eventos del ciclo de vida con AWS Control Tower.

- Eventos del ciclo de vida: esta entrada de blog describe cómo usar los eventos del ciclo de vida con AWS Control Tower.
- Creación automática de cuentas: esta entrada de blog describe cómo configurar la creación automática de cuentas en AWS Control Tower.
- Automatización de los registros de flujo de Amazon VPC: en esta entrada de blog se describe cómo automatizar y centralizar los registros de flujo de Amazon VPC en un entorno de varias cuentas.

- Automatice el etiquetado de las VPC con los eventos del ciclo de vida de la Torre de Control de AWS: en esta entrada de blog se describe cómo automatizar el etiquetado de recursos para las VPC mediante los eventos del ciclo de vida en la Torre de Control de AWS.
- Administración automatizada de cuentas: esta entrada de blog describe cómo automatizar las tareas de administración de cuentas una vez configurado el entorno de AWS Control Tower.

Migración de cargas de trabajo

Utilice otros AWS servicios con AWS Control Tower para facilitar la migración de las cargas de trabajo.

- CloudEndure migración: esta entrada de blog describe cómo combinar CloudEndure y otros AWS servicios con AWS Control Tower para facilitar la migración de la carga de trabajo.

Servicios de AWS relacionados

AWS Control Tower actúa como capa de orquestación para AWS Organizations. Por lo tanto, mediante la consola y las API de AWS Organizations, tiene acceso a más de 20 servicios de AWS adicionales que funcionan con la Torre de Control de AWS. No se puede acceder a estos servicios adicionales directamente a través de la consola de la Torre de Control de AWS.

- Para obtener una lista completa de los servicios disponibles para AWS Control Tower a través de AWS Organizations, consulte los servicios de AWS que puede usar con AWS Organizations.
- Para habilitar las capacidades de múltiples cuentas para estos servicios de AWS relacionados, debe habilitar el acceso confiable. Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS.

> **Note**
>
> Recuerde que AWS IAM Identity Center y IAM AWS CloudTrail están configurados para usted en AWS Control Tower y están completamente integrados. AWS Config No necesita modificar su configuración de acceso confiable o administración delegada para estos servicios.

- Algunos AWS servicios disponibles mediante AWS Organizations la administración delegada, como AWS Systems Manager y AWS Firewall Manager. Para obtener más información, consulte

Configuración de un administrador delegado y Habilitación de una cuenta de administrador delegado para Firewall Manager. Consulte también este vídeo, Configuración de grupos de seguridad con AWS Firewall Manager.

AWS Marketplace soluciones

Descubra soluciones de AWS Marketplace.

- AWS Control Tower Marketplace: AWS Marketplace ofrece una amplia gama de soluciones para AWS Control Tower que le ayudan a integrar software de terceros. Estas soluciones ayudan a resolver casos de uso operativos y de infraestructura clave, como la administración de identidades, la seguridad para un entorno de múltiples cuentas, las redes centralizadas, la inteligencia operativa y la gestión de eventos e información de seguridad (SIEM).

Notas de la versión de AWS Control Tower

En las siguientes secciones se muestran detalles sobre las versiones de AWS Control Tower que requieren una actualización para una zona de aterrizaje de AWS Control Tower, así como las versiones que se incorporan automáticamente al servicio.

Las características y los lanzamientos se enumeran en orden cronológico inverso (primero los más recientes) en función de la fecha en que se anunciaron oficialmente al público. Como puede haber un desfase entre el momento en que se documenta la función o versión y el momento en que se anuncia oficialmente, la fecha indicada aquí para una función o versión puede diferir ligeramente de la fecha indicada en. Historial del documento

Funciones publicadas en 2024

Funciones lanzadas en 2023

Funciones lanzadas en 2022

Funciones lanzadas en 2021

Funciones lanzadas en 2020

Funciones lanzadas en 2019

Enero de 2024 - actualidad

Desde enero de 2024, AWS Control Tower ha publicado las siguientes actualizaciones:

- AWS Control Tower admite hasta 100 operaciones de control simultáneas
- La Torre de Control de AWS está disponible en el oeste de AWS Canadá (Calgary)
- AWS Control Tower admite los ajustes de cuota de autoservicio
- AWS Control Tower publica la guía de referencia de controles
- AWS Control Tower actualiza y cambia el nombre de dos controles proactivos
- Los controles obsoletos ya no están disponibles
- AWS Control Tower admite el etiquetado de `EnabledControl` recursos en AWS CloudFormation
- AWS Control Tower admite las API para el registro y la configuración de unidades organizativas con líneas base

AWS Control Tower admite hasta 100 operaciones de control simultáneas

20 de mayo de 2024

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite múltiples operaciones de control con una mayor simultaneidad. Puede enviar hasta 100 operaciones de control de la Torre de Control de AWS, en varias unidades organizativas (OU), al mismo tiempo, desde la consola o con las API. Se pueden ejecutar hasta diez (10) operaciones simultáneamente y las adicionales se ponen en cola. De esta forma, puede establecer una configuración más estandarizada en varias operaciones Cuentas de AWS, sin la carga operativa que representan las operaciones de control repetitivas.

Para supervisar el estado de sus operaciones de control en curso y en cola, puede ir a la nueva página de operaciones recientes en la consola de la Torre de Control de AWS o puede llamar a la nueva `ListControlOperations`API.

La biblioteca de la Torre de Control de AWS contiene más de 500 controles, que se asignan a diferentes objetivos, marcos y servicios de control. Para un objetivo de control específico, como cifrar los datos en reposo, puede activar varios controles con una sola operación de control, lo que le ayudará a alcanzar el objetivo. Esta capacidad facilita el desarrollo acelerado, permite una adopción más rápida de los controles de mejores prácticas y mitiga las complejidades operativas.

La Torre de Control de AWS está disponible en el oeste de AWS Canadá (Calgary)

3 de mayo de 2024

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

A partir de hoy, puede activar la Torre de Control de AWS en la región Canadá Oeste (Calgary). Si ya ha implementado AWS Control Tower y desea extender sus funciones de gobierno a esta región, puede hacerlo con las API de zonas de aterrizaje de AWS Control Tower. O bien, desde la consola, vaya a la página de configuración del panel de control de AWS Control Tower, seleccione sus regiones y, a continuación, actualice su landing zone.

La región Canadá Oeste (Calgary) no es compatible AWS Service Catalog. Por este motivo, algunas funciones de la Torre de Control de AWS son diferentes. El cambio de funcionalidad más notable es que Account Factory no está disponible. Si elige Canada West (Calgary) como su región de

origen, los procedimientos para actualizar las cuentas, configurar las automatizaciones de cuentas y cualquier otro proceso que involucre a Service Catalog son diferentes a los de otras regiones.

Aprovisionamiento de cuentas

Para crear y aprovisionar una nueva cuenta en la región Canadá Oeste (Calgary), le recomendamos que cree una cuenta fuera de AWS Control Tower y, a continuación, la inscriba en una OU registrada. Para obtener más información, consulte Inscribir una cuenta existente y Pasos para inscribir una cuenta.

Las API de Service Catalog no están disponibles en la región Canadá Oeste (Calgary). El script de ejemplo que se muestra en Automatizar el aprovisionamiento de cuentas en las API de AWS Control Tower by Service Catalog no funciona.

Account Factory Customizations (AFC), Account Factory for Terraform (AFT) y Customizations for AWS Control Tower (cFCT) no están disponibles en Canadá Occidental (Calgary) debido a la falta de otras dependencias subyacentes de AWS Control Tower. Si amplía la gobernanza a la región Canadá Oeste (Calgary), podrá seguir gestionando los planos de AFC en todas las regiones compatibles con AWS Control Tower, siempre y cuando Service Catalog esté disponible en su región de origen.

Controles

Controles y controles proactivos para el estándar de AWS Security Hub administración de servicios: AWS Control Tower no está disponible en la región Canadá Oeste (Calgary). El control preventivo no `CT.CLOUDFORMATION.PR.1` está disponible en Canada West (Calgary) porque solo es necesario para activar los controles proactivos basados en anzuelos. Algunos controles de detección basados en no AWS Config están disponibles. Para obtener más detalles, consulte Limitaciones de control.

Proveedor de identidad

El centro de identidad de IAM no está disponible en Canada West (Calgary). La mejor práctica recomendada es configurar la landing zone en una región en la que esté disponible el IAM Identity Center. Como alternativa, tiene la opción de gestionar usted mismo la configuración de acceso a su cuenta si utiliza un proveedor de identidad externo en Canada West (Calgary).

La falta de disponibilidad de Service Catalog en la región Canadá Oeste (Calgary) no afecta a las demás regiones compatibles con AWS Control Tower. Estas diferencias solo se aplican si su región de origen es Canadá Oeste (Calgary).

Para obtener una lista completa de las regiones en las que AWS Control Tower está disponible, consulte la tabla de AWS regiones.

AWS Control Tower admite los ajustes de cuota de autoservicio

25 de abril de 2024

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite ajustes de cuotas de autoservicio a través de la consola Service Quotas. Para obtener más información, consulte Solicitud de un aumento de cuota.

AWS Control Tower publica la guía de referencia de controles

21 de abril de 2024

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower publicó la Guía de referencia de controles, un nuevo documento en el que puede encontrar información detallada sobre los controles específicos del entorno de la Torre de Control de AWS. Anteriormente, este material se incluía en la Guía del usuario de AWS Control Tower. La guía de referencia de controles cubre los controles en un formato ampliado. Para obtener más información, consulte la Guía de referencia de controles de la Torre de Control de AWS.

AWS Control Tower actualiza y cambia el nombre de dos controles proactivos

26 de marzo de 2024

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ha cambiado el nombre de dos controles proactivos para adaptarlos a las actualizaciones de Amazon OpenSearch Service.

- [CT.OPENSEARCH.PR.8] Requiere un dominio de Elasticsearch Service para usar TLSv1.2
- [CT.OPENSEARCH.PR.16] Requiere un dominio de Amazon OpenSearch Service para usar TLSv1.2

Hemos actualizado los nombres de los controles y los artefactos de estos dos controles para adaptarlos a la versión reciente de Amazon OpenSearch Service, que ahora es compatible con la

versión 1.3 de Transport Layer Security (TLS) entre sus opciones de seguridad de transporte para la seguridad de puntos finales de dominio.

Para añadir compatibilidad con TLSv1.3 a estos controles, hemos actualizado el artefacto y el nombre de los controles para que reflejen la intención del control. Ahora evalúan la versión TLS mínima del dominio de servicio. Para realizar esta actualización en su entorno, debe deshabilitar y habilitar los controles para implementar el artefacto más reciente.

Este cambio no afecta a ningún otro control proactivo. Le recomendamos que revise estos controles para asegurarse de que cumplen sus objetivos de control.

Si tiene alguna pregunta o duda, póngase en contacto con AWS Support.

Los controles obsoletos ya no están disponibles

12 de marzo de 2024

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ha dejado obsoletos algunos controles. Estos controles ya no están disponibles.

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower admite el etiquetado de **`EnabledControl`** recursos en AWS CloudFormation

22 de febrero de 2024

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

Esta versión de AWS Control Tower actualiza el comportamiento del `EnabledControl` recurso para adaptarlo mejor a los controles configurables y mejorar la capacidad de administrar el

entorno de la Torre de Control de AWS con automatización. Con esta versión, puede añadir etiquetas a `EnabledControl` los recursos configurables mediante AWS CloudFormation plantillas. Anteriormente, solo podía añadir etiquetas a través de la consola y las API de la Torre de Control de AWS.

Las operaciones de la `ListTagsforResource` API y la Torre `GetEnabledControl` de Control de AWS se actualizan con esta versión porque dependen de la funcionalidad de los `EnabledControl` recursos. `EnableControl`

Para obtener más información, consulte `EnabledControl`los recursos de etiquetado en la Torre de Control de AWS y `EnabledControl`en la Guía del AWS CloudFormation usuario.

AWS Control Tower admite las API para el registro y la configuración de unidades organizativas con líneas base

14 de febrero de 2024

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

Estas API permiten el registro programático de la unidad organizativa durante la `EnableBaseline` llamada. Cuando habilita una base en una OU, las cuentas de los miembros de la OU se inscriben en el gobierno de AWS Control Tower. Es posible que se apliquen ciertas advertencias. Por ejemplo, el registro de la OU a través de la consola de la Torre de Control de AWS permite controles opcionales y controles obligatorios. Al llamar a las API, es posible que deba completar un paso adicional para habilitar los controles opcionales.

La base de referencia de AWS Control Tower incorpora las mejores prácticas para la gobernanza de AWS Control Tower de una OU y de las cuentas de los miembros. Por ejemplo, cuando habilita una línea base en una OU, las cuentas de los miembros de la OU reciben un grupo definido de recursos, que incluye AWS CloudTrail el centro de identidad de IAM y las funciones de AWS IAM requeridas. AWS Config

Las líneas base específicas son compatibles con versiones específicas de zonas de aterrizaje de la AWS Control Tower. AWS Control Tower puede aplicar la última línea base compatible a su zona de aterrizaje al cambiar la configuración de la misma. Para obtener más información, consulte Compatibilidad de las versiones de las líneas base y de las zonas de aterrizaje de la OU.

Esta versión incluye cuatro elementos esenciales Tipos de líneas de base

- `AWSControlTowerBaseline`

- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

Con las nuevas API y las líneas base definidas, puede registrar las unidades organizativas y automatizar el flujo de trabajo de aprovisionamiento de unidades organizativas. Las API también pueden administrar las unidades organizativas que ya están bajo el gobierno de la Torre de Control Tower de AWS, de modo que puede volver a registrar las unidades organizativas después de las actualizaciones de landing zone. Las API incluyen soporte para un AWS CloudFormation `EnabledBaseline` recurso que le permite administrar sus unidades organizativas con la infraestructura como código (IaC).

APIs de referencia

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Tome medidas sobre la base de referencia de una unidad organizativa.
- GetEnabledBaseline, ListEnabledBaselines: Descubra las configuraciones para las líneas base habilitadas.
- GetBaselineOperation: Vea el estado de una operación de referencia concreta.
- ResetEnabledBaseline: corrija la desviación de recursos en una unidad organizativa con una línea base habilitada (incluidas las unidades organizativas anidadas y la desviación de control obligatoria). También corrige la desviación para la región, deniega el control landing-zone-level
- GetBaseline, ListBaselines: Descubra el contenido de las líneas base de la Torre de Control de AWS.

Para obtener más información sobre estas API, consulte las líneas de referencia en la Guía del usuario de AWS Control Tower y en la Referencia de API. Las nuevas API están disponibles en los Regiones de AWS lugares donde está disponible la Torre de Control de AWS, excepto en las regiones GovCloud (EE. UU.). Para ver una lista de los Regiones de AWS lugares donde está disponible AWS Control Tower, consulte la Región de AWS tabla.

Enero de 2023: actualidad

Desde enero de 2023, AWS Control Tower ha publicado las siguientes actualizaciones:

- Transición a un nuevo tipo de producto AWS Service Catalog externo (fase 3)

- Versión 3.3 de la zona de aterrizaje de AWS Control Tower
- Transición a un nuevo tipo de producto AWS Service Catalog externo (fase 2)
- AWS Control Tower anuncia controles para ayudar a la soberanía digital
- AWS Control Tower admite las API de landing zone
- AWS Control Tower admite el etiquetado de los controles habilitados
- La Torre de Control de AWS está disponible en la región de Asia Pacífico (Melbourne)
- Transición a un nuevo tipo de producto AWS Service Catalog externo (fase 1)
- Nueva API de control disponible
- AWS Control Tower añade controles adicionales
- Se ha informado de un nuevo tipo de desviación: acceso de confianza desactivado
- Cuatro adicionales Regiones de AWS
- La Torre de Control de AWS está disponible en la región de Tel Aviv
- AWS Control Tower lanza 28 nuevos controles proactivos
- AWS Control Tower deja en desuso dos controles
- Versión 3.2 de la zona de aterrizaje de AWS Control Tower
- AWS Control Tower gestiona las cuentas en función de su ID
- Los controles de detección adicionales de Security Hub están disponibles en la biblioteca de controles de la Torre de Control de AWS
- AWS Control Tower publica tablas de metadatos de control
- Soporte de Terraform para la personalización de Account Factory
- AWS La autogestión del IAM Identity Center está disponible para landing zone
- AWS Control Tower aborda la gobernanza mixta para las unidades organizativas
- Hay controles proactivos adicionales disponibles
- Controles proactivos de Amazon EC2 actualizados
- Regiones de AWS Hay siete más disponibles
- Seguimiento de solicitudes de personalización de cuentas de Account Factory for Terraform (AFT)
- Versión 3.1 de la zona de aterrizaje de AWS Control Tower
- Los controles proactivos están disponibles de forma general

Transición a un nuevo tipo de producto AWS Service Catalog externo (fase 3)

14 de diciembre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ya no admite el código abierto de Terraform como tipo de producto (modelo) al crear nuevos. Cuentas de AWS Para obtener más información e instrucciones sobre cómo actualizar los esquemas de su cuenta, consulte el tipo de producto Transition to the AWS Service Catalog External.

Si no actualiza los planes de su cuenta para utilizar el tipo de producto externo, solo podrá actualizar o cancelar las cuentas que haya aprovisionado mediante los planes de código abierto de Terraform.

Versión 3.3 de la zona de aterrizaje de AWS Control Tower

14 de diciembre de 2023

(Se requiere una actualización para la versión 3.3 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio).

Actualizaciones de la política de cubos de S3 en la cuenta de auditoría de la Torre de Control de AWS

Hemos modificado la política de segmentos de auditoría de Amazon S3 que AWS Control Tower implementa en las cuentas, de modo que se debe cumplir una `aws:SourceOrgID` condición para cualquier permiso de escritura. Con esta versión, AWS los servicios solo tienen acceso a sus recursos cuando la solicitud proviene de su organización o unidad organizativa (OU).

Puede usar la clave de `aws:SourceOrgID` condición y establecer el valor del ID de su organización en el elemento de condición de su política de bucket de S3. Esta condición garantiza que CloudTrail solo pueda escribir registros en nombre de las cuentas de su organización en su bucket de S3; evita que CloudTrail los registros ajenos a su organización se escriban en su bucket de S3 de AWS Control Tower.

Hemos realizado este cambio para corregir una posible vulnerabilidad de seguridad, sin afectar a la funcionalidad de sus cargas de trabajo actuales. Para ver la política actualizada, consulte. Política de bucket de Amazon S3 en la cuenta de auditoría

Para obtener más información sobre la nueva clave de condición, consulte la documentación de IAM y la entrada del blog de IAM titulada «Utilice controles escalables para los AWS servicios que acceden a sus recursos».

Actualizaciones de la política en el tema SNS AWS Config

Hemos agregado la nueva clave de `aws:SourceOrgID` condición a la política del tema de AWS Config SNS. Para ver la política actualizada, consulte la política del tema de SNS. AWS Config

Actualizaciones de la región de landing zone Deny control

- Eliminado`discovery-marketplace:`. Esta acción está cubierta por la `aws-marketplace:*` exención.
- Se ha agregado `quicksight:DescribeAccountSubscription`

AWS CloudFormation Plantilla actualizada

Hemos actualizado la AWS CloudFormation plantilla de la pila nombrada `BASELINE-CLOUDTRAIL-MASTER` para que no muestre desviaciones cuando no se utiliza el AWS KMS cifrado.

Transición a un nuevo tipo de producto AWS Service Catalog externo (fase 2)

7 de diciembre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

HashiCorp actualizaron sus licencias de Terraform. Como resultado, AWS Service Catalog cambiaron el soporte para los productos de código abierto de Terraform y los productos aprovisionados por un nuevo tipo de producto, denominado Externo.

Para evitar interrumpir las cargas de trabajo y AWS los recursos existentes en sus cuentas, siga los pasos de transición de la Torre de Control de AWS que aparecen en la sección Transición al tipo de producto AWS Service Catalog externo antes del 14 de diciembre de 2023.

AWS Control Tower anuncia controles para ayudar a la soberanía digital

27 de noviembre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower anuncia 65 nuevos controles AWS gestionados para ayudarle a cumplir sus requisitos de soberanía digital. Con esta versión, podrá descubrir estos controles en un nuevo grupo de soberanía digital en la consola de la Torre de Control de AWS. Puede usar estos controles para evitar acciones y detectar cambios en los recursos relacionados con la residencia de los datos, la restricción de acceso granular, el cifrado y las capacidades de resiliencia. Estos controles están diseñados para que le resulte más fácil abordar los requisitos a escala. Para obtener más información sobre los controles de soberanía digital, consulte Controles que mejoran la protección de la soberanía digital.

Por ejemplo, puede optar por habilitar controles que ayuden a aplicar sus estrategias de cifrado y resiliencia, como Exigir una caché de AWS AppSync API para habilitar el cifrado en tránsito o Requerir que se implemente un AWS Network Firewall en varias zonas de disponibilidad. También puede personalizar la región de la Torre de Control de AWS (denegar el control) para aplicar las restricciones regionales que mejor se adapten a sus necesidades empresariales específicas.

Esta versión incluye capacidades mejoradas de denegación de regiones de AWS Control Tower. Puedes aplicar un nuevo control de denegación de región parametrizado a nivel de OU para aumentar la granularidad de la gobernanza y, al mismo tiempo, mantener una gobernanza regional adicional a nivel de landing zone. Este control de denegación regional personalizable le ayuda a aplicar las restricciones regionales que mejor se adapten a sus necesidades empresariales específicas. Para obtener más información sobre el nuevo control de denegación regional configurable, consulte el control de denegación regional aplicado a la OU.

Como nueva herramienta para la nueva mejora de denegación regional, esta versión incluye una nueva API que le permite restablecer los controles habilitados a la configuración predeterminada. `UpdateEnabledControl` Esta API resulta especialmente útil en los casos de uso en los que es necesario resolver las desviaciones rápidamente o garantizar mediante programación que un control no se encuentre en estado de desviación. Para obtener más información sobre la nueva API, consulte la referencia de la API de AWS Control Tower

Nuevos controles proactivos

- CT.APIGATEWAY.PR.6: Exija que un dominio REST de Amazon API Gateway utilice una política de seguridad que especifique una versión mínima del protocolo TLS de TLSv1.2
- CT.APPSYNC.PR.2: Requiere que se configure una API de AWS AppSync GraphQL con visibilidad privada
- CT.APPSYNC.PR.3: Exigir que una API de AWS AppSync GraphQL no esté autenticada con claves de API

- CT.APPSYNC.PR.4: Requiere una caché de API AWS AppSync GraphQL para activar el cifrado en tránsito.
- CT.APPSYNC.PR.5: Requiere una caché de API AWS AppSync GraphQL para activar el cifrado en reposo.
- CT.AUTOSCALING.PR.9: Requerir un volumen de Amazon EBS configurado mediante una configuración de lanzamiento de Auto Scaling de Amazon EC2 para cifrar los datos en reposo
- CT.AUTOSCALING.PR.10: Exigir que un grupo de Auto Scaling de Amazon EC2 utilice solo tipos de instancias AWS Nitro al anular una plantilla de lanzamiento
- CT.AUTOSCALING.PR.11: Exija que solo los tipos de instancias AWS Nitro que admitan el cifrado del tráfico de red entre instancias se agreguen a un grupo de Auto Scaling de Amazon EC2, al anular una plantilla de lanzamiento
- CT.DAX.PR.3: Requerir un clúster de DynamoDB Accelerator para cifrar los datos en tránsito con Transport Layer Security (TLS)
- CT.DMS.PR.2: Requerir un punto final del AWS Database Migration Service (DMS) para cifrar las conexiones de los puntos finales de origen y destino
- CT.EC2.PR.15: Exigir que una instancia de Amazon EC2 utilice un tipo de instancia AWS Nitro al crear a partir del tipo de recurso `AWS::EC2::LaunchTemplate`
- CT.EC2.PR.16: Exigir que una instancia Amazon EC2 utilice un tipo de instancia AWS Nitro cuando se cree con el tipo de recurso `AWS::EC2::Instance`
- CT.EC2.PR.17: Requiere un host dedicado de Amazon EC2 para usar un tipo de instancia AWS Nitro
- CT.EC2.PR.18: Exija que una flota de Amazon EC2 anule solo las plantillas de lanzamiento con AWS tipos de instancias Nitro
- CT.EC2.PR.19: Exigir que una instancia Amazon EC2 utilice un tipo de instancia nitro que admita el cifrado en tránsito entre instancias cuando se cree con el tipo de recurso `AWS::EC2::Instance`
- CT.EC2.PR.20: Exija que una flota de Amazon EC2 anule solo las plantillas de lanzamiento con tipos de instancias AWS Nitro que admitan el cifrado en tránsito entre instancias
- CT.ELASTICACHE.PR.8: Requerir un grupo de ElastiCache replicación de Amazon de versiones posteriores de Redis para activar la autenticación RBAC
- CT.MQ.PR.1: Exija a un agente ActiveMQ de Amazon MQ que utilice el modo de implementación activo/en espera para obtener una alta disponibilidad

- CT.MQ.PR.2: Exija a un agente MQ de Amazon MQ Rabbit que utilice el modo de clúster Multi-AZ para obtener una alta disponibilidad
- CT.MSK.PR.1: Requerir un clúster Amazon Managed Streaming for Apache Kafka (MSK) para aplicar el cifrado en tránsito entre los nodos del intermediario del clúster
- CT.MSK.PR.2: Requiere que un clúster de Amazon Managed Streaming for Apache Kafka (MSK) esté configurado con deshabilitado PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Exigir AWS la implementación de un firewall de Network Firewall en varias zonas de disponibilidad
- CT.RDS.PR.26: Requerir un proxy de base de datos Amazon RDS para requerir conexiones de Transport Layer Security (TLS)
- CT.RDS.PR.27: Requerir un grupo de parámetros de clúster de base de datos de Amazon RDS para requerir conexiones de seguridad de capa de transporte (TLS) para los tipos de motores compatibles
- CT.RDS.PR.28: Requerir un grupo de parámetros de base de datos de Amazon RDS para requerir conexiones de seguridad de capa de transporte (TLS) para los tipos de motores compatibles
- CT.RDS.PR.29: Exigir que un clúster de Amazon RDS no esté configurado para que sea de acceso público mediante la propiedad 'PubliclyAccessible'
- CT.RDS.PR.30: Exija que una instancia de base de datos de Amazon RDS tenga el cifrado en reposo configurado para usar una clave de KMS que especifique para los tipos de motores compatibles
- CT.S3.PR.12: Exigir que un punto de acceso Amazon S3 tenga una configuración de acceso público en bloque (BPA) con todas las opciones configuradas como true

Nuevos controles preventivos

- CT.APPSYNC.PV.1Exigir que una API de AWS AppSync GraphQL esté configurada con visibilidad privada
- CT.EC2.PV.1Requerir que se cree una instantánea de Amazon EBS a partir de un volumen EC2 cifrado
- CT.EC2.PV.2Exija que un volumen de Amazon EBS adjunto esté configurado para cifrar los datos en reposo
- CT.EC2.PV.3Exigir que una instantánea de Amazon EBS no pueda restaurarse públicamente
- CT.EC2.PV.4Exigir que no se llame a las API directas de Amazon EBS

- CT.EC2.PV.5No permitir el uso de la importación y exportación de máquinas virtuales Amazon EC2
- CT.EC2.PV.6No permitir el uso de acciones de Amazon RequestSpotFleet RequestSpotInstances EC2 y API obsoletas
- CT.KMS.PV.1Exija que una política AWS KMS clave incluya una declaración que limite la creación de AWS KMS subvenciones a los servicios AWS
- CT.KMS.PV.2Exija que una clave AWS KMS asimétrica con material de clave RSA que se utilice para el cifrado no tenga una longitud de clave de 2048 bits
- CT.KMS.PV.3Exija que la AWS KMS clave esté configurada con la comprobación de seguridad de bloqueo por política de elusión activada
- CT.KMS.PV.4Exigir que una clave AWS KMS gestionada por el cliente (CMK) esté configurada con material clave originado en CloudHSM AWS
- CT.KMS.PV.5Exija que una clave AWS KMS gestionada por el cliente (CMK) esté configurada con material clave importado
- CT.KMS.PV.6Exija que una clave AWS KMS gestionada por el cliente (CMK) esté configurada con material clave procedente de un almacén de claves externo (XKS)
- CT.LAMBDA.PV.1Requiere una URL de AWS Lambda función para usar la autenticación basada en IAM AWS
- CT.LAMBDA.PV.2Requiere que AWS Lambda la URL de una función esté configurada para que solo puedan acceder a ella los directores de su Cuenta de AWS
- CT.MULTISERVICE.PV.1: Denegar el acceso a una unidad organizativa AWS en función de lo solicitado Región de AWS

Los nuevos controles de detección que mejoran su postura de gobernanza de la soberanía digital forman parte del estándar de administración de AWS Security Hub servicios (AWS Control Tower).

Nuevos controles detectivescos

- SH.ACM.2: Los certificados RSA administrados por ACM deben utilizar una longitud de clave de al menos 2048 bits
- SH.AppSync.5: Las API de AWS AppSync GraphQL no deben autenticarse con claves de API
- SH.CloudTrail.6: Asegúrese de que el depósito de S3 utilizado para almacenar CloudTrail los registros no sea de acceso público:
- SH.DMS.9: Los puntos de conexión del DMS deben usar SSL

- SH.DocumentDB.3: Las instantáneas de clústeres manuales de Amazon DocumentDB no deben ser públicas
- SH.DynamoDB.3: Los clústeres de DynamoDB Accelerator (DAX) deben cifrarse en reposo
- SH.EC2.23: Las pasarelas de tránsito de EC2 no deberían aceptar automáticamente las solicitudes de adjuntos de VPC
- SH.EKS.1: Los puntos finales del clúster EKS no deben ser de acceso público
- SH.ElastiCache.3: los grupos ElastiCache de replicación deben tener habilitada la conmutación por error automática
- SH.ElastiCache.4: los grupos ElastiCache de replicación deberían estar habilitados encryption-at-rest
- SH.ElastiCache.5: los grupos de ElastiCache replicación deberían estar encryption-in-transit habilitados
- SH.ElastiCache.6: los grupos de ElastiCache replicación de versiones anteriores de Redis deberían tener habilitada la autenticación de Redis
- SH.EventBridge.3: los buses EventBridge de eventos personalizados deben tener adjunta una política basada en los recursos
- SH.KMS.4: la rotación de AWS KMS claves debe estar habilitada
- SH.Lambda.3: Las funciones Lambda deben estar en una VPC
- SH.MQ.5: Los corredores de ActiveMQ deberían utilizar el modo de despliegue activo/en espera
- SH.MQ.6: Los corredores de RabbitMQ deberían usar el modo de despliegue de clústeres
- SH.MSK.1: Los clústeres de MSK deben cifrarse en tránsito entre los nodos de los corredores
- SH.RDS.12: La autenticación de IAM debe configurarse para los clústeres de RDS
- SH.RDS.15: Los clústeres de bases de datos de RDS deben configurarse para varias zonas de disponibilidad
- SH.S3.17: Los cubos S3 deben cifrarse en reposo con claves AWS KMS

Para obtener más información sobre los controles añadidos al estándar AWS Security Hub gestionado por servicios (AWS Control Tower), consulte Controles que se aplican al estándar gestionado por servicios: AWS Control Tower en la documentación. AWS Security Hub

Para ver una lista de los controles Regiones de AWS que no son compatibles con determinados controles que forman parte del estándar AWS Control Tower AWS Security Hub , gestionado por servicios, consulte Regiones no compatibles.

Nuevo control configurable para la denegación de regiones a nivel de unidad organizativa

CT.MULTISERVICE.PV.1: Este control acepta parámetros para especificar las regiones, los principios de IAM y las acciones exentas que están permitidos, a nivel de unidad organizativa, en lugar de en toda la zona de aterrizaje de AWS Control Tower. Se trata de un control preventivo, que se implementa mediante la política de control de servicios (SCP).

Para obtener más información, consulte el control de denegación regional aplicado a la OU.

La API de **`UpdateEnabledControl`**

Esta versión de AWS Control Tower añade la siguiente compatibilidad con las API para los controles:

- La `EnableControl` API actualizada puede configurar controles que son configurables.
- La `GetEnabledControl` API actualizada muestra los parámetros configurados en un control habilitado.
- La nueva `UpdateEnabledControl` API puede cambiar los parámetros de un control habilitado.

Para obtener más información, consulte la referencia de la API de AWS Control Tower.

AWS Control Tower admite las API de landing zone

26 de noviembre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite la configuración y el lanzamiento de las zonas de landing zone mediante API. Puede crear, actualizar, obtener, enumerar, restablecer y eliminar zonas de aterrizaje mediante las API.

Las siguientes API te permiten configurar y gestionar tu landing zone de forma programática mediante AWS CloudFormation o el AWS CLI.

AWS Control Tower admite las siguientes API para las zonas de aterrizaje:

- `CreateLandingZone`—Esta llamada a la API crea una zona de aterrizaje mediante una versión de landing zone y un archivo de manifiesto.
- `GetLandingZoneOperation`—Esta llamada a la API devuelve el estado de una operación de landing zone específica.

- `GetLandingZone`—Esta llamada a la API devuelve detalles sobre la landing zone especificada, incluida la versión, el archivo de manifiesto y el estado.
- `UpdateLandingZone`—Esta llamada a la API actualiza la versión de la zona de aterrizaje o el archivo de manifiesto.
- `ListLandingZone`—Esta llamada a la API devuelve un identificador de zona de aterrizaje (ARN) para una configuración de zona de aterrizaje en la cuenta de gestión.
- `ResetLandingZone`—Esta llamada a la API restablece la zona de aterrizaje a los parámetros especificados en la última actualización, lo que puede reparar la deriva. Si la zona de aterrizaje no se ha actualizado, esta llamada restablece la zona de aterrizaje a los parámetros especificados en la creación.
- `DeleteLandingZone`—Esta llamada a la API retira del servicio la landing zone.

Para empezar a utilizar las API de landing zone, consulta laCómo empezar a utilizar AWS Control Tower mediante las API.

AWS Control Tower admite el etiquetado de los controles habilitados

10 de noviembre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite el etiquetado de recursos para los controles habilitados, desde la consola de AWS Control Tower o mediante API. Puede añadir, eliminar o enumerar las etiquetas de los controles habilitados.

Con el lanzamiento de las siguientes API, puede configurar etiquetas para los controles que habilita en AWS Control Tower. Las etiquetas son útiles a la hora de administrar, identificar, organizar, buscar y filtrar recursos. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio.

AWS Control Tower admite las siguientes API para el etiquetado de control:

- `TagResource`—Esta llamada a la API agrega etiquetas a los controles habilitados en AWS Control Tower.
- `UntagResource`—Esta llamada a la API elimina las etiquetas de los controles habilitados en AWS Control Tower.
- `ListTagsForResource`—Esta llamada a la API devuelve etiquetas de los controles habilitados en AWS Control Tower.

Las API de control de AWS Control Tower están disponibles en los Regiones de AWS lugares donde está disponible AWS Control Tower. Para obtener una lista completa de los Regiones de AWS lugares en los que está disponible la Torre de Control de AWS, consulte la tabla de AWS regiones. Para obtener una lista completa de las API de AWS Control Tower, consulte la Referencia de API.

La Torre de Control de AWS está disponible en la región de Asia Pacífico (Melbourne)

3 de noviembre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower está disponible en la región Asia Pacífico (Melbourne).

Si ya utiliza AWS Control Tower y desea extender sus funciones de gobierno a esta región en sus cuentas, vaya a la página de configuración del panel de control de AWS Control Tower, seleccione la región y, a continuación, actualice su zona de aterrizaje. Tras una actualización de la zona de aterrizaje, debe actualizar todas las cuentas que estén gobernadas por AWS Control Tower para que sus cuentas y unidades organizativas estén bajo el control de la nueva región. Para obtener más información, consulte Acerca de las actualizaciones.

Para ver una lista completa de las regiones en las que está disponible AWS Control Tower, consulte la Región de AWS tabla.

Transición a un nuevo tipo de producto AWS Service Catalog externo (fase 1)

31 de octubre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

HashiCorp actualizaron sus licencias de Terraform. Como resultado, AWS Service Catalog actualizaron el soporte para los productos de código abierto de Terraform y los aprovisionaron a un nuevo tipo de producto, denominado Externo.

AWS Control Tower no admite las personalizaciones de Account Factory que dependan del tipo de producto AWS Service Catalog externo. Para evitar interrumpir las cargas de trabajo y AWS los recursos existentes en sus cuentas, siga los pasos de transición de la Torre de Control de AWS en este orden sugerido, antes del 14 de diciembre de 2023:

1. Actualice su motor de referencia de Terraform actual para AWS Service Catalog incluir soporte para los tipos de productos externos y de código abierto de Terraform. Para obtener instrucciones sobre cómo actualizar su motor de referencia de Terraform, consulte el repositorio.AWS Service Catalog GitHub
2. Ve a cualquier plano de código abierto de Terraform existente AWS Service Catalog y duplícalo para usar el nuevo tipo de producto externo. No cancele los planos de código abierto de Terraform existentes.
3. Siga utilizando sus planos de código abierto de Terraform existentes para crear o actualizar cuentas en AWS Control Tower.

Nueva API de control disponible

14 de octubre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite una API adicional que puede usar para implementar y administrar los controles de la Torre de Control de AWS a escala. Para obtener más información sobre las API de control de la Torre de Control de AWS, consulte la Referencia de API.

AWS Control Tower agregó una nueva API de control.

- `GetEnabledControl`—La llamada a la API proporciona detalles sobre un control habilitado.

También actualizamos esta API:

`ListEnabledControls`—Esta llamada a la API muestra los controles habilitados por AWS Control Tower en la unidad organizativa especificada y las cuentas que contiene. Ahora devuelve información adicional de un `EnabledControlSummary` objeto.

Con estas API, puede realizar varias operaciones comunes mediante programación. Por ejemplo:

- Obtenga una lista de todos los controles que ha activado en la biblioteca de controles de la Torre de Control de AWS.
- Para cualquier control habilitado, puede obtener información sobre las regiones en las que se admite el control, el identificador del control (ARN), el estado de desviación del control y el resumen del estado del control.

Las API de control de AWS Control Tower están disponibles en los Regiones de AWS lugares donde está disponible AWS Control Tower. Para obtener una lista completa de los Regiones de AWS lugares en los que está disponible la Torre de Control de AWS, consulte la tabla de AWS regiones. Para obtener una lista completa de las API de AWS Control Tower, consulte la Referencia de API.

AWS Control Tower añade controles adicionales

5 de octubre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower anuncia nuevos controles proactivos y de detección.

Los controles proactivos de AWS Control Tower se implementan mediante AWS CloudFormation Hooks, que identifican y bloquean los recursos no conformes antes de AWS CloudFormation aprovisionarlos. Los controles proactivos complementan las capacidades de control preventivo y de detección existentes en AWS Control Tower.

Nuevos controles proactivos

- [CT.ATHENA.PR.1] Requerir un grupo de trabajo de Amazon Athena para cifrar los resultados de las consultas de Athena en reposo
- [CT.ATHENA.PR.2] Requerir que un grupo de trabajo de Amazon Athena cifre los resultados de las consultas de Athena en reposo con una clave (KMS) AWS Key Management Service
- [CT.CLOUDTRAIL.PR.4] Requiere un almacén de datos de eventos de AWS CloudTrail Lake para permitir el cifrado en reposo con una clave AWS KMS
- [CT.DAX.PR.2] Requiere un clúster de Amazon DAX para implementar nodos en al menos tres zonas de disponibilidad
- [CT.EC2.PR.14] Requerir un volumen de Amazon EBS configurado mediante una plantilla de lanzamiento de Amazon EC2 para cifrar los datos en reposo
- [CT.EKS.PR.2] Exigir que un clúster de Amazon EKS se configure con cifrado secreto mediante AWS claves del Servicio de administración de claves (KMS)
- [CT.ELASTICLOADBALANCING.PR.14] Requiere un Network Load Balancer para activar el equilibrio de carga entre zonas
- [CT.ELASTICLOADBALANCING.PR.15] Exigir que un grupo objetivo de Elastic Load Balancing v2 no deshabilite explícitamente el equilibrio de carga entre zonas

- [CT.EMR.PR.1] Exigir que se configure una configuración de seguridad de Amazon EMR (EMR) para cifrar los datos en reposo en Amazon S3
- [CT.EMR.PR.2] Exigir que se configure una configuración de seguridad de Amazon EMR (EMR) para cifrar los datos en reposo en Amazon S3 con una clave AWS KMS
- [CT.EMR.PR.3] Exigir que la configuración de seguridad de Amazon EMR (EMR) esté configurada con el cifrado del disco local por volumen de EBS mediante una clave AWS KMS
- [CT.EMR.PR.4] Exigir que se configure una configuración de seguridad de Amazon EMR (EMR) para cifrar los datos en tránsito
- [CT.GLUE.PR.1] Requiere un trabajo de AWS Glue para tener una configuración de seguridad asociada
- [CT.GLUE.PR.2] Requiere una configuración de seguridad de AWS Glue para cifrar los datos en los destinos de Amazon S3 mediante claves de AWS KMS
- [CT.KMS.PR.2] Exija que una clave AWS KMS asimétrica con material de clave RSA utilizada para el cifrado tenga una longitud de clave superior a 2048 bits
- [CT.KMS.PR.3] Exija que una política AWS KMS clave incluya una declaración que limite la creación de AWS KMS subvenciones a los servicios AWS
- [CT.LAMBDA.PR.4] Requiere un permiso de AWS Lambda capa para conceder acceso a una AWS organización o AWS cuenta específica
- [CT.LAMBDA.PR.5] Se requiere una URL de AWS Lambda función para usar la autenticación basada AWS en IAM
- [CT.LAMBDA.PR.6] Requiere una política CORS de URL de AWS Lambda función para restringir el acceso a orígenes específicos
- [CT.NEPTUNE.PR.4] Requiere un clúster de base de datos de Amazon Neptune para permitir la exportación de registros de Amazon para CloudWatch registros de auditoría
- [CT.NEPTUNE.PR.5] Exija un clúster de base de datos de Amazon Neptune para establecer un período de retención de copias de seguridad superior o igual a siete días
- [CT.REDSHIFT.PR.9] Exigir que un grupo de parámetros de clúster de Amazon Redshift esté configurado para utilizar Secure Sockets Layer (SSL) para el cifrado de los datos en tránsito

Estos nuevos controles proactivos están disponibles en tiendas Regiones de AWS donde AWS Control Tower está disponible. Para obtener más información sobre estos controles, consulte Controles proactivos. Para obtener más información sobre dónde están disponibles los controles, consulte Limitaciones de control.

Nuevos controles de detección

Se agregaron nuevos controles al estándar gestionado por el servicio Security Hub: AWS Control Tower. Estos controles le ayudan a mejorar su postura de gobierno. Actúan como parte del estándar gestionado por el servicio Security Hub: AWS Control Tower, después de habilitarlos en una unidad organizativa específica.

- [SH.Athena.1] Los grupos de trabajo de Athena deben estar cifrados en reposo
- [SH.Neptune.1] Los clústeres de bases de datos de Neptune deben cifrarse en reposo
- [SH.Neptune.2] Los clústeres de bases de datos de Neptune deberían publicar registros de auditoría en Logs CloudWatch
- [SH.Neptune.3] Las instantáneas del clúster de base de datos de Neptune no deben ser públicas
- [SH.Neptune.4] Los clústeres de base de datos de Neptune deben tener habilitada la protección contra eliminación
- [SH.Neptune.5] Los clústeres de Neptune DB deberían tener habilitadas las copias de seguridad automatizadas
- [SH.Neptune.6] Las instantáneas del clúster de base de datos de Neptune deben cifrarse en reposo
- [SH.Neptune.7] Los clústeres de base de datos de Neptune deben tener habilitada la autenticación de bases de datos de IAM
- [SH.Neptune.8] Los clústeres de bases de datos de Neptune deben configurarse para copiar etiquetas a las instantáneas
- [SH.RDS.27] Los clústeres de bases de datos de RDS deben cifrarse en reposo

Los nuevos controles AWS Security Hub de detección están disponibles en la mayoría de los Regiones de AWS lugares donde AWS Control Tower está disponible. Para obtener más información sobre estos controles, consulte Controles que se aplican al estándar gestionado por servicios: AWS Control Tower. Para obtener más información sobre dónde están disponibles los controles, consulte. Limitaciones de control

Se ha informado de un nuevo tipo de desviación: acceso de confianza desactivado

21 de septiembre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

Después de configurar la zona de aterrizaje de la Torre de Control de AWS, puede deshabilitar el acceso de confianza a la Torre de Control de AWS en AWS Organizations. Sin embargo, si lo hace, se produce una desviación.

Con el tipo de deriva desactivado con acceso confiable, AWS Control Tower le notifica cuando se produce este tipo de deriva para que pueda reparar la zona de aterrizaje de su AWS Control Tower. Para obtener más información, consulte Tipos de cambios en la gobernanza.

Cuatro adicionales Regiones de AWS

13 de septiembre de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ya está disponible en Asia Pacífico (Hyderabad), Europa (España y Zúrich) y Oriente Medio (Emiratos Árabes Unidos).

Si ya utiliza AWS Control Tower y desea extender sus funciones de gobierno a esta región en sus cuentas, vaya a la página de configuración del panel de control de AWS Control Tower, seleccione la región y, a continuación, actualice su zona de aterrizaje. Tras una actualización de la zona de aterrizaje, debe actualizar todas las cuentas que estén gobernadas por AWS Control Tower para que sus cuentas y unidades organizativas estén bajo el control de la nueva región. Para obtener más información, consulte Acerca de las actualizaciones.

Para ver una lista completa de las regiones en las que está disponible AWS Control Tower, consulte la Región de AWS tabla.

La Torre de Control de AWS está disponible en la región de Tel Aviv

28 de agosto de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower anuncia su disponibilidad en la región de Israel (Tel Aviv).

Si ya utiliza AWS Control Tower y desea extender sus funciones de gobierno a esta región en sus cuentas, vaya a la página de configuración del panel de control de AWS Control Tower, seleccione la región y, a continuación, actualice su zona de aterrizaje. Tras una actualización de la zona de aterrizaje, debe actualizar todas las cuentas que estén gobernadas por AWS Control Tower para que

sus cuentas y unidades organizativas estén bajo el control de la nueva región. Para obtener más información, consulte Acerca de las actualizaciones.

Para ver una lista completa de las regiones en las que está disponible AWS Control Tower, consulte la Región de AWS tabla.

AWS Control Tower lanza 28 nuevos controles proactivos

24 de julio de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower añade 28 nuevos controles proactivos para ayudarlo a administrar su AWS entorno.

Los controles proactivos mejoran las capacidades de gobierno de AWS Control Tower en sus AWS entornos de múltiples cuentas, al bloquear los recursos no conformes antes de que se aprovisionen. Estos controles ayudan a administrar AWS servicios como Amazon CloudWatch, Amazon Neptune, Amazon y Amazon ElastiCache AWS Step Functions DocumentDB. Los nuevos controles le ayudan a cumplir los objetivos de control, como establecer el registro y la supervisión, cifrar los datos en reposo o mejorar la resiliencia.

Esta es una lista completa de los nuevos controles:

- [CT.APPSYNC.PR.1] Requiere una API de AWS AppSync GraphQL para activar el registro
- [CT.CLOUDWATCH.PR.1] Requiere que una alarma de CloudWatch Amazon tenga una acción configurada para el estado de alarma
- [CT.CLOUDWATCH.PR.2] Exigir que un grupo de registros de CloudWatch Amazon se conserve durante al menos un año
- [CT.CLOUDWATCH.PR.3] Exigir que un grupo de registros de CloudWatch Amazon esté cifrado en reposo con una clave KMS AWS
- [CT.CLOUDWATCH.PR.4] Requiere que se active una acción de alarma de Amazon CloudWatch
- [CT.DOCUMENTDB.PR.1] Exigir que un clúster de Amazon DocumentDB esté cifrado en reposo
- [CT.DOCUMENTDB.PR.2] Requiere que un clúster de Amazon DocumentDB tenga habilitadas las copias de seguridad automáticas
- [CT.DYNAMODB.PR.2] Exigir que una tabla de Amazon DynamoDB se cifre en reposo mediante claves AWS KMS

- [CT.EC2.PR.13] Requiere que una instancia de Amazon EC2 tenga habilitada la supervisión detallada
- [CT.EKS.PR.1] Exigir que un clúster de Amazon EKS esté configurado con el acceso público desactivado al punto final del servidor API de Kubernetes del clúster
- [CT.ELASTICACHE.PR.1] Requiere que un clúster de ElastiCache Amazon for Redis tenga activadas las copias de seguridad automáticas
- [CT.ELASTICACHE.PR.2] Requiere que un clúster de ElastiCache Amazon for Redis tenga activadas las actualizaciones automáticas de las versiones secundarias
- [CT.ELASTICACHE.PR.3] Exigir que un grupo de replicación de ElastiCache Amazon for Redis tenga activada la conmutación por error automática
- [CT.ELASTICACHE.PR.4] Exigir que un grupo de replicación de ElastiCache Amazon tenga activado el cifrado en reposo
- [CT.ELASTICACHE.PR.5] Exigir que un grupo de replicación de ElastiCache Amazon for Redis tenga activado el cifrado en tránsito
- [CT.ELASTICACHE.PR.6] Requiere un clúster de caché de ElastiCache Amazon para usar un grupo de subredes personalizado
- [CT.ELASTICACHE.PR.7] Requiere un grupo de replicación de ElastiCache Amazon de versiones anteriores de Redis para tener la autenticación AUTH de Redis
- [CT.ELASTICBEANSTALK.PR.3] Requiere un entorno de AWS Elastic Beanstalk para tener una configuración de registro
- [CT.LAMBDA.PR.3] Requiere que una AWS Lambda función esté en una Amazon Virtual Private Cloud (VPC) gestionada por el cliente
- [CT.NEPTUNE.PR.1] Requiere que un clúster de base de datos de Amazon Neptune tenga autenticación de base de datos (IAM) AWS Identity and Access Management
- [CT.NEPTUNE.PR.2] Requiere que un clúster de base de datos de Amazon Neptune tenga habilitada la protección de eliminación
- [CT.NEPTUNE.PR.3] Requiere que un clúster de base de datos de Amazon Neptune tenga habilitado el cifrado de almacenamiento
- [CT.REDSHIFT.PR.8] Requerir cifrar un clúster de Amazon Redshift
- [CT.S3.PR.9] Requiere que un bucket de Amazon S3 tenga activado el bloqueo de objetos S3
- [CT.S3.PR.10] Requiere que un bucket de Amazon S3 tenga el cifrado del lado del servidor configurado mediante claves AWS KMS

- [CT.S3.PR.11] Requiere que un bucket de Amazon S3 tenga habilitado el control de versiones
- [CT.STEPFUNCTIONS.PR.1] Requiere que una máquina de estados tenga el registro activado AWS Step Functions
- [CT.STEPFUNCTIONS.PR.2] Requiere que una máquina de estados tenga activado el rastreo AWS Step Functions AWS X-Ray

Los controles proactivos de AWS Control Tower se implementan mediante AWS CloudFormation Hooks, que identifican y bloquean los recursos no conformes antes de AWS CloudFormation aprovisionarlos. Los controles proactivos complementan las capacidades de control preventivo y de detección existentes en AWS Control Tower.

Estos nuevos controles proactivos están disponibles en todos los Regiones de AWS lugares donde AWS Control Tower esté disponible. Para obtener más información sobre estos controles, consulte Controles proactivos.

AWS Control Tower deja en desuso dos controles

18 de julio de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower lleva a cabo revisiones periódicas de sus controles de seguridad para garantizar que estén actualizados y que sigan considerándose prácticas recomendadas. Los dos controles siguientes han quedado obsoletos, con efecto a partir del 18 de julio de 2023, y se eliminarán de la biblioteca de controles a partir del 18 de agosto de 2023. Ya no puedes activar estos controles en ninguna unidad organizativa. Puedes optar por desactivar estos controles antes de la fecha de retirada.

- [SH.S3.4] Los buckets S3 deben tener habilitado el cifrado del lado del servidor
- [CT.S3.PR.7] Requiere que un bucket de Amazon S3 tenga configurado el cifrado del lado del servidor

Motivo de la obsolescencia

A partir de enero de 2023, Amazon S3 configuró el cifrado predeterminado en todos los buckets no cifrados nuevos y existentes para aplicar el cifrado del lado del servidor con claves administradas de S3 (SSE-S3) como nivel base de cifrado para los nuevos objetos cargados en estos buckets. No se

ha realizado ningún cambio en la configuración de cifrado predeterminada de un depósito existente que ya tenía configurado el SSE-S3 o el cifrado del lado del servidor con AWS claves del Servicio de administración de claves (KMS) (SSE-KMS).AWS

Versión 3.2 de la zona de aterrizaje de AWS Control Tower

16 de junio de 2023

(Se requiere una actualización para la versión 3.2 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio).

La versión 3.2 de la zona de aterrizaje de AWS Control Tower pone a disposición del público general los controles que forman parte del estándar AWS Security Hub gestionado por servicios: AWS Control Tower. Introduce la posibilidad de ver el estado de desviación de los controles que forman parte de este estándar en la consola de la Torre de Control de AWS.

Esta actualización incluye un nuevo rol vinculado a un servicio (SLR), denominado. AWSServiceRoleForAWSControlTower Esta función ayuda a AWS Control Tower a crear una regla EventBridge gestionada, denominada AWSControlTowerManagedRuleen la cuenta de cada miembro. Esta regla administrada recopila los eventos de AWS Security Hub búsqueda, ya que con AWS Control Tower se puede determinar la desviación de control.

Esta regla es la primera regla administrada que crea AWS Control Tower. La regla no se implementa mediante una pila, sino que se implementa directamente desde las EventBridge API. Puede ver la regla en la EventBridge consola o mediante las EventBridge API. Si el `managed-by` campo está completo, se mostrará el director de servicio de la Torre de Control de AWS.

Anteriormente, AWS Control Tower asumía la AWSControlTowerExecutionfunción de realizar operaciones en las cuentas de los miembros. Este nuevo rol y esta nueva regla están mejor alineados con el principio de mejores prácticas de permitir el mínimo de privilegios al realizar operaciones en un AWS entorno de múltiples cuentas. La nueva función proporciona permisos restringidos que permiten específicamente: crear la regla administrada en las cuentas de los miembros, mantener la regla administrada, publicar notificaciones de seguridad a través de las redes sociales y verificar las desviaciones. Para obtener más información, consulte AWSServiceRoleForAWSControlTower.

La actualización 3.2 de landing zone también incluye un nuevo StackSet recurso en la cuenta de administraciónBP_BASELINE_SERVICE_LINKED_ROLE, que inicialmente despliega la función vinculada al servicio.

Cuando se informa de una desviación de control del Security Hub (en la zona de aterrizaje 3.2 y versiones posteriores), AWS Control Tower recibe una actualización de estado diaria de Security Hub. Aunque los controles están activos en todas las regiones gobernadas, la Torre de Control de AWS envía los eventos AWS Security Hub Finding únicamente a la región de origen de la Torre de Control de AWS. Para obtener más información, consulte Informes de desviaciones de control de Security Hub.

Actualización de la región: deniega el control

Esta versión de landing zone también incluye una actualización del control Region Deny.

Se agregaron servicios y API globales

- AWS Billing and Cost Management (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) para permitir la visibilidad de los eventos globales en las cuentas de los miembros.
- AWS Facturación unificada (`consolidatedbilling:*`)
- AWS Aplicación Mobile Console (`consoleapp:*`)
- AWS Nivel gratuito (`freetier:*`)
- Facturación de AWS (`invoicing:*`)
- AWS IQ (`iq:*`)
- AWS Notificaciones de usuario (`notifications:*`)
- AWS Contactos de notificaciones de usuario (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS Configuración fiscal (`tax:*`)

Se eliminaron los servicios y las API globales

- Se ha eliminado `s3:GetAccountPublic` porque no es una acción válida.
- Se ha eliminado `s3:PutAccountPublic` porque no es una acción válida.

AWS Control Tower gestiona las cuentas en función de su ID

14 de junio de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora crea y administra las cuentas que usted crea en Account Factory mediante el seguimiento del ID de la AWS cuenta, en lugar de la dirección de correo electrónico de la cuenta.

Al aprovisionar una cuenta, el solicitante de la cuenta siempre debe tener los permisos `CreateAccount` y los `DescribeCreateAccountStatus` permisos. Este conjunto de permisos forma parte de la función de administrador y se otorga automáticamente cuando el solicitante asume la función de administrador. Si delegas el permiso para aprovisionar cuentas, es posible que tengas que añadir estos permisos directamente a los solicitantes de la cuenta.

Los controles de detección adicionales de Security Hub están disponibles en la biblioteca de controles de la Torre de Control de AWS

12 de junio de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ha añadido diez nuevos AWS Security Hub controles de detección a la biblioteca de controles de la Torre de Control de AWS. Estos nuevos controles se dirigen a servicios como API Gateway AWS CodeBuild, Amazon Elastic Compute Cloud (EC2), Amazon Elastic Load Balancer, Amazon Redshift, Amazon y. SageMaker AWS WAF Estos nuevos controles lo ayudan a mejorar su postura de gobierno al cumplir con los objetivos de control, como establecer el registro y la supervisión, limitar el acceso a la red y cifrar los datos en reposo.

Estos controles actúan como parte del estándar gestionado por el servicio Security Hub: AWS Control Tower, después de habilitarlos en una unidad organizativa específica.

- [Sh.Account.1] La información de contacto de seguridad debe proporcionarse para un Cuenta de AWS
- [SH.APIGateway.8] Las rutas de API Gateway deben especificar un tipo de autorización
- [SH.APIGateway.9] El registro de acceso debe configurarse para las etapas V2 de API Gateway
- [SH. CodeBuild.3] Los registros de CodeBuild S3 deben estar cifrados
- [SH.EC2.25] Las plantillas de lanzamiento de EC2 no deben asignar direcciones IP públicas a las interfaces de red
- [SH.ELB.1] Application Load Balancer debe configurarse para redirigir todas las solicitudes HTTP a HTTPS
- [Sh.redshift.10] Los clústeres de Redshift deben cifrarse en reposo

- [SH. SageMaker.2] las instancias de SageMaker notebook deberían lanzarse en una VPC personalizada
- [SH. SageMaker.3] Los usuarios no deberían tener acceso root a las instancias de SageMaker notebook
- [SH.WAF.10] Una ACL web de WAFV2 debe tener al menos una regla o grupo de reglas

Los nuevos controles AWS Security Hub de detección están disponibles en todos los Regiones de AWS lugares donde esté disponible la Torre de Control de AWS. Para obtener más información sobre estos controles, consulte Controles que se aplican al estándar gestionado por servicios: AWS Control Tower.

AWS Control Tower publica tablas de metadatos de control

7 de junio de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora incluye tablas completas de metadatos de control como parte de la documentación publicada. Al trabajar con las API de control, puede buscar el ControlIdentifier de la API de cada control, que es un ARN único asociado a cada una. Región de AWS Las tablas incluyen los marcos y los objetivos de control que cubre cada control. Anteriormente, esta información solo estaba disponible en la consola.

Las tablas también incluyen los metadatos de los controles de Security Hub que forman parte del estándar de administración de AWS Security Hub servicios: AWS Control Tower. Para obtener más información, consulte Tablas de metadatos de control.

Para ver una lista abreviada de identificadores de control y algunos ejemplos de uso, consulta Identificadores de recursos para API y controles.

Soporte de Terraform para la personalización de Account Factory

6 de junio de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ofrece soporte en una sola región para Terraform mediante Account Factory Customization (AFC). A partir de esta versión, puede usar AWS Control Tower y Service Catalog

juntos para definir los planos de cuentas de AFC en el código abierto de Terraform. Puede personalizar sus recursos nuevos y existentes Cuentas de AWS antes de aprovisionar recursos en AWS Control Tower. De forma predeterminada, esta función le permite implementar y actualizar cuentas, con Terraform, en su región de origen de la Torre de Control de AWS.

Un plan de cuenta describe los recursos y las configuraciones específicos que se requieren cuando se aprovisiona una Cuenta de AWS . Puede utilizar el plano como plantilla para crear varios Cuentas de AWS a escala.

Para empezar, utilice el motor de referencia de Terraform en. GitHub El motor de referencia configura el código y la infraestructura necesarios para que el motor de código abierto de Terraform funcione con Service Catalog. Este proceso de configuración único tarda unos minutos. Después, puede definir los requisitos de sus cuentas personalizadas en Terraform y, a continuación, implementarlas con el flujo de trabajo bien definido de fábrica de cuentas de AWS Control Tower. Los clientes que prefieran trabajar con Terraform pueden utilizar la personalización de cuentas de AWS Control Tower a escala con AFC y obtener acceso inmediato a cada cuenta una vez aprovisionada.

Para obtener información sobre cómo crear estas personalizaciones, consulte Creación de productos y Introducción al código abierto de Terraform en la documentación de Service Catalog. Esta función está disponible en todos los Regiones de AWS lugares donde AWS Control Tower esté disponible.

AWS La autogestión del IAM Identity Center está disponible para landing zone

6 de junio de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite la opción de elegir un proveedor de identidad para una zona de aterrizaje de AWS Control Tower, que puede configurar durante la configuración o la actualización. De forma predeterminada, la landing zone está habilitada para usar el Centro de identidad de AWS IAM, de acuerdo con las recomendaciones de mejores prácticas definidas en Cómo organizar su AWS entorno con varias cuentas. Ahora tiene tres alternativas:

- Puede aceptar la configuración predeterminada y permitir que AWS Control Tower configure y administre el AWS IAM Identity Center por usted.
- Puede optar por gestionar automáticamente el centro de identidad de AWS IAM para reflejar sus requisitos empresariales específicos.

- Si lo desea, puede contratar y autogestionar un proveedor de identidades externo, conectándolo a través del Centro de identidades de IAM, si es necesario. Debe utilizar la opción de proveedor de identidad si su entorno reglamentario exige que utilice un proveedor específico o si trabaja en un Regiones de AWS lugar donde el Centro de Identidad de AWS IAM no esté disponible.

Para obtener más información, consulte Guía sobre el Centro de Identidad de IAM.

No se admite la selección de proveedores de identidad a nivel de cuenta. Esta función solo se aplica a la zona de landing zone en su conjunto. La opción de proveedor de identidad de AWS Control Tower está disponible en todos los Regiones de AWS lugares donde esté disponible AWS Control Tower.

AWS Control Tower aborda la gobernanza mixta para las unidades organizativas

1 de junio de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

Con esta versión, AWS Control Tower impide que los controles se desplieguen en una unidad organizativa (OU) si esa OU se encuentra en un estado de gobierno mixto. La gobernanza mixta se produce en una OU si las cuentas no se actualizan después de que AWS Control Tower amplíe la gobernanza a una nueva Región de AWS o la elimine. Esta versión le ayuda a mantener las cuentas de los miembros de esa OU en conformidad uniforme. Para obtener más información, consulte Evite la gobernanza mixta al configurar las regiones.

Hay controles proactivos adicionales disponibles

19 de mayo de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower añade 28 nuevos controles proactivos para ayudarle a gestionar su entorno de múltiples cuentas y a cumplir objetivos de control específicos, como el cifrado de datos en reposo o la limitación del acceso a la red. Los controles proactivos se implementan mediante AWS CloudFormation enlaces que comprueban sus recursos antes de aprovisionarlos. Los nuevos controles pueden ayudar a controlar AWS servicios como Amazon OpenSearch Service, Amazon EC2 Auto Scaling, Amazon SageMaker, Amazon API Gateway y Amazon Relational Database Service (RDS).

Los controles proactivos son compatibles con todos los anuncios comerciales Regiones de AWS en los que AWS Control Tower esté disponible.

OpenSearch Servicio Amazon

- [CT.OPENSEARCH.PR.1] Requiere un dominio de Elasticsearch para cifrar los datos en reposo
- [CT.OPENSEARCH.PR.2] Requiere que se cree un dominio de Elasticsearch en una Amazon VPC especificada por el usuario
- [CT.OPENSEARCH.PR.3] Requiere un dominio de Elasticsearch para cifrar los datos enviados entre nodos
- [CT.OPENSEARCH.PR.4] Requiere un dominio de Elasticsearch para enviar los registros de errores a Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.5] Requiere un dominio de Elasticsearch para enviar los registros de auditoría a Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.6] Requiere que un dominio de Elasticsearch tenga reconocimiento de zona y al menos tres nodos de datos
- [CT.OPENSEARCH.PR.7] Requiere que un dominio de Elasticsearch tenga al menos tres nodos maestros dedicados
- [CT.OPENSEARCH.PR.8] Requiere un dominio de Elasticsearch Service para usar TLSv1.2
- [CT.OPENSEARCH.PR.9] Requiere un dominio de OpenSearch Amazon Service para cifrar los datos en reposo
- [CT.OPENSEARCH.PR.10] Requiere que se cree un dominio de Amazon Service en una OpenSearch Amazon VPC especificada por el usuario
- [CT.OPENSEARCH.PR.11] Requiere un dominio de OpenSearch Amazon Service para cifrar los datos enviados entre nodos
- [CT.OPENSEARCH.PR.12] Requiere un dominio de Amazon Service para enviar los registros de errores a OpenSearch Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.13] Requiere un dominio de Amazon Service para enviar los registros de auditoría a OpenSearch Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.14] Requiere que un dominio de OpenSearch Amazon Service tenga reconocimiento de zona y al menos tres nodos de datos
- [CT.OPENSEARCH.PR.15] Requiere un dominio de OpenSearch Amazon Service para utilizar un control de acceso detallado

- [CT.OPENSEARCH.PR.16] Requiere un dominio de Amazon Service para usar TLSv1.2 OpenSearch

Amazon EC2 Auto Scaling

- [CT.AUTOSCALING.PR.1] Requerir que un grupo de Auto Scaling de Amazon EC2 tenga varias zonas de disponibilidad
- [CT.AUTOSCALING.PR.2] Requiere una configuración de lanzamiento grupal de Amazon EC2 Auto Scaling para configurar las instancias de Amazon EC2 para IMDSv2
- [CT.AUTOSCALING.PR.3] Requiere una configuración de lanzamiento de Auto Scaling de Amazon EC2 para tener un límite de respuesta de metadatos de un solo salto
- [CT.AUTOSCALING.PR.4] Requiere que un grupo de Amazon EC2 Auto Scaling asociado a un Amazon Elastic Load Balancing (ELB) tenga activadas las comprobaciones de estado del ELB
- [CT.AUTOSCALING.PR.5] Exigir que una configuración de lanzamiento grupal de Amazon EC2 Auto Scaling no tenga instancias de Amazon EC2 con direcciones IP públicas
- [CT.AUTOSCALING.PR.6] Requiere que cualquier grupo de Auto Scaling de Amazon EC2 utilice varios tipos de instancias
- [CT.AUTOSCALING.PR.8] Requiere que un grupo de Amazon EC2 Auto Scaling tenga configuradas las plantillas de lanzamiento de EC2

Amazon SageMaker

- [CT.SAGEMAKER.PR.1] Requiere una instancia de SageMaker Amazon Notebook para evitar el acceso directo a Internet
- [CT.SAGEMAKER.PR.2] Requiere que las instancias de Amazon Notebook se desplieguen en una SageMaker Amazon VPC personalizada
- [CT.SAGEMAKER.PR.3] No se permite el acceso root a las instancias de SageMaker Amazon Notebook

Amazon API Gateway

- [CT.APIGATEWAY.PR.5] Requiere que las rutas Websocket y HTTP de Amazon API Gateway V2 especifiquen un tipo de autorización

Amazon Relational Database Service (RDS)

- [CT.RDS.PR.25] Requiere que un clúster de base de datos de Amazon RDS tenga configurado el registro

Para obtener más información, consulte Controles proactivos.

Controles proactivos de Amazon EC2 actualizados

2 de mayo de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ha actualizado dos controles proactivos: CT.EC2.PR.3 yCT.EC2.PR.4.

Para el CT.EC2.PR.3 control actualizado, se bloquea el AWS CloudFormation despliegue de cualquier implementación que haga referencia a una lista de prefijos para un recurso de grupo de seguridad, a menos que sea para el puerto 80 o 443.

Para el CT.EC2.PR.4 control actualizado, cualquier AWS CloudFormation implementación que haga referencia a una lista de prefijos para un recurso de grupo de seguridad se bloquea si el puerto es 3389, 20, 23, 110, 143, 3306, 8080, 1433, 9200, 9300, 25, 445, 135, 21, 1434, 4333, 5432, 5500, 5601, 22, 3000, 5000, 8088, 8888.

Regiones de AWS Hay siete más disponibles

19 de abril de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ya está disponible en otros siete países Regiones de AWS: norte de California (San Francisco), Asia Pacífico (Hong Kong, Yakarta y Osaka), Europa (Milán), Oriente Medio (Bahréin) y África (Ciudad del Cabo). Estas regiones adicionales de AWS Control Tower, denominadas regiones opcionales, no están activas de forma predeterminada, excepto la región EE.UU. Oeste (norte de California), que está activa de forma predeterminada.

Algunos controles de la Torre de Control de AWS no funcionan en algunas de estas Regiones de AWS áreas adicionales en las que AWS Control Tower está disponible, ya que esas regiones no admiten la funcionalidad subyacente requerida. Para obtener más detalles, consulte Limitaciones de control.

Entre estas nuevas regiones, cFCT no está disponible en Asia Pacífico (Yakarta y Osaka). La disponibilidad en otras Regiones de AWS no ha cambiado.

Para obtener más información sobre cómo AWS Control Tower gestiona las limitaciones de las regiones y los controles, consulteConsideraciones a la hora de activar las regiones con AWS suscripción.

Los puntos de enlace vPCE requeridos por AFT no están disponibles en la región de Oriente Medio (Bahréin). Los clientes que desplieguen AFT en esta región deben realizar la implementación con un parámetro. `aft_vpc_endpoints=false` Para obtener más información, consulte el parámetro en el archivo README.

Las VPC de AWS Control Tower tienen dos zonas de disponibilidad en la región EE.UU. Oeste (Norte de California)`us-west-1`, debido a una limitación en Amazon EC2. En el oeste de EE. UU. (norte de California), seis subredes se dividen en dos zonas de disponibilidad. Para obtener más información, consulte Información general sobre AWS Control Tower y las VPC.

AWS Control Tower agregó nuevos permisos `AWSControlTowerServiceRolePolicy` que permiten a AWS Control Tower realizar llamadas al servicio de administración de cuentas y a las `EnableRegion` `GetRegionOptStatus` API implementadas por el servicio de administración de AWS cuentas, para que estén Regiones de AWS disponibles adicionalmente para sus cuentas compartidas en la zona de aterrizaje (cuenta de administración, cuenta de archivo de registros, cuenta de auditoría) y sus cuentas de miembros de la OU. `ListRegions` Para obtener más información, consulte Políticas administradas para AWS Control Tower.

Seguimiento de solicitudes de personalización de cuentas de Account Factory for Terraform (AFT)

16 de febrero de 2023

AFT admite el seguimiento de las solicitudes de personalización de cuentas. Cada vez que envía una solicitud de personalización de una cuenta, AFT genera un token de rastreo único que pasa por una máquina de AWS Step Functions estados de personalización de AFT, que registra el token como parte de su ejecución. Puedes usar las consultas de estadísticas de Amazon CloudWatch Logs para buscar rangos de marcas de tiempo y recuperar el token de solicitud. Como resultado, puede ver las cargas útiles que acompañan al token, de modo que puede rastrear la solicitud de personalización de su cuenta a lo largo de todo el flujo de trabajo de AFT. Para obtener más información sobre AFT, consulte Descripción general de AWS Control Tower Account Factory for Terraform. Para obtener información sobre CloudWatch Logs y Step Functions, consulte lo siguiente:

- ¿Qué es Amazon CloudWatch Logs? en la Guía del usuario CloudWatch de Amazon Logs
- ¿Qué es AWS Step Functions? en la Guía AWS Step Functions para desarrolladores

Versión 3.1 de la zona de aterrizaje de AWS Control Tower

9 de febrero de 2023

(Se requiere una actualización para la versión 3.1 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio)

La versión 3.1 de AWS Control Tower landing zone incluye las siguientes actualizaciones:

- Con esta versión, AWS Control Tower desactiva el registro de acceso innecesario para su depósito de registro de acceso, que es el depósito de Amazon S3 en el que se almacenan los registros de acceso en la cuenta de Log Archive, al tiempo que sigue habilitando el registro de acceso al servidor para los cubos de S3. Esta versión también incluye actualizaciones del control Region Deny que permiten realizar acciones adicionales para los servicios globales, como los AWS Support planes y. AWS Artifact
- La desactivación del registro de acceso al servidor para el depósito de registro de acceso de la Torre de Control de AWS hace que Security Hub busque el depósito de registro de acceso de la cuenta de Log Archive. Debido a una AWS Security Hub regla, [S3.9] El registro de acceso al servidor del bucket S3 debe estar habilitado. De acuerdo con Security Hub, le recomendamos que suprima este hallazgo concreto, tal y como se indica en la descripción de esta regla en Security Hub. Para obtener información adicional, consulte la información sobre los hallazgos suprimidos.
- El registro de acceso al depósito de registro (normal) de la cuenta de Log Archive no ha cambiado en la versión 3.1. De acuerdo con las prácticas recomendadas, los eventos de acceso a ese depósito se registran como entradas de registro en el depósito de registro de acceso. Para obtener más información sobre el registro de acceso, consulte Registrar solicitudes mediante el registro de acceso al servidor en la documentación de Amazon S3.
- Hemos actualizado el control de denegación de regiones. Esta actualización permite que más servicios globales realicen acciones. Para obtener más información sobre este SCP, consulte Denegar el acceso a en AWS función de lo solicitado Región de AWS y Controles que mejoran la protección de la residencia de los datos.

  Se agregaron los siguientes servicios globales:

  - AWS Account Management (`account:*`)
  - AWS Activar (`activate:*`)

- AWS Artifact (`artifact:*`)
- AWS Billing Conductor (`billingconductor:*`)
- AWS Compute Optimizer (`compute-optimizer:*`)
- AWS Data Pipeline (`datapipeline:GetAccountLimits`)
- AWS Device Farm(`devicefarm:*`)
- AWS Marketplace (`discovery-marketplace:*`)
- Amazon ECR () `ecr-public:*`
- AWS License Manager (`license-manager:ListReceivedLicenses`)
- AWS `lightsail:Get*`Lightsail ()
- Explorador de recursos de AWS (`resource-explorer-2:*`)
- Amazon S3 (`s3:CreateMultiRegionAccessPoint`,`s3:GetBucketPolicyStatus`,`s3:PutMultiRegionAcc`
- AWS Savings Plans (`savingsplans:*`)
- Centro de identidad de IAM () `sso:*`
- AWS Support App (`supportapp:*`)
- AWS Support Planes () `supportplans:*`
- AWS Sostenibilidad (`sustainability:*`)
- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace Información sobre los proveedores (`vendor-insights:ListEntitledSecurityProfiles`)

Los controles proactivos están disponibles de forma general

24 de enero de 2023

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

Los controles proactivos opcionales, anunciados anteriormente en estado de versión preliminar, ya están disponibles de forma general. Estos controles se denominan proactivos porque comprueban sus recursos (antes de desplegarlos) para determinar si los nuevos recursos cumplen con los controles que están activados en su entorno. Para obtener más información, consulte Los controles integrales ayudan en el aprovisionamiento y la AWS administración de los recursos.

De enero a diciembre de 2022

En 2022, AWS Control Tower publicó las siguientes actualizaciones:

- Operaciones de cuentas simultáneas
- Personalización de Account Factory (AFC)
- Los controles integrales ayudan en el aprovisionamiento y la AWS administración de los recursos
- Se puede ver el estado de conformidad de todas las reglas AWS Config
- API para controles y un nuevo AWS CloudFormation recurso
- cFct admite la eliminación de conjuntos de pilas
- Retención de registros personalizada
- Se encuentra disponible la reparación de la desviación de
- Versión 3.0 de la zona de aterrizaje de AWS Control Tower
- La página de la organización combina vistas de unidades organizativas y cuentas
- Inscripción y actualización más sencillas para las cuentas de los miembros individuales
- AFT admite la personalización automatizada de las cuentas compartidas de AWS Control Tower
- Operaciones simultáneas para todos los controles opcionales
- Cuentas de registro y seguridad existentes
- Versión 2.9 de la zona de aterrizaje de AWS Control Tower
- Versión 2.8 de la zona de aterrizaje de AWS Control Tower

Operaciones de cuentas simultáneas

16 de diciembre de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite acciones simultáneas en la fábrica de cuentas. Puede crear, actualizar o inscribir hasta cinco (5) cuentas a la vez. Envía hasta cinco acciones seguidas y consulta el estado de finalización de cada solicitud mientras tus cuentas terminan de crearse en segundo plano. Por ejemplo, ya no tienes que esperar a que se complete cada proceso para actualizar otra cuenta o para volver a registrar una unidad organizativa (OU) completa.

Personalización de Account Factory (AFC)

28 de noviembre de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

La personalización de fábrica de cuentas le permite personalizar cuentas nuevas y existentes desde la consola de AWS Control Tower. Estas nuevas capacidades de personalización le ofrecen la flexibilidad de definir los planos de cuentas, que son AWS CloudFormation plantillas incluidas en un producto especializado de Service Catalog. Los planos proporcionan recursos y configuraciones totalmente personalizados. También puede optar por utilizar planes predefinidos, creados y gestionados por AWS socios, que le ayuden a personalizar las cuentas para casos de uso específicos.

Anteriormente, la fábrica de cuentas de AWS Control Tower no permitía la personalización de cuentas en la consola. Con esta actualización de Account Factory, puede predefinir los requisitos de la cuenta e implementarlos como parte de un flujo de trabajo bien definido. Puede aplicar planos para crear nuevas cuentas, inscribir otras AWS cuentas en la Torre de Control de AWS y actualizar las cuentas de la Torre de Control de AWS existentes.

Cuando aprovisione, inscriba o actualice una cuenta en Account Factory, seleccionará el blueprint que desee implementar. Los recursos especificados en el plan se aprovisionan en su cuenta. Cuando su cuenta haya terminado de crearse, todas las configuraciones personalizadas estarán disponibles para su uso inmediato.

Para empezar a personalizar las cuentas, puede definir los recursos para el caso de uso previsto en un producto de Service Catalog. También puede seleccionar soluciones administradas por socios de la biblioteca de AWS introducción. Para obtener más información, consulte Personaliza las cuentas con Account Factory Customization (AFC).

Los controles integrales ayudan en el aprovisionamiento y la AWS administración de los recursos

28 de noviembre de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite una gestión integral de los controles, que incluye nuevos controles proactivos opcionales, que se implementan mediante AWS CloudFormation enlaces. Estos

controles se denominan proactivos porque comprueban sus recursos, antes de implementarlos, para determinar si los nuevos recursos cumplen con los controles que están activados en su entorno.

Más de 130 nuevos controles proactivos le ayudan a cumplir objetivos políticos específicos para su entorno de AWS Control Tower, a cumplir los requisitos de los marcos de conformidad estándar del sector y a regular las interacciones de la Torre de Control de AWS en más de veinte AWS servicios más.

La biblioteca de controles de la Torre de Control de AWS clasifica estos controles según los AWS servicios y recursos asociados. Para obtener más información, consulte Controles proactivos.

Con esta versión, AWS Control Tower también se integra con AWS Security Hub el nuevo estándar gestionado por el servicio Security Hub: AWS Control Tower, que es compatible con el estándar AWS Foundational Security Best Practices (FSBP). Puede ver más de 160 controles de Security Hub junto con los controles de la Torre de Control de AWS en la consola y puede obtener una puntuación de seguridad de Security Hub para su entorno de Torre de Control de AWS. Para obtener más información, consulte Controles de Security Hub.

Se puede ver el estado de conformidad de todas las reglas AWS Config

18 de noviembre de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora muestra el estado de conformidad de todas AWS Config las reglas implementadas en las unidades organizativas registradas en AWS Control Tower. Puede ver el estado de conformidad de todas AWS Config las normas que afectan a sus cuentas en la Torre de Control de AWS, estén inscritas o no, sin necesidad de salir de la consola de la Torre de Control de AWS. Los clientes pueden elegir configurar las reglas de Config, denominadas controles de detección, en AWS Control Tower o configurarlas directamente a través del AWS Config servicio. AWS Config Se muestran las reglas implementadas por, junto con las reglas implementadas por AWS Control Tower.

Anteriormente, AWS Config las reglas implementadas a través del AWS Config servicio no estaban visibles en la consola de AWS Control Tower. Los clientes tenían que ir al AWS Config servicio para identificar las reglas que no cumplían con AWS Config las normas. Ahora puede identificar cualquier AWS Config regla no conforme en la consola de AWS Control Tower. Para ver el estado de conformidad de todas sus reglas de Config, vaya a la página de detalles de la cuenta en la consola de AWS Control Tower. Verá una lista que muestra el estado de conformidad de los controles

gestionados por la Torre de Control de AWS y las reglas de configuración implementadas fuera de la Torre de Control de AWS.

API para controles y un nuevo AWS CloudFormation recurso

1 de septiembre de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite la administración programática de los controles, también conocidos como barandas, mediante un conjunto de llamadas a la API. Un nuevo AWS CloudFormation recurso es compatible con la funcionalidad de la API para los controles. Para obtener más información, consulte Automatice las tareas en AWS Control Tower y Creación de AWS Control Tower recursos con AWS CloudFormation.

Estas API le permiten habilitar, deshabilitar y ver el estado de las aplicaciones de los controles de la biblioteca de la Torre de Control de AWS. Las API incluyen soporte para AWS CloudFormation, por lo que puede administrar AWS los recursos como infrastructure-as-code (IaC). AWS Control Tower proporciona controles preventivos y de detección opcionales que expresan las intenciones de su política con respecto a toda una unidad organizativa (OU) y a todas las AWS cuentas de la OU. Estas reglas permanecen en vigor a medida que crea cuentas nuevas o realiza cambios en las cuentas existentes.

Las API se incluyen en esta versión

- EnableControl— Esta llamada a la API activa un control. Inicia una operación asíncrona que crea AWS recursos en la unidad organizativa especificada y en las cuentas que contiene.
- DisableControl— Esta llamada a la API desactiva un control. Inicia una operación asíncrona que elimina los AWS recursos de la unidad organizativa especificada y las cuentas que contiene.
- GetControlOperation— Devuelve el estado de una operación u operación concreta. EnableControlDisableControl
- ListEnabledControls— Muestra los controles habilitados por AWS Control Tower en la unidad organizativa especificada y las cuentas que contiene.

Para ver una lista de los nombres de los controles opcionales, consulte Identificadores de recursos para API y controles en la Guía del usuario de AWS Control Tower.

cFct admite la eliminación de conjuntos de pilas

26 de agosto de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

Las personalizaciones de AWS Control Tower (cFCT) ahora admiten la eliminación de conjuntos de pilas mediante la configuración de un parámetro en el `manifest.yaml` archivo. Para obtener más información, consulte Eliminación de un conjunto de pilas.

> **Important**
>
> Al establecer inicialmente el valor de `enable_stack_set_deletion` en`true`, la próxima vez que invoque cFct, se eliminarán por etapas TODOS los recursos que comiencen por el prefijo`CustomControlTower-`, que tengan la etiqueta `Key:AWS_Solutions, Value: CustomControlTowerStackSet` clave asociada y que no estén declarados en el archivo de manifiesto.

Retención de registros personalizada

15 de agosto de 2022

(Se requiere una actualización para la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio)

AWS Control Tower ahora ofrece la posibilidad de personalizar la política de retención de los buckets de Amazon S3 que almacenan los CloudTrail registros de la Torre de Control de AWS. Puede personalizar su política de retención de registros de Amazon S3, en incrementos de días o años, hasta un máximo de 15 años.

Si decide no personalizar la retención de registros, la configuración predeterminada es de 1 año para el registro de cuentas estándar y 10 años para el registro de acceso.

Esta función está disponible para los clientes actuales a través de la Torre de Control de AWS cuando actualiza o repara su zona de aterrizaje, y para los nuevos clientes a través del proceso de configuración de la Torre de Control de AWS.

Se encuentra disponible la reparación de la desviación de

11 de agosto de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora admite la reparación por desviación de roles. Puedes restaurar un rol obligatorio sin reparar por completo tu landing zone. Si se necesita este tipo de reparación de derrapes, la página de error de la consola proporciona los pasos para restaurar el rol, de modo que tu landing zone vuelva a estar disponible.

Versión 3.0 de la zona de aterrizaje de AWS Control Tower

29 de julio de 2022

(Se requiere una actualización para la versión 3.0 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio)

La versión 3.0 de AWS Control Tower landing zone incluye las siguientes actualizaciones:

- La opción de elegir AWS CloudTrail rutas a nivel de organización o de excluirse de las CloudTrail rutas gestionadas por AWS Control Tower.
- Dos nuevos controles de detección para determinar si AWS CloudTrail se está registrando actividad en sus cuentas.
- La opción de agregar AWS Config información sobre los recursos globales solo en su región de origen.
- Una actualización de la región niega el control.
- Una actualización de la política gestionada, AWSControlTowerServiceRolePolicy.
- Ya no creamos el rol `aws-controltower-CloudWatchLogsRole` de IAM ni el grupo de CloudWatch registros `aws-controltower/CloudTrailLogs` en cada cuenta inscrita. Anteriormente, los creábamos en cada cuenta para su registro de cuentas. Con los registros de la organización, solo creamos uno en la cuenta de administración.

En las siguientes secciones se proporcionan más detalles sobre cada nueva capacidad.

CloudTrail Rutas a nivel de organización en la Torre de Control de AWS

Con la versión 3.0 de landing zone, AWS Control Tower ahora admite rutas a nivel de organización AWS CloudTrail .

Al actualizar la zona de aterrizaje de AWS Control Tower a la versión 3.0, tiene la opción de seleccionar AWS CloudTrail rutas a nivel de organización como su preferencia de registro o de

excluirse de las CloudTrail rutas gestionadas por AWS Control Tower. Al actualizar a la versión 3.0, AWS Control Tower elimina los registros existentes a nivel de cuenta de las cuentas inscritas tras un período de espera de 24 horas. AWS Control Tower no elimina los registros a nivel de cuenta de las cuentas no inscritas. En el improbable caso de que la actualización de la zona de aterrizaje no se realice correctamente, pero el error se produzca después de que AWS Control Tower ya haya creado la ruta a nivel de la organización, es posible que se le cobren cargos duplicados por las rutas a nivel de la organización y de la cuenta, hasta que la operación de actualización se complete correctamente.

A partir de la versión 3.0 de landing zone, AWS Control Tower ya no admite rastreos a nivel de cuenta que AWS administre. En su lugar, AWS Control Tower crea un registro a nivel de organización, que está activo o inactivo, según su selección.

> **Note**
>
> Tras actualizar a la versión 3.0 o posterior, no tendrá la opción de continuar con las CloudTrail rutas a nivel de cuenta gestionadas por AWS Control Tower.

No se pierde ningún dato de registro de los registros agregados de su cuenta, ya que los registros permanecen en el depósito de Amazon S3 existente donde están almacenados. Solo se eliminan los registros, no los registros existentes. Si selecciona la opción de añadir rutas a nivel de organización, AWS Control Tower abrirá una nueva ruta a una nueva carpeta dentro de su bucket de Amazon S3 y seguirá enviando información de registro a esa ubicación. Si opta por excluirse de las rutas gestionadas por AWS Control Tower, sus registros existentes permanecerán en el depósito sin cambios.

Convenciones de nomenclatura de rutas para el almacenamiento de registros

- Los registros de las cuentas se almacenan con una ruta de este formato: `/org id/AWSLogs/…`
- Los registros de la organización se almacenan con una ruta de este formulario: `/org id/AWSLogs/org id/…`

La ruta que AWS Control Tower crea para las CloudTrail rutas a nivel de la organización es diferente de la ruta predeterminada para una ruta a nivel de la organización creada manualmente, que tendría el siguiente formato:

- `/AWSLogs/org id/…`

Para obtener más información sobre la denominación de las CloudTrail rutas, consulte Cómo encontrar los archivos de registro. CloudTrail

> **Tip**
>
> Si tiene pensado crear y gestionar sus propias rutas a nivel de cuenta, le recomendamos que cree las nuevas rutas antes de completar la actualización a la versión 3.0 de la zona de aterrizaje de AWS Control Tower, para empezar a registrarlas de inmediato.

En cualquier momento, puede optar por crear nuevos CloudTrail senderos a nivel de cuenta o de organización y administrarlos por su cuenta. La opción de elegir CloudTrail rutas a nivel de organización gestionadas por AWS Control Tower está disponible durante cualquier actualización de landing zone a la versión 3.0 o posterior. Puedes activar y desactivar las rutas a nivel de organización siempre que actualices tu landing zone.

Si tus registros los gestiona un servicio de terceros, asegúrate de asignar el nombre de la nueva ruta a tu servicio.

> **Note**
>
> Para las zonas de aterrizaje de la versión 3.0 o posterior, AWS Control Tower no admite las AWS CloudTrail rutas a nivel de cuenta. Puede crear y mantener sus propias rutas a nivel de cuenta en cualquier momento, o puede optar por las rutas a nivel de organización administradas por AWS Control Tower.

Registre AWS Config los recursos únicamente en la región de origen

En la versión 3.0 de landing zone, AWS Control Tower actualizó la configuración básica para AWS Config que registre los recursos globales únicamente en la región de origen. Después de actualizar a la versión 3.0, el registro de recursos para los recursos globales solo está habilitado en su región de origen.

Esta configuración se considera una práctica recomendada. Está recomendada por AWS Security Hub y AWS Config, además, permite ahorrar costes al reducir la cantidad de elementos de configuración que se crean al crear, modificar o eliminar los recursos globales. Anteriormente, cada vez que un cliente o un AWS servicio creaban, actualizaban o eliminaban un recurso global, se creaba un elemento de configuración para cada elemento de cada región gobernada.

Dos nuevos controles de detección para el AWS CloudTrail registro

Como parte del cambio en los registros a nivel de organización AWS CloudTrail , AWS Control Tower presenta dos nuevos controles de detección que comprueban si están habilitados CloudTrail . El primer control tiene una guía obligatoria y se habilita en la unidad organizativa de seguridad durante la configuración o las actualizaciones de landing zone de la versión 3.0 y versiones posteriores. El segundo control tiene una guía muy recomendable y se puede aplicar opcionalmente a cualquier unidad organizativa distinta de la unidad organizativa de seguridad, que ya cuenta con la protección de control obligatoria.

Control obligatorio: detecta si las cuentas compartidas de la unidad organizativa de Seguridad tienen AWS CloudTrail o están habilitadas para CloudTrail Lake

Control muy recomendable: detecta si una cuenta tiene AWS CloudTrail o CloudTrail Lake está activado

Para obtener más información sobre los nuevos controles, consulte la biblioteca de controles de la Torre de Control de AWS.

Una actualización de la región niega el control

Hemos actualizado la NotActionlista de denegaciones de control de la región para incluir las acciones de algunos servicios adicionales, que se enumeran a continuación:

```
        “chatbot:*”,
        "s3:GetAccountPublic",
        "s3:DeleteMultiRegionAccessPoint",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListMultiRegionAccessPoints",
        "s3:GetStorageLensConfiguration",
        “s3:GetStorageLensDashboard",
        “s3:ListStorageLensConfigurations”
        “s3:GetAccountPublicAccessBlock“,,
        “s3:PutAccountPublic",
        “s3:PutAccountPublicAccessBlock“,
```

Tutorial en vídeo

En este vídeo (3:07) se describe cómo actualizar su zona de aterrizaje de AWS Control Tower existente a la versión 3. Para una mejor visualización, seleccione el icono situado en la esquina inferior derecha del vídeo para agrandarlo a pantalla completa. Hay subtítulos disponibles.

Tutorial en vídeo sobre la actualización de una zona de aterrizaje de la Torre de Control de AWS existente a la zona de aterrizaje 3.

La página de la organización combina vistas de unidades organizativas y cuentas

18 de julio de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

La nueva página de organización de la Torre de Control de AWS muestra una vista jerárquica de todas las unidades organizativas (OU) y las cuentas. Combina la información de las páginas de unidades organizativas y cuentas, que existían anteriormente.

En la nueva página, puede ver las relaciones entre las unidades organizativas principales y sus unidades organizativas y cuentas anidadas. También puede tomar medidas en relación con las agrupaciones de recursos. Puede configurar la vista de página. Por ejemplo, puede expandir o contraer la vista jerárquica, filtrar la vista para ver solo las cuentas o unidades organizativas, elegir ver solo las cuentas inscritas y las unidades organizativas registradas, o puede ver grupos de recursos relacionados. Es más fácil asegurarse de que toda la organización esté actualizada correctamente.

Inscripción y actualización más sencillas para las cuentas de los miembros individuales

31 de mayo de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora le ofrece una capacidad mejorada para actualizar e inscribir las cuentas de los miembros de forma individual. Cada cuenta muestra cuándo está disponible para una actualización, por lo que puede asegurarse más fácilmente de que las cuentas de sus miembros incluyen la configuración más reciente. Puedes actualizar tu landing zone, corregir el desvío de cuentas o inscribir una cuenta en una OU registrada siguiendo unos pocos pasos sencillos.

Al actualizar una cuenta, no es necesario incluir la unidad organizativa (OU) completa de la cuenta en cada acción de actualización. Como resultado, se reduce considerablemente el tiempo necesario para actualizar una cuenta individual.

Puede inscribir cuentas en las unidades organizativas de la Torre de Control de AWS con más ayuda de la consola de la Torre de Control de AWS. Las cuentas existentes que inscriba en AWS Control Tower deben seguir cumpliendo los requisitos previos de la cuenta y debe añadir el `AWSControlTowerExecution` rol. A continuación, puede elegir cualquier OU registrada e inscribir la cuenta en ella pulsando el botón Inscribir.

Hemos separado la funcionalidad de inscripción de cuentas del flujo de trabajo de creación de cuentas en Account Factory para diferenciar mejor estos procesos similares y evitar errores de configuración al introducir la información de la cuenta.

AFT admite la personalización automatizada de las cuentas compartidas de AWS Control Tower

27 de mayo de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

Account Factory for Terraform (AFT) ahora puede personalizar y actualizar mediante programación cualquiera de sus cuentas administradas por AWS Control Tower, incluidas la cuenta de administración, la cuenta de auditoría y la cuenta de archivo de registros, junto con las cuentas inscritas. Puede centralizar la personalización de su cuenta y la administración de actualizaciones y, al mismo tiempo, proteger la seguridad de las configuraciones de su cuenta, ya que usted determina la función que lleva a cabo el trabajo.

El AWSAFTExecutionrol actual ahora implementa las personalizaciones en todas las cuentas. Puede configurar los permisos de IAM con límites que limiten el acceso al AWSAFTExecutionrol en función de sus requisitos empresariales y de seguridad. También puede delegar mediante programación los permisos de personalización aprobados en ese rol para usuarios de confianza. Como práctica recomendada, le recomendamos que restrinja los permisos a los necesarios para implementar las personalizaciones requeridas.

AFT ahora crea la nueva AWSAFTServicefunción para implementar los recursos de AFT en todas las cuentas administradas, incluidas las cuentas compartidas y la cuenta de administración. Anteriormente, los recursos los desplegaba el AWSAFTExecutionrol.

Las cuentas compartidas y de administración de AWS Control Tower no se aprovisionan a través de la fábrica de cuentas, por lo que no incluyen los productos aprovisionados correspondientes. AWS Service Catalog Por lo tanto, no puede actualizar las cuentas compartidas y de administración en Service Catalog.

Operaciones simultáneas para todos los controles opcionales

18 de mayo de 2022

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora admite operaciones simultáneas para controles preventivos y controles de detección.

Con esta nueva función, cualquier control opcional ahora se puede aplicar o quitar simultáneamente, lo que mejora la facilidad de uso y el rendimiento de todos los controles opcionales. Puede activar varios controles opcionales sin tener que esperar a que se completen las operaciones de control individuales. Los únicos momentos restringidos son cuando AWS Control Tower está configurando una zona de landing zone o cuando extiende la gobernanza a una nueva organización.

Funcionalidad compatible para los controles preventivos:

- Aplique y elimine diferentes controles preventivos en la misma unidad organizativa.
- Aplique y elimine diferentes controles preventivos en diferentes unidades organizativas de forma simultánea.
- Aplique y retire el mismo control preventivo en varias unidades organizativas de forma simultánea.
- Puede aplicar y eliminar todos los controles preventivos y de detección al mismo tiempo.

Puede disfrutar de estas mejoras de control simultáneo en todas las versiones publicadas de AWS Control Tower.

Al aplicar controles preventivos a las unidades organizativas anidadas, los controles preventivos afectan a todas las cuentas y unidades organizativas anidadas en la unidad organizativa de destino, incluso si esas cuentas y unidades organizativas no están registradas en AWS Control Tower. Los controles preventivos se implementan mediante políticas de control de servicios (SCP), que forman parte de ellas. AWS Organizations Los controles de Detective se implementan mediante AWS Config reglas. Las barreras permanecen en vigor a medida que crea nuevas cuentas o realiza cambios en las cuentas existentes, y AWS Control Tower proporciona un informe resumido sobre cómo

cada cuenta se ajusta a las políticas habilitadas. Para obtener una lista completa de los controles disponibles, consulte la biblioteca de controles de la Torre de Control de AWS.

Cuentas de registro y seguridad existentes

16 de mayo de 2022

(Disponible durante la configuración inicial).

AWS Control Tower ahora ofrece la opción de especificar una AWS cuenta existente como cuenta de seguridad o de registro de AWS Control Tower durante el proceso de configuración inicial de la landing zone. Esta opción elimina la necesidad de que AWS Control Tower cree nuevas cuentas compartidas. La cuenta de seguridad, que de forma predeterminada se denomina cuenta de auditoría, es una cuenta restringida que permite a tus equipos de seguridad y cumplimiento acceder a todas las cuentas de tu landing zone. La cuenta de registro, que de forma predeterminada se denomina cuenta Log Archive, funciona como repositorio. Almacena los registros de las actividades de la API y las configuraciones de recursos de todas las cuentas de tu landing zone.

Al incorporar sus cuentas de registro y seguridad existentes, es más fácil extender la gobernanza de AWS Control Tower a sus organizaciones actuales o migrar a AWS Control Tower desde una landing zone alternativa. La opción de usar las cuentas existentes se muestra durante la configuración inicial de landing zone. Incluye comprobaciones durante el proceso de configuración, que garantizan el éxito de la implementación. AWS Control Tower implementa las funciones y los controles necesarios en sus cuentas existentes. No elimina ni fusiona ningún recurso o dato existente que exista en estas cuentas.

Limitación: si planea incorporar AWS las cuentas existentes a AWS Control Tower como cuentas de auditoría y archivo de registros, y si esas cuentas tienen AWS Config recursos existentes, debe eliminar los AWS Config recursos existentes antes de poder inscribir las cuentas en AWS Control Tower.

Versión 2.9 de la zona de aterrizaje de AWS Control Tower

22 de abril de 2022

(Se requiere una actualización para la versión 2.9 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio)

La versión 2.9 de AWS Control Tower landing zone actualiza el reenviador de notificaciones Lambda para que utilice el entorno de ejecución de Python versión 3.9. Esta actualización corrige la

obsolescencia de la versión 3.6 de Python, prevista para julio de 2022. Para obtener la información más reciente, consulta la página de obsolescencia de Python.

Versión 2.8 de la zona de aterrizaje de AWS Control Tower

10 de febrero de 2022

(Se requiere una actualización para la versión 2.8 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio)

La versión 2.8 de AWS Control Tower landing zone añade una funcionalidad que se ajusta a las actualizaciones recientes de las prácticas recomendadas de seguridad AWS fundamentales.

En esta versión:

- El registro de acceso está configurado para el depósito de registro de acceso de la cuenta de Log Archive, a fin de realizar un seguimiento del acceso al depósito de registro de acceso de S3 existente.
- Se añade el soporte para la política de ciclo de vida. El registro de acceso del depósito de registro de acceso de S3 existente tiene un tiempo de retención predeterminado de 10 años.
- Además, en esta versión se actualiza AWS Control Tower para que utilice el rol vinculado a AWS servicios (SLR) proporcionado por AWS Config todas las cuentas administradas (excepto la cuenta de administración), de modo que pueda configurar y administrar las reglas de Config para que se ajusten a las prácticas AWS Config recomendadas. Los clientes que no se actualicen seguirán utilizando su función actual.
- Esta versión optimiza el proceso de configuración de AWS Control Tower KMS para cifrar AWS Config datos y mejora los mensajes de estado relacionados. CloudTrail
- La versión incluye una actualización de la función Denegar el control por región para permitir la entrada de `route53-application-recovery` esta función. `us-west-2`
- Actualización: el 15 de febrero de 2022, eliminamos la cola de cartas muertas para las funciones de AWS Lambda.

Detalles adicionales:

- Si retira su landing zone, AWS Control Tower no elimina la función vinculada al AWS Config servicio.
- Si anula el aprovisionamiento de una cuenta de Account Factory, AWS Control Tower no elimina el rol vinculado al AWS Config servicio.

Para actualizar tu landing zone a 2.8, ve a la página de configuración de Landing zone, selecciona la versión 2.8 y, a continuación, selecciona Actualizar. Después de actualizar su landing zone, debe actualizar todas las cuentas que estén gobernadas por AWS Control Tower, tal y como se indica en la sección Administración de actualizaciones de configuración en AWS Control Tower.

De enero a diciembre de 2021

En 2021, AWS Control Tower publicó las siguientes actualizaciones:

- Capacidades de denegación regional
- Funciones de residencia de datos
- AWS Control Tower presenta el aprovisionamiento y la personalización de cuentas de Terraform
- Nuevo evento de ciclo de vida disponible
- AWS Control Tower permite unidades organizativas anidadas
- Simultaneidad de controles de Detectives
- Hay dos nuevas regiones disponibles
- Deselección de región
- AWS Control Tower funciona con sistemas de administración de AWS claves
- Se cambió el nombre de los controles y la funcionalidad no
- AWS Control Tower escanea los SCP a diario para comprobar si hay desviaciones
- Nombres personalizados para unidades organizativas y cuentas
- Versión 2.7 de la zona de aterrizaje de AWS Control Tower
- Hay tres nuevas AWS regiones disponibles
- Gobierna únicamente las regiones seleccionadas
- AWS Control Tower ahora amplía la gobernanza a las unidades organizativas existentes en sus AWS organizaciones
- AWS Control Tower ofrece actualizaciones masivas de cuentas

Capacidades de denegación regional

30 de noviembre de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower).

AWS Control Tower ahora ofrece funciones de denegación regional, que le ayudan a limitar el acceso a AWS los servicios y las operaciones de las cuentas inscritas en su entorno de AWS Control Tower. La función de denegación de regiones complementa las funciones de selección y deselección de regiones existentes en AWS Control Tower. En conjunto, estas características le ayudan a abordar los problemas normativos y de conformidad, a la vez que equilibran los costes asociados a la expansión a otras regiones.

Por ejemplo, AWS los clientes de Alemania pueden denegar el acceso a AWS los servicios en regiones fuera de la región de Fráncfort. Puede seleccionar regiones restringidas durante el proceso de configuración de la Torre de Control de AWS o en la página de configuración de la zona de aterrizaje. La función de denegación de regiones está disponible al actualizar la versión de la zona de aterrizaje de AWS Control Tower. Algunos AWS servicios están exentos de las capacidades de denegación regional. Para obtener más información, consulte Configurar el control de denegación regional.

Funciones de residencia de datos

30 de noviembre de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora ofrece controles diseñados específicamente para garantizar que los datos de los clientes que suba a AWS los servicios se encuentren únicamente en las AWS regiones que especifique. Puede seleccionar la AWS región o las regiones en las que se almacenan y procesan los datos de sus clientes. Para obtener una lista completa de AWS las regiones en las que AWS Control Tower está disponible, consulte la tabla de AWS regiones.

Para un control detallado, puede aplicar controles adicionales, como no permitir las conexiones de la red privada virtual (VPN) de Amazon o no permitir el acceso a Internet para una instancia de Amazon VPC. Puede ver el estado de conformidad de los controles en la consola de AWS Control Tower. Para obtener una lista completa de los controles disponibles, consulte la biblioteca de controles de la Torre de Control de AWS.

AWS Control Tower presenta el aprovisionamiento y la personalización de cuentas de Terraform

29 de noviembre de 2021

(Actualización opcional para la zona de aterrizaje de AWS Control Tower)

Ahora puede utilizar Terraform para aprovisionar y actualizar cuentas personalizadas a través de AWS Control Tower, con AWS Control Tower Account Factory for Terraform (AFT).

AFT proporciona una única canalización de infraestructura de Terraform como código (IaC), que aprovisiona las cuentas administradas por AWS Control Tower. Las personalizaciones durante el aprovisionamiento ayudan a cumplir sus políticas empresariales y de seguridad antes de entregar las cuentas a los usuarios finales.

El proceso de creación automática de cuentas de AFT supervisa hasta que se completa el aprovisionamiento de cuentas y, luego, continúa, activando módulos de Terraform adicionales que mejoran la cuenta con las personalizaciones necesarias. Como parte adicional del proceso de personalización, puede configurar la canalización para instalar sus propios módulos personalizados de Terraform y puede optar por añadir cualquiera de las opciones de funciones de AFT, que se proporcionan para las personalizaciones más habituales. AWS

Comience a utilizar AWS Control Tower Account Factory para Terraform siguiendo los pasos que se indican en la guía del usuario de AWS Control Tower y descargando AFT para su instancia de Terraform. Implemente AWS Control Tower Account Factory para Terraform (AFT) AFT es compatible con las distribuciones de código abierto Terraform Cloud, Terraform Enterprise y Terraform.

Nuevo evento de ciclo de vida disponible

18 de noviembre de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

El `PrecheckOrganizationalUnit` evento registra si algún recurso impide que la tarea de gobierno de Extend se lleve a cabo correctamente, incluidos los recursos de las unidades organizativas anidadas. Para obtener más información, consulte `PrecheckOrganizationalUnit`.

AWS Control Tower permite unidades organizativas anidadas

16 de noviembre de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora le permite incluir unidades organizativas anidadas como parte de su landing zone.

AWS Control Tower admite unidades organizativas (OU) anidadas, lo que le permite organizar las cuentas en varios niveles jerárquicos y aplicar controles preventivos de forma jerárquica. Puede registrar unidades organizativas que contengan unidades organizativas anidadas, crear y registrar unidades organizativas en las unidades organizativas principales y habilitar los controles en cualquier unidad organizativa registrada, independientemente de su profundidad. Para admitir esta funcionalidad, la consola muestra el número de cuentas y unidades organizativas gobernadas.

Con las unidades organizativas anidadas, puede alinear las unidades organizativas de la Torre de Control de AWS con la estrategia de AWS múltiples cuentas y reducir el tiempo necesario para habilitar los controles en varias unidades organizativas mediante la aplicación de los controles a nivel de la unidad organizativa principal.

Consideraciones clave

1. Puede registrar las unidades organizativas de varios niveles existentes en AWS Control Tower, una unidad organizativa a la vez, empezando por la unidad organizativa de nivel superior y, a continuación, siguiendo por el árbol. Para obtener más información, consulte Pase de una estructura de unidad organizativa plana a una estructura de unidad organizativa anidada.
2. Las cuentas que estén directamente bajo una unidad organizativa registrada se inscriben automáticamente. Las cuentas que se encuentran más abajo en el árbol se pueden inscribir registrando su OU principal inmediata.
3. Los controles preventivos (SCP) se heredan automáticamente en la jerarquía; los SCP aplicados a la unidad principal los heredan todas las OU anidadas.
4. Los controles de Detective (reglas de AWS Config) NO se heredan automáticamente.
5. Cada OU informa del cumplimiento de los controles de detección.
6. La desviación del SCP en una OU afecta a todas las cuentas y unidades organizativas incluidas en ella.
7. No puede crear nuevas unidades organizativas anidadas bajo la unidad organizativa de seguridad (unidad organizativa principal).

Simultaneidad de controles de Detectives

5 de noviembre de 2021

(Actualización opcional para la zona de aterrizaje de AWS Control Tower)

Los controles de detección de AWS Control Tower ahora admiten operaciones simultáneas para los controles de detección, lo que mejora la facilidad de uso y el rendimiento. Puede activar varios controles de detección sin tener que esperar a que se completen las operaciones de control individuales.

Funcionalidad compatible:

- Habilite diferentes controles de detección en la misma OU (por ejemplo, detecte si la MFA para el usuario raíz está habilitada y detecte si se permite el acceso de escritura pública a los buckets de Amazon S3).
- Active diferentes controles de detección en diferentes unidades organizativas de forma simultánea.
- Se han mejorado los mensajes de error de Guardrail para ofrecer una orientación adicional sobre las operaciones de control simultáneas compatibles.

No se admite en esta versión:

- No se admite la activación simultánea del mismo control de detección en varias unidades organizativas.
- No se admite la simultaneidad del control preventivo.

Puede disfrutar de las mejoras en la simultaneidad de los controles de detección en todas las versiones de AWS Control Tower. Se recomienda que los clientes que actualmente no utilicen la versión 2.7 realicen una actualización de landing zone para aprovechar otras funciones, como la selección y deselección de regiones, que están disponibles en la última versión.

Hay dos nuevas regiones disponibles

29 de julio de 2021

(Se requiere una actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ya está disponible en dos AWS regiones adicionales: Sudamérica (São Paulo) y Europa (París). Esta actualización amplía la disponibilidad de la Torre de Control de AWS a 15 AWS regiones.

Si es la primera vez que utiliza AWS Control Tower, puede lanzarlo de inmediato en cualquiera de las regiones compatibles. Durante el lanzamiento, puede seleccionar las regiones en las que desea que AWS Control Tower cree y gobierne su entorno de cuentas múltiples.

Si ya dispone de un entorno de AWS Control Tower y desea ampliar o eliminar las funciones de gobierno de la Torre de Control de AWS en una o más regiones compatibles, vaya a la página de configuración de la zona de destino en su panel de control de AWS Control Tower y, a continuación, seleccione las regiones. Tras actualizar su landing zone, debe actualizar todas las cuentas que estén gobernadas por AWS Control Tower.

Deselección de región

29 de julio de 2021

(Actualización opcional para la zona de aterrizaje de AWS Control Tower)

La deselección de la región de AWS Control Tower mejora su capacidad de administrar la presencia geográfica de los recursos de la Torre de Control de AWS. Puede anular la selección de las regiones que no quiere que gobierne AWS Control Tower. Esta función le permite abordar las cuestiones normativas y de conformidad y, al mismo tiempo, equilibrar los costes asociados a la expansión a otras regiones.

La desselección de regiones está disponible al actualizar la versión de la zona de aterrizaje de AWS Control Tower.

Cuando usa Account Factory para crear una cuenta nueva o inscribir una cuenta de miembro preexistente, o cuando selecciona Extend Governance para inscribir cuentas en una unidad organizativa preexistente, AWS Control Tower despliega sus capacidades de gobierno, que incluyen el registro, la supervisión y los controles centralizados, en las regiones de las cuentas que elija. Si decide deseleccionar una región y eliminar la gobernanza de la Torre de Control de AWS de esa región, se elimina esa funcionalidad de gobierno, pero no inhibe la capacidad de los usuarios de implementar AWS recursos o cargas de trabajo en esas regiones.

AWS Control Tower funciona con sistemas de administración de AWS claves

28 de julio de 2021

(Actualización opcional para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower le ofrece la opción de usar una AWS clave del Servicio de administración de claves (AWS KMS). Usted proporciona y administra una clave para proteger los servicios que implementa AWS Control Tower AWS CloudTrail AWS Config, incluidos los datos de Amazon S3

asociados. AWS El cifrado KMS es un nivel de cifrado mejorado con respecto al cifrado SSE-S3 que AWS Control Tower utiliza de forma predeterminada.

La integración del soporte de AWS KMS en la Torre de Control de AWS se ajusta a las prácticas recomendadas de seguridad AWS fundamentales, que recomiendan una capa de seguridad adicional para los archivos de registro confidenciales. Debe usar claves AWS administradas por KMS (SSE-KMS) para el cifrado en reposo. AWS La compatibilidad con el cifrado de KMS está disponible al configurar una nueva zona de aterrizaje o al actualizar la zona de aterrizaje de AWS Control Tower existente.

Para configurar esta funcionalidad, puedes seleccionar la configuración clave de KMS durante la configuración inicial de landing zone. Puede elegir una clave de KMS existente o puede seleccionar un botón que le dirija a la consola de AWS KMS para crear una nueva. También tiene la flexibilidad de cambiar del cifrado predeterminado al SSE-KMS o a una clave SSE-KMS diferente.

En el caso de una zona de aterrizaje de AWS Control Tower existente, puede realizar una actualización para empezar a utilizar las claves de AWS KMS.

Se cambió el nombre de los controles y la funcionalidad no

26 de julio de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower está revisando algunos nombres y descripciones de los controles para reflejar mejor las intenciones políticas del control. Los nombres y las descripciones revisados le ayudan a comprender de forma más intuitiva las formas en que los controles incorporan las políticas de sus cuentas. Por ejemplo, cambiamos parte de los nombres de los controles de detección, de «No permitir» a «Detectar», porque el control de detección en sí mismo no detiene una acción específica, solo detecta las infracciones de las políticas y envía alertas a través del panel de control.

La funcionalidad, la orientación y la implementación del control permanecen inalteradas. Solo se han revisado los nombres y las descripciones de los controles.

AWS Control Tower escanea los SCP a diario para comprobar si hay desviaciones

11 de mayo de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora realiza escaneos automatizados diarios de los SCP administrados para comprobar que los controles correspondientes se aplican correctamente y que no se han desviado. Si al escanear se detecta una desviación, recibirá una notificación. AWS Control Tower envía solo una notificación por cada problema de deriva, por lo que si su zona de aterrizaje ya se encuentra en un estado de deriva, no recibirá notificaciones adicionales a menos que encuentre un nuevo elemento de deriva.

Nombres personalizados para unidades organizativas y cuentas

16 de abril de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora le permite personalizar la denominación de su landing zone. Puede conservar los nombres que AWS Control Tower recomienda para las unidades organizativas (OU) y las cuentas principales, o puede modificarlos durante el proceso inicial de configuración de la landing zone.

Los nombres predeterminados que AWS Control Tower proporciona para las unidades organizativas y las cuentas principales coinciden con la guía de prácticas recomendadas para AWS varias cuentas. Sin embargo, si su empresa tiene políticas de nomenclatura específicas o si ya tiene una OU o cuenta con el mismo nombre recomendado, la nueva funcionalidad de nomenclatura de la OU y de las cuentas le ofrece la flexibilidad necesaria para abordar esas limitaciones.

Además del cambio en el flujo de trabajo durante la configuración, la unidad organizativa anteriormente conocida como unidad organizativa principal ahora se denomina unidad organizativa de seguridad, y la unidad organizativa anteriormente conocida como unidad organizativa personalizada ahora se denomina unidad organizativa Sandbox. Hicimos este cambio para mejorar nuestra alineación con la guía general de AWS mejores prácticas en materia de nomenclatura.

Los nuevos clientes verán estos nuevos nombres de unidades organizativas. Los clientes actuales seguirán viendo los nombres originales de estas OU. Es posible que encuentre algunas inconsistencias en la denominación de las unidades organizativas mientras actualizamos nuestra documentación para adaptarla a los nuevos nombres.

Para empezar a usar AWS Control Tower desde la consola de AWS administración, ve a la consola de AWS Control Tower y selecciona Configurar landing zone en la parte superior derecha. Para obtener información adicional, consulte cómo planificar su zona de aterrizaje en la AWS Control Tower.

Versión 2.7 de la zona de aterrizaje de AWS Control Tower

8 de abril de 2021

(Se requiere una actualización para la versión 2.7 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio)

Con la versión 2.7 de AWS Control Tower, AWS Control Tower presenta cuatro nuevos controles preventivos obligatorios de archivo de registros que implementan la política únicamente en los recursos de la Torre de Control de AWS. Hemos modificado las directrices sobre cuatro controles de archivo de registros existentes, pasando de ser obligatorios a optativos, ya que establecen políticas para los recursos ajenos a la Torre de Control de AWS. Este cambio y expansión de control permiten separar la gobernanza de Log Archive para los recursos de la Torre de Control de AWS de la gobernanza de los recursos ajenos a la Torre de Control de AWS.

Los cuatro controles modificados se pueden utilizar junto con los nuevos controles obligatorios para gestionar un conjunto más amplio de archivos de AWS registro. Los entornos AWS Control Tower existentes mantendrán estos cuatro controles modificados habilitados automáticamente para garantizar la coherencia del entorno; sin embargo, estos controles opcionales ahora se pueden deshabilitar. Los nuevos entornos de AWS Control Tower deben habilitar todos los controles electivos. Los entornos existentes deben deshabilitar los controles anteriormente obligatorios antes de añadir el cifrado a los buckets de Amazon S3 que no despliega AWS Control Tower.

Nuevos controles obligatorios:

- No permitir cambios en la configuración de cifrado de los buckets S3 creados por AWS Control Tower en el archivo de registro
- No permitir cambios en la configuración de registro de los buckets S3 creados por AWS Control Tower en el archivo de registro
- No permitir cambios en la política de buckets para los buckets S3 creados por AWS Control Tower en el archivo de registro
- No permitir cambios en la configuración del ciclo de vida de los buckets S3 creados por AWS Control Tower en el archivo de registro

La guía cambió de obligatoria a electiva:

- No permitir cambios en la configuración de cifrado para todos los buckets de Amazon S3 [Anteriormente: habilitar el cifrado en reposo para el archivo de registros]

- No permitir cambios en la configuración de registro para todos los buckets de Amazon S3 [Anteriormente: habilitar el registro de acceso para el archivo de registros]
- No permitir cambios en la política de buckets para todos los buckets de Amazon S3 [anteriormente: no permitir cambios de política en el archivo de registros]
- No permitir cambios en la configuración del ciclo de vida de todos los buckets de Amazon S3 [Anteriormente: establecer una política de retención para el archivo de registros]

La versión 2.7 de AWS Control Tower incluye cambios en el esquema de la zona de aterrizaje de AWS Control Tower que pueden provocar incompatibilidad con versiones anteriores tras la actualización a la 2.7.

- En concreto, la versión 2.7 de la Torre de Control de AWS `BlockPublicAccess` se activa automáticamente en los buckets S3 implementados por la Torre de Control de AWS. Puede desactivar esta opción predeterminada si su carga de trabajo requiere el acceso a todas las cuentas. Para obtener más información sobre lo que ocurre con la `BlockPublicaccess` activación, consulte Bloquear el acceso público a su almacenamiento de Amazon S3.
- La versión 2.7 de AWS Control Tower incluye un requisito de HTTPS. Todas las solicitudes enviadas a los buckets de S3 implementados por AWS Control Tower deben usar una capa de conexión segura (SSL). Solo se permite el paso de las solicitudes HTTPS. Si utilizas HTTP (sin SSL) como punto final para enviar las solicitudes, este cambio generará un error de acceso denegado, lo que podría interrumpir tu flujo de trabajo. Este cambio no se puede revertir después de la actualización 2.7 de tu landing zone.

  Te recomendamos que cambies tus solicitudes para que usen TLS en lugar de HTTP.

Hay tres nuevas AWS regiones disponibles

8 de abril de 2021

(Se requiere una actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower está disponible en tres AWS regiones adicionales: la región de Asia Pacífico (Tokio), la región de Asia Pacífico (Seúl) y la región de Asia Pacífico (Mumbai). Se requiere una actualización de landing zone a la versión 2.7 para expandir la gobernanza a estas regiones.

Tu landing zone no se expande automáticamente a estas regiones cuando realizas la actualización a la versión 2.7, debes verlas y seleccionarlas en la tabla de regiones para incluirlas.

Gobierna únicamente las regiones seleccionadas

19 de febrero de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

La selección de regiones de la Torre de Control de AWS proporciona una mejor capacidad para administrar la huella geográfica de los recursos de la Torre de Control de AWS. Para ampliar el número de regiones en las que aloja AWS recursos o cargas de trabajo (por motivos de conformidad, reglamentarios, económicos u otros motivos), ahora puede seleccionar las regiones adicionales que desee controlar.

La selección de regiones está disponible al configurar una nueva zona de aterrizaje o al actualizar la versión de la zona de aterrizaje de AWS Control Tower. Cuando usa Account Factory para crear una cuenta nueva o inscribir una cuenta de miembro preexistente, o cuando usa Extend Governance para inscribir cuentas en una unidad organizativa preexistente, AWS Control Tower despliega sus capacidades de gobierno de registro, monitoreo y controles centralizados en las regiones que elija en las cuentas. Para obtener más información sobre la selección de regiones, consulte. Configure sus regiones de AWS Control Tower

AWS Control Tower ahora amplía la gobernanza a las unidades organizativas existentes en sus AWS organizaciones

28 de enero de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

Amplíe la gobernanza a las unidades organizativas (OU) existentes (las que no se encuentran en la Torre de Control de AWS) desde la consola de la Torre de Control de AWS. Con esta función, puede incorporar las unidades organizativas de alto nivel y las cuentas incluidas al gobierno de la Torre de Control de AWS. Para obtener información sobre cómo extender la gobernanza a toda una OU, consulteRegistrar una unidad organizativa existente en AWS Control Tower.

Al registrar una OU, AWS Control Tower realiza una serie de comprobaciones para garantizar la correcta extensión de la gobernanza y la inscripción de las cuentas dentro de la OU. Para obtener más información sobre los problemas habituales asociados con el registro inicial de una OU, consulteCausas frecuentes de error durante el registro o la reinscripción.

También puede visitar la página web del producto AWS Control Tower o YouTube visitar este vídeo sobre cómo empezar a utilizar AWS Control Tower for AWS Organizations.

AWS Control Tower ofrece actualizaciones masivas de cuentas

28 de enero de 2021

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

Con la función de actualización masiva, ahora puede actualizar todas las cuentas de una unidad AWS Organizations organizativa (OU) registrada que contenga hasta 300 cuentas, con un solo clic, desde el panel de control de AWS Control Tower. Esto resulta especialmente útil en los casos en los que actualiza la zona de aterrizaje de AWS Control Tower y también debe actualizar las cuentas inscritas para alinearlas con la versión actual de la zona de aterrizaje.

Esta función también le ayuda a mantener sus cuentas actualizadas cuando actualiza su zona de aterrizaje de AWS Control Tower para ampliarla a nuevas regiones o cuando quiere volver a registrar una OU para asegurarse de que todas las cuentas de esa OU tienen aplicados los controles más recientes. La actualización masiva de cuentas elimina la necesidad de actualizar una cuenta a la vez o utilizar un script externo para realizar la actualización en varias cuentas.

Para obtener información sobre la actualización de una landing zone, consulteActualizar la zona de inicio.

Para obtener información sobre cómo registrar o volver a registrar una OU, consulteRegistrar una unidad organizativa existente en AWS Control Tower.

De enero a diciembre de 2020

En 2020, AWS Control Tower publicó las siguientes actualizaciones:

- La consola AWS Control Tower ahora enlaza con reglas de AWS Config externas
- AWS Control Tower ya está disponible en más regiones
- Actualización de Guardrail
- La consola AWS Control Tower muestra más detalles sobre las unidades organizativas y las cuentas
- Utilice AWS Control Tower para configurar nuevos AWS entornos de cuentas múltiples en AWS Organizations
- Personalizaciones para la solución AWS Control Tower
- Disponibilidad general de la versión 2.3 de la Torre de Control de AWS
- Aprovisionamiento de cuentas en un solo paso en AWS Control Tower

- Herramienta de desmantelamiento de AWS Control Tower
- Notificaciones de eventos del ciclo de vida de AWS Control Tower

La consola AWS Control Tower ahora enlaza con reglas de AWS Config externas

29 de diciembre de 2020

(Se requiere una actualización para la versión 2.6 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio)

AWS Control Tower ahora incluye un agregador a nivel de organización, que ayuda a detectar reglas de Config AWS externas. Esto le proporciona visibilidad en la consola de la Torre de Control de AWS para ver la existencia de reglas de AWS Config creadas externamente, además de las reglas de AWS configuración creadas por la Torre de Control de AWS. El agregador permite a AWS Control Tower detectar reglas externas y proporcionar un enlace a la consola AWS Config sin necesidad de que AWS Control Tower tenga acceso a cuentas no administradas.

Con esta función, ahora tiene una vista consolidada de los controles de detección aplicados a sus cuentas para poder realizar un seguimiento del cumplimiento y determinar si necesita controles adicionales para su cuenta. Para obtener más información, consulte Cómo AWS Control Tower agrega AWS Config reglas en unidades organizativas y cuentas no administradas.

AWS Control Tower ya está disponible en más regiones

18 de noviembre de 2020

(Se requiere una actualización para la versión 2.5 de la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio)

AWS Control Tower ya está disponible en 5 AWS regiones adicionales:

- Región de Asia-Pacífico (Singapur)
- Región de Europa (Fráncfort)
- Región de Europa (Londres)
- Región Europa (Estocolmo)
- Región de Canadá (centro)

La adición de estas 5 AWS regiones es el único cambio introducido en la versión 2.5 de AWS Control Tower.

AWS Control Tower también está disponible en la región EE.UU. Este (Norte de Virginia), la región EE.UU. Este (Ohio), la región EE.UU. Oeste (Oregón), la región Europa (Irlanda) y la región Asia Pacífico (Sídney). Con este lanzamiento, AWS Control Tower ya está disponible en 10 AWS regiones.

Esta actualización de landing zone incluye todas las regiones de la lista y no se puede deshacer. Tras actualizar tu landing zone a la versión 2.5, debes actualizar manualmente todas las cuentas inscritas en AWS Control Tower para que gobiernen en las 10 AWS regiones compatibles. Para obtener más información, consulte Configure sus regiones de AWS Control Tower.

Actualización de Guardrail

8 de octubre de 2020

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

Se ha publicado una versión actualizada para el control obligatorio`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED`.

Este cambio en el control es obligatorio porque las cuentas que se inscriban automáticamente en AWS Control Tower deben tener la `AWSControlTowerExecution` función habilitada. La versión anterior del control impedía la creación de este rol.

Para obtener más información, consulte No permitir cambios en las funciones de AWS IAM configuradas por AWS Control Tower y AWS CloudFormation en la Guía de referencia de controles de AWS Control Tower.

La consola AWS Control Tower muestra más detalles sobre las unidades organizativas y las cuentas

22 de julio de 2020

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

Puede ver sus organizaciones y cuentas que no están inscritas en AWS Control Tower, junto con las organizaciones y cuentas que están inscritas.

En la consola de AWS Control Tower, puede ver más detalles sobre sus AWS cuentas y unidades organizativas (OU). La página de cuentas ahora incluye todas las cuentas de su organización, independientemente de la OU o del estado de inscripción en AWS Control Tower. Ahora puede buscar, ordenar y filtrar en todas las tablas.

Utilice AWS Control Tower para configurar nuevos AWS entornos de cuentas múltiples en AWS Organizations

22 de abril de 2020

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Organizations los clientes ahora pueden usar AWS Control Tower para administrar las unidades organizativas (OU) y las cuentas recién creadas gracias a estas nuevas capacidades:

- AWS Organizations Los clientes actuales ahora pueden configurar una nueva landing zone para las nuevas unidades organizativas (OU) en su cuenta de administración existente. Puede crear nuevas unidades organizativas en la Torre de Control de AWS y crear nuevas cuentas en esas unidades organizativas con la gobernanza de la Torre de Control de AWS.
- AWS Organizations los clientes pueden inscribir las cuentas existentes mediante el proceso de inscripción de cuentas o mediante scripts.

AWS Control Tower proporciona un servicio de organización que utiliza otros AWS servicios. Está diseñado para organizaciones con varias cuentas y equipos que buscan la forma más sencilla de configurar su AWS entorno de múltiples cuentas nuevo o existente y de gobernar a escala. Al ser una organización gobernada por la Torre de Control de AWS, los administradores de la nube saben que las cuentas de la organización cumplen con las políticas establecidas. Los creadores se benefician de ello porque pueden aprovisionar nuevas AWS cuentas rápidamente, sin preocuparse indebidamente por el cumplimiento.

Para obtener información sobre la configuración de una landing zone, consulte Planifique la zona de aterrizaje de su AWS Control Tower. También puede visitar la página web del producto AWS Control Tower o YouTube visitar este vídeo sobre cómo empezar a utilizar AWS Control Tower for AWS Organizations.

Además de este cambio, la función de aprovisionamiento rápido de cuentas de AWS Control Tower pasó a llamarse Inscribir cuenta. Ahora permite la inscripción de AWS cuentas existentes, así

como la creación de cuentas nuevas. Para obtener más información, consulte Inscriba una cuenta existente.

Personalizaciones para la solución AWS Control Tower

17 de marzo de 2020

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora incluye una nueva implementación de referencia que le facilita la aplicación de plantillas y políticas personalizadas a la zona de aterrizaje de AWS Control Tower.

Con las personalizaciones de AWS Control Tower, puede usar AWS CloudFormation plantillas para implementar nuevos recursos en las cuentas nuevas y existentes de su organización. También puede aplicar políticas de control de servicios (SCP) personalizadas a esas cuentas, además de las SCP que ya proporciona AWS Control Tower. Las personalizaciones de AWS Control Tower Pipeline se integran con los eventos y las notificaciones del ciclo de vida de AWS Control Tower (Eventos del ciclo de vida en AWS Control Tower) para garantizar que las implementaciones de recursos estén sincronizadas con tu landing zone.

La documentación de implementación de esta arquitectura de soluciones de la Torre de Control de AWS está disponible en la página web de AWS soluciones.

Disponibilidad general de la versión 2.3 de la Torre de Control de AWS

5 de marzo de 2020

(Se requiere una actualización para la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio.)

AWS Control Tower ya está disponible en la AWS región de Asia Pacífico (Sídney), además de en las regiones EE.UU. Este (Ohio), EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón) y Europa (Irlanda). La adición de la región Asia-Pacífico (Sídney) es el único cambio introducido en la versión 2.3 de AWS Control Tower.

Si no ha utilizado AWS Control Tower anteriormente, puede lanzarla hoy mismo en cualquiera de las regiones compatibles. Si ya utiliza la Torre de Control de AWS y desea ampliar sus funciones de gobierno a la región de Asia Pacífico (Sídney) en sus cuentas, vaya a la página de configuración del panel de control de la Torre de Control de AWS. Desde allí, actualiza tu landing zone a la última versión. A continuación, actualiza tus cuentas de forma individual.

> **Note**
>
> La actualización de tu landing zone no actualiza automáticamente tus cuentas. Si tienes más de unas cuantas cuentas, las actualizaciones necesarias pueden llevar mucho tiempo. Por ese motivo, le recomendamos que evite expandir su zona de aterrizaje de AWS Control Tower a regiones en las que no necesite que se ejecuten sus cargas de trabajo.

Para obtener información sobre el comportamiento esperado de los controles de detección como resultado de una implementación en una nueva región, consulte Configurar las regiones de la Torre de Control de AWS.

Aprovisionamiento de cuentas en un solo paso en AWS Control Tower

2 de marzo de 2020

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora admite el aprovisionamiento de cuentas en un solo paso a través de la consola de AWS Control Tower. Esta función le permite aprovisionar nuevas cuentas desde la consola de AWS Control Tower.

Para usar el formulario simplificado, diríjase a Account Factory en la consola de AWS Control Tower y, a continuación, seleccione Aprovisionamiento rápido de cuentas. AWS Control Tower asigna la misma dirección de correo electrónico a la cuenta aprovisionada y al usuario de inicio de sesión único (IAM Identity Center) que se crea para la cuenta. Si necesita que estas dos direcciones de correo electrónico sean diferentes, debe aprovisionar su cuenta a través de Service Catalog.

Actualice las cuentas que cree mediante el aprovisionamiento rápido de cuentas mediante Service Catalog y la fábrica de cuentas de AWS Control Tower, como si actualizara cualquier otra cuenta.

> **Note**
>
> En abril de 2020, la función de aprovisionamiento rápido de cuentas pasó a llamarse Inscribir una cuenta. En junio de 2022, la posibilidad de crear y actualizar cuentas en la consola de AWS Control Tower se separó de la posibilidad de inscribir AWS cuentas. Para obtener más información, consulte Inscriba una cuenta existente.

Herramienta de desmantelamiento de AWS Control Tower

28 de febrero de 2020

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora admite una herramienta de desmantelamiento automatizada que le ayuda a limpiar los recursos asignados por la Torre de Control de AWS. Si ya no tiene intención de utilizar AWS Control Tower para su empresa o si necesita una redistribución importante de los recursos de su organización, puede que desee limpiar los recursos creados cuando configuró inicialmente su landing zone.

Para desmantelar tu landing zone mediante un proceso en su mayoría automatizado, ponte en contacto con nosotros AWS Support para obtener ayuda con los pasos adicionales necesarios. Para obtener más información sobre el desmantelamiento, consulte. Tutorial: Retirar del servicio una zona de aterrizaje de una Torre de Control de AWS

Notificaciones de eventos del ciclo de vida de AWS Control Tower

22 de enero de 2020

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower anuncia la disponibilidad de las notificaciones de eventos del ciclo de vida. Un evento del ciclo de vida marca la finalización de una acción de la Torre de Control de AWS que puede cambiar el estado de los recursos, como las unidades organizativas (OU), las cuentas y los controles que la Torre de Control de AWS crea y administra. Los eventos del ciclo de vida se registran como AWS CloudTrail eventos y se envían a Amazon EventBridge como eventos.

AWS Control Tower registra los eventos del ciclo de vida al completar las siguientes acciones que se pueden realizar con el servicio: crear o actualizar una landing zone; crear o eliminar una OU; habilitar o deshabilitar un control en una OU; y usar Account Factory para crear una nueva cuenta o mover una cuenta a otra OU.

AWS Control Tower utiliza varios AWS servicios para crear y gestionar un AWS entorno de cuentas múltiples basado en las mejores prácticas. Una acción de la Torre de Control de AWS puede tardar varios minutos en completarse. Puede realizar un seguimiento de los eventos del ciclo de vida en CloudTrail los registros para comprobar si la acción originaria de AWS Control Tower se completó correctamente. Puede crear una EventBridge regla para que le notifique cuando CloudTrail registre

un evento del ciclo de vida o para activar automáticamente el siguiente paso de su flujo de trabajo de automatización.

De enero a diciembre de 2019

Del 1 de enero al 31 de diciembre de 2019, AWS Control Tower publicó las siguientes actualizaciones:

- Disponibilidad general de la versión 2.2 de la Torre de Control de AWS
- Nuevos controles optativos en la Torre de Control de AWS
- Nuevos controles de detección en la Torre de Control de AWS
- AWS Control Tower acepta direcciones de correo electrónico para cuentas compartidas con dominios diferentes a los de la cuenta de administración.
- Disponibilidad general de la versión 2.1 de la Torre de Control de AWS

Disponibilidad general de la versión 2.2 de la Torre de Control de AWS

13 de noviembre de 2019

(Se requiere una actualización para la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulteActualizar la zona de inicio.)

La versión 2.2 de AWS Control Tower ofrece tres nuevos controles preventivos que evitan la desviación de cuentas:

- No permitir cambios en los grupos de CloudWatch registros de Amazon Logs configurados por AWS Control Tower
- No permitir la eliminación de las autorizaciones de AWS Config agregación creadas por AWS Control Tower
- No permitir la eliminación del archivo de registros

Un control es una regla de alto nivel que proporciona un control continuo del AWS entorno general. Al crear la zona de aterrizaje de AWS Control Tower, la zona de aterrizaje y todas las unidades organizativas (OU), las cuentas y los recursos cumplen con las normas de gobierno aplicadas por los controles que haya elegido. A medida que tú y los miembros de tu organización utilizáis la landing zone, pueden producirse cambios (accidentales o intencionados) en este estado de

conformidad. La detección de desviaciones le ayuda a identificar los recursos que necesitan cambios o actualizaciones de configuración para resolver las desviaciones. Para obtener más información, consulte Detecte y resuelva desviaciones en la Torre de Control de AWS.

Nuevos controles optativos en la Torre de Control de AWS

5 de septiembre de 2019

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora incluye los siguientes cuatro controles optativos nuevos:

- No permitir acciones de eliminación en buckets de Amazon S3 sin MFA
- No permitir cambios en la configuración de replicación de los buckets de Amazon S3
- No permita acciones como usuario root
- Impedir la creación de claves de acceso para el usuario root

Un control es una regla de alto nivel que proporciona un control continuo del AWS entorno general. Las medidas de seguridad le permiten expresar sus intenciones en forma de política. Para obtener más información, consulte Acerca de los controles de AWS Control Tower.

Nuevos controles de detección en la Torre de Control de AWS

25 de agosto de 2019

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

AWS Control Tower ahora incluye los siguientes ocho nuevos controles de detección:

- Detecte si el control de versiones para los buckets de Amazon S3 está habilitado
- Detecte si la MFA está habilitada para los usuarios de IAM de la consola AWS
- Detecte si la MFA está habilitada para los usuarios de IAM
- Detecte si la optimización de Amazon EBS está habilitada para las instancias de Amazon EC2
- Detecte si los volúmenes de Amazon EBS están conectados a instancias de Amazon EC2
- Detecte si el acceso público a las instancias de bases de datos de Amazon RDS está habilitado
- Detecte si el acceso público a las instantáneas de bases de datos de Amazon RDS está habilitado
- Detecte si el cifrado de almacenamiento está habilitado para las instancias de bases de datos de Amazon RDS

Un control es una regla de alto nivel que proporciona una gobernanza continua para todo el AWS entorno. Un control detectivesco detecta el incumplimiento de los recursos de sus cuentas, como las infracciones de las políticas, y envía alertas a través del panel de control. Para obtener más información, consulte Acerca de los controles de AWS Control Tower.

AWS Control Tower acepta direcciones de correo electrónico para cuentas compartidas con dominios diferentes a los de la cuenta de administración.

1 de agosto de 2019

(No se requiere ninguna actualización para la zona de aterrizaje de AWS Control Tower)

En AWS Control Tower, ahora puede enviar direcciones de correo electrónico para cuentas compartidas (archivo de registro y miembro de auditoría) y cuentas secundarias (vendidas mediante Account Factory) cuyos dominios son diferentes de la dirección de correo electrónico de la cuenta de administración. Esta función solo está disponible cuando creas una nueva landing zone y cuando aprovisionas nuevas cuentas infantiles.

Disponibilidad general de la versión 2.1 de la Torre de Control de AWS

24 de junio de 2019

(Se requiere una actualización para la zona de aterrizaje de AWS Control Tower. Para obtener más información, consulte Actualizar su zona de aterrizaje.)

AWS Control Tower ya está disponible de forma general y es compatible con su uso en producción. AWS Control Tower está pensado para organizaciones con varias cuentas y equipos que buscan la forma más sencilla de configurar su nuevo AWS entorno de múltiples cuentas y gobernar a escala. Con AWS Control Tower, puede asegurarse de que las cuentas de su organización cumplen con las políticas establecidas. Los usuarios finales de los equipos distribuidos pueden aprovisionar nuevas AWS cuentas rápidamente.

Con AWS Control Tower, puede configurar una zona de aterrizaje que emplee las mejores prácticas, como configurar una estructura de varias cuentas mediante AWS Organizations, administrar las identidades de los usuarios y el acceso federado con AWS IAM Identity Center, habilitar el aprovisionamiento de cuentas a través de Service Catalog y crear un archivo de registro centralizado mediante y. AWS CloudTrail AWS Config

Para una gobernanza continua, puede habilitar controles preconfigurados, que son reglas claramente definidas en materia de seguridad, operaciones y conformidad. Las barreras ayudan a evitar el

despliegue de recursos que no se ajustan a las políticas y supervisan continuamente los recursos desplegados para detectar si no se ajustan a las normas. El panel de control de AWS Control Tower proporciona una visibilidad centralizada de un AWS entorno, incluidas las cuentas aprovisionadas, los controles habilitados y el estado de conformidad de las cuentas.

Puede configurar un nuevo entorno de múltiples cuentas con un solo clic en la consola de AWS Control Tower. El uso de AWS Control Tower no conlleva cargos adicionales ni compromisos por adelantado. Solo pagas por los AWS servicios que habilitaste para configurar una landing zone e implementar controles seleccionados.

Historial del documento

- Última actualización de la documentación: 20 de mayo de 2024

En la siguiente tabla se describen los cambios importantes en la Guía del usuario de AWS Control Tower. Para obtener notificaciones sobre las actualizaciones de la documentación, puede suscribirse a la fuente RSS.

Cambio	Descripción	Fecha
AWS Control Tower admite hasta 100 operaciones de control simultáneas	Un aumento de la cuota de operaciones de control simultáneas a 100.	20 de mayo de 2024
La Torre de Control de AWS está disponible en la región Oeste de AWS Calgary (Canadá)	AWS Control Tower está disponible en la región Canadá Oeste (Calgary).	3 de mayo de 2024
AWS Control Tower admite los ajustes de cuota de autoservicio	AWS Control Tower está integrado con AWS Service Quotas en la consola.	25 de abril de 2024
Se trasladó la documentación sobre los controles a una nueva guía	AWS Control Tower publicó la Guía de referencia de controles.	21 de abril de 2024
Etiquetado de `EnabledControl` recursos en AWS CloudFormation	AWS Control Tower permite añadir etiquetas a `EnabledControl` los recursos mediante AWS CloudFormation plantillas.	22 de febrero de 2024
Las API de referencia están disponibles	AWS Control Tower lanzó nuevas API para registrar las unidades organizativas mediante programación.	14 de febrero de 2024

Versión 3.3 de la zona de aterrizaje de AWS Control Tower	Disponible la versión 3.3 de la zona de aterrizaje de AWS Control Tower.	14 de diciembre de 2023
AWS Control Tower anuncia controles para ayudar a la soberanía digital	AWS Control Tower publicó un grupo de controles para ayudar a los clientes con los requisitos de soberanía digital.	27 de noviembre de 2023
AWS Control Tower admite las API de landing zone	AWS Control Tower admite la configuración y el lanzamien to de zonas de aterrizaje mediante nuevas API.	26 de noviembre de 2023
AWS Control Tower admite controles habilitados para etiquetar	AWS Control Tower admite el etiquetado de controles habilitados, en la consola y con las nuevas API.	10 de noviembre de 2023
La Torre de Control de AWS está disponible en Asia Pacífico (Melbourne) Región de AWS	Disponible en la región Asia Pacífico (Melbourne).	3 de noviembre de 2023
Nueva API de control disponibl e	AWS Control Tower lanzó una nueva API de control.	14 de octubre de 2023
AWS Control Tower lanza nuevos controles	AWS Control Tower lanzó nuevos controles proactivos y de detección.	5 de octubre de 2023
Los informes de AWS Control Tower se están desviando de la desactivación del acceso confiable	La Torre de Control de AWS notifica a los clientes cuando se produce una desviación, si los clientes desactivan el acceso de confianza a la Torre de Control de AWS en AWS Organizations.	21 de septiembre de 2023

AWS Control Tower está disponible en cuatro versiones adicionales Regiones de AWS	Disponible en Asia Pacífico (Hyderabad), Europa (España y Zúrich) y Oriente Medio (Emiratos Árabes Unidos).	13 de septiembre de 2023
La Torre de Control de AWS está disponible en la región de Tel Aviv	La Torre de Control de AWS está disponible en la región de Tel Aviv, il-central-1.	28 de agosto de 2023
AWS Control Tower lanza 28 nuevos controles proactivos	AWS Control Tower lanzó 28 nuevos controles proactivos.	24 de julio de 2023
AWS Control Tower desaprueba 2 controles	AWS Control Tower eliminará dos controles de la biblioteca de controles a partir del 18 de agosto de 2023.	18 de julio de 2023
Disponible la zona de aterrizaje 3.2 de AWS Control Tower	Ya está disponible la versión 3.2 de la zona de aterrizaje de AWS Control Tower.	16 de junio de 2023
AWS Control Tower gestiona las cuentas en función de su ID	AWS Control Tower rastrea el ID de la AWS cuenta, en lugar de la dirección de correo electrónico de la cuenta.	14 de junio de 2023
Controles de detección adicionales de Security Hub disponibles	AWS Control Tower añade diez nuevos controles a la biblioteca de controles para el estándar gestionado por el servicio Security Hub: AWS Control Tower.	12 de junio de 2023
AWS Control Tower publica tablas de metadatos de control	AWS Control Tower ahora incluye tablas de metadatos de control como parte de la documentación publicada.	7 de junio de 2023

Soporte de Terraform para la personalización de Account Factory	Soporte de una sola región para los planos de código abierto de Terraform en AFC.	6 de junio de 2023
AWS La autogestión de IAM está disponible para landing zone	AWS Control Tower ahora ayuda a los clientes a elegir su proveedor de identidad para una landing zone.	6 de junio de 2023
Se agregó un nuevo rol	AWS Control Tower agregó una nueva función vinculada al servicio y una política asociada AWSServic eRoleForAWSControlTower,. AWSControlTowerAcc ountServiceRolePolicy	1 de junio de 2023
Actualización de gobernanza mixta	Actualización para asesorar a los clientes sobre la gobernanza mixta.	1 de junio de 2023
Hay controles proactivos adicionales disponibles	Los nuevos controles proactivos le ayudan a controlar su entorno de múltiples cuentas y a cumplir objetivos de control específic os.	19 de mayo de 2023
Siete regiones adicionales disponibles	AWS Control Tower ya está disponible en otros siete países Regiones de AWS: norte de California (San Francisco), Asia Pacífico (Hong Kong, Yakarta y Osaka), Europa (Milán), Oriente Medio (Bahréin) y África (Ciudad del Cabo).	19 de abril de 2023

Cambiar a una política gestionada	La cambiamos AWSControlTowerServiceRolePolicypara que AWS Control Tower pueda llamar a las`EnableRegion` ,`ListRegions` , `GetRegionOptStatus` API implementadas por el servicio de administración de AWS cuentas.	6 de abril de 2023
El seguimiento de las solicitudes de personalización de cuentas está disponible de forma general	AWS Control Tower ahora admite la capacidad de rastrear las solicitudes de personalización de cuentas mediante el flujo de trabajo Account Factory for Terraform (AFT).	16 de febrero de 2023
Actualizaciones de las prácticas recomendadas de IAM	Guía actualizada para adaptarla a las recomendaciones de prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomendadas de seguridad en IAM.	15 de febrero de 2023
Disponible la zona de aterrizaje 3.1 de AWS Control Tower	Ya está disponible la zona de aterrizaje 3.1 de AWS Control Tower.	9 de febrero de 2023
Los controles proactivos están disponibles de forma general	Los controles proactivos se lanzan desde el estado de vista previa hasta la disponibilidad general.	24 de enero de 2023

Operaciones de cuentas simultáneas	AWS Control Tower ahora admite hasta cinco (5) acciones simultáneas en la fábrica de cuentas. Puede crear, actualizar o inscribir hasta cinco cuentas a la vez.	16 de diciembre de 2022
Los controles proactivos ayudan al aprovisionamiento de recursos	AWS Control Tower ahora admite controles proactivos, que se implementan mediante AWS CloudFormation enlaces.	28 de noviembre de 2022
La personalización de la cuenta de fábrica está disponible	AWS Control Tower ahora admite el aprovisionamiento de cuentas con plantillas de cuentas personalizables, denominadas blueprints, directamente desde la consola de la Torre de Control de AWS.	28 de noviembre de 2022
El estado de cumplimiento se puede ver para todas las reglas AWS Config	La Torre de Control de AWS ahora muestra el estado de conformidad de todas AWS Config las reglas implementadas en las unidades organizativas registradas en la Torre de Control de AWS.	18 de noviembre de 2022

Cambiar a una política gestionada	La cambiamos AWSControlTowerServiceRolePolicypara que AWS Control Tower pueda asumir la `AWSControlTowerBlueprintAccess` función, que es necesaria para las personalizaciones de Account Factory.	28 de octubre de 2022
APIs para controles, recursos AWS CloudFormation	AWS Control Tower ahora admite la activación y desactivación de los controles mediante un conjunto de llamadas a la API y un nuevo AWS CloudFormation recurso.	1 de septiembre de 2022
cFct admite la eliminación de conjuntos de pilas	cFct admite la eliminación de conjuntos de pilas mediante la configuración de un parámetro en el archivo de manifiesto.	26 de agosto de 2022
Retención de registros personalizada	Puede personalizar la política de retención de los depósitos de Amazon S3 que almacenan los CloudTrail registros de la Torre de Control de AWS, en incrementos de días o años, hasta un máximo de 15 años.	15 de agosto de 2022
Se encuentra disponible la reparación de la deriva de	AWS Control Tower admite la reparación por desviación de roles, sin necesidad de reparar por completo la zona de aterrizaje.	11 de agosto de 2022

Disponible en la versión 3.0	La versión 3.0 de AWS Control Tower landing zone cambia de rutas basadas en cuentas a AWS CloudTrail rutas basadas en organizaciones, y actualiza la política administrada para habilitar las rutas a nivel de organización. Le permite agregar AWS Config información únicamente en su región de origen. La versión 3.0 también incluye una actualización de la región para denegar el control y dos nuevos controles de detección.	29 de julio de 2022
La página de la organización combina vistas de unidades organizativas y cuentas	La nueva página de organización de la Torre de Control de AWS muestra una vista jerárquica de todas las unidades organizativas (OU) y las cuentas.	18 de julio de 2022
Cambiar a una política administrada	La cambiamos AWSControlTowerServiceRolePolicypara que los clientes puedan tener registros a nivel de organización AWS CloudTrail para agregar AWS CloudTrail registros.	20 de junio de 2022

Inscripción y actualización más sencillas para las cuentas de los miembros	AWS Control Tower ahora le permite inscribir y actualizar las cuentas de los miembros de forma individual, desde su landing zone. Cada cuenta muestra cuándo está disponibl e para una actualización. Separamos el botón Inscribir cuenta del flujo de trabajo Crear cuenta en Account Factory.	31 de mayo de 2022
AFT admite la personalización de cuentas compartidas	AWS Control Tower Account Factory for Terraform ahora admite la personalización de la cuenta de administración, el archivo de registros y las cuentas de auditoría de AWS Control Tower.	27 de mayo de 2022
Operaciones simultáneas para todos los controles opcionales	AWS Control Tower ahora le permite aplicar y quitar barandillas preventivas opcionales de forma simultáne a, así como controles de detección.	18 de mayo de 2022
Cuentas de registro y seguridad existentes	AWS Control Tower ahora admite la posibilidad de incorporar las cuentas de registro y seguridad existente s, en lugar de crear cuentas nuevas durante la configura ción de la landing zone.	16 de mayo de 2022

Disponible la versión 2.9	La versión 2.9 de la zona de landing zone de AWS Control Tower actualiza el reenviador de notificaciones Lambda para que utilice el entorno de ejecución de la versión 3.9 de Python.	22 de abril de 2022
Soporte actualizado para las AWS mejores prácticas, disponible en la versión 2.8	La versión 2.8 de AWS Control Tower landing zone proporciona soporte adicional para garantizar que sus cargas de trabajo y AWS cuentas se ajusten a las prácticas AWS recomendadas.	10 de febrero de 2022
Región: denegar el control	AWS Control Tower ahora incluye un control que le ayuda a restringir el acceso a AWS las regiones, a fin de abordar cuestiones de conformidad y normativas.	30 de noviembre de 2021
Controles de residencia de datos	AWS Control Tower ahora admite controles que le ayudan a administrar la residencia de los datos con un control granular.	30 de noviembre de 2021
Fábrica de cuentas de AWS Control Tower para Terraform	AWS Control Tower ahora es compatible con Terraform para el aprovisionamiento y la actualización automatizados de cuentas.	29 de noviembre de 2021

Disponible un nuevo evento sobre el ciclo de vida	El `PrecheckOrganizationalUnit` evento registra si algún recurso impide que la tarea de gobierno de Extend se lleve a cabo correctamente, incluidos los recursos de las unidades organizativas anidadas.	18 de noviembre de 2021
Unidades organizativas anidadas disponibles	AWS Control Tower ahora permite que su landing zone contenga estructuras de unidades organizativas anidadas.	16 de noviembre de 2021
Simultaneidad de controles de Detectives	Los controles de detección de AWS Control Tower ahora admiten operaciones simultáneas de activación y desactivación.	5 de noviembre de 2021
Hay dos nuevas regiones disponibles	AWS Control Tower ya está disponible en dos nuevas AWS regiones, la región de Europa (París) y la región de Sudamérica (São Paulo).	29 de julio de 2021
Deselección de región	Puede anular la selección de AWS las regiones que ya no desee gobernar a través de AWS Control Tower.	29 de julio de 2021
Claves KMS disponibles	Si lo desea, puede crear o elegir las claves de KMS que administre para cifrar sus datos y recursos.	28 de julio de 2021

Cambie a una política gestionada	La cambiamos AWSControlTowerServiceRolePolicypara que los clientes puedan usar sus propias claves de cifrado de KMS para AWS CloudTrail los registros.	28 de julio de 2021
Los nombres de los controles han cambiado, la funcionalidad no ha cambiado	Algunos nombres y descripciones de los controles se actualizaron para reflejar mejor las intenciones políticas del control, sin cambios en la funcionalidad.	26 de julio de 2021
Escaneos automatizados de los SCP gestionados	AWS Control Tower realiza escaneos automatizados diarios de los SCP gestionados para comprobar si hay desviaciones.	11 de mayo de 2021
Nombres personalizados para unidades organizativas y cuentas	AWS Control Tower le permite proporcionar nombres personalizados durante el proceso de configuración de la landing zone para las unidades organizativas y cuentas esenciales, sin crear problemas.	16 de abril de 2021

El desmantelamiento de una landing zone es autoservicio	AWS Control Tower ahora le permite desmantelar una landing zone sin necesidad de ponerse en contacto con AWS Support. El desmantelamiento es un proceso semiautom atizado que no se puede deshacer. No es lo mismo que eliminar todos los recursos de la Torre de Control de AWS de forma manual.	9 de abril de 2021
Tres regiones adicionales	AWS Control Tower ya está disponible en tres AWS regiones adicionales: la región de Asia Pacífico (Tokio), la región de Asia Pacífico (Seúl) y la región de Asia Pacífico (Mumbai).	8 de abril de 2021

Nuevos controles de Log Archive, disponible la versión 2.7 de landing zone	Cuatro nuevos controles de Log Archive proporcionan la gobernanza de Log Archive sobre los recursos de la Torre de Control de AWS, de forma independiente de la gobernanza de los recursos ajenos a la Torre de Control de AWS. Las directrices sobre los cuatro controles existentes han pasado de ser obligatorias a ser optativas. La versión 2.7 de la zona de aterrizaje de la Torre de Control de AWS incluye un requisito de HTTPS, que no se puede deshacer tras la actualización.	8 de abril de 2021
Selección de región	La selección de regiones de la Torre de Control de AWS proporciona una mejor capacidad para administrar la huella geográfica de los recursos de la Torre de Control de AWS. Para ampliar el número de regiones en las que aloja AWS recursos o cargas de trabajo (por motivos de conformidad, reglamentarios, económicos u otros motivos), ahora puede seleccionar las regiones adicionales que desee controlar.	19 de febrero de 2021

Registre una OU y gestione todas sus cuentas con AWS Control Tower al mismo tiempo	AWS Control Tower añade la capacidad de registrar una OU, que es una forma de incorporar varias cuentas a la gobernanza al mismo tiempo.	28 de enero de 2021
Varias actualizaciones de cuentas en unidades organizativas registradas	Ahora puede actualizar todas las cuentas de cualquier unidad AWS Organizations organizativa (OU) registrada que contenga hasta 300 cuentas, con un solo clic, desde el panel de control de AWS Control Tower. La función de actualización de varias cuentas, también conocida como actualización masiva, elimina la necesidad de actualizar una cuenta a la vez o de utilizar un script externo para realizar la actualización en varias cuentas a la vez.	28 de enero de 2021
Nueva función para agregar unidades organizativas y cuentas no administradas	Un nuevo rol ayuda a detectar AWS Config reglas externas, por lo que AWS Control Tower no necesita acceder a cuentas no administradas.	29 de diciembre de 2020

AWS Control Tower está disponible en más AWS regiones.	AWS Control Tower ya está disponible para su implementación en la región de Asia Pacífico (Singapur), la región de Europa (Fráncfort), la región de Europa (Londres), la región de Europa (Estocolmo) y la región de Canadá (Central). Con este lanzamiento, AWS Control Tower ya está disponible en 10 AWS regiones. Esta actualización de landing zone incluye todas las regiones de la lista y no se puede deshacer. Tras actualizar tu landing zone a la versión 2.5, debes actualizar manualmente todas las cuentas inscritas en AWS Control Tower para que gobiernen en las 10 AWS regiones compatibles.	18 de noviembre de 2020
Actualización de control	Se ha publicado una versión actualizada para el control obligatorio`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED` . El control actualizado permite una inscripción automática de cuentas más sencilla.	8 de octubre de 2020

La página de información relacionada ya está disponible para AWS Control Tower	La página de información relacionada facilita la búsqueda de tareas habituales que pueden resultar útiles después de configurar la zona de aterrizaje de la AWS Control Tower.	18 de septiembre de 2020
La consola AWS Control Tower muestra más detalles sobre las unidades organizativas y las cuentas.	En la consola de AWS Control Tower, puede ver más detalles sobre sus AWS cuentas y unidades organizativas (OU). La página «Cuentas» ahora incluye todas las cuentas de su organización, independientemente de la OU o del estado de inscripción en AWS Control Tower. Ahora puede buscar, ordenar y filtrar en todas las tablas.	22 de julio de 2020
AWS Control Tower permite a las organizaciones existentes configurar una landing zone	Ahora puede lanzar una landing zone para la Torre de Control de AWS en una organización existente, a fin de llevar a la organización a la gobernanza. La función de aprovisionamiento rápido de cuentas de AWS Control Tower pasó a llamarse Inscribir cuenta y ahora permite la inscripción de AWS cuentas existentes y la creación de cuentas nuevas.	16 de abril de 2020

AWS Control Tower ya está disponible en Asia Pacífico	AWS Control Tower ya está disponible para su implement ación en la AWS región de Asia Pacífico (Sídney). Esta versión requiere la actualiza ción manual de las cuentas vendidas, solo si planea ejecutar cargas de trabajo en Asia Pacífico (Sídney).	3 de marzo de 2020
Es posible desmantelar una zona de aterrizaje de la AWS Control Tower	AWS Support puede ayudarte a desmantelar permanent emente una landing zone mediante un proceso en su mayoría automatizado que preserva tus organizaciones, aunque es necesario realizar una limpieza manual.	27 de febrero de 2020
El aprovisionamiento rápido de cuentas está disponible en AWS Control Tower	El aprovisionamiento rápido de cuentas facilita el lanzamien to de nuevas cuentas de miembro cuando la zona de inicio está actualizada, con la característica Enroll account (Inscribir cuenta).	20 de febrero de 2020
Los eventos del ciclo de vida se rastrean en AWS Control Tower	Los eventos del ciclo de vida proporcionan detalles adicionales sobre determina dos eventos de la Torre de Control de AWS, a fin de facilitar la automatización del flujo de trabajo.	12 de diciembre de 2019

Las páginas de configuración y actividades están disponibles para AWS Control Tower	Las páginas de configuración y actividades facilitan la actualización de su zona de destino y la visualización de los eventos registrados.	30 de noviembre de 2019
Hay controles preventivos adicionales disponibles para AWS Control Tower	Los controles preventivos de AWS Control Tower mantienen su organización y sus recursos alineados con su entorno.	6 de septiembre de 2019
Hay controles de detección adicionales disponibles para AWS Control Tower	Los controles de Detective de la Torre de Control de AWS proporcionan información sobre el estado de su organización y sus recursos.	27 de agosto de 2019
AWS Control Tower ya está disponible de forma general	AWS Control Tower es un servicio que ofrece la forma más sencilla de configurar y gestionar su AWS entorno de cuentas múltiples a escala.	24 de junio de 2019

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de laGlosario de AWS Referencia.

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.