centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 887D

Guía de configuración segura para entornos multi-cuenta en AWS

Marzo 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.03.26 16:56:21 +01'00'

Pº de la Castellana 109, 28046 Madrid

Nipo: 083-24-122-4

Fecha de Edición: marzo de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA PARA ENTORNOS MULTI-CUENTAEN AWS

1.1. DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es documentar las recomendaciones y las tecnologías de referencia en AWS para la implementación de una estrategia multi-cuenta segura en AWS. Las recomendaciones de seguridad incluidas en esta guía son específicas para aquellos entornos en los que se desee utilizar más de una cuenta en AWS y se deberán, en su caso, complementar con los requisitos y recomendaciones de seguridad explicados, para cualquier entorno AWS en la guía ***CCN-STIC 887A – Guía de Configuración Segura para AWS***, especialmente cuando se busque el cumplimiento del Esquema Nacional de Seguridad en el sistema desplegado en AWS***.***

Es por ello por lo que el uso de esta guía se recomienda para aquellas entidades que por su dimensión u otras necesidades hayan optado por un uso de AWS basado en el modelo de multi-cuenta.

Los principales casos de uso y ventajas de este tipo de estrategia son:

- Perímetros de seguridad y de cargas de trabajo. Algunas entidades precisan un gobierno de todo el entorno que les permita definir restricciones sobre determinados grupos o unidades de trabajo o poder disponer de diferentes controles administrativos sobre los recursos de AWS que les permita aislar cuentas basadas en las cargas de trabajo, el ciclo de vida de desarrollo o la categoría de los datos manejados.

- Definición de perímetros operacionales o administrativos. La entidad puede aprovechar la definición de múltiples cuentas de AWS para limitar departamentos y organizaciones internas.

- Perímetros de cuotas o limites (valores máximos de recursos, acciones e ítems por cada servicio en una cuenta) para que no exista afectación entre entornos o aplicaciones. También es una forma de “sobrepasar” dichas cuotas o límites al poder acceder a mayor cantidad al usar más de una cuenta.

- Control de costes. Al tener los costes correspondientes a los recursos de cada cuenta diferenciados, se puede hacer una mejor gestión y seguimiento.

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS, la cual puede ser consultada en la guía ***CCN-STIC 887A Guía de Configuración Segura para AWS*** en la sección 1.3.

2. SERVICIOS DE AWS DISPONIBLES PARA LA ESTRATEGIA MULTI-CUENTA

Una "Cuenta AWS" es un contenedor de los recursos y datos en la nube de AWS. Una cuenta actúa como un perímetro de aislamiento bien definido de identidad y acceso. Por defecto no hay acceso entre cuentas y debe ser activado haciendo uso de las capacidades de identidad y acceso. Al mismo tiempo, una "Cuenta AWS", funciona como un perímetro de facturación o gasto y un perímetro de consumo o uso de cuotas y límites de llamadas de APIs.

La estrategia multi-cuenta ayuda a crear diferentes perímetros de seguridad y operación separados en entornos, unidades de negocio, equipos con diferentes funciones o incluso diferentes usuarios. A nivel de seguridad, una estrategia multi-cuenta adecuada ofrece a una entidad unas garantías de segregación y permisos operacionales mucho mayores que los de entornos con una única cuenta. Cada entidad deberá valorar la viabilidad de esta estrategia en función de su dimensión e infraestructura.

Con carácter general, la estrategia multi-cuenta será apropiada para organizaciones que requieran profundizar en el aislamiento de diferentes sistemas o entornos, llevar a cabo un control de costos por departamentos o áreas de la organización, limitar el uso de servicios de AWS y gestionar una infraestructura cloud a gran escala. Dentro de estas organizaciones, la decisión sobre las tecnologías a utilizar variará normalmente en función de la sujeción de la organización a un importante control regulatorio y al tamaño:

- Si se trata de una organización grande o sujeta a importantes controles regulatorios, Control Tower resulta una tecnología muy adecuada.

- En caso contrario, normalmente sería suficiente con implementar una estrategia multi-cuenta basada en AWS Organizations.

Desde el punto de vista de definición de la cantidad y función de las diferentes cuentas AWS que puede tener una organización, AWS ha publicado en base a la experiencia de años y miles de clientes, una guía de recomendaciones y ejemplos de este tipo de entornos que se encuentra en este enlace.A continuación, se describen estos servicios y las diferentes recomendaciones de configuración de seguridad, así como otros servicios y recomendaciones adicionales para la implementación de la estrategia multi-cuenta.

2.1. AWS Organizations

AWS Organizations es un servicio de gestión de cuentas que permite consolidar varias cuentas de AWS en una organización que se crea y administra de forma centralizada como una única entidad. En el ámbito de AWS Organizations es importante distinguir entre la cuenta de administración y las cuentas de miembros:

- La cuenta de administración es la cuenta que se usa para crear y

administrar la organización, pudiendo crear o invitar a otras cuentas, eliminar cuentas, aplicar políticas, etc. Solo existe una cuenta de administración, pero una capacidad importante que se debe considerar es la capacidad de delegar algunas funciones de administración de AWS Organizations y algunos servicios en otras cuentas.

- La cuenta de miembros son el resto de las cuentas de la organización. Las cuentas de miembros solamente pueden pertenecer a una organización.

Otros conceptos importantes en AWS Organizations son los de nodo raíz y unidad organizativa. El nodo raíz es el contenedor principal de todas las cuentas de la organización. Si se aplica una política al nodo raíz, esta se aplica a todas las unidades organizativas y cuentas de la organización. La unidad organizativa (OU) es un contenedor de cuentas y de otras unidades organizativas, de modo que se puede crear una jerarquía de árbol con un nodo raíz en la parte superior y ramas de unidades organizativas que terminan en las cuentas. Las OUs pueden anidarse dentro de otras OUs hasta una profundidad de cinco niveles, lo que proporciona flexibilidad en cómo estructurar los grupos de cuentas. Esta capacidad de anidación de OUs conlleva una complejidad adicional para la gestión por lo que deberá implementarse cuando sus beneficios estén correctamente justificados. Cuando se asocia una política a uno de los nodos, ésta se transmite y aplica a todas las cuentas organizativas y hojas que se encuentran debajo. Asimismo, las OUs proporcionan un medio para organizar cuentas de manera que resulte más fácil compartir recursos gestionados de forma centralizada entre cuentas similares. Por ejemplo, con AWS RAM, se pueden utilizar las OUs como base para para compartir recursos de red administrados de forma centralizada, como las subredes de Amazon Virtual Private Cloud (Amazon VPC).

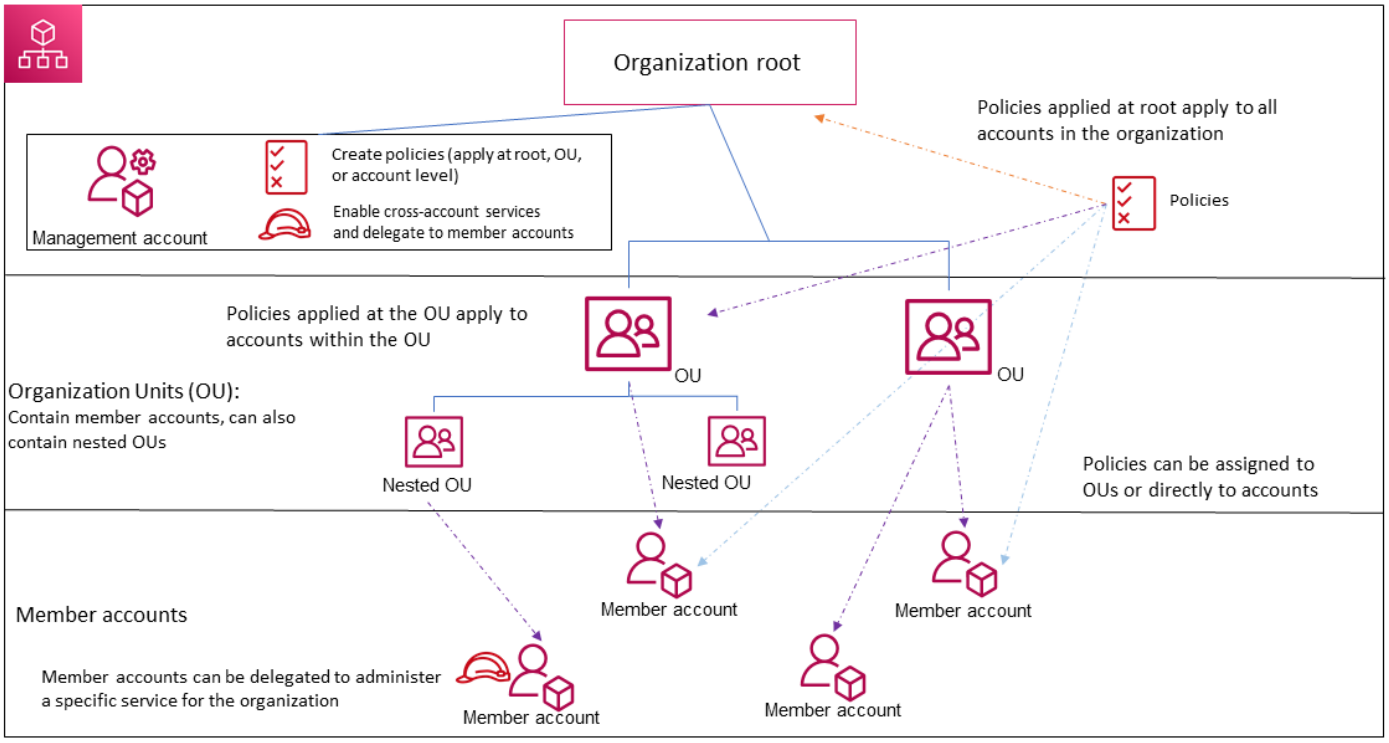

Fig. 1 – Visualización de la distribución jerárquica de cuentas en un entorno multi-cuenta

AWS Organizations incluye todas las prestaciones de facturación unificada y posibilidades de administración de cuentas para satisfacer mejor las necesidades presupuestarias, de seguridad y de conformidad de una entidad. Se recomienda habilitar la opción all features. Esta característica es la mejor forma de trabajar con AWS Organizations e incluye las características de facturación unificada. Al crear una organización, las características se habilitan de manera predeterminada. Si están habilitadas todas las características, puede utilizar las de administración avanzada de cuentas disponibles en AWS Organizations como Integración con servicios admitidos de AWS y políticas de administración de la organización. AWS Organizations ofrece las siguientes funcionalidades:

Administración centralizada de todas las cuentas de AWS

Permite combinar las cuentas existentes en una organización para poder administrar las cuentas de forma centralizada. Se pueden crear cuentas que se conviertan automáticamente en parte de la organización y puede invitarse a otras cuentas a que se unan a una organización.

Facturación unificada para todas las cuentas miembro

Es posible utilizar la cuenta de administración de la organización para consolidar y pagar por todas las cuentas miembro. En la facturación consolidada, las cuentas de administración también pueden obtener acceso a la información de facturación, la información de cuenta y la actividad de cuenta de las cuentas miembro de la organización. Esta información se puede utilizar para servicios como AWS Cost Explorer, que puede ayudar a las cuentas de administración a mejorar el rendimiento de los costes de la organización.

Utilización de Políticas de Control de Servicios (SCPs)

El administrador de la cuenta de administración de una organización puede utilizar políticas de control de servicios (SCP) para especificar los permisos máximos para las cuentas miembro de la organización. En SCPs, se pueden restringir los servicios, recursos y acciones individuales de la API de AWS a los que pueden obtener acceso los usuarios y roles de cada cuenta miembro. También permiten definir condiciones respecto a cuándo restringir el acceso a los servicios, los recursos y las acciones de la API de AWS. Estas restricciones se aplican incluso a los administradores de las cuentas miembro de la organización. Cuando AWS Organizations bloquea el acceso a una acción de la API, un recurso o un servicio en una cuenta de miembro, un usuario o rol de dicha cuenta no puede acceder a ella. Este bloqueo permanece en vigor, aunque un administrador de una cuenta de miembro conceda dichos permisos de forma explícita en una política de AWS IAM. Es decir, los bloqueos de las políticas de control de servicios prevalecen sobre los permisos de las políticas AWS IAM.

Los permisos de las políticas de control de servicios se heredan de los niveles más altos a los más bajos de la organización. Es decir, cuando se asignan a una unidad organizativa, son heredados por las cuentas y unidades organizativas que dependen de esa unidad organizativa. Cada SCP puede filtrar los permisos que pasan a los niveles inferiores. Si una instrucción de denegación bloquea una acción, se deniega esa acción a todas las unidades organizativas afectadas por esa SCP. Una SCP en un nivel inferior no puede agregar un permiso después de que una SCP lo deniegue en un nivel superior ni puede agregar permisos. Además, las SCP admiten operadores de herencia que alteran la forma en la que se heredan los elementos de una política.

Para obtener más información, puede consultarse la documentación de Políticas de Control de Servicios (SCP).

Pueden aplicarse políticas de control de servicios para múltiples finalidades como, por ejemplo, excluir servicios como los de IA, denegar acceso a regiones específicas de AWS, evitar que los usuarios y roles realicen determinados cambios, o aplicar planes de AWS Backup a los recursos de todas las cuentas.

A la hora de gestionar las políticas se debe asignar una acción a las políticas creadas para mantener una estrategia de permitir/denegar. Encontrará más información de la administración de permisos en este enlace.

Agrupación jerárquica de cuentas para satisfacer las necesidades de seguridad, de conformidad y presupuestarias

AWS Organizations permite agrupar diferentes cuentas en unidades organizativas y asociar diferentespolíticas de acceso a cada una de ellas, así como aislar cargas de trabajo o aplicaciones con requisitos de seguridad específicos. Por ejemplo, si una organización dispone de diferentes aplicaciones ejecutándose en AWS y necesita cumplir el Esquema Nacional de Seguridad sobre solamente una de ellas, puede incluirse en una unidad organizativa y asociar una política a dicha OU

que bloquee el acceso a los servicios que no cumplan con los requisitos normativos.

Integración con otros servicios de AWS

Se pueden aprovechar los servicios de administración de varias cuentas de AWS Organizations con servicios seleccionados de AWS para realizar tareas en todas las cuentas que son miembros de una organización. Para obtener una lista de los servicios y los beneficios de utilizar cada servicio en la organización se puede consultar la documentación de: Servicios de AWS que se pueden utilizar con AWS Organizations.

Recomendaciones para el control de acceso - AWS Organizations

Utilización de un alias de correo para la cuenta de administración de AWS Organizations

La seguridad de la cuenta de administración en AWS Organizations ha de ser correctamente protegida mediante el uso de un correo electrónico administrado por la entidad. No debe usarse un proveedor de correo electrónico público ni uno administrado por un tercero.

Es recomendable utilizar una dirección de correo electrónico que reenvíe los mensajes recibidos directamente a una lista de administradores. En caso de que AWS necesite ponerse en contacto con el propietario de la cuenta, por ejemplo, para confirmar el acceso, el mensaje de correo electrónico se distribuye a varias partes. Este enfoque ayuda a reducir el riesgo de retrasos en las respuestas, por ejemplo, en casos de indisponibilidad del personal.

Implementación de mecanismos robustos de autenticación

Para una protección adecuada del acceso a las cuentas de los usuarios en AWS, en línea con las medidas de seguridad que se describen en el apartado *Mecanismo de Autenticación (Usuarios de la organización) [op.acc.6]* de la Guía ***CCN-STIC 887A Guía de Configuración Segura para AWS,*** se recomienda la implantación de las siguientes medidas, también en el ámbito de un entorno multi-cuenta:

- Utilizar políticas de contraseñas seguras, tanto para el usuario root como para el resto de los usuarios, si bien es recomendable que el usuario root esté configurado de forma más restrictiva.

- Almacenar la contraseña en un sistema o herramienta de administrador de contraseñas bajo controles y procesos adicionales. Si se utiliza un administradorde contraseñas, deberá funcionar sin conexión. Para evitar la creación de una dependencia circular, no se deberán almacenar la contraseña de usuario root con herramientas que dependan de servicios de AWS en los que se inicie sesión con la cuenta protegida.

- Implementación del doble factor de autenticación con mecanismos de software o hardware para proporcionar una capa adicional de verificación. (Desde mediados de 2024 esta medida será de obligatorio cumplimiento para la cuenta root de la organización, por lo que se recomienda incluirlo

tan pronto como sea posible).

Para obtener más información de estas recomendaciones se puede consultar las Prácticas recomendadas para la administración de varias cuentas.

Integración de AWS Organizations e IAM

El administrador de la cuenta de administración de una organización puede controlar el acceso a los recursos de AWS asociando políticas de permisos a identidades (usuarios, grupos y roles) de AWS Identity and Access Management (AWS IAM) dentro de la organización. AWS IAM permite un control detallado de los usuarios y las funciones en las cuentas individuales. Al conceder permisos, se decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas se permiten en esos recursos. Si los permisos se conceden a un rol, ese rol puede ser asumido por usuarios de otras cuentas de la organización. AWS Organizations amplía ese control a nivel de cuenta para permitir el control de lo que los usuarios y funciones de una cuenta o grupo de cuentas pueden hacer. Los permisos resultantes son la intersección lógica de lo que permite AWS Organizations en el nivel de cuenta y los permisos que AWS IAM concede explícitamente en el nivel de usuario o de rol dentro de esa cuenta. Esta integración también incluye la capacidad de definir "permission boundaries" o límites de permisos a nivel de la organización. Un límite de permisos es una característica avanzada para usar una política administrada con el fin de definir los permisos máximos que una política basada en identidad puede conceder a una entidad de AWS IAM. Un límite de permisos para una entidad le posibilita realizar las acciones que le permitan tanto sus políticas basadas en identidad como sus límites de permisos.

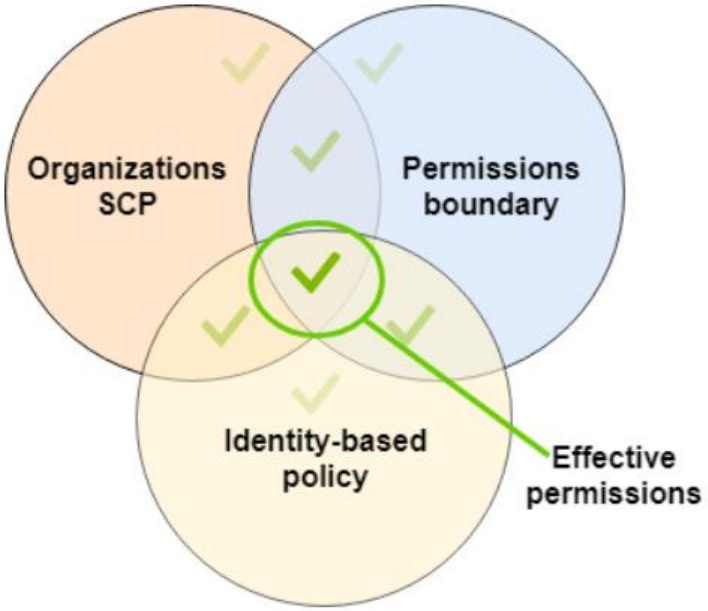

Fig. 3 – Ejemplo de uso de límites de permisos

Es recomendable dejar la cuenta de administración sin uso y con las medidas de seguridad pertinentes y delegar la administración de la organización en cuentas

con privilegios de administración. Para ello, se deben crear usuarios, grupos o roles con la siguiente política para realizar las tareas de administración desde AWS IAM mediante la siguiente configuración de la política “Action”: ”organizations:*” Otras políticas recomendadas son la limitación del consumo de recursos a determinadas regiones específicas definidas por los administradores o impedir que los usuarios puedan deshabilitar o modificar servicios relacionados con el área de seguridad como AWS Config o Amazon CloudWatch.

En todo caso, la asignación de privilegios a los usuarios a través de las políticas de AWS IAM deberá hacerse siguiendo el principio de privilegios mínimos y concediendo únicamente aquellos permisos que sean estrictamente necesarios.

La asignación de permisos a través de políticas AWS IAM, es decir, asignando permisos a identidades de AWS IAM (usuarios, grupos y roles) se constituye como una estrategia RBAC (*Role Based Access Control*), mientras que el modelo ABAC (*Attribute Based Access Control*) en AWS se implementa a través del uso de etiquetas, tal y como se describe en el siguiente apartado.

Recomendaciones para el inventariado y etiquetado de activos - AWS Organizations

El etiquetado de recursos en AWS, consistente en la asignación de metadatos en forma de etiquetas (tags) a los diferentes recursos, es una técnica esencial para mantener una coherencia en la identificación y la gestión unificada de configuración de recursos pertenecientes, por ejemplo, a un mismo departamento de la entidad o a una pila aplicativa concreta, en función de la estrategia de etiquetado escogida por la organización.

Además del etiquetado de recursos a nivel de cuenta, AWS Organizations admite el etiquetado, desde la cuenta de administración, de cuentas de AWS, unidades organizativas, nodos raíz de la organización y políticas.

Las políticas de etiquetas son un tipo de política que le puede ayudar a estandarizar las etiquetas en todos los recursos en las cuentas de la organización. En una política de etiquetas, se especifican las reglas de etiquetado aplicables a los recursos cuando se etiquetan. Una política de etiquetas también puede especificar que no se puedan completar las solicitudes de etiquetado no conformes con la política en los tipos de recursos especificados, siendo recomendable su aplicación para impedir que los usuarios creen recursos que no cumplan con las políticas de etiquetado.

Algunas buenas prácticas que se recomienda seguir en el uso de políticas de etiquetas son las siguientes:

- Elegir una estrategia de uso de mayúsculas y minúsculas: Determinar cómo se desean utilizar las mayúsculas y minúsculas en las etiquetas e implementar de forma coherente esta estrategia en todos los recursos, utilizando la misma convención para todas las etiquetas. Esto permite obtener resultados coherentes en los informes de conformidad.
- Utilizar el flujo de trabajo recomendado: Comenzar poco a poco creando una política de etiquetas sencilla y asociarla a una cuenta miembro que se

pueda utilizar con fines de prueba. Utilizar los flujos de trabajo descritos en el documento: Introducción a las políticas de etiquetas.

- Determinar las reglas de etiquetado. Cree políticas de etiquetas que definan etiquetas conformes y asócielas a entidades de la organización en las que desee que entren en vigor dichas reglas de etiquetado.
- Forme a los administradores de la cuenta, en relación con la estrategia del etiquetado, el uso de las etiquetas y las instrucciones para la comprobación de la conformidad de las políticas de etiquetas.
- Actúe con precaución al ejecutar el cumplimiento. Forzar el cumplimiento puede impedir que los usuarios de las cuentas de la organización etiqueten los recursos que necesiten.

Puede encontrar más información sobre el uso de políticas de etiquetas en: Políticas de etiquetas

Recomendaciones para la monitorización y el registro de la actividad - AWS Organizations

Además de la monitorización de los recursos desplegados en AWS a nivel de cuenta, AWS Organizations permite su integración con dos tecnologías de monitorización de AWS que permiten monitorizar la organización y la actividad que allí se produce:

Registrar llamadas a la API de AWS Organizations con AWS CloudTrail

En primer lugar, AWS se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones hechas por usuarios, roles o servicios de AWS, capturando llamadas a la API de AWS Organizations como eventos, incluidas las llamadas procedentes de la consola de AWS Organizations y las llamadas de código a las API de AWS Organizations. En la integración de AWS Organizations con AWS CloudTrail es recomendable:

- Habilitar el servicio AWS CloudTrail para todas las regiones como una política de la organización para todas las unidades organizativas.
- Habilitar la entrega continua de aquellos eventos que sean especialmente relevantes a un bucket de Amazon S3, si bien los eventos más recientes se pueden ver en el historial de eventos de AWS CloudTrail.

Cada una de las entradas de registro contiene información sobre quién generó la solicitud. La información de identidad del usuario en la entrada de registro ayuda a determinar:

- Si la solicitud se realizó con las credenciales del usuario root o del usuario de AWS IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol AWS IAM o un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Algunas de las entradas de registro registradas por AWS CloudTrail para el

registro de los eventos relacionados con AWS Organizations son las siguientes:

- CloseAccount: Cierre de una cuenta.
- CloseAccountResult: Resultado después de que el flujo de trabajo en segundo plano para cerrar una cuenta se complete correctamente.
- CreateAccount: Creación de una cuenta.
- CreateAccountResult: Resultado después de que el flujo de trabajo en segundo plano de creación de una cuenta se complete correctamente.
- CreateOrganizationalUnit: Creación de una unidad organizativa.
- InviteAccountToOrganization: Invitación de una cuenta a una organización.
- AttachPolicy: Asignación de política a entidad.

AWS Organizations y Amazon CloudWatch Events

Asimismo, AWS Organizations puede operar con Amazon CloudWatch Events para iniciar eventos cuando se producen las acciones especificadas por el administrador en una organización. Es posible configurar Amazon CloudWatch Events para que los eventos registrados se envíen a un objetivo definido por el administrador. Por ejemplo, que cuando se produzca una de las acciones definidas se envíe un correo electrónico o un mensaje de texto a los suscriptores de un tema de Amazon SNS, o que se ejecute una función AWS Lambda creada para registrar los detalles de la acción de modo que pueda revisarse más adelante.

Recomendaciones para las copias de seguridad - AWS Organizations

Con AWS Organizations se pueden asociar políticas de copias de seguridad a cualquiera de los elementos de la estructura de la organización, como el nodo raíz, las unidades organizativas y las cuentas individuales. AWS Organizations aplica las reglas de herencia para combinar las políticas del nodo raíz de la organización, de las unidades organizativas principales o asociadas a la cuenta, dando como resultado una política de copia de seguridad para cada cuenta. Por ejemplo, se puede asociar una política de copia de seguridad al nodo raíz que especifique la frecuencia de las copias de seguridad y, a continuación, asociar una política a las unidades organizativas que sobrescriben la frecuencia de las copias de acuerdo con los requisitos de frecuencia de las copias de seguridad de cada cuenta.

Es importante tener en cuenta que las políticas resultantes deben tener todos los elementos necesarios, de lo contrario, AWS Backup considera que la política no es válida y no hace copia de seguridad de los recursos afectados. Por ello, aunque una estrategia de política parcial como la anteriormente descrita puede funcionar, es recomendable que todas las políticas de copia de seguridad estén completas y sean válidas por sí mismas. Para ello, se puede utilizar los valores predeterminados asociados al nivel más alto de la jerarquía y remplazarlos cuando sea necesario en las políticas secundarias.

Algunas buenas prácticas que se recomienda seguir en el uso de políticas de

copias de seguridad son las siguientes:

- Decidir una estrategia de política de copia de seguridad. Tal y como se ha expuesto, si se crean políticas de copias de seguridad en partes incompletas que se heredan y fusionan para crear una política completa de cada cuenta miembro, se corre el riesgo de terminar con una política en vigor incompleta si se realiza un cambio en un nivel sin considerar detenidamente el impacto en todas las cuentas que estén por debajo de ese nivel. Por ello, se recomienda que las políticas de copias de seguridad a implementar en cada cuenta estén completas por sí mismas. Gracias a ello, en todo caso, la política de seguridad de cada cuenta estará completa.
- Validar los cambios realizados en las políticas de copias de seguridad. Cuando se realiza un cambio, se recomienda comprobar las políticas en vigor de las cuentas que están por debajo del nivel que haya realizado el cambio para asegurarse que el cambio tenga el impacto previsto. Esto se puede hacer mediante la consola de administración o mediante la operación de la API GetEffectivePolicy o una de sus variantes de AWS SDK, describe-effective-policy o AWS CLI, DescribeEffectivePolicy.
- Comenzar de forma sencilla y hacer pequeños cambios. Para simplificar la depuración, es recomendable comenzar con políticas sencillas y realizar cambios de un elemento cada vez, validando el comportamiento y el impacto de cada cambio antes de realizar el siguiente.
- Almacenar copias en otras regiones de AWS y cuentas de la organización[1].
    - Si se almacenan las copias de seguridad en Regiones de AWS, se ayuda a proteger la copia contra daños accidentales o eliminaciones en la región original.
    - Si se almacena en una cuenta diferente, se añade una barrera de seguridad que ayuda a proteger contra un actor malintencionado que pone en peligro una de las cuentas.
- Limitar el número de planes por política. En las políticas que contienen varios planes es más complicado solucionar problemas ya que hay que validar un mayor número de salidas.
- Utilizar stack sets para crear los almacenes de copias de seguridad y los roles de AWS IAM necesarios. La integración de AWS Organizations con los stack sets de AWS CloudFormation permite crear automáticamente los almacenes de las copias de seguridad y los roles de AWS IAM.
- Comprobar los resultados revisando la primera copia de seguridad creada en cada cuenta. Tras la realización de un cambio en una política, es recomendable comprobar la siguiente copia de seguridad creada después del cambio para asegurarse de que el cambio tuvo el impacto deseado.

[1] Esta funcionalidad permite soportar el cumplimiento de la medida de seguridad del ENS Copias de Seguridad [mp.info.6]: Ver la Guía ***CCN-STIC 887A Guía de Configuración Segura para AWS***, apartado Copias de seguridad [mp.info.6].

Puede encontrar más información sobre la integración de AWS Organizations y AWS Backup en el recurso, Políticas de copia de seguridad.

2.2. AWS Control Tower

AWS Control Tower crea una abstracción u orquestación que combina e integra las capacidades de otros servicios de AWS, incluidos AWS Organizations, AWS Identity Center (sucesor de AWS SSO) y AWS Service Catalog. Al emplear el modelo multi-cuenta, es beneficioso tener una capa de orquestación que facilite el despliegue y el gobierno de las cuentas, pudiendo emplear Control Tower como principal forma de aprovisionar servicios e infraestructura.

Con AWS Control Tower, los usuarios finales en equipos distribuidos pueden aprovisionar rápidamente nuevas cuentas de AWS. Mientras tanto, los administradores de la nube central saben que todas las cuentas están alineadas con las políticas de cumplimiento establecidas centralmente en toda la entidad.

AWS Control Tower incluye las siguientes características:

Landing zone

Una landing zone es un entorno multi-cuenta de AWS que se configura automáticamente con una buena arquitectura basada en las mejores prácticas de seguridad y conformidad. Es la infraestructura base que contiene todas las unidades organizativas (OU), cuentas, usuarios y otros recursos que la entidad desea que estén sujetos a la normativa de cumplimiento. Una landing zone puede escalarse para adaptarse a las necesidades de una empresa de cualquier tamaño.

Cuando se crea una landing zone, AWS Control Tower realiza las siguientes acciones en la cuenta de administración (la cuenta creada específicamente para la landing zone):

- Crea dos Unidades Organizativas incluidas en la estructura raíz de la organización: Security y Sandbox (opcional).
- Crea o agrega dos cuentas compartidas en la unidad organizativa de seguridad:
  - La cuenta Log Archive: Esta cuenta funciona como un repositorio de registro de las actividades de las API y las configuraciones de los recursos de todas las cuentas de la landing zone.
  - La cuenta Audit. Una cuenta restringida que está diseñada para que los equipos de seguridad y de cumplimiento, mediante permisos de lectura y escritura, puedan revisar las cuentas de la landing zone.

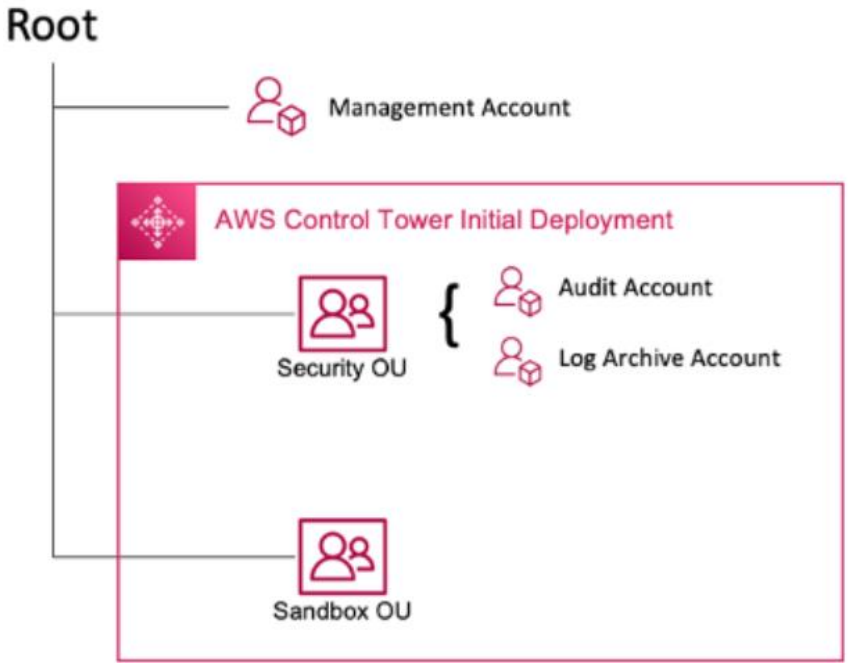

Fig. 4 – Estructura de unidades organizativas y cuentas creadas en la cuenta de administración

Posteriormente, AWS Control Tower permite la creación, registro y gestión de unidades organizativas adicionales para implementar los controles:

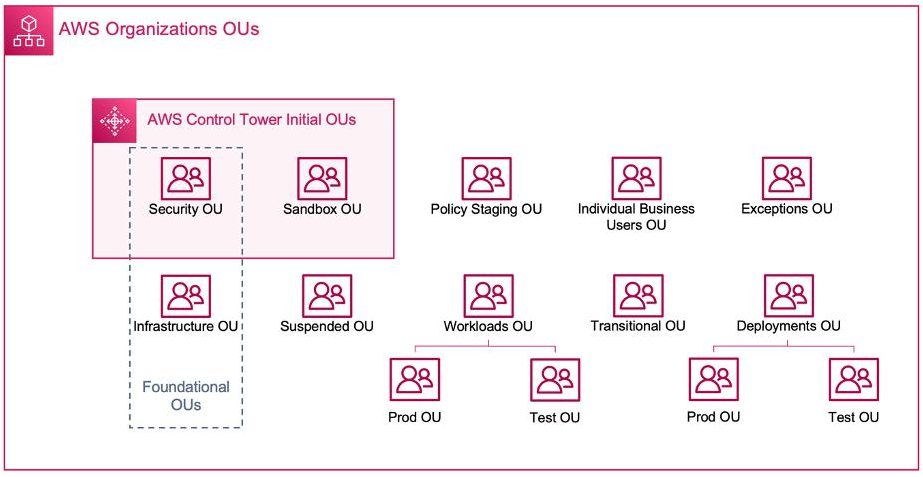

Fig. 5 Unidades organizativas inicialmente desplegadas por AWS Control Tower y ejemplos de unidades organizativas adicionales desplegadas

- Crea un directorio nativo de la nube en AWS IAM Identity Center, con grupos preconfigurados y acceso con inicio de sesión único.

- Aplica todos los controles preventivos obligatorios para hacer cumplir las políticas (los controles preventivos no se aplican a la cuenta de administración, a excepción de esta, todos los controles se aplican a la organización en su conjunto.).

- Aplica todos los controles de detección obligatorios para detectar infracciones de configuración.

Controles

Un control es una regla de alto nivel implementada por Control Tower que proporciona una gobernanza continua para el entorno de AWS. Los controles aplican a toda una unidad organizativa (siempre y cuando la OU se haya creado dentro de la landing zone) y afecta a todas las cuentas de dicha OU. Por lo tanto, cuando los usuarios trabajan en cualquier cuenta de la landing zone, siempre están sujetos a los controles que rigen la unidad organizativa.

Los controles se clasifican según su comportamiento y su orientación.

- Controles por comportamiento:
    - Preventivos: garantizan que las cuentas cumplan con las normas ya que impide las acciones que provocan infracciones de las políticas. Se implementan mediante políticas de control de servicios, que forman parte de AWS Organizations.
    - Detectivos: Detecta incumplimientos de los recursos de las cuentas y envía alertas as través del panel de control. Se implementan mediante AWS Config rules.
    - Proactivos: Comprueban los recursos antes de aprovisionarlos y se aseguran de que cumplan con el control. Si un recurso no cumple las normas, no se aprovisionarán. Se implementan mediante AWS CloudFormation hooks.
- Controles por orientación:
    - Obligatorios: Siempre se aplican en la landing zone, no se pueden desactivar en ninguna unidad organizativa.
    - Altamente recomendados: Diseñados para aplicar algunas de las mejores prácticas comunes en entornos con varias cuentas.
    - Electivos: Permiten rastrear o bloquear las acciones que normalmente están restringidas en un entorno empresarial.

Al crear una landing zone, AWS Control Tower habilita todos los controles obligatorios de forma predeterminada. Los controles altamente recomendados y electivos no están habilitados de forma predeterminada y se aplican a discreción de los administradores. Para consultar el listado de controles de AWS Control Tower, consulte la biblioteca de controles.

Account Factory

Un Account Factory es una plantilla de cuentas configurable que ayuda a estandarizar el aprovisionamiento de nuevas cuentas 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 la organización. Para más información, consultar el documento: Account Factory.

Panel de control

El panel de control ofrece una supervisión continua de la landing zone al equipo de administradores centrales de la nube. El panel de control puede usarse para ver las cuentas aprovisionadas en toda la entidad, los controles habilitados para la aplicación de políticas y para la detección continua del incumplimiento y los recursos no conformes organizados por cuentas y unidades organizativas.

Recomendaciones para la arquitectura de seguridad – AWS Control Tower

Más allá de la arquitectura predeterminada de la landing zone, se debe implementar una correcta distribución de recursos entre cuentas para contar con una buena arquitectura de seguridad. Una vez que AWS Control Tower haya configurado la primera unidad organizativa (la unidad organizativa de seguridad), es recomendable crear algunas unidades organizativas y cuentas adicionales:

- Unidad organizativa (OU) de seguridad[2]. Desplegada por defecto por la landing zone, se utiliza para alojar los accesos y servicios relacionados con la seguridad. La OU de seguridad, así como sus OU hijas y cuentas de AWS asociadas, deben pertenecer y ser administradas por su organización de seguridad. Dentro de esta OU se pueden asociar las siguientes cuentas:
    - Archivo de logs. Actuaría como punto de consolidación para el acceso orientado a los registros de auditoría recopilados de todas las cuentas.
    - Seguridad – solo lectura. Permitiría que los miembros del equipo de seguridad accedan a otras cuentas de AWS con permisos de solo lectura para llevar a cabo auditorías, pruebas de seguridad e investigaciones.
    - Breakglass. Se utilizaría únicamente para el caso de incidentes de seguridad. Esta cuenta permitiría un acceso de escritura secundario al resto de cuentas de AWS y se utilizaría para asignar permisos de acceso temporales (durante el incidente) a los miembros del equipo de seguridad.
    - Herramientas de seguridad. Una o varias cuentas destinadas al alojamiento de cargas de trabajo y servicios de seguridad, herramientas y datos de soporte. Es recomendable disponer de

[2] La utilización de la unidad organizativa de seguridad y sus cuentas asociadas, con una asignación de permisos basada en el principio de privilegios mínimos, puede servir para el cumplimiento de los refuerzos opcionales R2 – Privilegios de auditoría y R3 – acceso a información de seguridad de la medida de seguridad del ENS Segregación de funciones y elementos de configuración [op.acc.3] en entornos multi-cuenta. (Ver Guía ***CCN-STIC 887A – Guía de Configuración Segura para AWS***, apartado Segregación de funciones y tareas [op.acc.3]).

una cuenta principal para Amazon GuardDuty, otra para AWS Security Hub, otra cuenta para Amazon Detective y una última para servicios de monitorización de terceros en caso de haberlos. El acceso humano a estas cuentas de AWS debería reducirse al mínimo imprescindible, tratando de llevar a cabo las tareas de administración a través de la Infraestructura como Código y técnicas de automatización.

- Unidad organizativa sandbox. El despliegue de esta unidad organizativa es opcional en el momento de creación de la landing zone. Se recomienda utilizar esta OU de manera aislada a las redes de producción para que los usuarios individuales profundicen y aprendan sobre los servicios de AWS. Es aconsejable establecer un límite de gasto fijo.

- Unidad organizativa de infraestructura. Utilizada para los servicios de infraestructura compartidos como redes y servicios TI, que pueden ser compartidos, por ejemplo, por las cuentas de producción y desarrollo. Esta unidad organizativa también se puede separar en dos unidades organizativas, una para los tests de infraestructura en preproducción y otra para la infraestructura en producción.

- Unidad organizativa de cargas de trabajo. Se recomienda aislar las cargas de trabajo en una unidad organizativa independiente que no dependa de otras OU para que la aplicación implementada sea más resistente a cambios organizativos. Esta unidad organizativa también se puede separar en dos unidades organizativas, una para los test de cargas de trabajo en preproducción[3] y otra para las cargas de trabajo en producción.

- Unidad organizativa PolicyStaging: Esta cuenta permite a los administradores del sistema probar los cambios en las políticas y los controles antes de aplicarlos definitivamente. Se recomienda crear unidades organizativas y cuentas hijas para probar los cambios y, cuando los cambios sean aprobados en este entorno, desplegarlos en toda la organización.

- Unidad organizativa suspendida: Ofrece una ubicación para las cuentas que han sido deshabilitadas temporalmente y que están a la espera de ser eliminadas de la organización. Se debe asignar una política de control de servicios a esta OU que deniegue todas las acciones y asegurarse de que las cuentas están etiquetadas con detalles (como su procedencia) para su trazabilidad para el caso de que sea necesario restaurarlas.

[3] La utilización de la unidad organizativa de cargas de trabajo y la su unidad organizativa asociada de cargas de trabajo en preproducción puede servir para el cumplimiento del refuerzo R2 – Pruebas de la medida de seguridad del ENS Aceptación y puesta en servicio [mp.sw.2] en entornos multi-cuenta.

Además, otras unidades organizativas adicionales también pueden ser:

- Unidad organizativa de usuarios de negocio individuales: OU de acceso limitado para cuentas de usuarios que no son tecnológicos y que utilizarían AWS para funciones de productividad, como la compartición de informes o archivos a través de buckets Amazon S3.

- Unidad organizativa excepciones: De uso residual, para cuando se necesite justificadamente aplicar excepciones a las condiciones de seguridad en las OU de cargas de trabajo. Las cuentas bajo esta OU deben tener políticas de control de servicios aplicadas directamente a la cuenta en vez de la OU, debido a la naturaleza personalizada de los casos de uso.

- Unidad organizativa transitoria. Está pensada como un área temporal para las cuentas y carga de trabajo existentes antes de integrarlas formalmente en las áreas más estandarizadas de la estructura del entorno AWS.

- Unidad organizativa de implementaciones: Contiene cuentas destinadas a despliegues CI/CD. Se puede crear esta OU si se tiene un modelo operativo y de gobierno diferente para las implementaciones de CI/CD en comparación con las cuentas de las OU de las cargas de trabajo.

Recomendaciones para el control de acceso – AWS Control Tower

Habilitación de AWS IAM Identity Center y utilización de un proveedor de identidades externo

Se recomienda la habilitación de AWS IAM Identity Center en la misma región que la de origen de AWS Control Tower. AWS IAM Identity Center solamente se puede instalar en la cuenta de administración de una organización y deberá utilizarse una de las tres fuentes de identidad que permite:

- Tienda de usuarios de AWS IAM Identity Center. Si se elige esta opción, AWS Control Tower crea grupos en el directorio de AWS IAM Identity Center y proporciona acceso a estos grupos para el usuario que seleccione y para las cuentas miembro.

- Active Directory. Si se elige esta opción, AWS Control Tower no administra el directorio del centro de identidades, no asigna usuarios ni grupos a cuentas nuevas.

- Proveedor de Identidades externo. Siendo la opción recomendada[4], AWS Control Tower crea grupos en el directorio de AWS IAM Identity Center y proporciona acceso a estos grupos a los usuarios que seleccione para las cuentas miembros. Puede especificar un usuario existente desde el

[4] Entre las opciones de identificación de usuarios admitidas por AWS, se recomienda la utilización de un proveedor de identidades que permita administrar las identidades en un lugar centralizado. (Ver guía ***CCN-STIC 887A Guía de Configuración Segura para AWS***, apartado Identificación [op.acc.1].

proveedor de identidad (IdP) externo en Account Factory y AWS Control Tower le da acceso a la cuenta recién vendida al sincronizar los usuarios del mismo nombre entre AWS IAM Identity Center y el IdP. También se puede crear grupos en el IdP que tengan nombres que coinciden con los de los grupos predeterminados de AWS Control Tower y estos usuarios tendrán acceso a las cuentas inscritas.

Utilización de cuentas de correo colaborativas para las cuentas de la OU de seguridad de la landing zone

En el despliegue de la landing zone, es necesario aportar cuentas de correo electrónico para la cuenta de auditoría y para la cuenta de archivo de registros (que se configuran en la unidad organizativa de seguridad). Es recomendable que las cuentas de correo electrónico aportadas sean cuentas colaborativas a las que tengan acceso los diferentes usuarios que realizan tareas específicas relacionadas con la cuenta de AWS Control Tower[5].

No utilizar la raíz

Más que una unidad organizativa, la raíz es un contenedor para la cuenta de administración y todas las unidades organizativas y cuentas de la organización que se crea automáticamente al crear la organización en AWS Organizations. La raíz no se puede eliminar, ni se pueden controlar a las cuentas inscritas a nivel de raíz en AWS Control Tower. Por ello, es recomendable no asociar cuentas directamente a la raíz, sino utilizar las cuentas que se encuadren en las unidades organizativas subyacentes y no utilizar la raíz salvo que sea imprescindible.

Gestión de los permisos con base en el principio de privilegios mínimos

En AWS Control Tower, el recurso principal es la landing zone. Del mismo modo que con el resto de los recursos, los recursos son propiedad de una cuenta de AWS y los permisos para crear o tener acceso a los recursos se rigen por las políticas de permisos. Estos permisos, en AWS Control Tower, se administran a través de los controles.

Concretamente, el propietario del recurso es la entidad principal de la cuenta de AWS (es decir, el usuario raíz de AWS, un usuario AWS IAM o un rol de AWS IAM) que autentica la solicitud de creación de recursos:

- Si se utiliza las credenciales del usuario raíz para configurar la landing zone, la cuenta de AWS será la propietaria del recurso. No obstante, esta opción no se recomienda, dado que es preferible limitar al máximo la actividad de la cuenta raíz y utilizarla únicamente para aquellas tareas que sea imprescindible ejecutar desde dicha cuenta.

[5] Del mismo modo, a nivel de cuenta, es recomendable aportar a AWS información de contacto alternativa para que el soporte de AWS pueda ponerse en contacto fácilmente con los responsables de la cuenta en caso de problemas de seguridad o facturación. (Ver Guía ***CCN-STIC 887A Guía de Configuración Segura para AWS***, apartado Gestión de incidentes [op.exp.7].

- Si se crea un usuario de AWS IAM en su cuenta de AWS y se concede permiso para establecer una landing zone, siendo esta la opción recomendada, la cuenta de AWS a la que pertenece el usuario será la propietaria del recurso.

- Si se crea un rol de AWS IAM con permisos para configurar una landing zone, cualquier persona que pueda asumir el rol podrá configurar una landing zone. La cuenta de AWS a la que pertenece el rol será la propietaria del recurso.

El control de acceso a los recursos de AWS Control Tower debe estar basado en el principio de privilegios mínimos. Para este control se debe elegir una estrategia de políticas basada en la identidad (AWS Control Tower no admite políticas basadas en recursos). Al utilizar las políticas de AWS IAM, es posible:

- Asociar una política de permisos a un usuario o un grupo de usuarios de una cuenta.

- Asociar una política de permisos a un rol. Esto permitiría la concesión de permisos entre cuentas. Por ejemplo, el administrador de la cuenta A puede crear un rol para conceder permisos a una cuenta B. A continuación, el administrador de la cuenta B puede delegar permisos para asumir el rol a cualquier usuario de la cuenta B. No obstante, la concesión de permisos entre cuentas está sujeta a una serie de riesgos específicos, por lo que conviene implementar políticas de confianza. Las políticas de confianza son políticas que especifican qué entidades pueden asumir un rol. Se recomienda modificar manualmente la política de confianza de AWS Control Tower y añadir, las siguientes condiciones:

    - aws:SourceArn: Limitar el acceso a un recurso concreto.

    - aws:SourceAccount: Limitar el acceso a una cuenta concreta.

Para permitir el acceso a la consola de AWS Control Tower, crea tres roles automáticamente al configurar la landing zone:

- AWSControlTowerAdmin rol: Proporciona acceso a la infraestructura fundamental para mantener la landing zone. Este rol requiere una política administrada adjunta que define los permisos para crear y administrar los recursos de AWS Control Tower (AWSControlTowerServiceRolePolicy) y una política de confianza. El acceso a este rol debe ser restringido lo máximo posible.

- AWSControlTowerStackSetRole: AWS Cloud Formation asume esta función para implementar conjuntos de pilas en las cuentas creadas por AWS Control Tower.

- AWSControlTowerCloudTrailRole: AWS Control Tower habilita AWS CloudTrail como práctica recomendada y proporciona esta función a AWS

CloudTrail para crear y publicar registros.

Se recomienda que la asunción de estos roles, particularmente el de ControlTowerAdmin, sea restringida a través de políticas de confianza.

Recomendaciones para la gestión de la configuración de seguridad – AWS Control Tower

Para llevar a cabo una gestión continua de la configuración de los controles de seguridad en las unidades organizativas y en las cuentas de la organización, se puede utilizar la integración de AWS Control Tower y AWS Config. En función del tipo de controles, la comprobación del estado de cumplimiento se realiza del siguiente modo:

- Controles de detección: En la consola de AWS Control Tower, seleccionar "Controles" elegir el nombre del control e ir a la sección "Cuentas" de la página de detalles del control.

- Controles preventivos: El estado de cumplimiento de los controles preventivos de una unidad organizativa se puede ver en la página de detalles de la unidad organizativa, desplazándose hasta la sección "controles habilitados".

- Controles proactivos: Su estado se puede consultar:
    - En la página del panel de control de AWS Control Tower, en la sección "controles".
    - En la página de "detalles de control".

En cualquier caso, es recomendable que cambios de cumplimiento sean reportados por correo electrónico a la cuenta de auditoría a través de la suscripción a un servicio de Amazon SNS.

Recomendaciones para la protección frente al código dañino – AWS Control Tower

AWS ofrece el servicio Amazon GuardDuty para la detección de amenazas. Este servicio monitoriza continuamente el comportamiento malicioso o no autorizado para ayudar a proteger las cuentas y cargas de trabajo de AWS.

Amazon GuardDuty debe usarse en los entornos multi-cuenta para monitorizar todas sus cuentas y hacer que sus hallazgos se envíen a otra cuenta de AWS, la cuenta maestra, que es propiedad de un equipo de seguridad. En una implementación multi-cuenta en la que el equipo de seguridad es responsable de monitorizar un grupo de cuentas de AWS a las que no tiene acceso directo, se recomienda habilitar Amazon GuardDuty en las cuentas de los miembros y configurar los resultados habilitando Amazon GuardDuty en la cuenta root e invitando a las cuentas de los miembros siguiendo las siguientes prácticas:

- Habilitar Amazon GuardDuty para todas las regiones tanto en la cuenta maestra como en las cuentas miembro de un entorno multi-cuenta.

- Añadir las cuentas miembros para la supervisión bajo la cuenta maestra.

- Delegar la administración de Amazon GuardDuty delegada exclusivamente en la cuenta de seguridad para garantizar una correcta segregación de roles para este servicio.

Recomendaciones para el cifrado – AWS Control Tower

AWS Control Tower función con el servicio AWS KMS, que se puede utilizar para cifrar y descifrar los recursos de Control Tower con una clave de cifrado que administre. Se puede añadir o cambiar una clave de AWS KMS cada vez que se actualice la landing zone, siendo recomendable utilizar las propias claves de AWS KMS y cambiarlas de vez en cuando.

Es importante tener en cuenta que, si bien AWS KMS permite crear claves multirregionales y asimétricas, AWS Control Tower no admite claves multirregionales ni asimétricas. Por lo que, si se selecciona una clave con estas características, aparecerá un mensaje de error y deberá generarse otra clave para usarla en AWS Control Tower.

Asimismo, se debe realizar una actualización específica de la política de permisos de una clave de AWS KMS para que funcione con AWS Control Tower.

Recomendaciones para la monitorización – AWS Control Tower

Al configurar la landing zone, una de las cuentas compartidas que se crean es la cuenta de archivo de registros, dedicada a recopilar todos los registros de forma centralizada, incluidos los registros de todas las demás cuentas. Como práctica recomendada, se debe recopilar datos de monitorización de todas las partes de la organización. AWS Control Tower registra las acciones y los eventos mediante su integración con AWS CloudTrail y AWS Config y los registra en Amazon CloudWatch.

La página “Actividades” del panel de AWS Control Tower describe las acciones de la cuenta de administración de AWS Control Tower.

Como práctica recomendada para la monitorización, es recomendable permitir que AWS Control Tower configure un registro de AWS CloudTrail a nivel de organización. Para ello, en el momento de lanzamiento de la landing zone aparecerá esta opción de configuración y se deberá seleccionar “Aceptar”. En caso de que se quiera gestionar los registros con otros trails de AWS CloudTrail o con herramientas de registros de terceros se deberá seleccionar “Excluir”.

Además, durante la fase de configuración, se puede personalizar la política de retención de registros de los buckets Amazon S3 que almacenan los registros de

AWS CloudTrail generados por AWS Control Tower. La configuración predeterminada es de un año para el registro de la cuenta estándar y diez años para el registro de acceso. Esta opción también se puede configurar cuando se actualiza o repara la landing zone.

Recomendaciones para la protección de las comunicaciones – AWS Control Tower

Es posible utilizar el servicio AWS Firewall Manager para proporcionar mejoras en la seguridad de la red desde Control Tower, pudiendo designar una cuenta de administrador de seguridad habilitada para configurar grupos de seguridad. La utilización de AWS Firewall Manager desde AWS Control Tower permite hacer más eficiente la gestión de ciertos controles de red, al permitir la aplicación de reglas y políticas de protección a través de varias cuentas y recursos.

Para habilitar esta opción, se recomienda designar una cuenta de administración de AWS Firewall Manager que se encuentre dentro de la unidad organizativa de seguridad creada por la landing zone. Accediendo al panel de AWS Firewall Manager desde dicha cuenta, se debe crear una política de AWS Firewall Manager del tipo “Grupo de Seguridad” y añadirla a un grupo de seguridad siendo recomendable crear un nuevo grupo de seguridad y no utilizar el grupo de seguridad por defecto. A continuación, se editan las reglas de entrada y salida de tráfico del grupo de seguridad.

Una vez añadida la política y creado el grupo de seguridad, se puede o bien elegir o bien identificar recursos que no cumplan con las reglas, o bien aplicar las reglas para auto remediar los recursos que no cumplan con ellas. Cuando se selecciona la auto remediación, AWS Firewall Manager replica el grupo de seguridad a todas las cuentas de AWS y aplica la política de AWS Firewall Manager a todos los recursos correspondientes utilizando AWS Config, si bien se puede elegir para la aplicación a todas las cuentas bajo la organización, o incluir o excluir las cuentas especificadas.

2.3. Amazon VPC

Una nube privada virtual o VPC (Virtual Private Cloud) es una red privada creada en la nube de AWS que permite implementar recursos como instancias de Amazon EC2 (Elastic Compute Cloud) o contenedores en Amazon ECS (Elastic Container Service) en ella.

De forma predeterminada, los recursos creados dentro de la misma Amazon VPC pueden comunicarse entre sí, suponiendo que los grupos de seguridad y listas de control de acceso así lo permitan. Por el contrario, los recursos creados en Amazon VPC separadas no pueden comunicarse, puesto que no hay una ruta que permita el tráfico entre ellas. Por supuesto, es posible abrirlos para acceder a otros servicios de AWS e internet, pero es algo que debe realizarse de forma explícita.

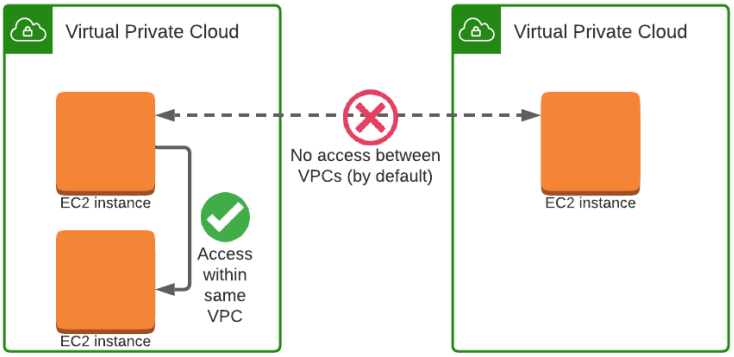

Fig. 6 – Diagrama de comunicación de dos VPC predeterminadas.

Las cuentas de AWS funcionan como mecanismos de aislamiento. De forma predeterminada, una cuenta de AWS no puede acceder a los recursos de otra cuenta diferente, de la misma manera que ocurre en el caso de las Amazon VPC.

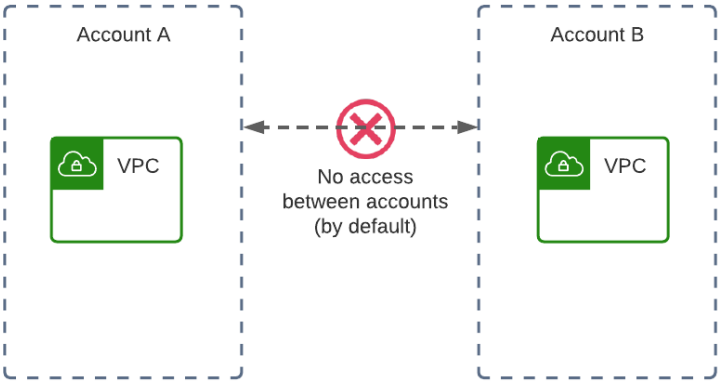

Fig. 7 – Diagrama de comunicación de dos cuentas de AWS predeterminadas.

Si bien el uso de Amazon VPC proporciona una serie de beneficios como pueden ser:

- Garantizar un mayor grado de aislamiento mediante el uso de Amazon VPC separadas.
- Separar una unidad es más fácil al ser único participante y propietario.
- Los propietarios de las aplicaciones serán poseedores de la pila completa si así lo desean.

Es posible que las organizaciones requieran de mecanismos para acceder a las Amazon VPC entre cuentas. Algunas de las potenciales razones podrían ser:

- La necesidad de acceso por parte de una unidad de negocio a los servicios de otra.
- La necesidad de los servicios de una cuenta de prueba de acceder a una cuenta de producción.
- La necesidad de una organización para proporcionar acceso a los servicios de otra sin exponer este mismo a redes públicas.

El uso compartido de las Amazon VPC permite a las organizaciones dar solución a estas necesidades, compartiendo subredes con otras cuentas de AWS que

pertenezcan a la misma organización, siendo propietarias o participantes. Esta extensión de uso se traduce en una serie de beneficios:

- A nivel de separación de funciones. Es posible controlar la estructura de una Amazon VPC, así como el enrutamiento y asignación de direcciones IP de esta.
- A nivel de gestión de permisos y roles. Los propietarios de las aplicaciones continúan siendo propietarios de los recursos, cuentas y grupos de seguridad.
- A nivel de eficiencia. Mediante el uso de servicios como AWS VPN o AWS Direct Connect.
- A nivel de optimización de costos. Permitiendo la reutilización de puertas de enlace y tráfico dentro de la misma zona de disponibilidad.

A raíz de las necesidades descritas, se plantean diferentes escenarios que aúnan tanto conceptos de configuración y conectividad híbrida como entornos multi-cuenta, dando como resultado diferentes casos de uso, siendo los más comunes:

Acceso entre cuentas mediante interconexión de Amazon VPC

Si dos Amazon VPC están interconectadas, significa que tienen una conexión de red entre ellas. Con una configuración de interconexión de Amazon VPC, las instancias de una Amazon VPC pueden comunicarse con las instancias de la otra, como si estuvieran ambas en la misma red. Esta conexión funciona en ambos sentidos entre las Amazon VPC y permite conectar Amazon VPC tanto en la misma cuenta como en cuentas separadas. Este proceso es conocido como Amazon VPC Connection Peering.

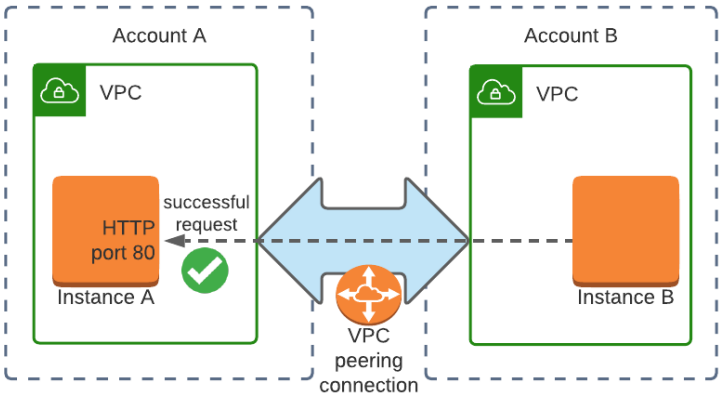

Fig. 8 – Diagrama de acceso ente cuentas mediante interconexión de Amazon VPC.

Acceso entre cuentas al servicio de punto final de la Amazon VPC (PrivateLink)

Se denomina punto de enlace de una Amazon VPC a la conexión desde una Amazon VPC a un servicio específico proporcionado por AWS o por otra persona u organización. El punto de enlace de la Amazon VPC se describe con una dirección IP privada dentro de la propia Amazon VPC, siendo esta accesible mediante un DNS privado. Generalmente, son estos puntos de enlace los que se utilizan para realizar

las llamadas a las API de AWS desde una Amazon VPC, evitando acceder para ello a la Internet pública.

La tecnología que realiza esta función es AWS PrivateLink. AWS PrivateLink configura instancias que ejecutan servicios en la Amazon VPC con un Network Load Balancer (NLB) como front-end. Se puede utilizar la interconexión de Amazon VPC tanto dentro de la misma región como entre regiones.

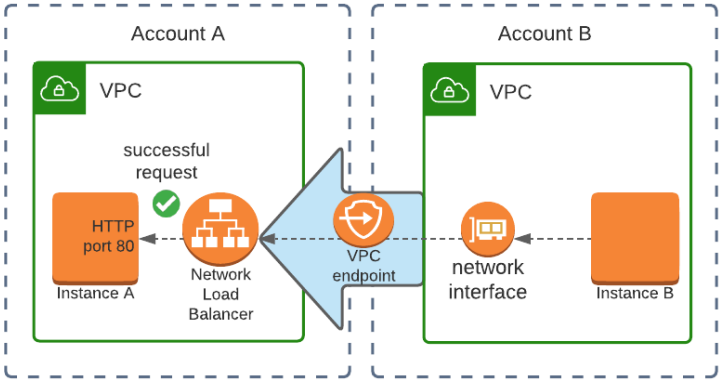

Fig. 9 – Diagrama de acceso entre cuentas al servicio de punto final de una VPC.

Acceso entre cuentas a través de la puerta de enlace de AWS Transit Gateway

AWS Transit Gateway es un enrutador en la nube que conecta varias Amazon VPC, o incluso redes locales, a través de un nodo central. Uno de los principales beneficios que aporta este servicio es que, para varias Amazon VPC interconectadas, cada una de ellas solo necesita una única conexión a la puerta de enlace.

La AWS Transit Gateway permite, de forma predeterminada, que solamente se adjunten las Amazon VPC de la misma cuenta de AWS. Es por ello por lo que, para abarcar un espectro más amplio de casos, en concreto, un escenario de cuentas cruzadas, se deberá hacer uso del servicio AWS Resource Access Manager (AWS RAM). AWS RAM permite compartir cientos de recursos entre cuentas de AWS. Compartir la AWS Transit Gateway con otra cuenta de AWS significa que se pueden adjuntar las Amazon VPC de esa cuenta destino a la puerta de origen.

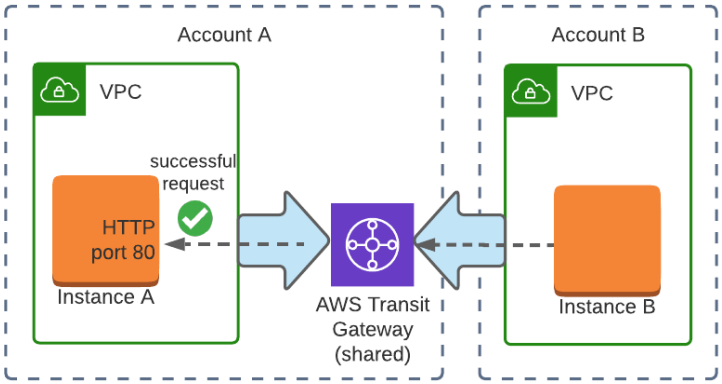

Fig. 10 – Diagrama de acceso entre cuentas (VPC) a través de AWS Transit Gateway.

De la misma manera que ocurría en el primero de los casos, las solicitudes

realizadas entre las Amazon VPC se pueden realizar en ambas direcciones.

La implementación de cualquiera de estas soluciones de Amazon VPC para uso compartido, conlleva, a nivel operativo, una serie de limitaciones; tanto para los propietarios de la Amazon VPC como para los participantes en la misma, tal y como se muestra en la siguiente tabla:

Propietarios	Participantes	Generales
• Los propietarios pueden compartir subredes solo con otras cuentas o unidades organizativas que estén en la misma organización de AWS Organizations. De la misma manera, no pueden compartir subredes que estén en una VPC predeterminada, puesto que, por defecto, no lo permiten. • Los propietarios no pueden iniciar recursos mediante grupos de seguridad que sean propiedad de otros participantes. • Solo los propietarios de la Amazon VPC pueden crear recursos a nivel de Amazon VPC. • Solo los propietarios de una subred pueden adjuntar una AWS Transit Gateway a la subred compartida.	• Los participantes no pueden lanzar recursos mediante grupos de seguridad que sean propiedad de otros participantes o propietario de la Amazon VPC. De la misma manera, no pueden lanzar recursos mediante el grupo de seguridad predeterminado. • Cuando los participantes inician recursos en una subred compartida, deben asegurarse de adjuntar su grupo de seguridad al recurso y no confiar en el grupo de seguridad predeterminado. (REC)	• Las etiquetas de Amazon VPC y las etiquetas de los recursos que contiene no se comparten con los participantes. • Las cuotas de servicio son aplicadas por cuenta individual.

Tabla 1 – Limitaciones derivadas del uso compartido de Amazon VPC.

Recomendaciones para la arquitectura de seguridad – Amazon VPC

Para una correcta configuración de la arquitectura de seguridad se recomienda seguir los controles señalados en la Guía ***CCN-STIC 887A Guía de Configuración Segura para AWS*** para todo lo relacionado con Amazon VPC.

Aunque, como ya se ha mencionado en el documento, de forma predeterminada los recursos creados en Amazon VPC separadas no pueden comunicarse, es posible configurar las Amazon VPC para un uso compartido de los recursos que albergan.

Los propietarios de una Amazon VPC son los responsables de crear, administrar y eliminar todos los recursos a nivel de Amazon VPC (independientemente de si esta ha sido compartida o no) incluyendo: Subredes, tablas de enrutamiento y ACL de red; Interconexiones, puntos de enlace de la Amazon VPC, puntos de enlace de AWS Private Link, puertas de enlace a internet, NAT, Virtual Private Gateway y archivos adjuntos de la Gateway. Es por ello por lo que:

- Como requisito previo para compartir una Amazon VPC con otras cuentas, el propietario de la Amazon VPC debe crear un recurso compartido con AWS RAM, tal y como se indica en este documento.

Dicho propietario no puede eliminar, modificar o expulsar a la fuerza los recursos de un participante. Es por ello por lo que, para garantizar la seguridad de las Amazon VPC, hay que tener en cuenta que:

- Las cuentas participantes en una Amazon VPC estén incluidas en AWS Organizations.
- Asignar a todas las nuevas cuentas una unidad organizativa (OU), de manera que dichas cuentas reciban una línea base de red en forma de Amazon VPC compartida (de forma similar a lo que se puede hacer con landing zones).

Además de ello, dado un escenario de cuentas cruzadas en las que se comunican instancias pertenecientes a diferentes Amazon VPC, se debe:

- Habilitar el servicio AWS Resource Access Manager (AWS RAM) desde la cuenta maestra de AWS Organizations (propietaria de la Amazon VPC).

AWS RAM permite crear recursos compartidos y compartirlos con toda la organización de AWS, unidades organizativas (OU) concretas o cuentas de AWS. Esto es necesario debido a que las subredes solo pueden ser compartidas dentro de una misma organización de AWS. (Más información sobre este servicio en el apartado 2.5 AWS Resource Access Manager de este mismo documento).

Recomendaciones para la monitorización – Amazon VPC

Dada la naturaleza de una Amazon VPC compartida, en la que diferentes miembros pueden acceder a los recursos compartidos, es necesario implantar, por parte de los propietarios de la Amazon VPC, un registro de flujo en el nivel de Amazon VPC, subred o ENI para monitorizar el tráfico y disponer de información para evaluar los incidentes que puedan ocurrir. Para ello, la organización puede activar los servicios Amazon VPC Flowlogs y Amazon CloudWatch para el registro del tráfico IP en las Amazon VPC.

Los logs de flujo de Amazon VPC son una característica que permite capturar información acerca del tráfico IP que entra y sale de las diferentes interfaces de red en la Amazon VPC. Estos logs de flujo pueden ayudar en:

- Diagnóstico de reglas de grupo de seguridad muy restrictivas.
- Supervisar el tráfico de entrada a una instancia.
- Determinar la dirección del tráfico entrante y saliente de las interfaces de red.

Para más información, consultar: Registro del tráfico de IP con registros de flujo de la Amazon VPC - Amazon Virtual Private Cloud

Recomendaciones para la protección de las comunicaciones – Amazon VPC

En lo referente a control de acceso, es posible utilizar diferentes mecanismos para controlar el acceso a una Amazon VPC compartida. En cualquier caso, es responsabilidad del propietario de la Amazon VPC aplicar las diferentes medidas y configuraciones de seguridad relacionadas con creación y asignación de políticas, permisos y roles de acceso. Se recomienda, por lo tanto:

- Utilizar listas de control de acceso (ACL) de red para controlar el tráfico hacia las subredes de una Amazon VPC.
- Utilizar Security Groups para controlar el tráfico hacia los recursos de las subredes de una Amazon VPC. De manera que los participantes no puedan lanzar recursos mediante grupos de seguridad que sean propiedad de otros participantes o propietario de la Amazon VPC.
- Disponer de una política de control de servicios (SCP) para denegar el acceso a los participantes para la creación de sus propias VPC; tal y como se describe en el apartado "Utilización de Políticas de Control de Servicios (SCPs)" de AWS Organizations de este mismo documento.
- En caso de utilizar AWS PrivateLink, además de hacer uso de Security Groups, la organización puede crear políticas de punto de enlace de Amazon VPC.

Una política de punto de enlace de una Amazon VPC, finalmente, una política de recursos de AWS IAM que se asocia a un punto de enlace concreto. Estas políticas no reemplazan las políticas de usuario AWS IAM ni políticas específicas de servicio (como son las de bucket Amazon S3). Se trata de una política concreta para un punto de enlace concreto. Para obtener más información acerca de la escritura de políticas, se puede consultar la Información general de las políticas AWS IAM en la guía de usuario AWS IAM.

2.4. AWS Direct Connect

AWS Direct Connect es una solución que facilita el establecimiento de una conexión de red exclusiva entre el entorno local y AWS. Con AWS Direct Connect, puede establecerse una conectividad privada entre AWS y el centro de datos, oficina o entorno de coubicación que emplee la organización, lo que en muchos casos puede reducir los costos de red, aumentar el rendimiento del ancho de banda y suministrar una experiencia de red más estable que las conexiones basadas en Internet.

Es posible asociar un Gateway de AWS Direct Connect con un Gateway virtual que sea propiedad de cualquier cuenta de AWS. Para ello, el propietario de la Gateway virtual crea una propuesta de asociación compartiendo el ID de la Gateway de AWS Direct Connect y el ID de la cuenta de AWS. A continuación, el propietario de la Gateway de AWS Direct Connect debe aceptar la propuesta de asociación.

Una propuesta de asociación puede contener los prefijos de Amazon VPC que se permitirán desde la Gateway privada virtual, pudiendo el propietario de la puerta de enlace de AWS Direct Connect anular opcionalmente cualquier prefijo solicitado en la propuesta de asociación. La lista de prefijos actúa como un filtro que permite que los mismos CIDRs sean anunciados a la pasarela de AWS Direct Connect. Por ejemplo, si el CIDR de la Amazon VPC es 10.0.0.0/16, se puede establecer este mismo CIDR como prefijo permitido o 10.0.0.0/15 (un valor más amplio que el CIDR de la Amazon VPC).

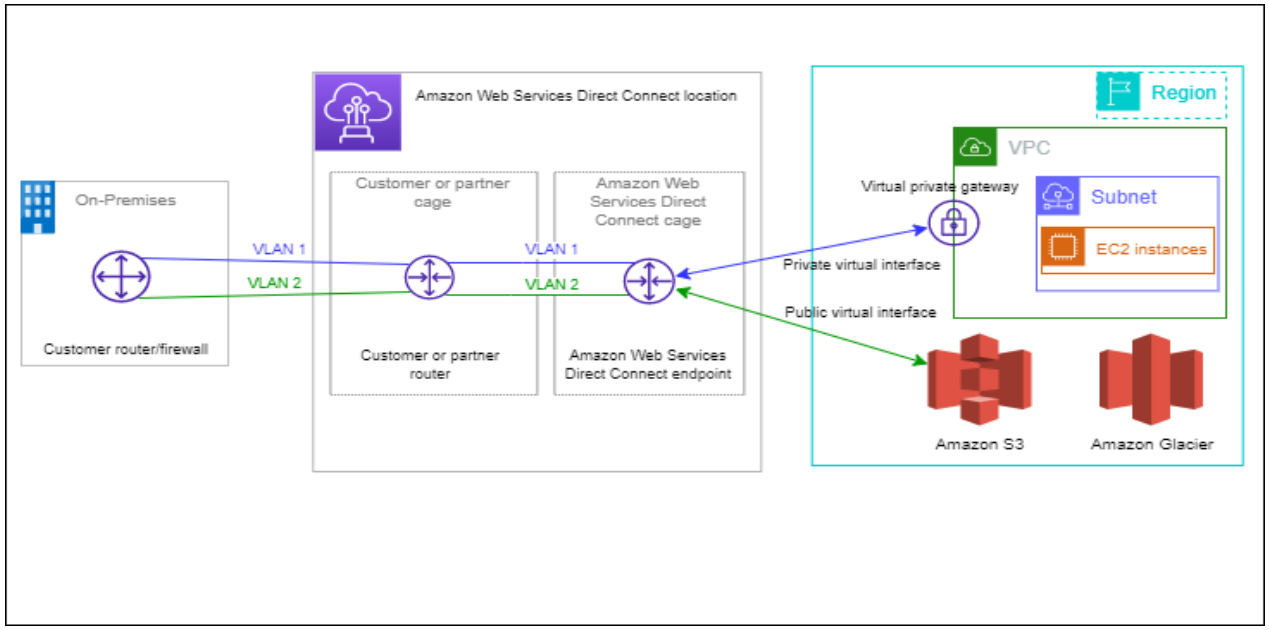

Fig. 11 – Diagrama de comunicación de AWS Direct Connect con la red local.

2.5. AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) es un servicio que le permite compartir de forma fácil y segura los recursos de AWS con cualquier cuenta de AWS o dentro de su organización de AWS.

AWS Resource Access Manager elimina la necesidad de crear recursos duplicados en múltiples cuentas, reduciendo la sobrecarga operativa de gestionar esos recursos en cada una de las cuentas que se poseen.

Si bien es posible compartir recursos sin necesidad de vincular AWS Resource Access Manager con AWS Organizations, esta integración permite compartir de modo más ágil (sin necesidad de utilizar invitaciones), los recursos con todas las demás cuentas de la organización o solo con las cuentas incluidas en una o más unidades organizativas especificadas. Para ello, en primer lugar, se debe utilizar la consola de AWS RAM o la CLI para habilitar el uso compartido con AWS Organizations.

Cuando se habilita el uso compartido de recursos dentro de la organización, AWS RAM crea un rol vinculado a servicios denominado AWSServiceRoleForResourceAccessManager que solo puede ser asumido por el servicio AWS RAM y sirve para otorgar a AWS RAM permiso para recuperar información sobre la organización mediante la política AWSResourceAccesManagagerServiceRolePolicy.

2.6. Recomendaciones Finales

Múltiples organizaciones

La mayoría de los clientes pueden operar sus entornos multi-cuenta de AWS utilizando una única organización de producción y en general la recomendación es que administren sus cuentas dentro de una sola organización. Esto permite garantizar la coherencia entre las cuentas de su entorno porque las políticas aplicadas centralmente o las configuraciones de nivel de servicio se aplican mediante programación en todas las cuentas de su organización.

Separar sus cuentas de carga de trabajo (aplicaciones, proyectos, etc.) entre diferentes organizaciones requiere una sobrecarga o personalización adicional para garantizar que se apliquen estándares centrales dentro de cada organización. Sin embargo, existen ciertas excepciones, o casos de uso, en las que es posible o conveniente trabajar en varias organizaciones.

- Múltiples proveedores o partners de re-facturación: en contextos donde los proyectos que se sacan a licitación incluyen los consumos de AWS asociados y tienen entidad propia ya sea por tamaño, complejidad o porque la operación está totalmente delegada en el adjudicatario, tiene sentido que se tenga una organización independiente para el mismo. En estos casos se puede alinear o asegurar el cumplimiento de mejores prácticas haciendo uso de mecanismos de autenticación y/o accesos delegados mediante roles IAM.
- Pruebas de cambios del entorno de AWS completo
- Entornos de AWS muy grandes
- Diferentes niveles de clasificación de las cargas, aplicaciones y proyectos, como un nivel de perímetro adicional

Arquitecturas de Referencia de entornos multi-cuentas

AWS ha publicado guías de referencia para entornos de multi-cuenta que incluyen código y explicaciones que pueden usarse como complementos a las automatizaciones vistas en la presente guía.

Arquitectura de referencia de seguridad (AWS SRA): guía de referencia de despliegue de los servicios de seguridad en entornos multi-cuenta, la cual puede consultarse en este enlace.

Landing Zone Accelerator on AWS (LZA): es una solución diseñada para desplegar las fundaciones de operación multi-cuenta AWS en entornos regulados la cual puede consultarse en este enlace.

3. GLOSARIO DE TÉRMINOS

A continuación, se describen los términos, acrónimos y abreviaturas relacionados conla tecnología objeto de esta guía con el objeto de facilitar la comprensión de la misma.

Término	Definición
ACL	Access Control List (Lista de Control de Acceso)
Active Directory	Directorio activo.
API	Application Programming Interface (Interfaz de Programación de Aplicaciones)
Backup	Copia de Seguridad.
Bucket	Contenedor para almacenar objetos (archivos) pertenecientes al servicio Amazon S3
Conectividad híbrida	La expresión "nube híbrida" hace referencia a la combinación de al menos dos entornos informáticos que comparten información entre sí y ejecutan una serie uniforme de aplicaciones para una empresa o negocio.
Connection Peering	El peering (conexión directa, intercambio de tráfico o emparejamiento) es la interconexión voluntaria de redes de Internet administrativamente independientes con el fin de intercambiar tráfico entre los usuarios de cada red.
ENI	Elastic Network Interface, interfaz de red virtual que puedes asociar a una instancia en una Amazon VPC.
Front-end	El frontend o «desarrollo del lado del cliente» se refiere a la práctica de producir HTML, CSS y JavaScript. Estos tres elementos se encargan de dar forma a la parte frontal de un sitio web o aplicación. Esto incluye los fondos, colores, texto, animaciones o efectos.
Gateway	Un gateway (puerta de enlace) es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.
Hipervisor	Un hipervisor o monitor de máquina virtual es una capa de software para realizar una virtualización de hardware que permite utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.

Landing Zones	Una landing zone es un entorno de AWS de múltiples cuentas y bien diseñado que es escalable y seguro. Este es un punto de partida desde el que su organización puede lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura.
Network Load Balancer	Un balanceador de carga actúa como único punto de contacto para los clientes. Los clientes envían las solicitudes al balanceador de carga y este se las envía a los destinos, tales como las instancias Amazon EC2, en una o más zonas de disponibilidad.
Política de Control de Servicio (SCP)	Las políticas de control de servicios (SCP) son un tipo de política de organización que puede utilizar para administrar permisos en su organización.
Sandbox	Un sandbox en informática o un entorno de pruebas, es una máquina virtual aislada en la que se puede ejecutar código de software potencialmente inseguro sin afectar a los recursos de red o a las aplicaciones locales.
SDK	Software Development Kit (Kit de Desarrollo de Software)
Subred	Una subred es una red dentro de una red.
Tags	Etiquetas
Unidad Organizativa (OU)	La unidad organizativa (OU) es un contenedor de cuentas y de otras unidades organizativas, de modo que se puede crear una jerarquía de árbol con un nodo raíz en la parte superior y ramas de unidades organizativas que terminan en las cuentas.
Usuario Breakglass	Cuenta que se utiliza con fines de emergencia para obtener acceso a un sistema o servicio al que no se puede acceder bajo los controles normales.
Usuario Root	Cuenta de administrador.
VPC	Virtual Private Cloud (Nube Privada Virtual)

4. GLOSARIO DE SERVICIOS AWS

A continuación, se reúnen los diferentes servicios mencionados a lo largo de esta guíaincluyendo enlaces a la documentación concreta de cada uno de ellos.

Servicio	URL de documentación servicio
Amazon CloudWatch	Amazon CloudWatch
Amazon Cost Explorer	Amazon Cost Explorer
Amazon Dynamo DB	Amazon DynamoDB
Amazon Elastic Computer Cloud (EC2)	Amazon Elastic Compute Cloud - AWS EC2
Amazon GuardDuty	Amazon GuardDuty
Amazon Private Link	AWS PrivateLink
Amazon S3	Amazon Simple Storage Service - Amazon S3
Autenticación Multifactor (MFA)	Uso de autenticación multifactor (MFA) en AWS - AWS IAM Configuración del acceso a una API protegido por MFA
AWS Backup	Copia de seguridad centralizada en la nube - AWS Backup
AWS Cloud Formation	AWS Cloud Formation
AWS CloudFormation hooks	Cloud Formation Developing hooks
AWS CloudTrail	AWS CloudTrail
AWS CloudWatch Events	Amazon CloudWatch Events
AWS Config	Documentación de AWS Config - AWS Config Tipos de recursos admitidos en AWS Config - AWS Config Required Tags - AWS Config
AWS Config Rules	AWS Config Rules - AWS Config
AWS Control Tower	AWS Control Tower

AWS Direct Connect	AWS Direct Connect
AWS Firewall Manager	AWS Firewall Manager
AWS Identity & Access Manager (IAM)	Identidades de IAM (usuarios, grupos de usuarios y roles) - AWS IAM
AWS Key Management Service (KMS)	AWS Key Management Service - AWS KMS Políticas de claves - AWS KMS
AWS Organizations	AWS Organizations
AWS Resource Access Manager (RAM)	AWS Resource Access Manager
AWS Service Catalog	AWS Service Catalog
AWS Transit Gateway	AWS Transit Gateway
AWS Virtual Private Cloud (VPC)	AWS Virtual Private Cloud - AWS VPC
Proveedores de identidad externos - Identity Provider (IdP)	Acceso mediante proveedores de identidad (IdP) a servicios AWS - AWS IdP
Regiones, zonas de disponibilidad y zonas locales	Regiones, zonas de disponibilidad y zonas locales
Security Groups	Security Groups
SNS	Amazon Simple Notification Service
VPN Site-to-Site	AWS VPN Site-to-Site

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL