

Descripción de la infraestructura física de Azure

A lo largo del recorrido con Microsoft Azure, escucharás y usarás términos como regiones, zonas de disponibilidad, recursos, suscripciones, etc. Este módulo se centra en los principales componentes arquitectónicos de Azure. Los componentes arquitectónicos principales de Azure se pueden dividir en dos grandes grupos: la infraestructura física y la infraestructura de administración.

Infraestructura física

La infraestructura física de Azure comienza con los centros de datos. Conceptualmente, los centros de datos son iguales que los grandes centros de datos corporativos. Son instalaciones con recursos organizados en bastidores, con potencia dedicada, refrigeración e infraestructura de red.

Como proveedor de nube global, Azure tiene centros de datos en todo el mundo. Pero estos centros de datos individuales no son accesibles directamente. Los centros de datos se agrupan en regiones de Azure o Azure Availability Zones, están diseñados para ayudarte a lograr resistencia y confiabilidad para las cargas de trabajo críticas para la empresa.

El sitio de [infraestructura global](#) le ofrece la oportunidad de explorar de manera interactiva la infraestructura subyacente de Azure.

Regions

Una región es un área geográfica del planeta que contiene al menos un centro de datos, aunque podrían ser varios cercanos y conectados mediante una red de baja latencia. Azure asigna y controla los recursos de forma inteligente dentro de cada región para garantizar que las cargas de trabajo están bien compensadas.

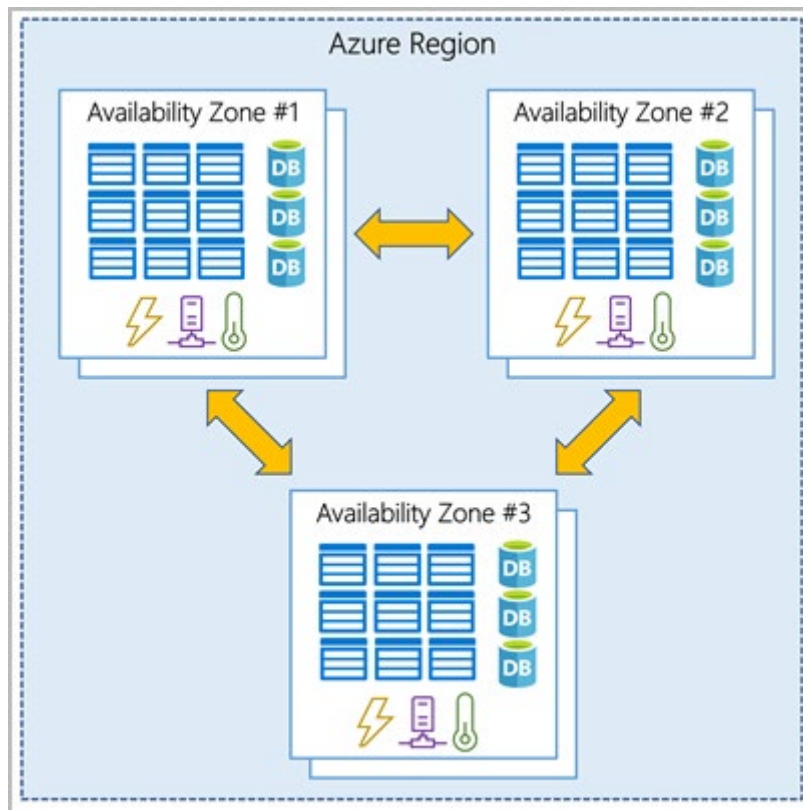
Al implementar un recurso en Azure, es habitual tener que elegir la región en la que quiere que se implemente el recurso.

Nota

Algunos servicios o características de las máquinas virtuales (VM) solo están disponibles en determinadas regiones, como, por ejemplo, tipos de almacenamiento o tamaños de VM específicos. También hay algunos servicios globales de Azure que no requieren que seleccione una región concreta, como Microsoft Entra ID, Azure Traffic Manager o Azure DNS.

Availability Zones

Las zonas de disponibilidad son centros de datos separados físicamente dentro de una región de Azure. Cada zona de disponibilidad consta de uno o varios centros de datos equipados con alimentación, refrigeración y redes independientes. Una zona de disponibilidad se configura para constituir un límite de aislamiento. Si una zona deja de funcionar, la otra continúa trabajando. Las zonas de disponibilidad están conectadas a través de redes de fibra óptica de alta velocidad privadas.



Importante

Para garantizar la resistencia, se configuran un mínimo de tres zonas de disponibilidad independientes en todas las regiones habilitadas. Pero no todas las regiones de Azure admiten actualmente las zonas de disponibilidad.

Uso de las zonas de disponibilidad en sus aplicaciones

A fin de proteger la información en caso de error, deberá asegurarse de que los servicios y datos son redundantes. Si hospeda su infraestructura, configurar su propia redundancia requiere la creación de entornos de hardware duplicados. Azure puede ayudar a que la aplicación tenga alta disponibilidad a través de zonas de disponibilidad.

Puede usar zonas de disponibilidad para ejecutar aplicaciones críticas y conseguir una alta disponibilidad en la arquitectura de sus aplicaciones si coloca los recursos de proceso, almacenamiento, red y datos dentro de una zona y los replica en otras. Recuerde que la duplicación de los servicios y la transferencia de datos entre zonas de disponibilidad podrían suponer un costo.

Las zonas de disponibilidad son principalmente para las máquinas virtuales, los discos administrados, los equilibradores de carga y las bases de datos SQL. Los servicios de Azure que admiten zonas de disponibilidad se dividen en tres categorías:

- Servicios de zona: ancle el recurso a una zona específica (por ejemplo, máquinas virtuales, discos administrados, direcciones IP).
- Servicios de redundancia de zona: la plataforma se replica automáticamente entre zonas (por ejemplo, almacenamiento con redundancia de zona, SQL Database).
- Servicios no regionales: los servicios siempre están disponibles en las ubicaciones geográficas de Azure y son resistentes a las interrupciones de toda la zona, así como a las de toda la región.

Incluso con la resistencia adicional que proporcionan las zonas de disponibilidad, es posible que un evento pueda ser tan grande que afecte a varias zonas de disponibilidad en una sola región. Para proporcionar una mayor resistencia, Azure tiene pares de regiones.

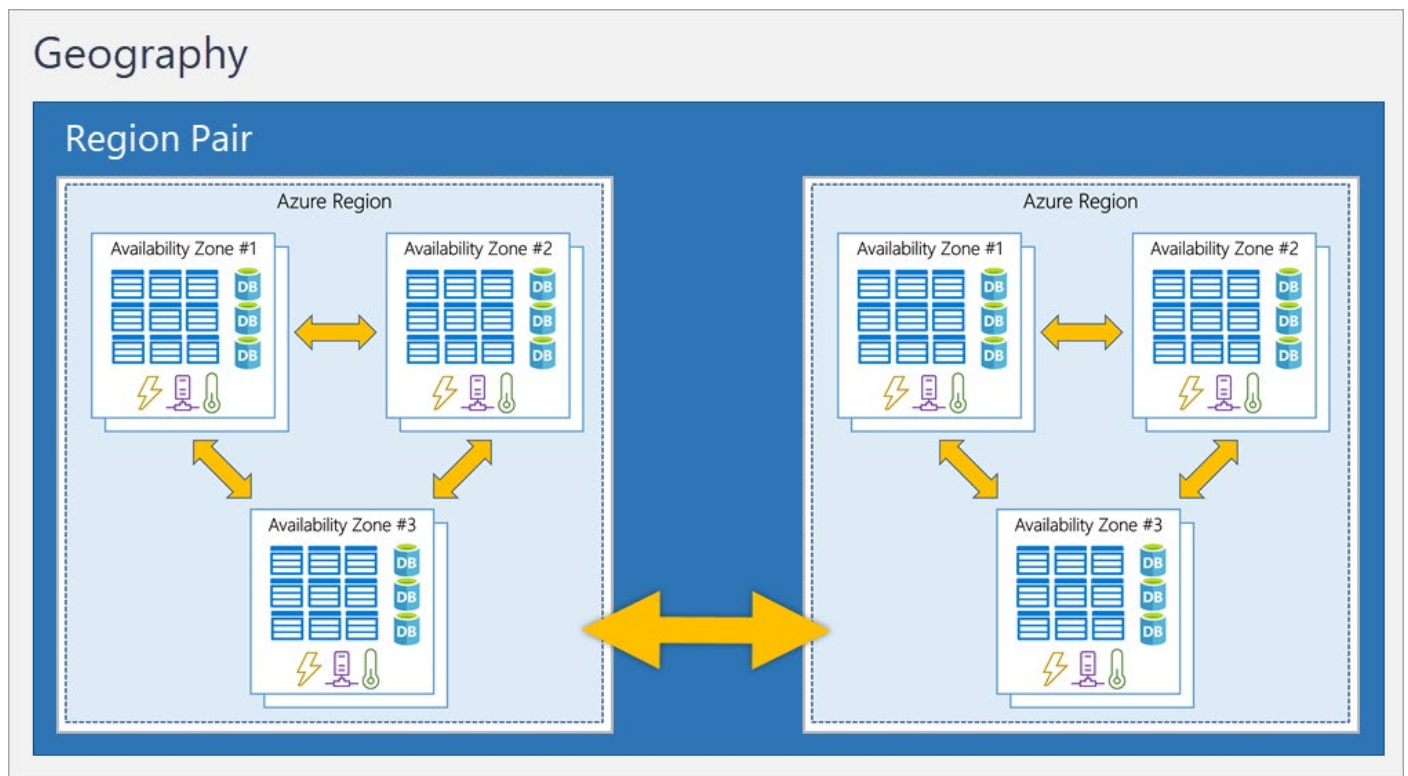
Pares de región

La mayoría de las regiones de Azure se emparejan con otra región de la misma zona geográfica (por ejemplo, EE. UU., Europa o Asia) que se encuentre como mínimo a 500 km de distancia. Este enfoque permite la replicación de recursos en una zona geográfica que ayuda a reducir la probabilidad de que se produzcan interrupciones provocadas por eventos como desastres naturales, disturbios sociales, cortes del suministro eléctrico o interrupciones de la red física que afecten a una región completa. Por ejemplo, si una región de un par se ve afectada por un desastre natural, los servicios conmutarán por error automáticamente a la otra región de su par de regiones.

Importante

No todos los servicios de Azure replican automáticamente los datos ni se replican automáticamente desde una región con errores para la replicación cruzada en otra región habilitada. En estos escenarios, el cliente debe configurar la replicación y la recuperación.

Algunos pares de regiones de ejemplo en Azure son Oeste de EE. UU. y Este de EE. UU., y Sudeste Asiático y Asia Pacífico. Como las dos regiones están directamente conectadas y lo suficientemente lejos como para estar aisladas contra desastres regionales, puede usarlas para proporcionar redundancia de datos y servicios de confianza.



Ventajas adicionales de los pares de región:

- Si se produce una gran interrupción de Azure, se da prioridad a una región de cada par para asegurarse de que al menos una se restaure lo más rápido posible para las aplicaciones hospedadas en ese par de regiones.
- Las actualizaciones planeadas de Azure se implementan una a una en regiones emparejadas para minimizar el tiempo de inactividad y el riesgo de interrupción de la aplicación.
- Los datos siguen residiendo en la misma zona geográfica que su pareja (excepto Sur de Brasil) con fines de jurisdicción fiscal y de aplicación de la ley.

Importante

La mayoría de las regiones se emparejan en dos direcciones, es decir, son la copia de seguridad de la región que proporciona una copia de seguridad para ellas (Oeste de EE. UU. y Este de EE. UU. se copian entre sí). Sin embargo, algunas regiones, como Oeste de la India y Sur de Brasil, se emparejan en una sola dirección. En un emparejamiento unidireccional, la región primaria no proporciona copia de seguridad para su región secundaria. Por tanto, aunque la región secundaria de la India Occidental es Sur de la India, Sur de la India no depende de la India Occidental. La región secundaria del India occidental es Sur de la India, pero la región secundaria esta última es Centro de la India. Sur de Brasil es un caso único porque se empareja con una región fuera de su ubicación geográfica. La región secundaria de Sur de Brasil es Centro-sur de EE. UU. La región secundaria de Centro-sur de EE. UU. no es Sur de Brasil.

Regiones soberanas

Además de las regiones normales, Azure también tiene regiones soberanas. Las regiones soberanas son instancias de Azure que están aisladas de la instancia principal de Azure. Es posible que tenga que usar una región soberana con fines legales o de cumplimiento.

Entre las regiones soberanas de Azure se incluyen las siguientes:

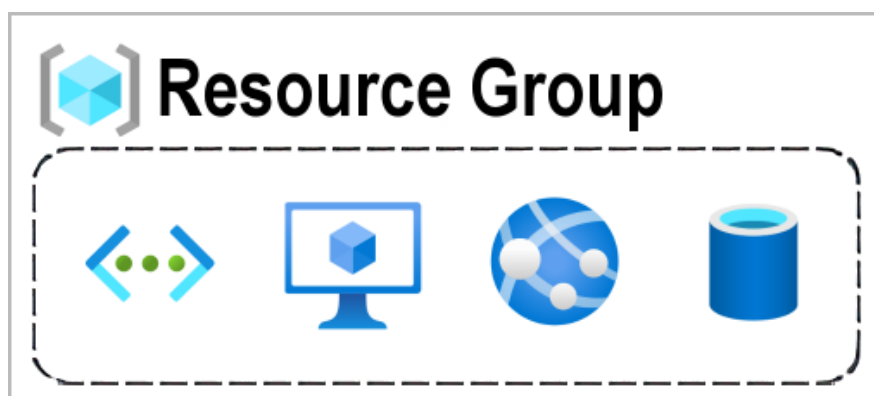
- US DoD (centro), US Gov Virginia, US Gov Iowa y más: Estas regiones son instancias físicas y lógicas con aislamiento de red de Azure para asociados y agencias de la administración pública de EE. UU. Estos centros de datos están operados por personal estadounidense sometido a evaluación e incluyen certificaciones de cumplimiento adicionales.
- Este de China, Norte de China y más: Estas regiones están disponibles gracias a una asociación exclusiva entre Microsoft y 21Vianet, por la cual Microsoft no mantiene directamente los centros de datos.

Descripción de la infraestructura de administración de Azure

La infraestructura de administración incluye recursos de Azure y grupos de recursos, suscripciones y cuentas. Comprender la organización jerárquica le ayudará a planear los proyectos y productos dentro de Azure.

Recursos y grupos de recursos de Azure

Un recurso es el bloque de creación básico de Azure. Todo lo que cree, aprovisiona, implementa, etc., es un recurso. Máquinas virtuales (VM), redes virtuales, bases de datos, servicios cognitivos, etc., se consideran recursos dentro de Azure.



Los grupos de recursos son simplemente agrupaciones de recursos. Al crear un recurso, es necesario colocarlo en un grupo de recursos. Aunque un grupo de recursos puede contener muchos recursos, un único recurso solo puede estar en un grupo de recursos a la vez. Es posible que algunos recursos se muevan entre grupos de recursos, pero al mover un recurso a un nuevo grupo, ya no estará asociado al grupo anterior. Además, los grupos de recursos no se pueden anidar, lo que significa que no se puede colocar el grupo de recursos B dentro del grupo de recursos A.

Los grupos de recursos proporcionan una manera cómoda de agrupar recursos. Al aplicar una acción a un grupo de recursos, se aplicará a todos los recursos que contiene. Si elimina un grupo de recursos, se eliminarán todos los recursos que contiene. Si concede o deniega el acceso a un grupo de recursos, habrá concedido o denegado acceso a todos los recursos que contiene.

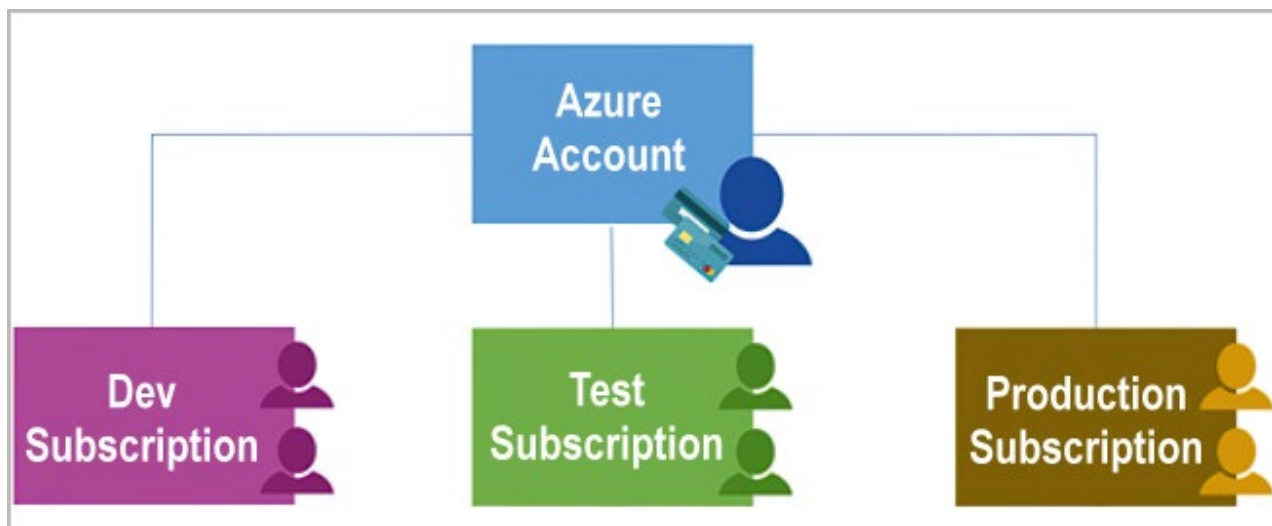
Al aprovisionar recursos, es conveniente pensar en la estructura del grupo de recursos que mejor se adapte a las necesidades.

Por ejemplo, si vas a configurar un entorno de desarrollo temporal, agrupar todos los recursos significa que puede desaprovechar todos los recursos asociados a la vez si elimina el grupo de recursos. Si vas a aprovisionar recursos de proceso que necesitarán tres esquemas de acceso diferentes, puede ser mejor agruparlos en función del esquema de acceso y, después, asignar acceso en el nivel de grupo de recursos.

No hay reglas rígidas sobre cómo se usan los grupos de recursos, por lo que debe tener en cuenta cómo configurarlos para maximizar su utilidad.

Suscripciones de Azure

En Azure, las suscripciones son una unidad de administración, facturación y escala. Al igual que los grupos de recursos son una manera de organizar lógicamente los recursos, las suscripciones permiten organizar lógicamente los grupos de recursos y facilitar la facturación.



* El uso de Azure requiere una suscripción de Azure. Una suscripción le proporciona acceso autenticado y autorizado a los servicios y productos de Azure. Además, también le permite aprovisionar los recursos. Una suscripción de Azure se vincula a una cuenta de Azure, que es una identidad de Microsoft Entra ID o en un directorio en el que confía Microsoft Entra ID.

Una cuenta puede tener varias suscripciones, pero solo es obligatorio tener una. En una cuenta de varias suscripciones, puede usarlas para configurar diferentes modelos de facturación y aplicar diferentes directivas de administración de acceso. Puede usar las suscripciones de Azure para definir límites en torno a los productos, servicios y recursos de Azure. Hay dos tipos de límites de suscripción que puede utilizar:

- **Límite de facturación:** Este tipo de suscripción determina cómo se factura una cuenta de Azure por el uso de Azure. Puede crear varias suscripciones para diferentes tipos de requisitos de facturación.

Azure genera facturas e informes de facturación independientes para cada suscripción, de modo que pueda organizar y administrar los costos.

- **Límite de control de acceso:** Azure aplica las directivas de administración de acceso en el nivel de suscripción, por lo que puede crear suscripciones independientes para reflejar distintas estructuras organizativas. Por ejemplo, dentro de una empresa hay diferentes departamentos a los que se pueden aplicar directivas de suscripción de Azure distintas. Este modelo de facturación le permite administrar y controlar el acceso a los recursos que los usuarios aprovisionan con suscripciones específicas.

Creación de una suscripción de Azure adicional

De forma similar al uso de grupos de recursos para separar los recursos por función o acceso, es posible que quiera crear suscripciones adicionales con fines de administración de recursos o facturación. Por ejemplo, puedes optar por crear suscripciones adicionales para separar lo siguiente:

- **Entornos:** puedes optar por crear suscripciones con el fin de configurar entornos independientes para el desarrollo y las pruebas, para seguridad o para aislar los datos por motivos de cumplimiento. Este diseño es especialmente útil porque el control de acceso a los recursos se produce en el nivel de suscripción.
- **Estructuras organizativas:** puedes crear suscripciones para reflejar las distintas estructuras organizativas. Por ejemplo, podría limitar un equipo a recursos de bajo costo, al tiempo que permite que el departamento de TI tenga un alcance completo. Este diseño permite administrar y controlar el acceso a los recursos que los usuarios aprovisionan en cada suscripción.
- **Facturación:** puedes crear suscripciones adicionales con fines de facturación. Dado que los costos se agregan primero en el nivel de suscripción, es posible que quieras crear suscripciones para administrar y realizar un seguimiento de los costos en función de sus necesidades. Por ejemplo, puede que quieras crear una suscripción para las cargas de trabajo de producción, y otra suscripción para las cargas de trabajo de desarrollo y pruebas.

Grupos de administración de Azure

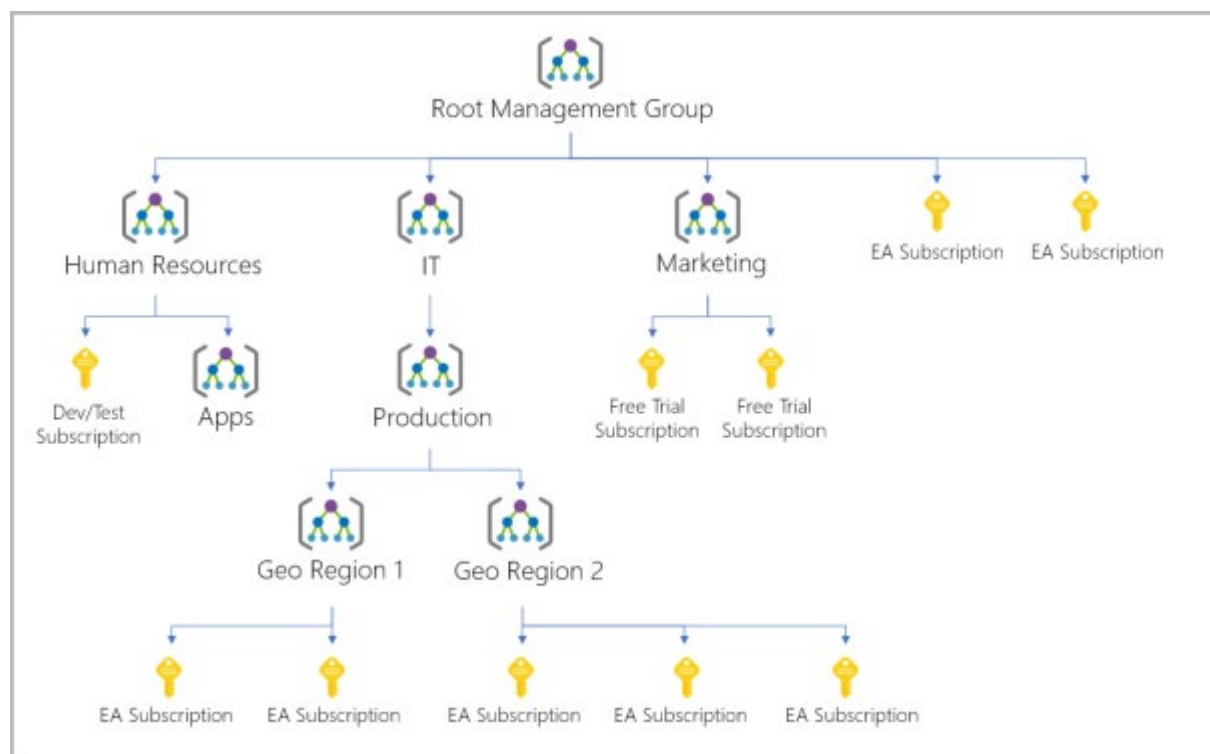
La última pieza es el grupo de administración. Los recursos se recopilan en grupos de recursos y los grupos de recursos se recopilan en suscripciones. Si acaba de empezar en Azure, podría parecer una jerarquía suficiente para mantener las cosas organizadas. Pero imagine que trabaja con varias aplicaciones, varios equipos de desarrollo, en varias zonas geográficas.

Si tienes muchas suscripciones, es posible que necesite una forma de administrar con eficacia el acceso, las directivas y el cumplimiento para esas suscripciones. Los grupos de administración de Azure proporcionan un nivel de ámbito por encima de las suscripciones. Las suscripciones se organizan en contenedores llamados grupos de administración, a los que se aplican condiciones de gobernanza. Todas las suscripciones de un grupo de administración heredan automáticamente las condiciones que tenga aplicadas, de la misma manera que los grupos de recursos heredan la configuración de las suscripciones y los recursos heredan de los grupos de recursos. Los grupos de administración proporcionan capacidad de administración de nivel empresarial a gran escala con independencia del tipo de suscripciones que tenga. Los grupos de administración se pueden anidar.

Jerarquía de grupo de administración, suscripciones y grupo de recursos

Puede compilar una estructura flexible de grupos de administración y suscripciones para organizar los recursos en una jerarquía para una administración unificada de las directivas y el acceso. El diagrama

siguiente muestra un ejemplo de creación de una jerarquía para la gobernanza mediante grupos de administración.



Algunos ejemplos de cómo podría usar los grupos de administración podrían ser los siguientes:

- **Crear una jerarquía que aplique una directiva.** Podría limitar las ubicaciones de las máquinas virtuales a la región Oeste de EE. UU. en un grupo denominado Producción. Esta directiva se heredaría en todas las suscripciones descendientes de ese grupo de administración y se aplicará a todas las máquinas virtuales de esas suscripciones. El propietario de los recursos o las suscripciones no puede modificar esta directiva de seguridad, lo que permite una gobernanza mejorada.
- **Proporcionar acceso de usuario a varias suscripciones.** Al mover varias suscripciones bajo un grupo de administración, puede crear una asignación del control de acceso basado en roles (RBAC) en el grupo de administración. La asignación de RBAC de Azure en el nivel de grupo de administración significa que todos los grupos de administración secundaria, las suscripciones, los grupos de recursos y los recursos bajo ese grupo de administración también heredarían esos permisos. Una asignación en el grupo de administración puede permitir a los usuarios tener acceso a todo lo que necesitan, en lugar de crear scripts de Azure RBAC sobre las distintas suscripciones.

Datos importantes sobre los grupos de administración:

- Se admiten 10 000 grupos de administración en un único directorio.
- Un árbol de grupo de administración puede admitir hasta seis niveles de profundidad. Este límite no incluye el nivel raíz ni el nivel de suscripción.
- Cada grupo de administración y suscripción solo puede admitir un elemento primario.