Descripción del propósito de Azure Blueprints

Qué ocurre cuando nuestra nube empieza a crecer por encima de una sola suscripción o entorno? ¿Cómo puede escalar la configuración de las características? ¿Cómo puede aplicar la configuración y las directivas en nuevas suscripciones?

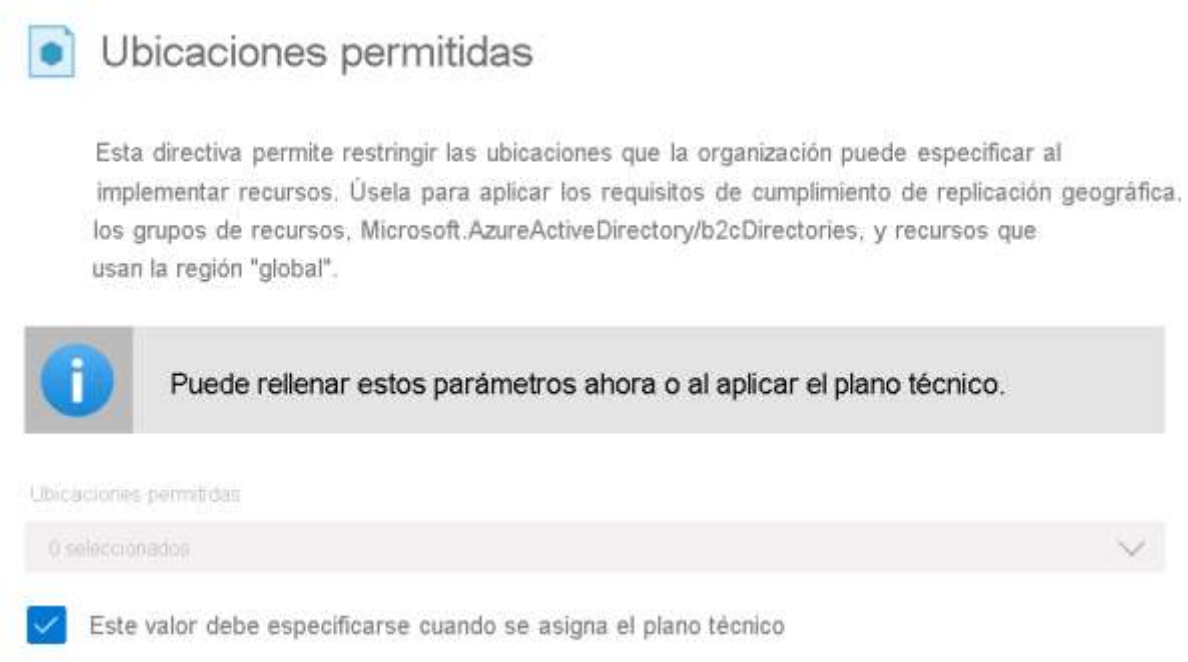
Azure Blueprints le permite estandarizar las implementaciones de entorno o suscripción en la nube. En lugar de tener que configurar características como Azure Policy para cada nueva suscripción, con Azure Blueprints puede definir la configuración repetible y las directivas que se aplican a medida que se crean suscripciones. ¿Necesita un nuevo entorno de pruebas y desarrollo? Azure Blueprints permite implementar un nuevo entorno de pruebas y desarrollo con las opciones de seguridad y cumplimiento ya configuradas. De este modo, los equipos de desarrollo pueden crear e implementar rápidamente nuevos entornos sabiendo que se crean de acuerdo con los estándares organizativos.

¿Qué son los artefactos?

Cada componente de la definición de un plano técnico se denomina artefacto.

Es posible que los artefactos no tengan parámetros adicionales (configuraciones). Un ejemplo es la directiva Implementar la detección de amenazas en servidores SQL Server, que no requiere ninguna configuración adicional.

Los artefactos también pueden contener uno o más parámetros que se pueden configurar. En la siguiente captura de pantalla se muestra la directiva Ubicaciones permitidas, que incluye un parámetro que especifica las ubicaciones que se pueden usar.



Puede especificar el valor de un parámetro al crear la definición del plano técnico o al asignar la definición del plano a un ámbito. De este modo, puede mantener un plano técnico estándar, pero

con la flexibilidad suficiente para especificar los parámetros de configuración pertinentes en cada ámbito en el que se asigne la definición.

Azure Blueprints implementa un nuevo entorno en función de todos los requisitos, las opciones y las configuraciones de los artefactos asociados. Los artefactos pueden incluir cosas como las siguientes:

- Asignaciones de roles
- Asignaciones de directivas
- Plantillas de Azure Resource Manager
- Grupos de recursos

¿Cómo ayuda Azure Blueprints a supervisar las implementaciones?

Azure Blueprints es capaz de crear versiones, lo que le permite establecer una configuración inicial y, después, realizar actualizaciones más adelante y asignar una nueva versión a la actualización. Con el control de versiones, puede realizar pequeñas actualizaciones y realizar un seguimiento de las implementaciones que se usan en el conjunto de configuración.

Con Azure Blueprints, la relación entre la definición del plano técnico (lo que debe ser implementado) y su asignación (lo que se ha implementado) permanece. En otras palabras, Azure crea un registro que asocia un recurso con el plano técnico que lo define, y gracias a esta conexión podemos realizar el seguimiento y la auditoría de nuestras implementaciones.

Descripción del propósito de Azure Policy

¿Cómo puede asegurarse de que estos recursos mantengan su cumplimiento? ¿Puede recibir un aviso cuando la configuración de un recurso cambie?

Azure Policy es un servicio de Azure que permite crear, asignar y administrar directivas que controlan o auditan los recursos. Dichas directivas aplican distintas reglas en las configuraciones de los recursos para que esas configuraciones sigan cumpliendo con los estándares corporativos.

¿Cómo se definen directivas en Azure Policy?

Azure Policy permite definir tanto directivas individuales como grupos de directivas relacionadas, lo que se conoce como iniciativas. Azure Policy evalúa los recursos y resalta los que no cumplen las directivas que hemos creado. Azure Policy también puede impedir que se creen recursos no conformes.

Las directivas de Azure se pueden establecer en cada nivel, lo que le permite establecer directivas en un recurso específico, un grupo de recursos, una suscripción, etc. Además, las directivas de Azure se heredan, por lo que si establece una directiva de nivel alto, se aplicará automáticamente a todas las agrupaciones que se encuentran dentro del elemento primario. Por ejemplo, si establece una directiva de Azure en un grupo de recursos, todos los recursos creados en ese grupo de recursos recibirán automáticamente la misma directiva.

Azure Policy incluye definiciones de iniciativas y directivas integradas para categorías como Almacenamiento, Redes, Proceso, Centro de Seguridad y Supervisión. Por ejemplo, si define una directiva que permite usar exclusivamente un determinado tamaño para las máquinas virtuales (VM) en el entorno, esa directiva se invoca al crear una nueva máquina virtual y cada vez que se cambia el tamaño de las ya existentes. Azure Policy también evalúa y supervisa todas las máquinas virtuales actuales del entorno, incluidas las máquinas virtuales que se crearon antes de crear la directiva.

En algunos casos, Azure Policy puede corregir automáticamente los recursos y configuraciones no conformes para garantizar la integridad del estado de los recursos. Por ejemplo, si todos los recursos de un determinado grupo de recursos deben etiquetarse con la etiqueta AppName y un valor de "SpecialOrders", Azure Policy aplicará automáticamente esa etiqueta si se ha quitado. Sin embargo, sigue conservando el control total del entorno. Si tiene un recurso específico que no desea que Azure Policy corrija automáticamente, puede marcar ese recurso como una excepción y la directiva no corregirá automáticamente ese recurso.

Azure Policy se integra con Azure DevOps aplicando directivas de integración continua y canalización de entrega que competen a las fases de implementación anterior y posterior de las aplicaciones.

¿Qué son las iniciativas Azure Policy?

Una iniciativa de Azure Policy es una forma de agrupar las directivas relacionadas. La definición de iniciativa contiene todas las definiciones de directiva para facilitar el seguimiento del estado de cumplimiento de cara a un objetivo mayor.

Por ejemplo, Azure Policy incluye una iniciativa denominada Habilitar la supervisión en Azure Security Center, Su objetivo es supervisar todas las recomendaciones de seguridad disponibles para todos los tipos de recursos de Azure en Azure Security Center.

En esta iniciativa se incluyen las siguientes definiciones de directiva:

- **Supervisar base de datos SQL sin cifrar en Security Center:** esta directiva supervisa servidores y bases de datos SQL sin cifrar.
- **Supervisión de los puntos vulnerables del sistema operativo en Security Center:** esta directiva supervisa los servidores que no cumplen la línea base de la vulnerabilidad del sistema operativo configurada.
- **Supervisar la falta de Endpoint Protection en Security Center:** esta directiva supervisa los servidores que no tienen instalado un agente de Endpoint Protection.

La iniciativa Habilitar la supervisión en Azure Security Center contiene más de 100 definiciones de directiva independientes, de hecho.

Descripción del propósito de bloqueos de recursos

Los bloqueos de recursos impiden que se eliminen o modifiquen recursos por error.

Aun cuando haya directivas de control de acceso basado en roles de Azure (RBAC de Azure) en vigor, sigue existiendo el riesgo de que alguien con el nivel de acceso adecuado elimine recursos de nube críticos. Los bloqueos de recursos impiden que los recursos se eliminen o actualicen, según el tipo de bloqueo. Los bloqueos de recursos se pueden aplicar a recursos individuales, grupos de recursos o incluso a una suscripción completa. Los bloqueos de recursos se heredan, lo que significa que si coloca un bloqueo de recursos en un grupo de recursos, también se aplicará el bloqueo a todos los recursos dentro del grupo.

Tipos de bloqueos de recursos

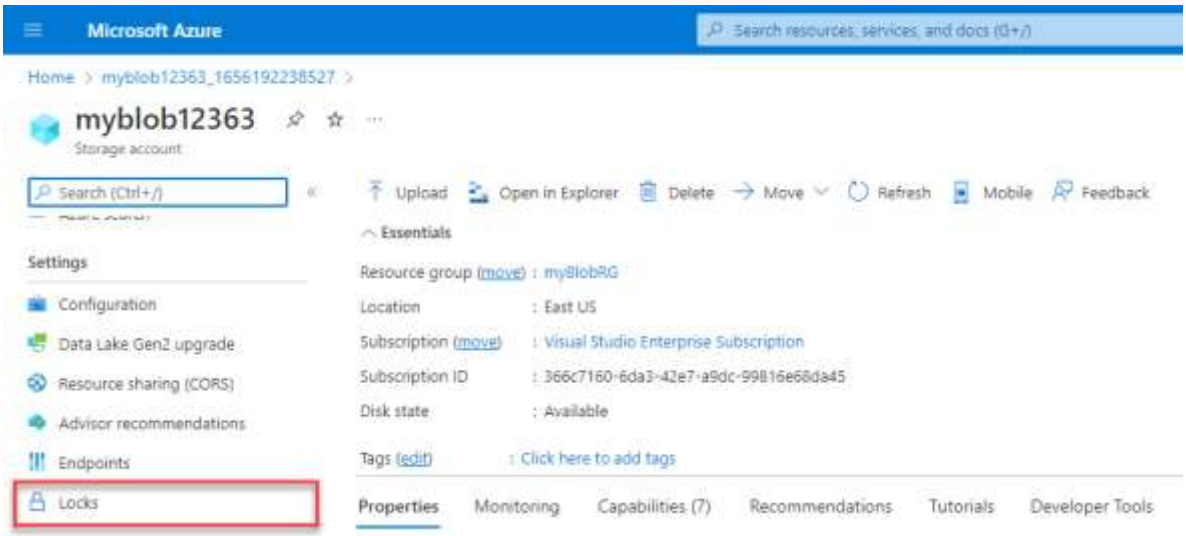
Hay dos tipos de bloqueos de recursos, uno que impide que los usuarios eliminen un recurso y otro que impide que los usuarios lo cambien o eliminen.

- Eliminar significa que los usuarios autorizados pueden leer y modificar un recurso, pero no eliminarlo.
- ReadOnly significa que los usuarios autorizados solo pueden leer recursos, pero no actualizarlos ni eliminarlos. Aplicar este bloqueo es similar a restringir todos los usuarios autorizados a los permisos concedidos por el rol Lector.

¿Cómo se administran los bloqueos de recursos?

Los bloqueos de recursos se pueden administrar en Azure Portal, PowerShell, la CLI de Azure o con una plantilla de Azure Resource Manager.

Para ver, agregar o eliminar bloqueos en Azure Portal, vaya a la sección Configuración del panel Configuración de cualquier recurso en Azure Portal.



¿Cómo se elimina o cambia un recurso bloqueado?

Aunque los bloqueos impiden que se produzcan cambios por error, se pueden seguir realizando cambios realizando un proceso de dos pasos.

Para modificar un recurso bloqueado, primero hay que quitar el bloqueo. Tras quitarlo, podemos aplicar cualquier acción que podamos realizar de acuerdo a nuestros permisos. Los bloqueos de

recursos se aplican con independencia de los permisos RBAC. Es decir, aun siendo el propietario del recurso, tendremos que quitar el bloqueo antes de poder realizar la actividad bloqueada.

Ejercicio: Configuración de un bloqueo de recurso

En este ejercicio, creará un recurso y configurará un bloqueo de recursos. Las cuentas de almacenamiento son uno de los tipos más fáciles de bloqueos de recursos para ver rápidamente el impacto, por lo que usará una cuenta de almacenamiento para este ejercicio.

Este ejercicio requiere que tenga su propia suscripción, lo que significa que deberá utilizar su suscripción de Azure para completar el ejercicio. Sin embargo, no se preocupe, todo el ejercicio se puede completar de forma gratuita con los servicios gratuitos durante 12 meses al registrarse para obtener una cuenta de Azure.

Para obtener ayuda para registrar una cuenta de Azure, consulte el módulo Creación de una cuenta de Azure.

Una vez que haya creado su cuenta gratuita, siga los pasos que se indican a continuación. Si no tiene una cuenta de Azure, puede revisar los pasos para ver el proceso para agregar un bloqueo de recursos simple a un recurso.

Tarea 1: Creación de un recurso

Para aplicar un bloqueo de recursos, debe tener un recurso creado en Azure. La primera tarea se centra en la creación de un recurso que, a continuación, puede bloquear en las tareas posteriores.

1. Inicie sesión en Azure Portal en https://portal.azure.com.
2. Seleccione Crear un recurso.
3. En Categorías, seleccione Almacenamiento.
4. En Cuenta de almacenamiento, seleccione Crear.
5. En la pestaña Aspectos básicos del panel Crear cuenta de almacenamiento, rellene la siguiente información. Deje los valores predeterminados para todo lo demás.

Configuración	Valor
Resource group	Crear nuevo
Nombre de la cuenta de almacenamiento	Escriba un nombre de cuenta de almacenamiento único.
Ubicación	default
Rendimiento	Estándar
Redundancia	Almacenamiento con redundancia local (LRS)

6. Seleccione Revisar y crear para revisar la configuración de su cuenta de almacenamiento y permitir que Azure valide la configuración.

7. Una vez validada, seleccione Crear. Espere la notificación de que la cuenta se creó correctamente.

8. Seleccione Ir al recurso.

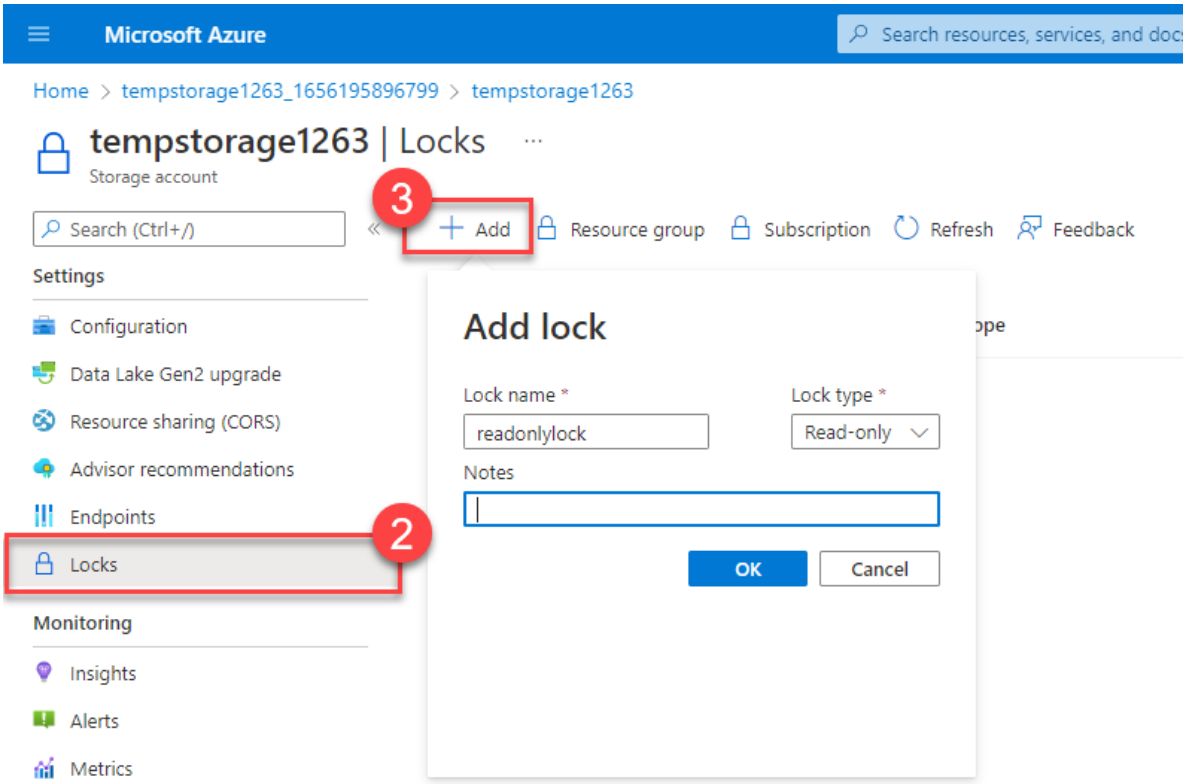
Tarea 2: Aplicación de un bloqueo de recursos de solo lectura

En esta tarea, aplicará un bloqueo de solo lectura a la cuenta de almacenamiento. ¿Qué impacto cree que tendrá en la cuenta de almacenamiento?

1. Desplácese hacia abajo hasta que encuentre la sección Configuración del panel de la izquierda de la pantalla.

2. Seleccione Bloqueos.

3. Seleccione +Agregar.



4. Escriba el nombre del bloqueo.

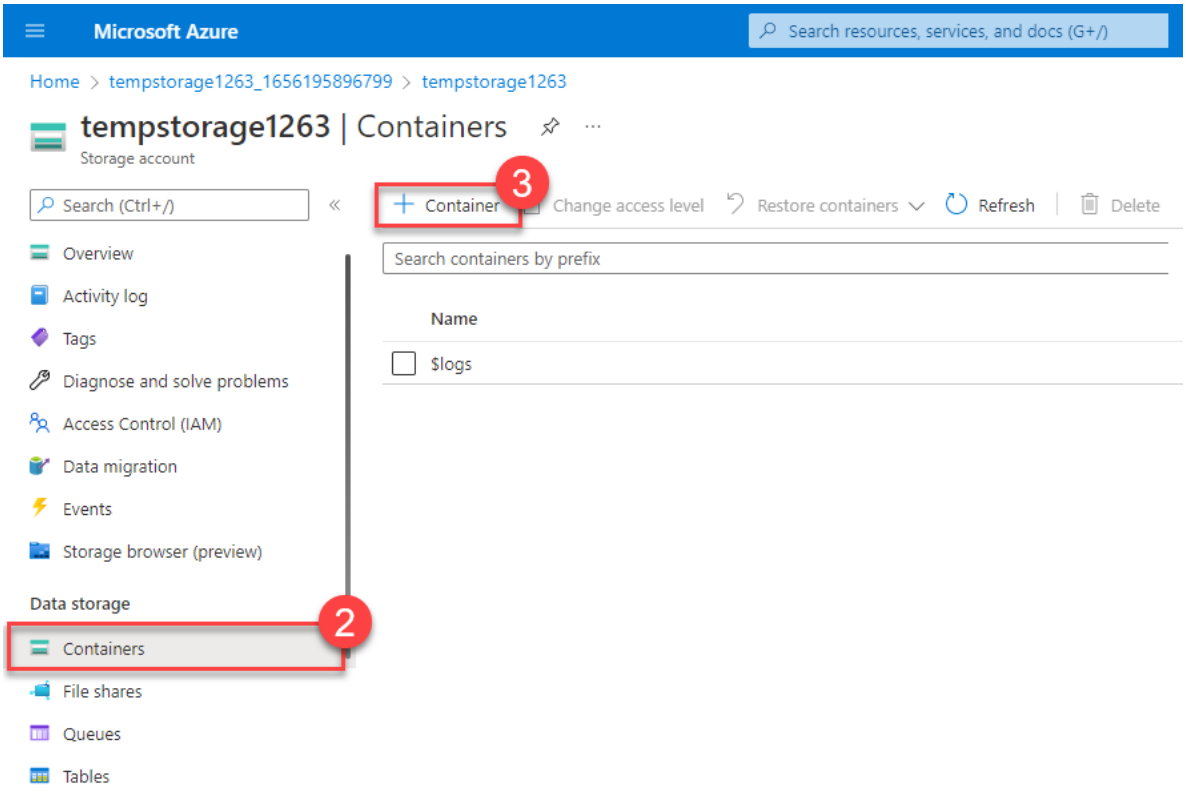
5. Compruebe que el tipo de bloqueo está establecido en Solo lectura.

6. Seleccione Aceptar.

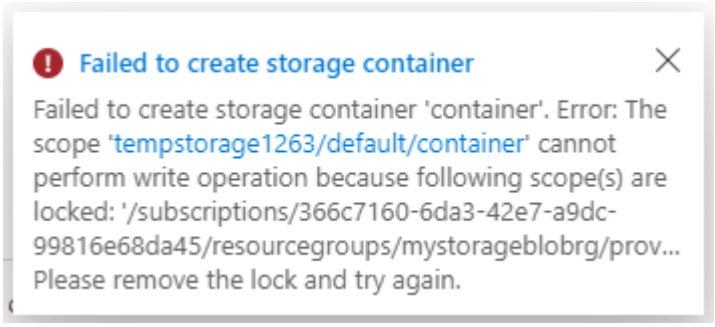
Tarea 3: Agregación de un contenedor a una cuenta de almacenamiento

En esta tarea, agregará un contenedor a la cuenta de almacenamiento; este contenedor es donde puede almacenar los blob.

1. Desplácese hacia arriba hasta que encuentre la sección Almacenamiento de datos del panel de la izquierda de la pantalla.
2. Seleccione Contenedores.
3. Seleccione + Contenedor.



4. Escriba el nombre del contenedor y seleccione Crear.
5. Deberá recibir un mensaje de error: No se pudo crear el contenedor de almacenamiento.

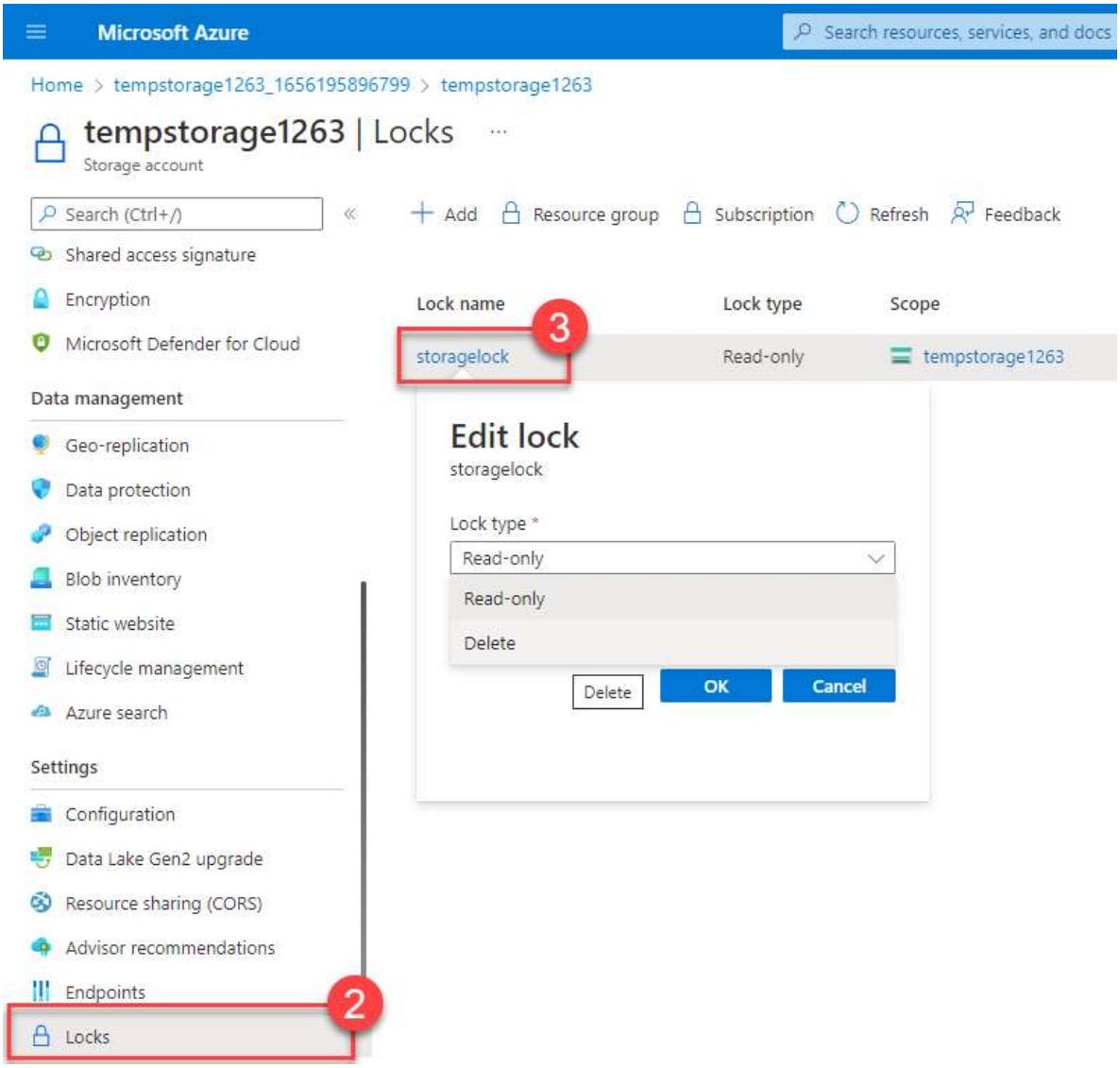


Nota

El mensaje de error le informa de que no se pudo crear un contenedor de almacenamiento porque hay un bloqueo establecido. El bloqueo de solo lectura impide realizar cualquier operación de creación o actualización en la cuenta de almacenamiento, por lo que no puede crear un contenedor de almacenamiento.

Tarea 4: Modificación del bloqueo de recursos y creación de un contenedor de almacenamiento

1. Desplácese hacia abajo hasta que encuentre la sección Configuración del panel de la izquierda de la pantalla.
2. Seleccione Bloqueos.
3. Seleccione el bloqueo de recursos de solo lectura que ha creado.
4. Cambie el tipo de bloqueo a Eliminar y seleccione Aceptar.



5. Desplácese hacia arriba hasta que encuentre la sección Almacenamiento de datos del panel de la izquierda de la pantalla.
6. Seleccione Contenedores.
7. Seleccione + Contenedor.

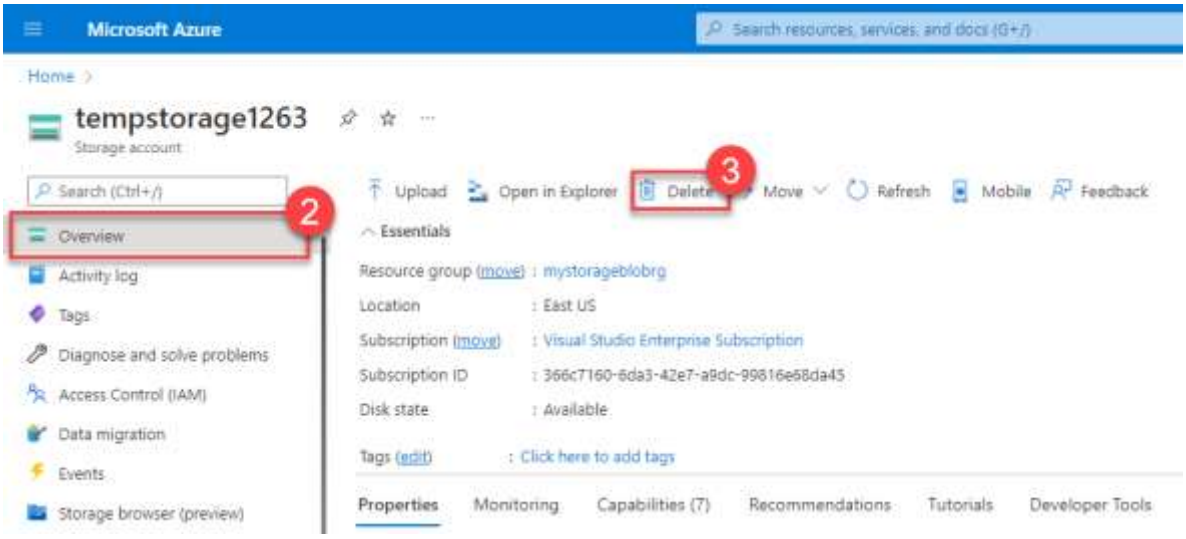
8. Escriba el nombre del contenedor y seleccione Crear.
9. El contenedor de almacenamiento debe aparecer en la lista de contenedores.

Ahora puede comprender cómo el bloqueo de solo lectura le impedía agregar un contenedor a la cuenta de almacenamiento. Una vez que se cambió el tipo de bloqueo (podría haberla quitado en su lugar), pudo agregar un contenedor.

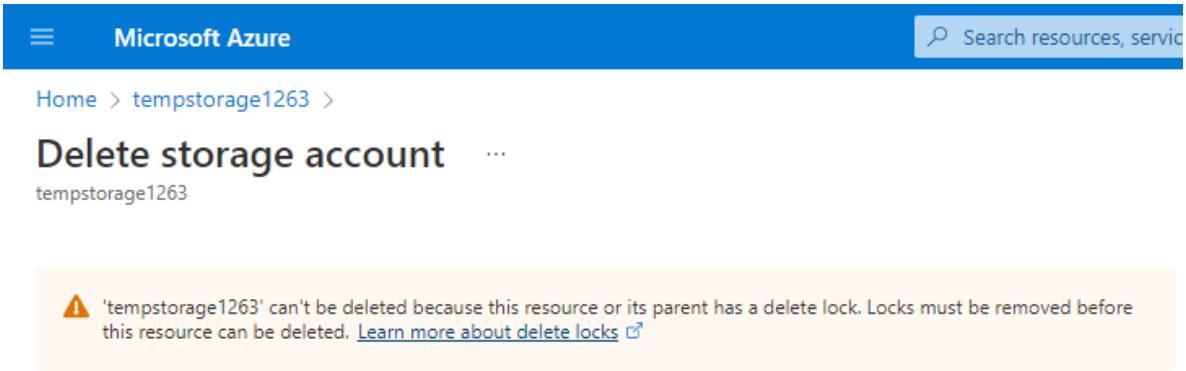
Tarea 5: Eliminación de la cuenta de almacenamiento

En realidad, hará esta última tarea dos veces. Recuerde que hay un bloqueo de eliminación en la cuenta de almacenamiento, por lo que aún no podrá eliminar la cuenta de almacenamiento.

1. Desplácese hacia arriba hasta que encuentre Información general en la parte superior del panel de la izquierda de la pantalla.
2. Seleccione Información general.
3. Seleccione Eliminar.



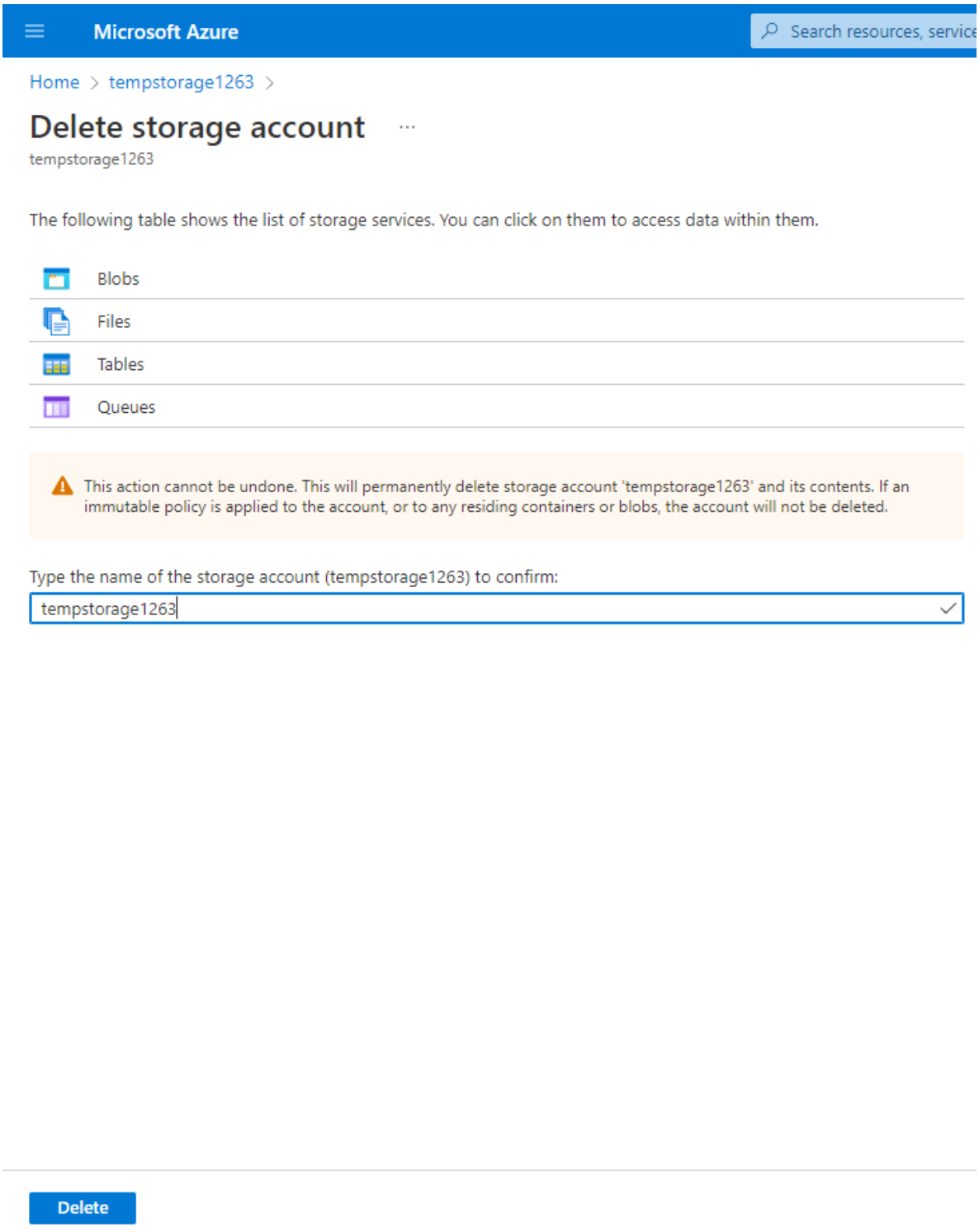
Debería recibir una notificación que le informa de que no puede eliminar el recurso porque tiene un bloqueo de eliminación. Para eliminar la cuenta de almacenamiento, deberá quitar el bloqueo de eliminación.



Tarea 6: Eliminación del bloqueo de eliminación y eliminación de la cuenta de almacenamiento

En la tarea final, quitará el bloqueo de recursos y eliminará la cuenta de almacenamiento de la cuenta de Azure. Este paso es importante. Querrá asegurarse de que no tiene ningún recurso inactivo en su cuenta.

1. Seleccione el nombre de la cuenta de almacenamiento en la ruta de navegación de la parte superior de la pantalla.
2. Desplácese hacia abajo hasta que encuentre la sección Configuración del panel de la izquierda de la pantalla.
3. Seleccione Bloqueos.
4. Seleccione Eliminar.
5. Seleccione Inicio en la ruta de navegación de la parte superior de la pantalla.
6. Seleccione Cuentas de almacenamiento.
7. Seleccione la cuenta de almacenamiento que usó para este ejercicio.
8. Seleccione Eliminar.
9. Para evitar la eliminación accidental, Azure le pide que escriba el nombre de la cuenta de almacenamiento que quiere eliminar. Escriba el nombre de la cuenta de almacenamiento y seleccione Eliminar.



10. Deberá recibir un mensaje que indica que se eliminó la cuenta de almacenamiento. Si va a Inicio > Cuentas de almacenamiento, debería ver que la cuenta de almacenamiento que creó para este ejercicio ha desaparecido.

¡Enhorabuena! Ha completado la configuración, actualización y eliminación de un bloqueo de recursos en un recurso de Azure.

Importante

Asegúrese de completar la tarea 6, la eliminación de la cuenta de almacenamiento. Usted es el único responsable de los recursos de su cuenta de Azure. Asegúrese de limpiar la cuenta después de completar este ejercicio.

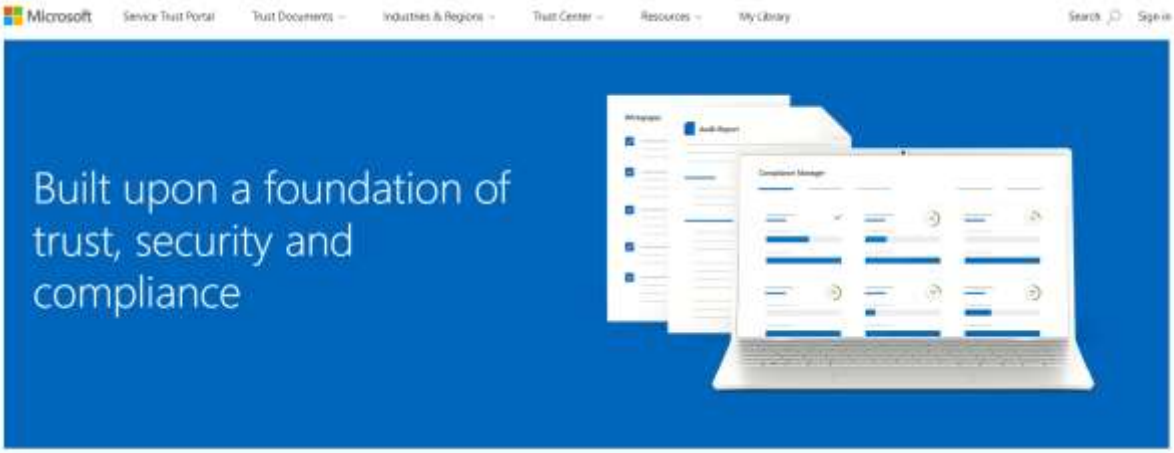
Descripción de las ventajas del portal de confianza de servicios

El Portal de confianza de servicios de Microsoft es un portal que proporciona contenido, herramientas y otros recursos sobre las prácticas de seguridad, privacidad y cumplimiento de Microsoft.

El Portal de confianza de servicios contiene detalles sobre la implementación de controles y procesos de Microsoft que protegen nuestros servicios en la nube y los datos de los clientes que contienen. Para acceder a algunos de los recursos del Portal de confianza de servicios, debe iniciar sesión con un usuario autenticado con su cuenta de Servicios en la nube de Microsoft (cuenta de organización de Azure Active Directory). Deberá revisar y aceptar el acuerdo de no divulgación de Microsoft para acceder a los materiales de cumplimiento.

Acceso al Portal de confianza de servicios

Puede acceder al Portal de confianza de servicios en https://servicetrust.microsoft.com/.



Las características y el contenido del Portal de confianza de servicios son accesibles desde el menú principal. Las categorías del menú principal son:

- El **Portal de confianza de servicios** proporciona un hipervínculo de acceso rápido para volver a la página principal del Portal de confianza de servicios.
- Los **Documentos de confianza** proporcionan una gran cantidad de información de diseño e implementación de seguridad. El objetivo de la información es facilitarle el cumplimiento de los objetivos reglamentarios mediante la comprensión de cómo los servicios de Microsoft Cloud mantienen los datos seguros. Los documentos de confianza tienen

elementos secundarios, entre los que se incluyen los informes de auditoría, la protección de datos y Azure Stack.

- **Sectores y regiones** proporciona información de cumplimiento específica de la región sobre los servicios de Microsoft Cloud.
- El **Centro de confianza** vincula al Centro de confianza de Microsoft. El Centro de confianza proporciona más información sobre la seguridad, el cumplimiento y la privacidad en Microsoft Cloud. Esto incluye: información sobre las funcionalidades de los servicios de Microsoft Cloud que puede usar para abordar requisitos específicos del Reglamento general de protección de datos; documentación útil para la responsabilidad del RGPD, y documentación útil para comprender las medidas técnicas y organizativas que Microsoft ha adoptado para respaldar el RGPD.
- Los **recursos** proporcionan acceso a más recursos, como el Centro de seguridad y cumplimiento, información sobre los centros de datos globales de Microsoft y Preguntas más frecuentes.
- **Mi biblioteca** le permite guardar (o fijar) documentos para acceder rápidamente a ellos en la página Mi biblioteca. También puede establecer una configuración para recibir notificaciones cuando se actualicen los documentos en Mi biblioteca.

Nota

Los informes y documentos del Portal de confianza de servicios están disponibles para descargarse durante al menos 12 meses después de la publicación o hasta que haya disponible una nueva versión del documento.