**Introducción**

Este módulo se centra en permitir que los administradores planeen, implementen y administren de forma eficaz la gobernanza de la seguridad en Azure, garantizando el cumplimiento de las directivas de la organización y los procedimientos recomendados.

**Escenario**

Imagine que es un administrador de seguridad responsable de mantener la posición de seguridad del entorno de Azure de su organización. Su organización se basa en Azure para cargas de trabajo críticas y debe establecer prácticas de gobernanza sólidas para proteger los datos confidenciales y mantener el cumplimiento normativo.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Cree, asigne e interprete las directivas e iniciativas de seguridad en Azure Policy para aplicar los estándares de cumplimiento y seguridad.
* Configure las opciones de seguridad mediante Azure Blueprint para simplificar la implementación de infraestructuras seguras.
* Implemente infraestructuras seguras mediante una zona de aterrizaje para garantizar entornos de Azure coherentes y seguros.
* Cree y configure una instancia de Azure Key Vault para administrar de forma segura certificados, secretos y claves.
* Proporcione recomendaciones sobre cuándo usar un módulo de seguridad de hardware (HSM) dedicado para mejorar la seguridad de administración de claves.
* Configurar el acceso a Key Vault, incluidas las directivas de acceso de almacén y el control de acceso basado en roles (RBAC) de Azure para controlar los permisos de forma eficaz.
* Administre certificados, secretos y claves en Azure Key Vault para proteger el almacenamiento y la distribución.
* Configure la rotación de claves para mejorar la seguridad mediante la actualización periódica de claves criptográficas.
* Implemente procesos de copia de seguridad y recuperación para certificados, secretos y claves para garantizar la resistencia y la disponibilidad de los datos.

**Objetivos**

El módulo tiene como objetivo equipar a los participantes con los conocimientos y aptitudes necesarios para establecer y administrar prácticas de gobernanza para la seguridad en Azure. Los participantes podrán aplicar directivas de seguridad, configurar infraestructuras seguras, administrar claves criptográficas de forma segura e implementar medidas de copia de seguridad y recuperación, mejorando en última instancia la posición de seguridad y el cumplimiento de sus entornos de Azure.

**Creación, asignación e interpretación directivas e iniciativas de seguridad en Azure Policy**

Comprender cómo se crean y administran las directivas en Azure es importante para mantener el cumplimiento de los estándares corporativos y los contratos de nivel de servicio. En este ejemplo, aprenderá a usar Azure Policy para realizar algunas de las tareas más comunes relacionadas con la creación, la asignación y la administración de directivas en toda la organización, como, por ejemplo:

* Asignar una directiva para aplicar una condición a los recursos que se creen en el futuro
* Crear y asignar una definición de iniciativa para realizar un seguimiento del cumplimiento para varios recursos
* Resolución de un recurso que no cumpla o que sea denegado
* Implementar una nueva directiva en toda la organización

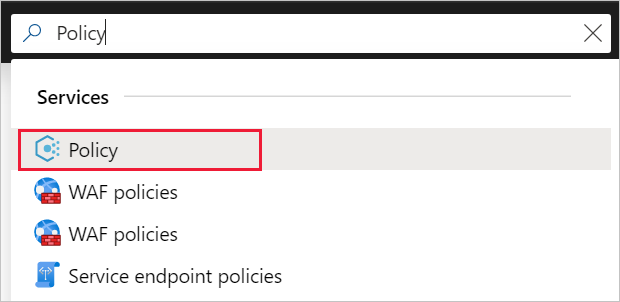
**Requisitos previos**

Si no tiene una suscripción a Azure, cree una cuenta gratuita antes de empezar.

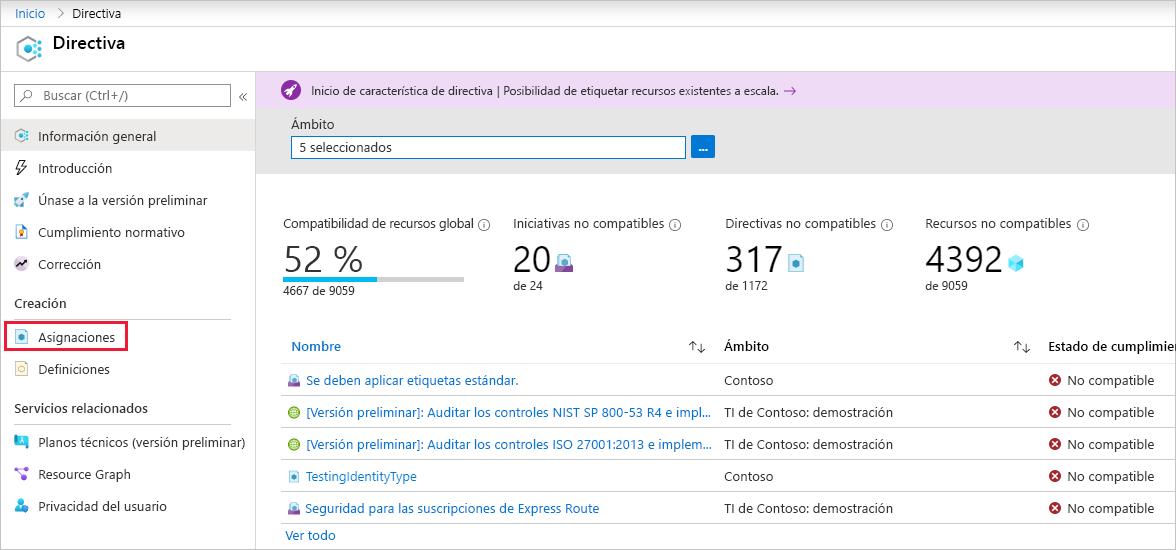
**Asignación de una directiva**

El primer paso para aplicar cumplimientos con Azure Policy es asignar una definición de directiva. Una definición de directiva precisa en qué condiciones se aplica una directiva y qué efecto debe tener. En este ejemplo, asigne la definición de directiva integrada llamada *Heredar una etiqueta del grupo de recursos si falta* para agregar la etiqueta especificada con su valor del grupo de recursos primario a los recursos nuevos o actualizados a los que les falta la etiqueta.

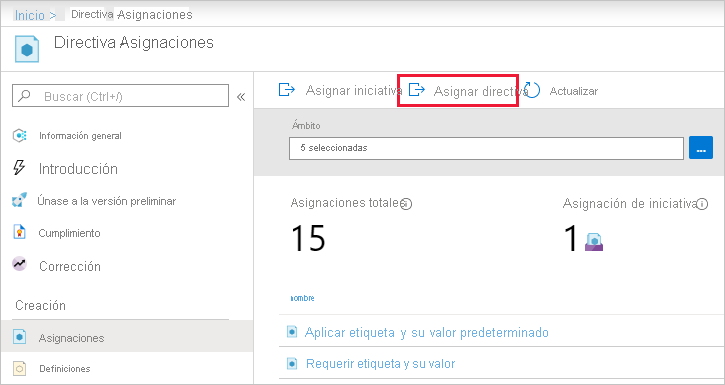
1. Vaya a Azure Portal para asignar directivas. Busque y seleccione **Directiva**.



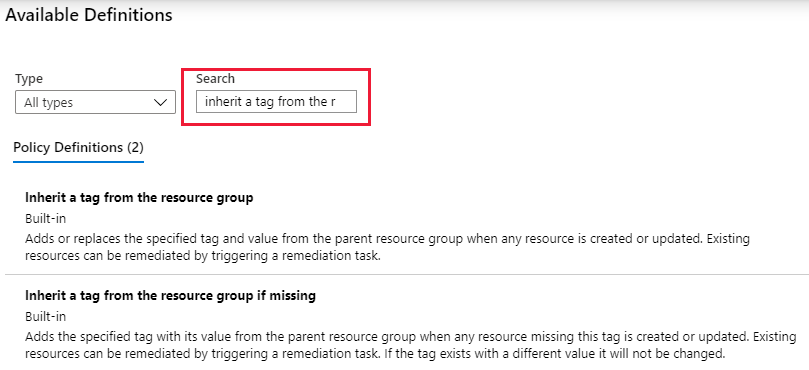
1. Seleccione **Asignaciones** en el panel izquierdo de la página de Azure Policy. Una asignación es una directiva que se asignó para que se lleve a cabo dentro de un ámbito específico.



1. Seleccione **Asignar directiva** en la parte superior de la página **Policy - Asignaciones**.



1. En la página **Asignar directiva** y en la pestaña **Aspectos básicos**, seleccione los puntos suspensivos y seleccione una suscripción o un grupo de administración como **Ámbito**. Opcionalmente, seleccione un grupo de recursos. Un ámbito determina en qué recursos o agrupación de recursos se implementa la asignación de directiva. Después, haga clic en **Seleccionar** en la parte inferior de la página **Ámbito**. En este ejemplo se usa la suscripción de **Contoso**. Su suscripción variará.
2. Los recursos se pueden excluir según el **ámbito**. Las **exclusiones** comienzan en un nivel inferior al nivel del **ámbito**. Las **exclusiones** son opcionales, así que déjelas en blanco por ahora.
3. Seleccione los puntos suspensivos de **Definición de directiva** para abrir la lista de definiciones disponibles. Puede filtrar el campo **Tipo** de la definición de directiva por Integrada para verlas todas y leer sus descripciones.
4. Seleccione **Heredar una etiqueta del grupo de recursos si falta**. Si no la encuentra inmediatamente, escriba **heredar una etiqueta** en el cuadro de búsqueda y, después, presione ENTRAR o haga clic fuera del cuadro de búsqueda. Haga clic en **Seleccionar** en la parte inferior de la página **Definiciones disponibles** después de encontrar y seleccionar la definición de directiva.



1. **Nombre de asignación** se rellena automáticamente con el nombre de directiva seleccionado, pero puede cambiarlo. En este ejemplo, deje *Heredar una etiqueta del grupo de recursos si falta*. También puede agregar una **Descripción** opcional. La descripción ofrece detalles sobre esta asignación de directiva.
2. Deje **Cumplimiento de directivas** como *Habilitado*. Cuando esta *Deshabilitado*, esta configuración permite probar el resultado de la directiva sin desencadenar el efecto. Para más información, consulte Modo de cumplimiento.
3. **Asignado por**: se rellena automáticamente en función de quién ha iniciado sesión. Este campo es opcional, así que se pueden especificar valores personalizados.
4. Seleccione la pestaña **Parámetros** en la parte superior del asistente.
5. En **Nombre de etiqueta**, escriba *Entorno*.
6. Seleccione la pestaña **Corrección** en la parte superior del asistente.
7. Deje sin marcar **Crear una tarea de corrección**. Este cuadro permite crear una tarea para modificar los recursos existentes, además de los recursos nuevos o actualizados.
8. La casilla **Crear una identidad administrada** se activa automáticamente, ya que esta definición de directiva usa el efecto modify. **Permisos** se establece automáticamente en *Colaborador* según la definición de directiva. Para obtener más información, consulte las identidades administradas y cómo funciona la seguridad de corrección.
9. Seleccione la pestaña **Non-compliance messages** (Mensajes de no cumplimiento) en la parte superior del asistente.
10. Establezca **Non-compliance message** (Mensaje de no cumplimiento) en*This resource doesn't have the required tag* (Este recurso no tiene la etiqueta necesaria). Este mensaje personalizado se muestra cuando se deniega un recurso o cuando hay recursos no compatibles durante la evaluación periódica.
11. Seleccione la pestaña **Revisar y crear** en la parte superior del asistente.
12. Revise las selecciones y, luego, seleccione **Crear** en la parte inferior de la página.

**Configuración de los valores de seguridad para Azure Blueprint**

Del mismo modo que un plano técnico permite a un ingeniero o a un arquitecto bosquejar los parámetros de diseño de un proyecto, Azure Blueprint permite a los grupos de arquitectos de la nube y de TI central definir un conjunto repetible de recursos de Azure que implementa y cumple los estándares de la organización, sus requisitos y sus patrones. Azure Blueprints permite a los equipos de desarrollo compilar e iniciar rápidamente nuevos entornos sabiendo que se compilan cumpliendo los estándares organizativos y que contienen un conjunto de componentes integrados, como las redes, para acelerar el desarrollo y la entrega.

Los planos técnicos son una manera declarativa de organizar la implementación de varias plantillas de recursos y de otros artefactos, como son:

* Asignaciones de roles
* Asignaciones de directiva
* Plantillas del Administrador de recursos de Azure
* Grupos de recursos

El servicio Azure Blueprints está respaldado por la distribución global Azure Cosmos DB. Los objetos de plano técnico se replican en varias regiones de Azure. Esta replicación proporciona baja latencia, alta disponibilidad y acceso coherente a los objetos de plano técnico, con independencia de la región en la que Azure Blueprints implemente el recurso.

¿En qué difiere de las plantillas de Azure Resource Manager?

El servicio está diseñado para ayudar con la configuración del entorno. A menudo, esta configuración consta de un conjunto de grupos de recursos, directivas, asignaciones de roles e implementaciones de plantillas de Azure Resource Manager. Un plano técnico es un paquete para reunir todos estos tipos de artefacto y permite componer y crear la versión del paquete, incluso mediante una canalización de integración continua y entrega continua (CI/CD). En última instancia, cada uno se asigna a una suscripción en una única operación que se puede auditar y seguir.

Casi todo lo que se puede querer incluir para la implementación en Azure Blueprints se puede conseguir con plantillas de Azure Resource Manager. Sin embargo, una plantilla de Azure Resource Manager es un documento que no existe de forma nativa en Azure, sino que cada una se almacena localmente o en el control de código fuente o en Plantillas (versión preliminar). La plantilla se usa para las implementaciones de uno o varios recursos de Azure pero, una vez implementados los recursos, no hay conexión activa ni relación con la plantilla.

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. Esta conexión permite un seguimiento mejorado y la auditoría de las implementaciones. Azure Blueprints también puede actualizar varias suscripciones a la vez que se rigen por el mismo plano técnico.

No hay que elegir entre una plantilla de Azure Resource Manager y un plano técnico. Cada plano técnico puede tener o no artefactos de una plantilla de Azure Resource Manager. Esta compatibilidad significa que se pueden reutilizar los trabajos anteriores para desarrollar y mantener una biblioteca de plantillas de Azure Resource Manager en Azure Blueprints.

**¿En qué difiere de Azure Policy?**

Un plano técnico es un paquete o contenedor para crear conjuntos muy específicos de estándares, patrones y requisitos relacionados con la implementación de los servicios en la nube de Azure, la seguridad y el diseño que se pueden reutilizar para garantizar la coherencia y el cumplimiento normativo.

Una directiva es un sistema de denegación explícita y permisos predeterminados que se centra en las propiedades de recursos durante su implementación y para los recursos ya existentes. Admite la gobernanza de la nube al validar que los recursos de una suscripción cumplen los requisitos y estándares.

La inclusión de una directiva en un plano técnico permite crear el patrón o diseño adecuado durante la asignación del plano. La inclusión de la directiva garantiza que solo se puedan realizar en el entorno cambios aprobados o esperados para proteger el cumplimiento continuo en relación al plano técnico.

Se puede incluir una directiva como uno de muchos *artefactos* en una definición de plano técnico. Los planos técnicos también permiten usar parámetros con las directivas y las iniciativas.

**Definición del plano técnico**

Un plano técnico se compone de *artefactos*. Azure Blueprints admite actualmente los siguientes recursos como artefactos:

| **Recurso** | **Opciones de jerarquía** | **Descripción** |
| --- | --- | --- |
| Grupos de recursos | Subscription | Cree un nuevo grupo de recursos para que lo usen otros artefactos incluidos en el plano técnico. Estos grupos de recursos de marcador de posición permiten organizar los recursos exactamente como desee que se estructuren y proporciona un limitador de ámbito para los artefactos de asignación de roles y directivas, así como plantillas de Resource Manager. |
| Plantilla del Administrador de recursos de Azure | Suscripción, grupo de recursos | Las plantillas, incluidas las plantillas anidadas y vinculadas, se usan para crear entornos complejos. Ejemplo de entornos: una granja de servidores SharePoint, Azure Automation State Configuration o un área de trabajo de Log Analytics. |
| Asignación de directiva | Suscripción, grupo de recursos | Permite la asignación de una directiva o iniciativa a la suscripción a la que está asignado el plano técnico. La directiva o iniciativa debe estar dentro del ámbito de la ubicación de la definición del plano técnico. Si la directiva o iniciativa tiene parámetros, estos se asignan en la creación del plano técnico o durante su asignación. |
| Asignación de roles | Suscripción, grupo de recursos | Agregue un grupo o usuario existente a un rol integrado para asegurarse de que las personas adecuadas siempre tienen derechos de acceso a los recursos. Las asignaciones de roles se pueden definir para toda la suscripción o anidarse para un grupo de recursos específico incluido en el plano técnico. |

**Ubicaciones de definición de plano técnico**

Al crear una definición de plano técnico, definirá dónde se guarda. Los planos técnicos se pueden guardar en un grupo de administración o suscripción a los que tenga acceso de colaborador. Si la ubicación es un grupo de administración, el plano técnico está disponible para asignarlo a cualquier suscripción secundaria de ese grupo de administración.

**Parámetros de plano técnico**

Los planos técnicos pueden pasar parámetros a una iniciativa o directiva, o a una plantilla de Azure Resource Manager. Cuando algún artefacto se agrega a un plano técnico, el autor decide si proporciona un valor definido para cada asignación de plano técnico o si permite que cada asignación de plano técnico proporcione un valor en el momento de la asignación. Esta flexibilidad permite definir un valor predeterminado para todos los usos del plano técnico o que esa decisión se tome en el momento de la asignación.

**Publicación de planos técnicos**

Cuando se crea por primera vez un plano técnico, se considera que está en modo borrador. Cuando está preparado para asignarse, se debe publicar. La publicación requiere la definición de una cadena de versión (letras, números y guiones con una longitud máxima de 20 caracteres) junto con notas de cambio opcionales. La versión la diferencia de los cambios futuros del mismo plano técnico y permite la asignación de cada versión. Esto también significa que a la misma suscripción se le pueden asignar versiones diferentes del mismo plano técnico. Cuando se realizan cambios adicionales en el plano técnico, la versión publicada seguirá existiendo, al igual que los cambios sin publicar. Una vez completados los cambios, el plano técnico actualizado se publica con una versión nueva y única, y ahora también se puede asignar.

**Asignación de plano técnico**

Cada versión publicada de un plano técnico (con una longitud máxima del nombre de 90 caracteres) se puede asignar a un grupo de administración o una suscripción existentes. En el portal, el plano técnico tiene de forma predeterminada la versiónpublicada más recientemente. Si hay parámetros de artefacto o parámetros de plano técnico, se definirán durante el proceso de asignación.

**Nota**

*Asignar una definición de plano técnico a un grupo de administración significa que el objeto de asignación existe en el grupo de administración. La implementación de artefactos sigue teniendo como destino una suscripción. Para realizar una asignación de grupo de administración, se debe usar la API de REST Crear o Actualizar, y el cuerpo de la solicitud debe incluir un valor para properties.scope para definir la suscripción de destino.*

**Permisos de Azure Blueprint**

Para poder utilizar planos técnicos, se le deben conceder permisos mediante el control de acceso basado en rol de Azure (Azure RBAC). Para leer o ver un plano técnico en Azure Portal, la cuenta debe tener acceso de lectura al ámbito en que se encuentra la definición del mismo.

Para crear planos técnicos, su cuenta necesita los siguientes permisos:

* Microsoft.Blueprint/blueprints/write: para crear una definición de plano técnico
* Microsoft.Blueprint/blueprints/artifacts/write: para crear artefactos en una definición de plano técnico
* Microsoft.Blueprint/blueprints/versions/write - Publish a blueprint

Para eliminar planos técnicos, su cuenta necesita los siguientes permisos:

* Microsoft.Blueprint/blueprints/delete
* Microsoft.Blueprint/blueprints/artifacts/delete
* Microsoft.Blueprint/blueprints/versions/delete

**Nota**

*Los permisos de definición del plano técnico deben ser concedidos o heredados en el ámbito de la suscripción o grupo de administración donde se guarde.*

**Nota**

*Como las asignaciones de planos técnicos se crean en una suscripción, los permisos de asignación y de cancelación de la asignación deben concederse o heredarse en el ámbito de una suscripción.*

Para asignar o cancelar la asignación de un plano técnico, la cuenta necesita los siguientes permisos:

* Microsoft.Blueprint/blueprintAssignments/write: para asignar un plano técnico
* Microsoft.Blueprint/blueprintAssignments/delete: para cancelar la asignación de un plano técnico

Están disponibles los siguientes roles integrados:

| **Rol de Azure** | **Descripción** |
| --- | --- |
| Propietario | Además de otros permisos, incluye todos los permisos relacionados con Azure Blueprints. |
| Colaborador | Además de otros permisos, puede crear y eliminar definiciones de planos técnicos, pero no tiene permisos para asignarlos. |
| Colaborador de plano técnico | Puede administrar las definiciones del plano técnico, pero no asignarlas. |
| Operador del plano técnico | Puede asignar los planos técnicos publicados existentes, pero no puede crear nuevos. Las asignaciones solo funcionan si se realizan con una identidad administrada asignada por el usuario. |

Si estos roles integrados no satisfacen sus necesidades de seguridad, considere la posibilidad de crear un rol personalizado.

**Nota**

*Si usa una identidad administrada asignada por el sistema, la entidad de servicio para Azure Blueprints requiere el rol****Propietario****en la suscripción asignada con el fin de habilitar la implementación. Si usa el portal, este rol se le concede automáticamente y se revoca para la implementación. Si usa la API REST, este rol se debe conceder manualmente, pero se sigue revocando de forma automática una vez finalizada la implementación. Si usa una identidad administrada asignada por el usuario, solo el usuario que crea la asignación del plano técnico necesita los* Microsoft.Blueprint/blueprintAssignments/write*permisos que se incluyen en los roles integrados****Propietario****y****Operador de plano técnico****.*

**Implementación de infraestructuras seguras mediante una zona de aterrizaje**

**Creación de zonas de aterrizaje de Azure escalables y modulares**

Microsoft ofrece Cloud Adoption Framework para proporcionar a los clientes un punto de partida demostrado para el recorrido en la nube, incluida la metodología de seguridad.

Otro componente crítico de Cloud Adoption Framework en la metodología de preparación es la zona de aterrizaje de Azure, que acelera la adopción de la nube al proporcionar una implementación automatizada de arquitecturas completas y entornos operativos, incluidos los elementos de seguridad. Los procedimientos recomendados de seguridad van integrados en las zonas de aterrizaje de Azure. Con las zonas de aterrizaje, puede migrar de forma rápida y segura las primeras cargas de trabajo con procedimientos recomendados de seguridad y gobernanza, que van incorporados.

Mientras diseña e implementa la zona de aterrizaje de la organización, use la arquitectura de referencia siguiente como estado final de destino. Sirve para capturar consideraciones de diseño del entorno maduras y escaladas horizontalmente.

Se recomienda usar zonas de aterrizaje de Azure siempre que sea posible en los planes de adopción de la nube. Las zonas de aterrizaje proporcionan un punto de partida arquitectónico. Las zonas de aterrizaje de Azure le ayudan a cumplir con la seguridad y con otros procedimientos recomendados en varias operaciones: si implementa una nueva carga de trabajo, si migra las cargas de trabajo existentes o si mejora las cargas de trabajo ya implementadas. El uso de zonas de aterrizaje le ayuda a seguir los procedimientos recomendados, tanto si los implementa todos a la vez como si lo hace de forma incremental.

**Nota**

*Su organización puede personalizar la arquitectura de la zona de aterrizaje de Azure para satisfacer sus requisitos empresariales únicos.*

Las zonas de aterrizaje de Azure contienen código que facilita la labor de los equipos de TI y de seguridad de la organización. Las zonas de aterrizaje ofrecen un método repetible y predecible para aplicar una implementación basada en plantillas. Esa implementación incluye un enfoque de implementación, unos principios de diseño y unas áreas de diseño. Las zonas de aterrizaje admiten procesos de seguridad, administración y gobernanza, así como procesos de automatización de la plataforma y de DevOps.

**Uso de principios de Confianza cero**

La organización puede adaptar las zonas de aterrizaje de Azure en función de los procedimientos recomendados y los principios de Confianza cero (ZT) de Azure Security Benchmark (ASB), que se incluyen en la arquitectura de destino. Pase a la arquitectura de destino alineada con procedimientos recomendados, mediante la implementación de otras consideraciones de seguridad y principios de Confianza cero que se aplican de forma incremental y mejoran el MVP de seguridad y gobernanza de la organización.

Aumente el uso de enfoques arquitectónicos de Confianza cero que *nunca se basan en la confianza y siempre hacen comprobaciones*. Integre una estrategia de un extremo a otro en el estado digital que abarque identidades, puntos de conexión, red, datos, aplicaciones e infraestructura.

**Siga las recomendaciones de seguridad de Azure Security Benchmark**

Se recomienda que la organización siga las recomendaciones de seguridad de gran impacto de Azure Security Benchmark. También hay instrucciones en las zonas de aterrizaje de Azure y en el propio Cloud Adoption Framework. Incluya recomendaciones de ASB como parte de la estrategia de arquitectura revisando toda la documentación pertinente y las líneas base específicas del servicio.

**Sugerencia**

*Las zonas de aterrizaje de Azure colocan la directiva ASB en la parte superior de su jerarquía de manera predeterminada. Este enfoque garantiza que todas las suscripciones y cargas de trabajo de la zona de aterrizaje se supervisan para el cumplimiento de ASB.*

**Creación y configuración de una instancia de Azure Key Vault**

Azure Key Vault es un servicio de almacenamiento seguro en la nube para claves, secretos y certificados.

**Inicio de sesión en Azure**

Inicie sesión en Azure Portal.

**Creación de un almacén**

1. En el menú de Azure Portal o en la **página principal**, seleccione **Crear un recurso**.
2. En el cuadro de búsqueda, escriba **Key Vault**.
3. En la lista de resultados, elija **Key Vault**.
4. En la sección Key Vault, elija **Crear**.
5. En la sección **Crear almacén de claves**, proporcione la siguiente información:
   * **Name**: se requiere un nombre único. En esta guía de inicio rápido se usará **Contoso-vault2**.
   * **Suscripción**: Elija una suscripción.
   * En **Grupo de recursos**, elija **Crear nuevo** y escriba un nombre para el grupo de recursos.
   * En el menú desplegable **Ubicación**, elija una ubicación.
   * Deje las restantes opciones con sus valores predeterminados.
6. Seleccione **Crear**.

Tome nota de estas dos propiedades:

* **Nombre del almacén**: en este ejemplo es Contoso-Vault2. Utilizará este nombre para otros pasos.
* **URI de Key Vault**: en el ejemplo, el URI de Key Vault es https://contoso-vault2.vault.azure.net/. Las aplicaciones que utilizan el almacén a través de su API de REST deben usar este identificador URI.

En este momento, su cuenta de Azure es la única autorizada para realizar operaciones en este nuevo almacén.

**Configuración de las redes de Azure Key Vault**

1. Vaya al almacén de claves que creó anteriormente.
2. Seleccione **Redes** y, luego, elija la pestaña **Firewalls and virtual networks** (Firewalls y redes virtuales).
3. Haga clic en **Redes seleccionadas** en **Permitir el acceso desde**.
4. Para agregar redes virtuales existentes a los firewall y las reglas de red virtual, haga clic en **+ Agregar redes virtuales existentes**.
5. En la nueva hoja que se abrirá, seleccione la suscripción, las redes virtuales y las subredes a las cuales desea otorgar acceso a este almacén de claves. Si las redes virtuales y subredes que seleccionó no tienen puntos de conexión de servicio habilitados, confirme que desea habilitar los puntos de conexión de servicio y seleccione **Habilitar**. Esta operación podría tardar hasta 15 minutos en surtir efecto.
6. En **Redes IP**, agregue intervalos de direcciones IPv4; para ello, escriba los intervalos de direcciones IPv4 en notación CIDR (enrutamiento de interdominios sin clases) o las direcciones IP individuales.
7. Si desea permitir que los servicios de confianza de Microsoft omitan el firewall de Key Vault, seleccione "Sí". Para ver una lista completa de los servicios de confianza Key Vault actuales, consulte el siguiente vínculo. Servicios de confianza de Azure Key Vault
8. Seleccione **Guardar**.

Asimismo, puede también agregar nuevas redes virtuales y subredes y habilitar los puntos de conexión de servicio de las redes virtuales y subredes recién creadas. Para ello, haga clic en **+ Agregar nueva red virtual**. A continuación, siga las indicaciones.

**Recomendación sobre cuándo usar un módulo de seguridad de hardware dedicado (HSM)**

Azure Dedicated HSM ofrece almacenamiento de claves criptográficas en Azure. Dedicated HSM cumple los requisitos de seguridad más estrictos. Es la solución idónea para los clientes que necesitan dispositivos validados con la certificación FIPS 140-2 nivel 3 y un control completo y exclusivo del dispositivo HSM.

Los dispositivos HSM se implementan de manera global en varias regiones de Azure. Se pueden aprovisionar fácilmente como un par de dispositivos y configurar para alta disponibilidad. Los dispositivos HSM también se pueden aprovisionar entre regiones para protección frente a conmutaciones por error en el nivel regional. Microsoft ofrece el servicio Dedicated HSM mediante el uso de los dispositivos Thales Luna 7 HSM modelo A790. Este dispositivo ofrece los mayores niveles de rendimiento y opciones de integración criptográficas.

Una vez aprovisionados, los dispositivos HSM se conectan directamente a la red virtual de un cliente. También son accesibles mediante una aplicación local y herramientas de administración si se configura la conectividad de punto a sitio o de VPN de sitio a sitio. Los clientes obtienen el software y la documentación para configurar y administrar los dispositivos HSM desde el portal de soporte técnico al cliente de Thales.

**Motivos para usar Azure Dedicated HSM**

**Cumplimiento de la norma FIPS 140-2 nivel 3**

Muchas organizaciones se rigen por estrictas regulaciones del sector que dictan que las claves criptográficas deben almacenarse en los HSM validados conforme a FIPS 140-2 (nivel 3). Azure Dedicated HSM y una nueva oferta de inquilino único, HSM administrado por Azure Key Vault, ayudan a los clientes de diversos segmentos del sector, como el sector de los servicios financieros, las agencias gubernamentales y otros a cumplir los requisitos del nivel 3 de FIPS 140-2. El servicio Azure Key Vault multiinquilino de Microsoft usa actualmente HSM validados por la norma FIPS 140-2 nivel 2.

**Dispositivos de un único inquilino**

Muchos de nuestros clientes requieren un único inquilino en el dispositivo de almacenamiento criptográfico. El servicio Azure Dedicated HSM les permite aprovisionar un dispositivo físico desde uno de los centros de datos distribuidos globalmente de Microsoft. Una vez que se aprovisiona a un cliente, solo ese cliente puede acceder al dispositivo.

**Control administrativo completo**

Muchos clientes requieren un control administrativo completo y acceso exclusivo a su dispositivo para fines administrativos. Una vez que se aprovisiona un dispositivo, solo el cliente tiene acceso de nivel administrativo o de aplicación al mismo.

Microsoft no tiene control administrativo una vez que el cliente accede por primera vez al dispositivo, momento en el cual el cliente cambia la contraseña. A partir de ese punto, el cliente es un único inquilino verdadero con control administrativo completo y funcionalidad de administración de aplicaciones. Microsoft sí conserva el acceso a nivel de supervisión (no un rol de administrador) para la telemetría a través de la conexión de puerto serie. Este acceso abarca indicadores de hardware, como temperatura, estado del suministro eléctrico y estado del ventilador.

Si lo desea, el cliente puede deshabilitar esta supervisión necesaria pero, si lo hace, no recibirá alertas de estado proactivas de parte de Microsoft.

**Alto rendimiento**

Para este servicio, se seleccionó el dispositivo Thales por diversos motivos. Ofrece una amplia variedad de compatibilidad con algoritmos criptográficos, una variedad de sistemas operativos compatibles y una amplia compatibilidad con API. El modelo específico implementado ofrece un rendimiento excelente con 10 000 operaciones por segundo para RSA-2048. Admite 10 particiones que se pueden usar para las instancias de aplicaciones únicas. Este dispositivo es de baja latencia, alta capacidad y alto rendimiento.

**Oferta única basada en la nube**

Microsoft reconoció una necesidad concreta en un conjunto exclusivo de clientes Es el único proveedor en la nube que ofrece a los nuevos clientes un servicio HSM dedicado validado por FIPS 140-2 de nivel 3 y ofrece una extensión de integración de aplicaciones local y basada en la nube.

**¿Es Azure Dedicated HSM adecuado para usted?**

Azure Dedicated HSM es un servicio especializado que permite cumplir los requisitos únicos de un tipo específico de organización a gran escala. Como resultado, es de esperar que la mayoría de los clientes de Azure no se encuadren en el perfil de cliente que usará este servicio. Muchos descubrirán que el servicio Azure Key Vault o Azure Managed HSM es más adecuado y rentable. Para ayudarlo a decidir si es adecuado para sus requisitos, hemos identificado los siguientes criterios.

**Casos en los que está indicado**

Azure Dedicated HSM es el más adecuado para escenarios de "migración mediante lift-and-shift" que requieren un acceso directo y exclusivo a los dispositivos HSM. Algunos ejemplos son:

* Migración de aplicaciones del entorno local a Azure Virtual Machines.
* Migración de aplicaciones de Amazon AWS EC2 a máquinas virtuales que usan el servicio AWS Cloud HSM Classic (Amazon no ofrece este servicio para los nuevos clientes).
* Ejecución de un software empaquetado como Apache/Ngnix SSL Offload, Oracle TDE y ADCS en Azure Virtual Machines.

**Casos en los que no está indicado**

Azure Dedicated HSM no es idóneo para el siguiente tipo de escenario: Los servicios en la nube de Microsoft que admiten el cifrado con claves administradas por los clientes (como Azure Information Protection, Azure Disk Encryption, Azure Data Lake Storage, Azure Storage, Azure SQL Database y Clave de cliente para Office 365) no están integrados con Azure Dedicated HSM.

**Nota**

Los clientes deben tener asignado un administrador de cuentas de Microsoft y cumplir el requisito monetario de cinco millones de dólares (5M USD) u otra cantidad superior en los ingresos totales confirmados de Azure anualmente para optar a la incorporación y uso de Azure Dedicated HSM.

**Depende**

Si Azure Dedicated HSM funcionará para usted dependerá de una posible combinación compleja de requisitos y compromisos que puede o no asumir. Un ejemplo es el requisito de la certificación FIPS 140-2 nivel 3. Se trata de un requisito común, y Azure Dedicated HSM y la nueva oferta de inquilino único, HSM administrado por Azure Key Vault son actualmente las únicas opciones que lo cumplen. Si estos requisitos obligatorios no proceden, a menudo se puede elegir entre Azure Key Vault y Azure Dedicated HSM. Evalúe sus requisitos antes de tomar una decisión.

Las situaciones en las que tendrá que ponderar sus opciones incluyen las siguientes:

* Nuevo código que se ejecuta en una máquina virtual de Azure del cliente
* TDE de SQL Server en una máquina virtual de Azure
* Cifrado en el lado de cliente de Azure Storage
* SQL Server y Azure SQL Database Always Encrypted

**Configurar el acceso a Key Vault, incluidas las directivas de acceso de almacén y el control de acceso basado en roles de Azure**

El control de acceso basado en rol de Azure es un sistema de autorización basado en Azure Resource Manager que proporciona administración de acceso específico a los recursos de Azure.

Azure RBAC permite a los usuarios administrar los permisos de las claves, secretos y certificados. Proporciona un lugar para administrar todos los permisos en todos los almacenes de claves.

El modelo de Azure RBAC permite establecer permisos en diferentes niveles de ámbito: grupo de administración, suscripción, grupo de recursos o recursos individuales. RBAC de Azure para Key Vault también permite a los usuarios tener permisos independientes en claves, secretos y certificados individuales.

**Procedimientos recomendados para las asignaciones de roles de certificados, secretos y claves individuales**

Nuestra recomendación es usar un almacén por aplicación y entorno (desarrollo, preproducción y producción).

Los permisos de claves, secretos y certificados individuales solo deben usarse para escenarios concretos:

* El uso compartido de secretos individuales entre varias aplicaciones, por ejemplo, una aplicación necesita acceder a los datos de otra

**Roles integrados de Azure para operaciones del plano de datos de Key Vault**

**Nota**

*El rol Colaborador de Key Vault es solo para operaciones en el plano de administración para administrar almacenes de claves. no permite el acceso a claves, secretos y certificados.*

| **Rol integrado** | **Descripción** | **ID** |
| --- | --- | --- |
| Administrador de Key Vault | Permite realizar todas las operaciones de plano de datos en un almacén de claves y en todos los objetos que contiene, incluidos los certificados, las claves y los secretos. No permite administrar los recursos del almacén de claves ni administrar las asignaciones de roles. Solo funciona para almacenes de claves que usan el modelo de permisos "Control de acceso basado en rol de Azure". | 00482a5a-887f-4fb3-b363-3b7fe8e74483 |
| Agente de certificados de Key Vault | Permite realizar cualquier acción en los certificados de un almacén de claves, excepto administrar permisos. Solo funciona para almacenes de claves que usan el modelo de permisos "Control de acceso basado en rol de Azure". | a4417e6f-fecd-4de8-b567-7b0420556985 |
| Agente criptográfico de Key Vault | Permite realizar cualquier acción en las claves de un almacén de claves, excepto administrar permisos. Solo funciona para almacenes de claves que usan el modelo de permisos "Control de acceso basado en rol de Azure". | 14b46e9e-c2b7-41b4-b07b-48a6ebf60603 |
| Usuario de cifrado de servicio criptográfico de Key Vault | Permite leer los metadatos de las claves y realizar operaciones de encapsulado/desencapsulado. Solo funciona para almacenes de claves que usan el modelo de permisos "Control de acceso basado en rol de Azure". | e147488a-f6f5-4113-8e2d-b22465e65bf6 |
| Usuario criptográfico de Key Vault | Permite realizar operaciones criptográficas mediante claves. Solo funciona para almacenes de claves que usan el modelo de permisos "Control de acceso basado en rol de Azure". | 12338af0-0e69-4776-bea7-57ae8d297424 |
| Lector de Key Vault | Permite leer metadatos de almacenes de claves y sus certificados, claves y secretos. No se pueden leer valores confidenciales, como el contenido de los secretos o el material de las claves. Solo funciona para almacenes de claves que usan el modelo de permisos "Control de acceso basado en rol de Azure". | 21090545-7ca7-4776-b22c-e363652d74d2 |
| Responsable de secretos de Key Vault | Permite realizar cualquier acción en los secretos de un almacén de claves, excepto administrar permisos. Solo funciona para almacenes de claves que usan el modelo de permisos "Control de acceso basado en rol de Azure". | b86a8fe4-44ce-4948-aee5-eccb2c155cd7 |
| Usuario de secretos de Key Vault | Lea el contenido del secreto, incluida la parte secreta de un certificado con clave privada. Solo funciona para almacenes de claves que usan el modelo de permisos "Control de acceso basado en rol de Azure". | 4633458b-17de-408a-b874-0445c86b69e6 |

**Nota**

No hay ningún usuario de certificado de Key Vault porque las aplicaciones requieren la parte de secretos del certificado con clave privada. El rol Usuario de secretos de Key Vault debe usarse para que las aplicaciones recuperen el certificado.

**Administración de asignaciones de roles integradas del plano de datos de Key Vault (versión preliminar)**

| **Rol integrado** | **Descripción** | **ID** |
| --- | --- | --- |
| Administrador de acceso a datos de Key Vault (versión preliminar) | Administre el acceso a Azure Key Vault mediante la adición o eliminación de asignaciones de roles para el administrador de Key Vault, el oficial de certificados de Key Vault, el oficial de cifrado de Key Vault, el usuario de cifrado del servicio criptográfico de Key Vault, el usuario criptográfico de Key Vault, el lector de Key Vault, el oficial de secretos de Key Vault o los roles de usuario de secretos de Key Vault. Incluye una condición de ABAC para restringir las asignaciones de roles. | 8b54135c-b56d-4d72-a534-26097cfdc8d8 |

**Uso de los permisos de secretos, claves y certificados de Azure RBAC con Key Vault**

El nuevo modelo de permisos de Azure RBAC para el almacén de claves proporciona una alternativa al modelo de permisos de la directiva de acceso del almacén.

**Requisitos previos**

Debe tener una suscripción de Azure. Si no la tiene, puede crear una cuenta gratuita antes de empezar.

Para agregar asignaciones de roles, debe tener permisos de Microsoft.Authorization/roleAssignments/write y Microsoft.Authorization/roleAssignments/delete, como administrador de acceso a datos de Key Vault (versión preliminar), administrador de acceso de usuario o propietario.

**Administración de certificados, secretos y claves**

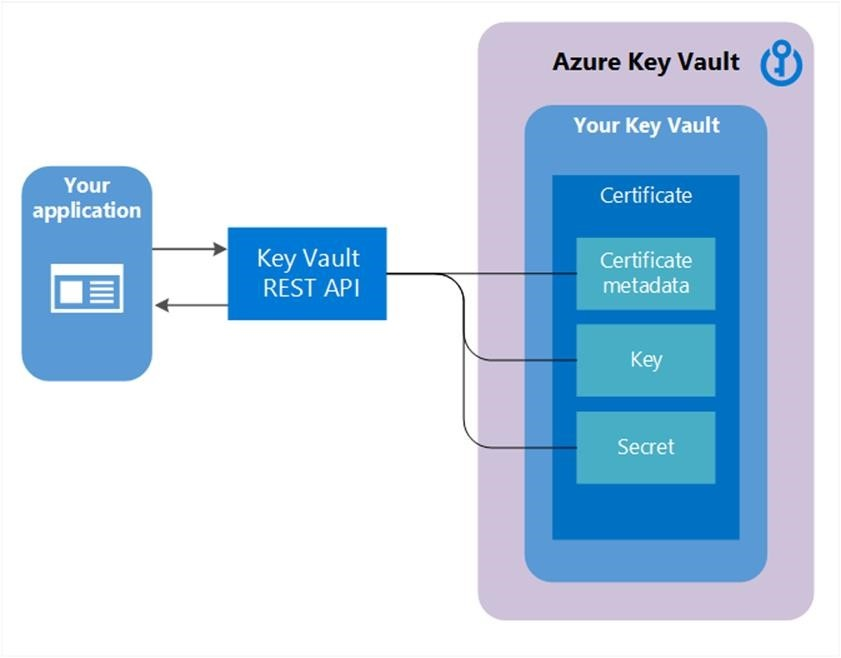
La compatibilidad con certificados de Azure Key Vault proporciona la administración de sus certificados X.509 y los comportamientos siguientes:

* Permite que el propietario de un certificado cree un certificado a través de un proceso de creación de almacén de claves o a través de la importación de un certificado existente. Los certificados importados incluyen los certificados autofirmados y los certificados generados desde una entidad de certificación (CA).
* Permite que el propietario de un certificado de Key Vault implemente un almacenamiento seguro y la administración de certificados X.509 sin interactuar con material de clave privada.
* Permite que el propietario de un certificado cree una directiva que indique a Key Vault cómo administrar el ciclo de vida de un certificado.
* Permite al propietario del certificado proporcionar información de contacto para las notificaciones sobre los eventos de ciclo de vida de expiración y renovación.
* Admite la renovación automática con emisores seleccionados: proveedores de certificados X.509 y CA asociados con Key Vault.

**Composición de un certificado**

Cuando se crea un certificado de Key Vault, se crean también una clave direccionable y un secreto con el mismo nombre. La clave de Key Vault permite operaciones de clave y el secreto de Key Vault permite recuperar el valor del certificado como secreto. Un certificado de Key Vault también contiene metadatos del certificado X.509 público.

El identificador y la versión de los certificados son similares a los de las claves y los secretos. Una versión específica de una clave direccionable y el secreto creados con la versión del certificado de Key Vault está disponible en la respuesta del certificado de Key Vault.



**Clave exportable o no exportable**

Cuando se crea un certificado de Key Vault, este se puede recuperar desde el secreto direccionable con la clave privada en formato PFX o PEM. La directiva que se utiliza para crear el certificado debe indicar que la clave es exportable. Si la directiva indica que la clave no es exportable, la clave privada no forma parte del valor cuando se recupera como un secreto.

La clave direccionable se vuelve más pertinente con los certificados de Key Vault no exportables. Las operaciones direccionables de la clave de Key Vault se asignan desde el campo uso de claves de la directiva de certificado de Key Vault que se usa para crear el certificado de Key Vault.

En la tabla siguiente se enumeran los tipos de clave admitidos.

| **Tipo de clave** | **Acerca de** | **Seguridad** |
| --- | --- | --- |
| RSA | Clave RSA protegida por software | FIPS 140-2 nivel 1 |
| RSA-HSM | Clave RSA protegida con HSM (solo SKU Premium) | HSM validados con FIPS 140-2 nivel 2 |
| EC | Clave de curva elíptica protegida con software | FIPS 140-2 nivel 1 |
| EC-HSM | Clave de curva elíptica protegida con HSM (solo SKU Premium) | HSM validados con FIPS 140-2 nivel 2 |
| oct | Clave de octeto protegida con software | FIPS 140-2 nivel 1 |

Las claves exportables solo se permiten con RSA y EC. Las claves HSM no son exportables.

**Etiquetas y atributos de certificado**

Además de los metadatos del certificado, una clave direccionable y un secreto direccionable, un certificado de Key Vault contiene atributos y etiquetas.

**Atributos**

Los atributos del certificado se reflejan en los atributos de la clave y el secreto direccionables que se crean cuando se crea el certificado de Key Vault.

Un certificado de Key Vault tiene el siguiente atributo:

* enabled: Este atributo booleano es opcional. El valor predeterminado es true. Se puede especificar para indicar si se pueden recuperar los datos del certificado como un secreto o es operativo como una clave.
  + Este atributo también se usa con nbf y exp cuando se produce una operación entre nbf y exp, pero solo si enabled está establecido en true. Las operaciones fuera de la franja entre nbf y exp se deniegan automáticamente.

Una respuesta incluye estos atributos de solo lectura adicionales:

* **created**: tipo IntDate, indica cuándo se creó esta versión del certificado.
* **updated**: tipo IntDate, indica cuándo se modificó esta versión del certificado.
* **exp**: tipo IntDate, contiene el valor de la fecha de expiración del certificado X.509.
* **nbf**: tipo intDate, contiene el valor de la fecha "no anterior" del certificado X.509.

**Nota**

*Si un certificado de Key Vault expira, todavía se puede recuperar, pero el certificado puede volverse inoperable en escenarios como la protección de seguridad de la capa de transporte donde se valida la expiración del certificado.*

**Etiquetas**

Las etiquetas de los certificados son un diccionario especificado por el cliente de pares clave y valor, similar a las etiquetas de las claves y los secretos.

**Nota**

*El autor de una llamada puede leer etiquetas si tiene la lista u obtiene permiso para ese tipo de objeto (claves, secretos o certificados).*

**Directiva de certificados**

Una directiva de certificados contiene información sobre cómo crear y administrar el ciclo de vida de un certificado de Key Vault. Cuando se importa un certificado con clave privada en Key Vault, el servicio de Key Vault crea una directiva predeterminada mediante la lectura del certificado X.509.

Cuando se crea un certificado de Key Vault desde el principio, debe proporcionarse una directiva. La directiva especifica cómo crear esta versión de certificado de Key Vault o la próxima versión de certificado de Key Vault. Tras establecerse una directiva, no se requiere en sucesivas operaciones create para futuras versiones. Solo hay una instancia de una directiva para todas las versiones de un certificado de Key Vault.

En un nivel general, una directiva de certificado contiene la siguiente información:

* Propiedades del certificado X.509, entre las que se incluyen el nombre del firmante, los nombres alternativos del firmante y otras propiedades que se usan para crear una solicitud de certificado X.509.
* Propiedades de la clave, entre las que se incluyen el tipo de clave, la longitud y los campos de exportable y ReuseKeyOnRenewal. Estos campos indican a Key Vault cómo generar una clave.
  + Estos son **los tipos de clave admitidos**: RSA, RSA-HSM, EC, EC-HSM y oct.
* Propiedades del secreto, como el tipo de contenido de un secreto direccionable para generar el valor secreto, para recuperar un certificado como un secreto.
* Acciones de vigencia para el certificado de Key Vault. Cada acción de vigencia contiene:
* Desencadenador: se especifica como días antes de la expiración o como un porcentaje del intervalo de vigencia.
* Acción: emailContacts o autoRenew.
* Tipo de validación de certificados: organización validada (Nivel de socket seguro validado por la organización) y validación extendida (Capa de socket seguro de validación extendida) para emisores DigiCert y GlobalSign.
* Parámetros sobre el emisor de certificado que se utiliza para emitir certificados X.509.
* Atributos asociados a la directiva.

**Correspondencia entre el uso de X.509 y las operaciones clave**

La tabla siguiente representa la correspondencia entre las directivas de uso de claves X.509 y las operaciones de clave efectivas de una clave creada como parte de la creación de certificados de Key Vault.

| **Marcas de uso de claves X.509** | **Operaciones clave de Key Vault** | **Comportamiento predeterminado** |
| --- | --- | --- |
| DataEncipherment | cifrar, descifrar | No aplicable |
| DecipherOnly | decrypt | No aplicable |
| DigitalSignature | firmar, verificar | Valor predeterminado de Key Vault sin una especificación de uso en el momento de creación del certificado |
| EncipherOnly | encrypt | No aplicable |
| KeyCertSign | firmar, verificar | No aplicable |
| KeyEncipherment | encapsular clave, desencapsular clave | Valor predeterminado de Key Vault sin una especificación de uso en el momento de creación del certificado |
| NonRepudiation | firmar, verificar | No aplicable |
| crlsign | firmar, verificar | No aplicable |

**Emisor de certificado**

Un objeto de certificado de Key Vault contiene una configuración que se usa para comunicarse con un proveedor de emisor de certificado seleccionado para solicitar certificados X.509.

Key Vault se asocia con los siguientes proveedores de emisores de certificados para certificados de seguridad de la capa de transporte o capa de sockets seguros.

Expandir tabla

| **Nombre del proveedor** | **Ubicaciones** |
| --- | --- |
| DigiCert | Compatible con todas las ubicaciones del servicio de Key Vault en la nube pública y Azure Government |
| GlobalSign | Compatible con todas las ubicaciones del servicio de Key Vault en la nube pública y Azure Government |

Para poder crear un emisor de certificado en un almacén de claves, un administrador debe seguir estos pasos de requisitos previos:

1. Incorporar la organización con al menos un proveedor de entidad de certificación.
2. Cree credenciales del solicitante para que Key Vault inscriba (y renueve) certificados de capa de transporte/Capa de sockets seguros. Este paso proporciona la configuración para crear un objeto de emisor del proveedor en el almacén de claves.

Para obtener más información acerca de cómo crear objetos de emisor desde el portal de certificados, consulte el blog del equipo de Key Vault.

Key Vault permite la creación de varios objetos de emisor con diferentes configuraciones del proveedor de emisor. Tras crear un objeto de emisor, se puede hacer referencia a su nombre en una o varias directivas de certificado. Al hacer referencia al objeto de emisor se indica a Key Vault que utilice la configuración de acuerdo con lo especificado en el objeto de emisor al solicitar el certificado X.509 al proveedor de la entidad de certificación durante la creación y la renovación de certificados.

Los objetos de emisor se crean en el almacén. Solo se pueden usar con certificados de Key Vault en el mismo almacén.

**Contactos de certificados**

Los contactos de certificados contienen información de contacto para enviar notificaciones desencadenadas por los eventos de vigencia del certificado. Todos los certificados del almacén de claves comparten la información de contacto.

Se envía una notificación a todos los contactos especificados para un evento de cualquier certificado del almacén de claves.

**Control de acceso a certificados**

Key Vault administra el control de acceso para los certificados. El almacén de claves que contiene esos certificados proporciona el control de acceso. La directiva de control de acceso para los certificados es distinta de las directivas de control de acceso para las claves y los secretos en el mismo almacén de claves.

Los usuarios pueden crear uno o varios almacenes para almacenar los certificados, para mantener la segmentación adecuada del escenario y la administración de los certificados.

**Casos de uso de certificados**

**Comunicación y autenticación seguras**

Los certificados de seguridad de la capa de transporte pueden ayudar a cifrar las comunicaciones a través de Internet y establecer la identidad de los sitios web. Este cifrado hace que el punto de entrada y el modo de comunicación sean más seguros. Además, un certificado encadenado firmado por una entidad de certificación pública puede ayudar a comprobar que las entidades que tienen los certificados son legítimas.

Por ejemplo, estos son algunos casos de uso del uso de certificados para proteger la comunicación y habilitar la autenticación:

* **Sitios web de Intranet o Internet**: Proteja el acceso a su sitio de intranet y garantice la transferencia cifrada de datos a través de Internet mediante certificados de seguridad de la capa de transporte.
* **Dispositivos IoT y de red**: proteja los dispositivos mediante certificados para la autenticación y la comunicación.
* **Nube o multinube**: proteja las aplicaciones basadas en la nube localmente, entre nubes o en el inquilino del proveedor de nube.

**Firma de código**

Un certificado puede ayudar a proteger el código o script de software para garantizar que el autor pueda compartir el software a través de Internet sin interferencias por parte de entidades malintencionadas. Una vez que el autor firma el código mediante un certificado y aprovechando la tecnología de firma de código, el software se marca con un sello de autenticación que muestra el autor y su sitio web. El certificado usado en la firma de código ayuda a validar la autenticidad del software, lo que refuerza la seguridad de un extremo a otro.

**Configuración de la rotación de claves**

La rotación automática de claves en Key Vault permite a los usuarios configurar Key Vault para generar automáticamente una nueva versión de clave con una frecuencia especificada. Para configurar la rotación, puede usar la directiva de rotación de claves, que se puede definir en cada clave individual.

La recomendación es girar las claves de cifrado al menos cada dos años para cumplir con los procedimientos recomendados criptográficos.

**Integración con servicios de Azure**

Esta característica permite el giro de cero toque de un extremo a otro para el cifrado en reposo para los servicios de Azure con la clave administrada por el cliente (CMK) almacenada en Azure Key Vault. Consulte la documentación específica del servicio de Azure para ver si el servicio cubre el giro de un extremo a otro.

**Precios**

Hay un coste adicional por rotación de claves programada.

**Permisos necesarios**

Para la característica de giro de claves de Key Vault se necesitan permisos de administración de claves. Puede asignar un rol de "Responsable de cifrado de Key Vault" para administrar la directiva de rotación y la rotación a petición.

**Directiva de giro de claves**

La directiva de rotación de claves permite a los usuarios configurar la rotación y las notificaciones de Event Grid a punto de expirar.

Configuración de directiva de giro de claves:

* Hora de expiración: intervalo de expiración de clave. Se usa para establecer la fecha de expiración en la clave rotada recientemente. No afecta a una clave actual.
* Habilitado/deshabilitado: marca para habilitar o deshabilitar el giro de la clave
* Tipos de rotación:
  + Renovación automática en un momento determinado después de la creación (predeterminado)
  + Renovación automática en un momento determinado antes de la expiración. Es necesario establecer "Hora de expiración" en la directiva de giro y "Fecha de expiración" en la clave.
* Tiempo de rotación: intervalo de rotación de la clave. El valor mínimo es siete días desde la creación y siete días desde la fecha de expiración
* Hora de notificación: clave cercana al intervalo del evento de expiración para la notificación de Event Grid. Es necesario establecer "Hora de expiración" en la directiva de giro y "Fecha de expiración" en la clave.

**Configuración de la directiva de giro de claves**

Configure la directiva de giro de claves durante la creación de claves.

**Configuración de la clave cerca de la notificación de expiración**

Configuración de la notificación de expiración para la clave cercana al evento de expiración de Event Grid. En caso de que no se pueda usar la rotación automatizada, como cuando se importa una clave desde HSM local, puede configurar una notificación de expiración cercana como recordatorio para la rotación manual o como un desencadenador para la rotación automatizada personalizada a través de la integración con Event Grid. Puede configurar la notificación con días, meses y años antes de la expiración para que se desencadene un evento de expiración cercana.

**Configuración de la gobernanza de directiva de giro de claves**

Con el servicio Azure Policy, puede controlar el ciclo de vida de la clave y asegurarse de que todas las claves están configuradas para girar dentro de un número especificado de días.

**Creación y asignación de una definición de directiva**

1. Vaya al recurso de la directiva.
2. Seleccione **Asignaciones** en **Creación** en el lado izquierdo de la página de Azure Policy.
3. Seleccione **Asignar directiva** en la parte superior de la página. Este botón abre la página de asignación de la directiva.
4. Escribe la siguiente información:
   * Defina el ámbito de la directiva eligiendo la suscripción y el grupo de recursos en el que se aplicará la directiva. Seleccione haciendo clic en el botón de tres puntos en el campo **Ámbito**.
   * Seleccione el nombre de la definición de directiva: "Las claves deben tener una directiva de rotación para asegurarse de que la rotación esté programada en el número especificado de días después de la creación. "
   * Vaya a la pestaña **Parámetros** en la parte superior de la página.
     + Establezca **el número máximo de días para rotar** el parámetro al número deseado de días, por ejemplo, 730.
     + Defina el efecto deseado de la directiva (Auditoría o Deshabilitado).
5. Rellene los campos adicionales. Navegue por las pestañas haciendo clic en los botones **Anterior** y **Siguiente** en la parte inferior de la página.
6. Seleccione **Revisar + crear**.
7. Seleccione **Crear**.

Una vez asignada la directiva integrada, puede tardar hasta 24 horas en completar el examen. Después de completar el examen, puede ver los resultados de cumplimiento tal como se muestra a continuación.

**Configurar la copia de seguridad y recuperación de certificados, secretos y claves**

Azure Key Vault proporciona automáticamente características para ayudarle a mantener la disponibilidad y evitar la pérdida de datos. Haga una copia de seguridad de los secretos solo si tiene una justificación empresarial crítica. La copia de seguridad de los secretos del almacén de claves puede plantear desafíos operativos adicionales, como el mantenimiento de varios conjuntos de registros, permisos y copias de seguridad cuando los secretos expiren o roten.

Key Vault mantiene la disponibilidad en escenarios de desastre y realizará automáticamente una conmutación por error de las solicitudes a una región emparejada sin intervención del usuario.

Si desea protección contra la eliminación accidental o malintencionada de los secretos, configure las características de eliminación temporal y protección de purga en el almacén de claves.

Key Vault no proporciona actualmente una forma de realizar una copia de seguridad de un almacén de claves completo en una sola operación. Cualquier intento de usar los comandos enumerados en este documento para realizar una copia de seguridad automatizada de un almacén de claves puede producir errores y no será admitida por Microsoft ni el equipo de Azure Key Vault.

Tenga en cuenta también las consecuencias siguientes:

* La copia de seguridad de secretos que tienen varias versiones podría producir errores de expiración del tiempo de espera.
* Una copia de seguridad crea una instantánea a un momento dado. Los secretos pueden renovarse durante una copia de seguridad, lo que provoca una falta de coincidencia de las claves de cifrado.
* Si se superan los límites de servicio de Key Vault en cuanto a solicitudes por segundo, el almacén de claves se limitará y se producirá un error en la copia de seguridad.

**Consideraciones de diseño**

Al realizar una copia de seguridad de un objeto almacenado en el almacén de claves (secreto, clave o certificado), la operación de copia de seguridad descargará el objeto como un blob cifrado. Este blob no se puede descifrar fuera de Azure. Para obtener datos que se puedan usar de este blob, debe restaurar el blob en un almacén de claves dentro de la misma suscripción de Azure y zona geográfica de Azure.

**Requisitos previos**

Para realizar una copia de seguridad de un objeto de Key Vault, debe tener:

* Permisos de nivel de colaborador o superior en una suscripción de Azure.
* Un almacén de claves principal que contenga los secretos de los que desea realizar una copia de seguridad.
* Un almacén de claves secundario en el que se restaurarán los secretos.

**Copia de seguridad y restauración desde Azure Portal**

Siga los pasos de esta sección para realizar copias de seguridad y restaurar objetos mediante Azure Portal.

**Copia de seguridad**

1. Vaya a Azure Portal.
2. Seleccione el almacén de claves.
3. Vaya al objeto (secreto, clave o certificado) del que desea realizar una copia de seguridad.
4. Seleccione el objeto.
5. Seleccione **Descargar copia de seguridad**.
6. Seleccione **Descargar**.
7. Almacene el blob cifrado en una ubicación segura.

**Restauración**

1. Vaya a Azure Portal.
2. Seleccione el almacén de claves.
3. Desplácese hasta el tipo de objeto (secreto, clave o certificado) que desea restaurar.
4. Seleccione **Restaurar copia de seguridad**.
5. Vaya a la ubicación donde almacenó el blob cifrado.
6. Seleccione **Aceptar**.

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. Una empresa quiere automatizar la creación y desmontaje de entornos para ofrecer plataformas de hospedaje de aplicaciones seguras y estables. ¿Cuál de las siguientes opciones lo permite?**

1. EncipherOnly
2. KeyCertSign
3. KeyEncipherment

**2. Una empresa quiere garantizar la protección contra la eliminación accidental o malintencionada de sus secretos. ¿Qué característica debe configurar en su almacén de claves?**

1. Configuración de características de eliminación temporal y protección de purga en sus secretos
2. Copia de seguridad de todos los secretos en el almacén de claves
3. Configuración de características de eliminación temporal y protección de purga en su almacén de claves

**3. Una empresa quiere asegurarse de que solo se pueden realizar cambios aprobados en su entorno para mantener el cumplimiento. ¿Qué artefacto se puede incluir en una definición de plano técnico para lograrlo?**

1. Jerarquía de recursos
2. Plantilla del Administrador de recursos de Azure
3. Asignación de directiva

**4. Una empresa quiere habilitar la automatización y validación de la creación y desmontaje de entornos para ayudar a ofrecer plataformas de hospedaje de aplicaciones seguras y estables. ¿Qué servicio de Azure se puede usar para este propósito?**

1. Azure Cosmos DB
2. Azure Functions
3. Azure DevTest Labs

**5. Una empresa quiere asegurarse de que sus plataformas de hospedaje de aplicaciones sean seguras y estables. ¿Qué permite la automatización y validación de la creación y desmontaje de entornos para ayudar a ofrecer esto?**

1. Un firewall
2. Un software antivirus
3. Una directiva integrada
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, aprendió a planear, implementar y administrar la gobernanza para la seguridad en Azure, incluyendo la creación e interpretación de directivas de seguridad con Azure Policy, establecer la configuración de seguridad mediante Azure Blueprint, la implementación de infraestructuras seguras mediante una zona de aterrizaje, la administración de claves criptográficas de forma segura con Azure Key Vault, proporcionando recomendaciones para el uso del módulo de seguridad de hardware (HSM) dedicado, la configuración del control de acceso mediante directivas de acceso del almacén y Azure RBAC, la administración de certificados, secretos y claves, así como la configuración de medidas de rotación, copia de seguridad y recuperación de claves para mejorar la seguridad y el cumplimiento.