**Introducción**

Completado100 XP

* 1 minuto

En este módulo se proporciona información sobre algunas de las herramientas de seguridad que pueden ayudar a proteger la infraestructura y los datos al trabajar en la nube.

Seguridad es una palabra pequeña para un concepto de gran importancia. Hay muchísimos factores que se deben tener en cuenta a la hora de proteger las aplicaciones y los datos. ¿Cómo ayuda Azure a proteger las cargas de trabajo que ejecuta en la nube y en el centro de datos local?

**Tailwind Traders**

[Tailwind Traders](https://www.tailwindtraders.com/) es una empresa ficticia que distribuye productos para la remodelación del hogar. Esta empresa cuenta con ferreterías minoristas en todo el mundo y en línea.



Tailwind Traders está especializada en precios competitivos, envío rápido y una amplia gama de artículos. Va a examinar las tecnologías en la nube para mejorar las operaciones comerciales y apoyar el crecimiento en nuevos mercados. Al migrar a la nube, la empresa tiene previsto mejorar su experiencia de compra para diferenciarse de sus competidores.

**¿Cómo ejecuta Tailwind Traders de forma segura en la nube y en el centro de datos?**

Tailwind Traders ejecuta una combinación de cargas de trabajo en Azure y en su centro de datos.

La empresa tiene que garantizar que todos sus sistemas cumplen un nivel mínimo de seguridad y que su información está protegida frente a ataques. También necesita una manera de recopilar eventos de seguridad de su patrimonio digital y de tomar medidas conforme a ellos.

Ahora se verá cómo puede Tailwind Traders usar algunas de las herramientas y características de Azure como parte de su estrategia de seguridad general.

**Objetivos de aprendizaje**

Después de completar este módulo, podrá:

* Fortalecer el nivel de seguridad y proteger frente a amenazas mediante Azure Security Center.
* Recopilar datos de seguridad de muchos orígenes diferentes mediante Azure Sentinel y tomar medidas conforme a ellos.
* Almacenar y acceder a información confidencial, como contraseñas y claves de cifrado, de forma segura en Azure Key Vault.
* Administrar servidores físicos dedicados para hospedar máquinas virtuales de Azure para Windows y Linux mediante Azure Dedicated Host.

**Requisitos previos**

* Debe estar familiarizado con la terminología y los conceptos básicos relacionados con la informática.
* Es útil estar familiarizado con la informática en la nube, pero no es necesario.

**Introducción**

Completado100 XP

* 1 minuto

En este módulo se proporciona información sobre algunas de las herramientas de seguridad que pueden ayudar a proteger la infraestructura y los datos al trabajar en la nube.

Seguridad es una palabra pequeña para un concepto de gran importancia. Hay muchísimos factores que se deben tener en cuenta a la hora de proteger las aplicaciones y los datos. ¿Cómo ayuda Azure a proteger las cargas de trabajo que ejecuta en la nube y en el centro de datos local?

**Tailwind Traders**

[Tailwind Traders](https://www.tailwindtraders.com/) es una empresa ficticia que distribuye productos para la remodelación del hogar. Esta empresa cuenta con ferreterías minoristas en todo el mundo y en línea.



Tailwind Traders está especializada en precios competitivos, envío rápido y una amplia gama de artículos. Va a examinar las tecnologías en la nube para mejorar las operaciones comerciales y apoyar el crecimiento en nuevos mercados. Al migrar a la nube, la empresa tiene previsto mejorar su experiencia de compra para diferenciarse de sus competidores.

**¿Cómo ejecuta Tailwind Traders de forma segura en la nube y en el centro de datos?**

Tailwind Traders ejecuta una combinación de cargas de trabajo en Azure y en su centro de datos.

La empresa tiene que garantizar que todos sus sistemas cumplen un nivel mínimo de seguridad y que su información está protegida frente a ataques. También necesita una manera de recopilar eventos de seguridad de su patrimonio digital y de tomar medidas conforme a ellos.

Ahora se verá cómo puede Tailwind Traders usar algunas de las herramientas y características de Azure como parte de su estrategia de seguridad general.

**Objetivos de aprendizaje**

Después de completar este módulo, podrá:

* Fortalecer el nivel de seguridad y proteger frente a amenazas mediante Azure Security Center.
* Recopilar datos de seguridad de muchos orígenes diferentes mediante Azure Sentinel y tomar medidas conforme a ellos.
* Almacenar y acceder a información confidencial, como contraseñas y claves de cifrado, de forma segura en Azure Key Vault.
* servidores físicos dedicados para hospedar máquinas virtuales de Azure para Windows y Linux mediante Azure Dedicated Host.

**Requisitos previos**

* Debe estar familiarizado con la terminología y los conceptos básicos relacionados con la informática.
* Es útil estar familiarizado con la informática en la nube, pero no es necesario.

# Protección frente a amenazas de seguridad mediante Azure Security Center

Completado100 XP

* 6 minutos

Tailwind Traders va a ampliar su uso de servicios de Azure. Todavía tiene cargas de trabajo en el entorno local con procedimientos recomendados actuales de configuración relacionados con la seguridad y procedimientos empresariales. ¿Cómo garantiza la empresa que todos sus sistemas cumplen un nivel mínimo de seguridad y que su información está protegida frente a ataques?

Muchos servicios de Azure incluyen características de seguridad integradas. Las herramientas de Azure también pueden ayudar a Tailwind Traders con este requisito. Vamos a empezar por examinar Azure Security Center.

## ¿Qué es Azure Security Center?

[Azure Security Center](https://azure.microsoft.com/services/security-center) es un servicio de supervisión que proporciona visibilidad del nivel de seguridad en todos los servicios, tanto en Azure como en el entorno local. El término nivel de seguridad se refiere a las directivas y a los controles de ciberseguridad, así como a la predicción, la prevención y la respuesta a las amenazas de seguridad.

Security Center puede:

* Supervisar la configuración de seguridad en las cargas de trabajo locales y en la nube.
* Aplicar automáticamente la configuración de seguridad necesaria a los nuevos recursos a medida que se publican en línea.
* Proporcionar recomendaciones de seguridad basadas en las configuraciones, los recursos y las redes actuales.
* Supervisar de forma continua los recursos y realizar valoraciones de seguridad automáticas para identificar posibles vulnerabilidades antes de que alguien las aproveche.
* Usar el aprendizaje automático para detectar y bloquear la instalación de malware en las máquinas virtuales (VM) y otros recursos. También puede usar controles de aplicaciones adaptables para definir reglas que indiquen las aplicaciones permitidas a fin de garantizar que solo se puedan ejecutar las aplicaciones permitidas.
* Detectar y analizar posibles ataques entrantes e investigar amenazas y otras actividades posteriores a una brecha que pudieran haberse producido.
* Proporcionar control de acceso Just-in-Time a los puertos de red. Esto reduce la superficie expuesta a ataques al garantizar que la red solo permite el tráfico necesario en el momento en que se necesita.

En este breve vídeo se explica cómo Security Center puede ayudar a proteger las redes, proteger y supervisar los recursos en la nube, y mejorar la posición de seguridad general.

## Reconocimiento del nivel de seguridad

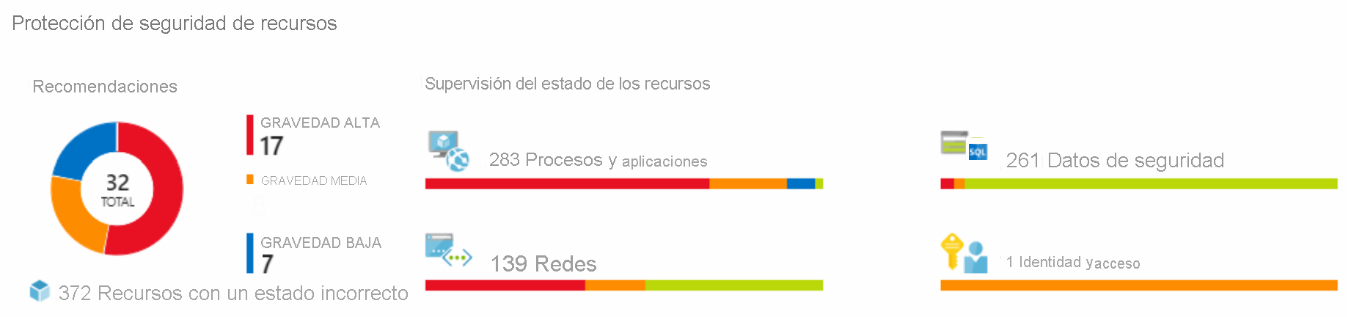
Tailwind Traders puede usar Security Center para obtener un análisis detallado de los distintos componentes de su entorno. Como los recursos de la empresa se analizan con respecto a los controles de seguridad de cualquier directiva de gobernanza que haya asignado, puede ver su cumplimiento normativo general desde una perspectiva de seguridad desde una sola ubicación.

Consulte el siguiente ejemplo de lo que se podría ver en Azure Security Center.



Imagine que Tailwind Traders debe cumplir el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS). En este informe se muestra que la empresa tiene recursos que debe corregir.

En la sección **Protección de seguridad de recursos**, Tailwind Traders puede ver el estado de sus recursos desde una perspectiva de seguridad. Para facilitar la clasificación por orden de prioridad de las acciones correctivas, las recomendaciones se clasifican como de gravedad baja, media y alta. A continuación se muestra un ejemplo.

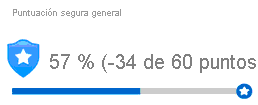


### ¿Qué es la puntuación de seguridad?

La [puntuación de seguridad](https://docs.microsoft.com/es-ES/azure/security-center/secure-score-security-controls/) es una medida del nivel de seguridad de una organización.

La puntuación de seguridad se basa en controles de seguridad, o en grupos de recomendaciones de seguridad relacionadas. La puntuación se basa en el porcentaje de controles de seguridad que se satisfacen. Cuantos más controles de seguridad se satisfacen, mayor es la puntuación que se recibe. La puntuación mejora cuando se corrigen todas las recomendaciones de un único recurso dentro de un control.

Este es un ejemplo de Azure Portal en el que se muestra una puntuación del 57 por ciento, o 34 de 60 puntos.



El seguimiento de las recomendaciones de la puntuación de seguridad ayuda a proteger a la organización frente a amenazas. Desde un panel centralizado de Azure Security Center, las organizaciones pueden supervisar la seguridad de sus recursos de Azure, como identidades, datos, aplicaciones, dispositivos e infraestructura, y trabajar en ella.

La puntuación de seguridad ayuda a:

* Notificar el estado actual del nivel de seguridad de la organización.
* Mejorar el nivel de seguridad al proporcionar detectabilidad, visibilidad, orientación y control.
* Comparar con los puntos de referencia y establecer indicadores clave de rendimiento (KPI).

## Protección frente a amenazas

Security Center incluye funciones avanzadas de defensa en la nube para máquinas virtuales, seguridad de red e integridad de archivos. Ahora se verá cómo se aplican algunas de estas funciones a Tailwind Traders.

* **Acceso Just-in-Time** Tailwind Traders configurará el acceso Just-in-Time a las máquinas virtuales. Este acceso bloquea el tráfico de forma predeterminada en puertos de red específicos de máquinas virtuales, pero permite el tráfico durante un tiempo especificado cuando un administrador lo solicita y lo aprueba.
* **Controles de aplicaciones adaptables** Tailwind Traders puede controlar qué aplicaciones se pueden ejecutar en sus máquinas virtuales. En segundo plano, Security Center usa aprendizaje automático para examinar los procesos que se ejecutan en una máquina virtual. Crea reglas de excepción para cada grupo de recursos que contiene las máquinas virtuales y proporciona recomendaciones. Este proceso proporciona alertas que notifican a la empresa si hay aplicaciones no autorizadas en ejecución en sus máquinas virtuales.
* **Protección de red adaptable** Security Center puede supervisar los patrones de tráfico de Internet de las máquinas virtuales y compararlos con la configuración actual de los grupos de seguridad de red (NSG) de la empresa. A partir de ahí, Security Center puede hacer recomendaciones sobre si los NSG deben bloquearse más y proporcionar pasos de corrección.
* **Supervisión de la integridad de los archivos** Tailwind Traders también puede configurar la supervisión de los cambios en archivos importantes tanto en Windows como en Linux, la configuración del registro, las aplicaciones y otros aspectos que podrían indicar un ataque de seguridad.

## Responder a alertas de seguridad

Tailwind Traders puede usar Security Center para obtener una vista centralizada de todas sus alertas de seguridad. Desde ahí, la empresa puede descartar las alertas falsas, investigarlas más, corregir una alerta de forma manual, o bien usar una respuesta automatizada con una automatización de flujo de trabajo.

La automatización de flujo de trabajo usa conectores de Azure Logic Apps y Security Center. La aplicación lógica se puede desencadenar mediante una alerta de detección de amenazas o una recomendación de Security Center, filtrada por nombre o por gravedad. Luego, se puede configurar para que ejecute una acción, como enviar un correo electrónico o publicar un mensaje en un canal de Microsoft Teams.

**Detección de amenazas de seguridad y respuesta a ellas mediante Azure Sentinel**

Completado100 XP

* 4 minutos

La administración de la seguridad a gran escala puede beneficiarse de un sistema de administración de eventos e información de seguridad (SIEM) dedicado. Un sistema SIEM agrega datos de seguridad de muchos orígenes diferentes (siempre y cuando esos orígenes admitan un formato de registro de estándar abierto). También proporciona funciones para la detección de amenazas y la respuesta a ellas.

[Azure Sentinel](https://azure.microsoft.com/services/azure-sentinel/) es el sistema SIEM basado en la nube de Microsoft. Usa análisis de seguridad inteligente y análisis de amenazas.

**Capacidades de Azure Sentinel**

Azure Sentinel permite:

* **Recopilación de datos en la nube a gran escala** Recopile datos de todos los usuarios, dispositivos, aplicaciones e infraestructura, tanto locales como de varias nubes.
* **Detección de amenazas no detectadas anteriormente** Minimice los falsos positivos mediante el análisis y la inteligencia sobre amenazas completos de Microsoft.
* **Investigación de amenazas con inteligencia artificial** Examine actividades sospechosas a gran escala y saque provecho de los años de experiencia en el campo de la ciberseguridad de Microsoft.
* **Respuesta rápida a los incidentes** Use la orquestación y la automatización de tareas comunes integradas.

**Conexión de los orígenes de datos**

Tailwind Traders decide explorar las capacidades de Azure Sentinel. En primer lugar, la empresa identifica y conecta sus orígenes de datos.

Azure Sentinel admite una serie de orígenes de datos que puede analizar en busca de eventos de seguridad. Estas conexiones las administran conectores integrados o API y formatos de registro estándar del sector.

* **Conexión de soluciones de Microsoft** Los conectores proporcionan integración en tiempo real para servicios como las soluciones de Protección contra amenazas de Microsoft, orígenes de Microsoft 365 (incluido Office 365), Azure Active Directory y Firewall de Windows Defender.
* **Conexión de otros servicios y soluciones** Hay conectores disponibles para servicios y soluciones comunes que no son de Microsoft, incluidos AWS CloudTrail, Citrix Analytics (Security), Sophos XG Firewall, VMware Carbon Black Cloud y Okta SSO.
* **Conexión de orígenes de datos estándar del sector** Azure Sentinel admite datos de otros orígenes que usan el estándar de mensajería Formato de evento común (CEF), Syslog o la API REST.

**Detectar amenazas**

Tailwind Traders debe recibir notificaciones de cualquier actividad sospechosa. Decide usar tanto análisis integrados como reglas personalizadas para detectar las amenazas.

Los **análisis integrados** usan plantillas diseñadas por el equipo de expertos y analistas de seguridad de Microsoft que se basan en amenazas conocidas, vectores de ataque comunes y cadenas de escalado de actividades sospechosas. Estas plantillas se pueden personalizar y buscan cualquier actividad que parezca sospechosa en el entorno. En algunas plantillas se usan análisis de comportamiento de aprendizaje automático que se basan en algoritmos propiedad de Microsoft.

Los **análisis personalizados** son reglas que se crean para buscar criterios concretos en el entorno. Se puede obtener una vista previa del número de resultados que generaría la consulta (en función de eventos de registro pasados) y establecer una programación para que se ejecute la consulta. También se puede establecer un umbral de alerta.

**Investigación y respuesta**

Cuando Azure Sentinel detecta eventos sospechosos, Tailwind Traders puede investigar alertas o *incidentes* (un grupo de alertas relacionadas) concretos. Con el grafo de investigación, la empresa puede revisar información de entidades directamente conectadas a la alerta y ver consultas de exploración comunes para ayudar a guiar la investigación.

Este es un ejemplo en el que se muestra el aspecto de un grafo de investigación en Azure Sentinel.

Diagram

Description automatically generated with medium confidence

La empresa también usará [Libros de Azure Monitor](https://docs.microsoft.com/es-ES/azure/azure-monitor/platform/workbooks-overview/) para automatizar las respuestas a las amenazas. Por ejemplo, puede establecer una alerta que busque direcciones IP malintencionadas que accedan a la red y crear un libro que siga estos pasos:

1. Cuando se desencadene la alerta, abrir una incidencia en el sistema de incidencias de TI.
2. Enviar un mensaje al canal de operaciones de seguridad de Microsoft Teams o Slack para asegurarse de que los analistas de seguridad conocen el incidente.
3. Enviar toda la información de la alerta al administrador de red sénior y al administrador de seguridad. El mensaje de correo electrónico incluye dos botones de opción de usuario: **Bloquear** u **Omitir**.

Cuando un administrador selecciona **Bloquear**, la dirección IP se bloquea en el firewall y el usuario se deshabilita en Azure Active Directory. Cuando un administrador selecciona **Omitir**, la alerta se cierra en Azure Sentinel y el incidente se cierra en el sistema de incidencias de TI.

El libro se sigue ejecutando después de recibir una respuesta de los administradores.

Los libros se pueden ejecutar manual o automáticamente cuando una regla desencadena una alerta.

**Almacenamiento y administración de secretos mediante Azure Key Vault**

Completado100 XP

* 3 minutos

A medida que Tailwind Traders compila sus cargas de trabajo en la nube, debe controlar con cuidado la información confidencial, como contraseñas, claves de cifrado y certificados. Esta información debe estar disponible para que una aplicación funcione, pero podría permitir que un usuario no autorizado accediera a los datos de la aplicación.

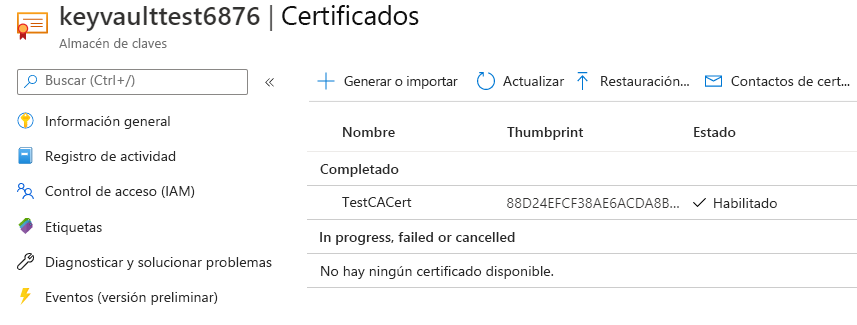
[Azure Key Vault](https://azure.microsoft.com/services/key-vault) es un servicio en la nube centralizado para almacenar los secretos de la aplicación en una única ubicación central. Proporciona un acceso seguro a la información confidencial mediante capacidades de control de acceso y registro.

**¿Qué puede hacer Azure Key Vault?**

Azure Key Vault puede ayudar a:

* **Administración de secretos** Puede usar Key Vault para almacenar de forma segura y controlar exhaustivamente el acceso a tokens, contraseñas, certificados, claves de API y otros secretos.
* **Administración de claves de cifrado** Puede usar Key Vault como solución de administración de claves. Key Vault facilita la creación y el control de las claves de cifrado que se emplean para cifrar los datos.
* **Administración de certificados SSL/TLS** Key Vault permite aprovisionar, administrar e implementar los certificados públicos y privados de Capa de sockets seguros/Seguridad de la capa de transporte (SSL/TLS) de los recursos de Azure y los recursos internos.
* **Almacenamiento de secretos basado en módulos de seguridad de hardware(HSMs)** Estas claves y secretos se pueden proteger mediante software o con dispositivos HSM validados por FIPS 140-2 de nivel 2.

Este es un ejemplo donde se muestra un certificado que se usa para realizar pruebas en Key Vault.



Más adelante en este módulo se agrega un secreto a Key Vault.

**¿Cuáles son las ventajas de Azure Key Vault?**

Las ventajas del uso de Key Vault incluyen:

* **Secretos de aplicación centralizados** La centralización del almacenamiento de los secretos de la aplicación permite controlar su distribución y reduce las posibilidades de que se filtren accidentalmente.
* **Almacenamiento seguro de secretos y claves** Azure usa algoritmos estándar del sector, longitudes de clave y HSM. El acceso a Key Vault requiere una autenticación y autorización adecuadas.
* **Supervisión y control del acceso** Con Key Vault, puede supervisar y controlar el acceso a los secretos de la aplicación.
* **Administración simplificada de sectores de aplicación** Key Vault facilita la inscripción y la renovación de certificados de entidades de certificación (CA) públicas. También puede escalar verticalmente y replicar contenido dentro de las regiones y usar herramientas de administración de certificados estándar.
* **Integración con otros servicios de Azure** Puede integrar Key Vault con cuentas de almacenamiento, registros de contenedor, centros de eventos y muchos más servicios de Azure. Después, estos servicios pueden hacer referencia de forma segura a los secretos almacenados en Key Vault.

**Ejercicio: Administración de una contraseña en Azure Key Vault**

Completado100 XP

* 5 minutos

Este módulo requiere un espacio aislado para completarse.

Un [**espacio aislado**](https://docs.microsoft.com/en-us/learn/support/faq?pivots=sandbox) le da acceso a recursos gratuitos. No se le cobrará en su suscripción personal. El espacio aislado solo podrá usarse para completar el aprendizaje en Microsoft Learn. El uso para cualquier otro motivo está prohibido y podría generar la pérdida permanente del acceso al espacio aislado.

Microsoft ofrece esta experiencia de laboratorio y el contenido relacionado con fines educativos. Toda la información presentada es propiedad de Microsoft y está destinada únicamente a brindar información sobre los productos y servicios abordados en este módulo de Microsoft Learn.

Activar espacio aislado

En este ejercicio se agrega una contraseña a Azure Key Vault. Una contraseña es un ejemplo de información confidencial que se debe proteger. Luego se lee la contraseña desde Azure Key Vault para comprobar que es accesible.

En la práctica, hay varias maneras de agregar secretos y de leer secretos en Key Vault. Puede usar Azure Portal, la CLI de Azure o Azure PowerShell. Mediante el lenguaje de programación que prefiera, las aplicaciones también pueden acceder de forma segura a los secretos que necesiten.

En este caso se crea un secreto en Key Vault mediante Azure Portal. Luego se accede al secreto desde el portal y desde la CLI de Azure en Azure Cloud Shell.

La CLI de Azure es una manera de trabajar con recursos de Azure desde la línea de comandos o desde scripts. Cloud Shell es una experiencia de shell basada en el explorador para administrar y desarrollar recursos de Azure. Piense en Cloud Shell como una consola interactiva que se ejecuta en la nube.

**Creación de un Almacén de claves**

1. Vaya a [Azure Portal](https://portal.azure.com/learn.docs.microsoft.com).
2. En el menú de Azure Portal o la página **Inicio**, en **Servicios de Azure**, seleccione **Crear un recurso**. Aparecerá el panel **Crear un recurso**.
3. En la barra de búsqueda, escriba *Almacén de claves* y, después, seleccione **Almacén de claves** en los resultados. Aparecerá el panel **Almacén de claves**.
4. Seleccione **Crear**. Aparece el panel **Crear un almacén de claves**.
5. En la pestaña **Aspectos básicos**, escriba los valores siguientes para cada opción.

**Nota**

Reemplace *NNN* por una serie de números. Esto ayuda a garantizar que el nombre del almacén de claves sea único.

**Configuración**

**Valor**

**Detalles del proyecto**

Suscripción

**Suscripción de Concierge**

Grupo de recursos

**[nombre del grupo de recursos del espacio aislado]**

**Detalles de instancia**

Nombre del almacén de claves

**my-keyvault-NNN**, donde NNN es un identificador único

Acepte las opciones restantes con sus valores predeterminados.

1. Seleccione **Revisar y crear** y, una vez superada la validación, seleccione **Crear**.  
     
   Espere a que la implementación se complete correctamente.
2. Haga clic en **Go to resource** (Ir al recurso).
3. Observe algunos detalles sobre el almacén de claves.  
     
   Por ejemplo, en el campo **Vault URI** (URI del almacén) se muestra el URI que puede usar la aplicación para acceder al almacén desde la API de REST.  
     
   Este es un ejemplo de un almacén de claves denominado **my-keyvault-321**: 
4. Como paso opcional, puede examinar algunas de las otras características en **Configuración**, en el panel de menús de la izquierda.  
     
   Aunque inicialmente están vacías, aquí encontrará ubicaciones donde puede almacenar claves, secretos y certificados.

**Nota**

La suscripción de Azure es la única que está autorizada a acceder a este almacén. En **Configuración**, la característica **Directivas de acceso** permite configurar el acceso al almacén.

**Adición de una contraseña al almacén de claves**

1. En el panel de menús de la izquierda, en **Configuración**, seleccione **Secretos**. Aparecerá el panel del almacén de claves.
2. En la barra de menús superior, seleccione **Generar/Importar**. Aparecerá el panel para **crear un secreto**.
3. Rellene los siguientes valores para cada configuración.

**Configuración**

**Valor**

Opciones de carga

**Manual**

Nombre

**MyPassword**

Value

**hVFkk96**

Acepte las opciones restantes con sus valores predeterminados. Tenga en cuenta que puede especificar propiedades como la fecha de activación y la de expiración. También puede deshabilitar el acceso al secreto.

1. Seleccione **Crear**.

**Mostrar la contraseña**

Aquí se accede a la contraseña del almacén de claves dos veces. En primer lugar se accede desde Azure Portal. Luego se accede desde la CLI de Azure.

1. En el panel **Almacén de claves/Secretos**, seleccione **MyPassword**. Aparecerá el panel **MyPassword/Versiones**. Se ve que la versión actual está habilitada.
2. Seleccione la versión actual. Aparecerá el panel **Versión del secreto**.  
     
   En **Identificador secreto** se ve un URI que ahora puede usar con las aplicaciones para acceder al secreto. Recuerde que solo las aplicaciones autorizadas pueden acceder a este secreto.
3. Seleccione **Mostrar valor secreto**. Se muestra el valor único de esta versión de la contraseña.  
     
   A screenshot of the Azure portal showing the secret value in the key vault.
4. Ejecute este comando en Cloud Shell.

**Nota**

Reemplace **my-keyvault-NNN** por el nombre que ha usado antes.

CLI de AzureCopiar

az keyvault secret show \

--name MyPassword \

--vault-name my-keyvault-NNN \

--query value \

--output tsv

Verá la contraseña en la salida.

ResultadoCopiar

hVFkk96

¡Excelente trabajo! En este punto, tiene un almacén de claves que contiene un secreto de contraseña que se almacena de forma segura para su uso con las aplicaciones.

**Limpieza**

El espacio aislado limpia los recursos automáticamente cuando haya terminado con este módulo.

Al trabajar en una suscripción propia, se recomienda identificar al final de un proyecto si aún necesita los recursos creados. Los recursos que deja en ejecución pueden costar dinero. Puede eliminar los recursos de forma individual o eliminar el grupo de recursos para eliminar todo el conjunto de recursos.

**Hospedaje de máquinas virtuales de Azure en servidores físicos dedicados mediante Azure Dedicated Host**

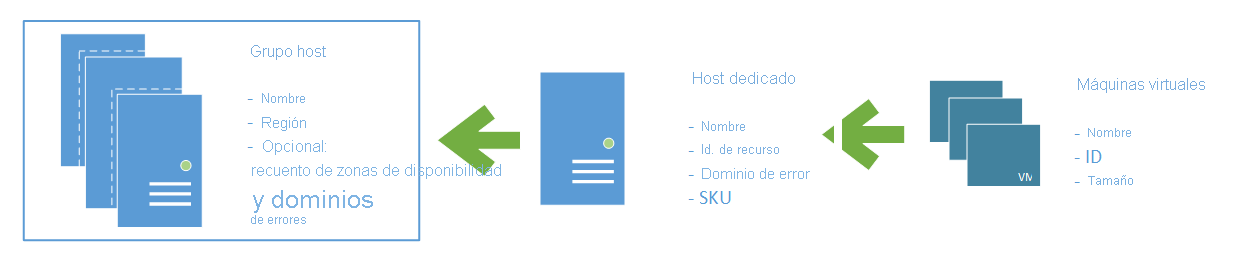
Completado100 XP

* 2 minutos

En Azure, las máquinas virtuales (VM) se ejecutan en hardware compartido administrado por Microsoft. Aunque el hardware subyacente se comparte, las cargas de trabajo de las máquinas virtuales están aisladas de las que ejecutan otros clientes de Azure.

Algunas organizaciones deben ajustarse a un cumplimiento normativo que las obliga a ser el único cliente que usa el equipo físico en el que se hospedan sus máquinas virtuales. [Azure Dedicated Host](https://azure.microsoft.com/services/virtual-machines/dedicated-host/) proporciona servidores físicos dedicados para hospedar las máquinas virtuales de Azure para Windows y Linux.

Este es un diagrama en el que se muestra la relación entre las máquinas virtuales y los hosts dedicados y los grupos host. Un *host dedicado* se asigna a un servidor físico en un centro de datos de Azure. Un *grupo host* es una colección de hosts dedicados.



**¿Cuáles son las ventajas de Azure Dedicated Host?**

Azure Dedicated Host:

* Ofrece visibilidad y control sobre la infraestructura de servidor que ejecuta las máquinas virtuales de Azure.
* Ayuda a satisfacer requisitos de cumplimiento mediante la implementación de las cargas de trabajo en un servidor aislado.
* Permite elegir el número de procesadores, capacidades de servidor, series de máquinas virtuales y tamaños de máquina virtual dentro del mismo host.

**Consideraciones de disponibilidad de Dedicated Host**

Después de aprovisionar un host dedicado, Azure lo asigna al servidor físico en el centro de datos en la nube de Microsoft.

Para lograr una alta disponibilidad, puede aprovisionar varios hosts en un *grupo host* e implementar las máquinas virtuales en este grupo. Las máquinas virtuales en hosts dedicados también pueden aprovechar las ventajas del *control de mantenimiento*. Esta característica permite controlar cuándo se producen las actualizaciones de mantenimiento regulares, dentro de una ventana gradual de 35 días.

**Consideraciones sobre precios**

Se cobra por host dedicado, con independencia de cuántas máquinas virtuales se implementen en él. El precio del host se basa en la familia de máquinas virtuales, el tipo (tamaño de hardware) y la región.

Las licencias de software, el almacenamiento y el uso de red se facturan por separado al host y las máquinas virtuales. Para obtener más información, vea [Precios de Azure Dedicated Host](https://aka.ms/ADHPricing/).