**Introducción**

Este módulo está diseñado para proporcionar a los administradores los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad avanzadas para los recursos de proceso de Azure, protegiendo las aplicaciones y los datos frente a unas amenazas de seguridad que están en constante evolución.

**Escenario**

Imagine que es un especialista en seguridad en la nube responsable de proteger los recursos de proceso de Azure en su organización. Su organización se basa en máquinas virtuales, servicios de contenedor y API, y debe asegurarse de que estos recursos están protegidos contra vulnerabilidades de acceso y seguridad no autorizadas.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Planee e implemente medidas de seguridad avanzadas para los recursos de proceso de Azure para protegerse frente a vulnerabilidades y ataques.
* Configure el acceso remoto a puntos de conexión públicos mediante Azure Bastion y el acceso a máquinas virtuales Just-In-Time (JIT) para mejorar el control de acceso.
* Implemente el aislamiento de red para Azure Kubernetes Service (AKS) para proteger las aplicaciones en contenedores.
* Proteja y supervise los clústeres de AKS para garantizar la integridad de las cargas de trabajo de contenedor.
* Configure la autenticación para que AKS controle el acceso a los recursos de Kubernetes.
* Configure la supervisión de seguridad para Azure Container Instances (ACI) para detectar y responder a amenazas.
* Establezca la supervisión de seguridad para Azure Container Apps (ACA) para proteger las aplicaciones sin servidor.
* Administre el acceso a Azure Container Registry (ACR) para controlar el acceso y la distribución de imágenes de contenedor.
* Configure el cifrado de disco, incluido Azure Disk Encryption (ADE), el cifrado como host y el cifrado de disco confidencial, para proteger los datos en reposo.
* Proporcione recomendaciones informadas sobre las configuraciones de seguridad en Azure API Management para proteger las API y administrar el acceso de forma eficaz.

**Planee e implemente el acceso remoto a puntos de conexión públicos, Azure Bastion y el acceso a una máquina virtual (VM) cuando sea necesario (JIT)**

Azure Bastion es un servicio que se implementa que le permite conectarse a una máquina virtual mediante el explorador y Azure Portal o a través del cliente RDP o SSH nativo ya instalado en el equipo local. Azure Bastion es un nuevo servicio PaaS totalmente administrado por la plataforma que se aprovisiona en las redes virtuales. Proporciona una conectividad RDP/SSH segura e ininterrumpida a las máquinas virtuales directamente sobre TLS desde Azure Portal o a través del cliente nativo. Cuando se conecta a través de Azure Bastion, las máquinas virtuales no necesitan una dirección IP pública, un agente ni software cliente especial.

Bastion proporciona conectividad segura de RDP y SSH a todas las máquinas virtuales de la red virtual en la que se aprovisiona. El uso de Azure Bastion protege las máquinas virtuales frente a la exposición de los puertos de RDP/SSH al mundo exterior, al tiempo que ofrece acceso seguro mediante RDP/SSH.

**Ventajas principales**

| **Prestación** | **Descripción** |
| --- | --- |
| RDP y SSH mediante Azure Portal | Con un solo clic en Azure Portal, podrá ir directamente a la sesión RDP o SSH. |
| Sesión remota a través de TLS y cruce seguro de firewall para RDP/SSH | Azure Bastion usa un cliente web basado en HTML5 que se transmite automáticamente al dispositivo local. La sesión RDP o SSH se encuentra en el puerto 443 a través del protocolo TLS. Esto permite que el tráfico atraviese los firewalls de forma más segura. Bastion admite TLS 1.2 y versiones posteriores. No se admiten versiones anteriores de TLS. |
| No requiere que la máquina virtual de Azure disponga de una dirección IP pública | Azure Bastion abrirá la conexión RDP o SSH para la dirección IP privada de la máquina virtual de Azure. La máquina virtual no necesita una dirección IP pública. |
| Sin la complicación de administrar grupos de seguridad de red (NSG) | No es necesario que aplique ningún NSG en la subred de Azure Bastion. Dado que Azure Bastion se conecta a las máquinas virtuales a través de la dirección IP privada, puede configurar los NSG para permitir RDP o SSH solo desde Azure Bastion. De este modo se evita tener que administrar los NSG cada vez que necesite conectarse de forma segura a las máquinas virtuales. |
| No requiere administrar un host bastión independiente en una máquina virtual | Azure Bastion es un servicio PaaS de Azure de plataforma totalmente administrada que se refuerza internamente para proporcionar una conexión RDP/SSH segura. |
| Protección frente al examen de puertos | Las máquinas virtuales quedan protegidas contra la detección de puertos por parte de usuarios no autorizados y malintencionados, ya que no es necesario exponerlas a Internet. |
| Protección en un solo lugar | Azure Bastion se encuentra en el perímetro de la red virtual, por lo que no es necesario preocuparse por proteger cada una de las máquinas virtuales de la red virtual. |
| Protección frente a vulnerabilidades de seguridad de día cero | La plataforma de Azure protege contra ataques de día cero manteniendo automáticamente el servicio Azure Bastion protegido y siempre actualizado. |

**SKU (unidades de almacenamiento de existencias)**

Azure Bastion tiene dos SKU disponibles, básica y estándar. En la tabla siguiente se muestran las características y las SKU correspondientes.

| **Característica** | **SKU de desarrollador** | **SKU básica** | **SKU Estándar** |
| --- | --- | --- | --- |
| Conexión a máquinas virtuales de destino en la misma red virtual | Sí | Sí | Sí |
| Conexión a máquinas virtuales de destino en redes virtuales emparejadas | No | Sí | Sí |
| Compatibilidad con conexiones simultáneas | No | Sí | Sí |
| Acceso a claves privadas de VM Linux en Azure Key Vault (AKV) | No | Sí | Sí |
| Conexión a una máquina virtual Linux mediante SSH | Sí | Sí | Sí |
| Conexión a una máquina virtual Windows mediante RDP | Sí | Sí | Sí |
| Conexión a una máquina virtual Linux mediante RDP | No | No | Sí |
| Conexión mediante SSH a una máquina virtual Windows | No | No | Sí |
| Especificación del puerto de entrada personalizado | No | No | Sí |
| Conexión a máquinas virtuales mediante la CLI de Azure | No | No | Sí |
| Escalado de host | No | No | Sí |
| Carga o descarga de archivos | No | No | Sí |
| Autenticación de Kerberos | No | Sí | Sí |
| Vínculo compartible | No | No | Sí |
| Conexión a máquinas virtuales a través de la dirección IP | No | No | Sí |
| Salida de audio de la máquina virtual | Sí | Sí | Sí |
| Deshabilitar copiar y pegar (clientes basados en web) | No | No | Sí |

**Architecture**

Azure Bastion se implementa en una red virtual y admite el emparejamiento de red virtual. En concreto, Azure Bastion administra la conectividad RDP/SSH con máquinas virtuales creadas en las redes virtuales locales o emparejadas.

RDP y SSH son algunos de los medios fundamentales a mediante los que puede conectarse a las cargas de trabajo que se ejecutan en Azure. La exposición de los puertos RDP/SSH a través de Internet no se conveniente y se considera una superficie de amenaza considerable. Esto suele deberse a las vulnerabilidades del protocolo. Para contener esta superficie de amenaza, puede implementar hosts de bastión (también conocidos como servidores de salto) en la parte pública de la red perimetral. Los servidores host de bastión están diseñados y configurados para resistir los ataques. Los servidores de bastión también proporcionan conectividad RDP y SSH con las cargas de trabajo que se encuentran detrás del bastión, así como más adentro en la red.

Actualmente, de forma predeterminada, las nuevas implementaciones de Bastion no admiten redundancias de zona. Los bastiones implementados anteriormente podrían ser o no con redundancia de zona. Las excepciones son las implementaciones de Bastion de las zonas Centro de Corea del Sur y Sudeste de Asia, que admiten redundancias de zona.

* El host bastión se implementa en la red virtual que contiene la subred AzureBastionSubnet que tiene un prefijo /26 mínimo.
* El usuario se conecta a Azure Portal con cualquier explorador HTML5.
* El usuario selecciona la máquina virtual a la que conectarse.
* Con un solo clic, la sesión RDP/SSH se abre en el explorador.
* No se requiere ninguna dirección IP pública en la máquina virtual de Azure.

**Escalado de host**

Azure Bastion admite el escalado de host manual. Puede configurar el número de instancias de host (unidades de escalado) para administrar el número de conexiones RDP/SSH simultáneas que Azure Bastion pueden admitir. Aumentar el número de instancias de host permite a Azure Bastion administrar más sesiones simultáneas. Al reducir el número de instancias, se reduce el número de sesiones admitidas simultáneas. Azure Bastion admite hasta 50 instancias de host. Esta característica solo está disponible para la SKU estándar de Azure Bastion.

**Configurar el aislamiento de redes en Azure Kubernetes Service (AKS)**

A medida que administra los clústeres en Azure Kubernetes Service (AKS), a menudo necesita aislar los equipos y las cargas de trabajo. AKS permite flexibilidad en la forma de ejecutar clústeres multiinquilino y aislar recursos. Para maximizar tu inversión en Kubernetes, es importante que comprenda las características de aislamiento y multiusuario de AKS.

**Diseño de clústeres para la configuración multiempresa**

Kubernetes permite aislar lógicamente equipos y cargas de trabajo en el mismo clúster. El objetivo es proporcionar el número mínimo de privilegios en el ámbito de los recursos que necesita cada equipo. Un espacio de nombres de Kubernetes crea un límite de aislamiento lógico. Otras características y consideraciones de Kubernetes para el aislamiento y la tenencia múltiple incluyen las siguientes áreas:

* Procedimientos recomendados para el aislamiento de clústeres en Azure Kubernetes Service (AKS)  
  + Diseño de clústeres para la configuración multiempresa
    - Scheduling
    - Redes
    - Autenticación y autorización
    - Contenedores
* Clústeres aislados lógicamente
* Clústeres aislados físicamente

**Scheduling**

La *programación* utiliza funciones básicas como cuotas de recursos y presupuestos de interrupción de pod.

Las siguientes son algunas de las características más avanzadas del programador:

* Intolerancias y tolerancias.
* Selectores de nodos.
* Afinidad o antiafinidad de nodos y pods.

**Redes**

Las *redes* usan directivas de red para controlar el flujo de tráfico de entrada y salida de pods.

**Autenticación y autorización**

Usos de la *autenticación y autorización*:

* Control de acceso basado en roles (RBAC).
* Integración de Microsoft Entra.
* Identidades de pod.
* Secretos en Azure Key Vault.

**Contenedores**

Los *contenedores* incluyen:

* El complemento de Azure Policy para AKS con el fin de aplicar la seguridad del pod.
* Admisión de seguridad de pod.
* Escaneo de imágenes y tiempo de ejecución en busca de vulnerabilidades.
* El uso de AppArmor o Seccomp (informática segura) para restringir el acceso del contenedor al nodo subyacente.

**Clústeres aislados lógicamente**

**Guía de procedimientos recomendados**: Separe los equipos y los proyectos mediante el aislamiento lógico. Minimice el número de clústeres físicos de AKS que implementa para aislar los equipos o las aplicaciones.

Con el aislamiento lógico, puede usar un único clúster de AKS para varias cargas de trabajo, equipos o entornos. Los espacios de nombres de Kubernetes forman el límite de aislamiento lógico para las cargas de trabajo y los recursos.

La separación lógica de clústeres normalmente proporciona una mayor densidad de pods que los clústeres aislados físicamente, con una menor capacidad de proceso inactiva en el clúster. Cuando se combina con el escalador automático de clúster de Kubernetes, puede escalar vertical u horizontalmente el número de nodos para satisfacer las necesidades. Este enfoque de procedimientos recomendados minimiza los costes al ejecutar solo la cantidad requerida de nodos.

Los entornos de Kubernetes no son del todo seguros para el uso multiinquilino hostil. En un entorno multiinquilino, varios inquilinos funcionan en una infraestructura compartida. Si no se puede confiar en todos los inquilinos, necesita una planificación adicional para evitar que los inquilinos afecten la seguridad y el servicio de los demás.

Otras características de seguridad, como Kubernetes RBAC para nodos, bloquean de manera eficiente las vulnerabilidades. Para tener una seguridad verdadera al ejecutar cargas de trabajo multiinquilino hostiles, solo debe confiar en un hipervisor. El dominio de seguridad de Kubernetes se convierte en todo el clúster y no en un nodo individual.

En el caso de estos tipos de cargas de trabajo multiinquilino hostiles, debe usar clústeres que estén físicamente aislados.

**Clústeres aislados físicamente**

**Guía de procedimientos recomendados**: Minimice el uso del aislamiento físico para cada implementación de aplicación o equipo independiente y use el aislamiento lógico en su lugar.

Separar físicamente los clústeres de AKS es un enfoque común para el aislamiento de clústeres. En este modelo de aislamiento, los equipos o las cargas de trabajo se asignan a su propio clúster de AKS. Aunque el aislamiento físico podría parecer la manera más fácil de aislar cargas de trabajo o equipos, agrega una sobrecarga financiera y administrativa. Con los clústeres aislados físicamente, debes mantener varios y proporcionar acceso y asignar permisos de forma individual. También se te cobrará por cada nodo individual.

Los clústeres aislados físicamente suelen tener una baja densidad de pods. Ya que cada equipo o carga de trabajo tiene su propio clúster de AKS, el clúster a menudo se aprovisiona en exceso con recursos de proceso. A menudo, se programan algunos pods en esos nodos. La capacidad de los nodos no utilizada no se puede usar para aplicaciones o servicios que están desarrollando otros equipos. Estos recursos en exceso contribuyen a los costos adicionales en clústeres aislados físicamente.

**Protección y supervisión de AKS**

Microsoft Defender para contenedores es la solución nativa de nube a fin de que pueda mejorar, supervisar y mantener la seguridad de los clústeres, los contenedores y sus aplicaciones.

Defender para contenedores le ayuda con cuatro aspectos básicos de la seguridad de los contenedores:

* **Protección del entorno**: Defender para Containers protege los clústeres de Kubernetes tanto si se ejecutan en Azure Kubernetes Service, Kubernetes local o IaaS, como en Amazon EKS. Defender para Contenedores evalúa continuamente los clústeres para proporcionar visibilidad de las configuraciones erróneas y directrices para ayudar a mitigar las amenazas identificadas.
* **Evaluación de vulnerabilidades**: herramientas de evaluación y administración de vulnerabilidades para imágenes almacenadas en Azure Container Registry y Elastic Container Registry.
* **Protección contra amenazas en tiempo de ejecución para nodos y clústeres**: la protección contra amenazas para clústeres y nodos genera alertas de seguridad de actividades sospechosas.
* **Detección sin agente para Kubernetes**: proporciona herramientas que proporcionan visibilidad sobre los componentes del plano de datos, generando información de seguridad basada en la configuración del entorno y Kubernetes y le permite buscar riesgos.

**Protección**

Supervisión continua de los clústeres de Kubernetes, dondequiera que estén hospedados

Defender for Cloud evalúa continuamente las configuraciones de los clústeres y las compara con las iniciativas aplicadas a las suscripciones. Cuando encuentra configuraciones incorrectas, Defender for Cloud genera recomendaciones de seguridad que están disponibles en la página Recomendaciones de Defender for Cloud. Las recomendaciones le permiten investigar y corregir problemas.

Puede usar el filtro de recursos para revisar las recomendaciones pendientes para los recursos relacionados con el contenedor, ya sea en el inventario de recursos o en la página de recomendaciones:

**Protección del plano de datos de Kubernetes**

Para proteger las cargas de trabajo de los contenedores de Kubernetes con recomendaciones a medida, puede instalar Azure Policy para Kubernetes. Obtenga información sobre la supervisión de componentes para Defender for Cloud.

Con el complemento en el clúster de AKS, todas las solicitudes al servidor de la API de Kubernetes se supervisarán según el conjunto predefinido de procedimientos recomendados antes de que se guarden en el clúster. Después, puede realizar la configurar para aplicar los procedimientos recomendados y exigirlos para futuras cargas de trabajo.

Por ejemplo, puede exigir que no se creen los contenedores con privilegios y que se bloqueen las solicitudes futuras para este fin.

**Evaluación de vulnerabilidades**

Defender para contenedores examina las imágenes de contenedor en Azure Container Registry (ACR) y Amazon AWS Elastic Container Registry (ECR) para proporcionar informes de vulnerabilidades para las imágenes de contenedor, lo que proporciona detalles para cada vulnerabilidad detectada, guía de corrección, información sobre vulnerabilidades de seguridad reales, etc.

Hay dos soluciones para la evaluación de vulnerabilidades en Azure, una con tecnología de Administración de vulnerabilidades de Microsoft Defender y otra con tecnología de Qualys.

**Protección en tiempo de ejecución de los clústeres y nodos de Kubernetes**

Defender para contenedores proporciona protección contra amenazas en tiempo real para los entornos en contenedores compatibles y genera alertas de actividades sospechosas. Puede usar esta información para corregir problemas de seguridad y mejorar la seguridad de los contenedores rápidamente.

La protección contra amenazas en el nivel de clúster se proporciona mediante el agente de Defender y el análisis de los registros de auditoría de Kubernetes. Esto quiere decir que las alertas de seguridad solo se desencadenan para las acciones e implementaciones que se producen después de habilitar Defender para contenedores en la suscripción.

Entre los ejemplos de eventos de seguridad que supervisa Microsoft Defender para contenedores, se incluyen los siguientes:

* Paneles de Kubernetes expuestos.
* Creación de roles con privilegios elevados.
* Creación de montajes confidenciales

**Configuración de la autenticación de AKS**

A medida que implementa y mantiene clústeres en Azure Kubernetes Service (AKS), deberá implementar maneras de administrar el acceso a los recursos y servicios. Sin estos controles:

* Las cuentas podrían tener acceso a recursos y servicios innecesarios.
* Puede ser difícil realizar el seguimiento de las credenciales que se utilizan para hacer cambios.

**Uso de Microsoft Entra ID**

**Guía de procedimientos recomendados**: Implemente clústeres de AKS con la integración de Microsoft Entra. Con Microsoft Entra ID, se centraliza la capa de administración de identidades. Cualquier cambio en el estado del grupo o cuenta del usuario se actualiza automáticamente al acceder al clúster de AKS. Establezca el ámbito de los usuarios o grupos en la cantidad mínima de permisos mediante roles, ClusterRoles o enlaces.

Los desarrolladores del clúster de Kubernetes y propietarios de aplicaciones necesitan acceder a diferentes recursos. Kubernetes carece de una solución de administración de identidades para controlar los recursos con los que los usuarios pueden interactuar. En su lugar, puede integrar el clúster con una solución de identidad existente como Microsoft Entra ID, una solución de administración de identidades lista para la empresa.

Con los clústeres integrados con Microsoft Entra en AKS, podrá crear roles o ClusterRoles que definan los permisos de acceso a los recursos. A continuación, enlaza los roles a usuarios o grupos de Microsoft Entra ID.

1. El desarrollador se autentica con Microsoft Entra ID.
2. El punto de conexión de emisión de tokens de Microsoft Entra emite el token de acceso.
3. El desarrollador realiza una acción mediante el token de Microsoft Entra, como kubectl create pod.
4. Kubernetes valida el token con Microsoft Entra ID y recupera las pertenencias a grupos del desarrollador.
5. Se aplican las directivas del clúster y de RBAC de Kubernetes.
6. La solicitud del desarrollador es correcta en función de la validación anterior de pertenencia a grupos de Microsoft Entra y las directivas y RBAC de Kubernetes.

**Uso del control de acceso basado en roles de Kubernetes (RBAC de Kubernetes)**

**Guía de procedimientos recomendados**: Defina permisos de usuario o grupo para los recursos de clúster con RBAC de Kubernetes. Cree roles y enlaces que asignen la mínima cantidad de permisos necesarios. Use la integración de Microsoft Entra ID para actualizar automáticamente cualquier cambio de estado de usuario o pertenencia a grupos y mantener el acceso a los recursos del clúster actual.

En Kubernetes se proporciona control de acceso pormenorizado a los recursos del clúster. Los permisos se definen en el nivel de clúster, así como en espacios de nombres específicos. Determine qué recursos se pueden administrar y con qué permisos. A continuación, aplique estos roles a los usuarios o grupos con un enlace. Para obtener más información sobre los roles, ClusterRoles y enlaces, consulte Opciones de acceso e identidad en Azure Kubernetes Service (AKS).

Cuando developer1@contoso.com se autentica en el clúster de AKS, se tienen los permisos completos sobre los recursos en el espacio de nombres finance-app. De esta forma, separa y controla el acceso a los recursos de forma lógica. Uso de RBAC de Kubernetes con la integración de Microsoft Entra ID.

**Uso de Azure RBAC**

**Guía de procedimientos recomendados**: Use Azure RBAC para definir los permisos mínimos necesarios de usuario y grupo para los recursos de AKS en una o varias suscripciones.

Hay dos niveles de acceso necesarios para operar completamente un clúster de AKS:

1. Este nivel de acceso le permite:
   * Controle el escalado o la actualización del clúster mediante las API de AKS.
   * Extraer kubeconfig.
   * Acceda al recurso de AKS en la suscripción de Azure.
2. Este nivel de acceso se controla mediante:
   * RBAC de Kubernetes (tradicionalmente), o bien,
   * mediante la integración de RBAC de Azure con AKS para la autorización de Kubernetes.
   * Acceso al API de Kubernetes.

**Configure la seguridad para Azure Container Instances (ACI)**

Azure Monitor proporciona información acerca de los recursos de proceso que utilizan las instancias de contenedor. Esta información sobre el uso de los recursos le ayuda a determinar cuál es la mejor configuración de recursos para los grupos de contenedores. Azure Monitor también proporciona métricas que realizan un seguimiento de la actividad en la red en sus instancias de contenedor.

**Limitaciones de vista previa**

En este momento, las métricas de Azure Monitor solamente están disponibles para los contenedores de Linux.

**Métricas disponibles**

Azure Monitor proporciona las siguientes métricas para Azure Container Instances. Estas métricas están disponibles para grupos de contenedores y contenedores individuales. De forma predeterminada, las métricas se agregan como promedios.

* Uso de CPU: medido en milinúcleos.  
  + 1 millar de núcleos corresponde a 1/1000 de un núcleo de CPU, por lo que 500 millares de núcleos representan un uso de 0,5 de un núcleo de CPU.
* Uso de memoria en bytes.
* Bytes de red recibidos por segundo.
* Bytes de red transmitidos por segundo.

**Obtención de métricas mediante Azure Portal**

Cuando se crea un grupo de contenedores, los datos de Azure Monitor están disponibles en Azure Portal. Para ver las métricas de un grupo de contenedores, vaya a la página Información general del grupo de contenedores. Aquí puede ver los gráficos creados previamente para cada una de las métricas disponibles.

En un grupo de contenedores que contenga varios contenedores, utilice una dimensión para mostrar las métricas por contenedor. Para crear un gráfico utilizando las métricas de cada contenedor, siga estos pasos:

1. En la página **Información general** página, seleccione uno de los gráficos de métricas, como **CPU**.
2. Seleccione el botón **Apply splitting** (Aplicar división) y, después, seleccione **Nombre del contenedor**.

**Configure la seguridad de Azure Container Apps (ACA)**

**Uso de un registro privado**

Los contenedores se crean a partir de imágenes que están almacenadas en uno o varios repositorios. Estos repositorios pueden pertenecer a un registro público, como Docker Hub, o en un registro privado. Un ejemplo de un registro privado es el Registro de confianza de Docker, que puede instalarse de forma local o en una nube privada virtual. También puede usar servicios de registro privado de contenedores basados en la nube, incluido Azure Container Registry.

Una imagen de contenedor disponible públicamente no garantiza la seguridad. Las imágenes de contenedor constan de varias capas de software, y cada capa de software podría tener vulnerabilidades. Para ayudar a reducir la amenaza de ataques, debe almacenar y recuperar las imágenes de un registro privado, como Azure Container Registry o Docker Trusted Registry. Además de proporcionar un registro privado administrado, Azure Container Registry admite la autenticación basada en la entidad de servicio a través de Microsoft Entra ID para flujos de autenticación básicos. Esta autenticación incluye el acceso basado en roles para permisos de solo lectura (extracción), escritura (inserción) y otros.

**Supervisar y analizar las imágenes de contenedor**

Aproveche las soluciones para analizar imágenes de contenedor en un registro privado e identificar posibles puntos vulnerables. Es importante comprender el nivel de detalles de la detección de amenazas que proporcionan las distintas soluciones.

Por ejemplo, Azure Container Registry ofrece la opción de integrarlo con Microsoft Defender para la nube para analizar automáticamente todas las imágenes de Linux insertadas en un registro. El analizador Qualys integrado de Microsoft Defender para la nube detecta puntos vulnerables en las imágenes, las clasifica y proporciona una guía de corrección.

En Azure Marketplace hay disponibles soluciones de supervisión de seguridad y análisis de imágenes, como Twistlock y Aqua Security.

**Proteger las credenciales**

Los contenedores pueden abarcar varios clústeres y regiones de Azure. Por lo tanto, debe proteger las credenciales necesarias para los inicios de sesión o el acceso a las API, como contraseñas o tokens. Asegúrese de que solo los usuarios con privilegios puedan acceder a esos contenedores en tránsito y en reposo. Haga un inventario de todos los secretos de credenciales y, luego, pida a los desarrolladores que usen las nuevas herramientas de administración de secretos que están diseñadas para plataformas de contenedores. Asegúrese de que la solución incluya bases de datos cifradas, cifrado TLS para datos de los datos de secretos en tránsito y control de acceso basado en roles de Azure (RBAC de Azure) con privilegios mínimos. Azure Key Vault es un servicio en la nube que protege las claves de cifrado y los secretos (como certificados, cadenas de conexión y contraseñas) de las aplicaciones en contenedores. Dado que estos datos son confidenciales y críticos para la empresa, proteja el acceso a los almacenes de claves, de modo que solo las aplicaciones y los usuarios autorizados puedan acceder a ellos.

**Consideraciones para el ecosistema de contenedores**

Las siguientes medidas de seguridad, implementas correctamente y administradas de forma eficaz, pueden ayudar a asegurar y proteger su ecosistema de contenedores. Estas medidas se aplican en todo el ciclo de vida del contenedor, desde el desarrollo hasta la implementación en producción, y en una gama de plataformas, hosts y orquestadores de contenedores.

**Usar la administración de vulnerabilidades como parte de su ciclo de vida de desarrollo de contenedores**

Al usar una administración de vulnerabilidades eficaz a lo largo del ciclo de vida de desarrollo de los contenedores, mejora las probabilidades de detectar y resolver problemas de seguridad antes de que sean un problema más grave.

**Análisis de vulnerabilidades**

Todo el tiempo se descubren nuevas vulnerabilidades, por lo que el análisis y la identificación de vulnerabilidades es un proceso continuo. Incorpore el análisis de vulnerabilidades a lo largo del ciclo de vida de los contenedores:

* Como comprobación final en la canalización de desarrollo, debe realizar un análisis de vulnerabilidades en los contenedores antes de insertar las imágenes en un registro público o privado.
* Continúe analizando imágenes de contenedor en el registro tanto para identificar cualquier error que pueda haberse pasado durante el desarrollo como para abordar las vulnerabilidades descubiertas recientemente que puedan existir en el código usado en las imágenes de contenedores.

**Asignar vulnerabilidades de imágenes a contenedores en ejecución**

Debe tener un medio para asignar las vulnerabilidades identificadas en las imágenes de contenedor a los contenedores en ejecución, de modo que los problemas de seguridad puedan mitigarse.

**Asegurarse de que solo se usen imágenes aprobadas en su entorno**

Existen suficientes cambios y volatilidad en un ecosistema de contenedores sin que se permitan, además, contenedores desconocidos. Permita solo imágenes de contenedor aprobadas. Ponga en práctica herramientas y procesos para supervisar y evitar el uso de imágenes de contenedor no aprobadas.

Una forma eficaz de reducir la superficie de ataque e impedir que los desarrolladores cometan errores de seguridad críticos consiste en controlar el flujo de imágenes de contenedor en el entorno de desarrollo. Por ejemplo, podría autorizar una única distribución de Linux como imagen de base, preferiblemente una que sea eficiente (Alpine o CoreOS, en lugar de Ubuntu), para minimizar la superficie de ataques potenciales.

La firma o creación de huellas digitales para imágenes puede generar una cadena de custodia que le permita verificar la integridad de los contenedores. Por ejemplo, Azure Container Registry es compatible con el modelo de contenido confianza de Docker, que permite a los editores de imágenes firmar las imágenes que se insertan en un registro, y a los consumidores de imágenes extraer solo imágenes firmadas.

**Permitir solo registros aprobados**

Una extensión para garantizar que su entorno use solo las imágenes aprobadas radica en permitir únicamente el uso de los registros de contenedor aprobados. Requerir el uso de registros de contenedor aprobados reduce la exposición a riesgos, ya que se limita la posibilidad de que se introduzcan vulnerabilidades o problemas de seguridad desconocidos.

**Garantizar la integridad de las imágenes a lo largo del ciclo de vida**

Parte de la administración de la seguridad a lo largo del ciclo de vida del contenedor es garantizar la integridad de las imágenes de contenedor en el registro, así como en la medida en que se modifican o implementan en producción.

* No debe permitirse que imágenes con vulnerabilidades, aunque sean menores, se ejecuten en un entorno de producción. Lo ideal es que todas las imágenes implementadas en producción se guarden en un registro privado donde solo algunas personas tengan acceso. Mantenga un número pequeño de imágenes de producción para asegurarse de que se puedan administrar eficazmente.
* Dado que es difícil identificar el origen del software desde una imagen de contenedor disponible públicamente, cree imágenes desde la fuente para garantizar el conocimiento del origen de la capa. Cuando surge una vulnerabilidad en una imagen de contenedor generada automáticamente, los clientes pueden encontrar una ruta más rápida a una resolución. Con una imagen pública, los clientes tendrían que encontrar la raíz de una imagen pública para corregirla u obtener otra imagen segura del publicador.
* No se garantiza que una imagen digitalizada exhaustivamente implementada en producción esté actualizada durante la vigencia de la aplicación. Se puede informar de las vulnerabilidades de seguridad para las capas de la imagen que no se conocían anteriormente o que se introdujeron después de la implementación de producción.
* Haga auditorías periódicas de imágenes implementadas en producción para identificar las imágenes que no están al día o que no se han actualizado en un tiempo. Puede usar metodologías de implementación de verde-azul y activar mecanismos de actualización para actualizar las imágenes de contenedor sin tiempo de inactividad. Puede analizar las imágenes con las herramientas descritas en la sección anterior.
* Use una canalización de integración continua (CI) con análisis de seguridad integrada para crear imágenes seguras e insertarlas en su registro privado. El análisis de vulnerabilidad creado en la solución de CI garantiza que las imágenes que pasan todas las pruebas se incluyan en el registro privado desde el que se implementan las cargas de trabajo de producción.
* Un error de canalización de CI garantiza que las imágenes vulnerables no se incluyan en el registro privado usado para las implementaciones de cargas de trabajo de producción. También automatiza el análisis de seguridad de imágenes si hay un número significativo de imágenes. De lo contrario, auditar las imágenes manualmente para buscar vulnerabilidades de seguridad puede ser bastante lento y estar propenso a errores.

**Exigir privilegios mínimos en tiempo de ejecución**

El concepto de privilegios mínimos es una práctica recomendada de seguridad básica que también se aplica a los contenedores. Cuando se aprovecha una vulnerabilidad, en general da al atacante acceso y privilegios iguales a los de la aplicación o proceso en peligro. Asegurarse de que los contenedores funcionen con privilegios mínimos y acceso requerido para realizar el trabajo reduce la exposición a riesgos.

**Reducir la superficie de ataque a contenedores mediante la eliminación de privilegios innecesarios**

También puede minimizar la superficie potencial de ataque al eliminar del tiempo de ejecución del contenedor los procesos o privilegios innecesarios o sin usar. Los contenedores con privilegios se ejecutan como raíz. Si un usuario o una carga de trabajo malintencionados se cuela en un contenedor con privilegios, el contenedor se ejecutará como raíz en el sistema.

**Preaprobación de archivos y ejecutables a los que el contenedor puede acceder o que este puede ejecutar**

Reducir el número de variables o valores desconocidos le ayuda a mantener un entorno estable y confiable. Limitar los contenedores para que puedan solo acceder a archivos o ejecutables incluidos en una lista segura o para que puedan ejecutarlos es un método demostrado de limitar la exposición a riesgos.

Es mucho más fácil administrar una lista segura cuando se implementa desde un principio. Una lista segura proporciona una medida de control y capacidad de administración a medida que aprende qué archivos y ejecutables son necesarios para que la aplicación funcione correctamente.

Una lista segura no solo reduce la superficie expuesta a ataques, sino que puede también proporcionar una línea de base para encontrar anomalías y evitar los casos de uso de los escenarios de "vecino ruidoso" y división de contenedores.

**Aplicar la segmentación de la red en contenedores en ejecución**

Para ayudar a proteger los contenedores en una subred frente a los riesgos de seguridad de otra subred, mantenga la segmentación de la red (o nanosegmentación) o segregación entre contenedores en ejecución. También puede ser necesario mantener la segmentación de red para usar contenedores en sectores que deben cumplir exigencias de cumplimiento.

Por ejemplo, la herramienta de partner Aqua proporciona un enfoque automatizado para la nanosegmentación. Aqua supervisa las actividades de red de los contenedores en tiempo de ejecución. Identifica todas las conexiones de red entrantes y salientes hacia y desde otros contenedores, servicios, direcciones IP e Internet pública. La nanosegmentación se crea automáticamente en función del tráfico supervisado.

**Supervisar la actividad de los contenedores y el acceso de los usuarios**

Al igual que con cualquier entorno de TI, debe supervisar constantemente la actividad y el acceso de los usuario al ecosistema de contenedores para identificar rápidamente cualquier actividad sospechosa o malintencionada. Azure proporciona soluciones de supervisión de contenedores, entre otras:

* Azure Monitor para contenedores para supervisar el rendimiento de las cargas de trabajo implementadas en entornos de Kubernetes hospedados en Azure Kubernetes Service (AKS). Azure Monitor para contenedores le brinda la posibilidad de visibilizar el rendimiento mediante la recopilación de métricas del procesador y de la memoria de los controladores, nodos y contenedores disponibles en Kubernetes mediante la API de métricas.
* La solución de supervisión de contenedores en Azure le ayuda a ver y administrar otros hosts de contenedores de Docker y Windows en una sola ubicación. Por ejemplo:  
  + Ver información de auditoría detallada que muestre los comandos usados con los contenedores.
  + Solucionar los problemas de los contenedores al ver y buscar registros centralizados sin tener que ver los hosts de Docker o Windows de forma remota.
  + Buscar los contenedores que puedan causar ruido o consuman un exceso de recursos en un host.
  + Ver la información centralizada acerca de la CPU, la memoria, el almacenamiento, y el uso y el rendimiento de la red en relación con los contenedores.

La solución admite orquestadores de contenedores como Docker Swarm, DC/OS, Kubernetes no administrado, Service

**Supervisar la actividad de recursos de contenedor**

Supervise la actividad de los recursos, como archivos, red y otros recursos, a los que acceden los contenedores. Supervisar el consumo y la actividad de los recursos resulta útil para la supervisión de rendimiento y como medida de seguridad.

Azure Monitor habilita la supervisión básica del servicio de Azure al permitir la recopilación de métricas, registros de actividad y registros de diagnóstico. Por ejemplo, el registro de actividad le indica cuándo se crean o modifican los recursos.

Se encuentran disponibles métricas que ofrecen estadísticas de rendimiento de diferentes recursos e incluso del sistema operativo de una máquina virtual. Puede ver estos datos con uno de los exploradores en Azure Portal y crear alertas basadas en estas métricas. Azure Monitor ofrece la canalización de métricas más rápida (desde 5 minutos hasta 1 minuto), por lo que debe usarse para las notificaciones y alertas donde el tiempo es fundamental.

**Registrar todos los accesos administrativos de usuarios al contenedor para auditoría**

Mantenga un registro de auditoría preciso del acceso administrativo a su ecosistema de contenedores, incluido el clúster de Kubernetes, el registro de contenedores y las imágenes de contenedor. Estos registros podrían ser necesarios para fines de auditoría y serán útiles como prueba forense después de un incidente de seguridad. Las soluciones de Azure incluyen:

* Integración de Azure Kubernetes Service con Microsoft Defender for Cloud para supervisar la configuración de seguridad del entorno del clúster y generar recomendaciones de seguridad.
* Solución de supervisión de contenedores de Azure.
* Registros de recurso para Azure Container Instances y Azure Container Registry.

**Administrar el acceso a Azure Container Registry (ACR)**

El servicio Azure Container Registry admite un conjunto de roles de Azure integrados que proporcionan distintos niveles de permisos a una instancia de Azure Container Registry. Use el control de acceso basado en roles de Azure (RBAC de Azure) para asignar permisos específicos a usuarios, entidades de servicio u otras entidades que necesiten interactuar con un registro, por ejemplo, para insertar o extraer imágenes de contenedor. También puede definir roles personalizados con permisos específicos en un registro para distintas operaciones.

| **Rol o permiso** | **Acceso a Resource Manager** | **Crear o eliminar un registro** | **Insertar imagen** | **Extraer imagen** | **Eliminar los datos de imagen** | **Cambiar directivas** | **Firmar imágenes** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Propietario | X | X | X | X | X | X |  |
| Colaborador | X | X | X | X | X | X |  |
| Lector | X |  |  | X |  |  |  |
| AcrPush |  |  | X | X |  |  |  |
| AcrPull |  |  |  | X |  |  |  |
| AcrDelete |  |  |  |  | X |  |  |
| AcrImageSigner |  |  |  |  |  |  | X |

**Asignación de roles**

Puede usar Azure Portal, la CLI de Azure, Azure PowerShell u otras herramientas de Azure. Al crear una entidad de servicio, también se configuran los permisos y el acceso a los recursos de Azure como, por ejemplo, un registro de contenedor.

**Diferenciar usuarios y servicios**

Cada vez que se aplican permisos, el procedimiento recomendado es proporcionar el conjunto de permisos más limitados para que una persona o servicio puedan completar una tarea. Los siguientes conjuntos de permisos representan un conjunto de funciones para usuarios humanos y servicios desatendidos.

**Soluciones de CI/CD**

Al automatizar los comandos de compilación de Docker desde soluciones de CI/CD, necesita funcionalidades de inserción de Docker. En estos escenarios de servicios desatendidos, se recomienda asignar el rol AcrPush. Este rol, al contrario que el rol Colaborador (que es más amplio), impide que la cuenta pueda realizar otras operaciones de registro o que acceda a Azure Resource Manager.

**Nodos de host de contenedor**

Del mismo modo, los nodos que ejecuten los contenedores han de tener asignado el rol AcrPull, pero no necesitan de forma obligatoria funciones de Lector.

**Extensión de Docker de Visual Studio Code**

Para herramientas como la extensión de Docker de Visual Studio Code, se necesita acceso adicional de proveedor de recursos para mostrar la lista de registros de contenedor de Azure. En este caso, proporcione a los usuarios acceso al rol Lector o Colaborador. Estos roles permiten docker pull, docker push, az acr list, az acr build y otras funcionalidades.

**Acceso a Resource Manager**

El acceso a Azure Resource Manager es necesario para Azure Portal y la administración del registro con la interfaz de la línea de comandos de Azure. Por ejemplo, para obtener una lista de registros mediante el comando az acr list, necesita este conjunto de permisos.

**Crear y eliminar registros**

Capacidad para crear y eliminar registros de contenedor de Azure.

**Imagen de inserción**

La capacidad de docker de extraer una imagen no en cuarentena o extraer otro artefacto compatible, como un gráfico de Helm, desde un registro. Se necesita autenticación con el registro mediante la identidad autorizada.

**Eliminación de los datos de la imagen**

La capacidad de eliminar imágenes de contenedor u otros artefactos admitidos, como gráficos de Helm, desde un registro.

**Cambiar directivas**

Capacidad para configurar directivas en un registro. En las directivas, se incluye la purga de imágenes, la activación de la cuarentena y la firma de imágenes.

**Firmar imágenes**

Capacidad para firmar imágenes, que suelen estar asignadas a un proceso automatizado, lo que usaría una entidad de servicio. Este permiso suele combinarse con la inserción de imágenes para permitir insertar una imagen de confianza en un registro.

**Roles personalizados**

Como con otros recursos de Azure, puede crear roles personalizados con permisos específicos para Azure Container Registry. A continuación, asigne los roles personalizados a los usuarios, entidades de servicio u otras identidades que necesiten interactuar con un registro.

**Configure el cifrado de disco, Azure Disk Encryption (ADE), el cifrado como host y el cifrado de disco confidencial**

El cifrado en reposo es un requisito de seguridad habitual. En Azure, las organizaciones pueden cifrar datos en reposo sin el riesgo o el costo de una solución de administración de claves personalizada. Las organizaciones tienen la opción de permitir a Azure administrar completamente el cifrado en reposo. Además, las organizaciones tienen varias opciones para administrar con detenimiento el cifrado y las claves de cifrado.

**¿Qué es el cifrado en reposo?**

El cifrado es la codificación segura de los datos usados para proteger la confidencialidad de la información. Los diseños del cifrado en reposo de Azure utilizan cifrado asimétrico para cifrar o descifrar rápidamente grandes cantidades de datos según un modelo conceptual sencillo:

* Se usa una clave de cifrado simétrico para cifrar datos mientras se escriben en el almacenamiento.
* La misma clave de cifrado se utiliza para descifrar los datos tal y como se prepararon para su uso en la memoria.
* Se pueden particionar datos y se pueden usar claves diferentes para cada partición.
* Las claves deben almacenarse en una ubicación segura con el control de acceso basado en identidades y directivas de auditoría. Las claves de cifrado de datos que se almacenan fuera de ubicaciones seguras se cifran con una clave de cifrado de claves que se conserva en una ubicación segura.

En la práctica, los escenarios de control y administración de la clave, así como las convicciones de escala y disponibilidad, requieren construcciones adicionales. A continuación se describen los componentes y conceptos del cifrado en reposo de Microsoft Azure.

**Propósito del cifrado en reposo**

El cifrado en reposo proporciona protección de datos para los datos almacenados (en reposo). Los ataques contra los datos en reposo incluyen intentos de obtener acceso físico al hardware en el que se almacenan los datos y, a continuación, poner en peligro los datos contenidos. En este tipo de ataque, la unidad del disco duro de un servidor puede utilizarse de forma incorrecta durante el mantenimiento permitiendo a un atacante eliminar la unidad de disco duro. Más adelante el atacante tendría que poner el disco duro en un equipo bajo su control para intentar obtener acceso a los datos.

El cifrado en reposo está diseñado para evitar que el atacante obtenga acceso a los datos sin cifrar asegurándose de que los datos se cifran en el disco. Si un atacante obtiene una unidad de disco duro con datos cifrados pero no las claves de cifrado, el atacante debe anular el cifrado para leer los datos. Este ataque es mucho más complejo y consume más recursos que el acceso a datos no cifrados en una unidad de disco duro. Por este motivo, el cifrado en reposo es muy recomendable y es un requisito de alta prioridad para muchas organizaciones.

También se requiere el cifrado en reposo por necesidad de la organización de los esfuerzos de cumplimiento y gobierno de datos. Las normas gubernamentales y del sector, como HIPAA, PCI y FedRAMP, diseñan las medidas de seguridad específicas a través de los requisitos de cifrado y la protección de datos. El cifrado en reposo es una medida obligatoria necesaria para el cumplimiento de algunas de esas regulaciones. Para más información sobre el enfoque de Microsoft en relación con la validación de FIPS 140-2, consulte Publicación del estándar federal de procesamiento de información (FIPS) 140-2.

Además de satisfacer los requisitos de cumplimiento y regulatorios, el cifrado en reposo proporciona protección de defensa en profundidad. Microsoft Azure proporciona una plataforma compatible para servicios, aplicaciones y datos. También proporciona servicios completos y seguridad física, control de acceso a los datos y auditoría. Sin embargo, es importante proporcionar medidas de seguridad "superpuestas" adicionales en caso de que se produzca un error en una de las otras medidas de seguridad y el cifrado en reposo proporciona dicha medida de seguridad.

Microsoft se compromete con el cifrado en las opciones de reposo a través de servicios en la nube y proporcionando a los clientes el control de las claves de cifrado y los registros de uso de claves. Además, Microsoft está trabajando para conseguir cifrar todos los datos en reposo de los clientes de forma predeterminada.

**Componentes del cifrado en reposo de Azure**

Como se describe anteriormente, el objetivo del cifrado en reposo es que los datos que se guardan en el disco se cifren con una clave de cifrado secreta. Para lograr la creación de una clave segura para el objetivo, se debe proporcionar almacenamiento, control del acceso y administración de las claves del cifrado. Aunque los detalles pueden variar, las implementaciones del cifrado en reposo de los servicios de Azure se pueden describir en los términos en los que se ilustran en el diagrama siguiente.

**Azure Key Vault**

La ubicación del almacenamiento de las claves de cifrado y el control de acceso a esas claves es fundamental para un modelo de cifrado en reposo. Las claves deben ser muy seguras pero fáciles de administrar por parte de los usuarios especificados y deben estar disponibles para servicios concretos. Para los servicios de Azure, Azure Key Vault es la solución de almacenamiento de claves recomendada y proporciona una experiencia de administración habitual en los servicios. Las claves se almacenan y administran en los almacenes de claves, y se puede proporcionar acceso a Key Vault a los usuarios o servicios. Azure Key Vault admite la creación del cliente de claves o importación de claves de cliente para su uso en escenarios de clave de cifrado administrada por el cliente.

**Microsoft Entra ID**

Los permisos para usar las claves almacenadas en Azure Key Vault, además de para administrar o tener acceso a ellas para el cifrado en reposo y el descifrado, se pueden dar a las cuentas de Microsoft Entra.

**Cifrado de sobres con una jerarquía de claves**

Se usa más de una clave de cifrado en una implementación de cifrado en reposo. Almacenar una clave de cifrado en Azure Key Vault garantiza el acceso de clave segura y la administración central de claves. Sin embargo, el acceso local del servicio a las claves de cifrado es más eficaz para el cifrado y descifrado masivo que la interacción con Key Vault para cada operación de datos, lo que permite un cifrado más seguro y un mejor rendimiento. Si se limita el uso de una clave de cifrado única, se reduce el riesgo de que la clave se encuentre en peligro y el costo de volver a cifrar cuando se debe reemplazar una clave. Los modelos de cifrado en reposo de Azure usan el cifrado de sobres, donde una clave de cifrado de claves cifra una clave de cifrado de datos. Este modelo forma una jerarquía de claves que puede abordar mejor los requisitos de rendimiento y seguridad:

* **Clave de cifrado de datos (DEK)** : una clave AES256 simétrica que se usa para cifrar una partición o bloque de datos, a veces también se denomina simplemente Clave de datos. Un único recurso puede tener muchas particiones y muchas claves de cifrado de datos. Cifrar cada bloque de datos con una clave diferente dificulta los ataques de análisis criptográficos. Y mantener las DEK en el entorno local del servicio de cifrado y descifrado de datos maximiza el rendimiento.
* **Clave de cifrado de claves (KEK)** : una clave de cifrado que se usa para cifrar las claves de cifrado de datos mediante el cifrado de sobres, también conocida como ajuste. El uso de una clave de cifrado de claves que siempre permanece en Key Vault permite a las propias claves de cifrado de datos cifrarse y controlarse. La entidad que tiene acceso a la KEK puede ser diferente de aquella que necesita la DEK. Una entidad puede adaptar el acceso a la DEK para limitar el acceso de cada DEK a una partición específica. Como la KEK es necesaria para descifrar las DEK, los clientes pueden borrar criptográficamente las DEK y los datos si deshabilitan la KEK.

Los proveedores de recursos y las instancias de aplicación almacenan las claves de cifrado de datos cifradas como metadatos. Solo una entidad con acceso a la clave de cifrado de claves puede descifrar estas claves de cifrado de datos. Se admiten diferentes modelos de almacenamiento de claves.

**Cifrado en reposo en servicios en la nube de Microsoft**

Los Servicios en la nube de Microsoft se utilizan en los tres modelos de la nube: IaaS, PaaS, SaaS. A continuación encontrará ejemplos de cómo encajan en cada modelo:

* Servicios de software, que se conocen como software como servicio o SaaS, que tienen las aplicaciones proporcionadas por la nube, como Microsoft 365.
* Servicios de plataforma en los que los clientes usan la nube en sus aplicaciones para tareas como las de almacenamiento, análisis y funcionalidad de bus de servicio.
* Servicios de infraestructura o infraestructura como servicio (IaaS) en los que el cliente implementa sistemas operativos y aplicaciones que se hospedan en la nube y, posiblemente, saca provecho de otros servicios en la nube.

**Cifrado en reposo para clientes de SaaS**

Los clientes del software como servicio (SaaS) suelen tener el cifrado en reposo habilitado o disponible en cada servicio. Microsoft 365 dispone de varias opciones para que los clientes comprueben o habiliten el cifrado en reposo.

**Cifrado en reposo para clientes PaaS**

Los datos del cliente de la plataforma como servicio (PaaS) residen normalmente en un servicio de almacenamiento como Blob Storage, pero también pueden estar guardados en caché o almacenados en el entorno de ejecución de la aplicación, como una máquina virtual.

**Cifrado en reposo para clientes de IaaS**

Los clientes de la infraestructura como servicio (IaaS) pueden tener una variedad de servicios y aplicaciones en uso. Los servicios de IaaS pueden habilitar el cifrado en reposo en sus discos duros virtuales y máquinas virtuales que se hospedan en Azure mediante Azure Disk Encryption.

**Almacenamiento cifrado**

Al igual que PaaS, las soluciones IaaS pueden sacar provecho de otros servicios de Azure que almacenan los datos que se cifran en reposo. En estos casos, puede habilitar el cifrado en el soporte del cifrado en reposo como proporciona cada servicio consumido de Azure. La tabla Modelos de cifrado de datos: servicios compatibles enumera las principales plataformas de aplicación, servicios y almacenamiento y el modelo de cifrado en reposo admitido.

**Proceso cifrado**

Todos los discos, instantáneas e imágenes administrados están cifrados mediante Storage Service Encryption con una clave administrada por servicio. Una solución de cifrado en reposo más completa requiere que los datos no se conserven nunca en un formato no cifrado. Al procesar los datos en una máquina virtual, los datos se pueden conservar en el archivo de paginación de Windows o el archivo de intercambio de Linux, un archivo de volcado o en un registro de aplicaciones. Para asegurarse de que estos datos se cifran en reposo, las aplicaciones IaaS pueden usar Azure Disk Encryption en una máquina virtual de IaaS de Azure (Windows o Linux) y un disco virtual.

**Cifrado de datos en reposo personalizado**

Se recomienda que siempre que sea posible, las aplicaciones IaaS saquen provecho de las opciones de cifrado en reposo y Azure Disk Encryption proporcionadas por los servicios de Azure consumidos. En algunos casos, como requisitos de cifrado irregulares o almacenamiento que no se basa en Azure, un desarrollador de una aplicación de IaaS podría necesitar implementar el cifrado en reposo. Las soluciones de los desarrolladores de IaaS podrían integrarse mejor con las expectativas de administración y del cliente de Azure mediante el aprovechamiento de ciertos componentes de Azure. En concreto, los desarrolladores deben usar el servicio Azure Key Vault para proporcionar almacenamiento seguro de claves, así como proporcionar a sus clientes opciones de administración de claves coherentes con la mayoría de los servicios de la plataforma de Azure. Además, las soluciones personalizadas deben usar identidades de servicio administradas por Azure para permitir que las cuentas de servicio accedan a las claves de cifrado. Para encontrar información para desarrolladores sobre Azure Key Vault y las identidades de servicio administradas, consulte sus respectivos SDK.

**Compatibilidad con modelo de cifrado de proveedores de recursos de Azure**

Los servicios de Microsoft Azure admitir uno o más modelos de cifrado en reposo. Para algunos servicios, sin embargo, podrían no ser aplicables uno o varios de los modelos de cifrado. Para los servicios que admiten escenarios clave administrados por el cliente, puede que estos solo admitan un subconjunto de los tipos de clave que admite Azure Key Vault para las claves de cifrado de claves. Además, los servicios pueden liberar compatibilidad para estos escenarios y tipos de claves en distintas programaciones. Esta sección describe el soporte del cifrado en reposo en el momento de redactar este artículo para cada uno de los servicios de almacenamiento de datos principales de Azure.

**Azure Disk Encryption**

Cualquier cliente mediante las características de la infraestructura de Azure como servicio (IaaS) puede lograr el cifrado en reposo para sus discos y máquinas virtuales de IaaS y discos mediante Azure Disk Encryption.

**Almacenamiento de Azure**

Todos los servicios de Azure Storage (Blob Storage, Queue Storage, Table Storage y Azure Files) admiten el cifrado en reposo en el lado servidor; algunos servicios admiten además el cifrado de las claves administradas por el cliente y el cifrado del lado cliente.

* Lado servidor: de forma predeterminada, todos los servicios de Azure Storage admiten el cifrado en el lado servidor mediante claves administradas por el servicio, lo que es transparente para la aplicación. Para más información, consulte Cifrado del servicio Azure Storage para datos en reposo. Azure Blob Storage y Azure Files también admiten las claves RSA de 2048 bits administradas por el cliente en Azure Key Vault.
* Lado cliente: Azure Blobs, Tables y Queues admiten el cifrado en el lado cliente. Cuando se usa el cifrado del lado cliente, los clientes cifran los datos y los cargan como un blob cifrado. El cliente se encarga de la administración de claves.

**Azure SQL Database**

Azure SQL Database admite actualmente el cifrado en reposo para escenarios de cifrado en el lado cliente y en el lado servicio administrados por Microsoft.

Actualmente, la compatibilidad con el cifrado del servidor se proporciona a través de una característica de SQL denominada Cifrado de datos transparente. Una vez que un cliente de Azure SQL Database habilita la clave TDE, se crea y administra automáticamente para él. El cifrado en reposo puede habilitarse en los niveles de base de datos y servidor. Desde junio de 2017, el cifrado de datos transparente (TDE) se habilita de forma predeterminada en las bases de datos recién creadas. Azure SQL Database admite claves RSA de 2048 bits administradas por el cliente en Azure Key Vault.

Se admite el cifrado del lado cliente de los datos de Azure SQL Database a través de la característica Always Encrypted. Always Encrypted utiliza una clave que el cliente crea y almacena. Los clientes pueden almacenar la clave maestra en el almacén de certificados de Windows, Azure Key Vault, o un módulo de seguridad de hardware. Al usar SQL Server Management Studio, los usuarios de SQL eligen qué clave les gustaría usar para cifrar cada columna.

**Recomendar configuraciones de seguridad para Azure API Management**

La línea de base de seguridad de Azure para API Management aplica instrucciones de la versión 1.0 de Microsoft Cloud Security Benchmark a API Management. El punto de referencia de seguridad en la nube de Microsoft proporciona recomendaciones sobre cómo puede proteger sus soluciones de nube en Azure. El contenido se agrupa mediante los controles de seguridad definidos por el banco de pruebas de seguridad en la nube de Microsoft y las instrucciones relacionadas aplicables a API Management.

Puede supervisar esta línea de base de seguridad y sus recomendaciones mediante Microsoft Defender for Cloud. Azure Policy definiciones se enumerarán en la sección Cumplimiento normativo de la página del portal de Microsoft Defender for Cloud.

Cuando una característica tiene definiciones de Azure Policy pertinentes, se muestran en esta línea de base para ayudarle a medir el cumplimiento de los controles y recomendaciones de pruebas comparativas de seguridad en la nube de Microsoft. Algunas recomendaciones pueden requerir un plan de Microsoft Defender de pago para habilitar determinados escenarios de seguridad.

**Seguridad de las redes**

**NS-1: Establecimiento de límites de segmentación de red**

**Característica**: Integración de Virtual Network

**Descripción**: El servicio admite la implementación en la red virtual privada (VNet) del cliente.

**Guía de configuración**: implemente Azure API Management dentro de una instancia de Azure Virtual Network (VNET), por lo que puede acceder a los servicios de back-end dentro de la red. El portal para desarrolladores y la puerta de enlace de API Management pueden configurarse para que sean accesibles desde Internet (de forma externa) o solo dentro de la VNet (de forma interna).

* De forma externa: la puerta de enlace de API Management y el portal para desarrolladores son accesibles públicamente desde Internet con un equilibrador de carga externo. La puerta de enlace puede acceder a recursos dentro de la red virtual.  
  + Configuración de red virtual externa
* De forma interna: la puerta de enlace de API Management y el portal para desarrolladores solo son accesibles desde la red virtual con un equilibrador de carga interno. La puerta de enlace puede acceder a recursos dentro de la red virtual.
  + Configuración de red virtual interna

**Característica**: compatibilidad con grupos de seguridad de red

**Descripción**: El tráfico de red de servicio respeta la asignación de reglas grupos de seguridad de red en sus subredes.

**Guía de configuración**: implemente grupos de seguridad de red (NSG) en las subredes de API Management para restringir o supervisar el tráfico por puerto, protocolo, dirección IP de origen o dirección IP de destino. Cree reglas de NSG para restringir los puertos abiertos del servicio (por ejemplo, impedir que se acceda a los puertos de administración desde redes que no son de confianza). Tenga en cuenta que, de forma predeterminada, los NSG deniegan todo el tráfico entrante, pero permiten el tráfico desde la red virtual y las instancias de Azure Load Balancer.

**Precaución**

Al configurar un grupo de seguridad de red en la subred de API Management, hay un conjunto de puertos que deben estar abiertos. Si alguno de estos puertos no está disponible, es posible que API Management no funcione correctamente y sea inaccesible.

**NS-2: Servicios en la nube seguros con controles de red**

**Característica**: Azure Private Link

**Descripción**: funcionalidad de filtrado de IP nativa del servicio para filtrar el tráfico de red (no confundirse con NSG o Azure Firewall).

**Guía de configuración**: en los casos en los que no puede implementar instancias de API Management en una red virtual, debe implementar un punto de conexión privado para establecer un punto de acceso privado para esos recursos.

**Nota**

Para habilitar los puntos de conexión privados, la instancia de API Management ya no se puede configurar con una red virtual externa o interna. Una conexión de punto de conexión privado solo admite tráfico de entrada a la instancia de API Management.

**Característica**: deshabilitación del acceso de la red pública

**Descripción**: el servicio admite la deshabilitación del acceso a la red pública mediante el uso de una regla de filtrado de ACL de IP de nivel de servicio (no NSG o Azure Firewall) o mediante un modificador de alternancia "Deshabilitar acceso a red pública".

**Guía de configuración**: deshabilite el acceso a la red pública mediante la regla de filtrado de ACL de IP en los NSG asignados a las subredes del servicio o un conmutador de alternancia para el acceso a la red pública.

**Nota**

API Management admite implementaciones en una red virtual, así como el bloqueo de implementaciones no basadas en red con un punto de conexión privado y la deshabilitación del acceso a la red pública.

**Característica**: supervisión de Microsoft Defender for Cloud

Definiciones integradas de Azure Policy: Microsoft.ApiManagement:

| **Nombre (Azure Portal)** | **Descripción** | **Efectos** | **Versión (GitHub)** |
| --- | --- | --- | --- |
| Los servicios de API Management deben usar una red virtual | La implementación de Azure Virtual Network ofrece una seguridad y aislamiento mejorados, y permite colocar el servicio de API Management en una red enrutable sin conexión a Internet cuyo acceso puede controlar. Estas redes se pueden conectar a las redes locales mediante diversas tecnologías de VPN, lo que permite el acceso a los servicios de back-end dentro de la red o de forma local. El portal para desarrolladores y la puerta de enlace de API pueden configurarse para que sea accesible desde Internet o solo dentro de la red virtual. | Audit, Deny, Disabled | 1.0.2 |
| API Management debe deshabilitar el acceso de red pública a los puntos de conexión de configuración del servicio | Para mejorar la seguridad de los servicios de API Management, restrinja la conectividad a los puntos de conexión de configuración del servicio, como la API de administración directa de acceso, el punto de conexión de administración de configuración de Git o el punto de conexión de configuración de puertas de enlace autohospedadas. | AuditIfNotExists, Disabled | 1.0.1 |

**NS-6**: **implementación del firewall de aplicaciones web**

**Otras instrucciones para NS-6**: para proteger las API Web y HTTP esenciales, configure API Management dentro de una red virtual (VNET) en modo interno y configure una instancia de Azure Application Gateway. Application Gateway es un servicio PaaS. Actúa como un proxy inverso y proporciona equilibrio de carga L7, enrutamiento, firewall de aplicaciones web (WAF) y otros servicios. Más información.

La combinación de una instancia de API Management aprovisionada en una red virtual interna con el front-end de Application Gateway permite los siguientes escenarios:

* Uso de un único recurso de API Management para exponer todas las API a los consumidores internos y externos.
* Uso de un único recurso de API Management para exponer un subconjunto de API a los consumidores externos.
* Proporcionar una forma de activar y desactivar el acceso a API Management desde la red pública de Internet.

**Administración de identidades**

**IM-1: Uso de una identidad centralizada y un sistema de autenticación**

**Característica**: Autenticación de Azure AD necesaria para el acceso al plano de datos

**Descripción**: El servicio admite el uso de la autenticación de Azure AD para el acceso al plano de datos.

**Guía de configuración**: use Azure Active Directory (Azure AD) como método de autenticación predeterminado para API Management siempre que sea posible.

* Configure el portal para desarrolladores de Azure API Management a fin de autenticar las cuentas de desarrollador mediante Azure AD.
* Configure la instancia de Azure API Management para proteger las API mediante el protocolo OAuth 2.0 con Azure AD.

**Característica**: Métodos de autenticación local para el acceso al plano de datos

**Descripción**: métodos de autenticación local admitidos para el acceso al plano de datos, como un nombre de usuario y una contraseña locales.

**Notas de características**: evite el uso de métodos o cuentas de autenticación local, que deben deshabilitarse siempre que sea posible. En su lugar, use Azure AD para autenticarse siempre que sea posible.

**Guía de configuración**: restrinja el uso de métodos de autenticación local para el acceso al plano de datos, mantenga el inventario de las cuentas de usuario de API Management y concilie el acceso según sea necesario. En API Management, los desarrolladores son los usuarios de las API que se exponen en este servicio. De forma predeterminada, las cuentas de desarrollador recién creadas se encuentran en estado activo y se asocian al grupo de desarrolladores. Las cuentas de desarrollador que se encuentran en estado activo se pueden usar para acceder a todas las API para las que tienen suscripciones.

Además, las suscripciones de Azure API Management son un medio para proteger el acceso a las API y vienen con un par de claves de suscripción generadas que admiten la rotación.

En su lugar de usar otros métodos de autenticación, siempre que sea posible use Azure Active Directory (Azure AD) como método de autenticación predeterminado para controlar el acceso al plano de datos.

**IM-3: Administración de identidades de aplicaciones de forma segura y automática**

**Característica**: Identidades administradas

**Descripción**: Las acciones del plano de datos admiten la autenticación mediante identidades administradas.

**Guía de configuración**: use una identidad de servicio administrada generada por Azure Active Directory (Azure AD) para permitir a la instancia de API Management acceder de forma fácil y segura a otros recursos protegidos de Azure AD, como Azure Key Vault en lugar de usar entidades de servicio. La plataforma administra totalmente, rota y protege las credenciales de identidad administrada, lo que evita las credenciales codificadas de forma rígida en el código fuente o en los archivos de configuración.

**Característica**: entidades de servicio

**Descripción**: El plano de datos admite la autenticación mediante entidades de servicio.

**Guía de configuración**: no hay ninguna guía actual de Microsoft para esta configuración de características. Revise y determine si su organización quiere configurar esta característica de seguridad.

**IM-5: Uso del inicio de sesión único (SSO) para acceder a las aplicaciones**

**Otras instrucciones para IM-5**: Azure API Management puede configurarse para aprovechar Azure Active Directory (Azure AD) como proveedor de identidades a fin de autenticar a los usuarios en el portal para desarrolladores y beneficiarse de las funcionalidades de SSO que Azure AD ofrece. Una vez configurados, los nuevos usuarios del portal para desarrolladores pueden optar por seguir en primer lugar el proceso de registro integrado mediante la autenticación con Azure AD y, a continuación, completar el proceso de registro en el portal una vez autenticados.

Como alternativa, el proceso de inicio de sesión o registro se puede personalizar aún más mediante la delegación. La delegación le permite usar su sitio web actual para controlar el inicio de sesión y la suscripción de los desarrolladores, así como sus suscripciones a productos, en contraposición al uso de la funcionalidad integrada en el portal para desarrolladores. Permite que el sitio web sea propietario de los datos de usuario y realice la validación de estos pasos de forma personalizada.

**IM-7: Restricción del acceso a los recursos en función de las condiciones**

**Características**: Acceso condicional para el plano de datos

**Descripción**: el acceso al plano de datos se puede controlar mediante directivas de acceso condicional de Azure AD.

**Guía de configuración**: esta característica no se admite para proteger este servicio.

**IM-8: Restricción de la exposición de credenciales y secretos**

**Característica**: Integración y almacenamiento de credenciales y secretos de servicio en Azure Key Vault

**Descripción**: el plano de datos admite el uso nativo de Azure Key Vault para el almacén de credenciales y secretos.

**Guía de configuración**: configuración de la integración de API Management con Azure Key Vault. Asegúrese de que los secretos de API Management (valores con nombre) se almacenan en una instancia de Azure Key Vault para que se pueda acceder a ellos y se puedan actualizar de forma segura.

**Acceso con privilegios**

**PA-1: Separación y limitación de usuarios administrativos o con muchos privilegios**

**Característica**: cuentas de administrador local

**Descripción**: el servicio tiene el concepto de una cuenta administrativa local.

**Notas de características**: evite el uso de métodos o cuentas de autenticación local, que deben deshabilitarse siempre que sea posible. en su lugar, use Azure AD para autenticarse siempre que sea posible.

**Guía de configuración**: si no es necesario para las operaciones administrativas rutinarias, deshabilite o restrinja las cuentas de administrador local solo para uso de emergencia.

**Nota**

API Management permite la creación de una cuenta de usuario local. En lugar de crear estas cuentas locales, habilite solo la autenticación de Azure Active Directory (Azure AD) y asigne permisos a estas cuentas de Azure AD.

**PA-7: Seguimiento del principio de administración suficiente (privilegios mínimos)**

**Característica**: RBAC de Azure para el plano de datos

**Descripción**: el control de acceso basado en rol de Azure (RBAC de Azure) se puede usar para administrar el acceso a las acciones del plano de datos del servicio.

**Guía de configuración**: use el control de acceso basado en rol de Azure (RBAC de Azure) para controlar el acceso a Azure API Management. Azure API Management utiliza el control de acceso basado en roles de Azure para permitir que pueda hacerse una administración de acceso detallada en servicios y entidades de API Management (por ejemplo, API y directivas).

**PA-8: Determinación del proceso de acceso para soporte técnico a proveedores de nube**

**Característica**: caja de seguridad del cliente

**Descripción**: caja de seguridad del cliente se puede usar para el acceso de soporte técnico de Microsoft.

**Guía de configuración**: en escenarios de soporte técnico en los que Microsoft tenga que acceder a los datos, use Caja de seguridad del cliente para revisar y después aprobar o rechazar cada una de las solicitudes de acceso a datos de Microsoft.

**Protección de los datos**

**DP-1: detección, clasificación y etiquetado de datos confidenciales**

**Característica**: clasificación y detección de datos confidenciales

**Descripción**: las herramientas (como Azure Purview o Azure Information Protection) se pueden usar para la detección y clasificación de datos en el servicio.

**Guía de configuración**: esta característica no se admite para proteger este servicio.

**DP-2: Supervisión de anomalías y amenazas dirigidas a datos confidenciales**

**Característica**: prevención de pérdida o pérdida de datos

**Descripción**: Service admite la solución DLP para supervisar el movimiento de datos confidenciales (en el contenido del cliente).

**Guía de configuración**: esta característica no se admite para proteger este servicio.

**DP-3: Cifrado de datos confidenciales en tránsito**

**Característica**: cifrado de los datos en tránsito

**Descripción**: el servicio admite el cifrado de datos en tránsito para el plano de datos.

**Característica**: no se requieren configuraciones adicionales, ya que están habilitadas en una implementación predeterminada.

**Otras instrucciones para DP-3**: las llamadas del plano de administración se hacen mediante Azure Resource Manager con TLS. Se requiere un token web de JSON (JWT) válido. Las llamadas del plano de datos pueden estar protegidas con TLS y uno de los mecanismos de autenticación admitidos (por ejemplo, el certificado de cliente o JWT).

**DP-6: Uso de un proceso seguro de administración de claves**

**Característica**: administración de claves en Azure Key Vault

**Descripción**: el servicio admite la integración de Azure Key Vault para cualquier clave de cliente, secretos o certificados.

**Guía de configuración**: configuración de la integración de API Management con Azure Key Vault. Asegúrese de que las claves que API Management usa se almacenan en una instancia de Azure Key Vault para que se pueda acceder a ellas y se puedan actualizar de forma segura.

**DP-7: Uso de un proceso seguro de administración de certificados**

**Característica**: administración de certificados en Azure Key Vault

**Descripción**: el servicio admite la integración de Azure Key Vault para cualquier certificado de cliente.

**Guía de configuración**: configuración de la integración de API Management con Azure Key Vault. Asegúrese de que los secretos de API Management (valores con nombre) se almacenan en una instancia de Azure Key Vault para que se pueda acceder a ellos y se puedan actualizar de forma segura.

use Azure Key Vault para crear y controlar el ciclo de vida del certificado, incluida la creación, importación, rotación, revocación, almacenamiento y purga del certificado. Asegúrese de que la generación de certificados sigue los estándares definidos sin usar ninguna propiedad no segura, como: tamaño de clave insuficiente, período de validez excesivamente largo, criptografía no segura. Configure la rotación automática del certificado en Azure Key Vault y el servicio de Azure (si se admite) en función de una programación definida o cuando haya una expiración del certificado. Si no se admite la rotación automática en la aplicación, asegúrese de que siguen girando mediante métodos manuales en Azure Key Vault y la aplicación.

**Administración de recursos**

**AM-2: Uso exclusivo de los servicios aprobados**

**Característica**: compatibilidad con Azure Policy

**Descripción**: las configuraciones de servicio se pueden supervisar y aplicar a través de Azure Policy.

**Guía de configuración**: use Azure Policy integrado para supervisar y aplicar la configuración segura en los recursos de API Management. Use alias de Azure Policy en el espacio de nombres "Microsoft.ApiManagement" para crear definiciones de Azure Policy personalizadas cuando sea necesario.

**Registro y detección de amenazas**

**LT-1: Habilitación de las funcionalidades de detección de amenazas**

**Características**: Microsoft Defender para la oferta de servicio o producto

**Descripción**: el servicio tiene una solución específica de Microsoft Defender para supervisar y alertar sobre problemas de seguridad.

**Guía de configuración**: esta característica no se admite para proteger este servicio.

**LT-4: Habilitación del registro para la investigación de seguridad**

**Característica**: registros de recursos de Azure

**Descripción**: el servicio genera registros de recursos que pueden proporcionar métricas y registros específicos del servicio mejorados. El cliente puede configurar estos registros de recursos y enviarlos a su propio receptor de datos, como una cuenta de almacenamiento o un área de trabajo de Log Analytics.

**Guía de configuración**: habilite los registros de recursos para API Management. Los registros de recursos proporcionan información enriquecida sobre las operaciones y los errores que son importantes para fines de auditoría y solución de problemas. Entre las categorías de registros de recursos de API Management se incluyen las siguientes:

* GatewayLogs
* WebSocketConnectionLogs

**Copia de seguridad y recuperación**

**BR-1: Garantía de copias de seguridad automáticas periódicas**

**Característica**: Azure Backup

**Descripción**: el servicio de Azure Backup puede realizar una copia de seguridad del servicio.

**Guía de configuración**: esta característica no se admite para proteger este servicio.

**Característica**: funcionalidad de copia de seguridad nativa del servicio

**Descripción**: el servicio admite su propia funcionalidad de copia de seguridad nativa (si no usa Azure Backup).

**Guía adicional**: aproveche las funcionalidades de copia de seguridad y restauración en el servicio Azure API Management. Al aprovechar las funcionalidades de copia de seguridad, Azure API Management escribe copias de seguridad en las cuentas de Azure Storage propiedad del cliente. Azure API Management proporciona operaciones de copia de seguridad y restauración para realizar copias de seguridad y restauración completas del sistema.

**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. ¿Cuál es el propósito del cifrado en reposo en Microsoft Cloud Services?**

1. Para cifrar datos solo para clientes de Infraestructura como servicio (IaaS).
2. Para cifrar los datos en tránsito entre los servicios en la nube.
3. Permite la automatización y validación de la creación y el desmontaje de entornos para contribuir a ofrecer plataformas de hospedaje de aplicaciones seguras y estables.

**2. ¿Cuál es el propósito de integrar Microsoft Entra ID con clústeres de AKS?**

1. Proporcionar un control de acceso pormenorizado a los recursos de Azure.
2. Proporcionar administración de identidades para clústeres de Kubernetes.
3. Centralizar la administración de identidades y actualizar automáticamente el estado de la cuenta de usuario o grupo en el acceso al clúster de AKS.

**3. ¿Cuál es el propósito del control de acceso basado en roles de Azure (RBAC de Azure) en Azure Container Registry?**

1. Restringir el acceso a Azure Container Registry solo para los usuarios, no para las entidades de servicio.
2. Proporcionar acceso a todos los recursos de Azure para un usuario o entidad de servicio.
3. Para asignar permisos específicos a usuarios, entidades de servicio u otras identidades que necesiten interactuar con un registro.

**4. Una empresa usa Azure Container Instances para hospedar sus aplicaciones contenedorizadas. Quieren optimizar la configuración de recursos para sus grupos de contenedores. ¿Qué servicio de Azure puede proporcionar información sobre los recursos de proceso usados por sus instancias de contenedor y ayudar a determinar la mejor configuración de recursos?**

1. Azure Functions
2. Azure Logic Apps
3. Azure Monitor

**5. Un equipo administra un clúster multiinquilino en AKS y quiere aislar los recursos. ¿Qué característica de Kubernetes crea un límite de aislamiento lógico para las cargas de trabajo y los recursos?**

1. Presupuestos de interrupciones de pods
2. Cuotas de recursos
3. Espacio de nombres de Kubernetes
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, aprendió a planear e implementar medidas de seguridad avanzadas para recursos de proceso de Azure, incluyendo la habilitación del acceso remoto seguro mediante Azure Bastion y el acceso Just-In-Time (JIT), la configuración del aislamiento de red para Azure Kubernetes Service (AKS), la protección y supervisión de clústeres de AKS, la configuración de la autenticación y la supervisión de seguridad para instancias de contenedor y aplicaciones, la administración de acceso a Azure Container Registry (ACR), la implementación de estrategias de cifrado de disco, como Azure Disk Encryption (ADE) y el cifrado de disco confidencial, así como proporcionar recomendaciones para proteger Azure API Management.