Notas de la sesión 01

lunes, 15 de agosto de 2022

0:55

Comprobación de conocimientos

1. ¿Cuál de las siguientes características de las redes de Azure permite redirigir el tráfico de Internet de vuelta a los servidores locales de la empresa para realizar la inspección de los paquetes?

Rutas definidas por el usuario y tunelización forzada. Utilice la tunelización forzada para redirigir el tráfico enlazado a Internet de vuelta a la infraestructura local de la empresa. Por lo general, la tunelización forzada se utiliza en escenarios en los que las organizaciones quieren implementar la inspección de los paquetes o auditorías corporativas. La tunelización forzada en Azure se configura a través de rutas definidas por el usuario (UDR) de redes virtuales.

1. Al configurar Azure Firewall, la organización debe permitir el tráfico de Windows Update a través del firewall. ¿Cuál de las reglas siguientes se debe configurar?

Reglas de aplicación. Las reglas de aplicación definen los nombres de dominio completo (FQDN) a los que se puede acceder desde una subred. El uso de FQDN sería adecuado para permitir el tráfico de Windows Update.

1. Una organización quiere limitar el tráfico saliente de Internet desde una subred. ¿Qué producto se debe instalar y configurar?

Azure Firewall. Azure Firewall puede limitar las direcciones IP de salida y los puertos a los que se puede acceder. Defina reglas de red que asignen la dirección de origen, el protocolo, el puerto de destino y la dirección de destino.

1. Una organización tiene una aplicación web y le preocupan los ataques que desbordan el nivel de red con una cantidad considerable de tráfico aparentemente legítimo. ¿Qué se puede hacer para bloquear este tipo de ataque?

Cree una directiva de DDoS para proporcionar defensa contra los recursos de agotamiento. Por ejemplo, este agotamiento podría hacer que una aplicación no esté disponible para los usuarios legítimos.

Resumen

Detener un ataque en el perímetro es la manera más segura y rentable de proteger las soluciones de Azure. Azure proporciona varias herramientas de seguridad en el nivel perimetral para respaldar su negocio.

Debería poder:

* Definir la defensa en profundidad
* Proteger el entorno de ataque por denegación de servicio
* Proteger las soluciones con firewalls y VPN
* Explorar la configuración de la seguridad perimetral de un extremo a otro en función de la posición de seguridad

Notas de la sesión 02

Comprobación de conocimientos

1. Al implementar Azure Application Gateway con la necesidad de asegurarse de que las solicitudes entrantes se comprueban en busca de amenazas de seguridad comunes, como los scripts y los rastreadores entre sitios, ¿qué se puede hacer para abordar esta preocupación?

Instale Web Application Firewall. El firewall de aplicaciones web (WAF) es un componente opcional que controla las solicitudes entrantes antes de que lleguen a un agente de escucha. El firewall de aplicaciones web comprueba cada solicitud en busca de muchos riesgos comunes, según la Open Web Application Security Project (OWASP).

1. ¿Qué servicios siguientes son características de Azure Application Gateway?

Equilibrio de carga de capa 7, descarga de terminación SSL intensiva de la CPU, distribución round robin del tráfico entrante. Azure Application Gateway es una oferta virtual dedicada que suministra varias funcionalidades de equilibrio de carga de capa 7 para la aplicación. Permite a los clientes optimizar la productividad de la granja de servidores web mediante la descarga de la terminación SSL intensiva de la CPU a la puerta de enlace de la aplicación, la distribución round robin del tráfico entrante, la afinidad de la sesión basada en cookies, el enrutamiento basado en rutas de acceso URL y la capacidad de hospedar varios sitios web detrás de una única instancia de Application Gateway.

1. Una empresa está configurando un grupo de seguridad de red. Para configurar el grupo para permitir el tráfico desde orígenes públicos, ¿qué regla debe agregarse a las reglas predeterminadas?

Permita la entrada de Internet. Los NSG tienen reglas de entrada y salida predeterminadas. Hay una regla predeterminada para permitir la salida de Internet, pero no una regla para permitir la entrada de Internet.

1. Una organización tiene servidores web en distintas regiones y esta organización quiere optimizar la disponibilidad de los servidores. ¿Cuál es la seguridad de la red más adecuada para este fin?

Azure Front Door. Azure Front Door permite definir, administrar y supervisar el enrutamiento global para el tráfico web mediante la optimización del mejor rendimiento y la conmutación por error global instantánea para lograr una alta disponibilidad.

Resumen

La configuración y el mantenimiento de la seguridad de la red son fundamentales para una solución Azure segura. Use herramientas como grupos de seguridad de red o Front Door, entre otras, para controlar y bloquear el acceso a los datos.

Debería poder hacer lo siguiente:

* Implementación y configuración de grupos de seguridad de red para proteger las soluciones de Azure
* Configuración y bloqueo de puntos de conexión de servicio y vínculos privados
* Protección de las aplicaciones con Application Gateway, firewall de aplicaciones web y Front Door
* Configuración de ExpressRoute para ayudar a proteger el tráfico de red
* Explicación de cómo actúa la seguridad de red como una capa en una estrategia de defensa en profundidad.

Notas de la sesión 03

Comprobación de conocimientos

1. Una organización tiene una directiva de seguridad que prohíbe exponer puertos SSH al mundo exterior. Debe conectarse a una máquina virtual Linux de Azure para instalar el software. ¿Qué debería hacer?

Configurar el servicio Bastion. El servicio Azure Bastion proporciona una conexión RDP y SSH segura e ininterrumpida a las máquinas virtuales directamente en Azure Portal a través de SSL. Cuando se conecta a través de Azure Bastion, las máquinas virtuales no necesitan una dirección IP pública.

1. ¿Qué tipo de cifrado de disco se usa para los discos Linux?

DM-Crypt. Azure Disk Encryption es una funcionalidad que le permite cifrar los discos de máquina virtual IaaS Windows y Linux. Azure Disk Encryption utiliza la característica estándar del sector BitLocker de Windows y la característica DM-Crypt de Linux para proporcionar el cifrado del disco del sistema operativo y de datos para ayudar a proteger sus datos.

1. Una empresa, con máquinas virtuales locales y de Azure, debe asegurarse de que las máquinas virtuales se mantienen actualizadas con los parches de seguridad. Update Management es la herramienta de Azure que usarán, con suerte a un costo limitado. ¿Update Management supervisará las actualizaciones de sus máquinas virtuales?

Update Management en Azure Automation recopila y administra la información de actualización del sistema para máquinas virtuales Windows y Linux en Azure, máquinas virtuales físicas o en entornos locales, y otros entornos en la nube.

1. ¿Cuál de las siguientes recomendaciones de Security Center es una recomendación de gravedad media para máquinas virtuales y servidores?

Instalar una solución de protección de punto de conexión en máquinas virtuales. La instalación de la solución Endpoint Protection en máquinas virtuales es una recomendación de gravedad media.

1. ¿De qué ataques protege a las empresas el uso de estaciones de trabajo con privilegios de acceso?

Protege a los roles y las tareas administrativas de TI de alto impacto. Una estación de trabajo con privilegios de acceso protegería los roles administrativos de TI, al hacer que solo usen una máquina dedicada para el acceso.

Resumen

La seguridad del host es el proceso y la estrategia de bloquear las máquinas virtuales y sus discos, así como el acceso a ellas.

Debería poder:

* Configuración e implementación de Endpoint Protection
* Implementación de una estrategia de acceso con privilegios para dispositivos y estaciones de trabajo con privilegios
* Protección de las máquinas virtuales y acceso a ellas
* Implementación de Windows Defender
* Práctica de la seguridad por capas mediante la revisión e implementación de Security Center y pruebas comparativas de seguridad
* Configuración e implementación de Endpoint Protection
* Implementación de una estrategia de acceso con privilegios para dispositivos y estaciones de trabajo con privilegios
* Protección de las máquinas virtuales y acceso a ellas
* Implementación de Windows Defender
* Práctica de la seguridad por capas mediante la revisión e implementación de Security Center y pruebas comparativas de seguridad

Notas de la sesión 04

Comprobación de conocimientos

1. Para interactuar con las API de Azure, ¿cuál de las opciones siguientes requiere el clúster de Azure Kubernetes Service (AKS)?

Entidad de servicio de Azure AD. Entidad de servicio, identidad administrada. Para interactuar con las API de Azure, un clúster de AKS requiere una entidad de servicio de Azure Active Directory (AD) o una identidad administrada. Se necesita una entidad de servicio o una identidad administrada para crear y administrar dinámicamente otros recursos de Azure, como un equilibrador de carga de Azure o un registro de contenedor de Azure.

1. Cuando se Azure Kubernetes Service (AKS) y es necesario controlar el flujo de tráfico entre pods y bloquear el tráfico directamente a la aplicación back-end; ¿cuál es la mejor configuración?

Cree una directiva de red de AKS. El principio de privilegios mínimos debe aplicarse a la manera en que el tráfico puede fluir entre pods de un clúster de Azure Kubernetes Service (AKS). La característica Directiva de red de Kubernetes define reglas para el tráfico de entrada y salida entre los pods de un clúster.

1. La organización está definiendo reglas de RBAC para el equipo de seguridad de Azure Kubernetes. ¿Cuál es la mejor solución para conceder permisos en todo el clúster?

ClusterRole, ClusterRoleBinding. Los roles se usan para conceder permisos en un espacio de nombres. Para conceder permisos a todo el clúster, o bien a recursos de clúster fuera de un espacio de nombres concreto, use ClusterRole en su lugar. Una vez que se definan los roles para conceder permisos a los recursos, asigne esos permisos de RBAC de Kubernetes con RoleBinding. Los enlaces de roles se usan para asignar roles para un espacio de nombres determinado. Para enlazar roles en todo el clúster, o bien a recursos de clúster fuera de un espacio de nombres determinado, use en su lugar ClusterRoleBindings.

Resumen

Mantenga sus contenedores seguros para proteger las aplicaciones que se ejecutan en ellos utilizando Azure Container Registry para proporcionar sus contenedores y Azure Container Instances y Azure Kubernete Service para ejecutarlos y administrarlos.

Debería poder:

* Definir las herramientas de seguridad disponibles para contenedores en Azure
* Configurar la seguridad de contenedores y servicios de Kubernetes
* Bloquear los recursos de red, almacenamiento e identidad conectados a sus contenedores
* Implementar RBAC para controlar el acceso a los contenedores

Notas de la sesión 01

miércoles, 3 de agosto de 2022

9:20

Servicios de Balanceo de Carga de Azure

* Azure Load Balancer (Regional)
* Azure Front Door (Global)

Azure AD sirve para

* Sincronizar usuarios entre hibrido y nube
* Gestionar usuarios y sus permisos
* Crear grupos de usuarios
* Ramificaciones de usuarios
* Delegar y crear roles
* Autenticar y autenticación multifactor
* Detectar riesgos de inicio de sesión
* Identidad
* Autenticación de herramientas y aplicaciones

Todos los servicios de Microsoft usan Azure AD para autenticar a sus usuarios

ASG Aplications Segurity Groups (Grupos de aplicaciones seguras)

* Apila componentes virtuales (Maquinas o Redes Virtuales)
* Aplica directivas de seguridad (filtrado de red, ubicaciones prohibidas, etc)
* Herramienta de administración de seguridad

Servicios de Defensa Perimetral de Azure

* Azure Firewall
* Azure DDoS Protection

Contenedor

Espacio virtual que almacena todo lo necesario para correr una aplicación

Kubernetes

Administrador de Contenedores (Escalamiento)

PaaS (Plataforma como Servicio o Servicio basado en la Plataforma)

Tiene la responsabilidad en el acceso, programación y datos

La ubicación de las bases de datos se puede bloquear mediante Directivas de Azure e Iniciativas de Azure (las Iniciativas son un conjunto de Directivas), los Azure Blueprints permiten realizar acciones correctivas cuando no se ejecutan las Directivas o Iniciativas.

Las métricas son valores numéricos que describen algunos aspectos de un sistema en un momento dado

Comprobación de conocimientos

1. Los datos recopilados por Azure Monitor se pueden clasificar en dos tipos fundamentales. ¿Cuáles son esos tipos de datos?

Registros y métricas. Todos los datos recopilados por Azure Monitor pueden clasificarse como uno de los dos tipos fundamentales: métricas y registros. Las métricas son valores numéricos que describen algunos aspectos de un sistema en un momento dado. Las métricas son ligeras y capaces de admitir escenarios de tiempo casi real. Los registros contienen distintos tipos de datos organizados en registros con diferentes conjuntos de propiedades para cada tipo. Los datos de telemetría, como los eventos y los seguimientos, se almacenan como registros junto con los datos de rendimiento para poder analizarlos de forma combinada.

1. Al ejecutar una consulta del área de trabajo de Log Analytics, ¿qué lenguaje de consulta se usa?

Lenguaje de consulta de Kusto Todos los datos se recuperan de un área de trabajo de Log Analytics mediante una consulta de registro escrita en el lenguaje de consulta Kusto (KQL). Puede escribir sus propias consultas o usar soluciones e información que incluyan consultas de registro para una aplicación o servicio.

1. Para recibir una notificación cuando se elimine cualquier máquina virtual del grupo de recursos de producción, ¿qué se debe configurar?

Alerta de registro de actividad. Una alerta del registro de actividad para recibir notificaciones cuando se producen cambios específicos en los recursos de la suscripción de Azure.

1. A los administradores de TI les gustaría usar una herramienta de visualización para los resultados de Azure Monitor. Cada una de las siguientes opciones está disponible, pero es necesario elegir la que permitirá obtener información e investigar los datos. ¿Qué se deberá usar?

Las Métricas de supervisión de Monitor son una característica de Azure Monitor que recopila datos numéricos de recursos supervisados en una base de datos de serie temporal. Las métricas son valores numéricos que se recopilan a intervalos regulares y describen algún aspecto de un sistema en un momento determinado. Las métricas de Azure Monitor son ligeras y capaces de admitir escenarios casi en tiempo real, por lo que son útiles para la creación de alertas y la detección rápida de incidencias. Puede analizarlas de forma interactiva con el Explorador de métricas, recibir una notificación anticipada con una alerta cuando un valor cruce un umbral o visualizarlas en un libro o panel.

Resumen

La supervisión y el mantenimiento de las soluciones seguras de Azure Monitor son prácticas comunes y necesarias para proteger las soluciones y los datos.

Debería poder:

* Configurar y supervisar Azure Sentinel
* Definir las métricas y los registros de los que quiera realizar un seguimiento para las aplicaciones de Azure
* Conectar orígenes de datos a Log Analytics y configurar el servicio
* Crear y supervisar alertas asociadas a la seguridad de las soluciones

Notas de la sesión 02

Azure Monitor

* AMA (Azure Monitor Agent) para Máquinas Virtuales (VM Azure)
* Dependency Agent (Monitor en maquina local)
* Los registros se conservan por 93 días, para extender su duración enviarlos a Azure Storage

Área de Trabajo de Log Analytics

* Se implementa en Azure
* Log Analytics funciona de manera local con AWS (Amazon Web Services) y GC (Google Cloud)

Local Active Directory

Nube Azure Active Directory

Data Collection Rules del AMA

* Que? (Métricas o Registros "Logs")
* Donde? (Azure Monitor u Otro servicio)
* Quien? (de donde se va a recolectar, Máquina Virtual "VM", Grupo de Recursos "RG", App Service "AppS")

Microsoft Defender for Cloud

* Gratis (Puntuación de Seguridad y Recomendaciones de Seguridad)
* Estándar (Just in Time para Máquinas Virtuales "Jit for VM", Controles Adaptativos de la Red, Cumplimiento Normativo, Protección de la Carga de Trabajo, Firewall Manager, Reportes de Compliance)

Comprobación de conocimientos

1. ¿Cuál de las siguientes directivas no se incluye en el nivel gratuito de Microsoft Defender for Cloud?

Supervise recursos que no son de Azure. El nivel gratuito de Microsoft Defender for Cloud no admite la supervisión de recursos externos en la nube o que no sean de Azure, el acceso a máquinas virtuales JIT, los informes de cumplimiento normativo, las recomendaciones de seguridad de red adaptables ni muchas otras características.

1. Un grupo de cumplimiento de la organización requiere que la autenticación del cliente use Azure AD y que los registros de diagnóstico de Key Vault estén habilitados. ¿Cuál es la manera más fácil de hacerlo?

Implemente directivas Microsoft Defender for Cloud. Microsoft Defender for Cloud puede supervisar el cumplimiento de las directivas en todas las suscripciones mediante un conjunto predeterminado de directivas de seguridad. Las directivas de seguridad definen el conjunto de controles recomendados para los recursos de la suscripción o el grupo de recursos especificados.

1. Una organización está trabajando con una agencia externa que necesita acceder a una máquina virtual. Existe una preocupación real por los ataques de inicio de sesión por fuerza bruta dirigidos a los puertos de administración de máquinas virtuales. ¿Cuál de las siguientes opciones se puede usar para abrir los puertos de administración durante un intervalo de tiempo definido? Seleccione una.

Acceso Just-In-Time a la máquina virtual. Cuando se habilita el acceso Just-In-Time, Security Center usa las reglas del grupo de seguridad de red (NSG) para restringir el acceso a los puertos de administración cuando no están en uso con el fin de que no puedan ser el objetivo de los atacantes. Los puertos protegidos son los puertos SSH y RDP.

1. Al usar Microsoft Defender for Cloud para proporcionar visibilidad sobre la configuración de seguridad de las máquinas virtuales, el sistema de supervisión se puede configurar para enviar una notificación a los administradores cuando se detecten problemas. ¿Cuál de los siguientes problemas necesitará una herramienta de supervisión diferente para detectarlo?

Hay disponible una versión más reciente del sistema operativo. Microsoft Defender for Cloud no busca comprobar cuándo se lanza un nuevo sistema operativo. Microsoft Defender for Cloud examina la configuración del sistema operativo mediante un servicio de supervisión que instala en cada máquina virtual Windows y Linux. Además de las opciones anteriores, Microsoft Defender for Cloud puede proporcionar una evaluación de vulnerabilidades con recomendaciones de corrección.

Resumen

Mantener la seguridad con Microsoft Defender for Cloud y Puntuación de seguridad son las claves para mantener las soluciones y los datos seguros.

Debería poder:

* Definir los tipos más comunes de ciberataques (Fuerza Bruta y DDoS)
* Configuración de Microsoft Defender para la nube en función de la posición de seguridad
* Revisar la Puntuación de seguridad y elevarla
* Bloquear las soluciones mediante Security Center y Defender
* Habilitar el acceso Just-In-Time y otras características de seguridad

Comprobación de conocimientos

1. ¿Dónde se pueden crear y administrar alertas de seguridad personalizadas?

Azure Sentinel. Las reglas de alerta personalizadas se retiraron de Azure Security Center el 30 de junio de 2019 porque se retiró su infraestructura subyacente. Se recomienda habilitar Azure Sentinel y volver a crear allí las alertas personalizadas. Como alternativa, las alertas se pueden crear con alertas de registro de Azure Monitor.

1. ¿Cuál de los siguientes elementos superaría las funcionalidades de un cuaderno de estrategias de Azure Sentinel?

Se creará un cuaderno de estrategias de Sentinel para controlar varias suscripciones a la vez. Un cuaderno de estrategias de seguridad es una colección de procedimientos que se pueden ejecutar desde Azure Sentinel en respuesta a una alerta. Un cuaderno de estrategias de seguridad puede ayudar a automatizar y orquestar la respuesta y se puede ejecutar manualmente o establecer para ejecutarse automáticamente cuando se desencadenan alertas específicas.  Cada cuaderno de estrategias se crea para una suscripción específica.

1. Sentinel se usa para investigar un incidente. Al ver la información detallada del incidente, ¿qué valor se debe asignar, en lugar de incluirse en los datos?

Propietario de un incidente. La información detallada del incidente incluye su gravedad, el resumen del número de entidades implicadas, los eventos sin procesar que desencadenaron este incidente y el identificador único del incidente. Todos los incidentes se inician sin tener un propietario asignado. Cada incidente se puede asignar a un propietario estableciendo el campo Propietario del incidente. También se pueden agregar comentarios para que otros analistas puedan comprender lo que se investigó y cuáles son sus preocupaciones en torno al incidente.

1. Al crear roles dentro de un equipo de operaciones de seguridad para conceder el acceso adecuado a Azure Sentinel. ¿Cuál de los roles siguientes tendría que crearse en lugar de integrarse?

Propietario de Azure Sentinel. Los roles integrados de Sentinel son lector, respondedor y colaborador.

1. Un investigador quiere ser proactivo a la hora de buscar amenazas de seguridad. El responsable de seguridad ha leído sobre las funcionalidades de búsqueda y los cuadernos de Sentinel. ¿Qué es un cuaderno de Azure Sentinel?

Un cuaderno de estrategias paso a paso. Un cuaderno es un cuaderno de estrategias paso a paso que permite seguir los pasos de una investigación y búsqueda.  Otras técnicas de búsqueda se describen en las otras opciones: consulta integrada, marcadores y tablas de eventos.

Resumen

Microsoft Sentinel es la herramienta para buscar e investigar posibles infracciones en las soluciones de Azure.

Debería poder hacer lo siguiente:

* Explicación de qué es Microsoft Sentinel y cómo se usa
* Implementación de Microsoft Sentinel
* Conectar datos a Microsoft Sentinel, como registros de Azure, Azure AD y otros
* Realizar un seguimiento de incidentes mediante libros, cuadernos de estrategias y técnicas de búsqueda