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