Configuración de la seguridad de Azure Container Instances

Hay muchas recomendaciones de seguridad para Azure Container Instances, úselas para optimizar la seguridad de los contenedores.

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 autenticación basada en la entidad de servicio a través de Azure Active Directory para los flujos de autenticación básica. Esta autenticación incluye el acceso basado en roles para permisos de solo lectura (extracción), escritura (inserción) y otros.

Supervisión y examen continuos de 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 de Qualys integrado en Microsoft Defender for Cloud detecta vulnerabilidades de imagen, las clasifica y proporciona instrucciones de corrección.

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 rol 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.

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.

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.

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.

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 para la nube 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

---