

Administración de la seguridad para Azure Container Instances (ACI)

Azure Container Instances (ACI) es un servicio PaaS para cualquier escenario que pueda funcionar en contenedores aislados, incluidas las aplicaciones simples, la automatización de tareas y los trabajos de compilación. En aquellos escenarios donde se necesita una orquestación completa de contenedores, lo que incluye la detección de servicios en varios contenedores, el escalado automático y las actualizaciones de aplicaciones coordinadas, se recomienda Azure Kubernetes Service (se tratará más adelante en esta lección).

Características de ACI

Tiempos de inicio rápidos Los contenedores ofrecen importantes ventajas de inicio con respecto a las máquinas virtuales. Azure Container Instances puede iniciar un contenedor en Azure en segundos sin que sea necesario aprovisionar y administrar máquinas virtuales.

Acceso a contenedores

- Azure Container Instances permite exponer los grupos de contenedores directamente a Internet con una dirección IP y un nombre de dominio completo (FQDN). Al crear una instancia de contenedor, se puede especificar una etiqueta de nombre DNS personalizada, con el fin de que se pueda acceder a la aplicación en `customlabel.azurecontainer.io`.
- Azure Container Instances también admite la ejecución de comandos en un contenedor en ejecución, para lo que proporciona un shell interactivo que ayuda en el desarrollo y la solución de problemas de las aplicaciones. El acceso se realiza a través de HTTPS y se usa TLS para proteger las conexiones de cliente.

Implementación de contenedores

Implemente contenedores desde DockerHub o Azure Container Registry.

Seguridad a nivel de hipervisor Históricamente, los contenedores han ofrecido el aislamiento de las dependencias de las aplicaciones y gobernanza de los recursos, pero no se han considerado lo suficientemente reforzados para un uso hostil de varios inquilinos. Azure Container Instances garantiza que la aplicación está tan aislada en un contenedor como lo estaría en una máquina virtual.

Tamaños personalizados Normalmente, los contenedores están optimizados para ejecutar una sola aplicación, pero las necesidades exactas de esas aplicaciones pueden diferir considerablemente. Azure Container Instances proporciona un uso óptimo al permitir especificaciones exactas de los núcleos y la memoria de la CPU. El usuario paga según lo que necesita y se le factura por segundo, para que pueda optimizar con precisión los gastos según sus necesidades reales.

En el caso de los trabajos de proceso intensivo, como el aprendizaje automático, Azure Container Instances puede programar contenedores Linux para que utilicen los recursos de la GPU NVIDIA Tesla.

Almacenamiento persistente: para recuperar y conservar el estado con Azure Container Instances, se ofrece el montaje directo de los recursos compartidos de Azure Files de quienes Azure Storage ha hecho una copia de seguridad.

Facturación flexible

Admite facturación por GB, por CPU y por segundo.

Contenedores de Linux y Windows Azure Container Instances puede programar contenedores de Windows y Linux con la misma API. Simplemente especifique el tipo de sistema operativo al crear los grupos de contenedor.

Algunas características están restringidas actualmente a los contenedores Linux:

- Varios contenedores por grupo de contenedor
- Montaje del volumen (Azure Files, emptyDir, GitRepo, secreto)
- Métrica de uso de recursos con Azure Monitor
- Implementación de Virtual Network
- Recursos de GPU (versión preliminar)

En el caso de las implementaciones de contenedores de Windows, use imágenes basadas en imágenes base de Windows comunes.

Grupos de programación conjunta Azure Container Instances admite la programación de grupos con varios contenedores que comparten una máquina host, la red local, el almacenamiento y el ciclo de vida. Esto le permite combinar el contenedor de la aplicación principal con otros contenedores que actúan en una función auxiliar, como los patrones sidecar de registro.

Implementación de red virtual Actualmente disponible para cargas de trabajo de producción en un subconjunto de regiones de Azure, esta característica de Azure Container Instances permite la implementación de instancias de contenedor en una red virtual de Azure. Al implementar instancias de contenedor en una subred dentro de la red virtual, pueden comunicarse de forma segura con otros recursos de la red virtual, incluidos los que están en el entorno local (mediante VPN Gateway o ExpressRoute).