Habilitación de la autenticación de Azure Container Registry

Hay varias maneras de autenticar con un Azure Container Registry que se pueden aplicar a uno o más escenarios de uso de registros.

Entre los modos recomendados se incluyen la autenticación en un registro directamente mediante el inicio de sesión individual o los organizadores de contenedores y aplicaciones pueden realizar una autenticación desatendida, mediante la entidad de servicio de Azure Active Directory (Azure AD).

Opciones de autenticación

En la tabla siguiente se enumeran los métodos de autenticación disponibles y los escenarios recomendados.

Identidad

Escenario de uso

Detalles

Identidades de Azure AD, incluidos las entidades de servicio de usuarios y servicios

Inserción desatendida desde DevOps, extracción desatendida en Azure o servicios externos

Control de acceso basado en rol: Lector, Colaborador, Propietario

Identidad de AD individual

Inserción y extracción interactivas por parte de desarrolladores y evaluadores

Usuario administrador

Inserción y extracción interactivas por parte de desarrolladores y evaluadores individuales

Valor predeterminado: deshabilitado.

Inicio de sesión individual con Azure AD

Al trabajar directamente con el registro, como al extraer imágenes desde una estación de trabajo de desarrollo e insertarlas en ellas, autentíquese mediante el comando az acr login de la CLI de Azure. Al iniciar sesión con az acr login, la CLI usa el token creado al ejecutar az login para autenticar de forma fluida la sesión con el registro. Para completar el flujo de autenticación, Docker debe estar instalado y ejecutarse en el entorno. az acr login usa el cliente de Docker para establecer un token de Azure Active Directory en el archivo docker.config. Una vez que haya iniciado sesión de esta manera, las credenciales se almacenan en caché y los siguientes comandos de Docker de la sesión no requieren un nombre de usuario ni una contraseña.

Entidad de servicio

Si asigna una entidad de servicio en el Registro, la aplicación o el servicio pueden usarla para la autenticación desatendida. Las entidades de servicio permiten el acceso basado en roles a un registro, y puede asignar varias entidades de seguridad de servicio a un registro. Las distintas entidades de servicio le permiten definir un acceso diferente para distintas aplicaciones.

Los roles disponibles para un Registro de contenedor incluyen:

- AcrPull: incorporación de cambios
- AcrPush: incorporación y envío de cambios
- Propietario: extracción, inserción y asignación de roles a otros usuarios

Cuenta de administrador

Cada registro de contenedor incluye una cuenta de usuario administrador, que está deshabilitada de forma predeterminada. Puede habilitar el usuario administrador y administrar sus credenciales en Azure Portal, mediante la CLI de Azure o con otras herramientas de Azure. A la cuenta de administrador se le proporcionan dos contraseñas, y las dos se pueden regenerar. Las dos contraseñas le permiten mantener la conexión con el registro mediante una contraseña mientras se regenera la otra. Si la cuenta de administrador está habilitada, puede pasar el nombre de usuario y la contraseña al comando docker login cuando se le solicite autenticación básica en el registro.
