Roles, responsabilidades y permisos

En una organización, varios equipos trabajan juntos para asegurarse de que la carga de trabajo y la infraestructura de soporte sean seguras. Para evitar confusiones que puedan crear riesgos de seguridad, defina líneas claras de responsabilidad y separación de funciones.

Según la experiencia de Microsoft con muchos proyectos de adopción de la nube, establecer roles y responsabilidades claramente definidos para funciones específicas en Azure evitará confusiones que pueden generar errores humanos y de automatización que crean un riesgo de seguridad.

Líneas claras de responsabilidad

¿Los equipos tienen una visión clara de las responsabilidades y los niveles de acceso individual/grupal?

Designar a los responsables de funciones específicas en Azure.

Documentar y compartir claramente los contactos responsables de cada una de estas funciones creará coherencia y facilitará la comunicación. Según nuestra experiencia con muchos proyectos de adopción de la nube, esto evitará la confusión que puede generar errores humanos y de automatización que crean un riesgo de seguridad.

Designe grupos (o roles individuales) que serán responsables de las funciones clave

Rol grupal o individual	Responsabilidad
Seguridad de la red	*Equipo de seguridad de red normalmente existente.* Configuración y mantenimiento de Azure Firewall, Network Virtual Appliances (y enrutamiento asociado), Web Application Firewall (WAF), Network Security Groups, Application Security Groups (ASG) y otro tráfico entre redes.
Administración de redes	*Equipo de operaciones de red normalmente existente.* Asignación de subredes y redes virtuales en toda la empresa.
Seguridad de punto final del servidor	*Por lo general, operaciones de TI, seguridad o en forma conjunta.* Supervise y corrija la seguridad del servidor (parches, configuración, seguridad de punto final).
Supervisión y respuesta a incidentes	*Por lo general, el equipo de operaciones de seguridad.* Supervisión y respuesta a incidentes para investigar y corregir incidentes de seguridad en la gestión de eventos e información de seguridad (SIEM) o en la consola de origen, como Microsoft Defender para Cloud Azure AD Identity Protection.

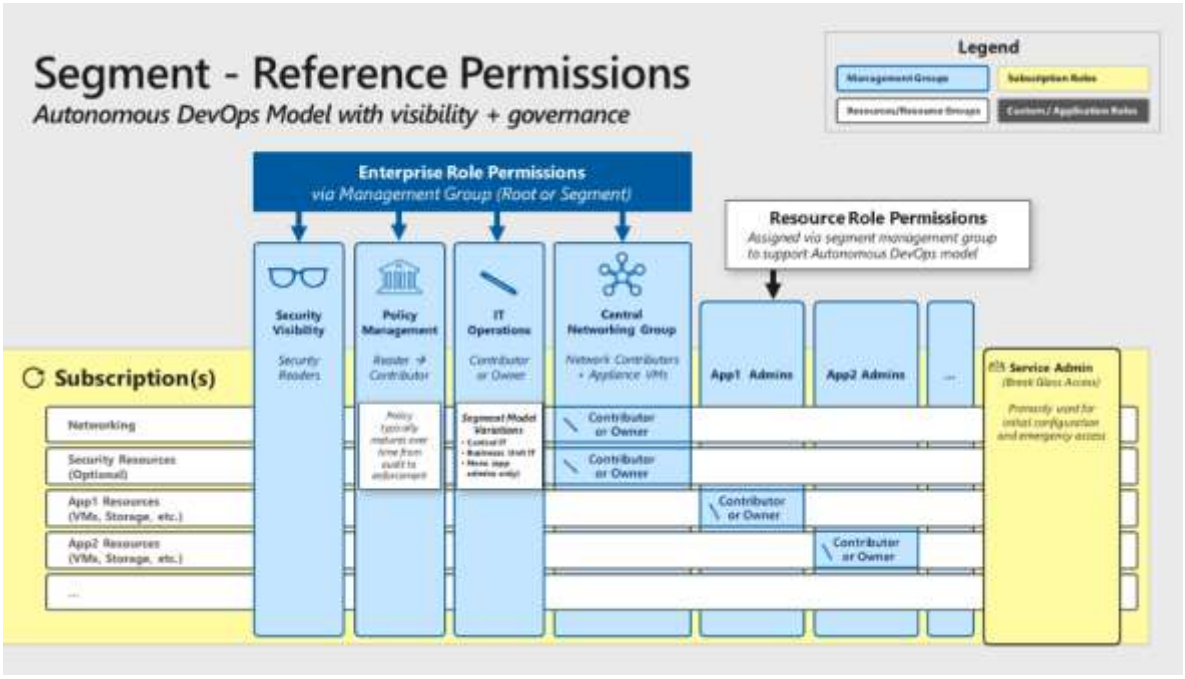
Rol grupal o individual	Responsabilidad
Gestión de políticas	*Típicamente equipo GRC + Arquitectura.* Aplicar la gobernanza basada en el análisis de riesgos y los requisitos de cumplimiento. Establezca la dirección para el uso del control de acceso basado en roles de Azure (Azure RBAC), Microsoft Defender para la nube, la estrategia de protección del administrador y la política de Azure para controlar los recursos de Azure.
Estándares y seguridad de identidad	*Normalmente, el Equipo de Seguridad + el Equipo de Identidad conjuntamente.* Establezca la dirección para los directorios de Azure AD, el uso de PIM/PAM, MFA, la configuración de contraseña/sincronización, los estándares de identidad de la aplicación.

Asignar permisos

Otorgue a los roles los permisos apropiados que comienzan con el privilegio mínimo y agregue más en función de sus necesidades operativas. Proporcione una guía clara a sus equipos técnicos que implementan permisos. Esta claridad hace que sea más fácil de detectar y corregir, lo que reduce los errores humanos, como el exceso de permisos.

- Asigne permisos en el grupo de administración para el segmento en lugar de las suscripciones individuales. Esto impulsará la consistencia y garantizará la aplicación a futuras suscripciones. En general, evite los permisos granulares y personalizados.
- Considere los roles integrados en Azure antes de crear roles personalizados para otorgar los permisos adecuados a las máquinas virtuales y otros objetos.
- **La pertenencia al grupo de administradores de seguridad** puede ser adecuada para equipos/organizaciones más pequeños donde los equipos de seguridad tienen amplias responsabilidades operativas.

Al asignar permisos para un segmento, tenga en cuenta la coherencia al tiempo que permite la flexibilidad para adaptarse a varios modelos organizativos. Estos modelos pueden variar desde un solo grupo de TI centralizado hasta equipos de TI y DevOps en su mayoría independientes.


Segment - Reference Permissions
Autonomous DevOps Model with visibility + governance
Legend
Enterprise Role Permissions
via Management Group (Root or Segment)
Resource Role Permissions
Assigned via segment management group
to support Autonomous DevOps model
Security Visibility
Security Readers
Policy Management
Reader → Contributor
IT Operations
Contributor or Owner
Central Networking Group
Network Contributors + Appliance VMs
App1 Admins
App2 Admins
...
Service Admin
(Break Glass Access)
Primarily used for initial configuration and emergency access
Subscription(s)
Networking
Security Resources (Optional)
App1 Resources (VMs, Storage, etc.)
App2 Resources (VMs, Storage, etc.)
...
Contributor or Owner
Contributor or Owner
Contributor or Owner
Contributor or Owner