Laboratorio 19

Imanol Muñiz Ramirez A0170713

¿En qué consiste el control de acceso basado en roles?

Es un mecanismo fundamental para gestionar y controlar el acceso a recursos en sistemas y aplicaciones. Consiste en asignar roles específicos a los usuarios y, a su vez, asigna permisos y privilegios a esos roles.

Tres Reglas Principales del RBAC:

* Asignación de Roles: Un usuario puede ejercer privilegios si se le ha asignado un rol.
* Autorización Basada en Roles: El rol de un usuario debe estar autorizado, lo que garantiza que solo pueda asumir roles para los que está autorizado.
* Autorización de Privilegios: Un usuario puede ejercer ciertos privilegios si está autorizado para hacerlo, según su autorización y asignación de roles.

Investiguen y describan 2 sistemas, uno que aplique RBAC y uno que no. Realicen un análisis de las ventajas y desventajas de cada uno con respecto al control de acceso.

Sistema con RBAC: Microsoft Azure:

Descripción:

* Azure RBAC es un sistema de autorización basado en Azure Resource Manager que permite administrar quién tiene acceso a los recursos de Azure, qué pueden hacer con esos recursos y a qué áreas pueden acceder.
* Permite asignar roles específicos a los usuarios según sus funciones laborales y otorgar permisos específicos a esos roles.

Ventajas:

* Eficiencia: Facilita la gestión de permisos al asignar roles en lugar de configurar permisos individuales para cada usuario.
* Visibilidad: Permite una visión clara de los permisos asignados a grupos de usuarios.
* Cumplimiento: Ayuda a cumplir con regulaciones y políticas de seguridad.

Desventajas:

* Complejidad: Configurar roles y permisos puede ser complejo en entornos grandes.
* Errores de Asignación: Si se asignan roles incorrectos, puede haber riesgos de seguridad.

Sistema sin RBAC: Listas de Control de Acceso (ACL):

Descripción:

* Las ACL son listas que especifican los permisos de acceso individuales para usuarios o grupos en recursos específicos.
* Cada recurso tiene una lista de usuarios autorizados y sus permisos.

Ventajas:

* Granularidad: Permite controlar permisos a nivel de usuario o grupo.
* Flexibilidad: Puede asignar permisos específicos a usuarios individuales.

Desventajas:

* Mantenimiento Intensivo: Requiere actualizaciones manuales para cada usuario o recurso.
* Complejidad Escalable: En entornos grandes, la gestión de ACL puede volverse complicada.

Source: Conversation with Copilot, 8/6/2024

(1) Control de acceso basado en funciones (RBAC). https://www.redhat.com/es/topics/security/what-is-role-based-access-control.

(2) RBAC vs ABAC: ¿Cuál elegir? - ingecom.net. https://www.ingecom.net/es/blog/320/rbac-vs-abac-cual-elegir/.

(3) ¿Qué es RBAC y cuándo debe usarlo?. https://es.linux-console.net/?p=7936.

(4) ¿Qué es el control de acceso basado en rol de Azure (RBAC)?. https://learn.microsoft.com/es-es/azure/role-based-access-control/overview.

(5) Control de acceso basado en roles (RBAC) ¿Qué es? - Grupo Atico34. https://protecciondatos-lopd.com/empresas/control-de-acceso-basado-en-roles-rbac/.

(6) Pros y Contras de Control De Acceso Basado En Roles. https://prosycontras.net/tecnologia/pros-y-contras-de-control-de-acceso-basado-en-roles/.

(7) RBAC - Role based access Control – Ratón de Biblioteca. https://www.ratondbiblioteca.com/role-based-access-control.

(8) ¿Qué es el control de acceso basado en roles (RBAC)? - Auth0. https://auth0.com/es/intro-to-iam/what-is-role-based-access-control-rbac.

(9) RBAC: ¿Qué es Role based access control? - IONOS MX. https://www.ionos.mx/digitalguide/servidores/seguridad/que-es-el-role-based-access-control-rbac/.

(10) ¿Qué es el control de acceso basado en roles? | Entrust. https://www.entrust.com/es/resources/learn/what-is-role-based-access-control.