

Laboratorio: Simulación de entorno seguro en Azure con Azure AD, RBAC y alertas de seguridad

Resumen ejecutivo

Este laboratorio simula la creación de un entorno seguro en la nube utilizando Microsoft Azure. El objetivo fue aplicar buenas prácticas de identidad y control de acceso mediante Azure Active Directory (Azure AD), el modelo de control basado en roles (RBAC) y la configuración de alertas automatizadas para eventos clave en la infraestructura virtual.

Objetivo del laboratorio

Diseñar y desplegar un entorno seguro en Azure mediante la gestión de identidades con Azure AD, la asignación de roles con RBAC y la implementación de alertas de seguridad usando Azure Monitor, sobre una máquina virtual con Windows Server.

Tecnologías y servicios utilizados

- Microsoft Azure
- Azure Active Directory (Azure AD)
- Control de acceso basado en roles (RBAC)
- Azure Monitor
- Network Security Groups (NSG)
- Máquina Virtual (Windows Server B1s)

Pasos principales del laboratorio

1. Creación de una máquina virtual Windows Server B1s dentro de los límites gratuitos de Azure.
2. Configuración de un Grupo de Seguridad de Red (NSG) para permitir RDP (puerto 3389) de forma segura.
3. Implementación de Azure Active Directory (Azure AD) con usuarios y grupos personalizados.
4. Asignación de roles RBAC para controlar accesos a nivel de suscripción o recurso.

- 5. Configuración de alertas desde Azure Monitor para detectar estados críticos como apagado inesperado de la VM.
- 6. Verificación de las alertas recibidas por correo electrónico y validación del comportamiento esperado.

Capturas de pantalla del laboratorio:

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure', 'Actualización', a search bar, and user information. Below the navigation bar, there's a section titled 'Servicios de Azure' with icons for 'Crear un recurso', 'Alertas', 'Máquinas virtuales', 'Grupos de seguridad de...', 'Azure Monitor para solucion...', 'Grupos de recursos', 'Microsoft Entra', 'Centro de inicio rápido', 'Azure AI services', and 'Más servicios'. Below this, there's a 'Recursos' section with tabs for 'Reciente' and 'Favorito'. The 'Reciente' tab is active, showing a table of resources.

Nombre	Tipo	Última consulta
Azure subscription 1	Suscripción	hace unos segundos
vm-demo	Máquina virtual	hace 26 minutos
demo-alerta	Regla de alertas del registro de actividad	hace 34 minutos
vm-demo-nsg	Grupo de seguridad de red	hace 57 minutos
nsg-demo	Grupo de seguridad de red	hace 59 minutos
NetworkWatcherRG	Grupo de recursos	hace 60 minutos
rg-seguridad-demo	Grupo de recursos	hace 1 hora

At the bottom of the resources list, there's a 'Ver todo' link. Below the resources section, there's a 'Navegar' section.

The screenshot shows the details page for a virtual machine named 'vm-demo'. The page has a left sidebar with navigation options like 'Inicio', 'Información general', 'Registro de actividad', 'Control de acceso (IAM)', 'Etiquetas', 'Diagnosticar y solucionar problemas', 'Visualizador de recursos', 'Conectar', 'Redes', 'Configuración de red', 'Equilibrio de carga', 'Grupos de seguridad de la aplicación', 'Administrador de red', 'Configuración', 'Disponibilidad y escala', 'Seguridad', and 'Copia de seguridad y recuperación'. The main content area is divided into several sections: 'Propiedades', 'Supervisión', 'Funcionalidades (7)', 'Recomendaciones', and 'Tutoriales'. The 'Propiedades' section is active, showing details about the virtual machine.

Máquina virtual	
Nombre del equipo	vm-demo
Sistema operativo	Linux
Generación de VM	V2
Arquitectura de VM	x64
Hibernación	Deshabilitado
Grupo host	-
Host	-
Grupo con ubicación por proximidad	-
Estado de ubicación	N/D
Grupo de reserva de capacidad	-
Tipo de controladora de disco	SCSI

Redes	
Dirección IP pública	172.172.141.152 (Interfaz de red vm-demo277)
Dirección IP pública (IPv6)	-
Dirección IP privada	10.0.0.4
Dirección IP privada (IPv6)	-
Red virtual/subred	rv-demo/default
Nombre DNS	Configurar

Tamaño	
Tamaño	Standard B1s
vCPU	1
RAM	1 GiB

Detalles de la imagen de origen	
Publisher de la imagen de origen	canonical
Oferta de la imagen de origen	0001-com-ubuntu-server-jammy

At the bottom of the page, there's a section for 'Azure de acceso puntual'.

Microsoft AzureActualización

Buscar recursos, servicios y documentos (G+/)

Copilot

alexis.g.g@hotmail.comDIRECTORIO PREDETERMINADO...

Inicio > vm-demo

vm-demo | Configuración de red

Máquina virtual

Buscar

Información general
Registro de actividad
Control de acceso (IAM)
Etiquetas
Diagnosticar y solucionar problemas
Visualizador de recursos
Conectar
Redes
Configuración de red
Equilibrio de carga
Grupos de seguridad de la aplicación
Administrador de red
Configuración
Disponibilidad y escala

Reglas

Contraer todo

Grupo de seguridad de red vm-demo-nsg (conectado a networkInterface: vm-demo277)
Afecta a 0 subredes, 1 interfaces de red

Crear ACL del puerto

Buscar reglas

Origen == todoDestino == todoProtocolo == todoAcción == todo

Prioridad	Nombre	Puerto	Protocolo	Origen	Destino	Acción
Reglas de puerto de entrada (4)						
1000	Allow-RDP	22	TCP	Cualquiera	Cualquiera	Allow
65000	AllowVnetInBound	Cualquiera	Cualquiera	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Cualquiera	Cualquiera	AzureLoadBalancer	Cualquiera	Allow
65500	DenyAllInBound	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Deny
Reglas de puerto de salida (3)						

Microsoft AzureActualización

Buscar recursos, servicios y documentos (G+/)

Copilot

alexis.g.g@hotmail.comDIRECTORIO PREDETERMINADO...

Inicio > Directorio predeterminado | Información general

Administrar inquilinos

CrearActualizarColumnasConmutadorEliminarDejar el inquilinoConvertir en inquilino predeterminadoMás información¿Tiene algún comentario?

Inquilino actual: Directorio predeterminado

Buscar inquilinosAgregar filtros

Se muestran 1 de 1 resultados.

Nombre de la organización	Nombre de dominio	Tipo de inquilino	Id. de la organización	Agregar a Favori...
Directorio predeterminado (Predeterminado)	alexisgghotmail.onmicrosoft.com	Microsoft Entra ID	1faf772f-f362-4d96-95c2-d11f9c48f7e	★

Microsoft AzureActualización

Buscar recursos, servicios y documentos (G+/)

Copilot

alexis.g.g@hotmail.comDIRECTORIO PREDETERMINADO...

Inicio > Directorio predeterminado | Usuarios

Usuarios

Directorio predeterminado

Nuevo usuarioEditar (versión preliminar)EliminarDescargar usuariosOperaciones masivasActualizarAdministrar vistaMFA por usuario

Todos los usuarios

Registros de auditoría
Registros de inicio de sesión
Diagnosticar y solucionar problemas
Usuarios eliminados
Restablecimiento de contraseña
Configuración del usuario
Resultados de la operación masiva
Nueva solicitud de soporte técnico

BúsquedaAgregar filtro

3 usuarios encontrados

Nombre para mostrar	Nombre principal de usuario	Tipo de usuario	Sincr...	Identities	Nombre de la empresa	Tipo de c...
Jhon Gutierrez Guzman	alexis_g_g_hotmail.com#EXT#@alexisgghotmail.onmicr...	Miembro	No	MicrosoftAccount		
usuario.lectura	usuario.lectura@alexisgghotmail.onmicrosoft.com	Miembro	No	alexisgghotmail.onmicrosoft.com		
usuario.operador	usuario.operador@alexisgghotmail.onmicrosoft.com	Miembro	No	alexisgghotmail.onmicrosoft.com		

Microsoft Azure

Actualización

Buscar recursos, servicios y documentos (G+/)

Copilot

alexis.g.g@hotmail.com

DIRECTORIO PREDETERMINADO ...

Inicio > Directorio predeterminado | Usuarios > Usuarios > usuario.lectura

usuario.lectura | Roles asignados

Usuario

Buscar

+ Agregar asignaciones X Quitar asignaciones Actualizar ¿Tiene algún comentario?

Información general

Registros de auditoría

Registros de inicio de sesión

Diagnosticar y solucionar problemas

Atributos de seguridad personalizados

Roles asignados

Unidades administrativas

Grupos

Aplicaciones

Licencias

Dispositivos

Asignaciones de roles de Azure

Métodos de autenticación

Nueva solicitud de soporte técnico

Roles administrativos

Los roles administrativos pueden usarse para conceder acceso a Microsoft Entra ID y a otros servicios de Microsoft. [Más información](#)

Buscar por nombre o descripción Agregar filtros

Rol	Descripción	Nombre del recu...	Tipo de recurso	Ruta de acceso d...	Tipo
<input type="checkbox"/> Lectores de directorios	Se puede leer la información básica del directorio; normalmente se usa para conceder acceso de lectura al directorio a aplicaciones e invitados.	Directory	Organization	Directo	Integrado

Microsoft Azure

Actualización

Buscar recursos, servicios y documentos (G+/)

Copilot

alexis.g.g@hotmail.com

DIRECTORIO PREDETERMINADO ...

Todos los servicios > alerta-demo > rg-seguridad-demo

demo-alerta

Regla de alertas del registro de actividad

Buscar

Editar Deshabilitar Duplicar Eliminar Actualizar

Información general

Registro de actividad

Control de acceso (IAM)

Etiquetas

Diagnosticar y solucionar problemas

Historial

Visualizador de recursos

Configuración

Configuración de la regla de alertas

Automation

Ayuda

Essentials

Grupo de recursos (mover) : rg-seguridad-demo

Ubicación (mover) : Global

Suscripción (mover) : Azure subscription 1

Id. de suscripción : 9c8996b8-f2a0-48e4-a070-613b330a71cd

Etiquetas (editar) : Agregar etiquetas

Gravedad : 4 - Detallado

Descripción : demo-alerta

Vista JSON

Ámbito

Recurso Jerarquía

vm-demo Azure subscriptio... rg-seguridad-demo

Acciones

Nombre Contiene acciones

alerta-demo 1 Correo electrónico

Condición

Siempre que el registro de actividades tenga un evento con el valor Category="Administrative", Nombre de la operación="Iniciar máquina virtual"

Ver eventos en Azure Monitor: Activity Log

Agregue o quite favoritos presionando Ctrl+Shift+F

Resultado y aprendizajes

El laboratorio permitió comprender y aplicar conceptos fundamentales de seguridad en la nube con Azure, incluyendo identidad, control de acceso y monitoreo. Se obtuvo experiencia práctica con herramientas reales usadas en roles de seguridad y administración de sistemas en la nube.

Ing. Jhon Alexis Gutierrez Guzman

Lima, Peru 2025.