Comparativa de Servicios de Seguridad en la Nube

Diplomatura Universitaria en Ciberseguridad

2024

Docente: Alfredo Pardo

Estudiante:

Valentina Solange, Vispo.

Abstract

Se hizo una comparativa de dos ofertas de servicios de nube con enfoque en ciberseguridad: IBM Cloud y Red Hat OpenShift. IBM Cloud es un proveedor con una oferta amplia de servicios que apunta a tener un gran nivel de seguridad pero que en ciertos puntos tiene algunos fallos de gran riesgo, mientras que Red Hat OpenShift no es un proveedor completo, sino más bien una plataforma que ofrece una conexión agnóstica a múltiples proveedores Cloud, con los estándares de seguridad empresariales de Red Hat embebidos.

Teniendo en cuenta el resultado de lo estudiado, se recomienda utilizar el servicio brindado por Red Hat OpenShift, como complemento para alguno de los clouds mencionados en el curso (AWS, Google, Azure), de este modo, tenemos nuestras aplicaciones preparadas para desplegarse en cualquier proveedor de la nube con los estándares de seguridad ofrecidos por Red Hat.

Índice

Abstract 2
Índice 2
Introducción 3
Proveedores 3
Comparativa 3
Gestión de Identidades y Accesos 3
Red Hat OpenShift 4
IBM Cloud 4
Seguridad de Datos 5
Red Hat OpenShift 6
IBM Cloud 6
Cumplimiento, Normas de Seguridad y Mejores Practicas 6
OpenShift 6
IBM Cloud 7
Conclusión 7
Bibliografía 7
Otras fuentes de información 7

Introducción

Actualmente, existe una calcificación del mercado respecto a los proveedores de nube, con gigantes (AWS, Google Cloud, Azure, etc.) que acaparan gran parte del mercado, pero no significa que no exista competencia. Algunos competidores son recién llegados a esta industria, mientras que otros son empresas de larga trayectoria que intentan imponer su presencia en la nube.

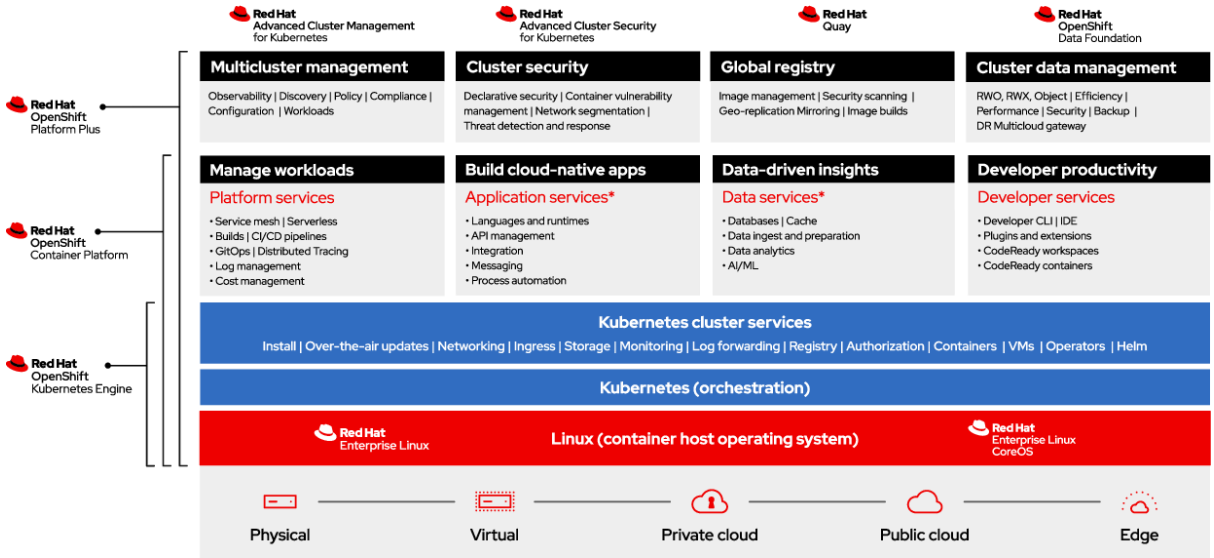
En este informe presentaremos una comparativa de dos ofertas de la nube que no vimos en el módulo, analizando sus perfiles, fortalezas y debilidades, enfocándonos en los pilares de ciberseguridad.

Es nuestro objetivo comparar el nivel, la granularidad, y la facilidad de entendimiento de los servicios de seguridad de estos proveedores, para ver si existe una mejora respecto a los proveedores que vimos en el módulo.

Proveedores

Los servicios elegidos son **IBM Cloud** y **Red Hat OpenShift**. IBM Cloud se eligió porque como empresa IBM tiene una larga trayectoria y ha sido muchas veces innovador en tecnología, por lo que es de interés ver como estos aspectos influyen en el producto final. IBM Cloud es un proveedor completo de nube, que incluye múltiples niveles de abstracción (IaaS, PaaS, y SaaS), y afirma ofrecer grandes estándares de seguridad.

En cuanto a Red Hat OpenShift, se eligió porque Red Hat es una organización que se dedica a realizar productos y servicios orientados a la seguridad específicamente para empresas, por lo que (de los proveedores menos conocidos) es el que a simple vista afirma ofrecer la mejor seguridad. OpenShift no es un proveedor de nube completo, sino más bien es una plataforma de aplicaciones en la nube a través de **contenedores** permitiendo optimizar las aplicaciones de manera que sean agnósticas a la infraestructura en la que estén. Red Hat OpenShift, o RHOS como será llamado de ahora en adelante, ofrece una manera sencilla para desplegar nuestras aplicaciones de manera multiplataforma o hibrido y agnóstico. RHOS soporta los tres proveedores que vimos en el módulo: AWS, Azure, Google Cloud, así como el otro proveedor que elegimos en este informe, IBM Cloud.



** Red Hat® OpenShift® includes supported runtimes for popular languages, /frameworks, and /databases. Additional capabilities listed are from the Red Hat Application Services and Red Hat Data Services portfolios.*

Comparativa

Gestión de Identidades y Accesos

IBM Cloud y RHOS tienen enfoques diferentes respecto a la Gestión de Identidad y Acceso (IAM), debido a sus respectivos enfoques y arquitecturas.

En resumen, RHOS tiene gestión por objetos denominada RBAC, mientras que IBM Cloud tiene una solución centralizada para administrar accesos a su amplio rango de servicios.

Red Hat OpenShift

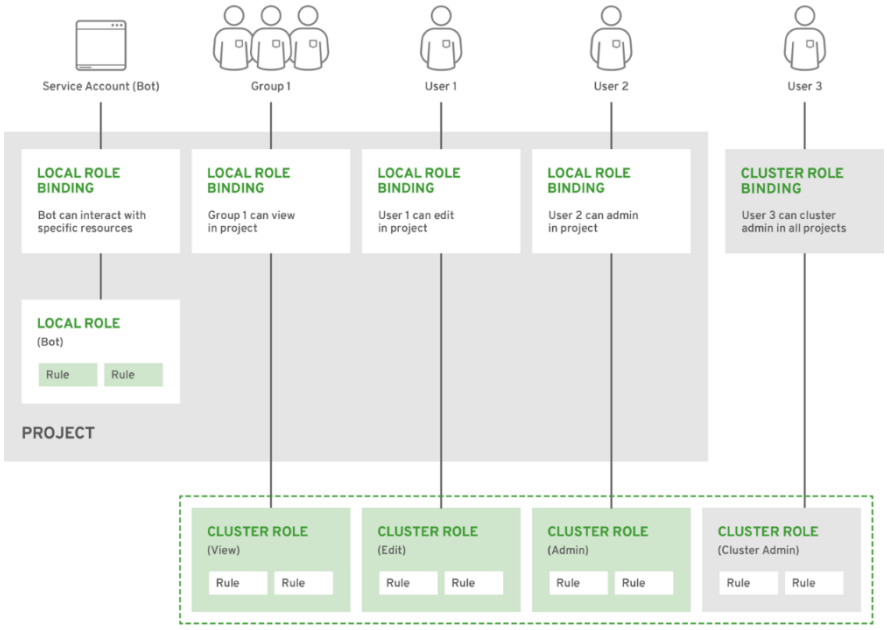
RHOS viene **preconfigurado** con servicios de autenticación y autorización, dividido en capas. La capa de **autenticación** asocia usuarios con las solicitudes a la API de la Plataforma de Contenedores, mientras que la capa de **autorización** utiliza información sobre el usuario solicitante para determinar si se permite la solicitud, si no está especificada, siempre deniega.

RHOS es una plataforma para aplicaciones contenerizadas **basada en Kubernetes**, por lo que utiliza el **Control de Acceso Basado en Roles** (RBAC) *nativo* de Kubernetes para gestionar el acceso a recursos dentro del clúster. En esta arquitectura los usuarios y aplicaciones obtienen permisos según los **roles** que posean, y los administradores tiene un gran nivel de granularidad respecto a la creación y control de estos roles.

RHOS se integra con varios proveedores de identidad (IdPs) como *LDAP*, *Active Directory* y *OAuth* para fines de autenticación. Permite a los administradores configurar mecanismos de autenticación según los requisitos de su organización. Además, OpenShift proporciona funciones para gestionar políticas de control de acceso, seguridad de red y cifrado para garantizar un acceso seguro a aplicaciones y datos dentro de la plataforma.

Los administradores pueden **definir permisos** y asignarlos a roles, y pueden controlar el acceso a través de proyectos, espacios de nombres y Restricciones de Contexto de Seguridad (SCC).

- Roles a por proyecto llamados “locales”.
- Roles “cluster-wide" que aplican a todos los proyectos.
- Acceso denegado por default.
- Tiene usuarios por default: *admin, basic-user, cluster-admin, cluster-status, cluster-reader, edit, self-provisioner* y *view*.



IBM Cloud

En cuanto a este proveedor, el manejo de identidad y acceso (IAM) es un **sistema centralizado** de gestión de identidades que proporciona capacidades de autenticación, autorización y gestión de usuarios.

Como IBM tiene un rango amplio de servicios de nube (servidores virtuales, bases de datos, almacenamiento, entre otros), admite varios métodos de autenticación, que incluye el básico **usuario/contraseña, API Keys y autenticación multifactor** (*MFA*), para mejorar la seguridad.

IBM Cloud IAM también se integra con proveedores de identidad empresariales (*IdPs*) como *Active Directory, LDAP, SAML*, y *SSO*.

Además, IBM Cloud IAM proporciona registros de auditoría y capacidades de monitorización para rastrear la actividad de los usuarios y garantizar el cumplimiento de las políticas de seguridad.

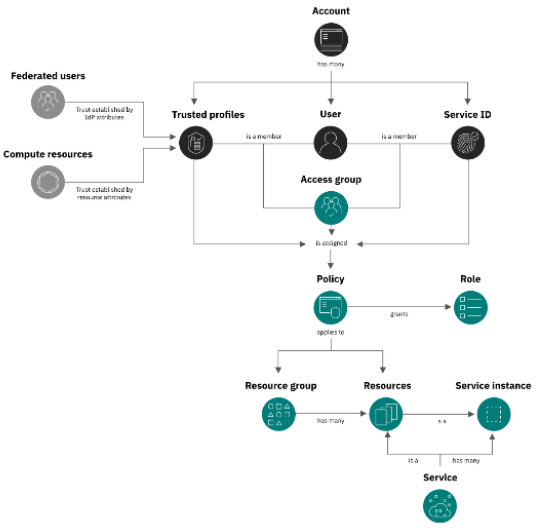
Parte de la infraestructura de IBM Cloud proviene de una empresa previa, Bluemix, adquirida por IBM, por lo que tiene aspectos de legado que hoy no consideraríamos seguros, y en la gestión de identidad y accesos hay uno de estos ejemplos. IBM

Cloud tiene dos modalidades de infraestructura: la "*moderna*", que consiste en roles, grupos, y políticas, muy similar a la estructura de proveedores populares como AWS, que hemos visto en el curso, y una "*clásica*", que otorga permisos en bloque por cuatro categorías. Antes de explorar la propuesta moderna, daremos una vista de esta estructura "clásica" y por qué puede ser insegura. Las categorías son: **Cuenta**, **Dispositivos**, **Red**, y **Servicios.** Y cada una otorga todos los permisos que cubren esos temas:

Cuenta	Dispositivos	Red	Servicios
Agregar y actualizar almacenamiento (storage). Administrar usuarios. Agregar y actualizar servicios. Agregar servidores.	Actualizar servidores. Manejar balanceadores de cargar. **Manejar Firewalls.**	**Agregar direcciones IP.** Administración de VPN. Gateways de red. Grupos de seguridad. Manejar servicios privados de endpoints.	Actualizar servicios. **Administrar DNS.** **Administrar llaves SSH.** **Administrar certificados.**

El sistema clásico posee dos grandes problemas de seguridad para la cuenta. Primero es que los permisos no son granulares, aumenta la superficie de ataque del cliente dado que no permite manejar una parte del sistema sin otorgarle permisos excesivos. Por otro lado, es un *Single Point of Failure* con mucho poder, si una cuenta se vulnera puede tener grandes repercusiones para el cliente. El sistema moderno de identidades y acceso es más robusto, compartiendo muchas de las ofertas de los proveedores líderes del mercado:

- **Gestión de usuarios**: Puede organizar un grupo de usuarios en un grupo de acceso para hacer que asignar acceso a más de un usuario o ID de servicio a la vez sea una tarea rápida y fácil.
- **Control de acceso granular**
- **Grupos de acceso para una gestión simplificada del acceso**
- **Perfiles de confianza para eliminar la necesidad de gestionar credenciales**
    - Usuarios federados
    - Recursos informáticos
- Plantillas de IAM gestionadas por la empresa
- API Keys
- Service IDs
- **Autenticación multi-factor (MFA)**
- **Autorizaciones de servicio a servicio**
- Controles relacionados de gestión de acceso



Seguridad de Datos

Los datos deben siempre estar disponibles y accesibles para cuando sea necesario su uso, para ello es necesario contar con un respaldo, un buen rendimiento, seguridad y compatibilidad. Esto se forma por escalabilidad, disponibilidad, y recuperación ante desastres, privacidad de datos, historial para rastreo de accesos, entre otros.

Red Hat OpenShift

OpenShift tiene una serie de conexiones dentro de su entorno dedicado a la protección de datos con la API **OADP** (OpenShift APIs for Data Protection), que proveen los servicios clave para la seguridad de datos:

- Backups
- Puntos de restauración
- Protección de imágenes de los contenedores.

Como OpenShift es un sistema de contenedores, OADP proporciona APIs para hacer copias de seguridad y restaurar los recursos del clúster de OpenShift (archivos *yaml*), imágenes internas (snapshots) y datos de volumen persistente.

El sistema está basado en *Velero*, que es una API *Open Source* para protección de datos de sistemas de *Kubernetes*. El sistema tiene cifrado fuerte, y ofrece opcionalmente módulos de cifrado compatibles con **FIPS 140-2 Nivel 1**.

IBM Cloud

Este proveedor unifica las copias de seguridad y recuperación de la carga de trabajo, proporcionando protección de los datos críticos de los clientes frente al ransomware y otras amenazas a la seguridad de los datos. IBM tiene un sistema de detección activa que continuamente supervisa las instancias por accesos mientras que otro sistema, *Safeguarded Copy*, maneja la copia de seguridad.

IBM Cloud también tiene un sistema llamado *Hyper Protect* y *Secure Execution* para sus servicios de computación y datos sensibles en las bases de datos como servicio (DBaaS). “Hyper Protect” es un sistema altamente aislado de contenedores que existe para desplegar trabajos sensibles. “Secure execution” utiliza funciones de seguridad de Linux para ejecución aislada. IBM Cloud afirma tener niveles de seguridad de estándar **FIPS 140-2 Nivel 4**.

Cumplimiento, Normas de Seguridad y Mejores Practicas

El cumplimiento de los estándares es una de las mejores formas que tiene una empresa para generar confianza en su producto. Estas mejores prácticas son desarrolladas, estudiadas, y probadas rigurosamente por los mejores especialistas de la industria, por lo que su cumplimiento es sinónimo de un producto de buena calidad, confiable y seguro. Incluso, en muchos casos esta práctica viene con beneficios externos en la forma de inmunidad o disminución a demandas, multas, y otros beneficios puestos en lugar para incentivar su uso, mientras que su incumplimiento acarrea perdida reputacional, pérdidas económicas y limitaciones operacionales.

OpenShift

Red Hat ofrece una herramienta llamada **Compliance Operator**, que permite a los administradores del producto a definir el nivel de cumplimiento de estándares que desean tener. OpenShift sigue el estándar **OpenSCAP**, desarrollado por el NIST, que define distintos estándares de seguridad y cumplimiento dentro de Estados Unidos. Este nivel de cumplimiento es granular al nivel clúster, por lo que algunos componentes más sensibles pueden tener una seguridad más estricta que otros menos críticos.

Estándares Generales	Estándares de Industria
International Organization for Standardization (ISO) 27000 Series	Payment Card Industry Security Council’s Data Security Standard (PCI-DSS)
Various National Institute of Standards and Technology (NIST) frameworks	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
General Data Protection Regulation (GDPR)	Federal Risk and Authorization Management Program (FedRAMP)
California Consumer Privacy Act (CCPA)	Family Educational Rights and Privacy Act (FERPA)
Various Center for Internet Security (CIS) Benchmarks	Federal Information Security Modernization Act (FISMA)
Systems and Organization Controls (SOC) 2 (Type 1 & 2)	

En cuanto a otras buenas prácticas respecto a la seguridad, vale la pena repetir que OpenShift está basado en Kubernetes, que de momento es el estándar abierto y más estudiado para la automatización de despliegue, escalamiento, y manejo de aplicaciones de contenedores.

IBM Cloud

En cuanto a IBM Cloud, ofrece una gran catalogo para de programas de cumplimiento soportados por sus productos. Como IBM compite contra AWS, Google Cloud, y Azure, su oferta cubre todos los estándares. Entre ellos podemos destacar que cumple con los estándares actualizados de:

- **CIS** (Centro de Seguridad en Internet)
- **FISMA** (Federal Information Security Management Act 2002), un acta de cumplimiento de estándares de alta seguridad del nivel federal de Estados Unidos.
- **ISO 31000**
- **SOC 1, 2, y 3** (Service Organization Control)
- **PCI DSS**, para Empresas Fintech que manejen información de tarjetas de crédito
- entre otras.

Con esta lista de estándares verificados por terceros, es claro que IBM Cloud sigue los estándares de la industria y tiene la seguridad como base fundamental de su servicio.

Conclusión

La propuesta de OpenShift es atractiva desde el punto de vista de seguridad y multi-nube, ya que ofrece una capa de seguridad que es el foco del producto con los estándares de la industria, y a su vez tener el mayor ***uptime*** posible para evitar el ***vendor lock-in***, dado que se puede desplegar la misma aplicación en diferentes proveedores, aunque esto junto con usar dos o más servicios de Cloud implique un costo mayor.

IBM Cloud es un proveedor que pretende competir con los más populares del mercado, y aunque tiene puntos de preocupación, parece estar a un nivel aceptable de seguridad y cumplir múltiples estándares. También cabe mencionar que, dentro de la oferta del producto, IBM menciona y sugiere el uso de OpenShift como capa de seguridad. La combinación de estos productos ofrecería un nivel bueno de protección en la nube.

Se recomienda utilizar los clouds analizados en clase con Openshift para una mayor capa de protección, siempre que se cuente con el capital necesario para capacitar al personal encargado de realizar la configuración y mantenimiento del sistema.

Bibliografía

Cómo funciona IBM Cloud IAM. https://cloud.ibm.com/docs/account?topic=account-iamoverview
Managing classic infrastructure access. https://cloud.ibm.com/docs/account?topic=account-mngclassicinfra
IBM Cloud Productos. https://www.ibm.com/ar-es/products
IBM Cloud Hyper Protect Dbaas. https://www.ibm.com/es-es/products/hyper-protect-dbaas
Soluciones de copia de seguridad y recuperación de datos de almacenamiento. https://www.ibm.com/es-es/backup-recovery?lnk=flatitem
Soluciones de seguridad zero trust. https://www.ibm.com/es-es/zero-trust?lnk=flatitem
IBM Security Verify Access Management. https://www.ibm.com/es-es/products/verify-identity
IBM Security Verify Privilege. https://www.ibm.com/es-es/products/verify-privilege
Soluciones de seguridad y protección de datos. https://www.ibm.com/es-es/data-security?lnk=flatitem
openshift-docs. https://github.com/openshift/openshift-docs
Managing Role-based Access Control (RBAC). https://docs.openshift.com/container-platform/3.11/admin_guide/manage_rbac.html
Official, tecnologías soportadas nativamente en OpenShift. https://github.com/openshift/library/tree/master/official
Openshift, Platform overview. https://developers.redhat.com/products/openshift/overview
Red Hat OpenShift features and benefits.https://docs.okd.io/latest/authentication/managing-security-context-constraints.html
IBM Cloud Pak for Security, Seguridad conectada para un mundo híbrido y multinube. https://www.ibm.com/mx-es/products/cloud-pak-for-security
Red Hat OpenShift features and benefits. https://www.redhat.com/en/technologies/cloud-computing/openshift/features
Red Hat's hybrid cloud portfolio wins in TrustRadius Best Of 2023 Awards across multiple products. https://www.redhat.com/en/blog/red-hats-hybrid-cloud-portfolio-wins-trustradius-best-2023-awards-across-multiple-products
Sean Rickerd, Ajmal Kohgadai. 2023. A Guide to OpenShift Compliance Operator Best Practices. https://www.redhat.com/en/blog/a-guide-to-openshift-compliance-operator-best-practices
OKD 4. https://www.okd.io/#okd-4
Managing access to resources. https://cloud.ibm.com/docs/account?topic=account-groups&interface=ui
Setting up access groups. https://cloud.ibm.com/docs/account?topic=account-assign-access-resources&interface=ui
IBM Cloud® compliance programs. https://www.ibm.com/cloud/compliance

Otras fuentes de información
¿Qué es OPENSHIFT? (en 3 minutos) - Video Youtube
Red Hat OpenShift overview - Video Youtube