Gestión segura de los servicios públicos gracias a la nube de AWS

NTT DATA despliega una red de nodos de máxima protección conectada al sistema gerencial de un gran organismo estatal

Perfil del cliente

Una de las gerencias más importantes de los servicios públicos españoles necesitaba una solución técnica para la infraestructura de sistemas, computación y comunicaciones. El objetivo era poner en marcha un proyecto llave en mano de servicios de operación y gestión en cloud. Este sistema necesitaba un robusto sistema de protección para administrar la protección de datos y permitir reembolsos periódicos de ámbito estatal.

¿Por qué NTT DATA?

El equipo de NTT DATA tiene equipos especializados para productos de arquitectura cloud en AWS. La arquitectura de gestión de pagos de esta prestación se basa en nodos de computación y servicios de base de datos en la nube de AWS, conectados a los sistemas de la entidad pública. El equipo técnico de NTT Data extiende su estructura de contenedores OpenShift (OCP) para desarrollar microservicios en la aplicación e incorporar elementos de alta seguridad AWS Config y AWS Security Hub. Estos recursos se encargan de realizar un seguimiento de los cambios de configuración y activar los

> **“La robustez es esencial para dotar de eficacia a una infraestructura de datos personales y pagos digitales periódicos e instantáneos. Por ello, se crean 4 cuentas AWS: para alojar entornos no productivos; recursos de producción; comunicaciones externas y para unificar la seguridad y la información integral de todas las cuentas”**

Sumario de necesidades

- Este organismo público necesita automatizar procesos para facilitar el acceso de los ciudadanos a sus servicios y mejorar sus procedimientos de gestión.
- La nueva arquitectura digital debe arranca con la administración de una de sus prestaciones con mayor demanda de solicitudes online.
- La propuesta técnica debe facilitar la escalabilidad y flexibilidad de la aplicación, desplegar los máximos niveles de seguridad que se requieren para una institución del Estado y asegurar su vinculación a los sistemas de comunicación.
- Oferta de software, Landing Zone e infraestructura de la plataforma.
- La red se provisiona en una VPC (Nube Privada Virtual) con acceso restringido. Solo las personas autorizadas pueden acceder a la misma.

Sumario de soluciones

- La plataforma de gestión usa contenedores OCP, solución OpenSource estandarizada que proporciona dinamismo operativo y automatiza de forma uniforme los recursos desplegados.
- Este recurso aporta simplicidad, agiliza la concesión de permisos sobre comunicaciones y ofrece modelos de suscripción On-Prem y Cloud.
- Varias herramientas garantizan los estándares de protección:
- **AWS Certificate Manager (ACM):** certificados y claves.
- **Bucket S3**: servicio de almacenamiento.
- **KMS (Key Management Service):** creación y control de contraseñas.
- **GuardDuty**: detector de amenazas.
- **AWS Inspector**: búsqueda de fallas de seguridad.
- **AWS Security Hub,** cuya misión es comprobar el estado de segurida de los recursos de todas las cuentas

Necesidades

El diseño de la infraestructura de la prestación requiere el despliegue de varios elementos en cada cuenta AWS:

- Instalación de un modelo de presentación pública y acceso compatible con OpenShift.
- Red privada con balanceadores NLB.
- Clúster sobre la aplicación, esencial para que operen los contenedores y la base de datos Oracle.
- Zonas de disponibilidad y salida a Internet centralizadas en Network Shared Services y con conexión a sistemas OnPremise y a la Plataforma SaaS de Appian.

Sistemas de respaldo y recuperación

El desarrollo de los sistemas de respaldo (backup) de los distintos componentes (clúster y base de datos) se someten a pruebas de restauración y disponen de servicios AWS para almacenamiento de datos.

También incluye un Versionado S3 que permite guardar diferentes versiones cuando se modifica un fichero almacenado en S3.

Solución

El equipo de NTT DATA diseñó una solución conectando los sistemas de la organización con la nube de AWS, asentada sobre varios bloques principales:

- Cuenta Platform-Dev, que contiene el clúster para la Plataforma OCP.
- Network Shared alberga elementos de networking como Transit Gateway (TGW) para gestionar el tráfico de distintos componentes, aislar redes de diversos entornos y proporcionar salida a los sistemas On-Premise.
- Cuenta específica para eventuales crecimientos de datos futuros donde centralizar comunicaciones de diferentes cuentas.

Inspección y seguridad

La Cuenta Security centraliza la inspección de componentes de seguridad desplegados en las cuentas. Pero, además, se añaden otros recursos de protección.

- Appian dev (pre) para entornos de desarrollo de la Plataforma Appian -ofrecida en modo SaaS- gestiona el Case Management y a los tramitadores de las solicitudes de prestaciones.
- El túnel VPN Site to Site se encarga de securizar la conexión entre los sistemas en Nube y los On Premise.
- Las conexiones con terceras entidades de la Administración llegan mediante este túnel y se redirigen a la plataforma SARA, el Sistema de Aplicaciones y Redes para las Administraciones públicas.

Un proyecto llave en mano

Para filtrar todos los puntos de salida de tráfico desde las AWS VPC a Internet se procedió a instaurar el sistema Firewall de restricción de flujos en redes privadas

De igual modo, para publicar los servicios de acceso público (Internet) y de gestores y tramitadores (Intranet) se utilizan subdominios con nomenclatura oficial de la entidad estatal.

Beneficios

NTT Data ha permitido desarrollar exitosamente la estrategia de transición de automatización del proceso de prestaciones a la nube de AWS. La funcionalidad de la arquitectura en los nodos del clúster OpenShift Container Platform(OCP) que acogen las comunicaciones existentes.

La configuración de la red y los proyectos tiene en cuenta la gestión periódica y permanente de las reglas de comunicación dentro del clúster y el filtrado con etiquetas en el tráfico de aplicaciones. El control de usuarios se realiza con el estándar de autenticación (OAuth). Esto permite aumentar la seguridad de los accesos y automatizar tareas, aumentando la eficiencia.

Apliques propios de protección

OCP incluye una serie de medidas de seguridad out-of-the-box que restringen despliegues sobre la plataforma. De forma que todos los componentes del clúster se actualizan constantemente para evitar vulnerabilidades. Aumentando la dificultad para ataques de denegación de servicio.

Además, la instalación expresa del Compliance Operator permite detectar anomalías en los cumplimientos normativos y provee correcciones a los errores que se puedan revelar.

> “AWS Security Hub centraliza todos los registros de seguridad de las diferentes cuentas desplegadas en AWS.
> Así se recaba la información que corresponde a cada necesidad y se puede realizar el oportuno seguimiento para operar ante posibles reconfiguraciones en cualquiera de los servicios implementados en la cuenta”