[Publish] Security and Compliance

Este documento resume los servicios y controles de seguridad configurados como parte del despliegue del AWS Landing Zone Accelerator (LZA).
La configuración aplica las mejores prácticas alineadas con la Arquitectura de Referencia de Seguridad de AWS y estándares de la industria para seguridad en la nube, monitoreo y cumplimiento normativo.

Región Principal (Home Region)

Región Principal: `us-east-1`
Todos los servicios de seguridad centralizados y configuraciones de monitoreo se despliegan en la Región Principal, a menos que se indique lo contrario.

Configuración de Servicios de Seguridad Centralizados

El despliegue de AWS Landing Zone Accelerator incluye servicios de seguridad centralizados para ayudar a aplicar políticas de seguridad, gestionar riesgos y mejorar la visibilidad entre cuentas de AWS.
A continuación, se describe cada servicio de seguridad configurado:

Servicio	Estado	Descripción
Cuenta de Administración Delegada	Habilitado (Cuenta de Auditoría)	Se asigna una cuenta centralizada como administradora de servicios de seguridad en toda la Organización de AWS. Facilita la gestión centralizada de hallazgos y cumplimiento.
Cifrado por Defecto de Volúmenes EBS	Habilitado	Aplica cifrado por defecto a todos los nuevos volúmenes EBS de Amazon para proteger

		automáticamente los datos en reposo.
Reversión de Cambios en SCPs	Habilitado	Revierte automáticamente cambios no autorizados en las Políticas de Control de Servicios (SCPs) mediante notificaciones SNS.
AWS Macie	Deshabilitado (configurado)	Servicio basado en machine learning que detecta y protege datos sensibles en buckets S3. Puede activarse para monitorear PII y riesgos de seguridad.
Amazon GuardDuty	Deshabilitado	Servicio de detección de amenazas que monitorea actividades maliciosas. La protección de eventos S3 está preconfigurada, aunque GuardDuty está deshabilitado.
AWS Audit Manager	Deshabilitado	Simplifica la preparación de auditorías mediante la recopilación continua de evidencias. Está preconfigurado para exportar reportes a S3,

		pero no está en ejecución.
Amazon Detective	Deshabilitado	Ayuda a analizar e investigar automáticamente problemas de seguridad usando ML y análisis gráfico. Disponible para activación.
AWS Security Hub	Deshabilitado (estándares preconfigurados)	Proporciona una vista centralizada de alertas de seguridad y estado de cumplimiento. Estándares como FSBP, CIS y NIST están listos para activarse.
AWS Access Analyzer	Habilitado	Monitorea continuamente las políticas de recursos para detectar accesos no intencionados a buckets S3, roles IAM, claves KMS, entre otros.
Política de Contraseñas de IAM	Aplicada	Se aplican requisitos estrictos de contraseña (longitud mínima, complejidad, expiración y prevención de reutilización) en todas las cuentas.
Grabador de AWS Config	Habilitado	Captura cambios de configuración en los

		recursos de AWS para auditorías y seguimiento de cumplimiento. Grabación continua y canal de entrega activados.

Importancia de Estas Configuraciones

- **Cuenta Delegada:** Centraliza la administración y mejora el control en múltiples cuentas de AWS.
- **Cifrado EBS / Bloqueo S3:** Proporcionan protección básica de datos sin intervención manual de los desarrolladores.
- **Reversión de SCPs:** Mitiga rápidamente cambios no autorizados en controles de seguridad.
- **Macie, GuardDuty, Detective y Audit Manager:** Desactivados, pero listos para activarse según necesidades del negocio o regulaciones.
- **Security Hub:** Al activarse, proporciona una consola única para hallazgos de seguridad en todo AWS.
- **Access Analyzer:** Asegura que cualquier recurso compartido pública o entre cuentas sea monitoreada e intencional.
- **Política de Contraseñas:** Refuerza la seguridad entre usuarios y administradores.
- **AWS Config:** Proporciona historial detallado de cambios y soporte para auditoría y cumplimiento.

Puntos Clave

- Los servicios marcados como **Deshabilitados** están preconfigurados y se pueden habilitar fácilmente sin rediseñar el entorno.
- Los controles de seguridad fundamentales (cifrado, control de acceso, monitoreo de cumplimiento) ya están activos.
- Servicios de monitoreo (Config, Access Analyzer) garantizan cumplimiento y gobernanza continua entre entornos.

AWS Security Hub (Estándares Preconfigurados)

Aunque Security Hub está inicialmente deshabilitado, los siguientes estándares están preconfigurados y listos para activarse:

- **AWS Foundational Security Best Practices (FSBP) v1.0.0**
- **CIS AWS Foundations Benchmark v1.4.0**
- **NIST SP 800-53 Revisión 5**

Esto permite una activación sencilla con evaluación inmediata frente a marcos de cumplimiento reconocidos.

Política de Contraseñas de IAM

Se aplica la siguiente política de contraseñas fuertes en todos los usuarios:

Configuración	Valor
Permitir a los usuarios cambiar contraseña	Sí
Expiración forzosa	No
Requiere mayúsculas	Sí
Requiere minúsculas	Sí
Requiere símbolos	Sí
Requiere números	Sí
Longitud mínima	14 caracteres
Prevención de reutilización	24 contraseñas anteriores
Edad máxima de la contraseña	90 días

Reglas de AWS Config

AWS Config está habilitado para evaluar continuamente configuraciones de recursos según las mejores prácticas de seguridad.
Las siguientes reglas están aplicadas:

Nombre de Regla	Descripción

IAM Group Has Users Check	Asegura que los grupos IAM tengan usuarios asignados
Internet Gateway Authorized VPC Only	Verifica que los gateways de internet estén solo en VPCs autorizadas
Account Part of AWS Organizations	Verifica que la cuenta pertenezca a una Organización de AWS
Secrets Manager Using CMK	Asegura que secretos estén cifrados con claves CMK
ELBv2 ACM Certificate Required	Requiere certificados válidos ACM en ALBs
ELBv2 Multiple Availability Zones	Asegura que los ALBs operen en al menos dos zonas
ALB WAF Enabled	Requiere asociación de WAF con ALBs
CLB Multiple AZ	Asegura que los CLBs estén en múltiples zonas
EBS Volume Protection by Backup Plan	Verifica que volúmenes EBS estén protegidos por planes de backup
Redshift Cluster KMS Enabled	Verifica que clústers Redshift usen cifrado con KMS

Reglas Opcionales de Config para Monitoreo de Backups

Reglas adicionales están preconfiguradas para monitorear respaldos de Aurora, EC2 y otros servicios, listas para activarse si se requiere visibilidad en protección de backups.

AWS Systems Manager (SSM) - Automatización

Aunque actualmente no se han desplegado documentos de automatización SSM, el entorno está preparado para soportar futuras ejecuciones automáticas para tareas como:

- Habilitar cifrado en buckets S3

- Habilitar logging en ELBs
- Forzar HTTPS en buckets S3
- Asociar perfiles de instancia IAM a instancias EC2

Monitoreo y Alarmas con AWS CloudWatch

Monitoreo de Métricas y Logs

CloudWatch está configurado para monitorear eventos clave de seguridad basados en los Controles del Benchmark CIS:

Control CIS	Evento Monitoreado
CIS 1.7	Uso de la cuenta root
CIS 4.4	Cambios en políticas IAM
CIS 4.5	Cambios en CloudTrail
CIS 4.6	Fallos en autenticación de consola
CIS 4.7	Eliminación/Desactivación de claves KMS
CIS 4.8	Cambios en políticas de bucket S3
CIS 4.9	Cambios en AWS Config
CIS 4.10	Cambios en grupos de seguridad
CIS 4.11	Cambios en NACLs
CIS 4.12	Cambios en gateways de red
CIS 4.13	Cambios en tablas de ruteo
CIS 4.14	Cambios en VPCs

Alarmas de CloudWatch

Cada evento monitoreado tiene una alarma asociada que envía notificaciones al tema SNS de Seguridad ante incumplimientos:

Nombre de Alarma	Descripción
CIS-1.7-RootAccountUsage	Se detectó uso de la cuenta root

CIS-4.4-IAMPolicyChanges	Se detectaron cambios en políticas IAM
CIS-4.6-ConsoleAuthenticationFailure	Fallo de autenticación en consola

---

Resumen del Estado de Seguridad

Característica	Estado
Controles de Seguridad Básicos	Implementados y preconfigurados
Protección de Identidad	Políticas de contraseña fuertes, Access Analyzer
Preparación para Cumplimiento	Estándares CIS, NIST y FSBP disponibles
Monitoreo y Auditoría	Habilitados mediante CloudWatch y AWS Config
Protección de Datos	Cifrado EBS y Bloqueo de acceso público S3 aplicados

---

Notas

- **Activación Opcional de Servicios:** Servicios como Security Hub, Macie, GuardDuty y Audit Manager están listos para activarse sin necesidad de rediseñar la arquitectura.
- **Expansión Futura:** Las reglas de Config para respaldo y los documentos de automatización SSM pueden activarse según las necesidades del cliente.