

Álex Fernández Salé

Ricardo Díaz Núñez

Pablo Rodríguez Alonso

Raymond Debasa Peralta



Eric Olden

Seguridad Informatica/ Gestión de identidades

- Secure and Clear Trust.
- Simplified.
- Cargos en Oracle.
- Coautor de SAML.



• Las seis "A" de la Gestión de identidad

- Autenticación
- Control de Acceso
- Autorización
- Atributos
- Administración
- Auditoria



- Es una nueva manera de pensar en la identidad.
- "Kubernetes o Terraform para la identidad"
- Aplicar principios de abstracción y automatización a la gestión de identidades.
- Normalizar las diversas API para crear una capa de abstracción.
- Gestionar de manera eficiente las identidades en entornos distribuidos y heterogéneos.

¿PARA QUE SE USA "IDENTITY ORCHESTATION" ?

LA ORQUESTACIÓN DE IDENTIDAD RESUELVE DESAFÍOS EMPRESARIALES

LA MODERNIZACIÓN

- Queremos migrar nuestra aplicación a la nube.
- ¿No es muy costoso?
- Caso Práctico: la adopción de autenticación.

FUSIONES Y ADQUISICIONES

Queremos juntar varias empresas.

- ¿No hay diferencias en las pilas tecnológicas?
- Caso Práctico: mapeo de espacios de nombres.

COMBINACIÓN DE SISTEMAS EN LA NUBE CON SISTEMAS LOCALES



Nube

Mayor disponibilidad de funcionalidades y servicios.

La resiliencia y la redundancia



Locales

Disponibilidad Mas limitado



La orquestación de identidad permite aprovechar lo mejor de ambos mundos

SOPORTE DE ESTÁNDARES

Los proveedores de identidad buenos soportan estándares.

La falta de integración basada en estándares ha causado muchos dolores de cabeza.

Los estándares nos permiten unir sistemas antiguos con nuevos:

- SAML: verifica quién es el usuario.
- OpenID Connect: verifica + restringe el acceso al usuario.

Funcionan muy bien y son seguros.

¿SISTEMAS DE IDENTIDAD ESPECÍFICOS O DE TERCEROS?

Los sistemas específicos suelen gestionar las identidades mediante una tabla de usuarios.

Inconvenientes:

Complejidad Desaprovechamiento Deuda técnica

Se recomienda utilizar software de terceros:

Auth0

AUTH0

- Autenticación
- Autorización

Se utiliza en móviles, aplicaciones web, etc..

Iniciar sesión mediante Google, Facebook, etc... Cumple las leyes y regulaciones de seguridad.

MEJORA DE UN SISTEMA DE IDENTIDAD ESPECÍFICO



Deshacerse de dependencias de contraseñas.



Implementar otros tipos de autenticaciones.

Factor Múltiple

Código QR

Aplicación de Autenticación



Desplegar el software de orquestación sobre la capa de abstracción.



Vincular autenticación con tabla de usuarios.

ID del usuario

GESTIÓN DE LA EXPERIENCIA DE USUARIO



Los usuarios suelen iniciar sesión a menudo de una manera específica.



Cambios reflexivos

Notificar a los usuarios.

Incentivar el uso de nuevas opciones

REDUNDANCIA EN LOS SISTEMAS DE AUTENTICACIÓN



Multitud de opciones de autenticación.

Hacen lo mismo de manera más o menos similar.



Previenen posibles desastres.



¿Cómo inicio sesión si no tengo Internet?

Tokens de Hardware.



Todas permiten autenticaciones fuertes y seguras-

DIFERENCIAS EN LA ORQUESTACIÓN ENTRE SERVICIOS

APIs servidorpersona:

• Similar a la orquestación directamente con personas.

APIs servidorservidor:

- Orquestación como PROXY.
- Uso de certificados.

SOLUCIÓN PARA APIS SERVIDOR-SERVIDOR

Tengo contraseñas en APIs servidor a servidor, ¿qué puedo hacer?

Dos pasos principales:

- Reducción vulnerabilidades:
 - Reemplazo de contraseñas por administradores de claves.
 - Contratación de plataformas en la nube como Azure o HashiCorp.
- Implementación de orquestación de identidad:
 - Utilizar claves para generar certificados.

CICLO DE VIDA DE LAS IDENTIDADES

- Dicotomía de la identidad:
 - Lado administrativo:
 - Certificados.
 - Validación de documentos.
 - Lado en tiempo de ejecución:
 - Recopilación de información.
 - Validación de las 6 A.
- Los lados están desacoplados.

ABRIR CUENTA EN UN BANCO FICTICIO

- I er paso: Recopilar información.
 - Nombre y apellidos, país de residencia, etc.
 - Árbol de decisiones de orquestación.
- 2° paso: Validación de documentos.
 - Tarea en segundo plano.
- 3er paso: Generación de credenciales.
 - QR sin contraseña.

SEGURIDAD Y PRIVACIDAD



Único proveedor de identidad.

Único lugar para almacenar datos. Leyes de protección de datos.



Distintos proveedores de identidad.

Capa de orquestación como controlador

Datos almacenados según la geografía

Datos sensibles no replicados

AUDITORÍA CON MÚLTIPLES SISTEMAS DE ORQUESTACIÓN DE IDENTIDAD



La orquestación mejora la capacidad de auditoría al proporcionar una vista unificada de la actividad a través de diferentes proveedores de identidad y nubes.



Facilita el seguimiento de las transacciones de los usuarios en entornos distribuidos.

COMPLEJIDAD DE LA ORQUESTACIÓN DE IDENTIDAD



Comparación con la virtualización: Ambas introducen complejidad adicional, pero ofrecen soluciones de gestión.



La orquestación simplifica la administración de múltiples sistemas de identidad.

COMPONENTES DE UNA ORQUESTACIÓN DE IDENTIDAD



Plano de Control: Establece reglas y políticas de seguridad.



Plano de Gestión: Aplica las políticas en tiempo real.



Orquestador: Componente central, actúa como proxy y proporciona servicios adicionales.



Se puede implementar en varios entornos y tiene un tamaño compacto de menos de 50 MB.

TIEMPO NECESARIO PARA IMPLEMENTAR UNA ORQUESTACIÓN DE IDENTIDAD



Record de menos de 10 minutos para implementar una solución de orquestación utilizando el servicio en la nube.



Para grandes empresas, el proceso de implementación generalmente lleva cinco días, incluyendo la integración con múltiples proveedores de identidad y aplicaciones.

NOVEDADES EMERGENTES EN LA ORQUESTACIÓN DE IDENTIDAD



Aumento del software autoservicio para que las personas puedan probarlo por sí mismas.



Potencial de la inteligencia artificial para mejorar la automatización y la detección de amenazas en los sistemas de orquestación.

¿PREGUNTAS?

