Authentication

MANAGEMENT

VU

Datasheet

Versión 6.19

Marzo 2025
Link a última versión disponible

¿Qué es?

Authentication Management® es una solución destinada a proteger a las organizaciones del robo o mal uso de las credenciales de acceso mediante mecanismos de Zero-Trust basados en múltiple factor de autenticación adaptativo.

Ofrece una capa extra de seguridad en los procesos de autenticación, a la vez que los simplifica a través de sus capacidades de inicio de sesión unificado (Single sign-on). Además, cuenta con la capacidad de integrar la herramienta Active Directory, tanto para la gestión de usuarios como para el control de acceso al *backoffice* de administración propio de la solución.

Authentication Management permite incorporar la tecnología de VU a cualquier recurso corporativo, incluidos VPNs, Intranets, aplicaciones y Office 365, utilizando las integraciones y protocolos más reconocidos en el mercado, como SAML2, OIDC, Radius, API y App.

Beneficios

• **Seguridad Zero-Trust** para entorno cloud, híbrido u on-premises. Mediante la autenticación multifactor se garantiza que el legítimo propietario de las credenciales sea la entidad que está accediendo al sistema.

• **Mejora la experiencia en los procesos de autenticación** gracias a la funcionalidad de Single sign-on. En un solo paso se logra autenticar a los usuarios en diversas aplicaciones y sistemas corporativos.

• **Ofrecido en modalidad SaaS,** permite un despliegue e integración fácil y sencillo con un mínimo impacto en la operación diaria de la organización.

• **Ofrecido en modalidad licenciamiento de software (on-premises)**, permite desplegar los componentes en la infraestructura del cliente.

• **Escalabilidad. Authentication Management** está concebido para que sea la pieza desde la que construir la estrategia de gestión de la identidad y los accesos.

Solución modular

VU ofrece soluciones modulares para brindar a los clientes fácil integración, rapidez y flexibilidad. Authentication Management cuenta con tres módulos principales: Server, SDK y App.

- **Server** es el módulo de autenticación de usuarios. Es multifactor y multiplataforma. Se puede desplegar on-premises o en la nube. En la modalidad SaaS, se generan instancias personalizadas que se conectan con la infraestructura del cliente a través de un agente.
- **SDK** es el módulo integrador de las funcionalidades de Authentication Management a las aplicaciones móviles de Android e iOS.
- **App** es una aplicación móvil *standalone*, "lista para usar", para el enrolamiento y la obtención del segundo factor de autenticación por parte de los usuarios finales.

Alcance funcional

Autenticación de identidades

Authentication Management permite autenticar usuarios en aplicaciones mediante las siguientes interfaces:

- SAML2
- OIDC – OpenID Connect
- Radius (a través de agente)
- WebServices REST

• Se integra con múltiples Active Directory —a través del módulo auxiliar **Agente**— posibilitando:

- verificar que el usuario se encuentre habilitado en Active Directory para poder validar su uso,
- validar las contraseñas de los usuarios en Active Directory,
- utilizar los usuarios propios del Active Directory para obtener el acceso al portal de administración (*backoffice*).

• Permite proveer de identidades y segundo factor de autenticación a cualquier aplicación compatible con las interfaces previamente mencionadas.

• La solución ofrece identidades que pueden estar almacenadas en un Active Directory o directamente en la solución, lo que significa que puede operar con o sin un Active Directory, y también puede tener algunas identidades AD y otras identidades nativas.

Single sign-on

• **Authentication Management** simplifica los procesos de autenticación mediante el reconocimiento de sesiones activas para evitar que los usuarios tengan que autenticarse en cada aplicación a la que desean ingresar.

• La solución brinda múltiples flujos de autenticación de usuarios, con uno o dos factores, configurables para cada aplicación.

Segundo factor de autenticación

Los factores de autenticación de un solo uso (OTP) permiten robustecer los procesos de autenticación. Por ejemplo, en el caso de VPN Segura, **Authentication Management** provee el segundo factor a través de la integración con un agente/FreeRadius.

Authentication Management posibilita el enrolamiento de segundo factor de autenticación en la aplicación del cliente (SDK) a través del envío de un cupón o código QR por correo electrónico, SMS u algún otro canal que el cliente posea. A su vez, permite enrolar en la aplicación móvil autenticaciones de tipo TOTP, push y sync.

Tipos de factores de autenticación

Authentication Management permite la configuración de los siguientes factores de autenticación:

• **TOTP:** contraseña de un solo uso basada en tiempo.

• **HOTP:** contraseña de un solo uso basada en eventos (contador HMAC).

• **SYNC:** notificaciones *in-app* en la aplicación standalone o a través del SDK. No tiene costo para el cliente y permite asociar más de un dispositivo por usuario.

• **PUSH**: notificaciones integradas al sistema operativo móvil (habilitadas a través del uso del SDK o aplicación *standalone*). Se implementa a través de Firebase (es requerida una API key del cliente para su configuración).

• **Magic Link**: permite la autenticación por medio de un link que se envía al email del usuario. Esto evita al usuario incrementar la cantidad de contraseñas a administrar.

• **Código QR**: método de autenticación basado en códigos QR. Está integrado con la App genérica de VU, lo que permite a los usuarios utilizar dispositivos móviles para verificar su identidad y autenticar transacciones, entre otras acciones.

NUEVO

Los factores de autenticación pueden ser enviados al usuario final a través de los siguientes canales:

	SMS	Correo electrónico	OS móvil	In-app (SDK)	App Authentication Management	2FA Wallets*
TOTP	-	-	-	✓	✓	✓
HOTP	✓	✓	-	✓	✓	✓
PUSH	-	-	✓	-	✓	-
SYNC	-	-	-	✓	✓	-
Magic Link	-	✓	-	-	-	-

* Google Authenticator, Microsoft Authenticator, entre otras.

Authentication Management soporta los siguientes canales por interfaz:

	WebServices REST	SAML2	OIDC	RADIUS
Correo electrónico	✓	✓	✓	✓
SMS	✓	✓	✓	✓
In-app (SDK)	✓	✓	✓	✓
App Authentication Management	✓	✓	✓	✓
2FA wallets*	✓	✓	✓	✓

* Google Authenticator, Microsoft Authenticator, entre otras.

Aplicaciones móviles

Authentication Management permite a los usuarios recibir el segundo factor de autenticación en su propia aplicación móvil a través del SDK nativo en iOS y Android, así como híbrido (Javascript), que puede ser integrado tanto para el enrolamiento como para la obtención del segundo factor de autenticación. Las aplicaciones móviles permiten la creación de múltiples cuentas con sus semillas, así como la sincronización de relojes.

También se encuentra disponible en los *stores* de Android y Apple la **aplicación móvil** standalone, lista para usar, para el enrolamiento y la obtención del segundo factor de autenticación por parte de los usuarios finales.

Características de mensajería

- **Authentication Management** permite dos tipos de notificaciones en aplicaciones móviles: SYNC y PUSH.
  - **SYNC:** notificaciones *in-app* en la aplicación *standalone* o a través del SDK. No tiene costo para el cliente y permite asociar más de un dispositivo por usuario.
  - **PUSH:** notificaciones integradas al sistema operativo móvil (habilitadas a través del uso del SDK o aplicación *standalone*).
- Envío de correo electrónico a través del servidor SMTP propio del cliente.
- Envío de SMS.

Portal de usuario

El portal permite a los usuarios realizar diversas tareas, entre las que se encuentran:

- ver sus datos y las aplicaciones a las que tienen acceso,
- ingresar a cada una de esas aplicaciones sin necesidad de reingresar credenciales (single sign-on),
- solicitar acceso a aplicaciones,
- gestionar dispositivos y sesiones,
- consultar su actividad dentro del portal,
- cambiar la contraseña,
- recuperar la contraseña en el formulario de autenticación.

El mismo formulario de autenticación permite autenticar a usuarios nativos de la solución y a usuarios autenticados en un Active Directory.

Si el usuario es administrador, una de sus aplicaciones es el portal de administración, al que puede ingresar desde el portal de usuario.

Portal de administración

El portal de administración permite:

- Configurar las políticas de contraseña, ver y crear usuarios (uno a uno o por lotes), configurar aplicaciones con sus flujos de usuario, y revisar los logs de ejecución.
- La sincronización de usuarios desde múltiples AD (repositorio centralizado).
- El alta masiva de usuarios nativos a través de archivos .CSV.
- Revisar las listas de usuarios (tanto nativos como de AD) incluyendo sus datos.
- Crear un usuario nativo ingresando sus datos.

Reportes, cuadros de mando y logs de auditoría

Se incluyen reportes y logs de auditoría para controlar la operación del sistema. Además, hay API con información para poder desarrollar cuadros de mando.

Reportes

- Número total de usuarios.
- Usuarios por su estado (habilitados, activos, inactivos, deshabilitados).
- Usuarios por Tipo (nativos y Active Directory).
- Creación/Eliminación/Modificación de usuarios.
- Reseteo y cambios de contraseñas.
- Tipo de MFA utilizado (SMS, email, OTP).
- Autenticaciones/accesos fallidos y exitosos.

Cuadros de mando (APIs)

- Número total de usuarios.
- Número de usuarios por estado.
- Estado de los agentes.
- Número y porcentaje de MFA utilizado.
- Número de autenticaciones exitosas y fallidas.
- Número de accesos exitosos y fallidos.
- Número y porcentaje de contraseñas reseteadas.
- Número acceso a las aplicaciones integradas.

Control de acceso basado en roles (RBAC)

El acceso a las aplicaciones se hace basado en los roles del usuario. Cada aplicación tiene un permiso de acceso que incluye el nombre de la aplicación. Este permiso se puede incluir en la definición de uno o más roles, de modo que los usuarios que tengan un rol apropiado podrán ingresar a la aplicación.

Los roles de usuarios se pueden asociar a grupos de AD. Así, un miembro de un grupo AD tendrá automáticamente todos los roles asociados a ese grupo. Esta asociación es dinámica, de modo que, si el usuario sale del grupo, pierde los roles. Asimismo, si se modifica la asociación de grupos y roles, los usuarios pueden ganar o perder roles.

Control de accesos basado en atributos (ABAC)

El acceso a las aplicaciones se hace basado en los atributos del usuario. Durante el proceso de login, incluyendo SSO, si el usuario ha entregado una contraseña correcta y si el motor de reglas está activo, se deberán validar las reglas que estén habilitadas.

Las reglas del motor estarán configuradas de modo que devuelven uno de dos posibles códigos de acción: permitir o denegar acceso.

Gestión de autenticación multifactor (MFA)

El sistema permite gestionar la existencia de múltiples factores de autenticación, tanto para aplicaciones conectadas con OIDC o SAML como para clientes RADIUS.

En el caso de aplicaciones **OIDC o SAML**, es posible configurar para cada aplicación el proceso de autenticación. El administrador puede elegir la política de autenticación, por ejemplo: solo contraseña, solo TOTP, contraseña y TOTP, contraseña y segundo factor elegido por el usuario, entre otras variantes adicionales.

En el caso de clientes **RADIUS**, es posible elegir el tipo de OTP de acuerdo con el rol del usuario. Los usuarios ingresarán con su contraseña y la OTP configurada para sus roles. También es posible dar acceso a un usuario que no se encuentra en ninguno de los roles configurados para este propósito. En ese caso, ingresarán solo con contraseña. Dado que los grupos de usuarios de AD se pueden vincular a roles, esta característica también puede funcionar con grupos de AD.

Perfiles de acceso

Los perfiles de acceso permiten establecer políticas de autenticación y restricciones de acceso para usuarios y aplicaciones.

Cada usuario puede tener uno o más perfiles de acceso según sus roles, al igual que las aplicaciones a las que acceden. Por lo tanto, se incorpora el concepto de **perfil de acceso dinámico**, que calcula la combinación de perfiles para permitir o restringir el acceso de los usuarios en cada caso, ya sea solicitando autenticación de doble factor (2FA), reautenticación o control de acceso basado en atributos.

Motor de reglas

El motor de reglas de Authentication Management está basado en la configuración de un conjunto de atributos para la restricción de acceso a los usuarios, que pueden ser adaptados a las necesidades de cada empresa u organización.

Las reglas de acceso disponibles en la versión actual son las siguientes:

- Direcciones IP
- Días de la semana
- Intervalo de horas
- Países

Las reglas aplican por zona horaria y puede configurarse una excepción para un rol específico, por ejemplo, para el rol Administrador.

Ingreso sin contraseña: FIDO2

FIDO2 constituye un estándar de autenticación global desarrollado por FIDO Alliance y basado en criptografía de clave pública. FIDO2 permite a los usuarios utilizar sus propios dispositivos (teléfonos, computadoras de escritorio, llaves de seguridad USB, etc.) para realizar la autenticación de forma rápida y segura en lugar de su contraseña habitual.

Alcance de FIDO2 en Authentication Management:

- Configuración de factor FIDO2 y registro de autenticadores desde el portal de administración para usuarios con rol Administrador.
- Autoservicio de registro de autenticadores FIDO2 desde el portal de usuario.
- Posibilidad de utilizar un autenticador FIDO2 registrado como alternativa a la contraseña en el login del portal de usuario.
- Posibilidad de utilizar un autenticador FIDO2 registrado como alternativa a la contraseña en el módulo de inicio de sesión único (SSO).

VU Access for Windows

VU Access for Windows es un proveedor de credenciales alternativo para Microsoft Windows, que implementa 2FA al solicitar el ingreso de una OTP de aplicaciones móviles (Microsoft Authenticator, VU App, entre otras) al iniciar sesión. Esto permite reforzar la seguridad de equipos personales y corporativos.

En la versión offline no es necesario que los usuarios estén conectados a internet para realizar la autenticación y el ingreso a Windows. Esta versión permite el autorregistro de los usuarios a través de una aplicación instalada en sus PC.

Características:

- Solicita usuario, contraseña y OTP.
- Incluye aplicación para configurar TOTP en app móvil.
- Compatible con diferentes aplicaciones móviles.
- Compatible con Windows 10 u 11.
- Incluye instalador de Windows.

Módulo Directory

El módulo Directory administra los datos (atributos) de las identidades de Authentication Management, lo que permite habilitar el registro de múltiples atributos de usuario en el sistema.

Al habilitar este módulo, se permite almacenar y recuperar atributos personalizados de los usuarios. En la actual versión se pueden crear usuarios nativos en Authentication Management con sus nombres personales.

Integración con VU Identity Link

La integración con VU Identity Link permite autenticar la identidad de los usuarios mediante reconocimiento biométrico y verificación de documentos.

Esto asegura que los usuarios que están intentando ingresar en Authentication Management o las aplicaciones administradas por el portal sean realmente quienes dicen ser. Además, esta integración ayuda a mejorar la calidad de los datos, detectar ataques y proteger tu negocio.

Otras características

- Permite definir las políticas de creación de nombres de usuarios y de contraseñas:
  - Configuraciones de complejidad de contraseñas.
  - Historial de contraseñas.
  - Lista de exclusión de contraseñas.

- Permite definir políticas de bloqueos automáticos de usuarios.

- Permite definir políticas de desbloqueo automático de contraseñas y tokens de correo electrónico y SMS después de un número configurable de minutos.

- Soporta la integración con *hard tokens*.

- La comunicación entre las capas de presentación y el servidor del producto se realiza mediante una conexión SSL/TLS.

- Los métodos disponibles a través de la API permiten:
  - Habilitar y deshabilitar usuarios y tipos de factores de autenticación.
  - Validar credenciales.
  - Eliminar usuarios y tipos de factores de autenticación de la plataforma.
  - Modificar y asignar la contraseña de un usuario en la plataforma.
  - Agregar grupos de Access Control Service.
  - Crear, dar de alta, validar, bloquear y desbloquear usuarios.
  - Dar de baja factores de autenticación asignados a usuarios.
  - Facilitar códigos OTP asignados al usuario en la aplicación móvil.
  - Validar el token de un usuario final.
  - Informar el estado de un usuario.

- Alta automática del factor OTP móvil a nuevos usuarios de Active Directory al momento de darlos de alta en Authentication Management.

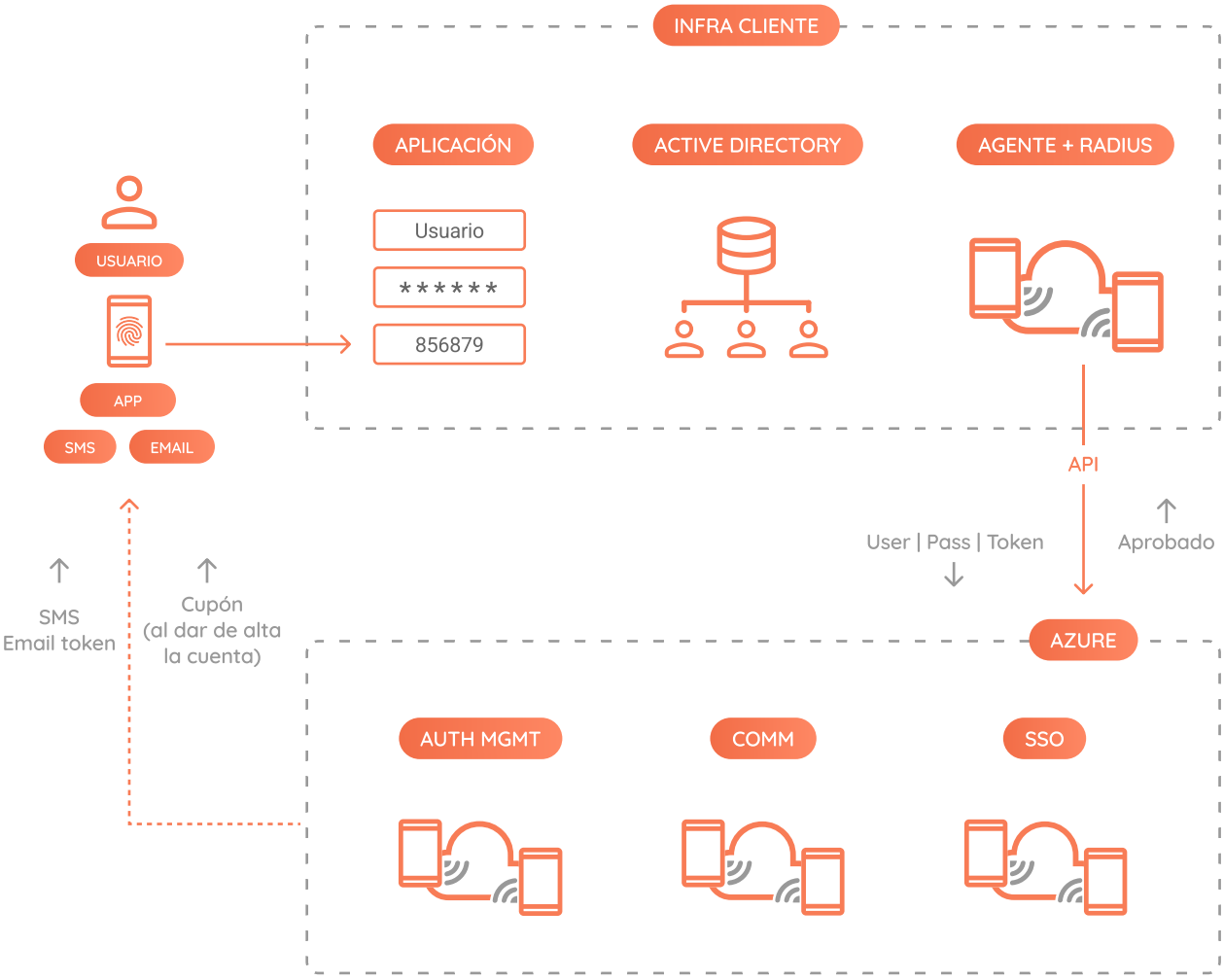
- Las notificaciones relacionadas con la creación/recuperación de contraseñas pueden incluir datos de usuario personalizados almacenados en el módulo Directorio.

Distribución

Authentication Management está disponible para su adquisición a través de licenciamiento de software (on-premises) o como servicio de software (SaaS).

Software como servicio (SaaS)

Su arquitectura cloud permite la gestión privada por distintos negocios o clientes internos. Se encuentra optimizada para Microsoft Azure e integrada a Azure DevOps, Azure Vault y Azure Monitor utilizando instancias dockerizadas.



Agente: requerimientos de software y hardware

Se utiliza para conectar la infraestructura del cliente (AD, terminador VPN) con el despliegue en la nube de Authentication Management. Se instala en una máquina virtual con sistema operativo Linux y tecnología de contenedores Docker.

Es un requisito que en dicha máquina virtual el agente pueda comunicarse con el AD y el servidor VPN contra el agente.

Componente de infraestructura	Requerimiento (*)	Entrega
Agente	Linux VM 2 core 4 Gb -RAM 20 Gb Disco Herramienta Docker (versión 3.x)	Imágenes Docker

(*) Para el caso de alta disponibilidad del agente se deberá disponer de 2 máquinas virtuales y un balanceador de cargas.

Monitoreo y alarmas

Los componentes de la solución son monitoreados por VU utilizando Azure Monitor, Azure Log Analytics y Azure Application Insights a fin de mantener métricas de performance de cada componente involucrado y una traza de logs para auditoría y troubleshooting tanto de la infraestructura como de las instancias de Authentication Management.

Alta disponibilidad

El servicio es gestionado por Azure Kubernetes Service, con replicación en 3 zonas dentro de la región Brazil South o Europa. La recuperación del servicio en otra región, en caso de interrupción, será ejecutada en un plazo máximo de 30 minutos.

Respaldos

Para todas las bases de datos, los respaldos se realizan varias veces por hora de manera incremental y bajo políticas de retención. Los respaldos son replicados en una región alternativa a la productiva.

Actualización

VU realizará actualizaciones correctivas y evolutivas según disponibilidad y en modalidad hot-swapping desde el entorno de preproducción exclusivamente. Las actualizaciones suceden bajo políticas incrementales con rollback ante eventuales fallos.

Uptime

- 99% de uptime anual fuera de la franja horaria de mantenimiento: 00:00 a 22:00, GMT-3.
- 98% de uptime anual dentro de la franja horaria de mantenimiento: 22:00 a 0:00, GMT-3.

Habrá una ventana de mantenimiento desde la 01:00 a 03:00 horas UTC. Fuera de ese horario no se realizarán actividades de mantenimiento. En el caso de la ventana de mantenimiento el SLA será del 98% de uptime anual, mientras que en el período de producción el SLA es de 99% de uptime.

Tiempo de recuperación ante discontinuación del servicio

Se configurará el servicio para sostener un Recovery Time Objective de tres horas y Recovery Point Objective de una hora.

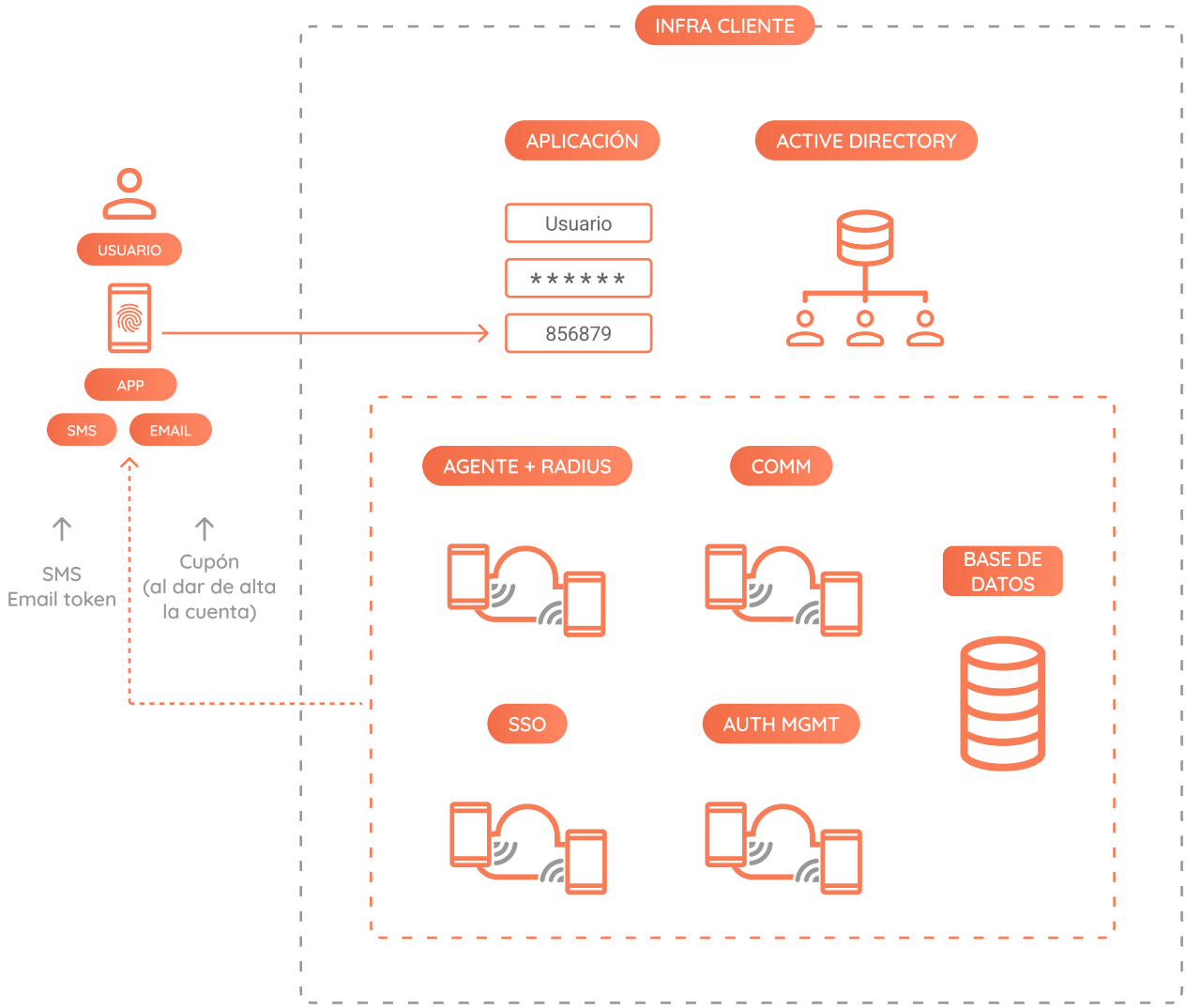
Tiempo de recuperación ante degradación del servicio

La infraestructura se monta sobre servicios elásticos y se extienden sus capacidades cuando se superan los umbrales configurados, resolviéndose la eventual degradación del servicio.

El proceso de ajuste de las instancias es automático y para dicho propósito se establece en tiempos máximos de 15 minutos.

Licenciamiento de software (on-premises)

Authentication Management on-premises permite desplegar los componentes single tenant en los servidores propios del cliente.



Requerimientos de hardware y software

La solución Authentication Management está conformada por 4 componentes, los cuales se despliegan en una arquitectura de microservicios que corre sobre Docker o Kubernetes.

Estos servicios son:

- Server de autenticación.
- Módulo single sign-on (IdP).
- Server de comunicaciones.
- Agente.

— Requerimientos de hardware

La máquina virtual mínima deberá ser:

vCPU	Memoria (Gb)	Almacenamiento del sistema (Gb)
2	8	60

Sobre esta base, se podrá escalar tanto verticalmente, agregando más CPU y memoria, o bien horizontalmente (recomendado) agregando réplicas. Para este último escenario, es recomendable la implementación con Kubernetes. Se debe proveer un balanceador de cargas.

Con el nodo base se pueden gestionar hasta 8 transacciones por segundo.

Usuarios (referencia)	Transacciones por segundo	Node / VM				DB	
		Cores	RAM	Réplicas	Almacenamiento del sistema	Almacenamiento mensual	Almacenamiento anual
250.000	8	2	8	1	60 GB	25 GB	300 GB
500.000	16	2	8	2	120 GB	50 GB	600 GB
1.000.000	32	2	8	4	240 GB	100 GB	1.2 TB
2.000.000	64	2	8	8	480 GB	200 GB	2.4 TB

— Requerimientos de software

Dado que toda la aplicación tiene arquitectura de contendores, solo se requiere el sistema operativo y las herramientas de Docker.

Sistema Operativo	Herramientas de contenedores	Base de datos
Linux Centos / Ubuntu / Red Hat	Esquema 1: Docker Engine (v. 19+) (*) con Docker Compose (v. 3+) (*) Esquema 2: Kubernetes (v. 1.24+)	SQL Server 2019 Otros esquemas de bases de datos: consultar

* VU dará soporte para la instalación y configuración de Docker y Docker Compose.

— Alta disponibilidad

- En el esquema de Docker + Docker Compose: duplicar la cantidad de máquina virtual.
- En implementaciones con Kubernetes: trabajar con n+1 nodos o lo que la política del cliente indique.
- Base de datos en esquema de alta disponibilidad con redundancia (activo - activo o activo - pasivo).

— Componentes de cliente

VU ofrece un SDK que se pueden integrar en las aplicaciones móviles Android e iOS y que permite la generación del TOTP.

Sistema Operativo	Tecnología	Entrega
Android	Java	SDK + Ejemplo
iOS	Swift	SDK + Ejemplo
Híbrido	Javascript	SDK + Ejemplo

Fin de soporte extendido (EOS) y fin de vida (EOL)

	Soporte completo	Mantenimiento	Sólo soporte	Sin soporte
Pueden esperarse nuevas funcionalidades	✓	No	No	No
Corrección de errores	✓	✓	No	No
Soporte al cliente	✓	✓	✓	No
Años desde la fecha de lanzamiento	2	3	4	-

Versión	Fecha de lanzamiento	Última entrega al cliente	Nuevas funcionalidades hasta	Correcciones hasta	Último día de soporte (LDOS)	Sin soporte desde
6.x	1/4/2022	1/4/2024	1/4/2024	1/4/2025	1/4/2026	2/4/2026

Contacto

Si necesitas más información o quieres agendar una demo de esta solución, por favor escríbenos a: sales@vusecurity.com

Otros productos de VU

Fraud & AML | Fraud Analysis | Device Finger Print

Onboarding Management | ID | Face | Voice | Touch

CIAM

Acerca de VU

VU es una compañía global de ciberseguridad, especializada en protección de la identidad y prevención de fraude, que desarrolla soluciones modulares, fáciles de integrar y adaptables tanto al ámbito corporativo como gubernamental.

Para lograrlo, utiliza tecnologías innovadoras basadas en la combinación de controles tradicionales de ciberseguridad, biometría, geolocalización, inteligencia artificial, *machine learning*, reconocimiento de documentación y análisis del comportamiento del usuario.

Más de 350 millones de personas en todo el mundo y más de 130 clientes en 30 países de América Latina, Europa y Estados Unidos utilizan la tecnología de VU para digitalizar sus negocios y aumentar el nivel de operaciones reduciendo los riesgos de ataques y la pérdida de información.

Sus alianzas estratégicas con Microsoft, Telefónica, IBM, BGH, Intel, Cisco y Accenture, entre otras compañías, ayudan a VU a cumplir su misión: crear experiencias seguras y sin fricción que mejoren la calidad de vida de ciudadanos y organizaciones.

vusecurity.com