Engineer

Usuario

Persona o proceso en su nombre con acceso a un sistema

Qué es

Un usuario es la persona o entidad para la que actúa un sistema. En la escritura técnica habitual, la palabra cumple tres funciones distintas, y la mayor parte de la confusión procede de mezclarlas.

El primer sentido es la persona: alguien que abre un producto e intenta hacer algo. Los diseñadores, el personal de soporte y los responsables de producto suelen referirse a ella, que no tiene una forma fija dentro del sistema. El segundo es la cuenta: el registro que conserva un sistema para reconocer a alguien de nuevo, normalmente con un nombre de acceso, un identificador interno, un conjunto de permisos y un estado como activo o suspendido. La mayor parte del código de las aplicaciones se refiere a este sentido. El tercero es el usuario del sistema operativo: en los sistemas de tipo Unix, una entrada de la base de datos de usuarios con un nombre y un identificador numérico de usuario. Los procesos en ejecución llevan credenciales de identificación de usuario que el núcleo utiliza para comprobar permisos.

Los tres rara vez se corresponden uno a uno. Una persona puede tener cuentas en muchos servicios, y las directrices de identidad digital de NIST dicen con claridad que puede tener varias identidades digitales, cada una única solo dentro de su propio servicio. Varias personas pueden compartir una cuenta, lo que casi siempre es un error. Y muchísimos usuarios no tienen ninguna persona detrás: el servidor web, la base de datos, la tarea de copia de seguridad y el script de despliegue se ejecutan cada uno con su propio usuario del sistema operativo y, a menudo, también tienen cuentas en otros sistemas. Por eso la definición de NIST dice «persona o proceso (del sistema) que actúa en nombre de una persona».

En una máquina Unix es fácil ver la separación entre nombre y número:

```
$ id ana
uid=1001(ana) gid=1001(ana) groups=1001(ana)
```

El núcleo trabaja con el número. POSIX define una base de datos que guarda, para cada usuario, su nombre, identificador numérico de usuario, identificador de grupo inicial, directorio de trabajo inicial y programa inicial que ejecutar. La propiedad de los archivos se guarda como número; el nombre se consulta solo al mostrar algo a una persona. Un proceso también lleva más de un identificador de usuario: uno real, que indica quién lo inició, y otro efectivo, que indica de quién son los permisos que usa en ese momento.

Las cuentas de aplicaciones suelen hacer la misma separación. El estándar SCIM, que se usa para dar de alta usuarios de un sistema en otro, exige un `userName` visible y utilizable para iniciar sesión, único dentro del servicio y comparado sin distinguir mayúsculas de minúsculas, y un `id` separado que asigna el servicio, permanece estable y nunca se reasigna. Un indicador `active` distingue una cuenta suspendida de una operativa.

Utilice el concepto en una decisión

Aplique «¿Qué es un usuario?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Resolver con rapidez y lenguaje claro los problemas del portátil, la impresora, el acceso o el correo, sin hacer sentir mal a nadie.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. Creación de un departamento de soporte técnico — 10,000 clientes atendidos por un departamento de soporte creado desde cero

Creación de un departamento de soporte técnico Póngase en contacto →

Por qué importa

Toda decisión de acceso es una decisión sobre un usuario; una idea confusa de quién es se convierte en una decisión confusa. La pregunta «¿puede esta persona ver esta factura?» se responde en el código como «¿tiene esta cuenta, en este contexto, un permiso que abarque este registro?». Cada paso de esa traducción es un punto en el que la persona prevista y la cuenta real pueden dejar de corresponderse.

En el límite entre persona y cuenta también se determina a quién se atribuyen las acciones. Los registros guardan cuentas. Cuando cada cuenta pertenece a una sola persona, una línea del registro indica quién hizo algo. Cuando una cuenta se

comparte, indica qué secreto se usó, pero no quién lo escribió; retirar el acceso de una persona exige cambiarlo para todos.

Los usuarios del sistema operativo son una herramienta de mínimo privilegio con una larga trayectoria. Un servicio que se ejecuta con su propio usuario sin privilegios queda limitado por los permisos de ese usuario, no solo por la propiedad de los archivos. Aun así puede modificar recursos compartidos que admitan escritura, hacer peticiones de red y usar las credenciales a su alcance. Separar los usuarios de los servicios reduce el daño de una intrusión; no proporciona aislamiento completo. El mismo servicio ejecutado como superusuario puede poner en riesgo toda la máquina. Dar a cada programa un usuario propio es un pequeño cambio de configuración que reduce los permisos disponibles cuando algo sale mal.

Por último, las personas y las cuentas tienen ciclos de vida distintos. Las personas cambian de nombre, correo y empleador; las cuentas se suspenden, se fusionan y se eliminan. Un sistema que usa un atributo modificable, como el correo electrónico, como identidad de una cuenta acabará vinculando el historial de una persona a otra.

Cómo se aplica en la práctica

En una plataforma marítima, los profesionales gestionan organizaciones, como empresas y academias, que no tienen credenciales de acceso propias. La página expone la regla directamente: la persona es la cuenta y la organización es la entidad en cuyo nombre actúa. El trabajo consistió en un cambio de contexto que permite actuar en nombre de cualquier organización que gestione el usuario. El almacenamiento local del navegador guarda la organización activa, por lo que cambiar es instantáneo; una cookie que lee el servidor refleja esa elección para que las páginas renderizadas en el servidor muestren el mismo contexto. Nada de eso decide el acceso. La autorización vuelve a comprobarse en el servidor en cada petición, de modo que editar el valor guardado solo cambia lo que aparece en la pantalla de quien lo edita.

En el servidor propio de la empresa, las versiones se publican con un usuario del sistema operativo que apenas tiene permisos. Al configurar la capa de contenedores, se separó el despliegue del aprovisionamiento: root prepara una vez la ruta de despliegue y, desde entonces, un usuario sin privilegios vuelve a

desplegar mediante un script fijo, autorizado por una regla de alcance limitado que permite ese comando sin argumentos. Una publicación rutinaria construye la imagen y reinicia el servicio, sin que nadie abra una shell de root para ello.

Saber quiénes son los usuarios también es objeto de un informe. Uno de los siete roles de generación de informes de solo lectura genera desde el servidor real un informe de acceso en Markdown dentro del repositorio, que reúne cuentas, alcance de sudo, huellas de claves, usuarios de la forja de Git y roles de base de datos. Los siete informes comparten una regla: una cifra solo aparece si la ejecución la midió; los datos que faltan se dejan en blanco, en lugar de sustituirse por una suposición verosímil que el lector creería. En conjunto, han descubierto problemas reales, entre ellos un puerto en escucha no declarado y dos controles de seguridad inoperantes.

Dónde surgen los problemas

Un usuario eliminado regresa como otra persona. Se borra una cuenta, su identificador se vuelve a asignar y la persona recién llegada hereda todo lo que siga apuntando al valor antiguo: filas de una tabla, un puesto en una lista, archivos en disco. En Unix, los archivos de un usuario eliminado conservan su propietario numérico, y el siguiente usuario creado con ese número pasa a ser su propietario. Asigne a las cuentas identificadores que nunca se reutilicen, como exige SCIM para su `id`, y decida qué hacer con los datos de quien se marcha antes de eliminar al usuario.

Se usa el correo electrónico como cuenta. Parece una clave natural hasta que alguien cambia de dirección, pierde acceso a la antigua o un empleador asigna la dirección a otra persona. Entonces el historial de una persona queda vinculado a otra, o una persona termina con dos cuentas. Use como clave un identificador interno estable y trate la dirección como un atributo modificable.

Todos acceden con la misma cuenta. Una cuenta de administrador compartida se configura deprisa y resulta imposible de auditar. Cuando alguien se marcha, solo pierde el acceso si el secreto cambia para todos, y el registro identifica un rol en lugar de una persona. Una cuenta por persona, con las facultades compartidas concedidas mediante grupos, roles o una regla sudo de alcance limitado, permite atribuir las acciones y retirar los accesos con rigor.

El navegador decide lo que puede hacer el usuario. Un rol guardado en el almacenamiento local, una cookie o un campo oculto de formulario es una propuesta del cliente que cualquiera puede editar. Si el servidor confía en ella, editarla constituye un ataque. El cliente puede recordar el contexto por comodidad; el servidor debe comprobar los permisos por sí mismo, en cada petición.

Un servicio se ejecuta como root porque era más sencillo. Todo funciona, pero un fallo explotable del servicio puede poner en riesgo todo el servidor. Asigne a cada servicio su propio usuario sin privilegios y conceda cualquier permiso adicional de forma limitada, para un comando concreto, en lugar de hacerlo con carácter general.

Lecturas adicionales

- Glosario de NIST CSRC: user — las definiciones usadas en las publicaciones de seguridad de NIST, cada una con el documento del que procede.
- POSIX.1-2024 Base Definitions: Definitions — el significado formal de base de datos de usuarios, identificador de usuario y nombre de usuario en los sistemas de tipo Unix.
- RFC 7643: SCIM Core Schema — el recurso User para trasladar cuentas entre servicios, con `userName`, `id` y `active`.
- NIST SP 800-63-4: Digital Identity Guidelines — cómo una persona puede tener varias identidades digitales y las funciones de solicitante, suscriptor y reclamante.
- POSIX.1-2024: File Access Permissions — el acceso mediante las clases de permisos de propietario, grupo y otros, los controles alternativos y los privilegios adecuados; la propiedad por sí sola no delimita el acceso.

Glosario

Elija según sus restricciones reales

Describa el dispositivo o servicio, los síntomas observados y los datos que deben conservarse. Podemos establecer el paso de diagnóstico útil más seguro.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es un usuario?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/user/