¿Qué es el aprovisionamiento just-in-time?

Si estás construyendo una aplicación SaaS B2B y deseas admitir funciones de membresía, permitiendo que los miembros se unan fácilmente a tu espacio de trabajo (tenant). Podrías necesitar funciones como las del siguiente cuadro, y el aprovisionamiento just-in-time es una de ellas, ayudando a agilizar el proceso.

Características	Flujo
Invitación iniciada por el admin	Los usuarios pueden recibir una invitación por correo electrónico para unirse a la organización.
Creación o importación de usuarios a través de API	Los usuarios pueden usar una cuenta de usuario precreada para unirse a la organización.
Aprovisionamiento just-in-time	Los usuarios que inician sesión en la aplicación por primera vez pueden unirse a la organización.
Sincronización de Directorio (por ejemplo, SCIM)	Usar la funcionalidad de Sincronización de Directorio del IdP para preaprovisionar usuarios en la aplicación con anticipación.

El aprovisionamiento just-in-time (JIT) es un proceso utilizado en sistemas de gestión de identidad y acceso para crear cuentas de usuario sobre la marcha a medida que se inician sesión en un sistema por primera vez. En lugar de preaprovisionar cuentas para los usuarios con anticipación, el aprovisionamiento JIT crea y configura las cuentas de usuario necesarias de manera dinámica cuando un usuario realiza una autenticación. El aprovisionamiento just-in-time es una característica popular con sus propias características, como la eficiencia, la no participación administrativa y la membresía automática en la organización, etc.

¿Cuáles son los casos de uso del aprovisionamiento just-in-time?

Estos casos son comunes al construir una aplicación B2B que involucra arquitectura multi-tenant, Enterprise SSO, trabajar con empresas o requerir funciones de incorporación de equipos. Aquí hay algunos escenarios de muestra que tus clientes pueden enfrentar.

Incorporación rápida

Tienes un cliente que experimenta contrataciones frecuentes o un rápido crecimiento, puede usar el aprovisionamiento JIT para configurar rápidamente cuentas de usuario para nuevos empleados. Aquí hay un ejemplo:

Sarah es una nueva empleada en la empresa SuperFantasy, que utiliza Okta como su Proveedor de Identidad Empresarial. El equipo de recursos humanos la agrega como una identidad empresarial en Okta solo una vez. Cuando Sarah usa este correo electrónico para iniciar sesión en una aplicación de productividad de uso corporativo llamada Smartworkspace por primera vez, el sistema crea automáticamente una cuenta y le asigna el rol correcto dentro del espacio de trabajo de la empresa. De esta manera, ni Sarah ni el equipo de recursos humanos de SuperFantasy necesitan pasar por múltiples pasos para la creación de la cuenta y la asignación del rol.

Fusiones, adquisiciones y trabajadores temporales

Tienes un cliente que experimenta fusiones o adquisiciones de otras empresas, el aprovisionamiento JIT puede simplificar el proceso de otorgar acceso a los sistemas de la empresa adquirente para muchos nuevos usuarios. Veamos otro ejemplo,

Peter trabaja para MagicTech, que fue recientemente adquirida por SuperFantasy. MagicTech es una organización más pequeña sin Enterprise SSO, pero también utiliza Smartworkspace, donde Peter ya tiene una cuenta empresarial.

El equipo de recursos humanos puede agregar a Peter en Okta. Cuando Peter inicia sesión en Smartworkspace por primera vez a través de Okta, el sistema vincula automáticamente su cuenta empresarial existente y otorga el acceso apropiado a SuperFantasy.

Los escenarios anteriores son ideales para implementar la función JIT.

¿Es específico de SAML y Enterprise SSO?

El aprovisionamiento just-in-time (JIT) a menudo se asocia con Enterprise SSO en la autenticación SAML, pero no es exclusivo de Lenguaje de marcado para declaraciones de seguridad (Security Assertion Markup Language, SAML) . El aprovisionamiento JIT también se puede usar con otros protocolos de autenticación como OAuth 2.0 y OpenID Connect (OIDC) , y no siempre requiere una configuración de Enterprise SSO .

Por ejemplo, el aprovisionamiento JIT basado en correo electrónico puede agilizar la incorporación de equipos al agregar automáticamente usuarios a un espacio de trabajo según su dominio de correo electrónico. Esto es particularmente útil para organizaciones que carecen del presupuesto y recursos para adquirir y gestionar Enterprise SSO.

La idea fundamental detrás del aprovisionamiento JIT es automatizar la creación o actualización de cuentas de usuario cuando un usuario intenta acceder a un servicio por primera vez, independientemente del protocolo específico utilizado.

¿Se aplica a usuarios nuevos o existentes de la aplicación?

El aprovisionamiento just-in-time (JIT) generalmente se refiere al primer intento de acceso a una aplicación. Sin embargo, diferentes productos perciben esta funcionalidad de manera diferente. Algunos utilizan el aprovisionamiento JIT solo para la creación de identidad y cuentas, mientras que otros también incluyen actualizaciones de cuentas just-in-time, como reprovisionamiento y sincronización de atributos.

Además de la creación automática de usuarios, el aprovisionamiento SAML JIT permite otorgar y revocar membresías de grupos como parte del aprovisionamiento. También puede actualizar usuarios aprovisionados para mantener sus atributos en el almacén del Proveedor de servicios (Service provider, SP) sincronizados con los atributos del almacén del Proveedor de identidad (Identity provider, IdP) .

Si deseas considerar el escenario de inicio de sesión de usuarios existentes subsiguiente, asegúrate de tener un sistema de aprovisionamiento robusto junto con tu sistema JIT. Por ejemplo,

- **Resolución de conflictos**: Tu sistema debe tener una estrategia para manejar conflictos si ya existe una cuenta con información diferente a la proporcionada por el IdP durante el proceso JIT. Esto puede requerir un control detallado de las políticas de tu organización y la configuración del IdP.
- **Registros de auditoría**: Es importante mantener registros tanto de las nuevas creaciones de cuentas como de las actualizaciones de cuentas existentes a través de procesos JIT por razones de seguridad y cumplimiento.

- **Rendimiento**: Aunque el aprovisionamiento JIT ocurre rápidamente, considera el impacto potencial en los tiempos de inicio de sesión, especialmente para usuarios existentes si estás actualizando su información en cada inicio de sesión.
- **Consistencia de datos**: Asegúrate de que tu proceso de aprovisionamiento JIT mantenga la consistencia de los datos, especialmente al actualizar cuentas de usuario existentes.

¿Cuál es la diferencia entre JIT y SCIM?

SCIM es un protocolo estándar abierto diseñado para simplificar y automatizar la gestión de identidad de usuarios en diferentes sistemas y dominios. Se utiliza comúnmente en escenarios de Sincronización de Directorios.

La principal diferencia entre JIT y SCIM es que JIT crea cuentas durante el intento de inicio de sesión del usuario, mientras que SCIM puede aprovisionar usuarios a través de un proceso automatizado sin conexión, independiente de los intentos de inicio de sesión del usuario.

Esto significa que JIT se enfoca en la incorporación de nuevos usuarios, mientras que SCIM se centra en la gestión completa del ciclo de vida de los usuarios.

Además, JIT es a menudo una extensión de SAML y carece de una implementación estandarizada en todos los sistemas, mientras que SCIM es un protocolo bien definido y estandarizado RFC 7644 para la gestión de identidad. Algunas organizaciones más grandes usan SCIM para el aprovisionamiento de cuentas, integrándolo con sus propios sistemas. Esto puede ser muy complejo y variar caso por caso. Estas organizaciones a menudo tienen un sistema de aprovisionamiento que involucra tanto procesos automatizados como participación manual del admin.

Revisión #3
Creado 11 noviembre 2024 17:59:24 por Marluan Espiritusanto
Actualizado 13 noviembre 2024 14:03:54 por Marluan Espiritusanto