Introducción a Sun Identity Manager

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Referencia: 821–0058
Julio de 2009

090810@22749

Contenido

Prefacio

Introducción a Sun Identity Manager 8.1 sirve para responder a la pregunta *¿Qué es Sun™ Identity Manager y cómo funciona?* En este libro se describe la arquitectura de producto de Identity Manager y se suministra información para planificar una implementación de alta disponibilidad.

Quiénes deben usar esta guía

Esta guía está destinada a los profesionales de la informática que desean conocer mejor Sun Identity Manager 8.1 y el software asociado. Resultará especialmente valiosa para quienes están evaluando Identity Manager y para quienes se hallan en las fases iniciales de planificación de una implementación de Identity Manager.

Organización de esta guía

Esta guía se divide en los capítulos siguientes:

Capítulo 1, "Descripción del producto", donde se explica la finalidad de Identity Manager y se destacan las características principales de la aplicación.

Capítulo 2, "Arquitectura del producto", donde se describe la arquitectura de Identity Manager, la arquitectura de Service Provider y la arquitectura de los servicios web. También se incluyen instrucciones sobre la separación y la proximidad física de los componentes del sistema.

Capítulo 3, "Agrupamiento en clúster y alta disponibilidad", que ofrece orientación para implementar un entorno de Identity Manager de alta disponibilidad / tolerante a fallos (HA/FT) . También ayuda a evaluar el nivel de disponibilidad que requiere una implementación de Identity Manager.

Guías relacionadas

La documentación de Sun Identity Manager 8.1 está formada por las guías indicadas a continuación.

Destinatarios principales	Título	Descripción
Todos	*Introducción a Sun Identity Manager*	Proporciona una descripción general de las características y la funcionalidad de Identity Manager. Incluye información sobre la arquitectura del producto y la integración de Identity Manager con otros productos de Sun, como Sun Open SSO Enterprise y Sun Role Manager.
	Notas de la versión de Sun Identity Manager 8.1	Incluye problemas específicos, problemas resueltos e información de última hora que no aparece en la documentación principal de Identity Manager.
Administradores del sistema	*Installation Guide*	Se explica cómo instalar Identity Manager y los componentes opcionales, como la Puerta de enlace de Sun Identity Manager y PasswordSync.
	Upgrade Guide	Contiene instrucciones para actualizar desde una versión anterior de Identity Manager a una más reciente.
	System Administrator's Guide	Contiene información e instrucciones que ayudan a los administradores del sistema a gestionar, mejorar y solucionar los problemas de la instalación de Identity Manager.
Administradores de negocio	*Guía del administrador de negocio*	Explica cómo usar las funciones de abastecimiento y auditoría de Identity Manager. Incluye información sobre las interfaces de usuario, la administración de usuarios y cuentas, la generación de informes y más.

Destinatarios principales	Título	Descripción
Integradores de sistemas	*Deployment Guide*	Explica cómo implementar Identity Manager en los entornos de TI complejos. Incluye temas que abarcan el uso de atributos de identidad, la carga y sincronización de datos, la configuración de acciones de usuario, la aplicación de marcas de identidad personalizadas, etc.
	Deployment Reference	Contiene información sobre flujos de trabajo, formularios, vistas, reglas y el lenguaje XPRESS.
	Resources Reference	Información para instalar, configurar y utilizar los adaptadores de recursos.
	Service Provider 8.1 Deployment	Explica cómo implementar Sun Identity Manager Service Provider y en qué se diferencian las vistas, los formularios y los recursos respecto al producto Identity Manager estándar.
	Web Services Guide	Explica cómo configurar la compatibilidad SPML, qué funciones SPML se admiten (y por qué) y cómo ampliar la compatibilidad en el campo.

Actualizaciones de la documentación

Las correcciones y actualizaciones para ésta y otras publicaciones sobre Sun Identity Manager se colocan en la web de actualizaciones a la documentación de Identity Manager:

`http://blogs.sun.com/idmdocupdates/`

Es posible utilizar un canal RSS para comprobar periódicamente este sitio y recibir notificaciones cuando haya actualizaciones disponibles. Para suscribirse, descargue un lector de RSS y haga clic bajo Feeds en el lado derecho de la página. Desde la versión 8.0, existen diferentes canales para cada versión principal.

Referencias a sitios web de terceros relacionados

En este documento se proporcionan direcciones de Internet de terceros e información adicional relacionada.

Nota – Sun no se responsabiliza de la disponibilidad de los sitios Web de terceros que se mencionan en este documento. Sun no avala ni se hace responsable del contenido, la publicidad, los productos ni otros materiales disponibles en dichos sitios o recursos, o a través de ellos. Sun declina toda responsabilidad sobre los posibles daños o pérdidas, reales o presuntos, causados o presuntamente causados directa o indirectamente por los contenidos, bienes o servicios citados u otros accesibles en o a través de esas páginas o recursos.

Documentación, asistencia y formación

El sitio web de Sun proporciona información sobre estas otras fuentes de recursos:

- Documentación (`http://www.sun.com/documentation/`)
- Asistencia técnica (`http://www.sun.com/support/`)
- Formación (`http://www.sun.com/training/`)

Sun valora sus comentarios

En Sun estamos interesados en mejorar nuestra documentación y, por tanto, agradecemos sus comentarios y sugerencias. Para enviarnos sus comentarios, entre en `http://docs.sun.com`

Convenciones tipográficas

En la tabla siguiente se describen las convenciones tipográficas utilizadas en este documento.

TABLA P–1 Convenciones tipográficas

Tipo de letra	Significado	Ejemplo
`AaBbCc123`	Nombres de comandos, archivos y directorios; mensajes del sistema que aparecen en la pantalla.	Edite el archivo `.login`. Utilice el comando `ls- a` para ver la lista de archivos. `nombre_máquina% ha recibido correo.`

TABLA P–1 Convenciones tipográficas *(Continuación)*

Tipo de letra	Significado	Ejemplo
AaBbCc123	Lo que escribe el usuario, frente a los mensajes del propio sistema.	`nombre_máquina%` **`su`** `Contraseña:`
aabbcc123	Elemento variable: se sustituye por un nombre o un valor real.	El comando para eliminar un archivo es `rm` *nombrearchivo*.
AaBbCc123	Títulos de libros, palabras o términos nuevos y palabras que deben enfatizarse.	Lea el Capítulo 6 de la *Guía de usuario*. Una copia en *caché* es aquella que se almacena localmente. *No* guarde el archivo. **Nota:** Algunos términos enfatizados aparecen en negrita en los documentos en línea.

Indicadores de shell en los ejemplos de comandos

La tabla siguiente muestra el indicador predeterminado y el indicador de superusuario de los sistemas UNIX® para los shells de C, Bourne y Korn.

TABLA P–2 Indicadores del shell

Shell	Mensaje de petición
C	`nombre-máquina%`
Shell de superusuario de C	`nombre_máquina#`
Shells de Bourne y Korn	`$`
Shells de Bourne y Korn para superusuario	`#`

◆ ◆ ◆ CAPÍTULO 1

Descripción del producto

En este capítulo se explica la finalidad de Sun™ Identity Manager y se destacan las características principales de la aplicación. También se describen brevemente otros productos de administración de identidades de Sun.

Este capítulo contiene los temas siguientes:

¿Qué es Identity Manager?

Sun Identity Manager permite automatizar el proceso de creación, actualización y eliminación de cuentas de usuario en múltiples sistemas de TI. En conjunto, este proceso se denomina *abastecimiento* (es decir, crear y actualizar cuentas de usuario) y *desabastecimiento* (eliminar cuentas de usuario).

Por ejemplo, cuando un empleado se incorpora a una empresa, Identity Manager ejecuta un flujo de trabajo que recupera las aprobaciones necesarias para conceder acceso al empleado. Una vez obtenidas estas aprobaciones, Identity Manager crea cuentas para el empleado en el sistema de recursos humanos de la empresa (PeopleSoft), el sistema de correo electrónico (Microsoft Exchange) y la aplicación de empresa (SAP). Si el empleado cambia de puesto en la empresa, Identity Manager actualiza su cuenta de usuario y amplía su acceso a los recursos necesarios para su nuevo rol. Por último, si el empleado deja de trabajar en la empresa, Identity Manager suprime automáticamente sus cuentas de usuario para impedir que siga accediendo.

Identity Manager también puede imponer directivas de auditoría continuadamente. Una *directiva de auditoría* determina qué tipos de acceso puede tener y no tener un usuario. Por ejemplo, en Estados Unidos se infringe la ley Sarbanes-Oxley (SOX) si el mismo usuario tiene

acceso tanto a los sistemas de cuentas por pagar y cuentas por cobrar. Se considera una infracción de la separación de deberes. Identity Manager puede realizar una exploración de auditoría para buscar diversas infracciones de estos tipos y, según la configuración, suprimir automáticamente el acceso o enviar una notificación a un administrador cuando detecte una infracción. Este proceso se denomina *remediación*.

¿Cómo interactúa Identity Manager con otros sistemas de TI?

En Identity Manager, las aplicaciones administradas y otros sistemas de TI se denominan *recursos*. Identity Manager utiliza *adaptadores* o bien *conectores* para interactuar con los recursos.

Los adaptadores y los conectores se instalan en el servidor de Identity Manager. (Identity Manager no requiere la instalación de software especial (denominado *agentes*) en los recursos de destino.) Existen muchos adaptadores y conectores para Identity Manager, pero además es posible crear otros nuevos para comunicarse prácticamente con cualquier recurso mediante protocolos estándar o interfaces de programación de aplicaciones (API) conocidas. Con Identity Manager se suministran varios adaptadores y conectores para comunicarse con muchos de los recursos más frecuentes. Además, hay disponibles plantillas y código básico que sirven de ayuda a los programadores para crear más adaptadores y conectores.

La comunicación directa con algunos recursos no es posible, en cuyo caso hay que usar la puerta de enlace de Sun Identity Manager. Entre los ejemplos de recursos que requieren la puerta de enlace hay productos de Microsoft como Exchange y Windows Active Directory, productos de Novell como eDirectory (antes Netware Directory Services) y varios más. En estos casos, Identity Manager se comunica directamente con la puerta de enlace, que a su vez interactúa con el recurso.

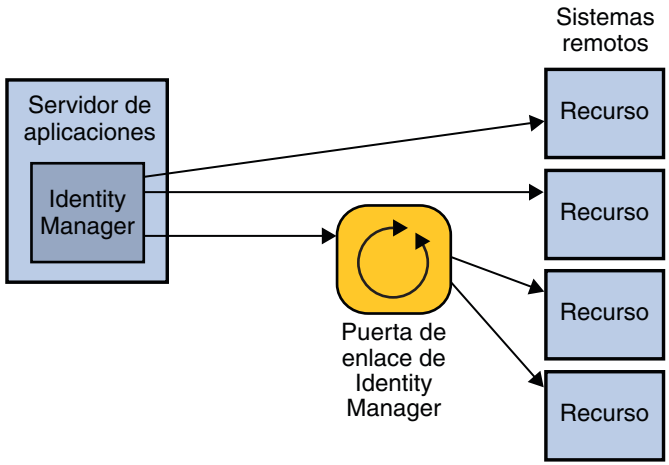

FIGURA 1–1 Identity Manager interactúa directamente con algunos recursos, mientras que otros requieren el uso de la puerta de enlace de Identity Manager

Encontrará una lista de recursos compatibles con Identity Manager en la sección "Recursos admitidos" de *Notas de la versión de Sun Identity Manager 8.1* .

¿Cómo se conectan los usuarios a Identity Manager?

Identity Manager tiene una interfaz de usuario (IU) para los administradores y otra para los usuarios finales. Los administradores y los usuarios finales utilizan un navegador web para iniciar la sesión en Identity Manager.

- Los administradores utilizan la *interfaz de administración* para administrar usuarios, configurar y asignar recursos, definir derechos y niveles de acceso, establecer directivas de auditoría, gestionar el cumplimiento y realizar otras funciones administrativas de negocio y de sistema.
- Los usuarios finales utilizan la *interfaz de usuario final* para efectuar diversas tareas de autoservicio, como cambiar contraseñas, configurar respuestas a preguntas de autenticación, solicitar acceso a sistemas de TI y administrar asignaciones delegadas.

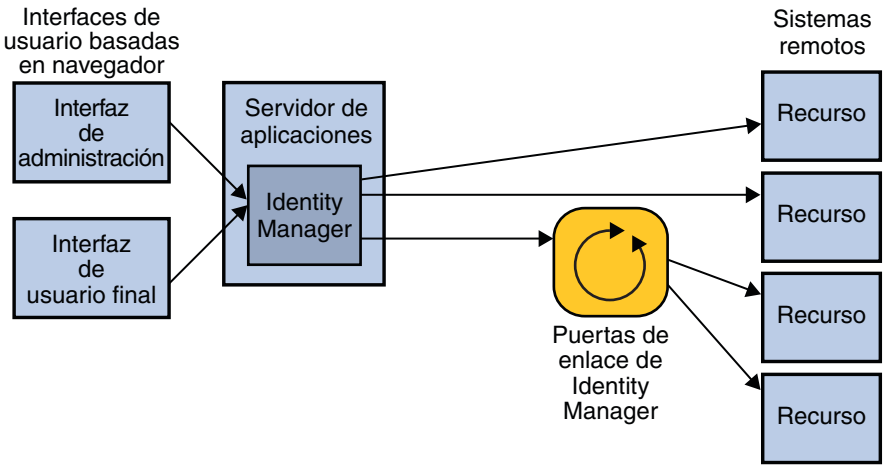

FIGURA 1–2 Los usuarios se pueden conectar a Identity Manager mediante la interfaz de administración y la interfaz de usuario final

Las empresas también pueden utilizar SPML (lenguaje de marcado de abastecimiento de servicios) para crear su propia interfaz de usuario o bien integrar un sistema frontal existente con Identity Manager.

Éstas son otras interfaces de Identity Manager:

- La interfaz telefónica IVR (respuesta de voz interactiva), que permite a los usuarios finales realizar funciones de Identity Manager a través del teléfono.
- El IDE (entorno de desarrollo integrado) de Identity Manager, que sirve a los desarrolladores para personalizar Identity Manager.
- La consola de Identity Manager, una interfaz de línea de comandos para los administradores.

¿Qué es Identity Manager Service Provider?

Identity Manager Service Provider es una función de administración de identidades centrada en extranets y altamente escalable que puede abastecer y mantener millones de cuentas de usuario final almacenadas en un servidor de directorios LDAP. Service Provider también es capaz de administrar miles de cuentas de administrador y sincronizar datos de cuenta de LDAP con otros recursos.

Service Provider utiliza un subconjunto de las características y la funcionalidad disponibles en Identity Manager. Por ejemplo, no ofrece funcionalidad de auditoría, ya que no resulta tan útil en los entornos de extranet.

Las diferencias entre la funcionalidad estándar de Identity Manager y la de Service Provider se detallan en la sección "Service Provider Features" de *Sun Identity Manager Service Provider 8.1 Deployment*.

Aunque antes se ofrecía como un producto complementario separado, Service Provider ahora forma parte de Identity Manager. No obstante, se necesita una planificación especial para aprovechar la funcionalidad de Service Provider.

- Encontrará información sobre la arquitectura de sistema de Identity Manager Service Provider en "Fundamentos de la arquitectura de sistema de Identity Manager Service Provider" en la página 22.
- Encontrará información para planificar una arquitectura de alta disponibilidad de Identity Manager Service Provider en "Arquitectura de alta disponibilidad recomendada de Service Provider" en la página 32.
- Encontrará información sobre cómo implementar Identity Manager para aprovechar la funcionalidad de Service Provider en *Sun Identity Manager Service Provider 8.1 Deployment* .

Otros productos de administración de identidades de Sun

Además de Identity Manager, otras soluciones de administración de identidades de Sun son Sun Java™ System Directory Server Enterprise Edition, Sun OpenSSO Enterprise y Sun Role Manager. Son productos complementarios para Identity Manager y, en el caso de Role Manager, pueden ampliar la funcionalidad de Identity Manager.

¿Qué es Sun Java System Directory Server Enterprise Edition?

Sun Java System Directory Server Enterprise Edition es un almacén de datos LDAP escalable y de alto rendimiento para información de identidades. Directory Server Enterprise Edition proporciona servicios de directorio principales y otros servicios de datos complementarios. Entre las ofertas de servicios de directorio de la competencia están Active Directory de Microsoft y eDirectory de Novell.

¿Qué es OpenSSO Enterprise?

Sun OpenSSO Enterprise (antes Sun Java System Access Manager y Sun Java System Federation Manager) centraliza e impone una directiva de seguridad completa para las aplicaciones y los servicios web internos y externos. Proporciona funcionalidad de control de acceso seguro y centralizado junto con inicio de sesión único (SSO). También ofrece administración de

identidades federadas, que permite compartir aplicaciones con empresas que tienen tecnologías diferentes de servicios de directorio, seguridad y autenticación. Los socios federados deben mantener una confianza mutua para autenticar a sus respectivos usuarios y responder de sus derechos de acceso a los servicios.

¿Qué es Sun Role Manager?

Sun Role Manager (antes Vaau RBACx) simplifica el cumplimiento de control de acceso mediante la administración del acceso basándose en los roles del usuario dentro de la empresa, en lugar de basarse individualmente en cada usuario. La creación de roles basados en directivas de uso y de empresa permite a las compañías disfrutar de mayor visibilidad sobre el acceso y gestionarlo de una forma más eficiente, segura y conforme.

◆ ◆ ◆ CAPÍTULO 2

Arquitectura del producto

En este capítulo se describe la arquitectura de producto de Sun™ Identity Manager.

Contiene los temas siguientes:

Componentes de Identity Manager

Identity Manager es una aplicación web en la plataforma Java 2, Enterprise Edition (plataforma J2EE™). La plataforma J2EE está formada por un conjunto de servicios, APIs y protocolos estándar que proporcionan funcionalidad para desarrollar aplicaciones de empresa multinivel basadas en web.

La arquitectura del sistema de Identity Manager se distribuye en cuatro niveles lógicos:

- Nivel de usuario
- Nivel de aplicación
- Nivel de base de datos
- Nivel de recursos administrados

En las siguientes secciones se trata cada nivel, empezando por el de aplicación.

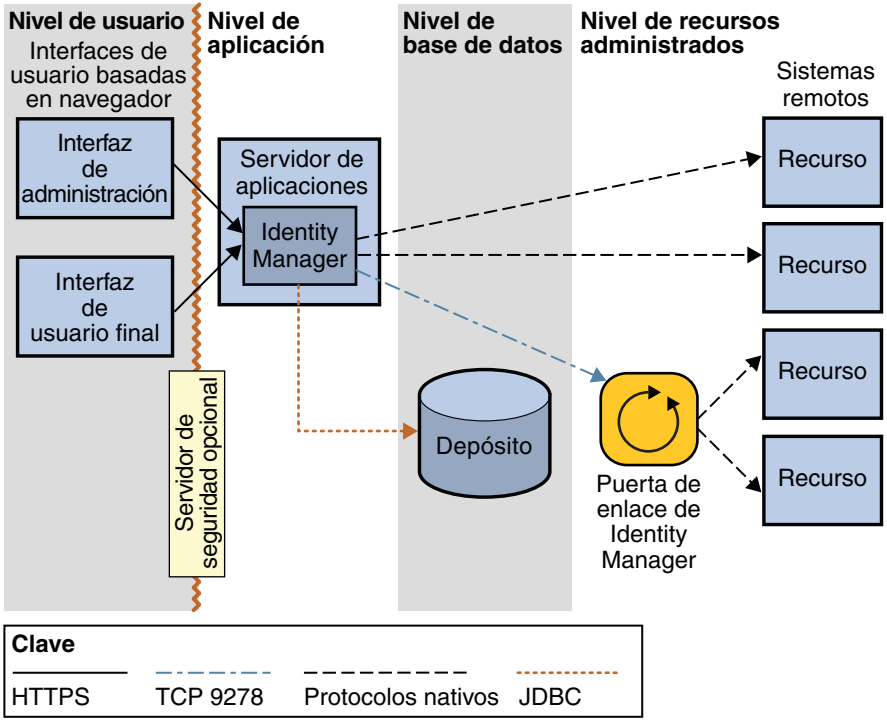

FIGURA 2–1 Arquitectura del sistema de Identity Manager

El nivel de aplicación

Identity Manager (también llamado servidor de Identity Manager) se instala en un contenedor web de J2EE dentro de un servidor de aplicaciones. El servidor de Identity Manager consta de archivos de JSP™, HTML, imágenes y clases de Java™. Los adaptadores y los conectores, que interactúan con otros sistemas de TI (también denominados *recursos*), se encuentran igualmente en el servidor de aplicaciones de Identity Manager.

Nota – En la sección "Servidores de aplicación" de *Notas de la versión de Sun Identity Manager 8.1* encontrará una lista de los servidores de aplicaciones admitidos.

Como Identity Manager es una aplicación web, la interfaz de usuario se halla en el servidor de aplicaciones y las páginas se suministran al nivel de usuario según se solicitan.

Es muy fácil instalar Identity Manager en el servidor de aplicaciones, porque se suministra un instalador gráfico guiado por asistente y, en el caso de los sistemas UNIX®, también hay

disponible un instalador de línea de comandos. El servidor de aplicaciones debe tener integrado o instalado un Kit de desarrollo de Java (JDK™) para ejecutar las clases de Java que realizan acciones dentro de Identity Manager.

El nivel de base de datos

Identity Manager almacena toda la información de abastecimiento y de estado en el *depósito* de Identity Manager. El depósito está formado por tablas que contienen todos los datos de configuración de Identity Manager. Constituye un punto único de consulta de datos y bloqueo de objetos para Identity Manager. El depósito también contiene un registro de auditoría, que es un historial de las acciones efectuadas en Identity Manager. Los datos de Identity Manager se almacenan en formato XML. El depósito puede residir en archivos locales o en una base de datos relacional, si bien ésta es imprescindible en producción.

Nota – En la sección "Servidores de repositorio de bases de datos" de *Notas de la versión de Sun Identity Manager 8.1* encontrará una lista de los servidores de base de datos admitidos.

Tenga presente que, aparte de una mínima información de identidad sobre usuarios individuales, los datos de usuario no se conservan en Identity Manager. En el depósito o repositorio sólo se almacenan los atributos necesarios para identificar y diferenciar a los usuarios dentro de Identity Manager (por ejemplo, *nombre* y *dirección de correo electrónico*).

Identity Manager puede conectarse al depósito mediante una conexión JDBC directa, o bien utilizar la funcionalidad de origen de datos que ofrezca el servidor de aplicaciones.

La funcionalidad de Identity Manager Service Provider requiere un depósito LDAP adicional para almacenar la información de los usuarios. Encontrará información más detallada en "Fundamentos de la arquitectura de sistema de Identity Manager Service Provider" en la página 22.

El nivel de recursos administrados

El nivel de recursos administrados está formado por las aplicaciones y los sistemas de TI para los que se desea abastecer y desabastecer cuentas de usuario. Incluye la puerta de enlace de Identity Manager, una aplicación auxiliar que permite a Identity Manager interactuar con determinados recursos.

Los adaptadores y los conectores proporcionan funciones de administración de usuarios, como crear, actualizar, eliminar y leer cuentas de usuario, o gestión de cambio de contraseñas. Los adaptadores y los conectores también pueden extraer información de cuentas de un sistema remoto.

Nota – Normalmente, Identity Manager administra los datos de usuario en el sistema remoto y no los mantiene en su propio almacén de datos.

Entre los recursos habituales que requieren utilizar la puerta de enlace Sun Identity Manager están Microsoft Exchange, Windows Active Directory, Novell eDirectory (antes Netware Directory Services), Lotus Domino y varios más. (Encontrará la lista completa en la sección "Puerta de enlace de Sun Identity Manager" de *Notas de la versión de Sun Identity Manager 8.1*.) La puerta de enlace se instala como un servicio en Windows y se comunica con Identity Manager mediante el puerto TCP número 9278. La comunicación se inicia en Identity Manager utilizando un protocolo cifrado propietario. A continuación, la puerta de enlace interactúa con los recursos administrados a través de los protocolos nativos de los recursos.

Bajo la perspectiva de la instalación, hay dos tipos de adaptadores y conectores: los de *Identity Manager* y *los personalizados*. Los adaptadores y conectores de Identity Manager están preinstalados en Identity Manager. En cambio, los adaptadores y conectores personalizados deben copiarse en un directorio designado en el directorio de instalación de Identity Manager ubicado en el servidor de aplicaciones.

Es fácil crear adaptadores personalizados con el kit *Resource Extension Facility (REF)* de Identity Manager. El kit REF proporciona la API y diversos adaptadores de plantilla que sirven a las empresas para iniciar enseguida el proceso de desarrollo. Sólo hace falta implementar ocho métodos de Java para obtener la funcionalidad de recursos básica.

El nivel de usuario

El nivel de usuario está formado por los administradores y usuarios finales que interactúan con Identity Manager a través de una de las interfaces de usuario. La interfaz de usuario principal del producto es un navegador browser que se comunica con Identity Manager vía HTTPS. Las dos interfaces basadas en navegador, que son la *interfaz de administración* y la *interfaz de usuario final*, están formadas principalmente por páginas HTML, aunque algunas funciones pueden utilizar applets de Java.

Para mayor claridad, en la figura Figura 2–1 sólo se muestran la interfaz de administración y la interfaz de usuario final. Sin embargo, el nivel de usuario incluye otras interfaces de usuario, como la interfaz telefónica IVR, el IDE de Identity Manager, la interfaz de servicios web SPML y la consola de Identity Manager.

Instrucciones sobre la separación y la proximidad física de los componentes del sistema

Esta sección contiene instrucciones básicas sobre los componentes de Identity Manager que deben ejecutarse en los servidores. También hay recomendaciones sobre los componentes que deben situarse próximos entre sí para reducir los problemas de rendimiento que pueden surgir debido a la latencia y la congestión de la red.

Nota – Aquí sólo se incluyen instrucciones básicas. Encontrará información para diseñar una arquitectura de alta disponibilidad de Identity Manager en el Capítulo 3, "Agrupamiento en clúster y alta disponibilidad".

En un entorno de desarrollo, el servidor de aplicaciones y la base de datos pueden residir en la misma máquina. En cambio, los entornos de prueba y producción requieren que la instancia de Identity Manager se instale en un servidor propio dedicado. También se precisa un servidor dedicado para la base de datos relacional.

La puerta de enlace de Identity Manager, en su caso, debe instalarse en una o más máquinas con Windows. La puerta de enlace es un componente liviano que no requiere un servidor dedicado. Todos los dominios de Windows administrados por una Puerta de enlace deben formar parte del mismo bosque. No es posible administrar dominios traspasando los límites del bosque. Si tiene varios bosques, instale al menos una Puerta de enlace en cada bosque. La puerta de enlace debe tener alta disponibilidad en entornos de producción. Encontrará más información en "Asignación de alta disponibilidad a la puerta de enlace" en la página 30.

En un entorno de producción, el máximo tráfico de red se produce entre los servidores de base de datos y de aplicaciones. Estos dos entornos deben hallarse en la misma LAN con el mínimo salto de red posible. No es necesario que las instancias de puerta de enlace ni los recursos administrados estén en la misma red que Identity Manager.

Para usar Identity Manager con usuarios externos en una configuración de Service Provider, es preciso instalar un conjunto de servidores web en una zona desmilitarizada (DMZ). Encontrará más información dentro de "Arquitectura de alta disponibilidad recomendada de Service Provider" en la página 32.

Arquitectura de sistema de SPML y de servicios web

Se puede utilizar el lenguaje de marcado de abastecimiento de servicios (SPML) y los servicios web de Identity Manager para implementar una arquitectura frontal personalizada para Identity Manager. Identity Manager envía y recibe mensajes y respuestas SPML a través del protocolo HTTPS.

Para obtener más información sobre SPML y servicios web, consulte *Sun Identity Manager 8.1 Web Services*.

Fundamentos de la arquitectura de sistema de Identity Manager Service Provider

En caso de implementar la funcionalidad de Identity Manager Service Provider se necesita un quinto nivel. Se trata del nivel de web, que consta de uno o más servidores web ubicados en una zona desmilitarizada (DMZ). En el nivel de web no se instala ningún componente de Identity Manager. Los servidores web de la DMZ permiten usar uno o más servidores de aplicaciones en el nivel de aplicación respondiendo a las solicitudes de página web. Si se añade uno o más servidores web en el nivel de web, se aumenta la escalabilidad, mientras que si los servidores web se ubican en una DMZ mejora la seguridad de la red.

La funcionalidad de Service Provider también precisa un depósito LDAP, que reside en el nivel de base de datos. Como el depósito LDAP puede ser un recurso administrado, también se puede considerar que el servidor LDAP reside en el nivel de recursos administrados.

Nota – Cuando sólo se implementa Service Provider, se recomienda tener un depósito de Identity Manager además del depósito LDAP, aunque no es indispensable. Si no se implementa un depósito de Identity Manager, no estarán disponibles ciertas funciones, como algunas de informes.

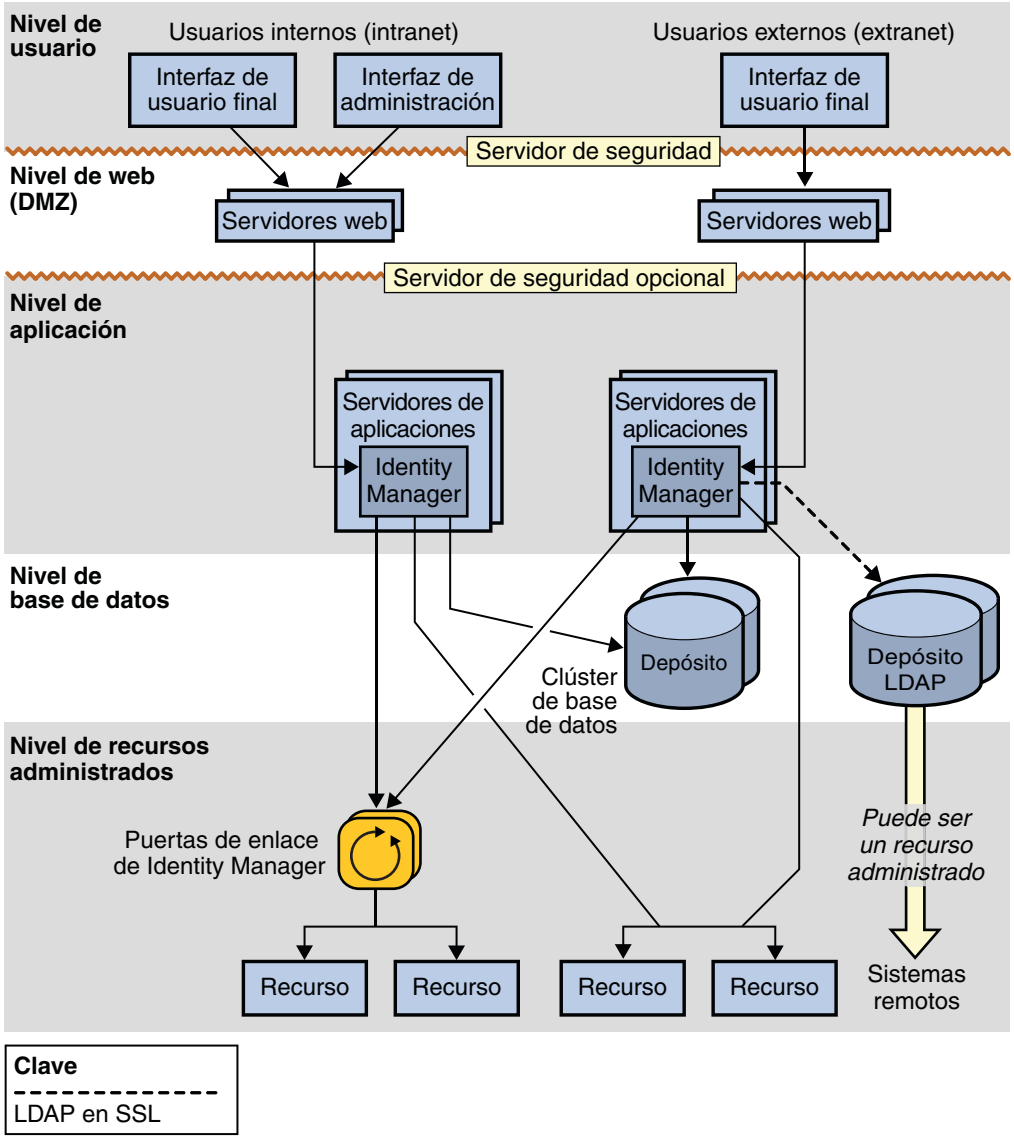

FIGURA 2–2 Arquitectura de sistema de Identity Manager Service Provider

◆ ◆ ◆ CAPÍTULO 3

Agrupamiento en clúster y alta disponibilidad

Este capítulo ofrece orientación para implementar un entorno de Identity Manager de alta disponibilidad / tolerante a fallos (HA/FT).

Nota – Consulte las prácticas recomendadas para asegurar una implementación de alta disponibilidad con cada tecnología en la documentación de su servidor web, servidor de aplicaciones y proveedor de base de datos. Esta guía no sustituye en absoluto a las recomendaciones específicas de los proveedores sobre los servidores web.

Evaluación de los requisitos de disponibilidad

En esta sección se explica cómo evaluar cuánta disponibilidad requiere una implementación específica.

Cálculo del coste del tiempo de inactividad

Como Identity Manager no se halla en la ruta de transacción entre los usuarios generales y los sistemas y aplicaciones a los que ya tienen acceso, el tiempo de inactividad de Identity Manager no se convierte en la pesadilla que podríamos temer. Si Identity Manager no está disponible, los usuarios finales aún pueden acceder a los recursos a través de sus cuentas abastecidas.

El coste principal del tiempo de inactividad de Identity Manager es la pérdida de productividad. Si Identity Manager no funciona, los usuarios finales no pueden utilizarlo para obtener acceso a los sistemas que tienen bloqueados o desabastecidos.

La primera cifra necesaria para calcular el coste del tiempo de inactividad es el coste medio por la pérdida de productividad de los usuarios finales que no pueden acceder a recursos de computación dentro de la empresa. En nuestra evaluación, esta cifra se denomina *productividad por hora de empleado*.

La otra cifra importante que interesa averiguar es el porcentaje de usuarios finales del total de usuarios que necesitan utilizar Identity Manager a cualquier hora. Esta población suele incluir las nuevas incorporaciones que es preciso abastecer y los usuarios finales que han olvidado su contraseña, en caso de que la administración de contraseñas forme parte de la implementación.

Consideremos la siguiente situación hipotética:

Número total de empleados	20.000
Número diario de contraseñas restablecidas	130
Número diario de nuevas incorporaciones	30
Número de horas de trabajo diarias	8

En esta situación específica se puede calcular lo siguiente:

- El número de empleados que necesitan Identity Manager a cualquier hora = (130 + 30) / 8 = 20
- El porcentaje de empleados que necesitan Identity Manager a cualquier hora = 20 / 20.000 = 0,1% o 1 de 1.000

Estas cifras nos permiten estimar el coste de una interrupción del funcionamiento de Identity Manager:

Productividad por hora de empleado	100$	
Pérdida de productividad	0,5	(50% de reducción de la productividad por la imposibilidad de acceder al sistema)
Número de empleados afectados	20	
Subtotal	1.000$	

Duración de la interrupción	2 horas
Pérdida total inmediata	2.000$

Este ejemplo indica que incluso aunque el número de usuarios administrados por Identity Manager sea alto, el número de usuarios que necesitan Identity Manager para obtener acceso a los sistemas a cualquier hora suele ser bajo.

Otro factor importante es que el tiempo que se tarda en volver a poner en funcionamiento un sistema como Identity Manager suele ser inferior al tiempo que se tarda en ejecutar los procesos de abastecimiento manuales que automatiza Identity Manager. Por tanto, aunque el tiempo de inactividad de Identity Manager acarrea un coste, suele ser menor que el coste de utilizar procesos manuales para proporcionar a los usuarios acceso a los recursos.

Causas del tiempo de inactividad

Al planificar una implementación de Identity Manager de alta disponibilidad, vale la pena determinar las causas del tiempo de inactividad.

Son las siguientes:

- Error del operador
- Fallo de hardware
- Fallo de software
- Tiempo de inactividad programado (actualizaciones de hardware y software)
- Bajo rendimiento (tiempo de inactividad percibido)

Cálculo de la rentabilidad de la inversión

Identity Manager automatiza los procesos y reduce la pérdida de productividad. La rentabilidad de invertir en una arquitectura de Identity Manager de alta disponibilidad se consigue al minimizar el tiempo de inactividad y evitar la pérdida de productividad.

El coste del tiempo de inactividad se puede aprovechar para averiguar cuánta disponibilidad se necesita en último término para Identity Manager. En general, una inversión moderada para que Identity Manager esté altamente disponible.

Al calcular el coste de la inversión, recuerde que adquirir hardware y software de HA/FT es sólo una parte de la implementación de una solución disponible. Otro coste es contar con personal experto para mantenerla activa y funcionando.

Características de alta disponibilidad de Identity Manager

Identity Manager está diseñado para aprovechar la infraestructura de alta disponibilidad que pueda haber. Por ejemplo, Identity Manager no necesita un clúster de servidores de aplicaciones para lograr alta disponibilidad, pero puede aprovecharlo si existe.

El diagrama siguiente ilustra los principales componentes de Identity Manager implementados en una arquitectura no redundante. En las secciones siguientes se explica cómo asignar alta disponibilidad al depósito, el servidor de aplicaciones y la puerta de enlace de Identity Manager.

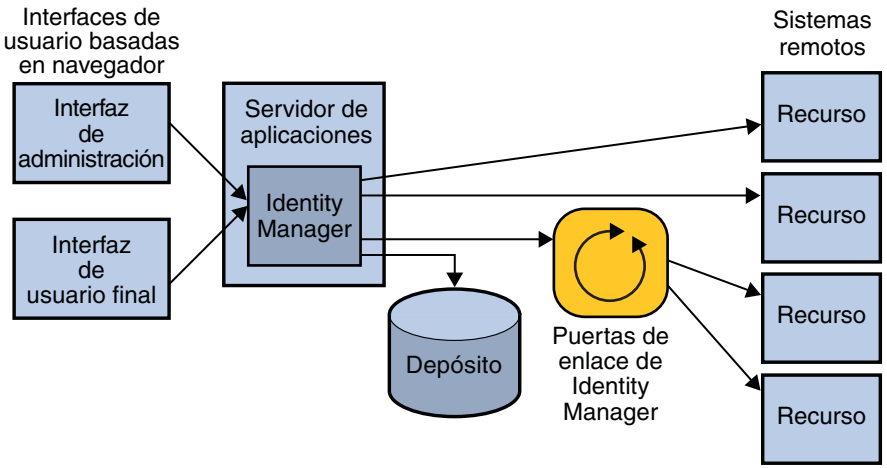

FIGURA 3–1 Arquitectura del sistema estándar de Identity Manager

Nota – En "Instrucciones sobre la separación y la proximidad física de los componentes del sistema" en la página 21 encontrará información sobre los componentes que deben situarse próximos entre sí para reducir los problemas de rendimiento que pueden surgir debido a la latencia y la congestión de la red.

Asignación de alta disponibilidad al depósito

Identity Manager almacena toda la información de abastecimiento y de estado en el depósito de Identity Manager.

La disponibilidad de la instancia de la base de datos donde se almacena el depósito de Identity Manager es el factor más crítico para lograr una implementación de Identity Manager altamente disponible. El depósito representa toda la instalación de Identity Manager, y los datos

que contiene deben protegerse, como en el caso de otras aplicaciones de base de datos importantes. Como mínimo hay que realizar copias de seguridad periódicas.

Nota – No aloje el depósito de Identity Manager en una plataforma virtual, como una máquina virtual VMware, porque se verá seriamente afectado el rendimiento (transacciones por segundo).

Sólo puede haber una imagen del depósito. No es posible tener dos bases de datos distintas para Identity Manager e intentar sincronizarlas por las noches. Sun recomienda usar las funciones de duplicación o agrupamiento en clúster de la base de datos para proporcionar tolerancia a fallos.

Asignación de alta disponibilidad al servidor de aplicaciones

Identity Manager puede ejecutarse dentro de un clúster de servidores de aplicaciones y aprovechar la mayor disponibilidad y equilibrio de carga que ofrece el clúster. Sin embargo, Identity Manager no usa las funciones de J2EE que requieren agrupamiento en clúster.

Identity Manager utiliza el objeto de sesión HTTP que está disponible a través de la API de servlet. Este objeto de sesión lleva un seguimiento de la visita del usuario cuando éste inicia la sesión y realiza acciones. Un clúster ofrece la posibilidad de que varios nodos gestionen las solicitudes del usuario durante una sesión concreta. Sin embargo, esto suele estar desaconsejado y la mayoría de las instalaciones se configuran para enviar al mismo servidor la solicitud completa de un usuario para una sesión determinada.

Es posible ampliar la disponibilidad y la capacidad del servidor de aplicaciones donde se ejecuta Identity Manager incluso sin configuración de clúster. Para ello, se instalan varios servidores de aplicaciones con Identity Manager, se conectan al mismo depósito y se sitúa un equilibrador de carga con *afinidad de sesiones* al frente de todos los servidores de aplicaciones.

Nota – Para obtener más información sobre la afinidad de sesiones, consulte "Preguntas frecuentes sobre afinidad de sesiones y persistencia de sesiones" en la página 40.

Identity Manager ejecuta determinadas tareas en segundo plano, por ejemplo, las tareas de reconciliación programadas. Estas tareas se almacenan en la base de datos y cualquier servidor de Identity Manager puede seleccionarlas para su ejecución. Identity Manager utiliza la base de datos para asegurarse de que estas tareas siempre se ejecuten por completo, incluso en caso de conmutación por error a otro nodo.

Configuración de clúster de Active Sync en nodos de servidor de aplicaciones

El valor de configuración `sources.hosts` del archivo `Waveset.properties` determina qué hosts de un entorno de instancias múltiples se utilizan para ejecutar las solicitudes de Active Sync. Este valor proporciona una lista de hosts donde pueden ejecutarse adaptadores de origen. Si se configura en *localhost* o *null*, los adaptadores de origen podrán ejecutarse en cualquier host de la granja de servidores web. (Éste es el comportamiento predeterminado.) Con una lista de uno o más hosts, puede restringir la ejecución a dicha lista. Si hay actualizaciones entrantes que proceden de otro sistema y van a un host concreto, utilice el valor `sources.hosts` para registrar los nombres de host.

También puede definir una propiedad llamada `sources.` *resourceName* `.hosts`, que controla dónde se ejecutará la tarea de Active Sync del recurso. Sustituya *resourceName* por el nombre del objeto de recurso que desea especificar.

Asignación de alta disponibilidad a la puerta de enlace

Identity Manager necesita una puerta de enlace liviana para administrar los recursos a los que no se puede acceder directamente desde el servidor. Ello incluye los sistemas que requieren llamadas a la API en el lado del cliente que son específicas de la plataforma. Por ejemplo, si Identity Manager se ejecuta en un servidor de aplicaciones basado en UNIX, no es posible realizar llamadas NTLM o ADSI a dominios administrados de NT o Active Directory. Como Identity Manager necesita una puerta de enlace para administrar estos recursos, es importante asegurarse de que la puerta de enlace de Identity Manager esté altamente disponible.

Para evitar que la puerta de enlace constituya un único punto de fallo, Sun recomienda ejecutar una instancia de puerta de enlace en varias máquinas. Conviene configurar un dispositivo de enrutamiento de red para suministrar conmutación por error en caso de que sucumba la instancia principal de la puerta de enlace. El dispositivo de conmutación por error debe configurarse para sesiones persistentes y utilizar un único esquema de operación por turnos. ¡No sitúe las puertas de enlace detrás de un dispositivo equilibrador de carga! Esta configuración no es compatible y hará que fallen algunas funciones de Identity Manager.

Todos los dominios de Windows administrados por una Puerta de enlace deben formar parte del mismo bosque. No es posible administrar dominios traspasando los límites del bosque. Si tiene varios bosques, instale al menos una Puerta de enlace en cada bosque.

Las herramientas de supervisión de Win32 pueden configurarse para observar el proceso de `gateway.exe` en el host de Win32. En caso de que falle `gateway.exe`, el proceso podrá reiniciarse automáticamente.

Arquitectura de alta disponibilidad recomendada

El diagrama siguiente ilustra la arquitectura de Identity Manager que Sun recomienda cuando no existe ninguna infraestructura de aplicación web.

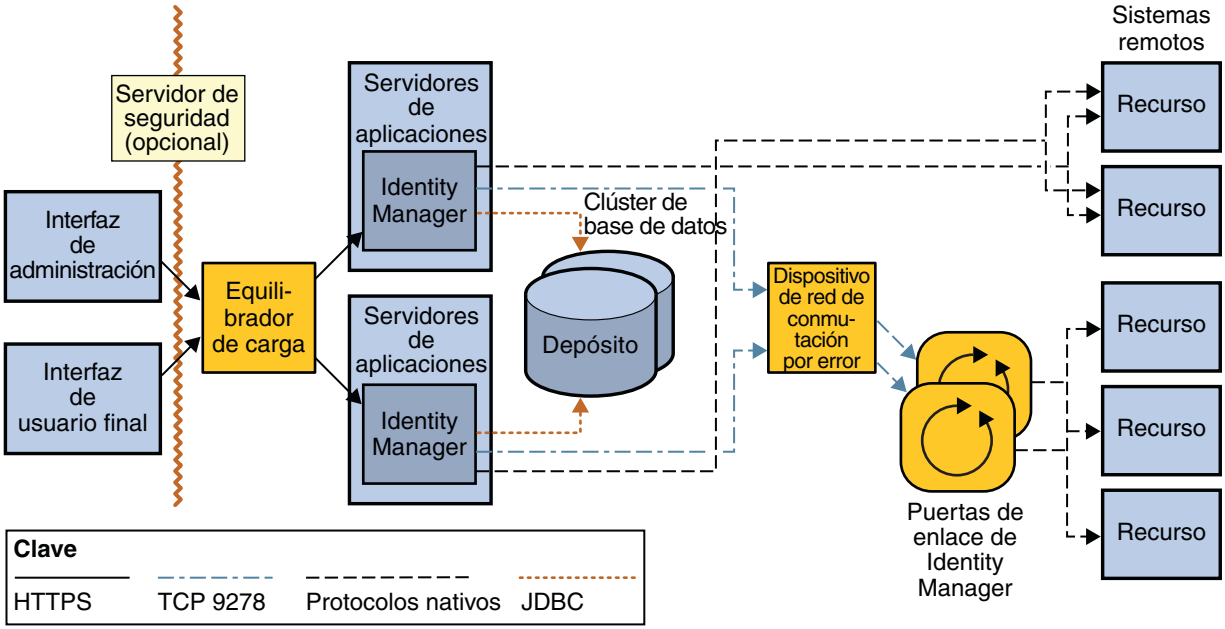

FIGURA 3–2 Arquitectura de alta disponibilidad de Identity Manager

En una implementación real, conviene utilizar en la mayor medida posible la infraestructura de servidor de aplicaciones redundante existente. El valor de esta arquitectura estriba en que sólo utiliza equilibradores de carga para lograr la redundancia en el servidor de aplicaciones. Los equilibradores de carga con afinidad de sesiones detectan las instancias de servidor de aplicaciones fallidas y conmutan por error a las instancias activas. Los equilibradores de carga también sirven para aportar escalamiento horizontal al entorno web repartiendo las solicitudes de usuario entre un clúster de servidores.

Aunque se trata de una arquitectura sencilla, las características de tiempo de actividad son equiparables a las de implementaciones más complejas. Dada su simplicidad, hay menos software que mantener y supervisar o menos piezas que puedan fallar. Como la causa principal del tiempo de inactividad son los errores humanos, una solución relativamente simple puede aportar mejores características de tiempo de actividad que otras más complejas. No existe una respuesta universal acertada. Lo que importa es conocer todas las causas del tiempo de inactividad y elegir la arquitectura que entrañe la mejor disponibilidad para el entorno.

Nota – Es imposible describir todas las distintas arquitecturas HA que pueden establecerse con una aplicación web como Identity Manager.

Como Identity Manager se puede implementar con gran variedad de combinaciones, quizá resulte más económico identificar la infraestructura existente y aprovecharla todo lo posible al implantar Identity Manager.

Arquitectura de alta disponibilidad recomendada de Service Provider

Si se va a utilizar la funcionalidad de Identity Manager Service Provider, Sun recomienda añadir un nivel de web entre el nivel de usuario y el de aplicación. El nivel de web consta de uno o varios servidores web ubicados en una zona desmilitarizada (DMZ) y separada del nivel de aplicación por un servidor de seguridad.

Para utilizar la funcionalidad de Service Provider se necesita un depósito LDAP. Cuando Identity Manager sólo va a usarse con clientes de extranet, se recomienda un depósito estándar de Identity Manager, aunque no es imprescindible. En cambio, si Identity Manager se va a utilizar con usuarios de intranet y de extranet, es indispensable un depósito estándar de Identity Manager.

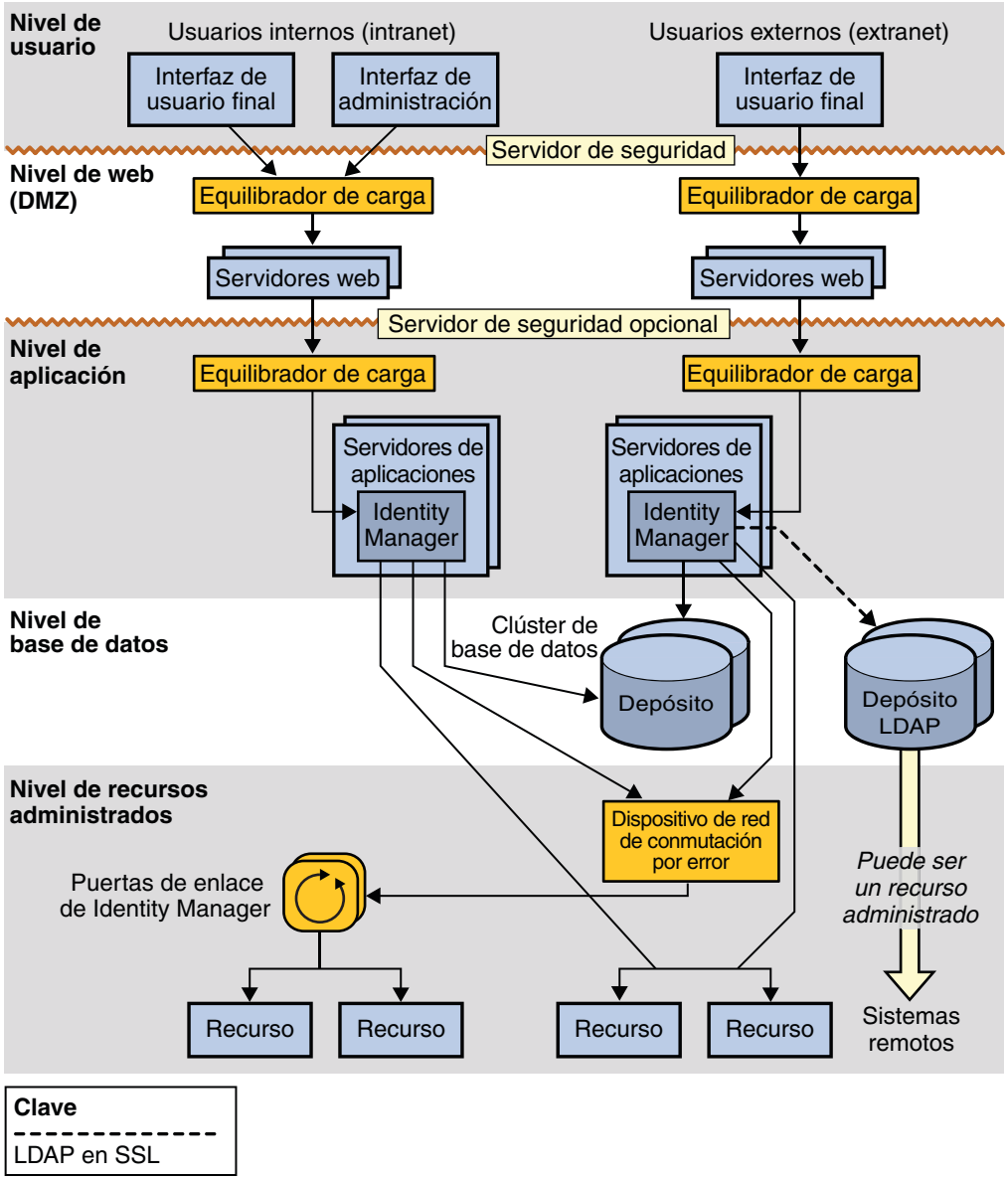

FIGURA 3–3 Arquitectura de alta disponibilidad de Identity Manager Service Provider

Escenarios de fallos

En esta sección se describen ocho escenarios de fallos y se comparan dos implementaciones: una con persistencia de sesiones y otra sin ella.

- La implementación *con* persistencia de sesiones incluye afinidad de sesiones en un equilibrador de carga. La implementación consta de diversas instancias en un clúster que tienen habilitado algún tipo de persistencia de sesiones de manera que los cambios de sesión se graben en un nodo de depósito físicamente diferenciado.
- La implementación *sin* persistencia de sesiones incluye afinidad de sesiones en un equilibrador de carga y diversas instancias que no forman parte de un clúster.

Escenario 1: fuera del flujo de trabajo

Descripción del escenario

El usuario final o el administrador editan un formulario no perteneciente a un flujo de trabajo. Deja de funcionar la instancia donde el usuario ha establecido la sesión.

Sin persistencia de sesiones

Experiencia de usuario: Una conmutación por error no transparente. Tras enviar el formulario, se devuelve al usuario a la página de inicio de sesión.

Acciones de recuperación: El usuario reintroduce su nombre de usuario y contraseña. A continuación, Identity Manager procesa el formulario y presenta los resultados en la página inmediatamente posterior a la de inicio de sesión.

Con persistencia de sesiones

Experiencia de usuario: El formulario del usuario se envía y los resultados se devuelven sin que salga de la sesión y deba volver a iniciarla.

Acciones de recuperación: No es necesaria ninguna acción del usuario.

Otros escenarios de ejemplo

- Un usuario final ha iniciado una sesión y ha recuperado los resultados de búsqueda de usuarios u otros objetos del depósito cuando la instancia deja de funcionar.
- Un administrador está a punto de enviar una solicitud de restablecimiento de contraseña o de edición de usuario a través de la interfaz de administración cuando la instancia deja de funcionar.

Escenario 2: Con flujo de trabajo en curso

Descripción del escenario

El usuario final o el administrador han enviado un formulario que ha activado un flujo de trabajo. La instancia donde se ejecuta el flujo de trabajo y donde se encuentra la sesión del usuario suele ser la misma, excepto con algunas tareas programadas, que pueden realizarse en distintas instancias. Esta instancia deja de funcionar mientras el flujo de trabajo está en curso.

Sin persistencia de sesiones

Experiencia de usuario: Una conmutación por error no transparente. El envío del formulario devuelve el usuario a la página de inicio de sesión. La instancia de la tarea del flujo de trabajo que se está ejecutando debe estar en el depósito, pero como el nodo de ejecución no funciona, el estado del flujo de trabajo es "terminado".

Acciones de recuperación: El flujo de trabajo debe volver a enviarse. Para ello hay que regresar al mismo formulario y reintroducir la misma información que sirvió para activar el flujo de trabajo antes de que fallara el nodo.

Enviar los mismos datos de solicitud no siempre funciona. Si el flujo de trabajo abastece más de un recurso durante su ejecución y alguno de esos recursos se había abastecido antes del fallo, el reenvío del flujo de trabajo por parte del usuario tendría que asumir los recursos ya abastecidos. No olvide que el flujo de trabajo terminado persiste en el depósito hasta que `resultLimit` caduca en el objeto `TaskInstance` .

Con persistencia de sesiones

Experiencia de usuario: Una conmutación por error no transparente. El usuario no logra cerrar la sesión porque es persistente y se restablece en la nueva instancia. Sin embargo, el envío del formulario seguramente generará un error, porque el flujo de trabajo se habrá terminado. Se trata de una conmutación por error no transparente, ya que son necesarias acciones de recuperación.

Acciones de recuperación: Las mismas que sin persistencia de sesiones. El usuario debe reenviar la solicitud que desactivó el flujo de trabajo anterior con parámetros iguales o modificados.

Otros escenarios de ejemplo

- Un usuario final acaba de enviar una solicitud de registro automático para crear una cuenta de Identity Manager y la instancia deja de funcionar.
- Un administrador acaba de enviar una solicitud de restablecimiento de contraseña que se halla en curso cuando la instancia deja de funcionar.

Escenario 3: Flujo de trabajo suspendido o postergado

Descripción del escenario

Este escenario abarca situaciones en que el flujo de trabajo ha comenzado, pero está esperando que un aprobador realice una acción manual.

Sin persistencia de sesiones

Experiencia de usuario: Conmutación por error transparente con respecto al aprobador siempre que éste aún no haya iniciado la sesión. Tras fallar el nodo, cuando el aprobador inicia la sesión todavía aparece la solicitud de aprobación en su bandeja de entrada, incluso aunque la solicitud haya sido activada desde un nodo que ha quedado inactivo.

Acciones de recuperación: No es necesaria ninguna acción del usuario.

Con persistencia de sesiones

Experiencia de usuario: La misma que sin persistencia de sesiones.

Acciones de recuperación: Las mismas que sin persistencia de sesiones.

Otros escenarios de ejemplo

- El flujo de trabajo está suspendido, por ejemplo, una acción manual pendiente de una fecha inicial o final de un empleado.
- Un administrador envió una solicitud de creación cuya aprobación se halla a la espera de que un aprobador inicie la sesión. El nodo desde donde se envió la solicitud ha fallado antes de que el aprobador pueda aprobarla.

Escenario 4: Edición de un elemento de trabajo

Descripción del escenario

Este escenario incluye los casos en que un usuario está editando un elemento de trabajo y el nodo donde se halla la sesión del usuario deja de funcionar antes de poder enviar el elemento de trabajo.

Sin persistencia de sesiones

Experiencia de usuario: Una conmutación por error no transparente. Cuando se envía el formulario de edición del elemento de trabajo, se cierra la sesión del usuario, que vuelve a la página de inicio de sesión.

Acciones de recuperación: Tras reenviar las credenciales de inicio de sesión, el elemento de trabajo del usuario se marca como completado y el flujo de trabajo puede reanudarse a partir de

ese punto. El flujo de trabajo debe seleccionarse en el nuevo modo para ejecutarlo a partir del punto en que se ha marcado como completada la acción manual del usuario.

Con persistencia de sesiones

Experiencia de usuario: Cuando se envía el formulario de edición del elemento de trabajo, el usuario ve el resultado de dicho envío; por ejemplo, el siguiente formulario del flujo de trabajo personalizado si lo hay o un mensaje satisfactorio.

Acciones de recuperación: No es necesaria ninguna acción del usuario.

Otros escenarios de ejemplo

- Un usuario final está rellenando un formulario asociado a una acción manual en un flujo de trabajo personalizado, por ejemplo, para solicitar acceso a determinados recursos. Antes de que el usuario pueda enviar la solicitud, sucumbe el nodo donde se halla la sesión del usuario.
- Un administrador ha iniciado la sesión en Identity Manager y ha abierto una solicitud de aprobación para editar. Antes de poder enviar la solicitud, falla el nodo donde se halla la sesión del administrador.

Escenario 5: Tareas programadas en curso

Descripción del escenario

Este escenario abarca los casos en que falla un nodo mientras está en curso una reconciliación o durante la ejecución de un informe.

Sin persistencia de sesiones

Experiencia de usuario: La tarea programada termina durante el proceso.

Acciones de recuperación: Hay que reiniciar la tarea programada que estaba realizándose. La tarea volverá a empezar desde el principio. (La tarea no se reiniciará a partir del punto de fallo.) Es parecido a crear e iniciar una tarea nueva.

Con persistencia de sesiones

Experiencia de usuario: La misma que sin persistencia de sesiones.

Acciones de recuperación: Las mismas que sin persistencia de sesiones.

Otros escenarios de ejemplo

- Un adaptador de Active Sync está configurado para ejecutarse en el nodo fallido.

Escenario 6: Tarea programada en suspensión

Descripción del escenario

Este escenario abarca los casos en que el flujo de trabajo personalizado de un usuario tiene una tarea programada para ejecutarse en una fecha posterior en un nodo específico. Antes de la fecha programada, falla el nodo donde estaba programada la tarea.

Sin persistencia de sesiones

Experiencia de usuario: La conmutación por error es transparente con respecto a las acciones de recuperación necesarias para asegurar la ejecución de esta tarea en la fecha prevista.

Acciones de recuperación: Cualquier nodo activo asume la tarea programada cuando llega la fecha de ejecución prevista.

Con persistencia de sesiones

Experiencia de usuario: La misma que sin persistencia de sesiones.

Acciones de recuperación: Las mismas que sin persistencia de sesiones.

Otros escenarios de ejemplo

- Mientras se crea una cuenta de usuario, se utiliza el Analizador de tareas aplazadas para implementar la habilitación de una cuenta en una fecha inicial o para implementar la deshabilitación de la cuenta en una fecha final. Antes de que llegue la fecha inicial o final, falla el nodo donde se había programado la tarea.
- Se ha programado un informe para que se ejecute en una fecha futura o una reconciliación para que se ejecute a una hora concreta, pero antes de ese momento falla el nodo donde se había programado la tarea.

Escenario 7: Solicitud de flujo de trabajo de servicios web aún no recibida por Identity Manager

Descripción del escenario

Este escenario abarca los casos en que no se utiliza la GUI de Identity Manager para iniciar el abastecimiento. En su lugar, la interfaz de usuario la suministra una aplicación que realiza una llamada interna a Identity Manager a través de SPML u otra interfaz de servicio web personalizada. La sesión relacionada con el usuario a través de la interfaz de usuario se administra mediante la aplicación que realiza la llamada. Para Identity Manager, todas las solicitudes se inician como asunto del administrador de SOAP ("soapadmin").

En tal caso de uso, este escenario de fallo abarca las situaciones en que aún no se ha recibido la solicitud por medio del punto final de Identity Manager y falla el nodo de destino.

Sin persistencia de sesiones

Experiencia de usuario: Una conmutación por error transparente. Las credenciales del administrador de SOAP se transmiten con cada solicitud de SOAP, ya sea mediante conexión o dentro de Identity Manager con un valor de configuración `Waveset.properties`. En tanto que el nodo que debía recibir esta solicitud de SOAP no la ha recibido antes de fallar, la conmutación por error es transparente con o sin persistencia de sesiones.

Acciones de recuperación: No es necesaria ninguna acción. La solicitud de SOAP se envía a un nodo activo que la ejecuta.

Con persistencia de sesiones

Experiencia de usuario: La misma que sin persistencia de sesiones.

Acciones de recuperación: Las mismas que sin persistencia de sesiones.

Escenario 8: Solicitud de flujo de trabajo de servicios web en curso por Identity Manager

Descripción del escenario

Es similar al escenario 7. La única diferencia es que el flujo de trabajo se está efectuando cuando el nodo falla, o que el nodo ha recibido la solicitud de SOAP cuando falla.

Sin persistencia de sesiones

Experiencia de usuario: Es similar al escenario 2 (flujo de trabajo en curso). El flujo de trabajo se marca como terminado y el usuario ve un error como resultado de la solicitud de SOAP.

Acciones de recuperación: El usuario debe reenviar el formulario con parámetros iguales o modificados (según dónde se produzca el fallo en el flujo de trabajo) a través de la interfaz de usuario en la aplicación de terceros.

Con persistencia de sesiones

Experiencia de usuario: La misma que sin persistencia de sesiones.

Acciones de recuperación: Las mismas que sin persistencia de sesiones.

Preguntas frecuentes sobre afinidad de sesiones y persistencia de sesiones

¿Debe estar habilitada la afinidad de sesiones al escalar horizontalmente los servidores de aplicaciones?

Sí.

¿Debe haber persistencia de sesiones al escalar horizontalmente los servidores de aplicaciones?

A no ser que sus requisitos de negocio hagan especial hincapié en tener conmutación por error transparente en las raras circunstancias en que la persistencia de sesiones puede suponer una diferencia, Sun desaconseja el uso de persistencia de sesiones. La persistencia de sesiones produce un deterioro específico del rendimiento, por lo que conviene prescindir de ella salvo que los requisitos de negocio impongan a toda costa la conmutación por errores transparente.

Si analiza las situaciones expuestas en "Escenarios de fallos" en la página 34, comprobará que seis de los casos no presentan ninguna diferencia en cuanto a la experiencia del usuario o las acciones de recuperación necesarias, con independencia de que esté habilitada la persistencia de sesiones. Sólo los escenarios 1 y 4 presentan diferencias en los casos con y sin persistencia de sesiones.

En ambos escenarios, la persistencia de sesiones puede aportar cierta transparencia a la conmutación por error, pero siempre a costa del rendimiento. Según el tamaño de los objetos de sesión, el depósito utilizado para la persistencia de sesiones y la optimización del código de administración de sesiones del servidor de aplicaciones específico, el rendimiento puede resultar perjudicado entre un 10% y un 20%, o incluso más.

¿Debe haber varias instancias de servidor de aplicaciones en un clúster al escalar horizontalmente?

No hay ninguna necesidad de tener varias instancias de servidor de aplicaciones salvo que se quiera persistencia de sesiones. Se puede conseguir conmutación por error sin persistencia de sesiones incluso aunque todos los nodos de servidor de aplicaciones no se encuentren en un clúster.