

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Las arquitecturas tecnológicas modernas demandan estándares que permitan la integración completa.

OpenLDAP es una alternativa a esta propuesta

Andrés Ricardo Almanza Junco

andres.almanza@ubiquando.com.co

Junio 2004

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Plan de Temas

- ★ Importancia de los sistemas de Directorios
- ★ Single Sign On
- ★ Esquemas de Implementación
- ★ Consideraciones de implementación de los sistemas Single Sing On en ambientes Open Source.
- ★ Conclusiones.
- ★ Bibliografía

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Importancia de los Sistemas de Directorios

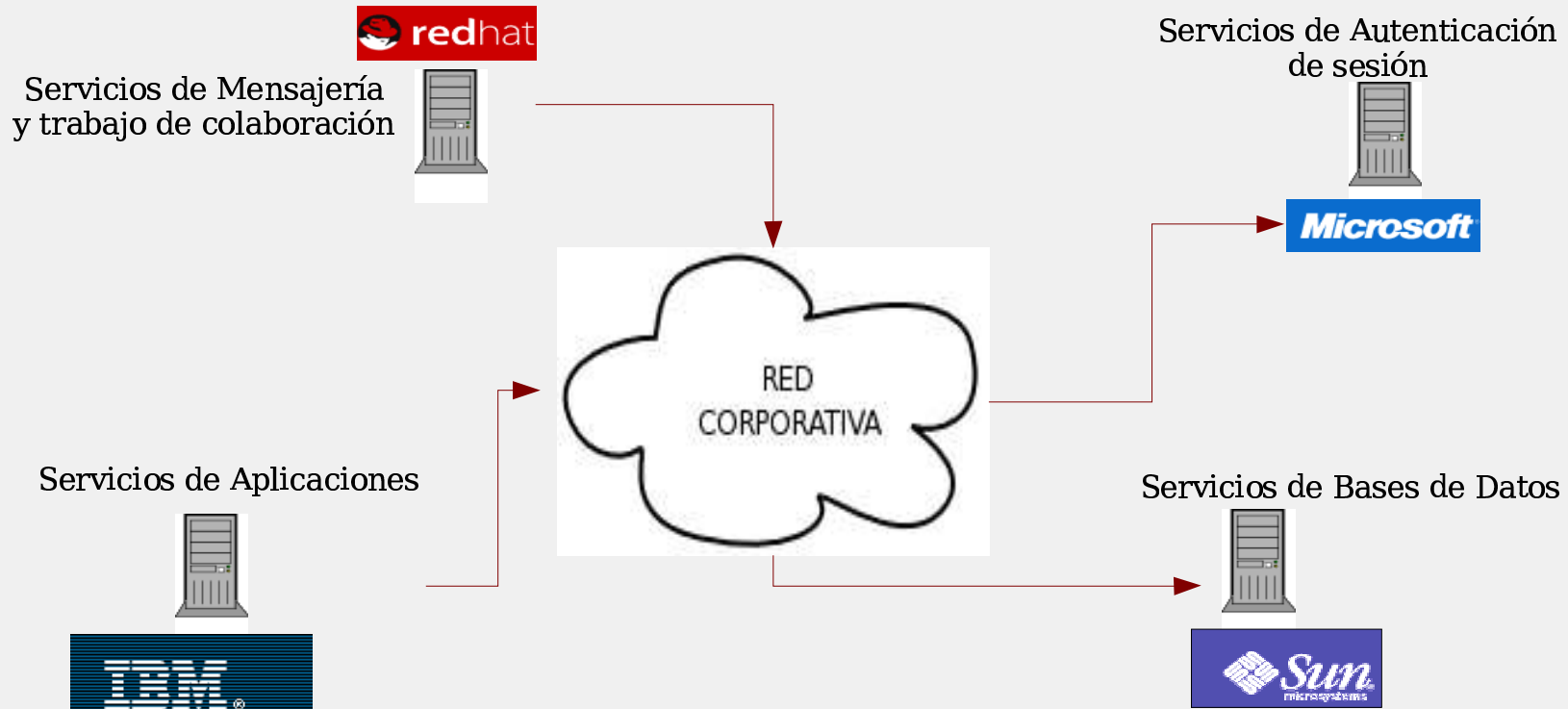
◆ Directorios

- ★ Listado de información sobre los objetos dispuestos con algún orden.
- ★ Estructura que permite el manejo y organización de la información.
- ★ En términos de informática, un directorio es una base de datos especializada, también llamado un repositorio de datos.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Importancia de los Sistemas de Directorios

- ♦ Infraestructuras de tecnologías complejas y no homogénea.



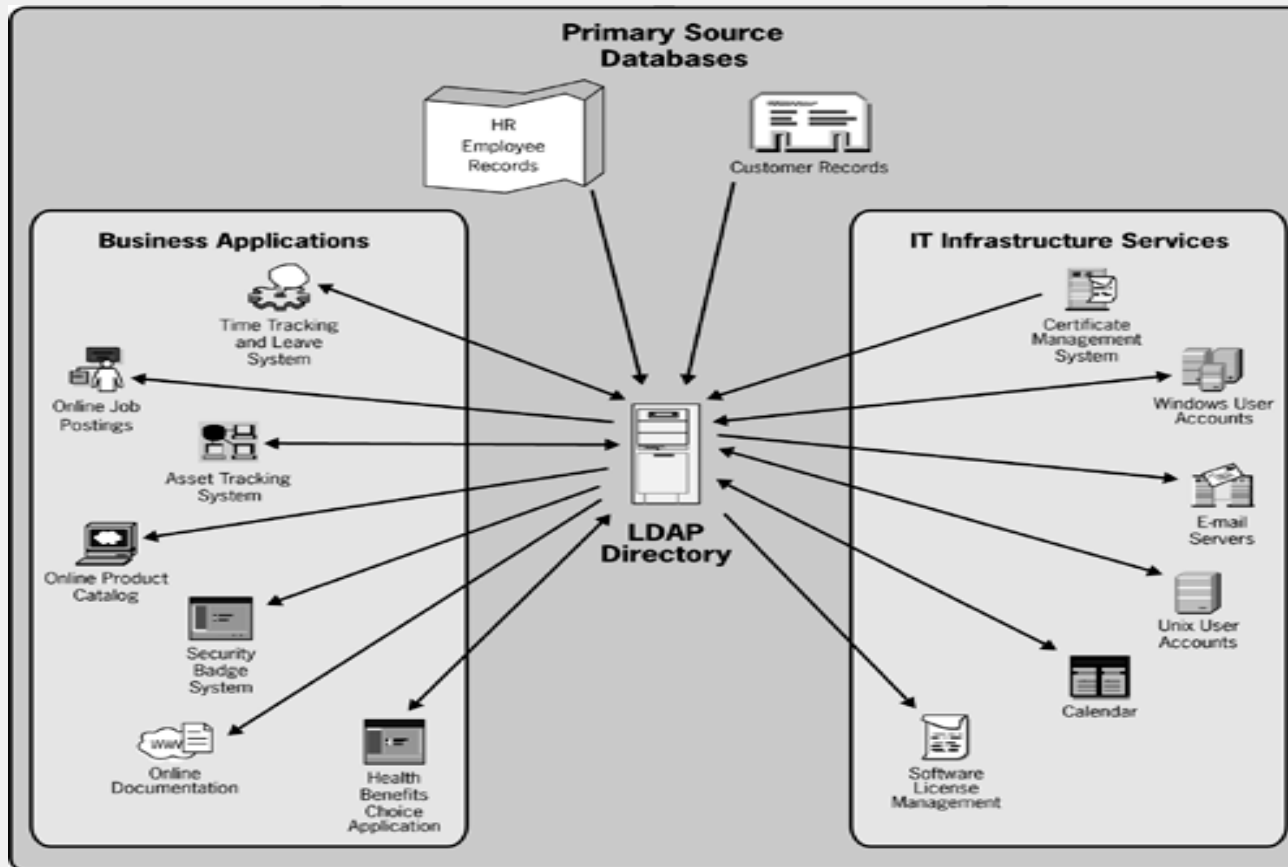
Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Importancia de los Sistemas de Directorios

- ▶ Permiten ordenar y manejar la información.
- ▶ Permiten centralizar la información, disminuyendo redundancia y facilitando la administración.
- ▶ Ayuda a optimizar los procesos del negocio.
- ▶ El estándar LDAP, ha sido ampliamente aceptado, como una solución ideal de acceso a directorios.
- ▶ Independencia de los proveedores de soluciones de Directorios.
- ▶ Unificación de accesos a recursos de red.
- ▶ Múltiples formas de manejo de la información (esquemas), y extensibles.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Importancia de los Sistemas de Directorios



Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Single Sign On

- ♦ *Es la capacidad de ingresar por mediante un solo conjunto de credenciales, a los diferentes recursos informáticos a los que se encuentre autorizados.*
- ♦ Es en este punto donde el sistema de directorios juega un papel importante.
- ♦ Mejora las labores de administración y seguridad de la infraestructura de servicios.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Single Sign On

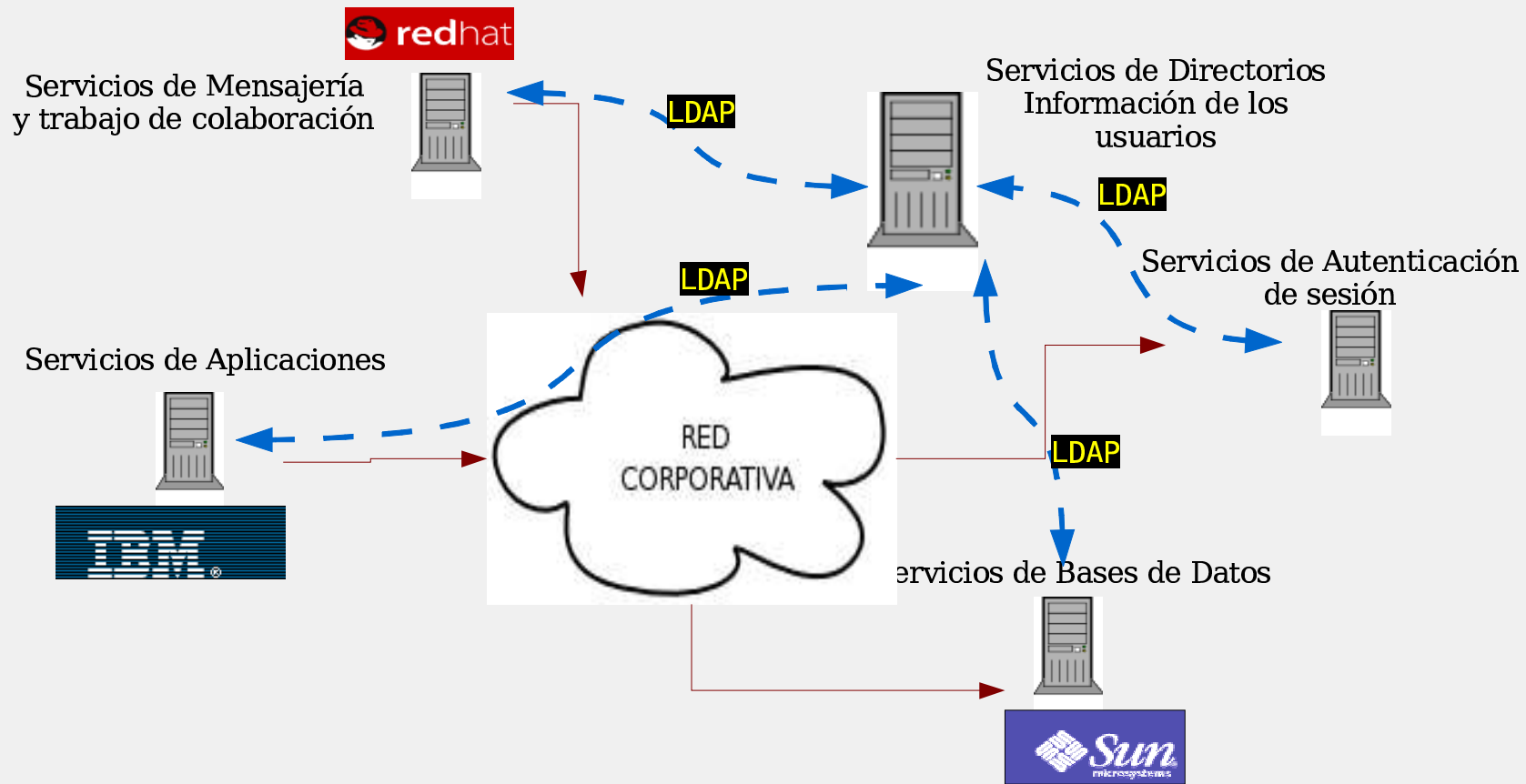
- ✦ No es una necesidad obligatorio ingresar una única vez las credenciales para ingresar a todos los recursos informáticos, mas en infraestructuras tecnológicas heterogéneas (single login).

✦ Sincronización Vs Single Sign On

- ✦ Sincronización = Mas de un sistema de autenticación
- ✦ Single Sign On = Un único sistema de autenticación

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Single Sign On



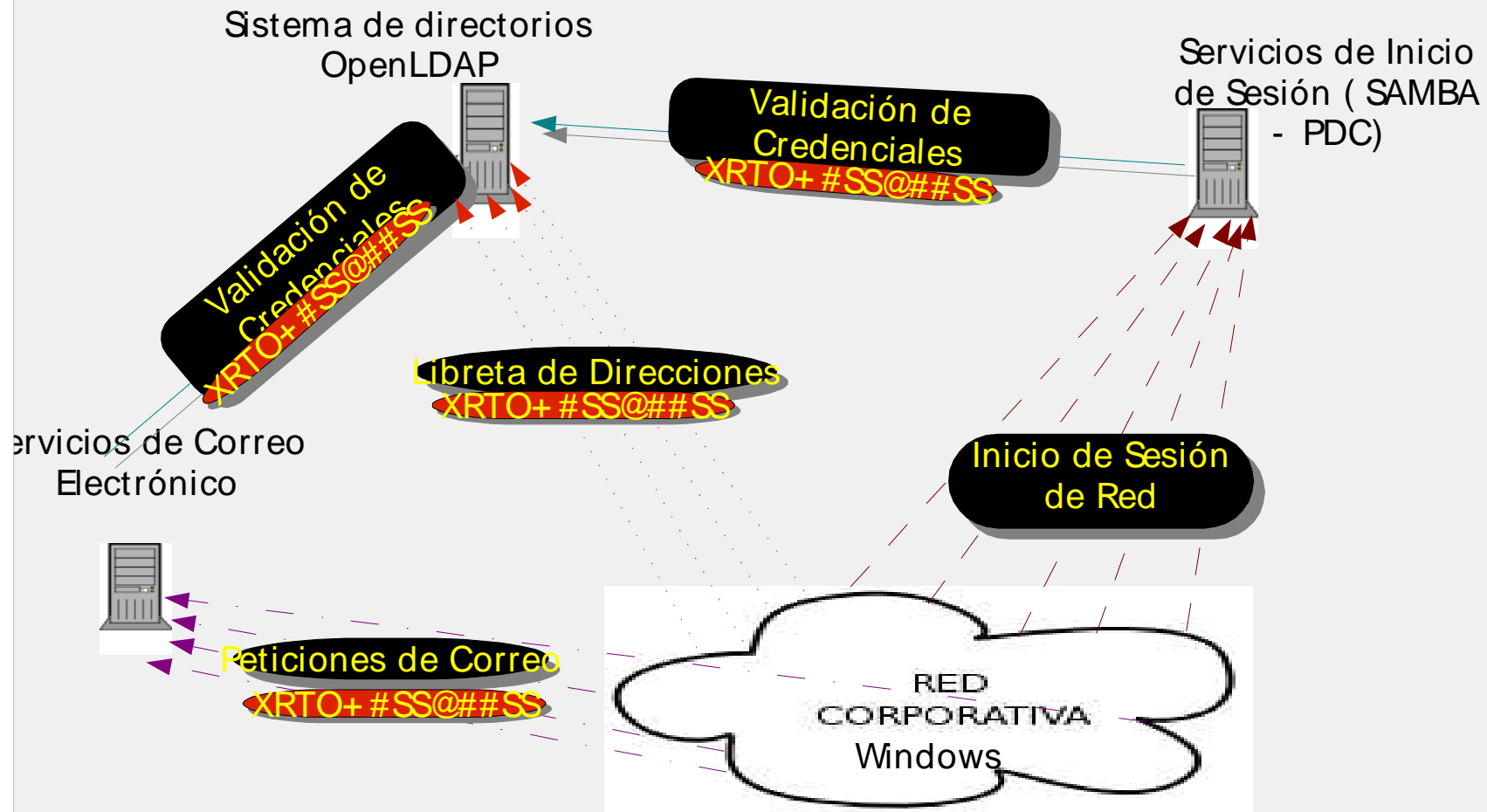
Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Porqué OpenLDAP ?

- ♦ Se ejecuta en cualquier plataforma y es free (Windows).
- ♦ Interacción mas directa con el usuario que implementa el servicio.
- ♦ Flexibilidad en cuanto a componentes, esquemas y clases, y tipos de repositorios utilizados.
- ♦ Características de Seguridad.
- ♦ Disminución de costos en implementaciones.
- ♦ Grupos de trabajo alrededor del software en procura de mejoras.
- ♦ Una alternativa más en la implementación de servicios de directorios.

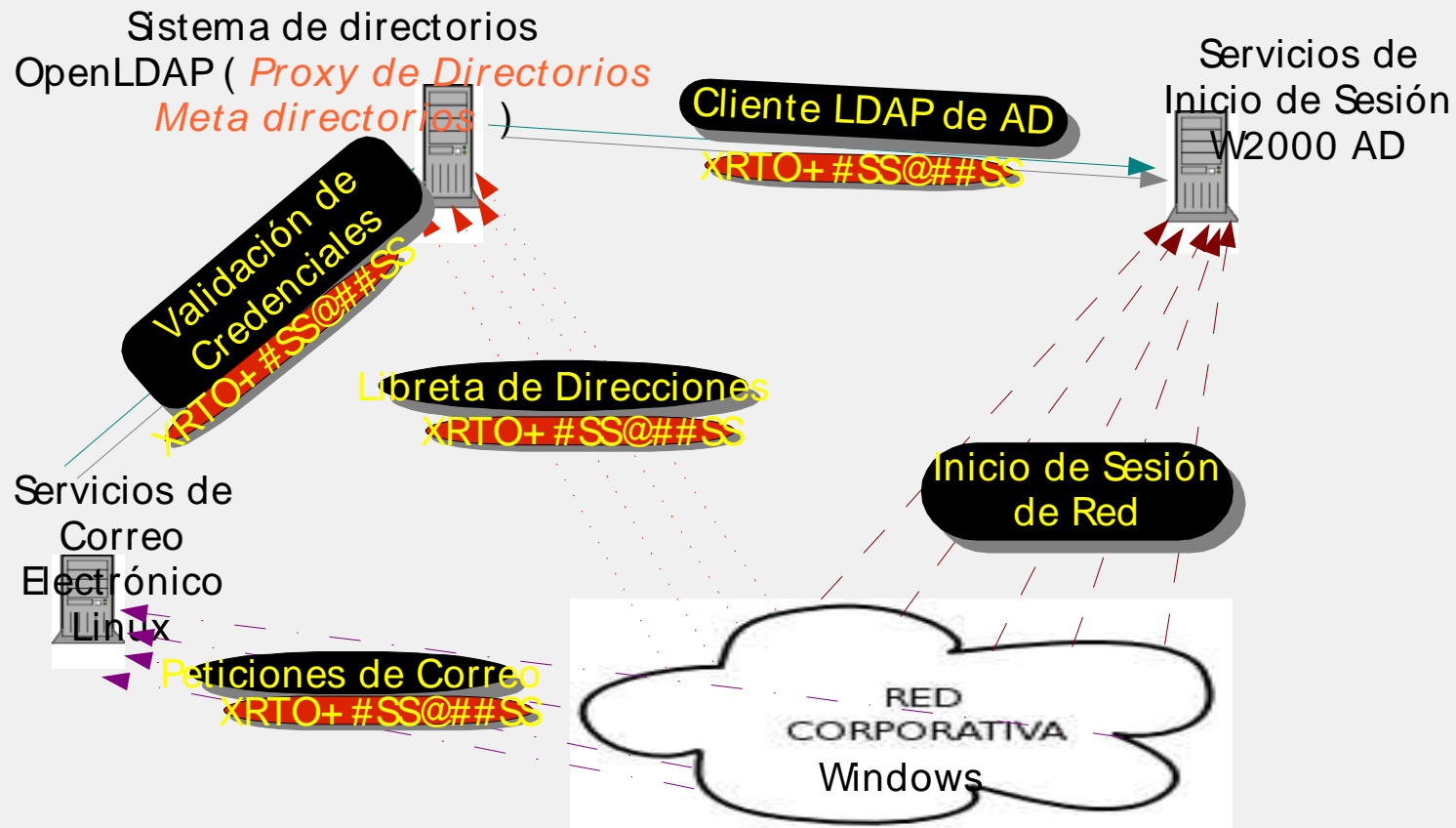
Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Esquemas de Implementación de SSO en Open Source Infraestructuras Homogéneas



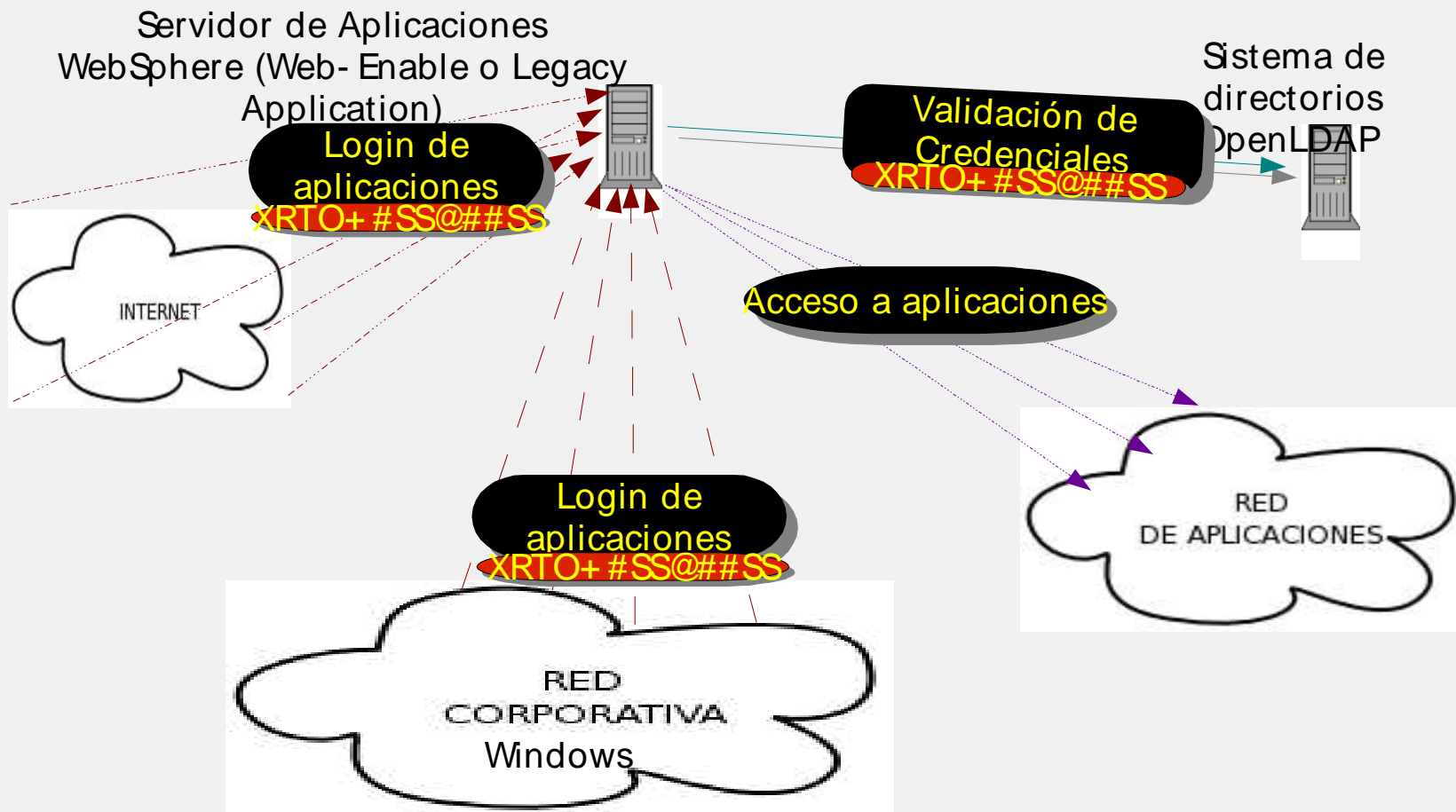
Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Esquemas de Implementación de SSO en Open Source Infraestructuras Heterogéneas



Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Esquemas de Implementación de SSO en Open Source Infraestructuras de Aplicaciones



Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

♦ En las consideraciones se deben tener presente:

Especificaciones Generales

Situaciones Adversas

Limitaciones de los sistemas de Directorios en Open Source

Seguridad en la implementación del servicio

Problemas en la implementación del servicio

Fallas de seguridad del modelo

Limitaciones del modelo

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Especificaciones Generales

- ♦ Planear el tipo de información y cual(es) podrían ser los servicios que encajan en la utilización de directorios. **Bases de datos Vs Directorios.**
- ♦ Determinar el grado de integración e interoperatividad.
 - ♦ Integración = Diferentes proveedores LDAP
 - ♦ Interoperatividad = comunicación de diferentes sistemas de directorio
- ♦ Al momento de migrar datos a los servicios de directorio comience por aplicaciones fácilmente migrables.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Especificaciones Generales

- Tener presente que las infraestructuras serán heterogéneas: (Windows + Linux +), una vez montado un directorio en ambiente Open Source.
- Recursos tecnológicos con los que cuenta para realizar el proceso de implementación.
- Unificación de información.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Situaciones Adversas

- ◆ Ambientes Gráficos de administración e instalación.
- ◆ Conocimiento acerca de los directorios.
 - ◆ Modelamiento de Nombres
 - ◆ Esquemas de Objetos, clases y atributos
 - ◆ Listas de Control de Acceso
 - ◆ Autenticación
 - ◆ Manejo de distribución y referencias, en ambientes de mas de un directorio
- ◆ La mayor parte del tiempo se deben utilizar las interfaces de texto para realizar configuraciones.
- ◆ En infraestructuras heterogéneas, no solo es necesario OpenLDAP. Se debe construir la pila de servicios.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Limitaciones de los sistemas de Directorios en Open Source

- ♦ Modificaciones de datos de manera continua.
- ♦ En el manejo de los sistemas de directorios para realizar Single Login, se deben pensar en el proceso de creación de cuentas como una fuerte labor de administración.
- ♦ Selección del sistema operacional Open Source a trabajar.
- ♦ Documentación de procedimientos es deficiente.
- ♦ Ausencia de herramientas completas de administración.
- ♦ Conocimiento pieza clave para la implementación de este tipo de servicios.

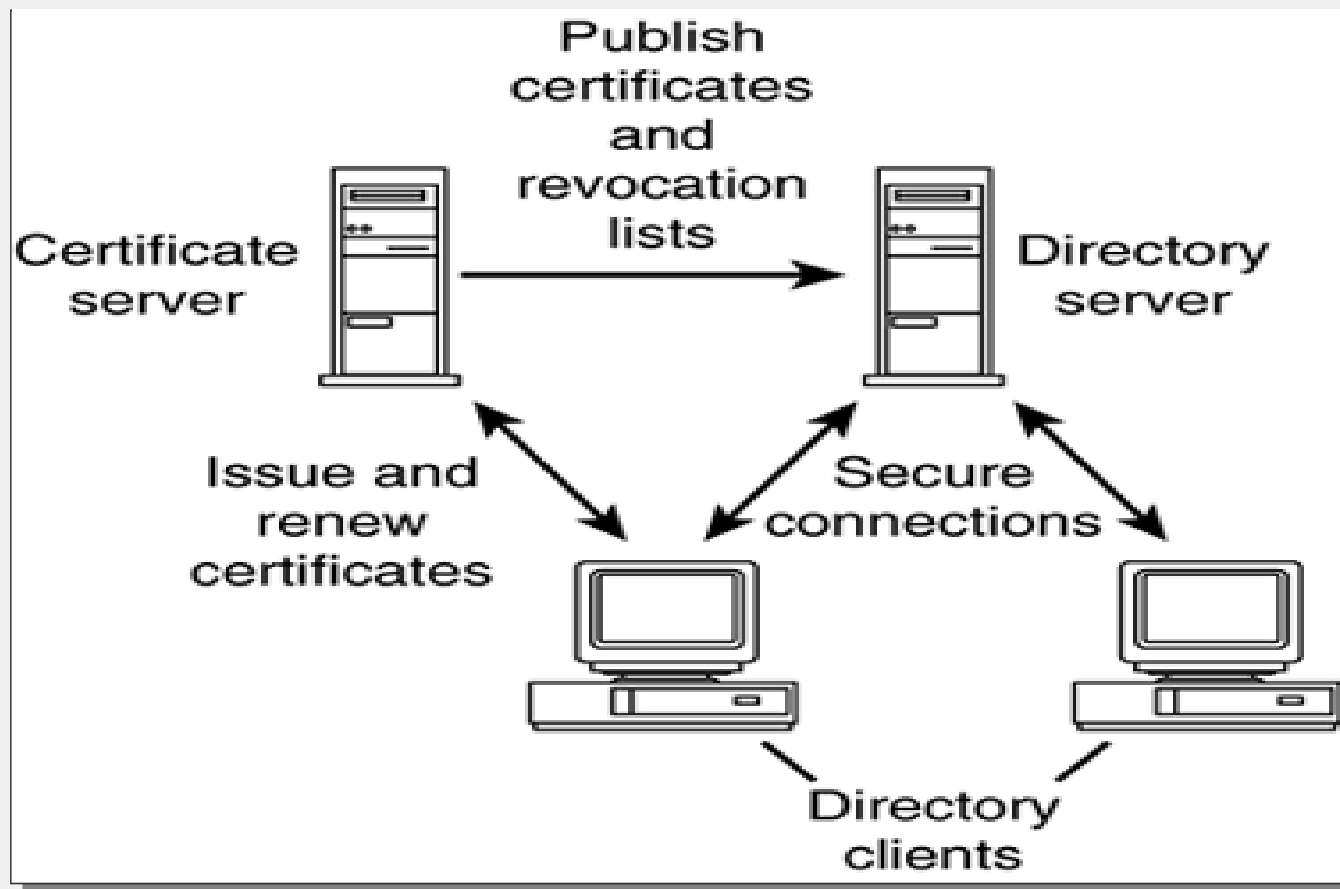
Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Seguridad en la Implementación del Servicio

- ♦ Fuertes elementos basados en los ACL, que garantizan la Autorización de las operaciones.
- ♦ Mecanismos de autenticación como SASL, GSAPI, protegen contra acceso no autorizado.
- ♦ Mecanismos como SSL y TLS, son de gran ayuda en el transporte de los datos a través de una red y garantizar la privacidad.
- ♦ LDAP, no es un modelo de seguridad.
- ♦ Integración adecuada en esquemas de PKI.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Seguridad en la Implementación del Servicio



Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Problemas en la Implementación del Servicio

- ✦ Interoperabilidad con diferentes proveedores de directorios.
- ✦ Soporte de software adicional, en clientes Windows contra directorio en Linux.
- ✦ Configuraciones adecuadas en el caso de referenciación de directorios. (AD – Linux).
- ✦ Requiere de software de terceros en ambientes de múltiples directorios (AD Linux).
- ✦ Reemplazar un ambiente de Dominio en infraestructura Windows a Open Source requiere no solo de un componente de software.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Problemas en la Implementación del Servicio

- ✦ En los casos de aplicaciones web-enable, no hay soporte a ldap.
- ✦ Conocimiento de el modelo de directorios para servidores de aplicaciones (WebSphere).
- ✦ La comunicación entre clientes y servidores no viaja cifrada. Requiere de configuraciones extras.
- ✦ Creación de las entradas iniciales.
- ✦ Definición de schemas, objetos y atributos.
- ✦ Fallas en configuraciones de aplicaciones y/o servicios indetectables (pam_ldap).

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Fallas de Seguridad del Modelo

- ✦ Único login y contraseña.
- ✦ Centralización de la información.
- ✦ Sincronización vs Single Sign On.
- ✦ Políticas de contraseñas débiles.
- ✦ Inyección de datos.
- ✦ Mecanismos frágiles de criptografía.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Limitaciones del Modelo

- ♦ Transparencia a nivel de usuarios (Single Login).
- ♦ Administración, elemento de alto impacto.
- ♦ Personal especializado para realizar dichas labores.
- ♦ Herramientas de administración son sencillas y muy generalizadas, herramientas de terceros con costo.
- ♦ La integración con otros sistemas de directorios suele ser compleja.
- ♦ La documentación es limitada a la hora de implementación de los servicios.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Conclusiones

- ♦ Los sistemas Single Sign On. Pueden ser implementables en ambientes Open Source.....
- ♦ Para arquitecturas tecnológicas heterogéneas se debe pensar en un sistema *SINGLE LOGIN*, y las repercusiones que involucra.
- ♦ Los sistemas Single Sign On, se aplican en principio a conjuntos de aplicaciones de un orden específico (web application o legacy application).

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Conclusiones

- ♦ Tener presente que el nivel técnico requerido para estas labores es alto, pero puede permitir general un alto nivel de funcionalidad y expansión del modelo.
- ♦ Los sistemas de directorios son herramientas que permiten **minimizar** los problemas de interoperatividad e **integración** en las arquitecturas actuales.
- ♦ Cada proyecto de integración de servicios de directorios es **único**.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Conclusiones

- ♦ Las implementaciones de los sistemas de directorios en general requieren de un grado de conocimiento.
- ♦ Las labores de administración de credenciales en arquitecturas tecnológicas pueden disminuir al implementar soluciones de directorios.

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Referencias Bibliográficas

- ♦ ISACA, capítulo Sud África Título. Understanding Single Sign-on, disponible en http://www.isaca.org.za/H_sso.htm
- ♦ eAdvantage 19 de septiembre de 2002. Título. Single sign-on solve some password problems but creates others. Disponible en: <http://techrepublic.com.co/5100-6269-1061289.html>
- ♦ David "Del" Elson 3 de abril de 2002. Título Active Directory and Linux. Disponible en: <http://www.securityfocus.com/infocus/1563>

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Referencias Bibliográficas

- ♦ Mathias Thurman 8 de Diciembre de 2003. Título. Single Sign- on Effort Falls Short. Disponible en: <http://www.computerworld.com/securitytopics/security/story/0,10801,87795,00.html>
- ♦ M- Tech Identify Managment Solution. Título. Synchronization is not Single Sign- On. Disponible en: <http://www.psynch.com/about/synch- not- sso.html>
- ♦ <http://www.criptored.upm.es/paginas/docencia.htm>

Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Referencias Bibliográficas

- ♦ Heinz Johner, Larry Brown, Franz-Stefan Hinner, Wolfgang Reis, Johan Westman. Título. Understanding LDAP. Disponible en: <http://www.redbooks.ibm.com/abstracts/sg244986.html>
- ♦ Tuttle Steven, Godbole Kedar, McCarthy Grant. Título. Using LDAP for Directory Integration. Disponible en <http://www.redbooks.ibm.com/sg246163.html>
- ♦ Iván m. Caballero, Jeimy J. Cano. Título. Consideraciones para implementar una arquitectura single sign-on. Disponible en:



Consideraciones Generales en la Implementación de Sistemas Single Sign On en Ambientes Open Source

Referencias Bibliográficas

- ♦ Gerald Carter, Ldap System Administration, O'Reilly, Marzo de 2003.
- ♦ Brian Arkills, Ldap Directories Explained: An Introduction and Analysis, February de 2003
- ♦ Timothy A. Howes, Mark C. Smith, Gordon S. Good, Understanding and Deploying LDAP Directory Service, Second Edition, Mayo de 2003