RedKlee

Servicio LDAP con interfaces de administración

Generalidades

Se describe la implementación de un servicio de autenticación LDAP usando una solución de código abierto llamada 389 Directory Server (389DS).
Además se detalla la implementación de interfaces de administración especialmente desarrolladas.
La solución está operativa en un ambiente corporativo con más de 6000 usuarios.

¿ Porqué 389 DS ?

El requerimiento recibido contemplaba varios aspectos:

- Estructura de alta disponibilidad con más de un server disponible en distintos sites.
- Los servers deberían mantener sus datos replicados en forma continua.
- Posibilidad de sincronizar los usuarios/contraseñas con un servicio de Active Directory ya instalado.
- Contar con interfaces web para las siguientes funciones:
  - ABM de usuarios por parte de los administradores.
  - Blanqueo de contraseñas para Mesa de Ayuda.
  - Autogestión de contraseñas para los usuarios finales.
- Tener capacidad para manejar aproximadamente 6000 usuarios.
- Poder implementar una política de contraseñas robusta.

Analizadas varias alternativas se concluyó que 389 DS era la alternativa más recomendable, ya que cuenta con muchas de estas funciones implementadas en forma nativa.

¿ Qué es 389 DS ?

389DS (389 Directory Server) se conoció previamente como FDS (Fedora Directory Server) y es un server LDAP de código abierto, desarrollado por Redhat como parte del Proyecto Fedora.
RedHat ofrece un producto denominado RHDS (RedHat Directory Server) que tiene una subscripción paga separada de RHEL (RedHat Entreprise Linux) que incluye versiones

estables certificadas, servicios al cliente y soporte técnico, pero funcionalmente es el

mismo producto que la version de código abierto.
389DS es la nueva encarnación de un proyecto de la Universidad de Michigan denominado *slapd,* que luego derivó en NDS (Netscape Directory Server) en el año 1996. Pueden verse más detalles en: http://en.wikipedia.org/wiki/389_Directory_Server

Caracteristicas destacadas

Algunas de las características que decidieron el uso en esta aplicación fueron:

- Variedad de mecanismos de replicación.
- Política de contraseñas.
- Posibilidad de sincronización con Microsoft Active Directory.
- Estabilidad del código fuente ampliamente probado.
- Documentación muy completa.

Ampliaremos algunos de los puntos más interesantes de la lista anterior.

- Mecanismos de replicación

389DS tiene varios escenarios posibles de replicación.

- Replicación de máster único
- Replicación multi master
- Replicación en cascada

Replicación de master único

Es la más sencilla. Los datos del directorio se mantienen en un único server llamado supplier y luego en uno o más servers con datos de solo lectura llamados consumer.

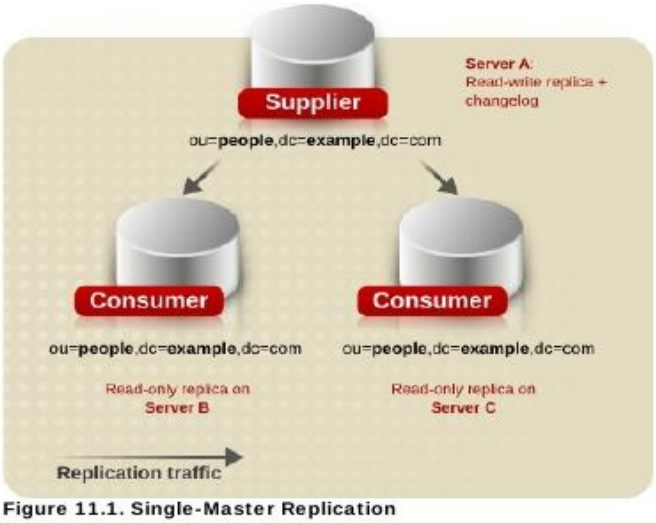


Figure 11.1. Single-Master Replication

Replicación multi-master

Es un escenario más complejo donde la misma base se mantiene en más de un server. 389DS admite hasta 20 servers en replicación multi-master y un número ilimitado de consumers.

Ejemplo con dos suppliers y dos consumers:

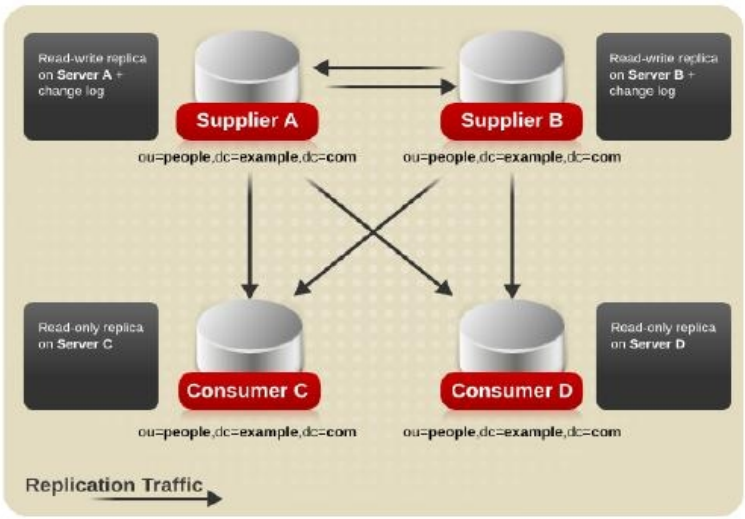


Figure 11.2. Multi-Master Replication (Two Masters)

Las ventajas principales de la replicación multi-master son:

- Alta disponibilidad sobre escritura de datos cuando uno de los “supplier” no está disponible.
- Las actualizaciones pueden hacerse en un server local en un ambiente geograficamente distribuído.

Replicación en cascada

En este escenario un server actua como consumer y como supplier, denominado HUB Server, que mantiene una réplica de solo lectura y el log de cambios, de manera que recibe actualizaciones desde el server que contiene la copia maestra de los datos y las transfiere al consumer.

Este tipo de replicación es importante para balancear cargas importantes de tráfico o para mantener servers en una ubicación local en un ambiente distribuído geográficamente.

Ejemplo de replicación en cascada:

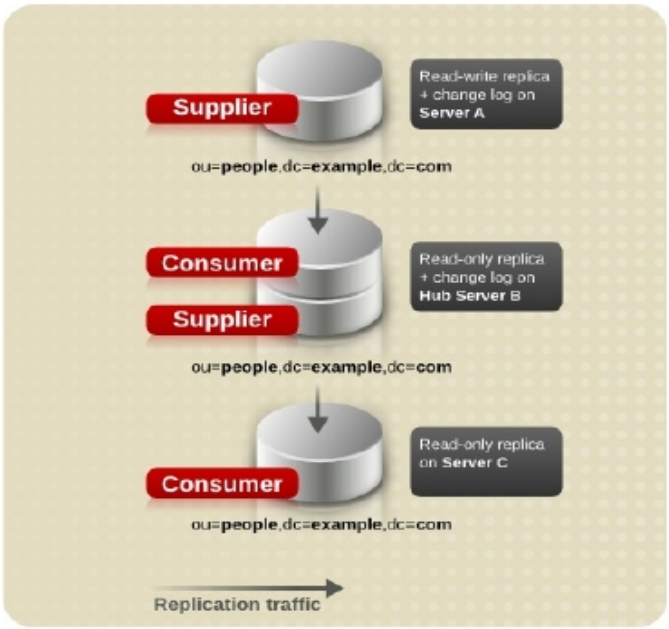


Figure 11.4. Cascading Replication

Se decidió utilizar una replicación multi-master con dos suppliers sin consumer.
Los supplier se instalaron en datacenter geograficamente separados.
De ser necesario se dejó para una etapa posterior la instalación de uno o más consumer.

- Política de contraseñas

389DS ofrece en forma nativa una variedad de opciones para definir una política de contraseñas robusta.
Se entiende por una política de contraseñas a un juego de reglas que gobiernan como son las contraseñas usadas en un dado sistema.
La política de 389DS especifica el criterio que una contraseña debe satisfacer para ser considerada válida, considerando el tiempo, el tipo y cantidad de caracteres y cuando el usuario puede reusar una contraseña.
La política puede aplicarse a cualquier nivel. Esto significa el árbol completo, una o más ramas o un usuario individual.

Básicamente la política de contraseñas se utiliza en dos situaciones:

- ✔ Cuando una aplicación hace una conexión con el servcio de LDAP para determinar si una contraseña es válida.

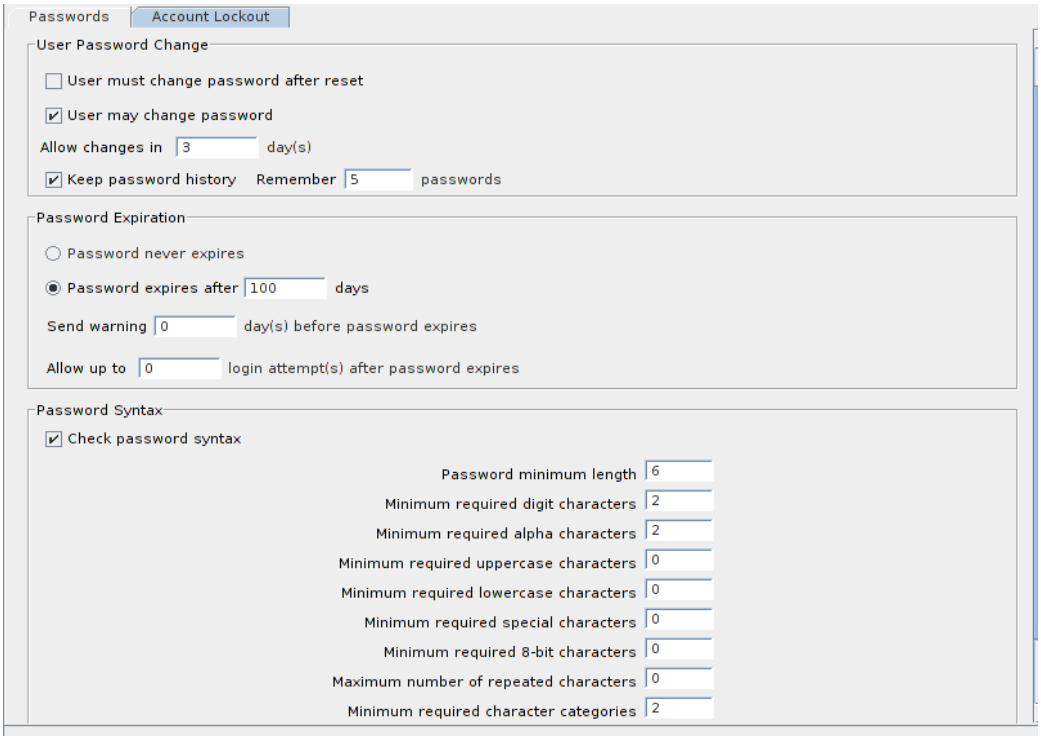
- ✔ Cuando se define o cambia la contraseña.

Cuando se verifica una contraseña además de controlar si es correcta, se verifica que no esté vencido el período de validez o el usuario se encuentre bloqueado.

Cuando se define o cambia una contraseña se verifica su largo y composición, así como

la comparación con respecto a contraseñas anteriores y si se está dentro del tiempo posible para el cambio.
En cuanto a la composición de la contraseña se puede especificar que tipo de caracteres (alfabético, numérico, especiales, etc) se requieren y que cantidad mínima de cada tipo.

El siguiente es el formulario para definir la política de contraseñas global de 389DS, accesible desde la consola de administración.



En la aplicación se configuraron estos valores generales y desde la interfaz de ABM de usuarios se permite cambiar algunos valores en forma personalizada, además se agregaron algunos controles adicionales.

- Sincronización de 389DS con Microsoft Active Directory

389DS se sincroniza con un server Microsoft Active Directory a través de un mecanismo denominado *Windows Sync*.
Windows Sync se compone de dos partes, una para usuarios y grupos y otra para las contraseñas.

- *Directory Server Windows Sync*. La sincronización de usuarios y grupos, se configura de una manera similar a una sincronización en un ambiente multi-master, donde se puede especificar si se sincronizan usuarios, grupos o ambos y tambien el sentido de la sincronización, desde 389DS hacia AD, desde AD hacia 389DS o en ambos sentidos.

- *Password Sync Service*. Los cambios de contraseña hechos en 389DS se sincronizan automaticamente en AD. Para que los cambios hechos en AD se repliquen en 389DS se necesita un servicio en el AD, denominado *Password Sync Service*. Este servicio captura los cambios hechos en las máquinas Windows y lo envía a 389DS usando el protocolo LDAPS.

El esquema se muestra en el siguiente gráfico:

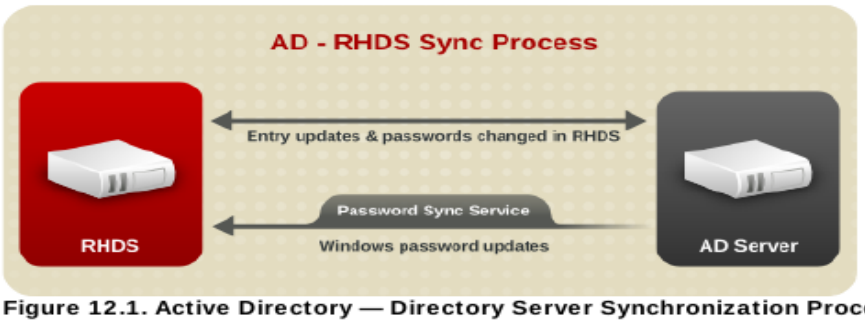


Figure 12.1. Active Directory — Directory Server Synchronization Process

Si bien la sincronización puede en teoría hacerse con un server hub, para lograr una sincronización bi-direccional ésta debe hacerse con un server master en una configuración multi-master, como la mostrada en el siguiente gráfico:

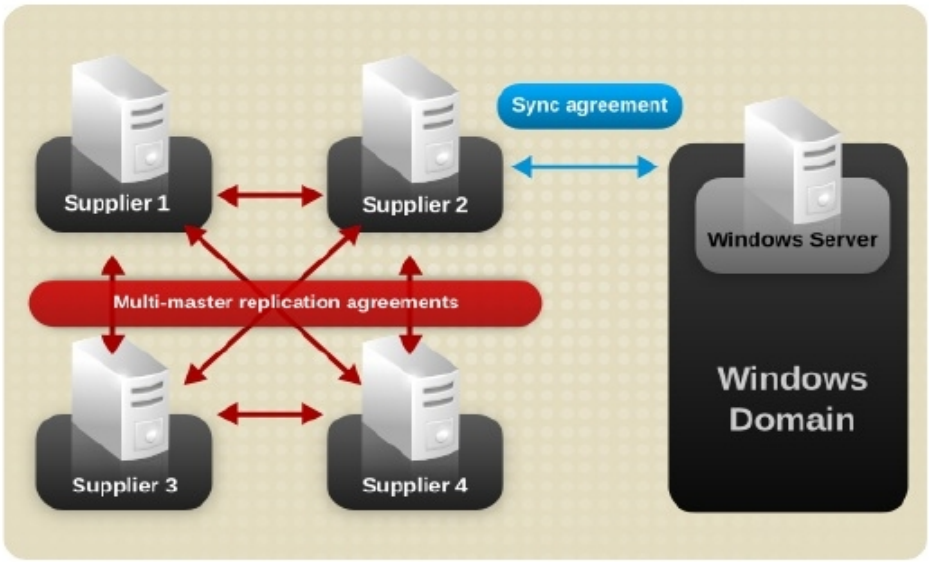


Figure 12.2. Multi-Master Directory Server — Windows Domain Synchronization

Para obtener información en detalle de 389DS puede consultarse:
http://directory.fedoraproject.org/wiki/Documentation

- Interfaces

El proyecto tenía el requisito de disponer de las siguientes interfaces:

- ABM de usuarios.
- Help Desk.

- Autogestión de contraseñas.

389-DS incluye una interfaz de administración, que permite realizar todas las tareas de administración del producto.
Sin embargo esta interfaz no es Web, tiene además un diseño no muy sencillo de usar y también es muy complicado limitar las funciones que un usuario puede desarrollar.

Se decidió reservarla para funciones específicas del área de sistemas y desarrollar una interfaz Web dedicada a cada necesidad.

El desarrollo se hizo en Python en un ambiente Django que permite configurar en forma sencilla los permisos de cada usuario sobre las distintas interfaces.

La interfaz de **ABM de usuarios** permite dar de alta o modificar datos como:

Nombre de usuario
Contraseña
Datos personales (nombre, apellido, mail, tel, sector, legajo, etc.)
Grupos a los que pertenece

Con respecto a la política de contraseñas, permite algunos cambios sobre la política global definida. Se pueden Anular o Habilitar atributos tales como:

- Vencimiento de la contraseña.
- Requisito de cambio de contraseña en el primer login.
- Obligación de carga de preguntas de seguridad para cambio de contraseña.

Además:

- Agrega el requisito que la contraseña no puede contener parte del nombre de usuario.
- Permite bloquear el acceso del usuario.

La interfaz para **Help Desk** permite solamente modificar la contraseña del usuario.

En el ambiente Django es muy sencillo otorgar permisos adicionales. Por ejemplo podría configurarse para que la interfaz de Help Desk pueda modificar también los datos personales del usuario y/o los grupos y no solo la contraseña.

La interfaz de **Autogestión de Contraseñas**, permite al usuario verificar cuando vence su contraseña y cambiarla.
Para cambiar la contraseña tienen que darse una serie de condiciones:

- Haber pasado el período mínimo en el que no se permite el cambio (configurado en 3 días).
- Tener cargadas las preguntas de seguridad, salvo que el usuario tenga configurado una excepción.

La contraseña debe cumplir con una serie de requisitos en su largo y tipo de caracteres y

ser distinta a un número determinado de contraseñas anteriores.

La contraseña puede cambiarse tanto si está vencida como si está vigente.

Esta interfaz no está accesible si el usuario está bloqueado.

Otro de los requisitos del proyecto era que el usuario debería contestar **Preguntas de Seguridad** previamente cargadas para el caso que hubiera olvidado su contraseña.

Se consideró inicialmente PWM (http://code.google.com/p/pwm) que es un producto de Código Abierto muy completo.
Luego de probarlo, se encontró que la versión disponible tenía algunas incompatibilidades con la política de contraseñas nativa de 389DS. Podrían haberse utilizado solo las que trae PWM, pero eso hubiera obligado a manejar todas las interfaces previamente descriptas desde ese producto, que no se adaptaba totalmente a los requisitos del cliente, ni resultaba posible sin un gran esfuerzo integrarlo en el ambiente de otras interfaces ya disponibles.

Se decidió agregar al desarrollo la interfaz para **Administración de Preguntas de Seguridad**, donde se permite elegir entre una serie de preguntas personales y cargarles respuestas. Estas preguntas y respuestas quedan almacenadas en forma encriptada dentro del registro LDAP del usuario.
Las preguntas deben obligatoriamente cargarse para poder cambiar la contraseña, si bien como se describe previamente este requisito puede cambiarse en forma individual.
Las preguntas se deben responder si el usuario no recuerda su contraseña, para poder elegir una nueva.

- Conclusiones

1. El uso de un producto como 389DS que cuenta con una gran cantidad de funcionalidades disponibles en forma nativa, que además es sumamente estable, sumando el desarrollo de una serie de interfaces adecuadas a las necesidades del cliente permitieron generar una solución totalmente funcional para un ambiente corporativo, con un costo cero de licencias o subscripciones.

2. De ser necesario la capacidad de replicación multi-master permite una sencilla expansión de la estructura.

3. Las interfaces desarrolladas pueden adaptarse a nuevos requerimientos.

4. La posibilidad de sincronización entre 389DS y Active Directory brinda la opción de integrar los dos ambientes, brindandole al usuario un único login y contraseña para todas sus aplicaciones.

Preparado por: Norberto Altalef
Fecha: Febrero 2014