Autenticación Centralizada - OpenLDAP

Tony García

Quien es Tony García?

- Egresado de UAA, ISC – 99-04.
- SysAdmin, DevOp wannabe.
- Rackspace, EA(softtek), Google(globant).
- Linuxero por convicción.
- Pro OpenSource.
- Casado con una egresada de LEI.(UAA)

Quien es Tony García?

- Egresado de UAA, ISC – 99-04.
- SysAdmin, DevOp wannabe.
- Rackspace, EA(softtek), Google(globant).
- Linuxero por convicción.
- Pro OpenSource.
- Casado con una egresada de LEI.(UAA)

Que es Autenticación?

- Confirmación de algo/alguien como auténtico/verdadero.
- Confirmación de que el usuario es quien dice ser, validando su contraseña.

- Se utiliza para:
  - Accesos.
  - Elevación de privilegios.

Tipos de Auth en Linux.

- Local (default)
  - files
  - etc, etc, etc.
- Centralizada
  - NIS/NIS+
  - LDAP
  - Kerberos
  - OTP
  - etc, etc, etc.

Por qué Auth Centralizada?

- Ventajas
  - Comodidad.
  - Orden.
  - Seguridad.
  - Mantenibilidad.
- Desventajas
  - Complicado???
  - Riesgo de fallo centralizado.

Ejemplos de Casos de Uso.

- Universidad con 3 Laboratorios de computo
  - 30 computadoras(PCs) por Laboratorio.
  - 6 grupos de 30 alumnos.
- Auth Local
  - 90 PCs, 180 usuarios.
    - Al menos 1 usuario con acceso a 1 PC por laboratorio.
      - 1 usuario x 3 PCs x 180 = 540 cuentas.
    - A lo mas 1 usuario con acceso a c/PC en cualquier laboratorio.
      - 180 usuarios x 90 PCs = 16,200 cuentas.

Ejemplos de Caso de Uso

- Compañia con 600 Trabajadores.
- 200 Servidores(Desarrollo, Prueba, Produccion)
- 120,000 cuentas!

Alternativas de Auth Centralizada

- NIS/NIS+
  - Network Information Services(Yellow Pages)
    - Cliente-Servidor, Creado por Sun.
- LDAP
  - Lightweight Directory Access Protocol
    - Estructura Jerarquica(Org),
- Kerberos
  - Cliente Servidor, Basado en tickets, encripcion.
- OTP
  - One Time Password
  - Generalmente dependen de otro dispositivo para funcionar.

Qué es LDAP?

- Lightweight Directory Access Protocol.
- 54 RFC para LDAP.
- RFC 4510, RFC 4511, RFC 4512, RFC 4513, RFC 4514, RFC 4515, RFC 4516, RFC 4517, RFC 4518, RFC 4519, RFC 4520, RFC 4521, RFC 2247, RFC 2307, RFC 2589, RFC 2649, RFC 2696, RFC 2798, RFC 2830, RFC 2849, RFC 2891, RFC 3045, RFC 3062, RFC 3296, RFC 3671, RFC 3672, RFC 3673, RFC 3687, RFC 3698, RFC 3829, RFC 3866, RFC 3909, RFC 3928, RFC 4370, RFC 4373, RFC 4403, RFC 4522, RFC 4523, RFC 4524, RFC 4525, RFC 4526, RFC 4527, RFC 4528, RFC 4529, RFC 4530, RFC 4531, RFC 4532, RFC 4533, RFC 4876, RFC 5020, RFC 1777, RFC 1778, RFC 1779, RFC 3494
- Para qué se usa?
  - Representación de una organización. (Organigrama)
  - Servicio para obtener información de una organización. (Directorio)
  - Control centralizado de usuarios. (Acceso mediante autenticación)

OpenLDAP

- Por qué usar openldap?
  - FOSS
  - Software para interactuar, controlar LDAP
  - Es un proyecto activo.
  - Buena documentación disponible.
  - Es ampliamente utilizado por las grandes compañias.

Trabajando con OpenLDAP

- Requerimientos
  - Servidor de OpenLDAP.
  - Clientes Configurados para comunicación con LDAP.
- Qué es necesario en un cliente?
  - nsswitch - /etc/nsswitch.conf
  - nss_ldap - /etc/ldap.conf
  - pam_ldap - /etc/pam.d/system-auth

OpenLDAP

Instalando - Servidor

- RedHat based
  - sudo yum install openldap-servers
- Debian based
  - sudo apt-get install slapd

Instalando - Herramientas

- RedHat based
  - sudo yum install openldap-clients
- Debian based
  - sudo apt-get install ldap-utils

- Estos programas no son necesarios para hacer uso de la autenticación en los clientes, pero es útil para validación de comunicación con el servidor

Herramientas

usr/bin/ldapadd

/usr/bin/ldapcompare

/usr/bin/ldapdelete

/usr/bin/ldapexop

/usr/bin/ldapmodify

/usr/bin/ldapmodrdn

/usr/bin/ldappasswd

/usr/bin/ldapsearch

/usr/bin/ldapurl

/usr/bin/ldapwhoami

Preparación

- Crear password seguro:
  - slappasswd -h '{SSHA}' -s openldap
- Detener LDAP:
  - sudo /etc/init.d/slapd stop
  - sudo /etc/init.d/ldap stop
- Remover la BD:
  - sudo rm -Rf /var/lib/ldap/*
- Verificar permisos:
  - sudo chown ldap:ldap /var/lib/ldap
  - sudo chown openldap:openldap /var/lib/ldap

Configuración Básica - Servidor

- Github + USBs
-

Registros Base

- dc=tonyskapunk,dc=net
- ou=People,dc=tonyskapunk,dc=net
- ou=Group,dc=tonyskapunk,dc=net

Registro de Usuario

dn: uid=tonyskapunk,ou=People,dc=tonyskapunk,dc=net
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: shadowAccount
homeDirectory: /home/tonyskapunk
cn: Tony G.
sn: G.
givenName: Tony
mail: tonyg@tonyskapunk.net
uidNumber: 2001
gidNumber: 2001
uid: tonyskapunk
loginShell: /bin/bash
userPassword::

Registro de grupo

dn: cn=tonyskapunk,ou=group,dc=tonyskapunk,dc=net

objectClass: posixGroup

gidNumber: 2001

cn: tonyskapunk

Usuario bind

dn: cn=binduser,dc=tonyskapunk,dc=net

objectClass: organizationalPerson

cn: binduser

sn: lastname

UserPassword: {SSHA}

Configuración básica - cliente

- /etc/nsswitch.conf
- /etc/ldap.conf
- /etc/pam.d/system-auth

nsswitch

- /etc/nsswitch.conf
  - passwd: files ldap
  - group: files ldap
  - shadow: files ldap

/etc/ldap.conf

- nss_ldap
- uri (Uniform Resource Identifier) | <ldap[is]://[name[:port]] ...>
- base | Specifies the default base distinguished name (DN) to use for searches.

- man nss_ldap
- bind_policy, binddn, pam_passwd, ssl, tls_cert, etc.

PAM(Pluggable Authentication Modules)

PAM defines the authentication in four independent group types:

- Authentication/credential acquisition – auth
  - Authenticate/validate users, set/remove credentials.
- Account management – account
  - Actions related to access, account, credential expiration, password restrictions, etc.
- Session management – session
  - Initializing/Ending sessions.
- Authentication token (password) updating – password
  - Change/update Password.

PAM Controls

- requisite: Failure instantly returns control to the application indicating the nature of the first module failure.
- required: All these modules are required to succeed for libpam to return success to the application, but just after validation the remaining modules.
- sufficient: Given that all preceding modules have succeeded, the success of this module leads to an immediate and successful return to the application (failure of this module is ignored).
- optional: The success or failure of this module is generally not recorded.
- include: Use the file defined in here.

- Is this program using PAM?
  - ldd /usr/sbin/sshd|grep libpam

Credits & License

- Tony García
  - identi.ca: tonyskapunk
  - twitter: @tonyskapunk
  - License: GPL-2+
    - http://www.gnu.org/licenses/gpl-2.0.html
- OpenOffice.org template by Raphaël Hertzog
  http://raphaelhertzog.com/go/ooo-template
  License: GPL-2+
- Background image by Alexis Younes “ayo”
  http://www.73lab.com
  License: GPL-2+