Sessão 3: Autenticação centralizada

Retomando o cenário apresentado na introdução da primeira sessão, num ambiente em que a virtualização é usada em larga escala, teremos diversas máquinas virtuais operando cada qual com seus serviços alocados. Imagine, hipoteticamente, que temos centenas de VMs dentro do *datacenter*. Vários desafios podem surgir à mente, mas tente responder a seguinte pergunta: com relação à gestão de contas, o que fazer quando um novo colaborar é integrado à equipe? Ou, por outro lado, quando um funcionário é desligado da empresa?

Ora, se temos centenas de VMs, é fácil supor que teremos que logar nas diferentes máquinas que novo colaborador (ou o antigo) deverá acessar e criar uma conta de usuário para ele — além disso, adicioná-lo a grupos e editar permissões relevantes. Fazer esse procedimento inúmeras vezes é claramente um processo que pode gerar erros de configuração, então poderia-se pensar em automatizá-lo, digamos, via *shell scripts*. Uma boa solução, mas não a ideal neste caso.

Sistemas de autenticação centralizados, como NIS (*Network Information Service*) ou LDAP (*Lightweight Directory Access Protocol*) são excelentes ferramentas para facilitar a gestão em cenários como o apresentado — adicionando o usuário em um único ponto, é possível distribuir essa configuração para dezenas, ou centenas, de máquinas de forma instantânea. O gerenciamento de grupos no sistema centralizado também permite atribuir permissionamento de forma fácil, ou removê-lo quando necessário.

Nesta sessão, iremos configurar um sistema de autenticação centralizado para o nosso laboratório usando LDAP, no qual gerenciaremos usuários e grupos, e faremos a integração desse sistema de autenticação com o Linux através do PAM (*Pluggable Authentication Modules*). Em lugar de fazer o controle de senhas dos usuários diretamente via `/etc/shadow` ou no LDAP, criaremos um sistema de autoridade certificadora (*Certificate Authority*) para o SSH, com o qual os usuários farão login nos servidores usando chaves assimétricas assinadas pela CA. Finalmente, para controlar ataques de força-bruta contra os servidores, usaremos o programa Fail2Ban para realizar o bloqueio automático de atacantes no firewall de *host* das máquinas.

1) Criação da VM para o servidor LDAP

1. Clone a máquina `debian-template` seguindo os mesmos passos da atividade (6) da sessão 1. Para o nome da máquina, escolha `ldap`.
2. Após a clonagem, na janela principal do Virtualbox, clique com o botão direito sobre a VM `ldap` e depois em *Settings*.

   Em *Network* > *Adapter 1* > *Attached to*, escolha *Host-only Adapter*. O nome da rede *host-only* deve ser o mesmo alocado para a interface de rede da máquina virtual `fw`, configurada durante a sessão 2, que está conectada à DMZ.

   Clique em *OK*, e ligue a máquina `ldap`.

3. Logue como o usuário `root` e usando o script `/root/changehost.sh` que criamos anteriormente, renomeie a máquina:

   ```
   # hostname
   debian-template
   ```

   ```
   # bash ~/changehost.sh ldap
   ```

   ```
   # hostname
   ldap
   ```

4. Em seguida, edite o arquivo `/etc/network/interfaces` como se segue, reinicie a rede e verifique o funcionamento:

   ```
   # nano /etc/network/interfaces
   (...)
   ```

   ```
   # cat /etc/network/interfaces
   source /etc/network/interfaces.d/*

   auto lo enp0s3

   iface lo inet loopback

   iface enp0s3 inet static
   address 10.0.0.2/24
   gateway 10.0.0.1
   ```

   ```
   # systemctl restart networking
   ```

```
# ip a s | grep '^ *inet '
    inet 127.0.0.1/8 scope host lo
    inet 10.0.0.2/24 brd 10.0.0.255 scope global enp0s3
```

Verifique o roteamento:

```
# ip r s
default via 10.0.0.1 dev enp0s3 onlink
10.0.0.0/24 dev enp0s3 proto kernel scope link src 10.0.0.2
```

Verifique, ainda, a configuração de DNS do sistema:

```
# nano /etc/resolv.conf
(...)
```

```
# cat /etc/resolv.conf
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Finalmente, teste o funcionamento da conexão de rede:

```
# nc -zv obsd3.srv.ualberta.ca 80
obsd3.srv.ualberta.ca [129.128.5.194] 80 (http) open
```

2) Configuração do servidor LDAP

apt-get install slapd ldap-utils ldapscripts

Senha admin: rnpesr

---

dpkg-reconfigure -plow slapd

Omitir a configuração do servidor OpenLDAP? Não Nome de domínio DNS: intnet Nome da organização: seg10 Senha do administrador: rnpesr (repetir) Backend da base de dados a ser usado: MDB Você deseja que a base de dados seja removida quando o pacote slapd for expurgado ("purged")? Não Move a base de dados antiga? Sim

apt-get install nslcd

URI do servidor LDAP: ldapi:/// Base de buscas do servidor LDAP: dc=intnet Serviços de nome para configurar: passwd, group, shadow

sed -i 's/^#\(BASE\).*/\1 dc=intnet/' /etc/ldap/ldap.conf

sed -i 's/^#\(URI\).*/\1 ldapi\:\/\/\//' /etc/ldap/ldap.conf

sed -i 's/^\(BINDDN=\).*/\1\"cn=admin,dc=intnet\"/' /etc/ldapscripts/ldapscripts.conf

echo -n "rnpesr" > /etc/ldapscripts/ldapscripts.passwd

ldapinit -s

ldapsearch -x -LLL

dn: dc=intnet objectClass: top objectClass: dcObject objectClass: organization o: seg10 dc: intnet

dn: cn=admin,dc=intnet objectClass: simpleSecurityObject objectClass: organizationalRole cn: admin description: LDAP administrator

dn: ou=People,dc=intnet objectClass: top objectClass: organizationalUnit ou: People

dn: ou=Groups,dc=intnet objectClass: top objectClass: organizationalUnit ou: Groups

dn: ou=Hosts,dc=intnet objectClass: top objectClass: organizationalUnit ou: Hosts

dn: ou=Idmap,dc=intnet objectClass: organizationalUnit ou: Idmap

3) Habilitando logs do LDAP

INCLUDE slapdlog.ldif # ldapmodify -Y external -H ldapi:/// -f slapdlog.ldif

---

INCLUDE slapd.conf # systemctl restart rsyslog.service # systemctl restart slapd.service

---

tail /var/log/slapd.log

[19-10-2018 18:25:46] slapd debug daemon: shutdown requested and initiated. [19-10-2018 18:25:46] slapd debug slapd shutdown: waiting for 0 operations/tasks to finish [19-10-2018 18:25:46] slapd debug slapd stopped. [19-10-2018 18:25:46] slapd debug @(#) $OpenLDAP: slapd (May 23 2018 04:25:19) $#012#011Debian OpenLDAP Maintainers <pkg-openldap-devel@lists.alioth.debian.org> [19-10-2018 18:25:46] slapd debug slapd starting

4) Adição de grupos e usuários no LDAP

ldapaddgroup sysadm

Successfully added group sysadm to LDAP

ldapsearch -x -LLL 'cn=sysadm'

dn: cn=sysadm,ou=Groups,dc=intnet objectClass: posixGroup cn: sysadm gidNumber: 10000 description: Group account

---

ldapadduser luke sysadm

Successfully added user luke to LDAP Successfully set password for user luke

ldapsearch -x -LLL 'cn=luke'

dn: uid=luke,ou=People,dc=intnet objectClass: account objectClass: posixAccount cn: luke uid: luke uidNumber: 10000 gidNumber: 10000 homeDirectory: /home/luke loginShell: /bin/bash gecos: luke description: User account

ldapsetpasswd luke

Changing password for user uid=luke,ou=People,dc=intnet New Password: Retype New Password: Successfully set password for user uid=luke,ou=People,dc=intnet

ldapsearch -x -LLL -D 'cn=admin,dc=intnet' -W 'cn=luke' userPassword

Enter LDAP Password: dn: uid=luke,ou=People,dc=intnet userPassword:: e1NTSEF9NHdUSWZRcUhGR0o5VU5jNS9tVnhoaGJzNFVvNkFzMmE=

ldapaddusertogroup luke sysadm

Successfully added user luke to group cn=sysadm,ou=Groups,dc=intnet

ldapsearch -x -LLL 'cn=sysadm'

dn: cn=sysadm,ou=Groups,dc=intnet objectClass: posixGroup cn: sysadm gidNumber: 10000 description: Group account memberUid: luke