Guia de instalação e configuração da ferramenta openldap

Histórico de Revisões

|  |  |  |  |
| --- | --- | --- | --- |
| Data | Versão | Descrição | Autor |
| 10/12/2020 | 1.0 | Craiação do documento | Rafael Alessandro de Morais |

**1 - Atualizando o sistema e instalando pacotes openldap**

Primeira coisa a fazer é atualizar o sistema.

|  |
| --- |
| :~# yum update |

Agora vamos instalar os pacotes OpenLDAP.

|  |
| --- |
| :~# yum install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel |

Com os pacotes instalados, devemos habilitar e inicializar o serviço do OpenLDAP

|  |
| --- |
| :~# systemctl enable slapd  :~# systemctl start slapd |

**2 - Configurando o openLDAP server**

Primeiro, devemos gerar a senha de root do OpenLDAP. É por isso que escrevemos:

|  |
| --- |
| :~# slappasswd -h {SSHA} -s your\_password |

Teremos algo assim:

{SSHA}XKrTsGmjsV0Rw1lZzLaOr7pqvZRrbv8A

Em seguida, crie o arquivo de configuração openLDAP para que ele possa funcionar corretamente:

|  |
| --- |
| :~# nano conf.ldif |

Colocamos o seguinte conteúdo::

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: dc=osradar,dc=local

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootDN

olcRootDN: cn=angelo,dc=osradar,dc=local

dn: olcDatabase={2}hdb,cn=config

changetype: modify

replace: olcRootPW

olcRootPW: {SSHA}XKrTsGmjsV0Rw1lZzLaOr7pqvZRrbv8A

Nesse arquivo, você deve modificar esses três parâmetros conforme sua conveniência:

olcSuffix: Basicamente, o sufixo é o seu nome de host. Para sua referência, neste tutorial, o nome do host é osradar.local.

olcRootDN: TRefere-se ao usuário administrador do openLDAP.

olcRootPW: Aqui está a senha gerada acima. Coloque a sua aqui.

Quando terminarmos de editar o arquivo, procedemos ao “upload” da configuração criada para openLDAP com ldapmodify.

|  |
| --- |
| :~# ldapmodify -Y EXTERNAL -H ldapi:/// -f conf.ldif |

**3 - Configurando o banco de dados openLDAP**

Agora vamos copiar o banco de dados de exemplo e conceder permissões a ele.

|  |
| --- |
| :~# cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG  :~# chown ldap:ldap /var/lib/ldap/\* |

E adicionamos o restante dos esquemas.

|  |
| --- |
| :~# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif  :~# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif  :~# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif |

Agora vamos criar nosso arquivo base.ldif

|  |
| --- |
| :~# nano base.ldif |

Nele adicionaremos o seguinte:

dn: dc=osradar,dc=local

dc: osradar

objectClass: top

objectClass: domain

dn: cn=angelo ,dc=osradar,dc=local

objectClass: organizationalRole

cn: angelo

description: LDAP Manager

dn: ou=users,dc=osradar,dc=local

objectClass: organizationalUnit

ou: Users

dn: ou=Group,dc=osradar,dc=local

objectClass: organizationalUnit

ou: Group

Agora devemos escrever o comando para criar a estrutura do diretório. Ao fazer isso, será solicitada a senha do openldap.

|  |
| --- |
| :~# ldapadd -x -W -D "cn=angelo,dc=osradar,dc=local" -f base.ldif |

Altere os parâmetros para os seus.

**4 - Criação de usuário openLDAP**

Precisamos criar um usuário para openLDAP. Uma maneira fácil de fazer isso é criar um arquivo para o novo usuário, podemos chamá-lo de newuser.ldif.

|  |
| --- |
| :~# nano newuser.ldif |

Nele iremos copiar o seguinte conteúdo:

dn: uid=user,ou=users,dc=osradar,dc=local

objectClass: top

objectClass: account

objectClass: posixAccount

objectClass: shadowAccount

cn: user

uid: user

uidNumber: 9999

gidNumber: 100

homeDirectory: /home/user

loginShell: /bin/bash

gecos: user

userPassword: {crypt}x

shadowLastChange: 17058

shadowMin: 0

shadowMax: 99999

shadowWarning: 7

Aletre o que precisar conforme os passos anteriores.

Agora, com o comando ldapadd, procedemos para criar o novo usuário.

|  |
| --- |
| :~# ldapadd -x -W -D "cn=angelo,dc=osradar,dc=local" -f newuser.ldif |

Agora vamos dar uma senha ao novo usuário.

|  |
| --- |
| :~# ldappasswd -s pass321 -W -D "cn=angelo,dc=osradar,dc=local" -x "uid=user,ou=users,dc=osradar,dc=local" |

**5 - Configurações finais**

Em seguida, acrescentamos as regras no firewall para que o openLDAP funcione sem problemas.

|  |
| --- |
| :~# firewall-cmd --permanent --add-service=ldap  :~# firewall-cmd --reload |

**6 - Testando o servidor**

Verificamos se tudo está em ordem:

|  |
| --- |
| :~# ldapsearch -x cn=user -b dc=osradar,dc=local |

Se o terminal exibir as informações do usuário, tudo correu bem.