

Исследование возможностей сервера OpenLDAP для аутентификации пользователей СУБД PostgreSQL

Воронин Д.Л., Муравьев С.К.

27 января 2014

Обзор основных методов аутентификации СУБД PostgreSQL

- Trust

Обзор основных методов аутентификации СУБД PostgreSQL

- Trust
- Password

Обзор основных методов аутентификации СУБД PostgreSQL

- Trust
- Password
- Ident

Обзор основных методов аутентификации СУБД PostgreSQL

- Trust
- Password
- Ident
- Peer

Обзор основных методов аутентификации СУБД PostgreSQL

- Trust
- Password
- Ident
- Peer
- PAM

Обзор основных методов аутентификации СУБД PostgreSQL

- Trust
- Password
- Ident
- Peer
- PAM
- LDAP

Информационное дерево каталога LDAP

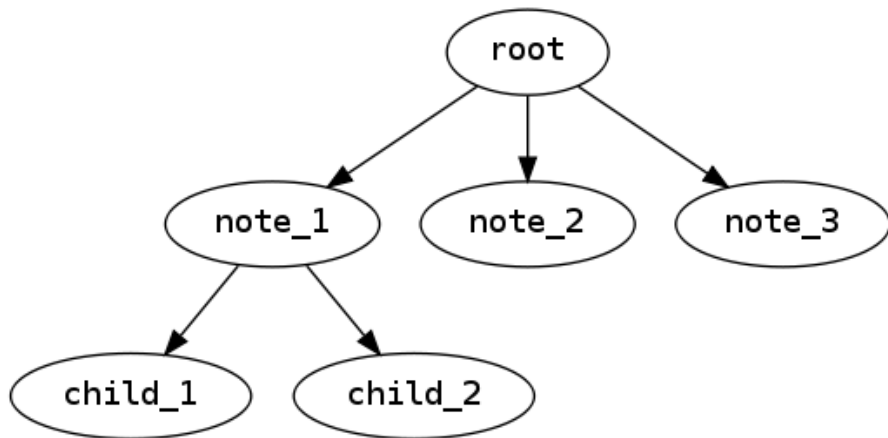
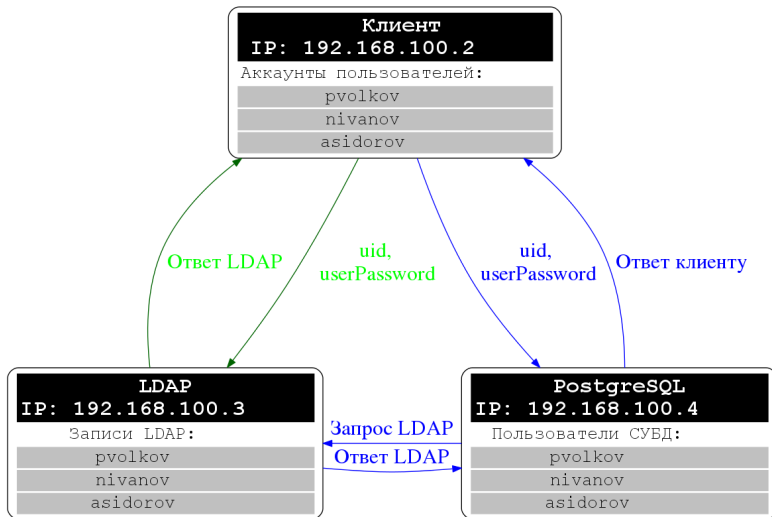


Схема работы стенда



Запись аккаунта пользователя LDAP

```
dn: uid=nivanov,ou=People,dc=ldap-server,dc=ru
uid: nivanov
cn: Nikolay Ivanov
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {SSHA}US0VGNxhxro/QD3B4wIbjRa5re9i8cX1
shadowLastChange:15997
shadowMin:0
shadowMax:99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 501
gidNumber: 501
homeDirectory: /home/nivanov
```

Аутентификация пользователя на клиентской машине

```
CentOS release 6.5 (Final)
Kernel 2.6.32-431.1.2.0.1.el6.x86_64 on an x86_64

ldap-client login: nivanov
Password:
Last login: Mon Dec 23 13:46:48 on tty1
[nivanov@ldap-client ~]$ getent passwd nivanov
nivanov:*:501:501:Nikolay Ivanov:/home/nivanov:/bin/bash
[nivanov@ldap-client ~]$ _
```

Соединение клиента с сервером LDAP

```
ldapuser@ldap-server:/home/ldapuser
File Edit View Search Terminal Help
0030 03 e1 45 ae 00 00 01 01 08 0a 00 2a 29 2f 00 2a ..E.....*)/*
0040 24 3f $?

0.003266 192.168.100.2 -> 192.168.100.3 LDAP 594 searchRequest(2) *dc=ldap-server,dc=ru
wholeSubtree

0000 08 00 27 81 c5 71 08 00 27 13 36 e6 08 00 45 00 ..'.q.'.'6...E.
0010 02 44 c4 35 40 00 40 06 2b 28 c0 a8 64 02 c0 a8 .D.50.0.+(.d...
0020 64 03 9d 40 01 85 90 04 ee 22 40 ae 2d 7a 08 18 d.0....."0.-2..
0030 03 e1 df 93 00 00 01 01 08 0a 00 2a 29 2f 00 2a .....*)/*
0040 24 3f 30 82 02 0c 01 02 03 82 02 05 04 14 64 $?0.....C.....d
0050 63 3d 6c 64 61 70 2d 73 65 72 76 65 72 2c 64 63 c=ldap-server,dc
0060 3d 72 75 0a 01 02 0a 01 00 02 01 00 02 01 00 01 =ru.....
0070 01 00 a0 2d a3 0e 04 03 75 69 64 04 07 70 76 6f .....uid..pvo
0080 6c 6b 6f 76 a3 1b 0a 0b 6f 62 6a 65 63 74 63 6c lkov...objectcl
0090 61 73 73 04 0c 70 6f 73 69 78 41 63 63 6f 75 6e ass..posixAccoun
00a0 74 30 82 01 ad 0a 0b 6f 62 6a 65 63 74 43 6c 61 t0.....objectcla
00b0 73 73 04 03 75 69 64 04 0c 75 73 65 72 50 61 73 ss..uid..userPas
00c0 73 77 6f 72 64 04 09 75 69 64 4e 75 6d 62 65 72 sword..uidNumber
00d0 04 09 6f 69 64 4e 75 6d 62 65 72 04 05 6f 65 63 ..gidNumber..gec
00e0 6f 73 04 0d 68 6f 6d 65 44 69 72 65 63 74 6f 72 os..homeDirector
00f0 79 04 0a 6c 6f 67 69 66 53 68 65 6c 6c 04 10 6b y..loginShell..k
0100 72 62 50 72 69 6c 63 69 70 61 6c 4e 61 6d 65 04 rbPrincipalName.
0110 02 63 6e 04 0f 6d 6f 64 69 66 79 54 69 6d 65 73 .cn..modifyTimes
0120 74 61 6d 70 04 0f 6d 6f 64 69 66 79 54 69 6d 65 tamp..modifyTime
0130 73 74 61 6d 70 04 10 73 68 61 64 6f 77 4c 61 73 stamp..shadowLas
0140 74 43 68 61 6e 67 65 04 09 73 68 61 64 6f 77 4d tChange..shadowW
```

```
ldapuser@ldap-server:/home/ldapuser
File Edit View Search Terminal Help
Running as user "root" and group "root". This could be dangerous.
Capturing on eth0
0.000000 192.168.100.2 -> 192.168.100.3 TLSv1 631 Application Data

0000 08 00 27 81 c5 71 08 00 27 13 36 e6 08 00 45 00 ..'.q.'.'6...E.
0010 02 09 c8 05 40 00 40 06 27 33 c0 a8 64 02 c0 a8 .i..@.'3..d...
0020 04 03 8e 73 02 7c ea 07 fa b4 61 87 e3 6b 80 18 d..s.[]...a..k..
0030 0b 58 d0 d3 00 00 01 01 08 0a 00 28 16 cf 00 27 .X.....{...'.
0040 0c b2 17 03 01 02 30 0d fb cd c3 ad 49 65 44 40 .....0.....Ie0@
0050 a0 98 95 13 aa 55 9f f3 ff 0d ea c8 8a 1e 13 0c .....U.....
0060 0f ce da f7 c6 81 d9 28 ab 6f fa 38 4e 46 9d b1 .....(o.8NF..
0070 c7 84 8d dd 3e de 2f e3 d1 c1 f3 27 ad 85 71 cd .....>/q.'.'q.
0080 91 5e 95 ea 80 e2 f8 64 d3 c3 7c ea c9 66 e1 .^.....d..f.
0090 68 08 21 4b d9 60 31 7e 4f f5 4c ef d1 18 b2 0c hhIK..l=0.L.....
00a0 7f 84 ee a1 ab 31 a0 9f 49 06 83 1f fe ae 8c 62 .....1.I.....b
00b0 60 95 53 f5 5a ff ad cb 47 31 73 6e db 21 0c 95 '.S.Z..G1sn.l..
00c0 64 1e 95 db 24 fa 21 61 ea de 73 c2 41 b3 07 70 d...$.la..s.A..p
00d0 39 b4 c8 fd 98 c9 57 13 ca 81 1d e4 df 6b 12 fd 9.....W.....k..
00e0 ea 56 38 ad 7c f3 2f d3 10 10 ea 4d 92 6e d1 42 .VB..[/.....M..n..B
00f0 bf ad b1 09 68 04 bf d0 a4 fd 54 31 36 8b bf bd .....h.....T16...
0100 21 df bf e8 a2 6b 76 b5 7c df 84 66 33 22 2e 72 ....kv.[]..f3'.r
0110 cb 17 0f 00 12 30 0d bc 11 4a fc df b9 97 93 cd .....0.....J...
0120 f0 6b 86 13 da 77 53 98 0d 0b 6f c7 fd 05 44 71 .k..wS...o...Dq
0130 b7 9a 66 ab 7a a8 43 8e 62 dc c8 04 6d 67 33 06 .f.z.C.b...0g3.
0140 61 fa cc 49 bc f1 6e 50 c7 d6 d1 0d 67 4f c9 1d a..i..nP.....g0..
0150 ba 66 81 78 5b 0a 2b 51 39 9c b5 ae 26 79 5b f1 .f.x[.+09...6.[.
0160 4d 6e 13 87 f3 de e7 ce 30 c6 08 04 ea 34 ac f1 Mn.....0.....4..
```

Вывод утилиты `tethreal` соединения клиента и сервера LDAP без TLS и с TLS.

Аутентификация пользователей СУБД PostgreSQL по методу LDAP

В файл `/var/lib/pgsql/9.3/data/pg_hba.conf` требуется добавить строку:

```
hostssl all all 192.168.100.0/24 ldap
ldapserver=192.168.100.3
ldapprefix="uid="
ldapsuffix=",ou=People,dc=ldap-server,dc=ru"
```

- Произведено исследование основных методов аутентификации СУБД PostgreSQL. Выявлены их достоинства и недостатки.
- Исследованы возможности сервера OpenLDAP.
- Описан процесс настройки метода аутентификации LDAP в PostgreSQL.

Спасибо за внимание!