OSSDEVCONF-2017 // Калуга

Samba AD и MIT Kerberos

Александр Боковой

Sr. Principal Software Engineer, Red Hat / Samba Team

Active Directory: домен

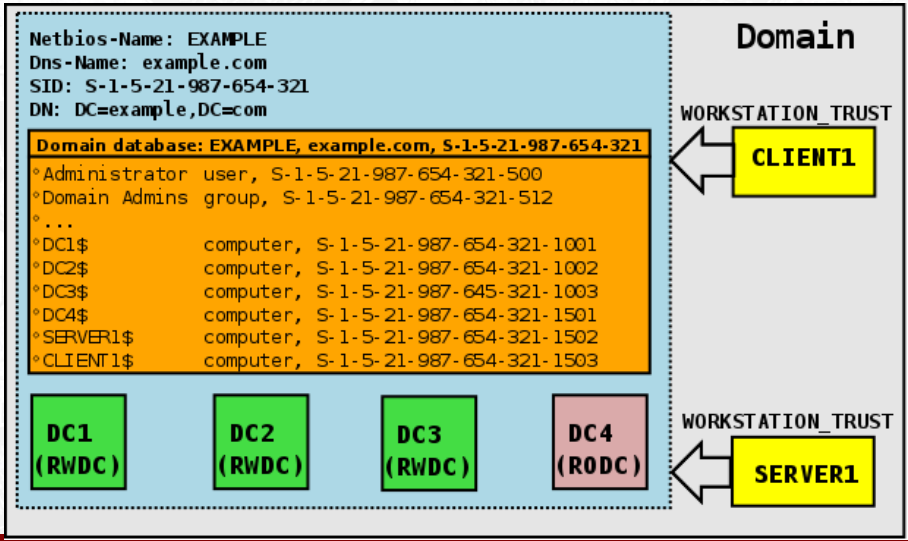

Figure 1:

Active Directory: лес

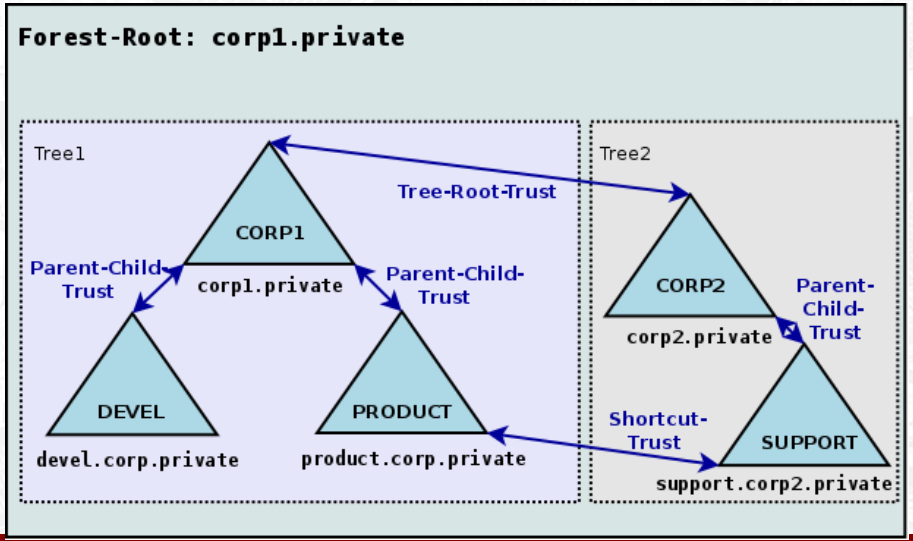

Figure 2:

Active Directory: база данных

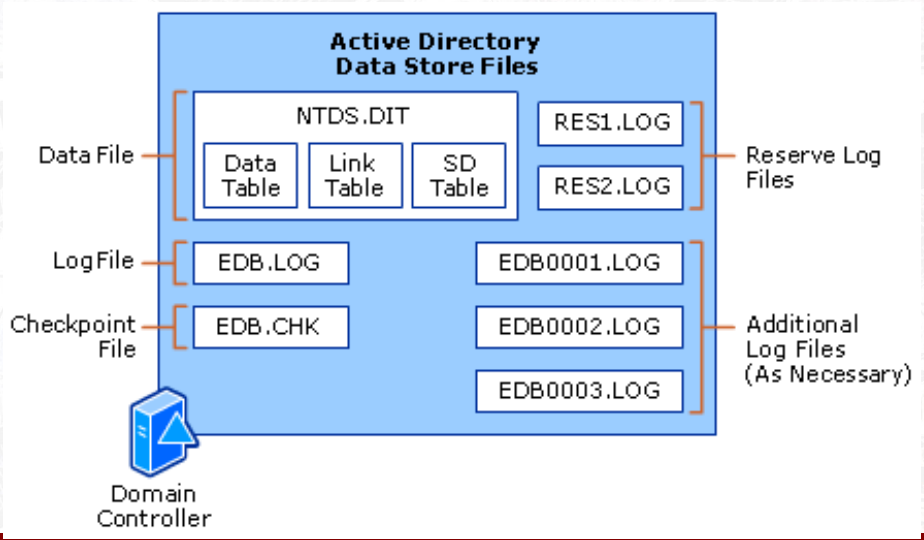

Figure 3:

Active Directory: сервисы

- Единая база данных
  - исторически Jet Database образца 90-х годов
  - https://blogs.technet.microsoft.com/askpfeplat/2012/07/22/mcm-core-active-directory-internals/

    Distributed Jet/ESE database that's exposed through LDAP by the Directory System Agent (DSA) with many dependent LDAP-enabled applications and services sitting on top of it including Kerberos, Authentication, DNS, etc.
- Kerberos
- LDAP
- DCE RPC

Всем службам доступно общее состояние

Samba AD DC

2000 A.D.

- Исследовательский проект Andrew Tridgell @ IBM Research
  - “как нам реорганизовать Samba?”
- Проблема общего состояния данных
  - единая база данных
  - единая очередь событий
  - автоматическая генерация кода для обработки DCE RPC
  - тесная интеграция реализаций LDAP, Kerberos, DCE RPC

2000 A.D.

```
commit ce74988dc831d856a94b341d7df3501932b1c43c
Author: Andrew Tridgell <tridge@samba.org>
Date:   Thu Dec 14 04:09:29 2000 +0000

    first version

    (This used to be commit 14135ed6bbff54d7b493f9be7748c2ad7440a97b)

 source4/build/pidl/dump.pm  | 166 +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
 source4/build/pidl/idl.gram | 135 ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
 source4/build/pidl/pidl.pl  |  95 ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
 source4/build/pidl/util.pm  | 128 +++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
 4 files changed, 524 insertions(+)
```

Клон или не он?

- Код Heimdal Kerberos вливается в Самба
  - Lorikeet-heimdal
  - интеграция с eventloop Samba (tevent)
- LDB - LDAP-подобное API поверх TDB

Попытаемся взлететь

```
commit 7c8284fefc40a89b7979a7a07bb4ec2c45a02d98
Author: Andrew Bartlett <abartlet@samba.org>
Date:   Thu May 19 11:23:31 2005 +0000

    r6902: Turn the LDAP server on by default.  It is no worse than the others...
    (no ACL support)

    Andrew Bartlett
    (This used to be commit 9f895f6482e45dd975baea7114748b65dbe6e688)

 source4/param/loadparm.c | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)
```

Попытаемся взлететь — 2

```
commit 45511bd09b62266904c547398037fd41fbb8871e
Author: Stefan Metzmacher <metze@samba.org>
Date:   Thu May 19 13:35:50 2005 +0000

    r6904: use "krb5:kdc=yes" in your smb.conf when you have the lorikeet-heimdal kdc running

    metze
    (This used to be commit fa652919bd6ab58ff15cab239cf88d2359b03d55)

 source4/cldap_server/netlogon.c     | 2 +-
 source4/nbt_server/dgram/netlogon.c | 2 +-
 2 files changed, 2 insertions(+), 2 deletions(-)
```

Промышленная эксплуатация

```
                    ============================
                    Release Notes for Samba 4.0.0
                          December 11, 2012
                    ============================
....

Major enhancements in Samba 4.0.0 include:

Active Directory services
=========================

Samba 4.0 supports the server-side of the Active Directory logon
environment used by Windows 2000 and later, so we can do full domain
join and domain logon operations with these clients.

Our Domain Controller (DC) implementation includes our own built-in
LDAP server and Kerberos Key Distribution Center (KDC) as well as the
Samba3-like logon services provided over CIFS.  We correctly generate
the infamous Kerberos PAC, and include it with the Kerberos tickets we
issue.

When running an AD DC, you only need to run 'samba' (not smbd/nmbd/winbindd),
as the required services are co-coordinated by this master binary.
The tool to administer the Active Directory services is called 'samba-tool'.
```

Как это все тестировать?

- Контейнеров в 2005 году нет
  - эмуляция среды исполнения
- 2005: `socket_wrapper` (Jelmer Vernooij)
- 2007: `nss_wrapper` (Stefan Metzmacher)
- 2008: `uid_wrapper` (Andrew Tridgell)
- 2014: `resolv_wrapper` (Andreas Schneier)
- 2016: `pam_wrapper` (Andreas Schneier)

Все эти компоненты теперь доступны в проекте CWrap: https://cwrap.org

2014 A.D.

The current work branch has a bit more then 130 patches right now, so
we would really like to start bringing pieces of it upstream now.

So what we did today was to move out all the krb5 wrapping calls out
of the main branch to a separate branch. Getting this first series of
patches upstream would make it much easier to step forward on this matter.

This new branch now contains most of the prerequisite work to make all
of samba's DC code to compile with both a MIT or a Heimdal kerberos
library in one of the next steps (in particular the krb5 client code
which currently is not compiled at all when using a system MIT
kerberos library).

Some of the commits might read a bit abstract and unrelated when seen
isolated in the new branch. In that case one can always check the
larger wip branch where - when seen in context - the order of commits
explains much better why this and that is needed.

...

Andrew, can you start reviewing this ?

Thanks,
Guenther

2015 A.D.

refs/heads/master-mit-krb5

- Часть патчей втащили в git master
- 140 патчей к лету 2015 года
- Смесь изменений в Samba, LDAP, MIT Kerberos, Heimdal, ...

kadmin ACL

- Статическое определение прав, несовместимое с NT ACL
- Драйвер KDB не вовлечен в процесс принятия решения
- `/var/kerberos/krb5kdc/kadm5.acl`
- Пример из `kadm5.acl(5)`

```
EXAMPLE
       Here is an example of a kadm5.acl file:

          */admin@ATHENA.MIT.EDU     *                               # line 1
          joeadmin@ATHENA.MIT.EDU    ADMCIL                          # line 2
          joeadmin/*@ATHENA.MIT.EDU  i   */root@ATHENA.MIT.EDU       # line 3
          */root@ATHENA.MIT.EDU      ci  *1@ATHENA.MIT.EDU           # line 4
          */root@ATHENA.MIT.EDU      l   *                           # line 5
          sms@ATHENA.MIT.EDU         x   * -maxlife 9h -postdateable # line 6
```

[MS-BKRP]

- Репликация паролей между контроллерами домена
- Независимость от реализации Kerberos
- Переписали код на GnuTLS
  - GnuTLS не поддерживает RC4 (шеф, всё пропало!)
  - Добавили в GnuTLS в декабре 2015 (новая зависимость)

Badlock

PAUSE (2015 - 2016)

MIT Kerberos 1.15

- Прекрасно! Все нужные функции для Samba
- Поломалось API KDB :(
  - Утечки памяти для каждого principal
  - MIT Kerberos 1.15.1!

2017 A.D.

SambaXP 2017

```
commit 68d0c295fbe0e8795bdd26589bd564542afd5a56
Author: Andreas Schneider <asn@samba.org>
Date:   Fri Jan 27 12:11:33 2017 +0100

    mit_samba: Fix principal lookup for cross domain referral

    Pair-Programmed-With: Stefan Metzmacher <metze@samba.org>

    Signed-off-by: Stefan Metzmacher <metze@samba.org>
    Signed-off-by: Andreas Schneider <asn@samba.org>
    Reviewed-by: Andrew Bartlet <abartlet@samba.org>
    Reviewed-by: Jeremy Allison <jra@samba.org>

    Autobuild-User(master): Andreas Schneider <asn@cryptomilk.org>
    Autobuild-Date(master): Sun Apr 30 03:29:35 CEST 2017 on sn-devel-144
```

Samba 4.7.0

```
$ git show samba-4.7.0
tag samba-4.7.0
Tagger: Karolin Seeger <kseeger@samba.org>
Date:   Thu Sep 21 08:33:38 2017 +0200

samba: tag release samba-4.7.0
-----BEGIN PGP SIGNATURE-----

iEYEABECAAYFAlnDXUMACgkQbzORW2Vot+pQoQCfe2sXqa+d7dyWDhZvVar/odam
8bQAoK9+gw/BZ1btsPRc8Pk8ua62qdmJ
=5F07
-----END PGP SIGNATURE-----
```

TO DO

- Поддержка PKINIT и смарткарт
- Поддержка имерсонификации (S4U2Self, S4U2Proxy)
  - в том числе и между лесами ([MS-KILE])
- Поддержка RODC
  - libkdc и интеграция с eventloop
- Доверительные отношения с FreeIPA
  - Работает с Heimdal, сломалось с MIT Kerberos
  - Всё дело в пузырьках^Wsalt

Спасибо за внимание!