EOLE AD DC - Tâche #21382

Scénario # 17261 (Terminé (Sprint)): Etude d'intégration de BIND sur le module SETH

Répertorier les conditions nécessaires à l'utilisation de bind comme backend pour Samba

09/18/2017 11:17 AM - Benjamin Bohard

Status:	Fermé	**Start date:**	09/11/2017
Priority:	Normal	**Due date:**	
Assigned To:	Benjamin Bohard	**% Done:**	100%
Target version:	sprint 2017 37-39 Equipe PNE-SR	**Estimated time:**	3.00 hours
		Spent time:	6.00 hours

Description

History

#1 - 09/18/2017 11:17 AM - Benjamin Bohard

- Status changed from Nouveau to En cours

#2 - 09/18/2017 11:39 AM - Benjamin Bohard

Les conditions auxquelles doit répondre bind selon le wiki de Samba :

- version supportée par ISC
- pas d'installation en mode chroot (bind doit accéder aux bases de données de samba directement)
- installation localement
- compilé avec l'option --with-gssapi=yes (pour les mises à jour sécurisées du DNS en utilisant Kerberos)
- compilé avec l'option --with-dlopen (pour le chargement dynamique des zones DLZ)

Sur EOLE 2.6 :

```
named -V
BIND 9.10.3-P4-Ubuntu <id:ebd72b3>
built by make with '--prefix=/usr' '--mandir=/usr/share/man' '--libdir=/usr/lib/x86_64-linux-gnu' '--infodir=/
usr/share/info' '--sysconfdir=/etc/bind' '--localstatedir=/' '--enable-threads' '--enable-largefile' '--with-l
ibtool' '--enable-shared' '--enable-static' '--with-openssl=/usr' '--with-gssapi=/usr' '--with-gnu-ld' '--with
-geoip=/usr' '--with-atf=no' '--enable-ipv6' '--enable-rrl' '--enable-filter-aaaa' '--enable-native-pkcs11' '-
-with-pkcs11=/usr/lib/x86_64-linux-gnu/softhsm/libsofthsm2.so' 'CFLAGS=-g -O2 -fPIE -fstack-protector-strong -
Wformat -Werror=format-security -fno-strict-aliasing -fno-delete-null-pointer-checks -DNO_VERSION_DATE' 'LDFLA
GS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now' 'CPPFLAGS=-Wdate-time -D_FORTIFY_SOURCE=2 -DDI
G_SIGCHASE'
```

1. la version proposée par Ubuntu est une version encore maintenue.
2. on n'utilise pas actuellement le mode chroot (possibilité de faire des mount --bind ?)
3. bind9 n'est pas installé sur Seth mais sur Amon (quid de l'interaction ?)
4. la version proposée par Ubuntu est compilée avec --with-gssapi=/usr
5. ~~la version proposée par Ubuntu n'est pas compilée avec --with-dlopen~~ (option par défaut depuis la version v9_9_0a1)

#3 - 09/18/2017 04:41 PM - Benjamin Bohard

~~Recompiler bind9 avec l'option --with-dlopen~~

L'option dlopen est par défaut depuis la version v9_9_0a1 de bind9 :

```
git show -s 422009fe5b15e31e7f5d09212bd1480121a1464e
commit 422009fe5b15e31e7f5d09212bd1480121a1464e
Author: Evan Hunt <each@isc.org>
Date:   Thu Mar 10 04:36:16 2011 +0000

    3066.   [func]          The DLZ "dlopen" driver is now built by default,
                            no longer requiring a configure option.  To
                            disable it, use "configure --without-dlopen".
                            Driver also supported on win32.  [RT #23467]
```

```
git describe --tags --contains 422009fe5b15e31e7f5d09212bd1480121a1464e
v9_9_0a1~556
```

installer bind9 et les bibliothèques en dépendance

```
apt install bind9
```

configurer samba pour utilisation de bind en backend

/etc/samba/smb.conf, dans la section [global]

```
server services = -dns
```

```
samba_upgradedns --dns-backend=BIND9_DLZ
```

Cela créé les fichiers /var/lib/samba/private/named.conf et /var/lib/samba/private/dns.key

configurer bind pour utiliser la bibliothèque de samba

/etc/bind/named.conf

```
include "/var/lib/samba/private/named.conf";
```

configurer la mise à jour utilisant kerberos

/etc/bind/named.conf.options

```
tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
```

configurer apparmor

/etc/apparmor.d/local/usr.sbin.named

```
/var/lib/samba/lib/** rm,
/var/lib/samba/private/dns.keytab r,
/var/lib/samba/private/named.conf r,
```

```
/var/lib/samba/private/dns/** rwk,
/var/tmp/** rwmk,
/etc/samba/smb.conf r,
```

```
systemctl restart apparmor.service
```

configurer rndc (optionnel : named démarre sans ça)

/etc/rndc.conf

```
key "rndc-key" {
  algorithm hmac-md5;
  secret "zc5uFkpD5z7UUGw6O2yzjw==";
};

options {
  default-server  localhost;
  default-key     "rndc-key";
};
```

/etc/bind/named.conf

```
controls {
  inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};
```

/etc/bind/rndc.key

```
key "rndc-key" {
    algorithm hmac-md5;
    secret "zc5uFkpD5z7UUGw6O2yzjw==";
};
```

#4 - 09/18/2017 05:22 PM - Benjamin Bohard

- Remaining (hours) changed from 3.0 to 0.0

#5 - 09/19/2017 10:41 AM - Benjamin Bohard

- Status changed from En cours to Résolu

#6 - 09/26/2017 12:10 PM - Emmanuel IHRY

- Status changed from Résolu to Fermé

- % Done changed from 0 to 100