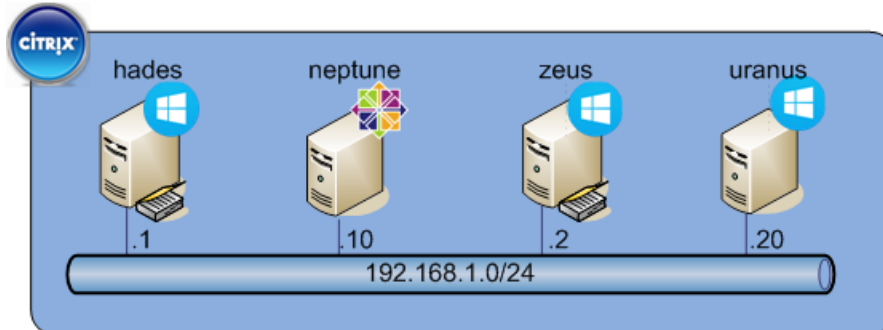


1 La maquette

1.1 Général

La maquette est réalisée sur une plateforme Citrix Xen Server non redondée.

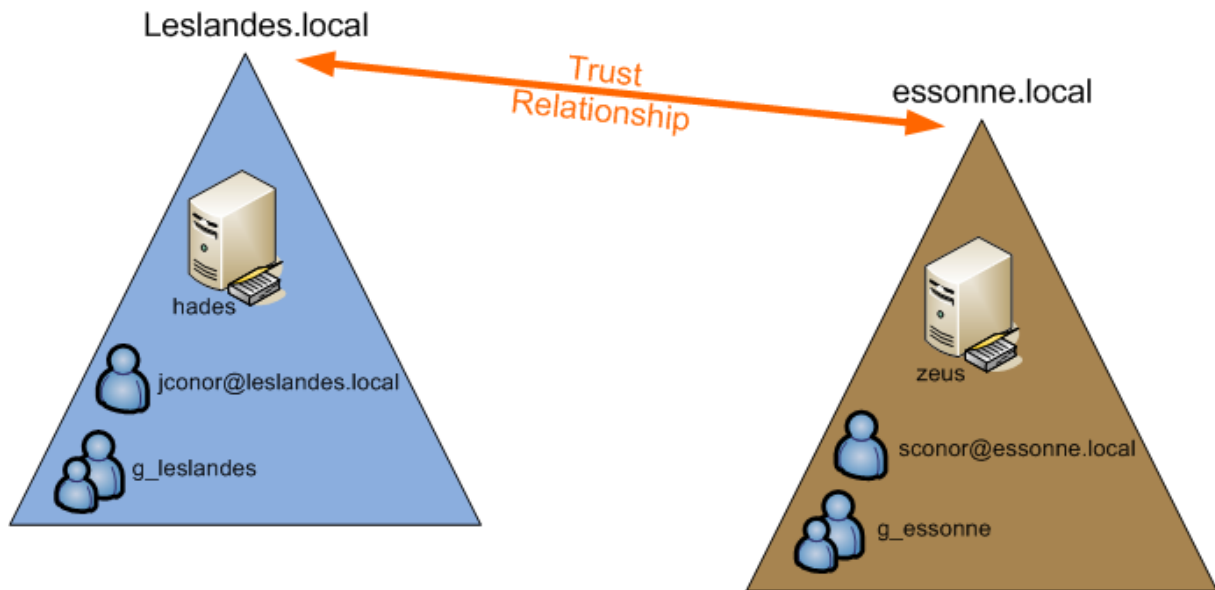


Nous avons quatre serveurs ;

- Deux serveur Windows Server 2012 R2 Datacenter qui ont comme rôles AD DS et DNS avec comme « option » :
 - o « Unix attribut » pour l'authentification des clients depuis une machine Linux
 - o « Condition Forwarders » pour que chaque domaines puissent résoudre les machines des différents domaines.
 - o « Trust Relationship » pour que les utilisateurs d'un domaine A puisse accéder aux ressources d'un domaine B et vice et versa.
- Un serveur Linux CentOS 6.6 dataserver avec les paquets sssd-1.11.6-30.el6_6.4.x86_64, krb5-workstation, openldap-clients, ntp, bind-utils,... d'installés.
- Un serveur Windows Server 2012 R2 Datacenter qui est un serveur d'application afin que les utilisateurs de la foret A et B puissent se connecter.

1.2 Configuration AD

Ici j'ai créé deux forets qui sont « leslandes.local » et « essonne.local ».



Sur le serveur hades.leslandes.local, j'ai créé un groupe g_leslandes avec les attributs unix suivants :

- NIS Domain : leslandes
- GID (Groupe ID) : 10 000

Ainsi qu'un utilisateur jconor@leslandes.local avec les attributs Unix suivants :

- NIS Domain : leslandes
- UID : 10 001
- Login shell : /bin/sh
- Home Directory : /home/jconor
- Primary group name/GID : g_leslandes

Sur le serveur zeus.essonne.local, j'ai créé un groupe g_essonne avec les attributs unix suivants :

- NIS Domain : essonne
- GID (Groupe ID) : 10 000

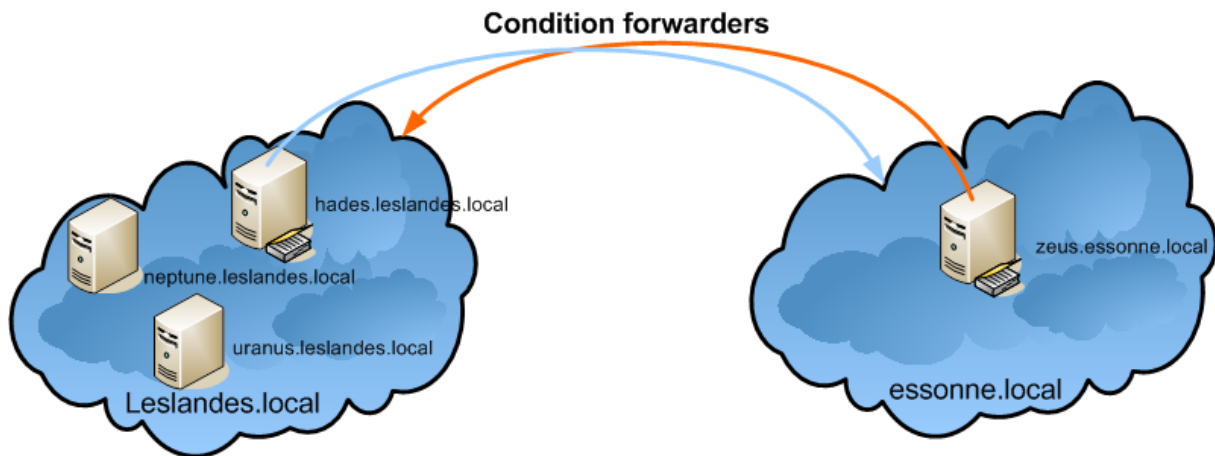
Ainsi qu'un utilisateur sconor@essonne.local avec les attributs Unix suivants :

- NIS Domain : essonne
- UID : 10 001
- Login shell : /bin/sh
- Home Directory : /home/sconor
- Primary group name/GID : g_essonne

Trust relationship est paramétré en bidirectionnel (2-Ways) entre deux forets. Un utilisateur user@domainA pourra se connecter sur une machine du domaine B et un utilisateur user@domainB pourra se connecter sur une machine du domaine A.

1.3 Configuration DNS

Il y a deux domaines :



Le principe de mettre en place du « conditional forwarder » est de pouvoir résoudre des noms de machines, adresse IP ou FQDN d'un autre domaine.

Hades.leslandes.local					
Forward lookup zone			Reverse lookup zone		
X	SOA	hades.leslandes.local	X	SOA	hades.leslandes.local
X	NS	hades.leslandes.local	X	NS	hades.leslandes.local
Hades	A	192.168.1.1	192.168.1.1	PTR	hades.leslandes.local
Neptune	A	192.168.1.10	192.168.1.10	PTR	neptune.leslandes.local
Uranus	A	192.168.1.20	192.168.1.20	PTR	uranus.leslandes.local
Conditionnal forwarders					
192.168.1.2			essonne.local		

Zeus.essonne.local					
Forward lookup zone			Reverse lookup zone		
X	SOA	zeus.essonne.local	X	SOA	zeus.essonne.local
X	NS	zeus.essonne.local	X	NS	zeus.essonne.local
Zeus	A	192.168.1.2	192.168.1.2	PTR	zeus.leslandes.local
Conditionnal forwarders					
192.168.1.1			leslandes.local		

1.4 Le client Linux

1.4.1 Fichiers de configurations

Le client est basé sur un CentOS 6.6 dataserver. Voici la configuration appliquée sur le client pour qu'il puisse intégrer un domaine Windows et que les utilisateurs de l'AD puissent s'authentifier.

/etc/hosts

```
127.0.0.1          localhost    localhost.localdomain  localhost4
localhost4.localdomain4
::1               localhost    localhost.localdomain  localhost6
localhost6.localdomain6
192.168.1.1       hades.leslandes.local  hades
192.168.1.2       zeus.essonne.local     zeus
192.168.1.10      neptune.leslandes.local neptune
```

/etc/resolv.conf

```
nameserver 192.168.1.1
nameserver 192.168.1.2
search leslandes.local
search essonne.local
```

/etc/samba/smb.conf

```
[global]
  workgroup = LESLANDES
  client signing = yes
  client use spnego = yes
  kerberos method = secrets and keytab
  log file = /var/log/samba/%m.log
  password server = MoTdePAsSe
  realm = LESLANDES.LOCAL
  security = ads
```

/etc/krb5.conf

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
# default_realm = LESLANDES.LOCAL
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
rdns = false
forwardable = yes

[realms]
LESLANDES.LOCAL = {
kdc = hades.leslandes.local
admin_server = hades.leslandes.local
}
ESSONNE.LOCAL = {
kdc = zeus.essonne.local
admin_server = zeus.essonne.local
}

[domain_realm]
.leslandes.local = LESLANDES.LOCAL
leslandes.local = LESLANDES.LOCAL
.essonne.local = ESSONNE.LOCAL
essonne.local = ESSONNE.LOCAL
```

/etc/sss/sss.conf

```
[sss]
config_file_version = 2
domains = leslandes.local, essonne.local
services = nss, pam
debug_level = 0

[nss]
[pam]

[domain/leslandes.local]

ldap_referrals = false
enumerate = false
id_provider = ldap
auth_provider = krb5
chpass_provider = krb5
access_provider = ldap
ldap_sasl_mech = GSSAPI
ldap_schema = rfc2307bis
ldap_user_search_base = dc=leslandes,dc=local
ldap_user_object_class = user
ldap_user_home_directory = unixHomeDirectory
ldap_user_principal = userPrincipalName
ldap_group_search_base = dc=leslandes,dc=local
ldap_group_object_class = group
ldap_access_order = expire
ldap_account_expire_policy = ad
ldap_force_upper_case_realm = true
krb5_realm = LESLANDES.LOCAL
krb5_canonicalize = false

[domain/essonne.local]

ldap_referrals = false
enumerate = false
id_provider = ldap
auth_provider = krb5
chpass_provider = krb5
access_provider = ldap
ldap_sasl_mech = GSSAPI
ldap_schema = rfc2307bis
ldap_user_search_base = dc=essonne,dc=local
ldap_user_object_class = user
ldap_user_home_directory = unixHomeDirectory
ldap_user_principal = userPrincipalName
ldap_group_search_base = dc=essonne,dc=local
ldap_group_object_class = group
ldap_access_order = expire
ldap_account_expire_policy = ad
ldap_force_upper_case_realm = true

krb5_realm = ESSONNE.LOCAL
krb5_canonicalize = false
```

1.4.2 Intégration au domaine et authentification AD

```
net ads join -U Administrator

Enter Administrator's password:
Using short domain name -- LESLANDES
Joined 'NEPTUNE' to dns domain 'leslandes.local'
Keytab name: FILE:/etc/krb5.keytab
```

Cette commande permet de joindre une machine linux à un domaine Windows. Le fichier qu'interroge l'AD lors de l'intégration est le fichier `/etc/samba/smb.conf`. Puis le mot de passe AD sera demandé. La machine sera par défaut ajouté dans l'OU Computers, et le fichier `/etc/krb5.keytab` sera généré automatiquement.

```
klist -ke

KVNO Principal
-----
-----
 2 host/neptune.leslandes.local@LESLANDES.LOCAL (des-cbc-crc)
 2 host/neptune.leslandes.local@LESLANDES.LOCAL (des-cbc-md5)
 2 host/neptune.leslandes.local@LESLANDES.LOCAL (aes128-cts-hmac-sha1-96)
 2 host/neptune.leslandes.local@LESLANDES.LOCAL (aes256-cts-hmac-sha1-96)
 2 host/neptune.leslandes.local@LESLANDES.LOCAL (arcfour-hmac)
 2 host/neptune@LESLANDES.LOCAL (des-cbc-crc)
 2 host/neptune@LESLANDES.LOCAL (des-cbc-md5)
 2 host/neptune@LESLANDES.LOCAL (aes128-cts-hmac-sha1-96)
 2 host/neptune@LESLANDES.LOCAL (aes256-cts-hmac-sha1-96)
 2 host/neptune@LESLANDES.LOCAL (arcfour-hmac)
 2 NEPTUNE$@LESLANDES.LOCAL (des-cbc-crc)
 2 NEPTUNE$@LESLANDES.LOCAL (des-cbc-md5)
 2 NEPTUNE$@LESLANDES.LOCAL (aes128-cts-hmac-sha1-96)
 2 NEPTUNE$@LESLANDES.LOCAL (aes256-cts-hmac-sha1-96)
 2 NEPTUNE$@LESLANDES.LOCAL (arcfour-hmac)
```

Cette commande permet d'afficher le ticket Kerberos (choisir le dernier NEPTUNE\$@LESLANDES.LOCAL)

```
kinit -k NEPTUNE$@LESLANDES.LOCAL
```

Cette commande permet de récupérer le ticket Kerberos

Une fois cela fait, vous pouvez tester en faisant une requête LDAP, ou une requête via SSSD qui utilise LDAP & RBR5.

```
/usr/bin/ldapsearch -H ldap://hades.leslandes.local/ -Y GSSAPI -N -b
"dc=leslandes,dc=local" "(&(objectClass=user)(sAMAccountName=jhades))"

SASL/GSSAPI authentication started
SASL username: NEPTUNE$@LESLANDES.LOCAL
SASL SSF: 56
SASL data security layer installed.
# extended LDIF
#
# LDAPv3
# base <dc=leslandes,dc=local> with scope subtree
# filter: (&(objectClass=user)(sAMAccountName=jhades))
# requesting: ALL
#
# john hades, administration, utilisateurs, leslandes.local
dn: CN=john hades,OU=administration,OU=utilisateurs,DC=leslandes,DC=local
... ..

# search result
search: 4
result: 0 Success

# numResponses: 5
# numEntries: 1
# numReferences: 3
```

Ou avec id

```
[root@neptune join_ad_sssd]# id jhades
uid=10000(jhades) gid=10000(g_leslandes) groupes=10000(g_leslandes)
```

A partir d'ici les utilisateurs du domaine leslandes.local peuvent s'authentifier sur la machine Linux mais pas les utilisateurs du domaine essonne.local.

2 Les tests

2.1 Requêtes vers les DNS

depuis	Hades.leslandes.local	Zeus.leslandes.local	Neptune.leslandes.local
nslookup	Hades.leslandes.local	Hades.leslandes.local	Hades.leslandes.local
	192.168.1.1	192.168.1.1	192.168.1.1
	neptune.leslandes.local	neptune.leslandes.local	neptune.leslandes.local
	192.168.1.10	192.168.1.10	192.168.1.10
	Zeus.leslandes.local	Zeus.leslandes.local	Zeus.leslandes.local
	192.168.1.2	192.168.1.2	192.168.1.2

non-existent domain	Non-authoritative answer	ok
---------------------	--------------------------	----

Depuis neptune.leslandes.local

```
[root@neptune join_ad_sssd]# dig -t SRV _ldap._tcp.hades.leslandes.local
@hades.leslandes.local

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.3 <<>> -t SRV
_ldap._tcp.hades.leslandes.local @hades.leslandes.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 1693
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;_ldap._tcp.hades.leslandes.local. IN SRV

;; AUTHORITY SECTION:
leslandes.local. 3600 IN SOA hades.leslandes.local.
hostmaster.leslandes.local. 31 900 600 86400 3600

;; Query time: 1 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Aug 6 16:46:57 2015
;; MSG SIZE rcvd: 118
```

```
[root@neptune join_ad_sssd]# dig -t SRV _ldap._tcp.zeus.essonne.local
@zeus.essonne.local

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6_6.3 <<>> -t SRV
_ldap._tcp.zeus.essonne.local @zeus.essonne.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 27349
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;_ldap._tcp.zeus.essonne.local. IN SRV

;; AUTHORITY SECTION:
essonne.local. 3600 IN SOA zeus.essonne.local.
hostmaster.essonne.local. 31 900 600 86400 3600

;; Query time: 3 msec
;; SERVER: 192.168.1.2#53(192.168.1.2)
;; WHEN: Thu Aug 6 16:48:21 2015
;; MSG SIZE rcvd: 112
```

Depuis hades.leslandes.local

```
C:\Users\Administrator>nslookup
Default Server: localhost
Address: 127.0.0.1

> set type=srv
> _ldap._tcp.leslandes.local
Server: localhost
Address: 127.0.0.1

_ldap._tcp.leslandes.local      SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = hades.leslandes.local
hades.leslandes.local internet address = 192.168.1.1
> _ldap._tcp.essonne.local
Server: localhost
Address: 127.0.0.1

Non-authoritative answer:
_ldap._tcp.essonne.local      SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = zeus.essonne.local
```

Depuis zeus.essonne.local

```
C:\Users\Administrator>nslookup
Default Server: localhost
Address: 127.0.0.1

> set type=srv
> _ldap._tcp.leslandes.local
Server: localhost
Address: 127.0.0.1

_ldap._tcp.leslandes.local      SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = hades.leslandes.local
hades.leslandes.local internet address = 192.168.1.1
> _ldap._tcp.essonne.local
Server: localhost
Address: 127.0.0.1

_ldap._tcp.essonne.local      SRV service location:
    priority = 0
    weight   = 100
    port     = 389
    svr hostname = zeus.essonne.local
zeus.essonne.local internet address = 192.168.1.2
```

2.2 Requête vers les AD

Depuis Neptune.leslandes.local requete vers l'AD du domaine leslandes.local.

```
[root@neptune]# /usr/bin/ldapsearch -H ldap://hades.leslandes.local/
-Y          GSSAPI          -N          -b          "dc=leslandes,dc=local"
"(&(objectClass=user)(sAMAccountName=jhades))"
SASL/GSSAPI authentication started
SASL username: NEPTUNE$@LESLANDES.LOCAL
SASL SSF: 56
SASL data security layer installed.
# extended LDIF
#
# LDAPv3
# base <dc=leslandes,dc=local> with scope subtree
# filter: (&(objectClass=user)(sAMAccountName=jhades))
# requesting: ALL
#
# john hades, administration, utilisateurs, leslandes.local
dn: CN=john
... ..
# search result
search: 4
result: 0 Success
# numResponses: 5
# numEntries: 1
# numReferences: 3
```

Depuis Neptune.leslandes.local requete vers l'AD du domaine l'essonne.local.

```
[root@neptune      join_ad_sssd]# /usr/bin/ldapsearch -H
ldap://zeus.essonne.local/ -Y GSSAPI -N -b "dc=essonne,dc=local"
"(&(objectClass=user)(sAMAccountName=jzeus))"
SASL/GSSAPI authentication started
SASL username: NEPTUNE$@LESLANDES.LOCAL
SASL SSF: 56
SASL data security layer installed.
# extended LDIF
#
# LDAPv3
# base <dc=essonne,dc=local> with scope subtree
# filter: (&(objectClass=user)(sAMAccountName=jzeus))
# requesting: ALL
#
# john zeus, finance, allusers, essonne.local
dn: CN=john zeus,OU=finance,OU=allusers,DC=essonne,DC=local
... ..
# search result
search: 4
result: 0 Success
# numResponses: 5
# numEntries: 1
# numReferences: 3
```

```
[root@neptune join_ad_sssd]# id jconor@LESLANDES.LOCAL
uid=10001(jconor@leslandes.local)
gid=10000(g_leslandes@leslandes.local)
groupes=10000(g\_leslandes@leslandes.local)

[root@neptune join_ad_sssd]# id sconor@ESSONNE.LOCAL
id: sconor@ESSONNE.LOCAL : utilisateur inexistant
```

2.3 Requêtes Kerberos

```
[root@neptune join_ad_sssd]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: NEPTUNE$@LESLANDES.LOCAL

Valid starting      Expires            Service principal
08/06/15            08:49:47          08/06/15          18:49:35
krbtgt/LESLANDES.LOCAL@LESLANDES.LOCAL
    renew until 08/13/15 08:49:47
08/06/15            08:49:35          08/06/15          18:49:35
ldap/hades.leslandes.local@LESLANDES.LOCAL
    renew until 08/13/15 08:49:35
08/06/15            08:50:13          08/06/15          18:49:35
krbtgt/ESSONNE.LOCAL@LESLANDES.LOCAL
    renew until 08/13/15 08:49:47
08/06/15            08:50:15          08/06/15          18:49:35
ldap/zeus.essonne.local@ESSONNE.LOCAL
    renew until 08/13/15 08:49:47
```

```
[root@neptune join_ad_sssd]# getent passwd jconor@LESLANDES.LOCAL
jconor@leslandes.local:*:10001:10000:john conor:/home/jconor:/bin/sh
```

```
[root@neptune join_ad_sssd]# getent passwd sconor@ESSONNE.LOCAL
[root@neptune join_ad_sssd]#
```

2.4 Les logs

```
[root@neptune join_ad_sssd]# ls -l /var/log/sss/
total 32
-rw----- 1 root root    0  4 août 17:47 krb5_child.log
-rw----- 1 root root 15358 7 août 09:54 ldap_child.log
-rw----- 1 root root    0  4 août 17:46 sssd_essonne.local.log
-rw----- 1 root root  323 6 août 10:25 sssd_leslandes.local.log
-rw----- 1 root root  294 6 août 10:25 sssd.log
-rw----- 1 root root  291 6 août 10:25 sssd_nss.log
-rw----- 1 root root  291 6 août 10:25 sssd_pam.log
```

```
(Fri Aug 7 09:57:18 2015) [[sssd[ldap_child[11396]]]]
[ldap_child_get_tgt_sync] (0x0010): Failed to init credentials:
Client 'host/neptune.leslandes.local@LESLANDES.LOCAL' not found in
Kerberos database
```

```
[root@neptune sssd]# tail -f sssd_leslandes.local.log
(Fri Sep 11 15:50:12 2015) [sssd[be[leslandes.local]]]
[be_get_account_info] (0x0200): Got request for [0x1003][1][name=bwillis]
(Fri Sep 11 15:50:12 2015) [sssd[be[leslandes.local]]]
[sdap_ad_tokengroups_get_posix_members] (0x0080): Domain not found for SID
S-1-5-32-545
(Fri Sep 11 15:50:12 2015) [sssd[be[leslandes.local]]]
[sdap_ad_tokengroups_get_posix_members] (0x0080): Domain not found for SID
S-1-5-21-3088001152-1634463833-1660011001-513
(Fri Sep 11 15:50:12 2015) [sssd[be[leslandes.local]]] [acctinfo_callback]
(0x0100): Request processed. Returned 0,0,Success
(Fri Sep 11 15:50:16 2015) [sssd[be[leslandes.local]]]
[resolve_gethostbyname_done] (0x0040): querying hosts database failed [5]:
Erreur d'entrée/sortie
(Fri Sep 11 15:50:16 2015) [sssd[be[leslandes.local]]]
[nsupdate_get_addrs_done] (0x0040): Could not resolve address for this
machine, error [5]: Erreur d'entrée/sortie, resolver returned: [12]:
Timeout while contacting DNS servers
(Fri Sep 11 15:50:16 2015) [sssd[be[leslandes.local]]]
[nsupdate_get_addrs_done] (0x0040): nsupdate_get_addrs_done failed: [5]:
[Erreur d'entrée/sortie]
(Fri Sep 11 15:50:16 2015) [sssd[be[leslandes.local]]]
[sdap_dyndns_dns_addrs_done] (0x0040): Could not receive list of current
addresses [5]: Erreur d'entrée/sortie
(Fri Sep 11 15:50:16 2015) [sssd[be[leslandes.local]]]
[ad_dyndns_sdap_update_done] (0x0040): Dynamic DNS update failed [5]:
Erreur d'entrée/sortie
(Fri Sep 11 15:50:16 2015) [sssd[be[leslandes.local]]]
[ad_dyndns_nsupdate_done] (0x0040): Updating DNS entry failed [5]: Erreur
d'entrée/sortie
^C
[root@neptune sssd]# ls -l
total 56
-rw----- 1 root root    0 11 sept. 15:49 krb5_child.log
-rw----- 1 root root 2050 11 sept. 15:50 ldap_child.log
-rw----- 1 root root 20977 11 sept. 15:50 sssd_essonne.local.log
-rw----- 1 root root 26733 11 sept. 15:50 sssd_leslandes.local.log
-rw----- 1 root root    0 11 sept. 15:49 sssd.log
-rw----- 1 root root    0 11 sept. 15:49 sssd_nss.log
-rw----- 1 root root    0 11 sept. 15:49 sssd_pam.log
[root@neptune sssd]# tail -f sssd_essonne.local.log
```

```

(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]]
[be_resolve_server_process] (0x0200): Found address for server
zeus.essonne.local: [192.168.1.2] TTL 7200
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]] [sdap_kinit_done]
(0x0100): Could not get TGT: 14 [Mauvaise adresse]
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]] [fo_set_port_status]
(0x0100): Marking port 389 of server 'zeus.essonne.local' as 'not working'
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]]
[fo_resolve_service_send] (0x0100): Trying to resolve service 'AD'
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]]
[fo_resolve_service_send] (0x0020): No available servers for service 'AD'
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]]
[sdap_id_op_connect_done] (0x0020): Failed to connect, going offline (5
[Erreur d'entrée/sortie])
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]] [be_run_offline_cb]
(0x0080): Going offline. Running callbacks.
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]] [acctinfo_callback]
(0x0100): Request processed. Returned 1,11,Offline
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]] [child_sig_handler]
(0x0100): child [28158] finished successfully.
(Fri Sep 11 15:50:50 2015) [sssd[be[essonne.local]]]
[remove_krb5_info_files] (0x0200): Could not remove
[/var/lib/sss/pubconf/kpasswdinfo.ESSONNE.LOCAL], [2][Aucun fichier ou
dossier de ce type]
^C
[root@neptune sssd]# ls -l
total 56
-rw----- 1 root root 0 11 sept. 15:49 krb5_child.log
-rw----- 1 root root 2050 11 sept. 15:50 ldap_child.log
-rw----- 1 root root 20977 11 sept. 15:50 sssd_essonne.local.log
-rw----- 1 root root 26733 11 sept. 15:50 sssd_leslandes.local.log
-rw----- 1 root root 0 11 sept. 15:49 sssd.log
-rw----- 1 root root 0 11 sept. 15:49 sssd_nss.log
-rw----- 1 root root 0 11 sept. 15:49 sssd_pam.log
[root@neptune sssd]# tail -f ldap_child.log
(Fri Sep 11 15:50:12 2015) [[sssd[ldap_child[28152]]]] [become_user]
(0x0200): Already user [0].
(Fri Sep 11 15:50:12 2015) [[sssd[ldap_child[28152]]]]
[ldap_child_get_tgt_sync] (0x0100): Principal name is:
[NEPTUNE$@LESLANDES.LOCAL]
(Fri Sep 11 15:50:12 2015) [[sssd[ldap_child[28152]]]]
[ldap_child_get_tgt_sync] (0x0100): Using keytab [MEMORY:/etc/krb5.keytab]
(Fri Sep 11 15:50:50 2015) [[sssd[ldap_child[28158]]]] [unpack_buffer]
(0x0200): Will run as [0][0].
(Fri Sep 11 15:50:50 2015) [[sssd[ldap_child[28158]]]] [become_user]
(0x0200): Trying to become user [0][0].
(Fri Sep 11 15:50:50 2015) [[sssd[ldap_child[28158]]]] [become_user]
(0x0200): Already user [0].
(Fri Sep 11 15:50:50 2015) [[sssd[ldap_child[28158]]]]
[ldap_child_get_tgt_sync] (0x0100): Principal name is:
[host/neptune.leslandes.local@LESLANDES.LOCAL]
(Fri Sep 11 15:50:50 2015) [[sssd[ldap_child[28158]]]]
[ldap_child_get_tgt_sync] (0x0100): Using keytab [MEMORY:/etc/krb5.keytab]
(Fri Sep 11 15:50:50 2015) [[sssd[ldap_child[28158]]]]
[ldap_child_get_tgt_sync] (0x0010): Failed to init credentials: Client
'host/neptune.leslandes.local@LESLANDES.LOCAL' not found in Kerberos
database
(Fri Sep 11 15:50:50 2015) [[sssd[ldap_child[28158]]]] [main] (0x0020):
ldap_child_get_tgt_sync failed.

```