

Installation des serveurs Kerberos

Cette page montre comment installer deux serveurs Kerberos redondants (**kerb1** le maître et **kerb2** l'esclave).

- [Installation du serveur maître](#)
 - [Installation du système](#)
 - [Installation du KDC \(Key Distribution Center\)](#)
- [Installation du serveur esclave](#)
 - [Installation du système](#)
 - [Installation du KDC \(Key Distribution Center\)](#)
- [Mise en place de la réplication](#)
- [Gestion des principals](#)

Installation du serveur maître

Installation du système

Nom du serveur	kerb1.univ-rennes1.fr
Système	RedHat Entreprise 5
Ouverture de ports	ssh (22 tcp) kinit (88 tcp/udp) kerberos password (749 tcp) kerberos auth (750 tcp)

Configurer la synchronisation de l'horloge sur le serveur **ntp.univ-rennes1.fr** (cf **/etc/ntp.conf**) et s'assurer que le démon **ntpd** est en marche :

```
[root@kerb1 ~]# chkconfig ntpd on
[root@kerb1 ~]# service ntpd start
ntpd: Synchronizing with time server:      [ OK ]
Syncing hardware clock to system time     [ OK ]
Starting ntpd:                             [ OK ]
[root@kerb1 ~]#
```

Installation du KDC (Key Distribution Center)

Editer le fichier **/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 = UNIV-RENNES1.FR
dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 24h
forwardable = yes

[realms]
UNIV-RENNES1.FR = {
    kdc = kerb1.univ-rennes1.fr:88
    admin_server = kerb1.univ-rennes1.fr:749
    default_domain = univ-rennes1.fr
}

[domain_realm]
.univ-rennes1.fr = UNIV-RENNES1.FR
univ-rennes1.fr = UNIV-RENNES1.FR

[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
}
```

Installer le package **krb5-server** (**yum install krb5-server**).

Editer le fichier **/var/kerberos/krb5kdc/kdc.conf** :

```
[kdcdefaults]
v4_mode = nopreauth
kdc_ports = 88,750
kdc_tcp_ports = 88

[realms]
UNIV-RENNES1.FR = {
    #master_key_type = des3-hmac-sha1
    acl_file = /var/kerberos/krb5kdc/kadm5.acl
    dict_file = /usr/share/dict/words
    admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
    supported_encetypes = des3-hmac-sha1:normal arcfour-hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-
cbc-crc:normal des-cbc-crc:v4 des-cbc-crc:afs3
}
```

Editer le fichier **/var/kerberos/krb5kdc/kadm5.acl** :

```
*/admin@UNIV-RENNES1.FR
```

Créer la base Kerberos :

```
[root@kerb1 ~]# kdb5_util create -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm 'UNIV-RENNES1.FR',
master key name 'K/M@UNIV-RENNES1.FR'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
[root@kerb1 ~]#
```

Ajouter le premier utilisateur (**root/admin**) :

```
[root@kerb1 ~]# kadmin.local -q "addprinc root/admin"
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
WARNING: no policy specified for root/admin@UNIV-RENNES1.FR; defaulting to no policy
Enter password for principal "root/admin@UNIV-RENNES1.FR":
Re-enter password for principal "root/admin@UNIV-RENNES1.FR":
Principal "root/admin@UNIV-RENNES1.FR" created.
[root@kerb1 ~]#
```

Démarrer les services :

```
[root@kerb1 ~]# chkconfig kadmin on
[root@kerb1 ~]# service kadmin start
Starting Kerberos 5 Admin Server: [ OK ]
[root@kerb1 ~]# chkconfig krb5kdc on
[root@kerb1 ~]# service krb5kdc start
Starting Kerberos 5 KDC: [ OK ]
[root@kerb1 ~]#
```

Vérification en affichant la liste des *principals* :

```
[root@kerb1 ~]# kadmin -p root/admin
Authenticating as principal root/admin with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin: listprincs
K/M@UNIV-RENNES1.FR
kadmin/admin@UNIV-RENNES1.FR
kadmin/changepw@UNIV-RENNES1.FR
kadmin/history@UNIV-RENNES1.FR
kadmin/localhost.localdomain@UNIV-RENNES1.FR
krbtgt/UNIV-RENNES1.FR@UNIV-RENNES1.FR
root/admin@UNIV-RENNES1.FR
kadmin: exit
[root@kerb1 ~]#
```

Installation du serveur esclave

Installation du système

Nom du serveur	kerb2.univ-rennes1.fr
Système	RedHat Entreprise 5
Ouverture de ports	ssh (22 tcp) kinit (88 tcp/udp) kerberos auth (750 tcp)

Installation du KDC (Key Distribution Center)

Installer le package `krb5-server`, puis répéter toutes les opérations faites sur le serveur **kerb1**, seule l'ouverture du port 749 n'est pas nécessaire.

Pour aller plus vite, copier les fichiers `/etc/krb5.conf`, `/var/kerberos/krb5kdc/kdc.conf` et `/var/kerberos/krb5kdc/kadm5.acl` depuis le serveur `kerb1` :

```
[root@kerb2 ~]# scp root@kerb1:/etc/krb5.conf /etc
root@kerb1's password:
krb5.conf                                100% 638      0.6KB/s   00:00
[root@kerb2 ~]# scp root@kerb1:/var/kerberos/krb5kdc/kdc.conf /var/kerberos/krb5kdc/
root@kerb1's password:
kdc.conf                                100% 414      0.4KB/s   00:00
[root@kerb2 ~]# scp root@kerb1:/var/kerberos/krb5kdc/kadm5.acl /var/kerberos/krb5kdc/
root@kerb1's password:
kadm5.acl                              100% 26       0.0KB/s   00:00
[root@kerb2 ~]#
```

Et modifier la partie **realms** du fichier `/etc/krb5.conf` (remplacer **kerb1** par **kerb2**):

```
[realms]
UNIV-RENNES1.FR = {
  kdc = kerb2.univ-rennes1.fr:88
  admin_server = kerb2.univ-rennes1.fr:749
  default_domain = univ-rennes1.fr
}
```

Créer la base Kerberos, ajouter le premier utilisateur (**root/admin**), démarrer les services et vérifier le fonctionnement en affichant les *principals*.

Mise en place de la réplication

Sur le serveur maître, créer les clés des serveurs **kerb1** et **kerb2** et les exporter dans la *keytab* par défaut du serveur (`/etc/krb5.keytab`) :

```
[root@kerb1 ~]# kadmin -p root/admin
Authenticating as principal root/admin with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin: addprinc -randkey host/kerb1.univ-rennes1.fr
WARNING: no policy specified for host/kerb1.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "host/kerb1.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin: addprinc -randkey host/kerb2.univ-rennes1.fr
WARNING: no policy specified for host/kerb2.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "host/kerb2.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin: ktadd host/kerb1.univ-rennes1.fr
Entry for principal host/kerb1.univ-rennes1.fr with kvno 3, encryption type Triple DES cbc mode with HMAC/sha1
added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/kerb1.univ-rennes1.fr with kvno 3, encryption type ArcFour with HMAC/md5 added to
keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/kerb1.univ-rennes1.fr with kvno 3, encryption type DES with HMAC/sha1 added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal host/kerb1.univ-rennes1.fr with kvno 3, encryption type DES cbc mode with RSA-MD5 added to
keytab WRFILE:/etc/krb5.keytab.
kadmin: ktadd host/kerb2.univ-rennes1.fr
Entry for principal host/kerb2.univ-rennes1.fr with kvno 3, encryption type Triple DES cbc mode with HMAC/sha1
added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/kerb2.univ-rennes1.fr with kvno 3, encryption type ArcFour with HMAC/md5 added to
keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/kerb2.univ-rennes1.fr with kvno 3, encryption type DES with HMAC/sha1 added to keytab
WRFILE:/etc/krb5.keytab.
Entry for principal host/kerb2.univ-rennes1.fr with kvno 3, encryption type DES cbc mode with RSA-MD5 added to
keytab WRFILE:/etc/krb5.keytab.
kadmin: exit
[root@kerb1 ~]#
```

Sur le serveur esclave, copier le fichier `/etc/krb5.keytab` :

```
[root@kerb2 ~]# scp root@kerb1.univ-rennes1.fr:/etc/krb5.keytab /etc
krb5.keytab                            100% 634      0.6KB/s   00:00
[root@kerb2 ~]#
```

Sur le serveur esclave, éditer le fichier `/var/kerberos/krb5kdc/kpropd.ac1` de la manière suivante :

```
host/kerb1.univ-rennes1.fr@UNIV-RENNES1.FR
host/kerb2.univ-rennes1.fr@UNIV-RENNES1.FR
```

Et démarrer le service **kpropd** :

```
[root@kerb2 ~]# chkconfig kprop on
[root@kerb2 ~]# service kprop start
Starting Kerberos 5 Propagation Server:           [ OK ]
[root@kerb2 ~]#
```

Sur le serveur maître, créer le script `/usr/local/bin/krb5prop.sh` :

```
[root@kerb1 ~]# cat > /usr/local/bin/krb5prop.sh
#!/bin/sh
/usr/kerberos/sbin/kdb5_util dump /var/kerberos/krb5kdc/slave_datatrans
/usr/kerberos/sbin/kprop -f /var/kerberos/krb5kdc/slave_datatrans kerb2.univ-rennes1.fr > /dev/null
[root@kerb1 ~]# chmod 700 /usr/local/bin/krb5prop.sh
[root@kerb1 ~]#
```

Exécuter le script « à la main » :

```
[root@kerb1 ~]# /usr/kerberos/sbin/kdb5_util dump /var/kerberos/krb5kdc/slave_datatrans
[root@kerb1 ~]# /usr/kerberos/sbin/kprop -f /var/kerberos/krb5kdc/slave_datatrans kerb2.univ-rennes1.fr
Database propagation to kerb2.univ-rennes1.fr: SUCCEEDED
[root@kerb1 ~]#
```

Pour vérifier la bonne propagation des *principals*, ajouter un *principal* fictif sur le serveur maître et propager vers le serveur esclave :

```
[root@kerb1 ~]# kadmin -p root/admin
Authenticating as principal root/admin with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin: addprinc dummy
WARNING: no policy specified for dummy@UNIV-RENNES1.FR; defaulting to no policy
Enter password for principal "dummy@UNIV-RENNES1.FR":
Re-enter password for principal "dummy@UNIV-RENNES1.FR":
Principal "dummy@UNIV-RENNES1.FR" created.
kadmin: exit
[root@kerb1 ~]# /usr/local/bin/krb5prop.sh
[root@kerb1 ~]#
```

Sur le serveur esclave, vérifier la présence du nouveau principal :

```
[root@kerb2 ~]# kadmin.local -q "listprincs"
Authenticating as principal rootifsic/admin@UNIV-RENNES1.FR with password.
K/M@UNIV-RENNES1.FR
dummy@UNIV-RENNES1.FR
host/kerb1.univ-rennes1.fr@UNIV-RENNES1.FR
host/kerb2.univ-rennes1.fr@UNIV-RENNES1.FR
kadmin/admin@UNIV-RENNES1.FR
kadmin/changepw@UNIV-RENNES1.FR
kadmin/history@UNIV-RENNES1.FR
kadmin/localhost.localdomain@UNIV-RENNES1.FR
krbtgt/UNIV-RENNES1.FR@UNIV-RENNES1.FR
root/admin@UNIV-RENNES1.FR
[root@kerb2 ~]#
```

Ne pas oublier de supprimer le principal fictif ensuite (**kadmin.local -q "delprinc dummy"** sur **kerb1**).

Modifier le fichier `/etc/crontab` pour faire en sorte que la synchronisation entre les deux KDCs soient effectuée de manière automatique toutes les 5 minutes (par exemple) :

```
*/5 * * * * /usr/local/bin/krb5prop.sh
```

Les deux serveurs **kerb1** et **kerb2** sont maintenant installés.

Gestion des principaux

La gestion des *principals* peut se faire à distance à l'aide **kadmin** depuis une machine d'administration (de confiance).

Pour cela, depuis la machine d'administration, on génère un *principal* **manager/admin** et on exporte sa clé dans une *keytab* locale :

```
[root@admin ~]# kadmin -p root/admin
Authenticating as principal root/admin with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin: addprinc -randkey manager/admin
WARNING: no policy specified for manager/admin@UNIV-RENNES1.FR; defaulting to no policy
Principal "manager/admin@UNIV-RENNES1.FR" created.
kadmin: ktadd -k /etc/manager.keytab manager/admin
Entry for principal manager/admin with kvno 3, encryption type Triple DES cbc mode with HMAC/sha1 added to
keytab WRFILE:/etc/manager.keytab.
Entry for principal manager/admin with kvno 3, encryption type ArcFour with HMAC/md5 added to keytab WRFILE:/etc
/manager.keytab.
Entry for principal manager/admin with kvno 3, encryption type DES with HMAC/sha1 added to keytab WRFILE:/etc
/manager.keytab.
Entry for principal manager/admin with kvno 3, encryption type DES cbc mode with RSA-MD5 added to keytab WRFILE:
/etc/manager.keytab.
kadmin: exit
[root@admin ~]#
```

On utilise ensuite la commande **kadmin -p manager/admin -k -t /etc/manager.keytab -q "commande_kadmin"** pour exécuter la commande **commande_kadmin**. Par exemple :

```
[root@admin ~]# kadmin -p manager/admin -k -t /etc/manager.keytab -q "listprincs"
Authenticating as principal manager/admin with keytab /etc/manager.keytab.
HTTP/cas-kerb.univ-rennes1.fr@UNIV-RENNES1.FR
K/M@UNIV-RENNES1.FR
cas/admin@UNIV-RENNES1.FR
host/cas-kerb.univ-rennes1.fr@UNIV-RENNES1.FR
host/clinix.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR
host/cwixnp.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR
host/kerb1.univ-rennes1.fr@UNIV-RENNES1.FR
host/kerb2.univ-rennes1.fr@UNIV-RENNES1.FR
kadmin/admin@UNIV-RENNES1.FR
kadmin/changepw@UNIV-RENNES1.FR
kadmin/history@UNIV-RENNES1.FR
kadmin/localhost.localdomain@UNIV-RENNES1.FR
krbtgt/UNIV-RENNES1.FR@UNIV-RENNES1.FR
manager/admin@UNIV-RENNES1.FR
paubry@UNIV-RENNES1.FR
root/admin@UNIV-RENNES1.FR
[root@admin ~]#
```

On pourra écrire un script **/usr/local/bin/kexec** pour exécuter plus facilement les commandes sous **kadmin** :

```
[root@admin ~]# cd /usr/local/bin
[root@admin bin]# cat > kexec
#!/bin/bash
kadmin -p manager/admin -k -t /etc/manager.keytab -q "$*"
[root@admin bin]# chown root.root kexec
[root@admin bin]# chmod 700 kexec
[root@admin bin]#
```

La récupération d'un principal dupont dans la base Kerberos pourra ainsi se faire par :

```
[root@admin bin]# kexec getprinc dupont
Authenticating as principal manager/admin with keytab /etc/manager.keytab.
Principal: dupont@UNIV-RENNES1.FR
Expiration date: [never]
Last password change: Wed Mar 10 12:23:31 CET 2010
Password expiration date: [none]
Maximum ticket life: 1 day 00:00:00
Maximum renewable life: 0 days 00:00:00
Last modified: Wed Mar 10 12:23:31 CET 2010 (cas/admin@UNIV-RENNES1.FR)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 6
Key: vno 1, Triple DES cbc mode with HMAC/sha1, no salt
Key: vno 1, ArcFour with HMAC/md5, no salt
Key: vno 1, DES with HMAC/sha1, no salt
Key: vno 1, DES cbc mode with RSA-MD5, no salt
Key: vno 1, DES cbc mode with CRC-32, Version 4
Key: vno 1, DES cbc mode with CRC-32, AFS version 3
Attributes:
Policy: [none]
[root@admin bin]#
```