Installation d'un serveur KDC Kerberos

Installer les packages requis pour le KDC :

```
dnf install krb5-server krb5-libs krb5-workstation
```

Modifier les fichiers de configuration /etc/krb5.conf et /var/kerberos/krb5kdc/kdc.conf pour refléter le nom de domaine et les mappages de domaine à domaine. Par exemple:

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

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    default_realm = LOCALDOMAIN
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
# EXAMPLE.COM = {
#     kdc = kerberos.example.com
#     admin_server = kerberos.example.com
# }
LOCALDOMAIN = {
     kdc = 127.0.0.1
     admin_server = 127.0.0.1
}
```

Par convention, tous les noms de domaine sont en majuscules et tous les noms d'hôte et noms de domaine DNS sont en minuscules. Les pages de manuel de ces fichiers de configuration contiennent tous les détails sur les formats de fichiers.

Créer la base de données à l'aide de l'utilitaire **kdb5_util**:

```
kdb5_util create -s
```

La commande create crée la base de données qui stocke les clés du domaine Kerberos. L'argument -s

crée un fichier de dissimulation dans lequel la clé du serveur maître est stockée. Si aucun fichier de dissimulation n'est présent pour lire la clé, le serveur Kerberos (krb5kdc) demande à l'utilisateur le mot de passe du serveur maître (qui peut être utilisé pour régénérer la clé) à chaque démarrage.

Le fichier `/var/kerberos/krb5kdc/kadm5.acl` est utilisé par **kadmind** pour déterminer quels principal ont un accès administratif à la base de données Kerberos et leur niveau d'accès. Par exemple:
`*/admin@EXEMPLE.COM *`

La plupart des utilisateurs sont représentés dans la base de données par un seul principal (avec une instance NULL ou vide, telle que joe@EXAMPLE.COM). Dans cette configuration, les utilisateurs avec un deuxième principal avec une instance d'admin (par exemple, joe/admin@EXAMPLE.COM) peuvent exercer un contrôle administratif total sur la base de données Kerberos du domaine.

Après le démarrage de **kadmind** sur le serveur, tout utilisateur peut accéder à ses services en exécutant **kadmin** sur n'importe quel client ou serveur du domaine. Toutefois, seuls les utilisateurs répertoriés dans le fichier kadm5.acl peuvent modifier la base de données de quelque manière que ce soit, à l'exception de la modification de leurs propres mots de passe.

L'utilitaire **kadmin** communique avec le serveur **kadmin** sur le réseau et utilise Kerberos pour gérer l'authentification. Par conséquent, le premier principal doit déjà exister avant de se connecter au serveur sur le réseau pour l'administrer. Créer le premier principal avec la commande **kadmin.local**, qui est spécifiquement conçue pour être utilisée sur le même hôte que le KDC et n'utilise pas Kerberos pour l'authentification:
`kadmin.local -q "addprinc username/admin"`

Démarrer **Kerberos** à l'aide des commandes suivantes :

```
systemctl start krb5kdc.service
systemctl start kadmin.service
```

Ajouter des principal pour les utilisateurs à l'aide de la commande **addprinc** dans **kadmin**. **kadmin** et **kadmin.local** sont des interfaces de ligne de commande vers le **KDC**. Ainsi, de nombreuses commandes, telles que **addprinc**, sont disponibles après le lancement du programme **kadmin**.

Vérifier que le KDC émet des tickets. Tout d'abord, exécuter **kinit** pour obtenir un ticket et le stocker dans un fichier de cache d'informations d'identification. Ensuite, utiliser **klist** pour afficher la liste des informations d'identification dans le cache et utiliser **kdestroy** pour détruire le cache et les informations d'identification qu'il contient.

Par défaut, **kinit** tente de s'authentifier en utilisant le même nom d'utilisateur de connexion au système (pas le serveur Kerberos). Si ce nom d'utilisateur ne correspond pas à un principal dans la base de données Kerberos, **kinit** émet un message d'erreur. Si

cela se produit, il faut fournir à kinit le nom du principal correct en tant qu'argument sur la ligne de commande :

```
kinit principal
```