

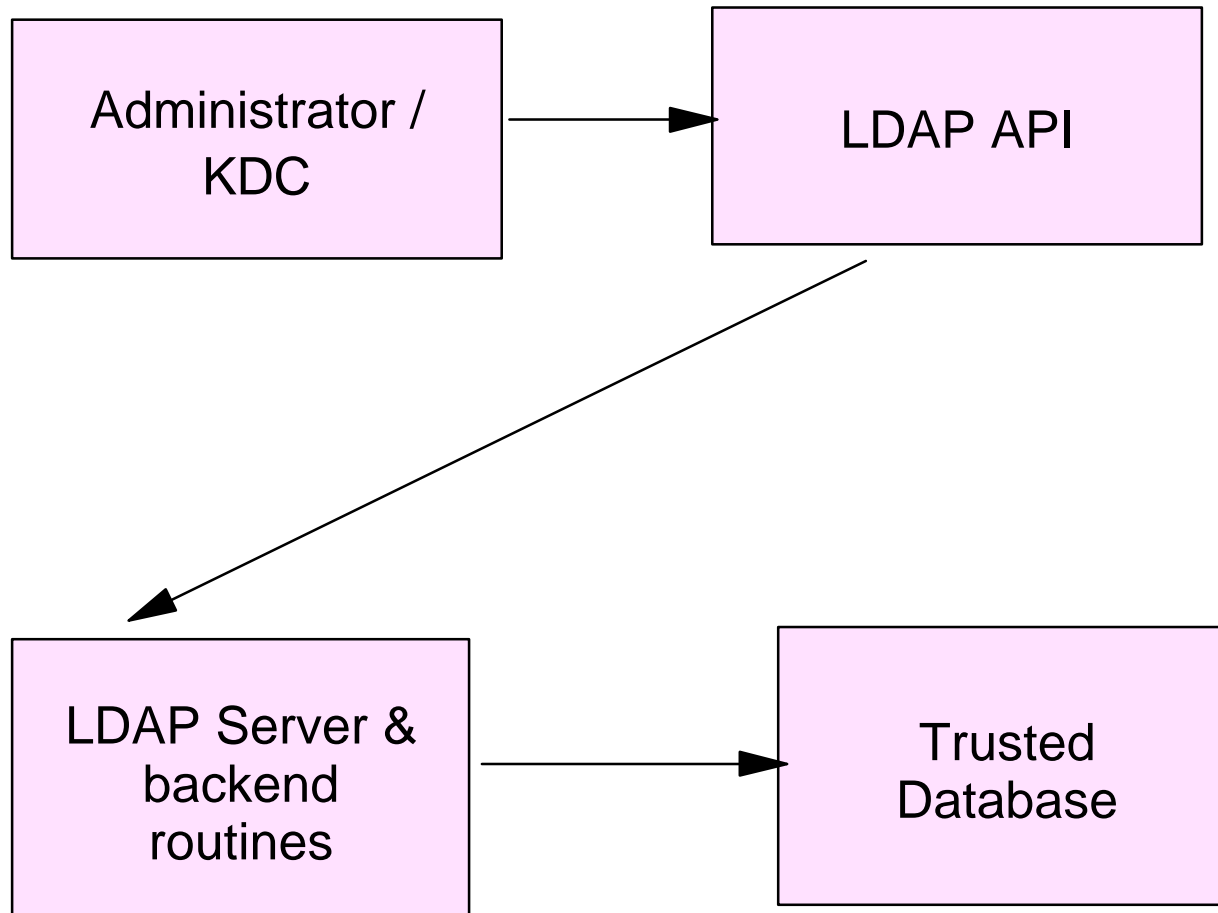
KDC LDAP Schema

Donna Skibbie, IBM

Advantages

- Standard KDC administration API
- Leverage LDAP tools
- Single view of user
- Attribute sharing

Flow of Data to LDAP



Progress

- 3/01: Version 1 of KDC LDAP schema draft submitted to IETF Kerberos working group
- 1/02: Started work on Version 2 of KDC LDAP schema draft and Keys Extension draft
- Plan to submit Version 2 of KDC LDAP schema draft and Keys Extension draft after 3/02 IETF meeting

Current Distribution List for Schema Drafts

- Tolga Acar <tacar@novell.com>
- John Griffith <john.griffith@entegrity.com>
- Timothy Hahn <hahnt@us.ibm.com>
- Paul B. Hill <pbh@mit.edu>
- Wyllys Ingersoll <wyllys.ingersoll@sun.com>
- Leif Johansson <leifj@it.su.se>
- Bob Joslin <bob_joslin@hp.com>
- Sabu Sheffeq <sst@india.hp.com>
- Donna Skibbie <donnas@us.ibm.com>
- Jonathan Trostle <john3725@world.std.com>

Attributes Defined in KDC LDAP Schema Draft

- Realm attributes (other than master keys)
- Principal attributes (other than principal keys)
- Policy attributes

KDC LDAP Schema Draft

```
-----
: any entry :      : realm entry      :      : referenced:
: (required;:      : (required)       :      : entry for :
: could be  :      :                  :      : realm     :
: the realm:<-----:      :----->: policy      :
: entry)    : n    1:      : 1        1 : (optional):
:          :      :      :          :          :
-----
    1::
      ::
        ::
          ::
            n::
----- 1
: principal :----->: (optional) :
: entry     :
: (required) : n      n -----
:          :<----->: associated :
-----
          : entry     :
            : (optional) :
          -----
    1:
      :
    1:
-----
: principal log :
: entry         :
: (optional)    :
:-----:
```

Attributes Defined in Keys Extension Draft

- Master keys
- Principal keys

Master Keys

```
-----  
: realm entry      :  
: as defined in the:  
: KDC LDAP schema :  
:                 :  
:                 :  
:                 :  
-----
```

1:

1:

```
:-----:  
: cn=MKEYS entry  :  
:                 :  
:                 :  
:-----:
```

1:

n:

```
-----  
: master key entry      :  
: (master key value     :  
: is stored in here or  :  
: a referenced URL      :  
: address, such as a file):  
-----
```

Principal Keys: KRBKEY Configuration

```
-----  
: principal          :  
: entry as defined  :  
: in the KDC LDAP   :  
: schema             :  
-----
```

```
    1:  
    :  
    n:
```

```
:-----  
: principal key:  
: entry        :  
:              :  
:-----:
```

Principal Keys: KRBKEY-SUBTREE Configuration

```

-----
: any entry      :
: as defined:
: in KDC        :
: LDAP          :<-----: schema
: schema        : n          1:
:               :
-----
      1::
      ::
      ::
      ::
      ::
      ::
      ::
      ::
      ::
      ::
-----
: principal      :
: entry as       :<-----: entry
: defined in     : 1          n :
: KDC LDAP       :
: schema         :
-----
: realm entry    :
: as defined in  :
: the KDC LDAP   :
: schema         :
:               :
-----
      1:
      1:
      :-----:
      : cn=KEYS entry :
      :               :
      :-----:
      1:
      n:
-----
: principal key referral :
: entry                   :
: defined in              : 1          n :
: KDC LDAP                :
: schema                   :
-----

```

Principal Keys: USERPASSWORD Configuration

```
-----  
: principal           :  
: entry as defined   :  
: in the KDC LDAP    :  
: schema with        :  
: userPassword       :  
: attribute from     :  
: RFC 2256           :  
-----
```

Principal Keys: AUTHPASSWORD Configuration

```
-----  
: principal           :  
: entry as defined   :  
: in the KDC LDAP    :  
: schema with        :  
: authPassword       :  
: attribute from     :  
: RFC 3112           :  
-----
```

For More Information

- Donna Skibbie, donnas@us.ibm.com