SSSD DNS Improvements in AD Environment

Lukáš Slebodník

2014-March-12

Content

- Preconditions and assumed setup
- **Dynamic DNS updates**
- **DNS site discovery**
- Troubleshooting

Preconditions and assumed setup

- features are implemented in sssd 1.11
- covers only sssd configuration.
- expects configured Active Directory with DNS server
- sssd must be joined to Active Directory. The easiest way is to use realmd
- `id_provider = ad must` be used in configuration

Dynamic DNS updates

Dynamic DNS updates content

- DNS aging and scavenging
- Client DNS updates
- DNS updates in SSSD
- Configuration in SSSD

Dynamic DNS updates

Situation:

- clients frequently move or change locations
- DHCP to obtain an IP address

Problem:

- to reduce the need for manual administration of zone records

Solution:

- RFC 2136 "Dynamic Updates in the Domain Name System."

DNS aging and scavenging

- mechanism for performing cleanup and removal of stale resource records, which accumulate in zone data over time.
- is disabled by default on AD Server
- http://technet.microsoft.com/en-us/library/cc759204(v=ws.10).aspx

Client DNS updates

SSSD:

- simulates the behavior of Windows AD clients
- keeps the address record from being removed using periodical updates
- updates the DNS record if IP address is changed
- authenticates to the DNS with gss-tsig

DNS updates in SSSD

Dynamic DNS update is performed when:

- the sssd back end becomes on-line
  - cover the case when computer is restarted
  - used for roaming users
- periodically
  - used to prevent scavenging

Configuration in SSSD 1/2

Options in domain section and default values in AD provider

`dyndns_update`

- enables automatic DNS updates in Active Directory DNS server with IP address of sssd client.
- enabled by default

`dyndns_ttl`

- TTL to apply to the client DNS record when updating it
- default is 3600 seconds (1 hour)

`dyndns_iface`

- network interface whose IP will be used for dynamic DNS update
- automatically detected

Configuration in SSSD 2/2

`dyndns_refresh_interval`

- time between two periodical updates
- default is 86400 (24 hours)

`dyndns_update_ptr`

- whether PTR records should be updated for the client
- enabled by default

`dyndns_force_tcp`

- whether TCP protocol should be used for comunication with the DNS server.
- disabled by default (nsupdate will choose the protocol itself)

DNS site discovery

DNS site discovery content

- Terminology
- Clients
- DNS site discovery in SSSD
- Configuration in SSSD

DNS site discovery

Situation:

Large enterprise environment has more than one domain controller. Some of them are used for redundancy, others for different administrative domains. Environments with multiple physical locations have at least one local domain controller.

Problem:

- reduce latency
- decrease network load

Solution:

- find the local or the nearest domain controller

Terminology

Sites:

- represent the physical structure or topology of network
- can be seen as physical location with unique name

Domains:

- represent the logical or administrative structure of organization

Sites and domains are two independent abstractions.

http://technet.microsoft.com/en-us/library/cc782048%28v=ws.10%29.aspx

Clients

- can change physical location (roaming users)
- have to find out which site they belong to
  - must be done dynamically
- try to find the needed services (LDAP, kerberos) in the local site
- fall back into the whole domain

DNS site discovery in SSSD

1) DNS lookup to find any DC in domain

```
_ldap._tcp.<DnsDomain>
```

2) CLDAP ping to the found DC to get the desirable site

3) DNS lookup to find SRV in the site

```
_<service>._<protocol>.<SiteName>._sites.<DnsDomain>
```

4) DNS lookup to find global SRV records

```
_<service>._<protocol>.<DnsDomain>
```

Configuration in SSSD

Option in domain section

`ad_enable_dns_sites`

- whether DNS site discovery should be used with Active Directory
- enabled by default

Troubleshooting

- check opened connection of SSSD
  - lsof -iTCP -a -c sssd_be
- enable verbose logging in the domain section and analyze log file
- analyze DNS network traffic
  - tcpdump
  - wireshark

freeIPA

identity | policy | audit