FreeIPA Client and Server

Improvements in version 3.0

Rob Crittenden & Martin Kosek

01-14-2013
Client Improvements

- Tool to configure automount client
  - `ipa-client-automount --location=LOCATION`
- Easier configuration of secure NFS mounts with Kerberos authentication
- Can be targeted on the chosen automount *location*, e.g. geographically close location (set *manually*)
- NFS share on server still needs to be configured *manually*
Client improvements, con't

• New enhanced static configuration of IPA servers
  • Useful in IPA+AD environment, if custom IPA DNS cannot be used
• FreeIPA 2.2 and older:
  • SSSD always used domain SRV records (IPA+AD!)
• FreeIPA 3.0 and Fedora 18:
  • Use --fixed-primary and --server options to define static list of IPA servers
  • SRV record autodiscovery is still available (and preferred option for client failover)
# New client autodiscovery process

<table>
<thead>
<tr>
<th>ipa-client-install options</th>
<th>sssd.conf's ipa_server</th>
<th>krb5.conf's dns_lookup_realm dns_lookup_kdc</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>no options</em></td>
<td><em>srv</em>, srv1</td>
<td>true, true</td>
<td>Discovery via client parent domain(s) SRV records</td>
</tr>
<tr>
<td>--domain=$DOMAIN</td>
<td><em>srv</em>, srv1</td>
<td>true, true</td>
<td>Discovery via specified domain SRV records</td>
</tr>
<tr>
<td>--server=$SERVER --domain=$DOMAIN</td>
<td><em>srv</em>, $SERVER</td>
<td>false, false; KDC fixed to $SERVER</td>
<td>Not recommended - <strong>no failover</strong></td>
</tr>
<tr>
<td>--server=$SERVER --domain=$DOMAIN --fixed-primary</td>
<td>$SERVER</td>
<td>false, false; KDC fixed to $SERVER</td>
<td>Not recommended - <strong>no SRV discovery, no failover</strong></td>
</tr>
<tr>
<td>--server=$SERVER1 --server=$SERVER2 --domain=$DOMAIN --fixed-primary</td>
<td>$SERVER1,$SERVER2</td>
<td>false, false; KDC fixed to $SERVER1, $SERVER2</td>
<td><strong>Failover in a static list of replicas</strong>. Replica lists need to be updated manually</td>
</tr>
</tbody>
</table>

**Notes:**

- **srv1**: First record returned by DNS SRV record search. Used as a fallback in case of broken domain SRV records (_srv_) 
- --fixed-primary and multiple servers with --server option was introduced in FreeIPA 3.0
Core Server Improvements

- The last administrator cannot be removed or disabled
- Stabilization of migration process
  - Set basedn of remote LDAP server
  - Don't create user-private groups in IPA
  - Properly handle migrated DN attributes such as manager and secretary
- Improvements to schema upgrade process
  - Safer updates of objectClasses and attributeTypes
  - Only new or modified indices are being updated
    - Significantly faster LDAP update process
- Set the e-mail attribute on new users by default
Core Server Improvements, con't

- Man page improvements and fixes
- `ipausers` group is non-POSIX on new installs
  - Large `ipausers` group affects SSSD performance
  - Affects only new IPA installations
- SUDO rule name uniqueness is now enforced
DNS interface improvements

- Introduce *per-domain permissions*
  - Read&write access can be assigned to one zone only
  - Use `dnszone-add-permission $ZONE` to create a new system permission 'Manage DNS zone $ZONE'
- DNS persistent search enabled by default
- SOA serial number is automatically incremented when any record is changed
  - Required for DNS zone transfer ability
  - SOA serial number now defaults to unix timestamp
  - SOA serial number is not synchronized between replicas to avoid replication issues
Directory Server integration improvements

- Support for 389-ds-base 1.2.11
- Internal change to LDAP Distinguished Name handling
  - More robust handling of DN and special characters in the DN
- Use new 389-ds-base winsync POSIX plugin
  - AD POSIX attributes can now be synced with IPA
- Expanded Referential Integrity checks
  - Affects referential attributes (hosts, SUDO, HBAC rule)
  - These objects should no longer have attributes pointing to non-existent or moved LDAP entry
Certificate Server Improvements

- Support for the Dogtag CA version 9
- Move CRL publish directory to IPA owned directory
  - New directory: /var/lib/ipa/pki-ca/publish/
- Single CRL generator
  - Only one IPA+CA is generating the CRL to avoid inconsistent CRLs and their serials
  - The initial server with a CA is configured to be the generator of the CRL, replica CAs do not generate CRL
  - The CRL is available on all masters at the same URL:
    - https://ipa.example.com/ipa/crl/MasterCRL.bin
CA subsystem certificate renewal

- Orchestrated by `certmonger` component
  - Renew operation performed by master CA server
    - The first installed CA by default is the CA master
    - Renewal configured both for new deployments and upgraded IPA CA masters
  - Renewed certificates placed in `cn=ca_renewal,cn=ipa,cn=etc,$SUFXIX`
    - Certificate nickname is the RDN
- `certmonger` on clone CAs watch for updated certificates and updates when available
- IPA specific actions performed by `pre/post renew scripts` in `/usr/lib(64)/ipa/certmonger/`
CA subsystem certificate renewal, con't

- Renewed certificates by CA master:
  - auditSigningCert, ocspSigningCert, subsystemCert, Server-Cert (tomcat), ipaCert
    - ipaCert (agent cert) in /etc/httpd/alias is a special case, agent entry in dogtag LDAP instance needs to be updated
  - Server-Cert for httpd, pki-ca and dirsrv services are still being renewed on each master separately
- Write access to NSS database had to be serialized to avoid database corruption caused by multiple writers
  - pki-ca is stopped before the renew transaction and started afterwards
Replication management improvements

- Run the CLEANALLRUV task when deleting a replication agreement
  - Removes replication meta-data about removed master
  - Introduces a set of related commands:
    - list-ruv, clean-ruv, abort-clean-ruv, list-clean-ruv
  - See ipa-replica-manage man page for details
- Try to prevent orphaning other servers when deleting a master
- memberOf is replicated during initial replication, otherwise calculated on each server
Performance improvements

- Sessions for command-line users
  - Uses key management facility in kernel to store the session ID (list with 'keyctl list @s')
  - Subsequent authentications are faster
- Improve LDAP query performance by adding missing indices
  - Affects automount, SUDO, HBAC and other queries
- Exclude some attributes from replication
  - nsds5ReplicaStripAttrs replication agreement is configured (modification name/timestamp attributes)
  - Avoids empty replication events in some cases
UI Improvements

- New Firefox extension for configuring the browser
  - Firefox 15 deprecated the interface used to set the Kerberos negotiation directives (about:config)
  - Older Firefox versions can use the old interface
- Better support for Internet Explorer 9
- Notify success on add, delete and update events
- Introduced action panels (e.g. Reset password)
- Warn user when password is about to expire
- Forms-based password reset
  - Automatically offered for users with expired password