What’s new in FreeIPA 4.9

Alexander Bokovoy

Red Hat
• FreeIPA core developer
• Engineer at Red Hat
• Identity management solution:
  • provides centralized infrastructure to manage POSIX identities across a fleet of Linux machines
  • combines together 389-ds LDAP server, MIT Kerberos, BIND DNS server, SSSD, Samba, and Python-based management tools
  • often seen as ‘Active Directory for Linux’ but this is not exactly correct comparison
  • Depends on a lot of OS components working together, can be used as a canary to detect breakage in many packages
FreeIPA and RHEL IdM

• RHEL IdM
  • a version of FreeIPA in Red Hat Enterprise Linux (RHEL)
  • supported by Red Hat support as a part of RHEL subscription
  • RHEL 7: FreeIPA 4.6.x, Python 2-based
  • RHEL 8: FreeIPA 4.8/4.9, Python 3-based
  • mostly rebranded but has few functional differences to FreeIPA
    • or had before FreeIPA 4.9 release …
  • CentOS:
    • debranded but otherwise should be equal to RHEL IdM functionally
FreeIPA 4.9 series

- FreeIPA 4.9.0 released on December 23rd, 2020
- about 370 bug fixes over FreeIPA 4.8.10
- Release cadence of 6-8 weeks
- 4.9.3 released on March 31st, 2021
  - ~80 bug-fixes over 4.9.0
- available in CentOS Stream:
  - CentOS 8 Stream since January 2021
  - CentOS 9 Stream since April 2021
Major themes for FreeIPA 4.9

• password management improvements
• group membership management
• ACME CA support
• FIPS mode operations
• Active Directory integration enhancements
• Kerberos-related improvements
• DNS infrastructure improvements
Password management improvements
Password policies

- **libpwquality support**
  - reuse of a user name
  - dictionary words using a cracklib package
  - numbers and symbols replacement
  - repeating characters in the passwords
Expiring Password Notification

- a standalone tool, `ipa-epn`
- available since FreeIPA 4.8.7
- allows determining list of users whose passwords are about to expire
- can send e-mail notifications to users
Password policies for system accounts

• system account
  • typically is not a Kerberos principal
  • located in cn=sysaccounts,cn=etc,$SUFFIX
  • used to interate 3rd-party software with FreeIPA LDAP server
• system accounts can now have non-expiring Kerberos keys
• Password authentication and validation
  • LDAP: set and synchronized with Kerberos keys
  • Kerberos: set and synchronized with LDAP password
• LDAP password wasn’t limited
• MIT Kerberos hard-codes password length to 1024 characters and there is no way to distinguish a cutoff and 1024-character passwords
• passwords now limited to 1000 characters everywhere
Group membership management
Fedora Accounts integration

- Group sponsors
  - ability to add users to a specific group only
  - `ipa group-[add|remove]-member-manager`
Group membership extensions

• Groups as access control aggregators
  • permission, privilege, role
    • permissions define access controls
    • privilege collects permissions
    • roles grant access to privileges

• Kerberos services
  • role members since 4.2
  • group members since 4.7.0

• ID user overrides since 4.8.7
  • role members
  • group members
ACME CA support
• Dogtag PKI supports ACME protocol (RFC 8555) since v10.10
• ACME support deployed automatically on all CA servers
  • not enabled by default
• accessible through ipa-ca.$DOMAIN end-point
• implements dns-01 and http-01 challenges
• works and tested against
  • certbot
  • mod_md
• known to not work with cert-manager
  • incorrect implementation of RFC 8555
  • cert-manager issue 3777
FIPS mode operations
Crypto policies

- FreeIPA obeys system-wide crypto policies
- Fedora 32+ and RHEL 8.3+ disable unsafe ciphers
  - TLS but also Kerberos
  - RC4-HMAC is required for interoperability with Active Directory
- AD-SUPPORT crypto sub-policy enables RC4-HMAC in Kerberos
  - update-crypto-policy --set DEFAULT:AD-SUPPORT
FIPS mode

• FreelPA 4.9.1+ can be operated in FIPS mode
  • only AES ciphers will be enabled
  • Trust to Active Directory will only use AES keys
    • shared secret trust is not supported
• Samba in RHEL 8.4+ can be operated in FIPS mode
  • only Kerberos authentication, no NTLMSSP support
  • only part of RHEL IdM or a member of AD domain
  • no SMB1 support
Active Directory integration enhancements
Manage IPA resources as Active Directory user

- AD users can manage IPA resources
  - create ID user override
  - add ID user override to IPA group
  - apply permission/privilege/role to a group
- Available in RHEL 8 through an external plugin
  - Merged to FreeIPA upstream and released in 4.9.0
**SUDO improvements**

- SUDO rules now can reference AD users and groups
  - allows avoiding non-POSIX/POSIX group dance
  - requires SSSD 2.4+ version (RHEL 8.4)
- AD user references supported in
  - `ipa sudorule-[add|remove]-user`
  - `ipa sudorule-[add|remove]-[runasuser|runasgroup]`
Samba integration improvements

- Samba file server
  - `ipa-client-samba` to set up Samba file server on IPA client
  - works for IPA users and users from trusted Active Directory domains
  - uses SSSD/Samba integration

- SMB user properties can be updated in IPA Web UI
- Available since RHEL 8.2, few fixes in FreeIPA 4.9
Kerberos improvements
Compatibility with Active Directory

• MS-PAC record in Kerberos tickets
  • IPA KDC issued tickets look closer to what Active Directory does
  • Adds asserted identity SIDs:
    • S-1-18-1 is a SID for an Authentication Authority Asserted Identity
    • S-1-18-2 is a SID for a Service Asserted Identity
Compatibility with Active Directory

- S4U2Self / S4U2Proxy support
  - closer to Active Directory behavior
  - enables complex workflow with MS SQL server
  - allows setting up S4U2Self services on IPA clients
Kerberos authentication to PAM services

- SSSD 2.4: new PAM module, pam_sss_gss.so
  - allows authenticating with Kerberos ticket to PAM
  - authentication indicators support
    - e.g. SUDO access only to Kerberos tickets obtained with smart-cards, not passwords
DNS improvements
DNS improvements

- systemd-resolved support
  - Fedora 34+
  - automatic enablement of IPA DNS server lookup on IPA server
- bind-dyndb-ldap LDAP module now supports BIND 9.16+
- enables native PKCS#11 support
  - could work with OpenSSL engines
- migrated to OpenDNSSEC v2
Performance improvements
Performance improvements

- LDAP caching layer in IPA API
  - ~30% performance boost for complex API calls
  - part of FreeIPA 4.9.4 (to be released)
- Better LDAP indexing
  - faster Kerberos KDC responses
What is ahead?
SUBID support

• Centralized management of user namespaces on Linux
  • new `shadow-utils` support for plugins in ‘libssubj’
  • needs new SSSD code to support IPA subid records
Two-way trust

- Global catalog support
  - allows login to Windows systems from Active Directory
  - enables two-way trust between two separate IPA deployments
External identity providers

• Authenticate against OAuth2 identity provider for IPA users
  • login with your IdP and get a Kerberos ticket on IPA clients
• Transparent integration with Keycloak / RH SSO
Thanks!