Identity Management in Red Hat Enterprise Linux

State of the Union

Thorsten Scherf
Sr. Principal Product Operations Engineer

Identity Management & Platform Security
Red Hat

About me

- 22 years @ Red Hat
- Working in Product Operations for Identity Management & Platform Security
- Focused on delivering data-driven recommendations that connect customer opportunities to the Engineering backlog

The Identity Challenge

- Local accounts on every server
- No central policy for access control or sudo rules
  - Inconsistent, unauditable
- Manual provisioning
  - Slow and error-prone
- No single audit trail across Linux infrastructure

What is RHEL IdM?

- FreeIPA upstream, Identity Managment (IdM) in RHEL
- Kerberos SSO
  - Single-Sign-On across all Linux hosts in your environment
- Access Control
  - Host-based access control (HBAC) and centralized sudo policies
- Certificate Authority (PKI)
  - Built in Dogtag Certificate Authority for automated certificate management
- **Think Active Directory for Linux**

Core Features

- Identity Store
  - LDAP
  - Users, Groups, Hosts, Services
- Authentication
  - Kerberos
  - Passwords, 2FA (Smart Cards, OTP soft/hardtokens, Passkeys)
  - X.509 certificates (PKI)
  - Single Sign On (SSO)
  - Multi-Factor Authentication
- Authorization
  - Host access rules
  - Kerberos Authentication Indicator
  - IdM RBAC - user roles and admin delegations
- Security-related service management
  - SUDO, SELinux, SSH-Keys
  - Secrets (passwords, keytabs, certificates)

Server setup

```
# ipa-server-install
```

- Directory server (dirsrv)
- Kerberos server (krb5kdc, kadmin)
- Certificate server (pki-tomcatd)
- HTTP server (httpd)
- DNS server (named)
- KRA (Key Recovery Authority) server
- Time synchronization (chronyd)
- OTPD configuration (ipa-otpd)
- Active Directory trust configuration (smb, winbind)
- Identity Provider configuration (ipa-otpd)

Client setup

```
# ipa-client-install
```

- Domain discovery and validation of parameters
- Time synchronization (ntp, chrony)
- IPA enrollment (Creation of host entry and keytab)
- SSSD, PAM, NSS configuration
- Kerberos client configuration
- PKI configuration
- DNS configuration

Active Directory integration

- AD / IdM both provide Kerberos realm
  - Cross-Forest Trust
    - Individual domains can be excluded
  - External Trust
    - Single domain trust
  - Linux-Native Policies
    - AD as an identity source, IdM as source for policies
  - SSSD Client
    - System Security Services Daemon provides consistent AD integration

External Identity Providers and OAuth2

- Extend IdM authentication to cloud identity providers and modern protocols
  - OAuth2/OIDC
    - Authenticate to Linux hosts using OAuth 2.0 tokens from external IdP
  - Entra ID
    - Integrate with Microsoft Entra ID for cloud native Identity Federation
  - Keycloak
    - Integrate with Red Hat Build of Keycloak for advanced SSO , social login and identity brokering
  - Other OAuth based IdPs that support Device Authorization Grant (rfc8628)

Zero Trust Foundations

- Authentication
  - Kerberos ensures every access is authenticated and authorized. OTP, Passkeys and Smart Cards enforce strong authentication at every boundary
- Authorization
  - HBAC + sudo + SELinux for fine grained, host-level access control
- Compliance
  - Centralized audit logging and policy enforcement across all hosts
- Encrypted DNS
  - DNS over HTTPS (DoH)
  - DNS over TLS (DoT)
  - NetworkManager, dnsconfd, local resolver

Integrations & Ecosystem

- Ansible Automation
  - ansible-freeipa collection for automated IdM deployements
- OpenShift
  - Identity Services to containerized workloads running in OCP
- Satellite
  - Automated host enrollment and certificate provisioning through Satellite
- RHEL System Roles
  - Declaritive system roles for consistent IdM deployments

Feature Roadmap

- Modern Web UI
  - Redesigned WebUI for improved usability
- OAuth2 Endpoint
  - Native OAuth2/OIDC endpoint for token-based authentication
  - OCP Workload Identity Support
- Post-Quantum Crypto
  - PQC algorithms support across all relevant IdM components
- IdM/IdM Trust
  - Cross-domain trust between separate IdM deployments
- IdM as Appliance
  - Simplified deployment as a pre-configured virtual appliance

Questions?

tscherf@redhat.com