PRESENTED BY RED HAT

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.

www.theredhatsummit.com

Red Hat Enterprise Identity (IPA)

Centralized Management of Identities & Authentication

Dmitri Pal

Sr. Engineering Manager, Red Hat Inc.

Robert Crittenden

Sr. Engineer, Red Hat Inc.

05/06/11

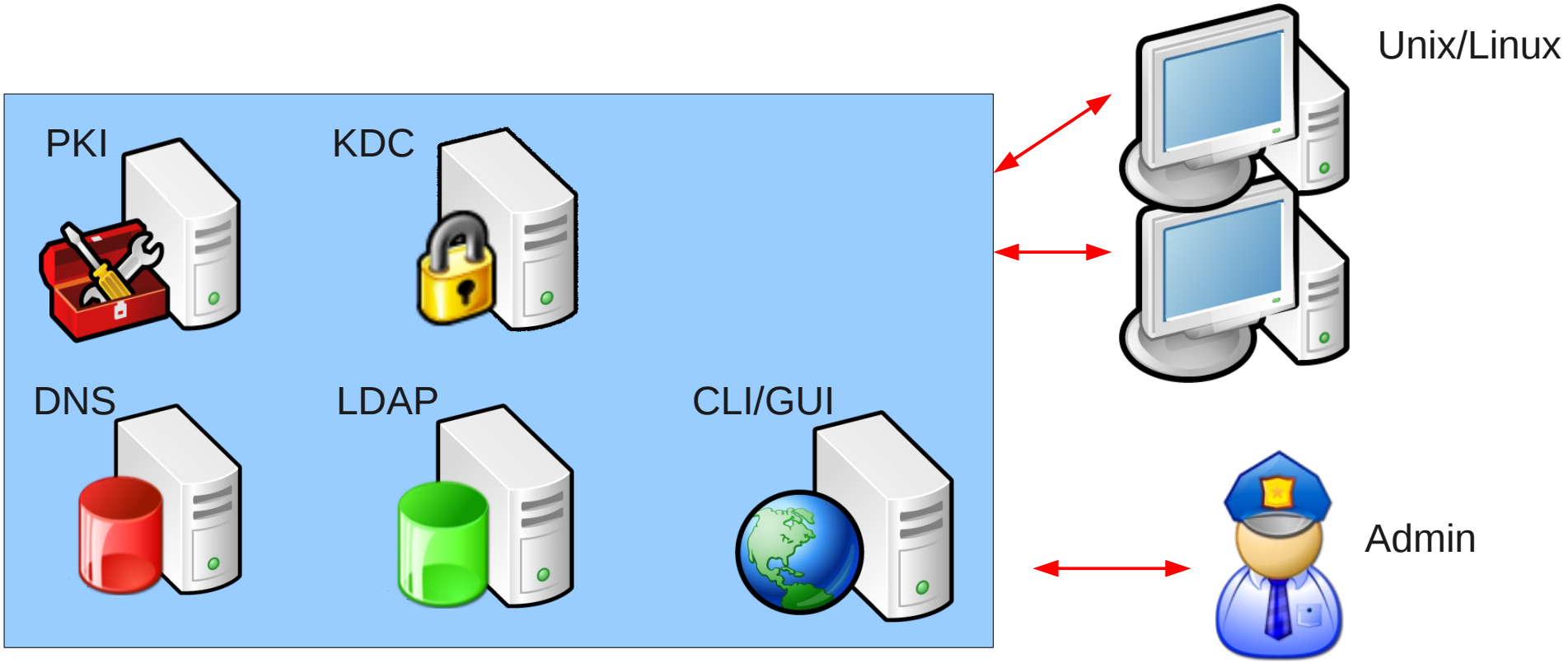
Agenda

- What is IPA?
- Main values
- Architecture
- Features
- Direction
- Roadmap
- Resources

What is IPA?

- IPA stands for Identity, Policy, Audit
  - FreeIPA upstream project was started in 2007
  - FreeIPA v1 was released in 2008
  - Since then worked on the version 2 that was released in late March 2011
- IPA is a domain controller for Linux/UNIX environment
  - Think Active Directory but for Linux
  - Central server that stores identity information, policies related to identities and performs authentication

High Level Architecture



Why IPA?

- Identity and authentication is a complex problem – many disjoint technologies exist
- We want to make it more simple to deploy and use
- With the growth of the Linux share of servers in the enterprises there should be a server that has needs of Linux clients in its heart

Why IPA? (continued)

- Cloud based deployments require even more security:
  - Flexible identity and policy management
  - Authentication and single sign on
  - Certificate and key provisioning and rotation

Features

- Centralized authentication via Kerberos or LDAP
- Identity management:
  - users, groups, hosts, host groups, netgroups, services
  - Integrated identities
- Manageability:
  - Pluggable and extensible framework for UI/CLI
  - Rich CLI and web-based user interface
  - Simple installation scripts for server and client
  - Flexible delegation and administrative model

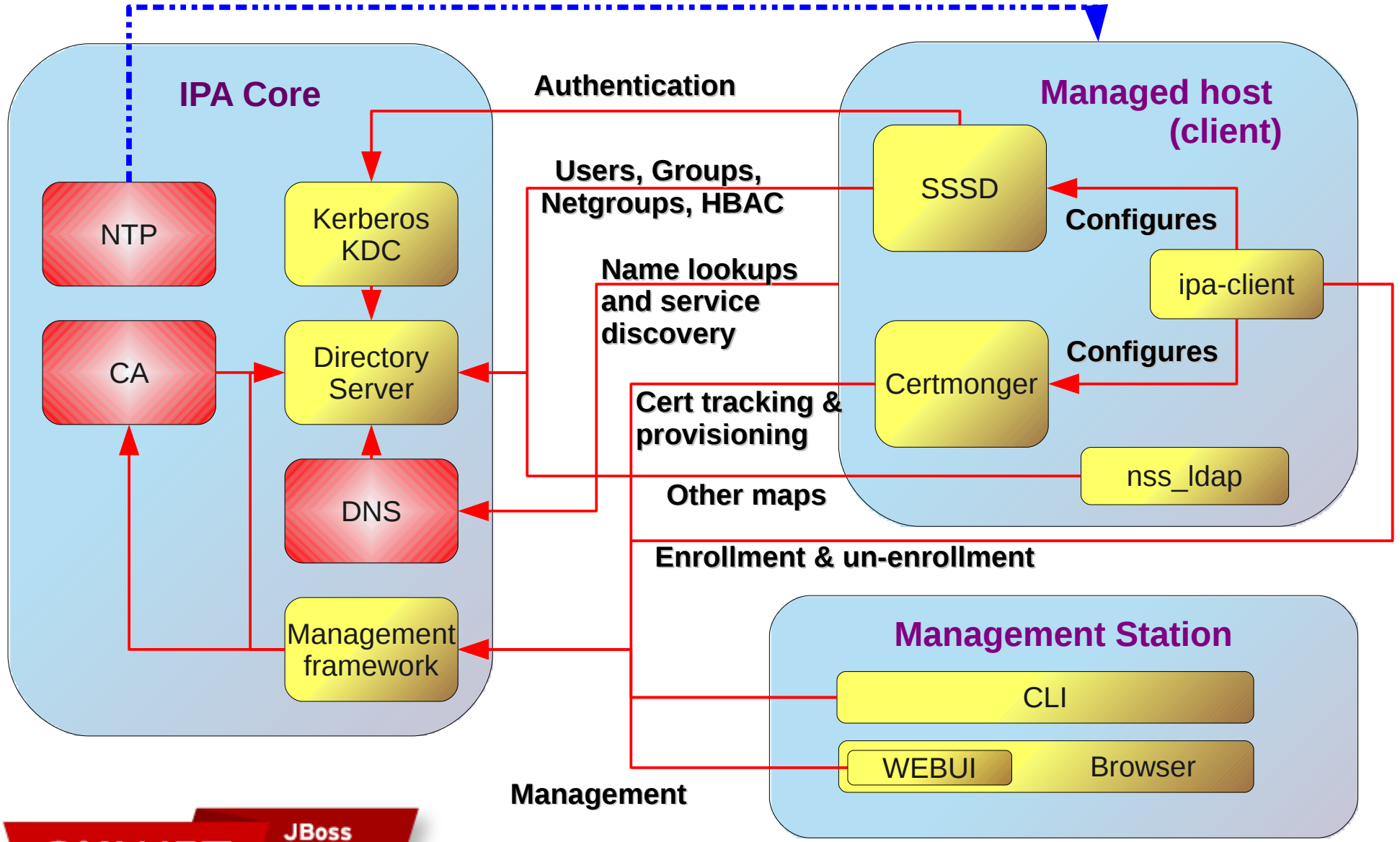
Features (Continued)

- Certificate provisioning for hosts and services
- Serving sets of automount maps to different clients
- Advanced features:
  - Host-based access control
  - Centrally-managed SUDO
  - Group-based password policies
  - Automatic management of private groups
  - Can act as NIS server for legacy systems
  - Painless password migration

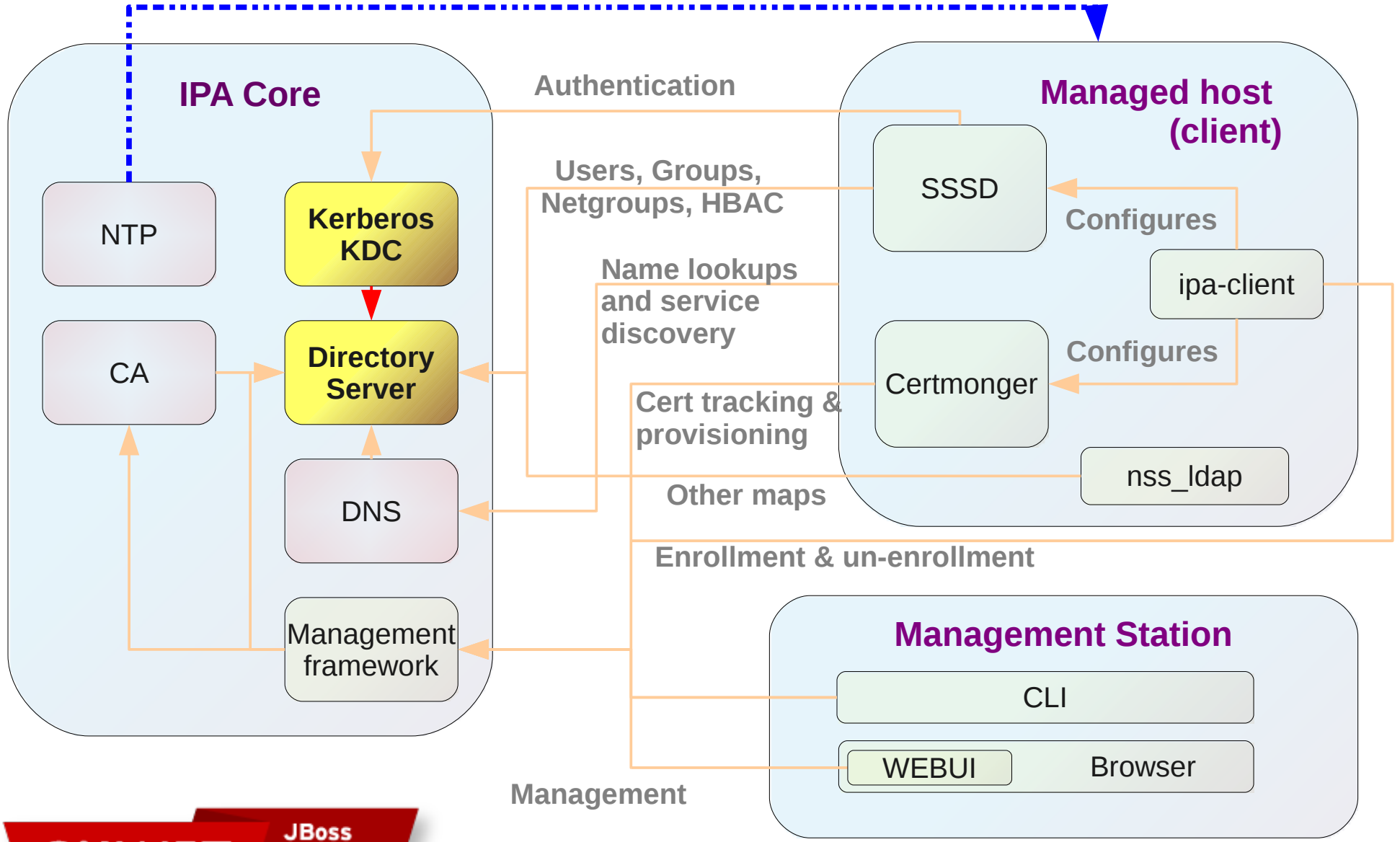
Features (Continued)

- Optional integrated DNS server managed by IPA
- Replication:
  - Supports multi-server deployment based on the multi-master replication
  - User replication with MS Active Directory
- Compatibility with broad set of clients

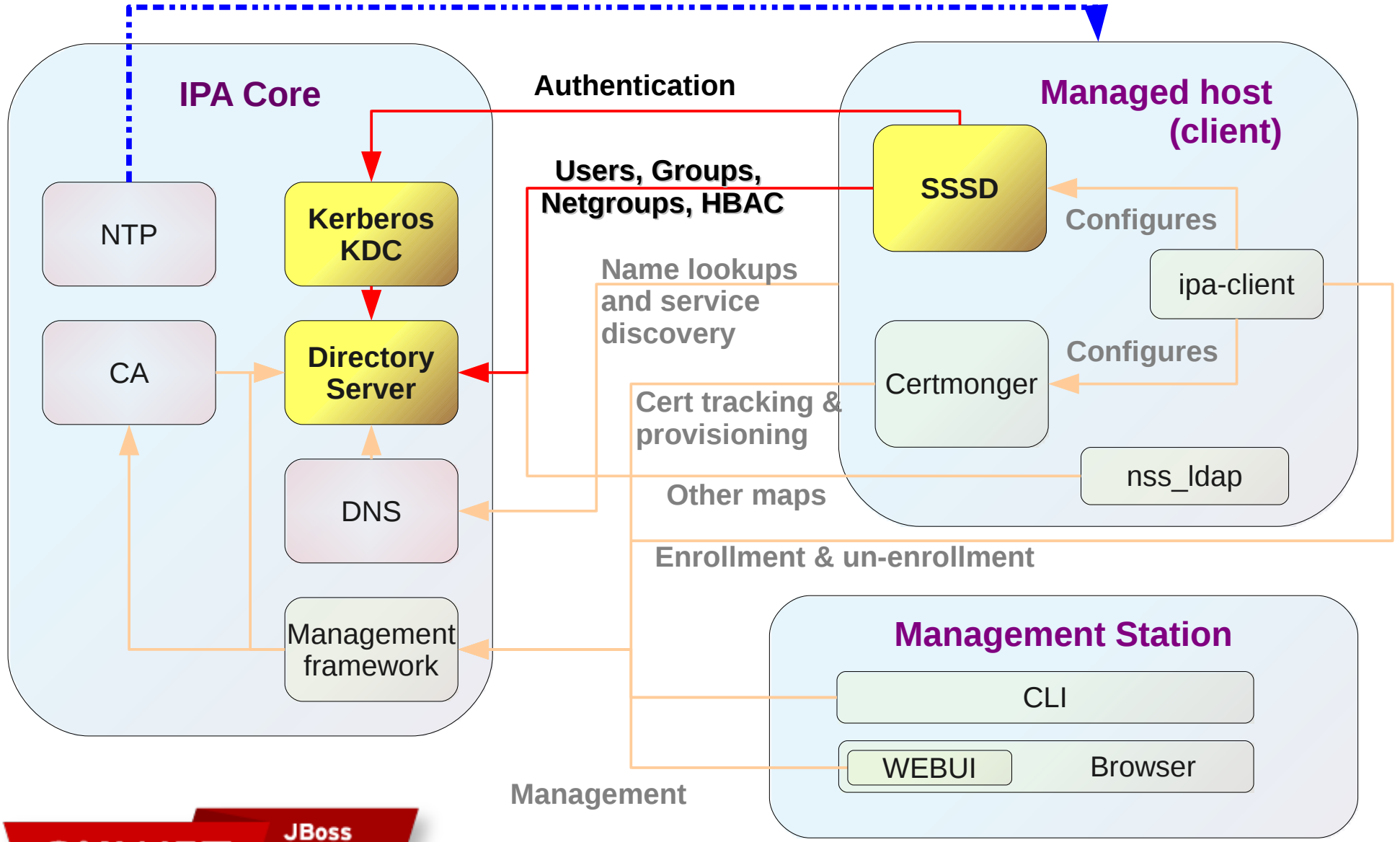
Under the Hood



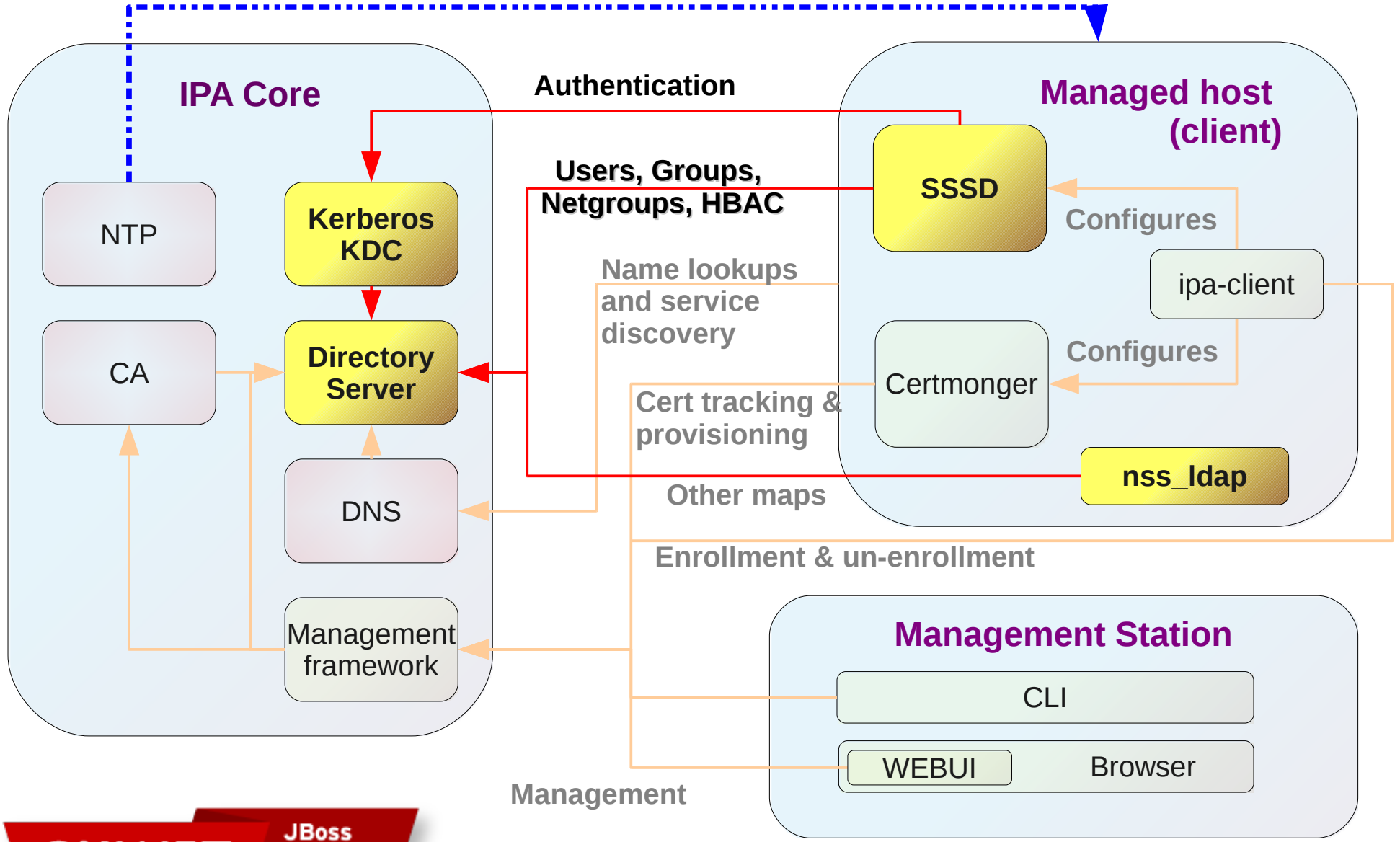
Under the Hood



Under the Hood



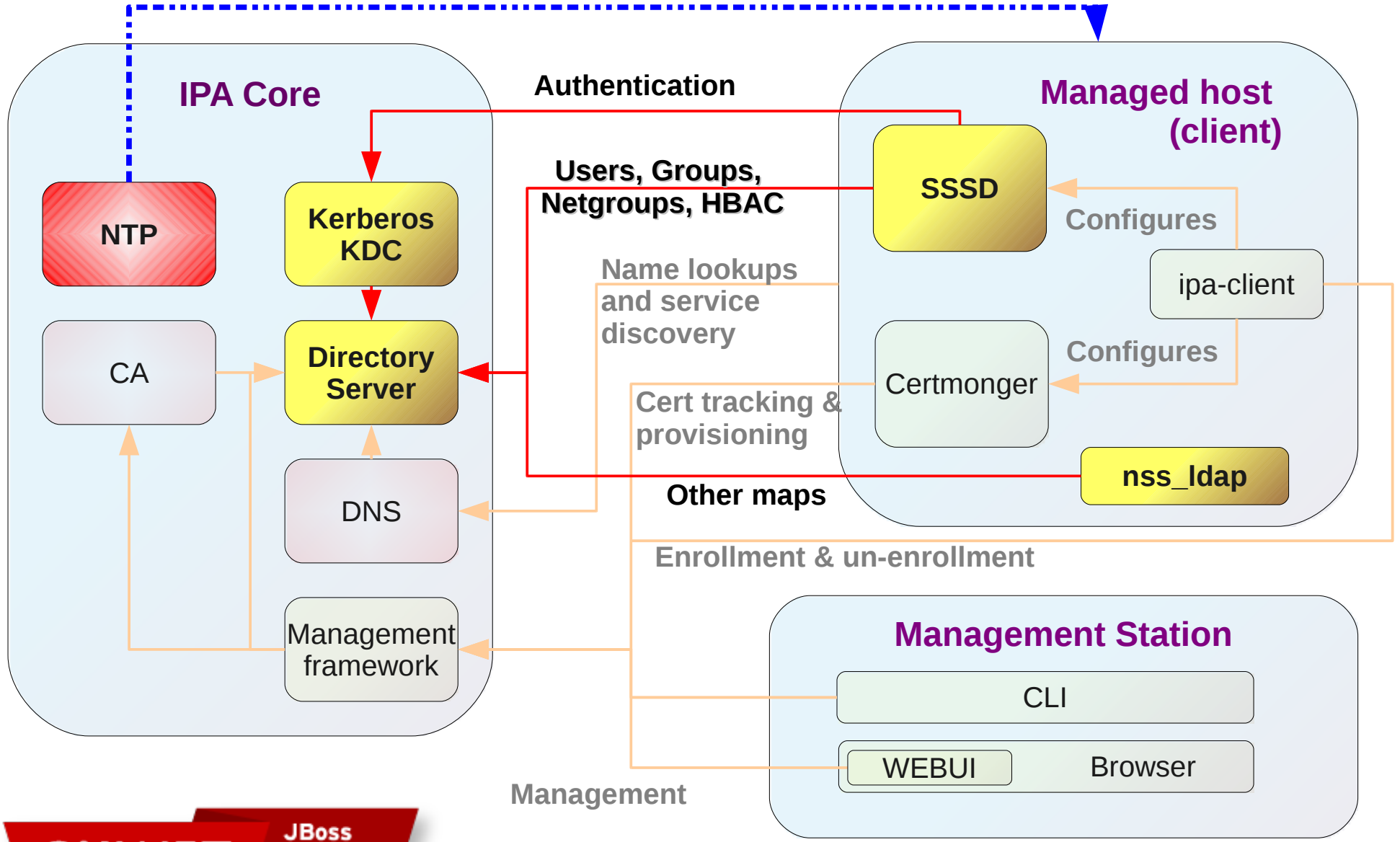
Under the Hood



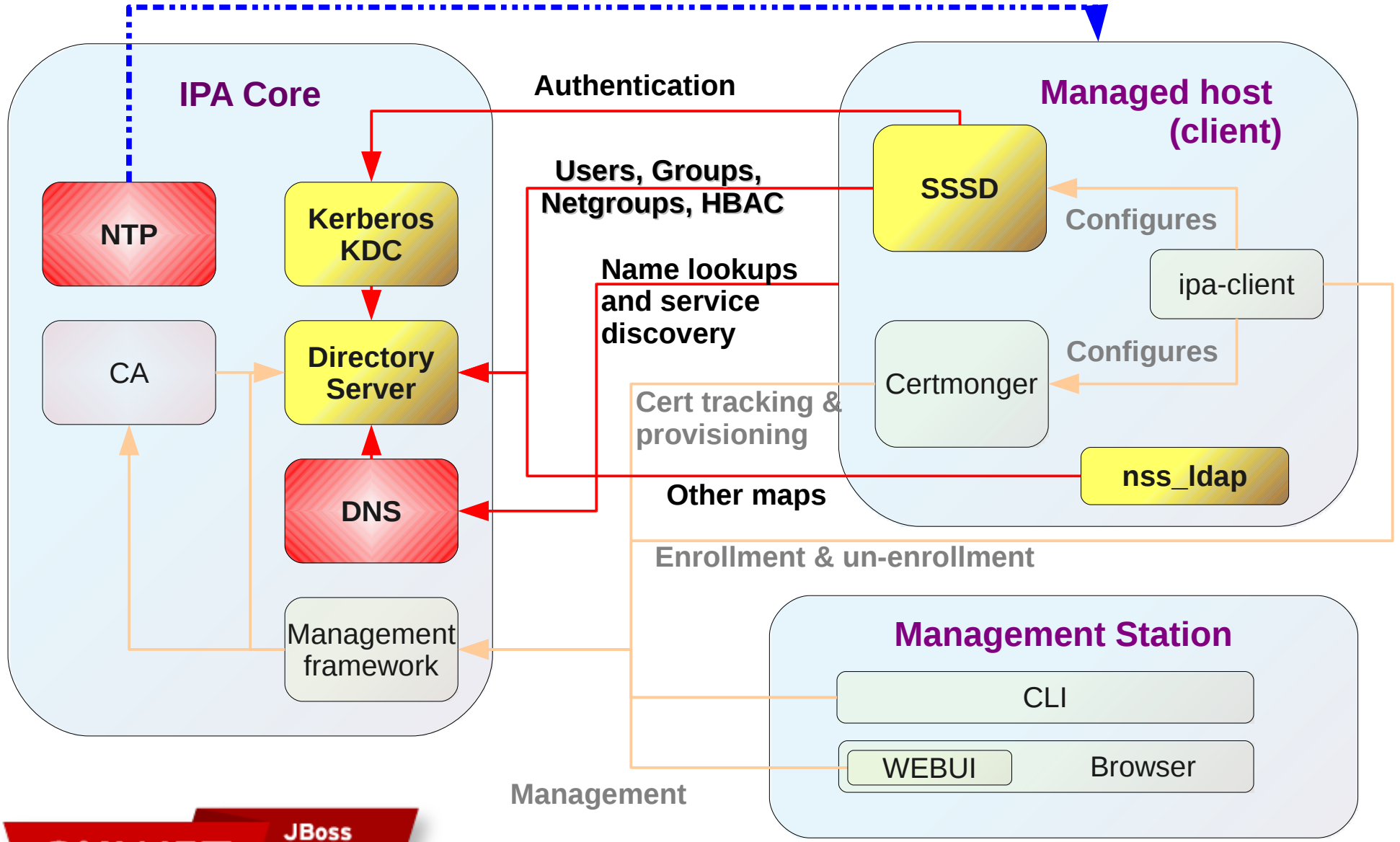
Client Configurations

- SSSD
  - With IPA back end
  - LDAP or Proxy for identity
  - Kerberos or LDAP for authentication
  - nss_ldap for other maps
  - nscd only for those maps
- Non-SSSD
  - LDAP (nss_ldap) or NIS (nss_nis) for identity
  - LDAP (pam_ldap) or Kerberos (pam_krb5) for auth

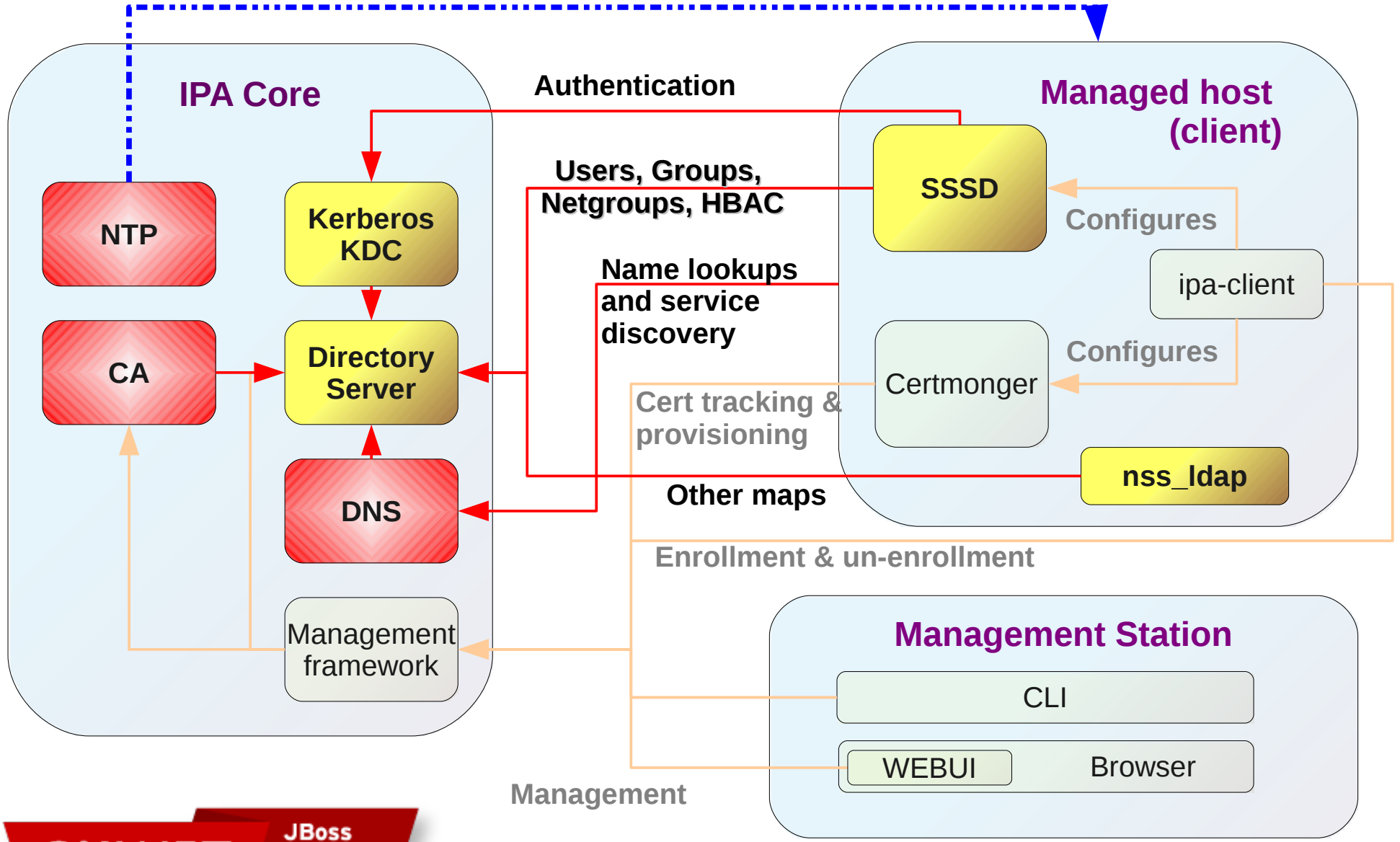
Under the Hood



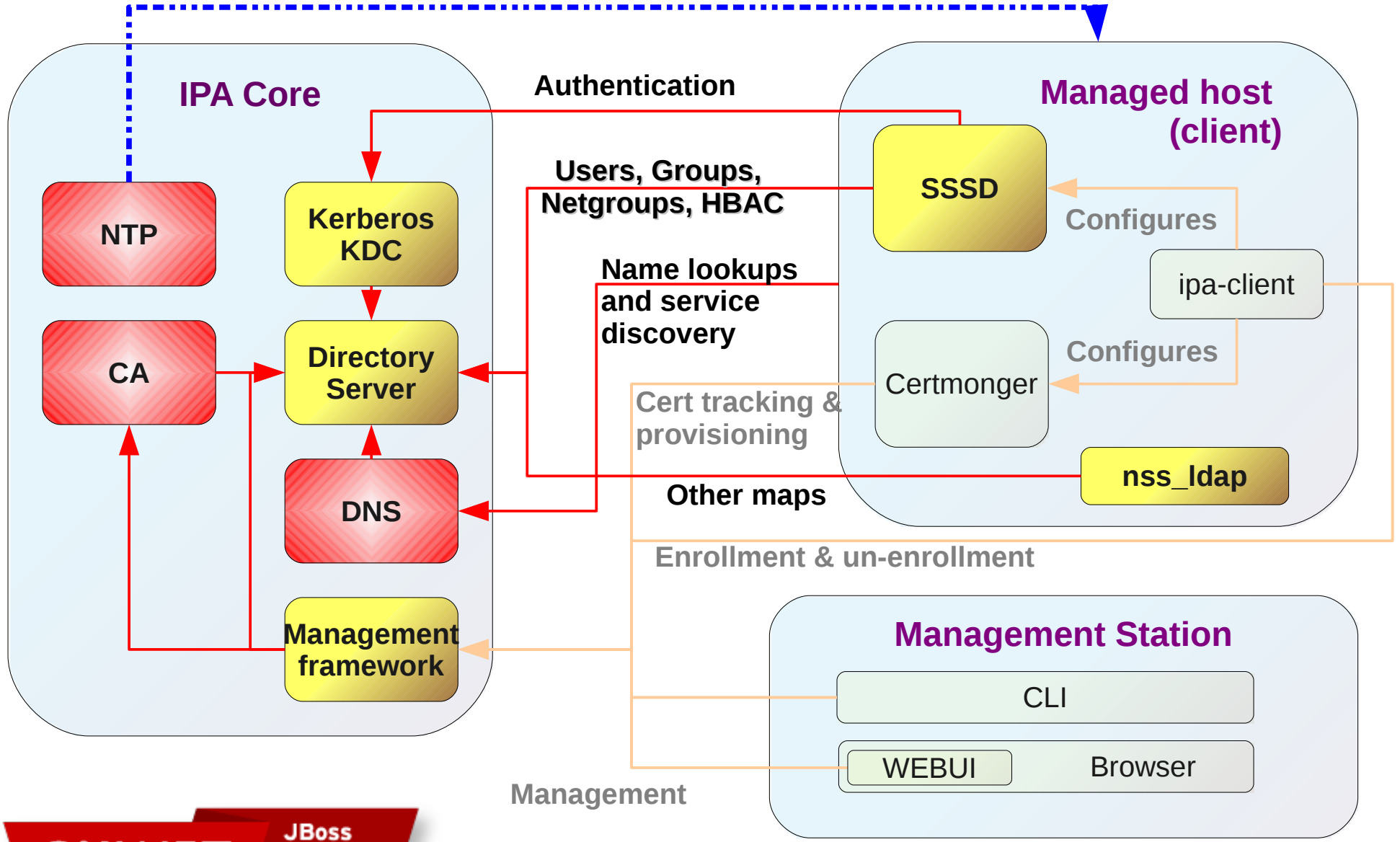
Under the Hood



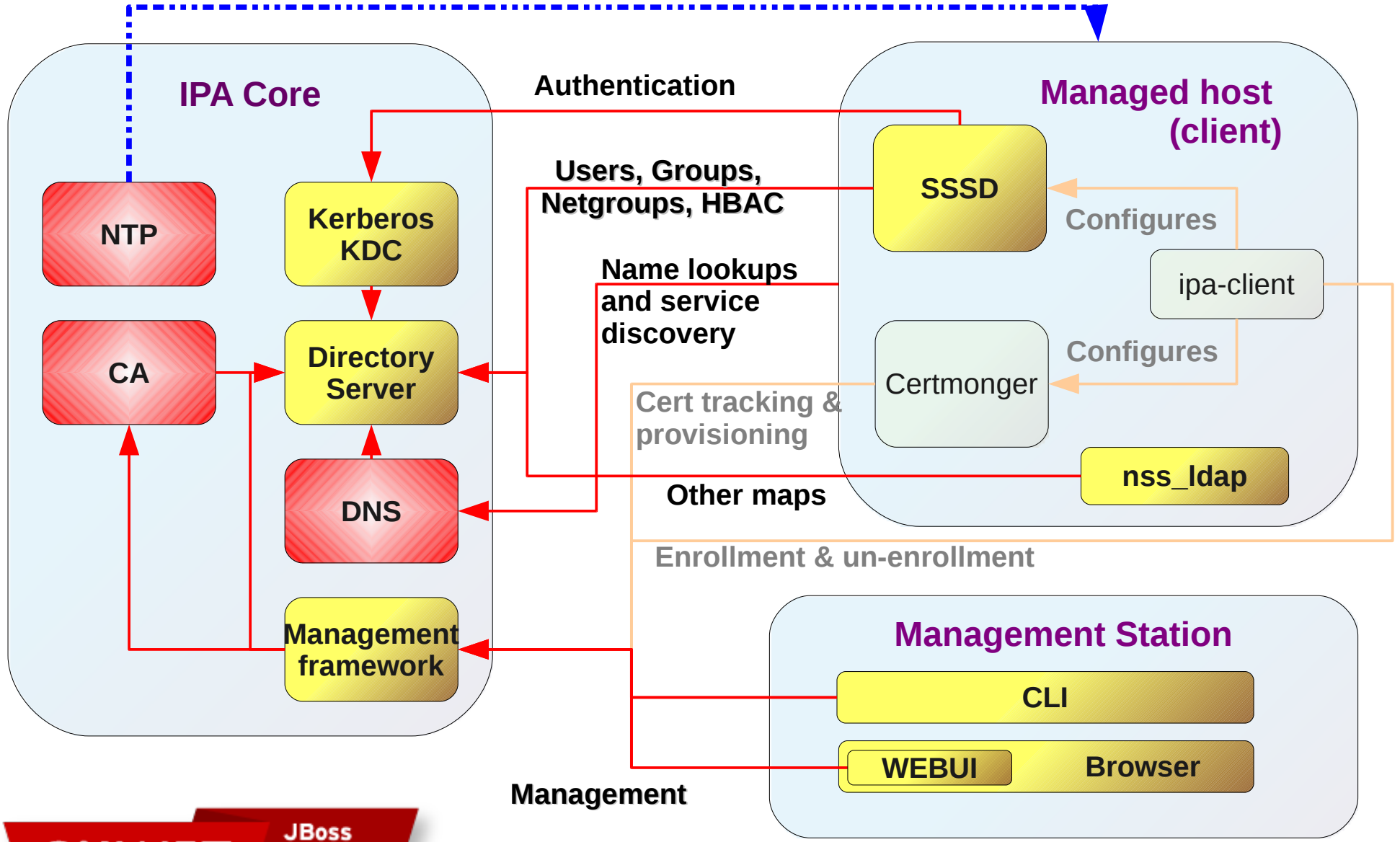
Under the Hood



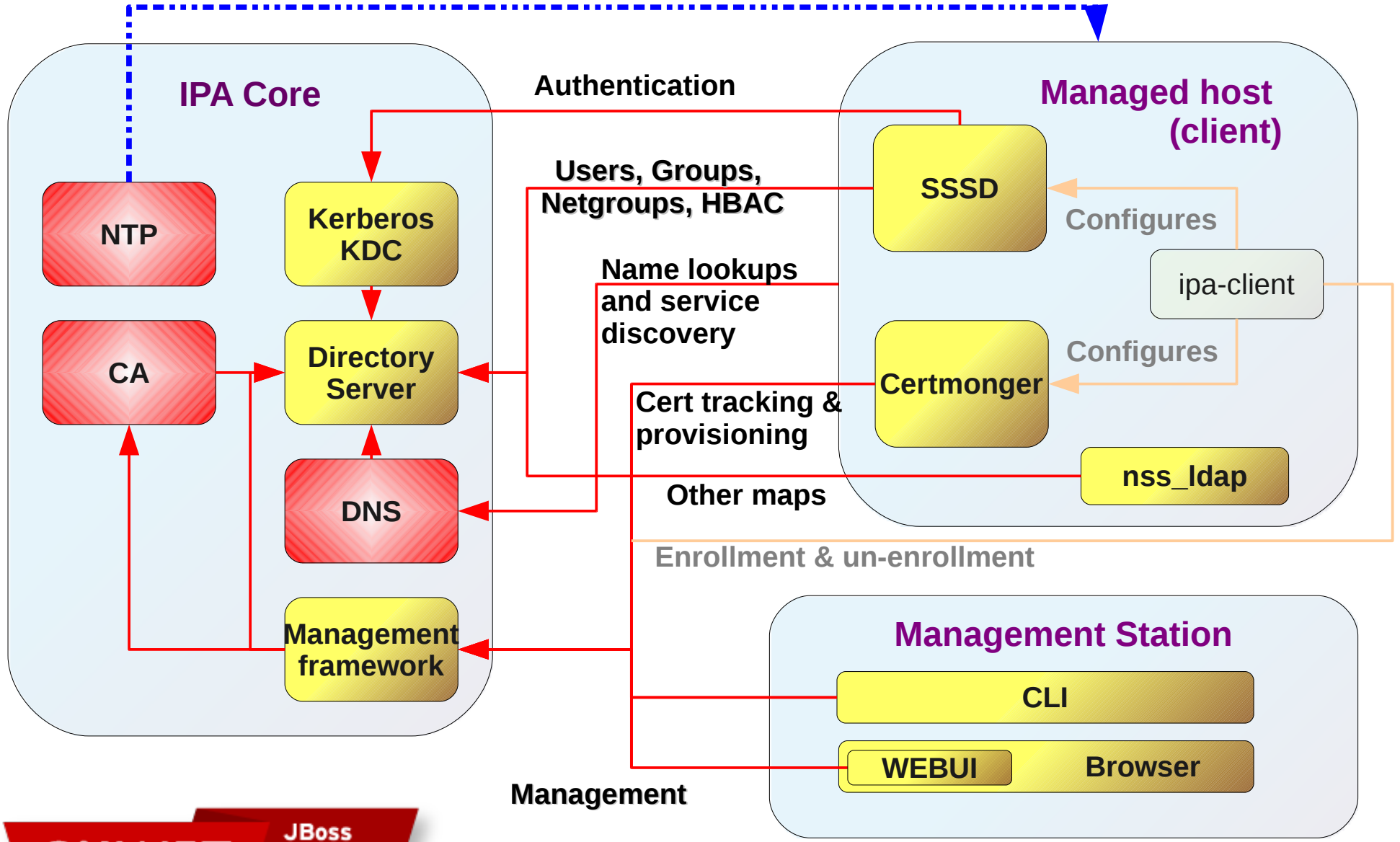
Under the Hood



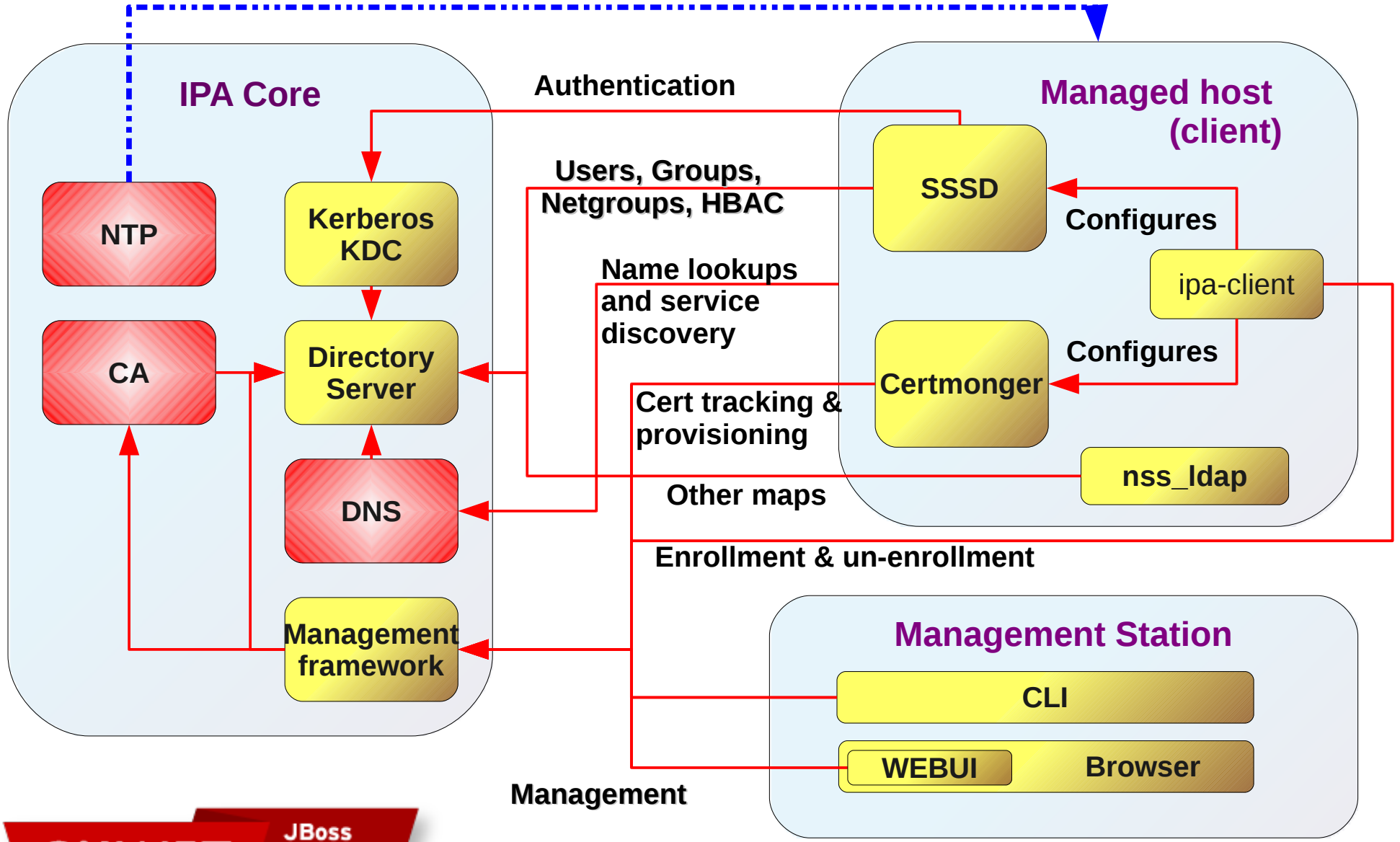
Under the Hood



Under the Hood



Under the Hood



Direction

- Bug fixing and cleanup
- UI improvements
- SELinux contexts, SSH key management
- Cross Kerberos trusts
- Native two factor authentication
- More certificate system integration
- Policies as needed
- RADIUS

Roadmap

- FreeIPA 2.0 -> Red Hat Enterprise Linux 6.1 tech preview
- FreeIPA 2.1 (bug fixing/UI improvements) -> Red Hat Enterprise Linux 6.2 full support
- FreeIPA 2.2/3.0 (SELinux/SSH key management/Cross Kerberos trusts) -> 2012 Red Hat Enterprise Linux releases

Resources

- Project wiki: www.freeipa.org
- Project trac: https://fedorahosted.org/freeipa/
- Code: http://git.fedorahosted.org/git/?p=freeipa.git
- SSSD: https://fedorahosted.org/sssd/
- Certmonger: https://fedorahosted.org/certmonger/
- Mailing lists:
  - freeipa-users@redhat.com
  - freeipa-devel@redhat.com
  - freeipa-interest@redhat.com

Questions?

LIKE US ON FACEBOOK

www.facebook.com/redhatinc

FOLLOW US ON TWITTER

www.twitter.com/redhatsummit

TWEET ABOUT IT

#redhat

READ THE BLOG

summitblog.redhat.com

GIVE US FEEDBACK

www.redhat.com/summit/survey