

RED HAT
SUMMIT

BOSTON, MA
JUNE 23-26, 2015

Integrating the RHCI Suite with IdM

INTRODUCTION

Who are we?

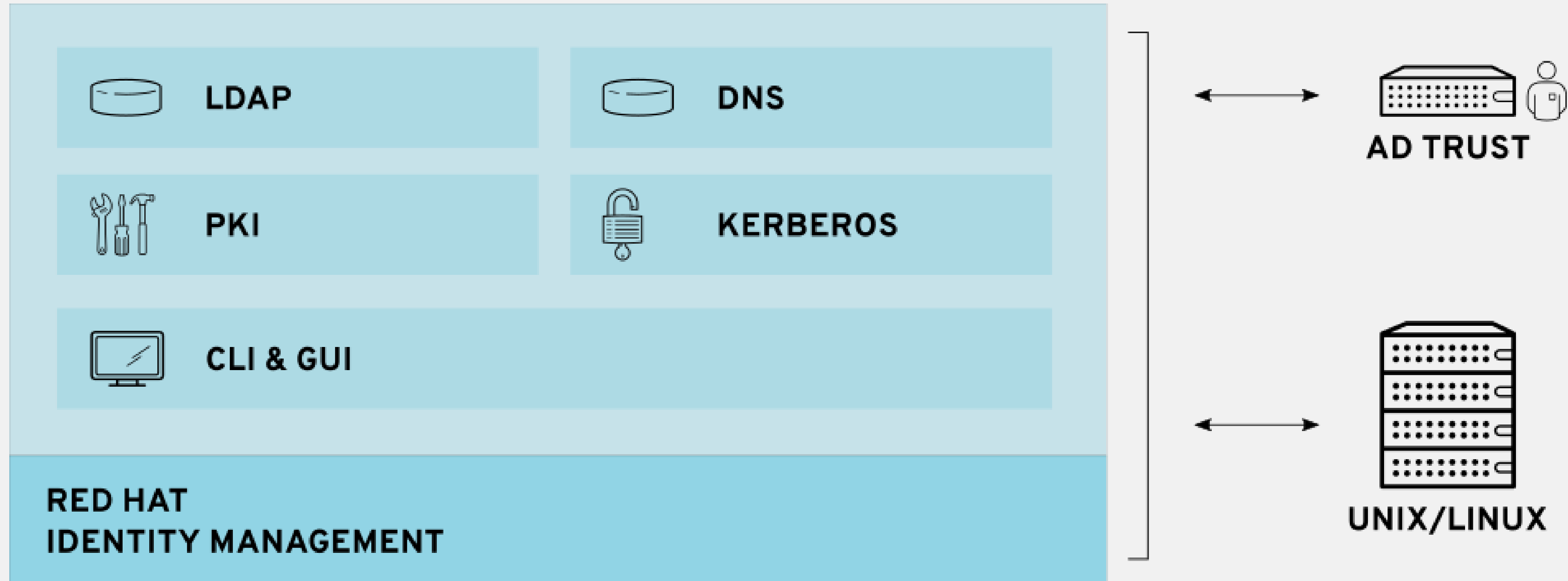


Chris Keller
Solutions Architect
Red Hat, Inc.

Nathan Kinder
Engineering Manager
Red Hat, Inc.



What is IdM?



IdM Features

- Numerous Capabilities
 - Identity management for users and machines
 - HBAC
 - 2FA (OTP)
 - Centralized sudo rules management
 - Other services including DNS, NTP



What is RHCI?

- Collection of products
 - Red Hat Enterprise Virtualization
 - Red Hat CloudForms
 - Red Hat Satellite
 - Red Hat Enterprise Linux Open Stack Platform
- Lets you build a private Infrastructure-as-a-Service (IaaS) based cloud for traditional workloads
- On-ramp to a highly scalable public-cloud-like infrastructure
- Built on Red Hat Enterprise Linux

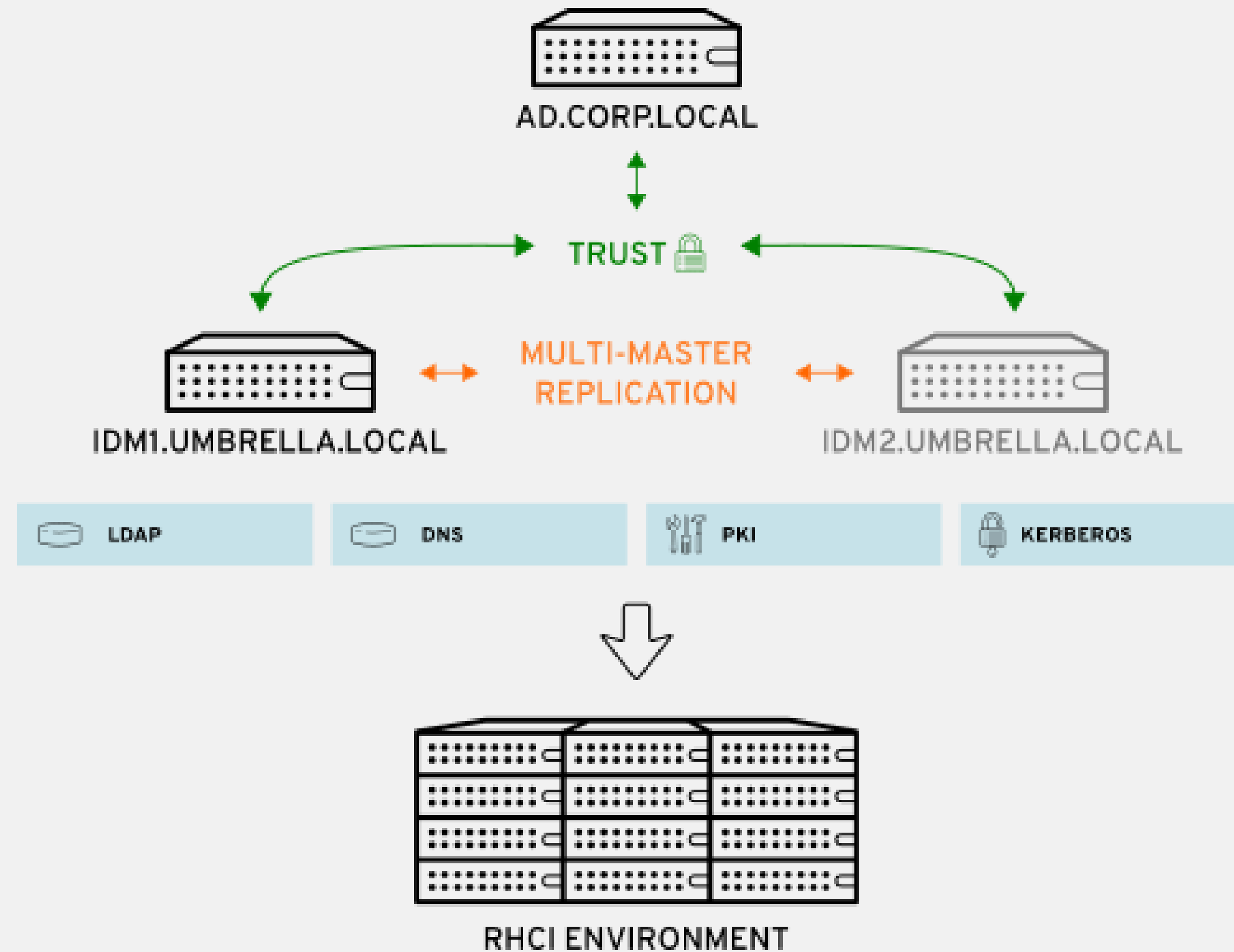
What are we integrating?

- RHEL
- Application User Interfaces
- Specific application functionality
 - Satellite system lifecycle in IdM
 - Application quotas
- Mapping application roles to groups
 - Common roles between products?
 - Overlap groups as much as possible (i.e. Administrators)

Why Centralized Authentication?

- Security!
- Most products have their own local user and group store
 - Managing multiple sets of users is difficult!
 - Who has access to what (difficult to audit)?
- IdM Provides centralized user and group management
 - Leverage AD users and groups
 - Align groups to roles in each application
 - Configure role/group assignment once

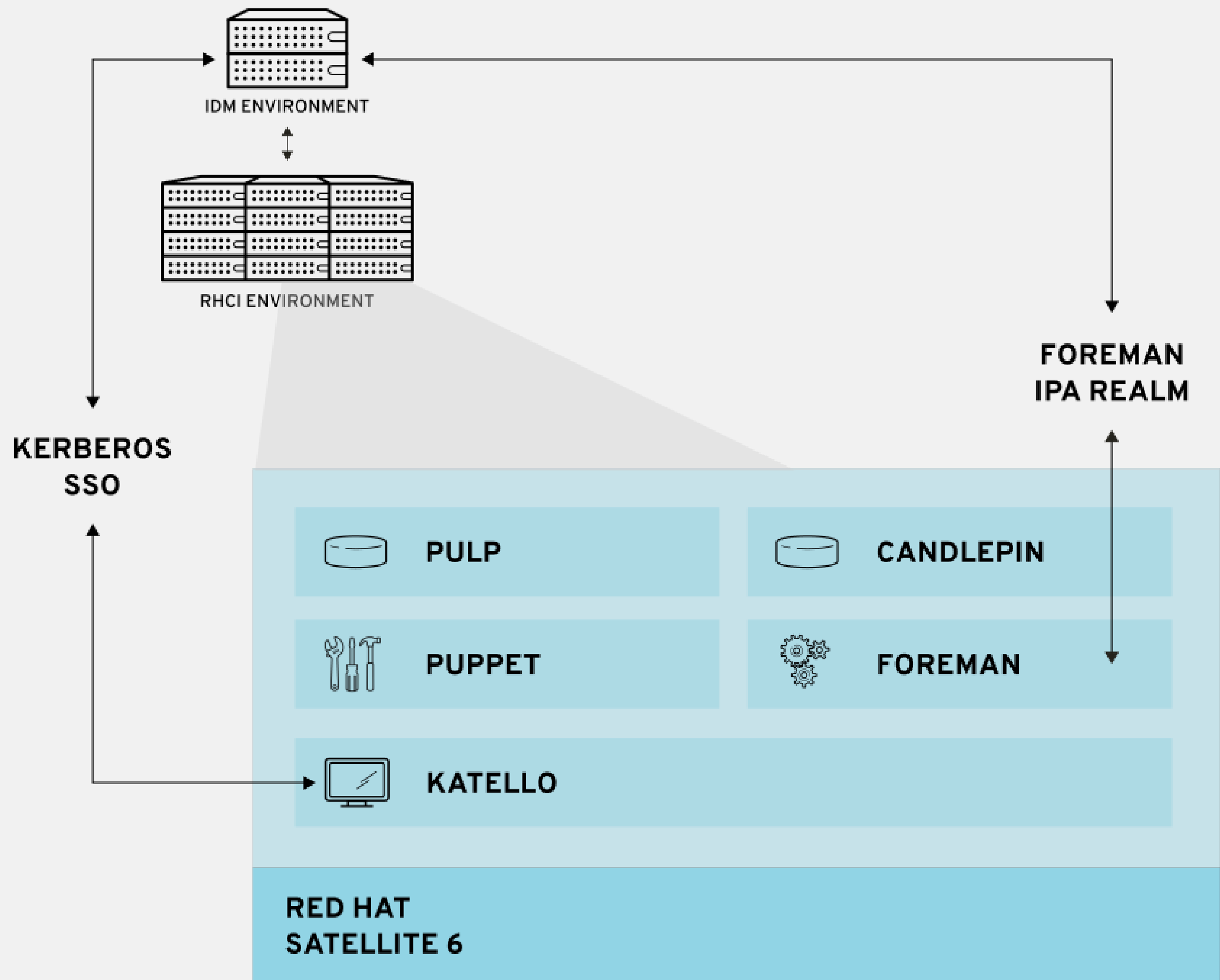
IdM Example Architecture



IdM Reference Environment

- RHEL 7.1 (Satellite, RHEL OSP)
- RHEL 6.6 (RHEV Manager, CloudForms Appliance)
- Provide for HA (multi-master replication)
- Integrate with Active Directory
- Will scale with your environment
 - Number of data centers
 - Number of hosts
- Developers and RHCI Administrators group

INTEGRATING RED HAT SATELLITE



Satellite Integration

- Satellite Server
- Satellite UI
- System life-cycle management in IdM
- Users
- Groups
- Roles
 - Administrators

Configuring RHEL

- Install Relevant Packages
 - ipa-client, foreman-proxy, ipa-admintools
- Connect system to IdM
 - # ipa-client-install**
 - (optional: --mkhomedir, etc)

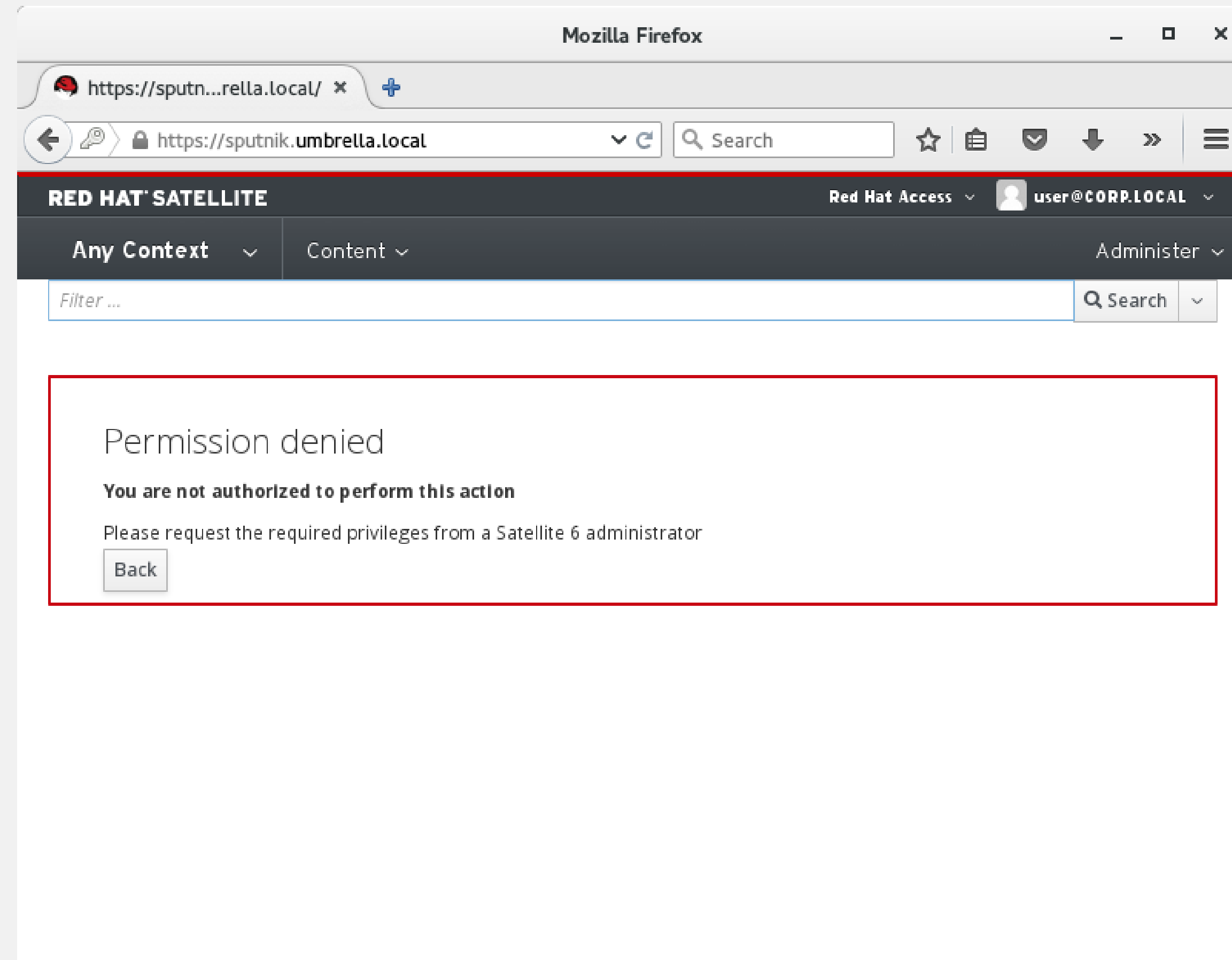
Access over SSH

```
user@corp.local@sputnik:~  
File Edit View Search Terminal Help  
0 chris@toaster:~ $ ssh -l user@CORP.LOCAL sputnik.umbrella.local  
user@CORP.LOCAL@sputnik.umbrella.local's password:  
Creating home directory for user@CORP.LOCAL.  
Last login: Thu Jun 18 15:04:13 2015 from 192.168.1.5  
[user@corp.local@sputnik ~]$  
[user@corp.local@sputnik ~]$ whoami  
user@corp.local  
[user@corp.local@sputnik ~]$  
[user@corp.local@sputnik ~]$ klist  
Ticket cache: KEYRING:persistent:1302401107:krb_ccache_u8RerQQ  
Default principal: user@CORP.LOCAL  
  
Valid starting      Expires            Service principal  
06/18/2015 15:04:48 06/19/2015 01:04:48 krbtgt/CORP.LOCAL@CORP.LOCAL  
        renew until 06/19/2015 15:04:48  
[user@corp.local@sputnik ~]$
```

Configuring UI

- Kerberos SSO
- Create Service Principal for Apache
 - # kinit admin**
 - # ipa service-add HTTP/sputnik.umbrella.local@UMBRELLA.LOCAL**
- Configure Foreman
 - # katello-installer --foreman-ipa-authentication=true**

What happens after logging in?



Assigning Groups to Roles

- Administrative access by group?
- Create a new User Group that includes an external user group from IdM
- rhci_administrators in Satellite which sources rhci_administrators in IdM
 - Assign this group the Admin role

Assign External Group

Usergroup Roles **External groups** ✕

Name	Auth source
------	-------------

Show linked external user groups

External user group ✕

Name

Auth source

+ Add external user group

Assign This Group a Role

The screenshot shows a web interface for managing user groups. At the top, there are three tabs: "Usergroup", "Roles", and "External groups". The "Roles" tab is active. Below the tabs, there is a section for "Admin" with a checked checkbox. Underneath, there is a "Roles" section. On the left, there is a list of roles with a search filter and a plus sign. The roles listed are "Boot disk access", "Discovery", "Edit hosts", "Edit partition tables", and "Manager". On the right, there is a "Selected items" box with a minus sign. A double-headed arrow indicates the relationship between the two boxes. At the bottom left, there are "Cancel" and "Submit" buttons.

Usergroup Roles External groups

Admin

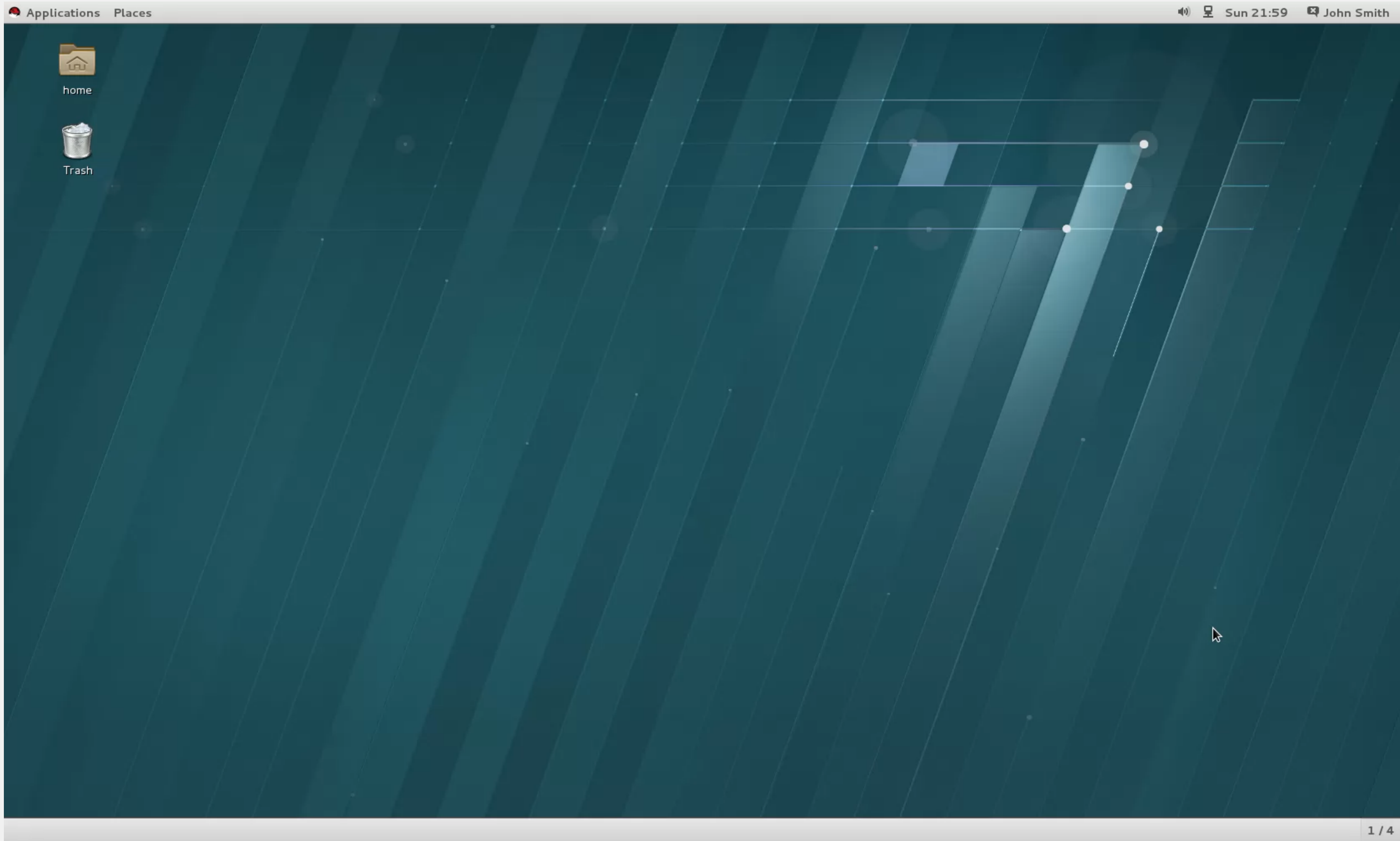
Roles

All items +

- Boot disk access
- Discovery
- Edit hosts
- Edit partition tables
- Manager

Selected items -

Cancel Submit



Enabling IdM Realm Support in Foreman

- Foreman can manage the lifecycle of hosts in IdM
- Can configure a series of realms (e.g. UMBRELLA.LOCAL) that can be associated with a host when initially provisioned
- IdM generates single-use password
 - Foreman embeds password in provisioning template
- Systems can be automatically enrolled in Host Groups
 - HBAC based on group membership
 - Self-service users have access to resources immediately

Realm Configuration

- Configure IdM to work with a Foreman Smart Proxy
 - Creates dedicated IdM role with appropriate permissions
 - Creates a user and retrieves keytab
- ```
foreman-prepare-realm admin realm-capsule
```

# Realm Configuration Continued

- Configure the realm in Katello



```
katello-installer --capsule-realm true
--capsule-realm-keytab /etc/foreman-proxy/freeipa.keytab
--capsule-realm-principal 'realm-capsule@UMBRELLA.LOCAL'
--capsule-realm-provider freeipa
```








- /etc/foreman-proxy/freeipa.keytab was created via foreman-prepare-realm command
- Restart the foreman-proxy service

```
systemctl restart foreman-proxy.service
```




# Creating IdM Realm in Satellite


RED HAT SATELLITE Red Hat Access  Admin User 

Any Context  Monitor  Content  Hosts  Configure  Infrastructure  Administer 

## Realms

Filter ...   

| Name           |
|----------------|
| UMBRELLA.LOCAL |

Realm Locations Organizations 

Name  Realm name, e.g. EXAMPLE.COM

Realm type  Type of realm, e.g. Red Hat Identity Management

Realm proxy  Realm proxy to use within this realm

# Assigning Systems to Host Groups

- Setup automatic membership rules based on a system's attributes
- When a system joins a Satellite Host Group, the system is joined to corresponding IdM Host Group as well
  - Allows for HBAC, sudo policies, etc.
  - Foreman Host Group is available as a parameter in IdM known as userclass
- In IdM, setup an automembership rule

```
ipa automember-add --type=hostgroup app_servers
```
- Define an automembership condition based on the userclass attribute

```
ipa automember-add-condition --key=userclass
--type=hostgroup --inclusive-regex=^app_server app_servers
```
- Note: automember rules only applied during initial add

# INTEGRATING RED HAT ENTERPRISE VIRTUALIZATION



# RHEV Integration

- RHEV-M Server
- RHEL Hypervisors
- RHEV UI
- Users
- Groups
  - Quota Management
- Roles
  - Administrator
  - User (Provisioning)



# Configuring RHEV-M Server

- Install Relevant Packages
  - ipa-client
- Connect system to IdM
  - # ipa-client-install**
  - (optional: --mkhomedir, etc)

# Configuring RHEV Manager

- Configure engine to use IPA

```
engine-manage-domains add --domain=UMBRELLA.LOCAL
--provider=IPA --user=admin
```

- Engine is now configured to use external users and groups
  - Need to align users/groups to roles

# Linking Users/Groups to Roles

The screenshot shows the Red Hat Enterprise Virtualization (RHEV) web interface. A 'Configure' dialog box is open, titled 'Add System Permission to User'. The dialog has a search field with 'umbrella.local (umbrella.local)' and a namespace dropdown set to '\*'. Below the search is a table of users and groups. The user 'accounts/groups/rhci\_administrators@umbrella.local' is selected. At the bottom, the 'Role to Assign' dropdown is set to 'SuperUser'. The dialog has 'OK', 'Cancel', and 'Close' buttons.

| First Name                          | Last Name                                          | User Name     |
|-------------------------------------|----------------------------------------------------|---------------|
| <input type="checkbox"/>            | Administrator                                      | admin         |
| <input type="checkbox"/>            | Chris Keller                                       | chris         |
| <input type="checkbox"/>            | Smart Proxy                                        | realm-capsule |
| <input type="checkbox"/>            | Katello LDAP                                       | katello-ldap  |
| <input type="checkbox"/>            | accounts/groups/admins@umbrella.local              |               |
| <input type="checkbox"/>            | accounts/groups/ipausers@umbrella.local            |               |
| <input type="checkbox"/>            | accounts/groups/editors@umbrella.local             |               |
| <input type="checkbox"/>            | accounts/groups/trust_admins@umbrella.local        |               |
| <input checked="" type="checkbox"/> | accounts/groups/rhci_administrators@umbrella.local |               |
| <input type="checkbox"/>            | accounts/groups/cfme_administrators@umbrella.local |               |

# Administrator Role Configured

The screenshot shows the Red Hat Enterprise Virtualization Administrator interface. A 'Configure' dialog box is open, displaying a table of roles. The table has columns for User, Authorization provider, Namespace, and Role. The roles listed are SuperUser and PowerUserRole, assigned to both internal users and external users from the umbrella.local domain.

| User                                             | Authorization provider | Namespace | Role          |
|--------------------------------------------------|------------------------|-----------|---------------|
| admin (admin@internal)                           | internal               | *         | SuperUser     |
| admin (admin@internal)                           | internal               | *         | PowerUserRole |
| accounts/groups/rhci_administrators@umbrella.... | umbrella.local         | *         | SuperUser     |
| accounts/groups/rhci_administrators@umbrella.... | umbrella.local         | *         | PowerUserRole |

# Creating a Developer Quota

**RED HAT ENTERPRISE VIRTUALIZATION** | chris | Configure | Guide | About | Market Place

DataCenter: [ ]

**Edit Quota** ?

Name:  Description:

Data Center:

**Memory & CPU**

80% 120% Cluster Threshold Cluster Grace

All Clusters  Specific Clusters

| Cluster Name | Memory            | vCPU              |                                     |
|--------------|-------------------|-------------------|-------------------------------------|
| All Clusters | 0 out of 30720 MB | 0 out of 16 vCPUs | <input type="button" value="Edit"/> |

**Storage**

80% 120% Storage Threshold Storage Grace

All Storage Domains  Specific Storage Domains

| Storage Name        | Quota           |                                     |
|---------------------|-----------------|-------------------------------------|
| All Storage Domains | 0 out of 128 GB | <input type="button" value="Edit"/> |

Last Message: 2015-Jun-22, 04:12 User chris@umbrella.local logged in. Alerts (0) Events Tasks (0)



# Assigning a Quota

The screenshot displays the Red Hat Enterprise Virtualization web console interface. At the top, the title bar reads "RED HAT ENTERPRISE VIRTUALIZATION" and includes navigation links for "chris", "Configure", "Guide", "About", and "Market Place". The main content area shows a breadcrumb trail: "Quota: storagepoolname = Default". A modal dialog box titled "Assign Users and Groups to Quota" is open in the center. The dialog has two radio buttons: "Specific User/Group" (selected) and "Everyone". Below these are search fields for "Search:" (containing "umbrella.local (umbrella.local)") and "Namespace:" (containing "\*"). A "GO" button is to the right of the namespace field. A list of users and groups is displayed below, each with a checkbox. The user "accounts/groups/rhci\_developers@umbrella.lo..." is selected. At the bottom of the dialog are "OK" and "Cancel" buttons. The background interface shows a sidebar with "System" and "Data Centers" sections, and a bottom status bar with a message: "User/Group accounts/groups/rhci\_developers@umbrella.local Role QuotaConsumer permission was remo...".

RED HAT ENTERPRISE VIRTUALIZATION

chris Configure Guide About Market Place

Quota: storagepoolname = Default

System

Expand All Collapse All

System

Data Centers

Default

Storage

Network

Templat

Clusters

External Prov

Assign Users and Groups to Quota

Specific User/Group  Everyone

Search: umbrella.local (umbrella.local) Namespace: \* GO

- accounts/groups/admins@umbrella.local
- accounts/groups/ipausers@umbrella.local
- accounts/groups/editors@umbrella.local
- accounts/groups/trust\_admins@umbrella.local
- accounts/groups/rhci\_administrators@umbrell...
- accounts/groups/cfme\_administrators@umbr...
- accounts/groups/rhci\_security@umbrella.local
- accounts/groups/rhci\_appdev@umbrella.local
- accounts/groups/ad\_linux\_administrators@u...
- accounts/groups/rhci\_developers@umbrella.lo...

OK Cancel

Bookmarks

Tags

Last Message: 2015-Jun-22, 04:16 User/Group accounts/groups/rhci\_developers@umbrella.local Role QuotaConsumer permission was remo... Alerts (0) Events Tasks (0)

# INTEGRATING RED HAT CLOUDFORMS

# CloudForms Integration

- CloudForms Appliance
- CloudForms UI
- Users
- Groups
- Roles
  - Administrator
  - User (Provisioning)

# Configuring the Appliance

- No need to Install Relevant Packages
  - ipa-client is already installed on the appliance
- Connect system to IdM & configure external auth

```
/bin/appliance_console_cli --host cloudforms.umbrella.local
--ipaserver idm1.umbrella.local --iparealm UMBRELLA.LOCAL
--ipaprincipal admin --ipapassword <secret>
```
- What just happened?
  - ipa-client-install
  - SSSD/PAM configuration
  - Apache configuration updated
  - SELinux Booleans



# Configure CloudForms

CFME: Configuration - Mozilla Firefox

CFME: Configuration

https://cloudforms.umbrella.local/ops/explorer

RED HAT® CLOUDFORMS MANAGEMENT ENGINE

Chris Keller | EVM

Cloud Intelligence Services Clouds Infrastructure Control Automate Optimize Configure

My Settings Tasks Configuration SmartProxies About

Settings

- CFME Region: Region 1 [1]
  - Analysis Profiles
    - host default
    - host sample
    - sample
  - Zones
    - Zone: Default Zone (curr)
    - Server: EVM [1000000]
  - Schedules

Access Control

Diagnostics

Database

### Settings Server "EVM [10000000000001]" (current)

#### Authentication

Session Timeout: 1 h 0 m

Mode: External (httpd)

#### External Authentication (httpd) Settings

Enable Single Sign-On:

#### Role Settings

Get User Groups from External Authentication (httpd):

Save Reset

6/19/15 12:08 UTC



# Adding LDAP Backed Groups w/ Roles

The screenshot shows the Red Hat CloudForms Management Engine interface in Mozilla Firefox. The browser address bar shows the URL `https://cloudforms.umbrella.local/ops/explorer`. The page title is "CFME: Configuration - Mozilla Firefox". The user is logged in as "Administrator | EVM".

The main navigation bar includes "Cloud Intelligence", "Services", "Clouds", "Infrastructure", "Control", "Automate", "Optimize", and "Configure". The "Configure" tab is active. Below this, there are sub-tabs: "My Settings", "Tasks", "Configuration", "SmartProxies", and "About".

The left sidebar shows the "Settings" menu with "Access Control" expanded. Under "Access Control", there is a tree view for "CFME Region: Region 1 [1]" containing "Users" (Administrator, Chris Keller) and "Groups" (EvmGroup-administrator, EvmGroup-approver, EvmGroup-auditor, EvmGroup-desktop, EvmGroup-operator, EvmGroup-security, EvmGroup-super\_administrator, EvmGroup-support, EvmGroup-user).

The main content area is titled "Adding a new Group". It is divided into three sections:

- Group Information:** Contains a "Description" field with the value "rhci\_administrators" and a checked checkbox "(Look Up LDAP Groups)". Below it is a "Role" dropdown menu set to "EvmRole-super\_administrator".
- LDAP Group Look Up:** Contains three input fields: "User to Look Up", "User Id", and "Password", along with a "Retrieve" button.
- Assign Filters:** Shows a list of filters under the heading "My Company Tags". The selected filters are "Hosts & Clusters" and "VMs & Templates". Below this list, a message states: "This user is limited to items with the selected tags." followed by a list of filter categories: "Auto Approve - Max CPU", "Auto Approve - Max Memory", "Auto Approve - Max Retirement Days", "Auto Approve - Max VM", "Cost Center", "Department", "Environment", and "EVM Operations".

At the bottom right of the main content area, there are "Add" and "Cancel" buttons. The footer of the page shows the date and time: "6/19/15 12:12 UTC".

# Configuring Quota



- CloudForms uses the notion of tagging
  - Virtual machines, physical assets, accounts, etc
  - Tags can be manually assigned or dynamically created
- Quotas work based off tags
  - Tags can be assigned based off group membership

# Quota Example

## Editing My Company Tags for "EVM Groups"


### Tag Assignment

Select a customer tag to assign:

|                                                                                   | Category                    | Assigned Value         |
|-----------------------------------------------------------------------------------|-----------------------------|------------------------|
|  | Auto Approve - Max Memory * | 8GB                    |
|  | Auto Approve - Max VM *     | 2                      |
|  | Line of Business            | Application Developers |

\* Only a single value can be assigned from these categories

### 1 EVM Group Being Tagged

|                                                                                     | Name            | Read Only | Number of Users | Role                      | Sequence |
|-------------------------------------------------------------------------------------|-----------------|-----------|-----------------|---------------------------|----------|
|  | rhci_developers | False     | 0               | EvmRole-user_self_service | 14       |

# INTEGRATING RHEL OPEN STACK PLATFORM



# Keystone

- Keystone focal point for identity in OpenStack
  - Used by all OpenStack for authentication, authorization, service catalogs, etc
- Supports a variety of identity providers
  - SQL (Keystone acts as identity provider)
  - LDAP
  - External
- Keystone best suited for authorization, not necessarily authentication



# Basic SQL Provider

- Leverages SQL database for identity
- User entry is stored in database that contains password hash
- Data is sent via clear text
- Password based authentication services (i.e. LDAP) have additional security capabilities
  - Dictionary checking
  - Password change intervals
  - Password history
  - Account lockouts

# LDAP Provider

- Keystone only supports simple BIND operations
- Works just like the SQL authentication source mentioned previously
- LDAP supports strong authentication via SASL
  - Keystone does not support SASL bind operations
- Offloads user provisioning and maintenance
  - Allows for centralized identity source that can be shared with other applications

# External Provider

- Allows for stronger form of authentication vs. simple password based authentication
- Keystone expects the web server to handle authentication
  - Can utilize a host of Apache authentication modules
  - Apache supplies keystone with authenticated user name via REMOTE\_USER environment variable
- User still stored in Keystone (or LDAP store) but no password credentials
- Obvious benefit for security

# Federation Extension

- Simpler for Keystone
- No need for LDAP schema extensions or LDAP connection management
- Have Apache provide pertinent information on authenticated user along with token request
  - Keystone can then map user info to applicable project and roles
- How does this work?

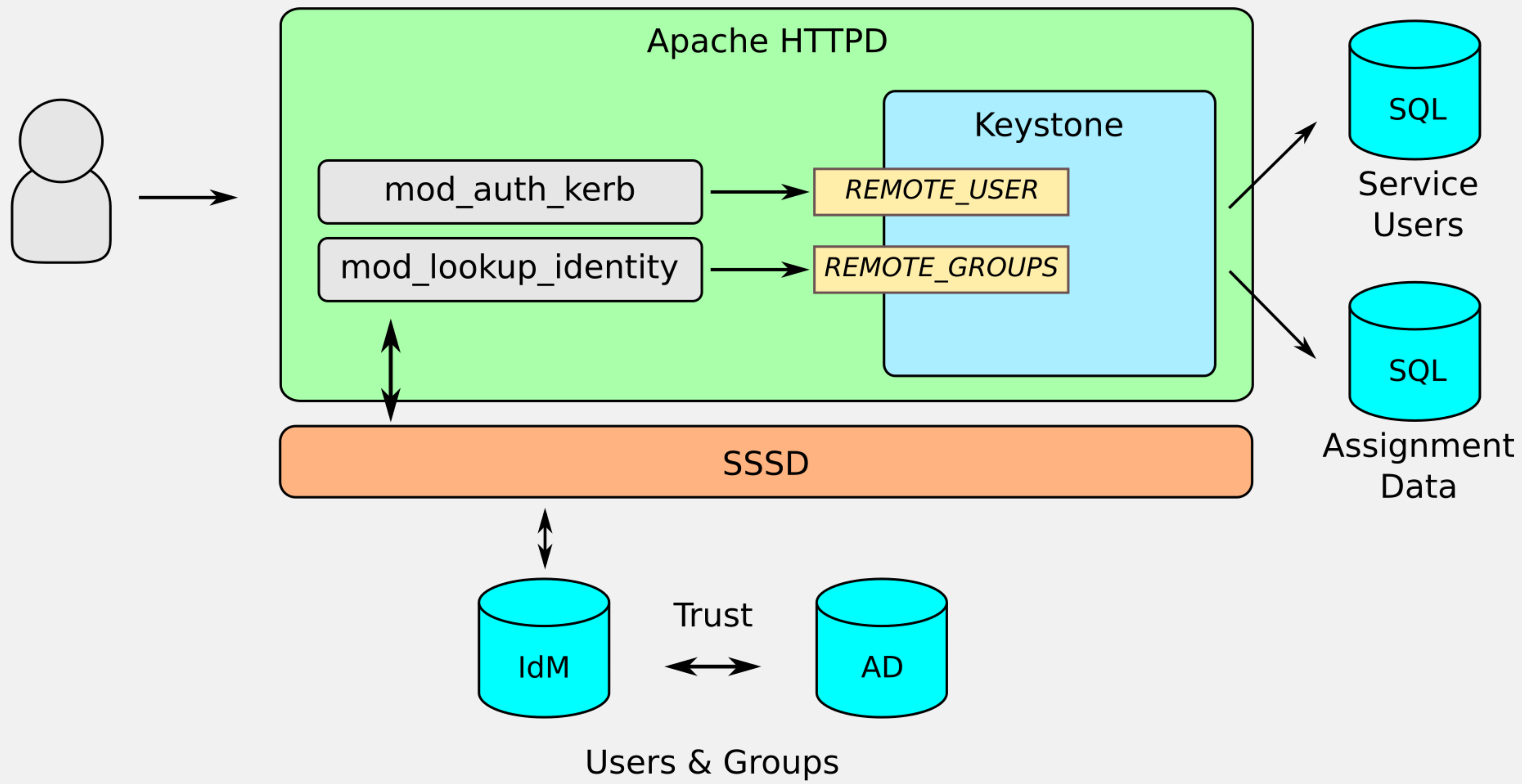
# Integrating with IdM

- mod\_identity\_lookup – Helps to eliminate the need for identity lookup in Keystone
- Utilizes SSSD from underlying platform to provide user and group information
  - Information can be source from various providers
    - **IdM**, LDAP and/or Active Directory
- SSSD provides additional capabilities that Keystone does not
  - Credential and attribute caching
  - Connection pooling
  - Multiple identity sources
- Allows for a more scalable and performant Keystone service



# SSSD & Cross Realm Trusts

- Leverage AD accounts via cross realm trusts in IdM
  - Users can use their TGT from AD to fetch Kerberos enabled services that are setup in IdM, such as Keystone and Horizon
- OpenStack specific groups defined locally in IdM
  - SSSD is able to extract group information from PAC
  - Matching external groups in IdM setup to match AD
- Multiple trusts allow users from multiple forests to leverage the same Keystone server



# Thank You!

- Chris Keller  
[ckeller@redhat.com](mailto:ckeller@redhat.com)
- Nathan Kinder  
[nkinder@redhat.com](mailto:nkinder@redhat.com)



RED HAT  
**SUMMIT**

LEARN. NETWORK.  
EXPERIENCE OPEN SOURCE.