Red Hat
Ansible Automation
Platform

Automating Identity Management with Ansible Automation

Brad Krumme
Solutions Architect

Red Hat

SysAdmin Background

RHCE and Ansible Specialist

Love Sports/Performance Cars

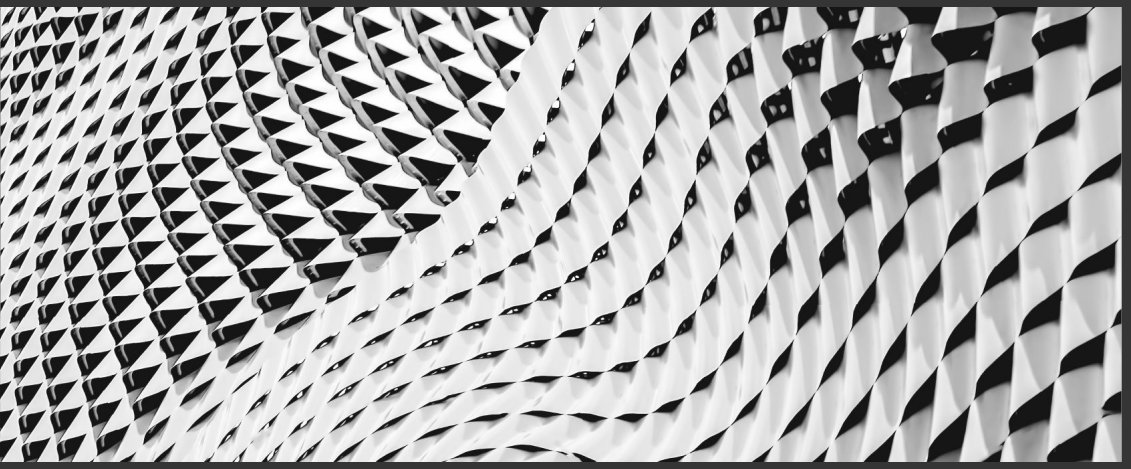
Also love Craft Beer and Bourbon

Brad Krumme
Solutions Architect

What we'll discuss today

- Overview of Red Hat Identity Management
- Overview of Ansible Automation Platform
- Identity Management Automation Use Case
- Ansible Setup Considerations
- Automation In Practice
- Extra Resources

Red Hat Identity Management Overview



Red Hat Identity Management provides a centralized and clear method for managing identities for users, machines, and services within large Linux/Unix enterprise environments.

Red Hat

IdM Server - responsibilities

What is expected from the service?

Identity Store

- Users, Hosts, Services
- Groups (User and Host)

Authentication

- Passwords, 2FA (Smart Cards, OTP soft/hard tokens)
- SSO
- Client/Server certificates (PKI)

Authorization

- Access rules per host
- Privileged operations
- IdM itself - RBAC - user roles and admin delegations

Security-related service management

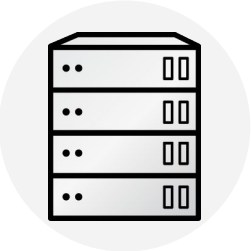
- Secrets (passwords)
- Linux - SUDO, SELinux, etc.

Auditing and reporting

Red Hat

IdM Server - standard interfaces

How Identity Servers interact with the outer world



Infrastructure

- **LDAP**: old & proven protocol for sharing data, sometimes authentication too (v3 from *1997)
- **Kerberos**: old & proven protocol for authentication (*1993, revised 2005)
- **Deprecated**: NIS, NTLM

Applications

- **LDAP**: user details, often authentication too
- **Kerberos**: authentication (SSO), mostly for **internal** applications
- **SAML**: old, robust, proven (but may go away too)
- **OAuth 1.0**: old, has weaknesses, should not be used
- **OAuth 2.0 / OpenID Connect** (OIDC): modern, proven, recommended for new applications

IdM Client - Responsibilities

What client (operating system) expects from IdM?

Retrieving Identity information

- Users, Groups, netgroups, host groups, roles
- Certificates, keytabs

Authentication

- Passwords, tickets

Authorization

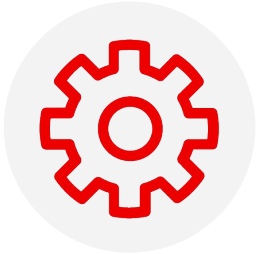
- HBAC, sudo rules, SSH keys

Misc

- SELinux users
- Automount maps, other configuration
- DNS discovery, DNS Updates, time synchronization

IdM Client - interfaces

Where do IdM services plug in



NSS - Name Service Switch

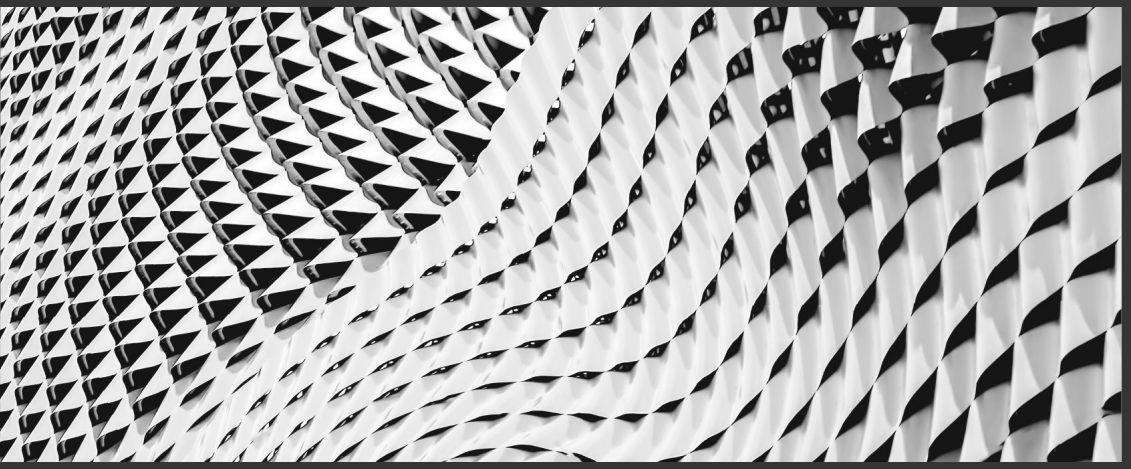
- Old protocol for Unix-like OS for common configuration databases and name resolution mechanisms (* ~1993)
- Configured in /etc/nsswitch.conf
- Example calls: getpwent(), gethostbyname(), ...

PAM - Pluggable authentication module

- Traditional (* ~1995), evolved from Unix PAM
- Mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface (API).
- Authentication stages/groups: account, authentication, password, session
- Example modules: login, sudo, gdm, vsftpd, ...

Source: Wiki - NSS, Wiki - PAM, abokovoy-fedora-auth-n-identity-state

Red Hat Ansible Automation Overview



Red Hat Ansible Automation is an automation solution that acts as a resource provisioner, configuration management tool, release automation utility, and can provision and manage entire application and infrastructure environments.

Red Hat

Red Hat Ansible Automation Platform

Network | Lines of business | Security |  | Operations | Infrastructure | Developers

Engage

Ansible SaaS: Engage users with an automation focused experience

Scale

Ansible Tower: Operate & control at scale

Create

Ansible Engine: Universal language of automation

Fueled by an open source community

Red Hat

Why Ansible?

Simple

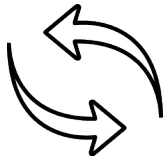
Human readable automation

No special coding skills needed

Tasks executed in order

Usable by every team

Get productive quickly



Powerful

App deployment

Configuration management

Workflow orchestration

Network automation

Orchestrate the app lifecycle

Agentless

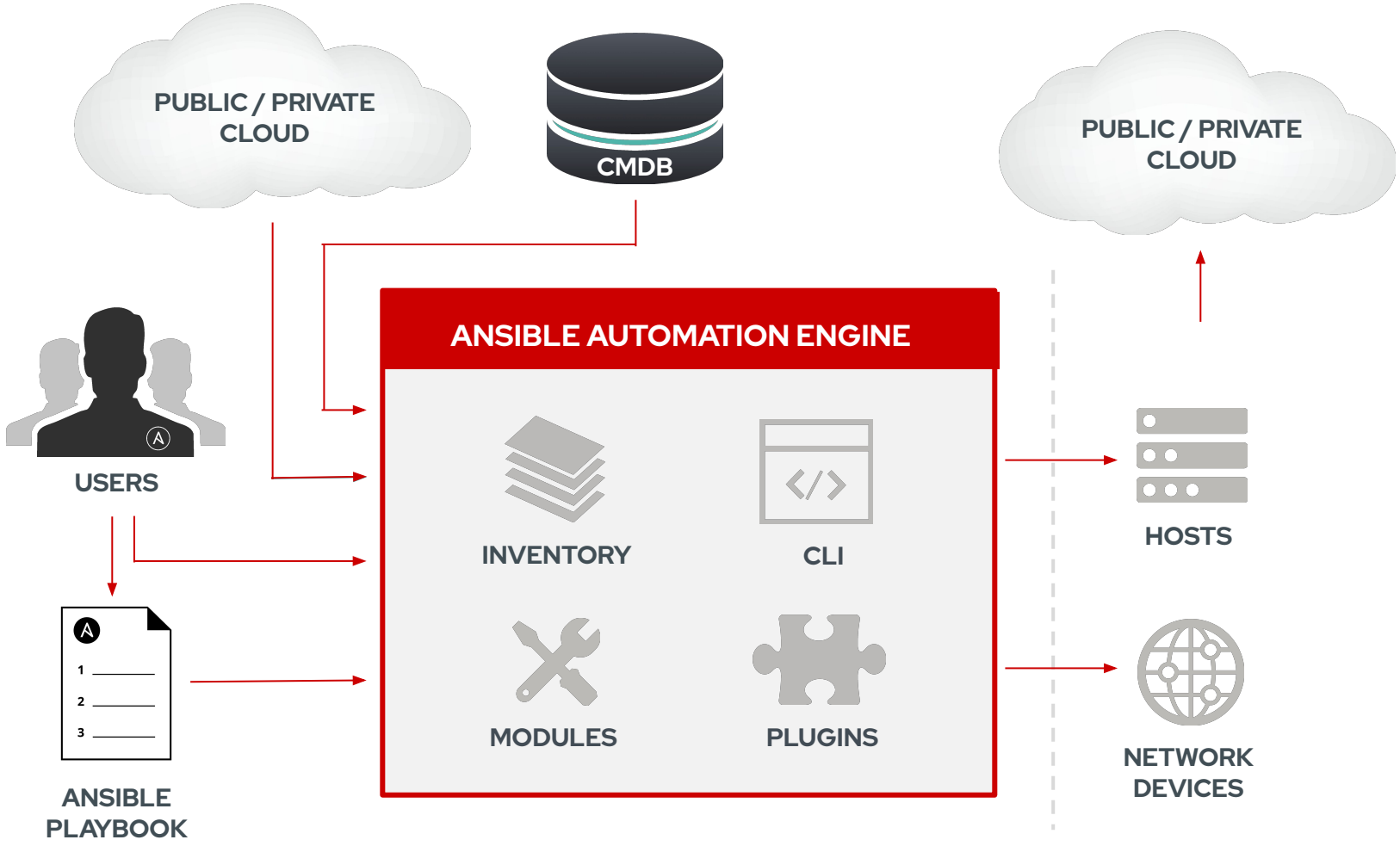
Agentless architecture

Uses OpenSSH & WinRM

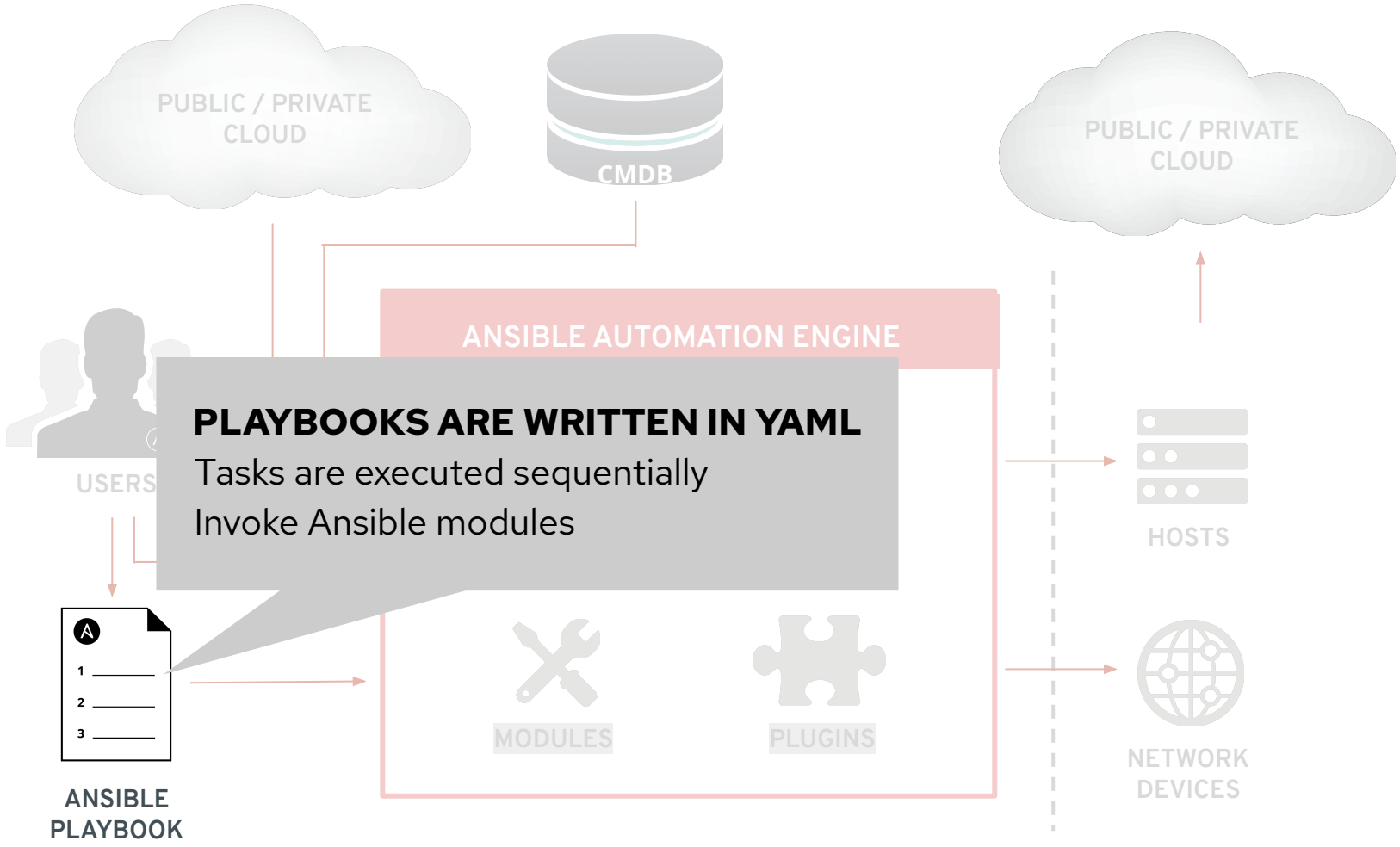
No agents to exploit or update

Get started immediately

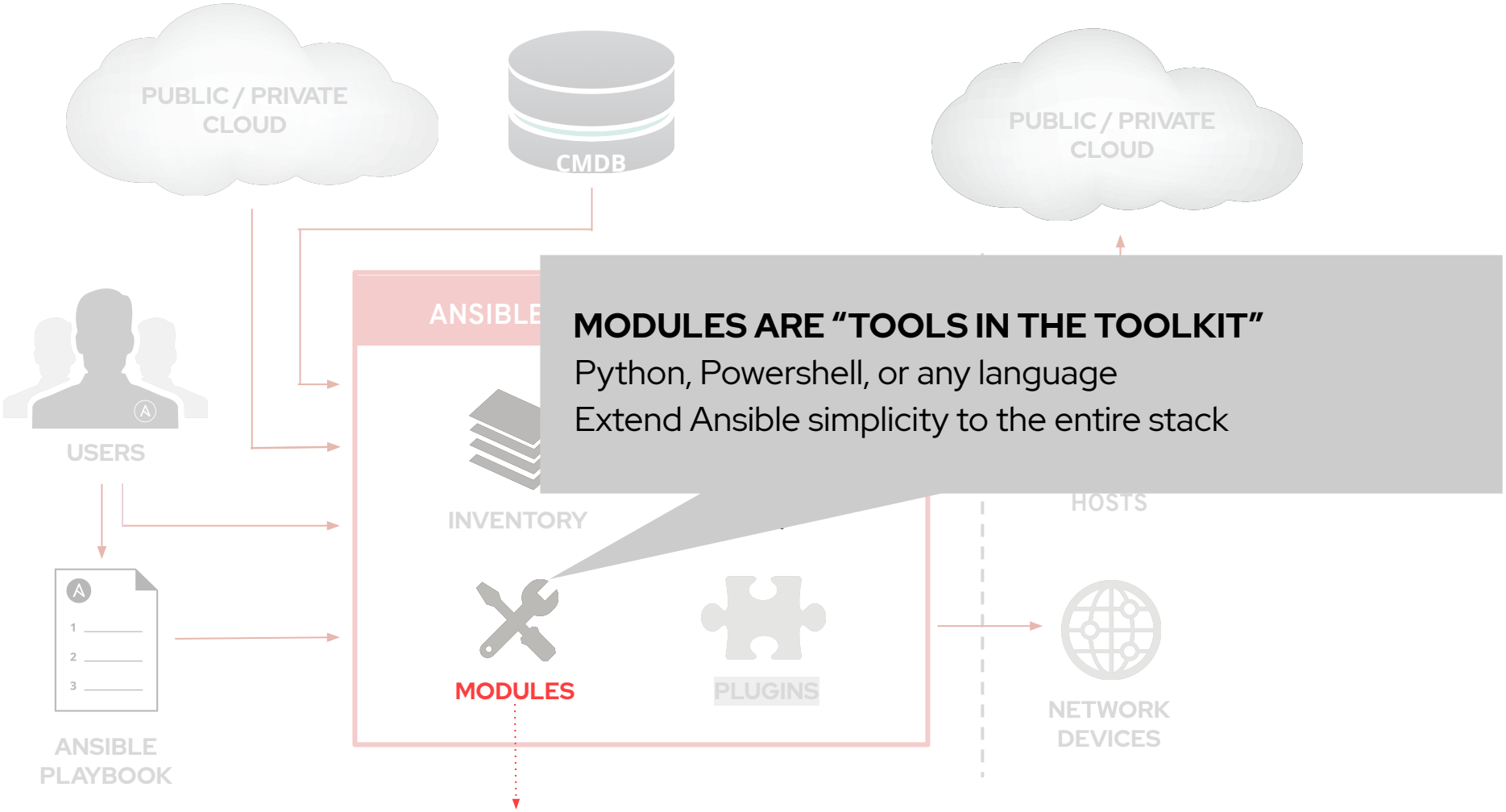
More efficient & more secure


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION ENGINE
USERS
INVENTORY
CLI
HOSTS
MODULES
PLUGINS
NETWORK DEVICES
1
2
3
ANSIBLE PLAYBOOK

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION ENGINE
USERS
PLAYBOOKS ARE WRITTEN IN YAML
Tasks are executed sequentially
Invoke Ansible modules
HOSTS
MODULES
PLUGINS
NETWORK DEVICES
1
2
3
ANSIBLE PLAYBOOK

Red Hat

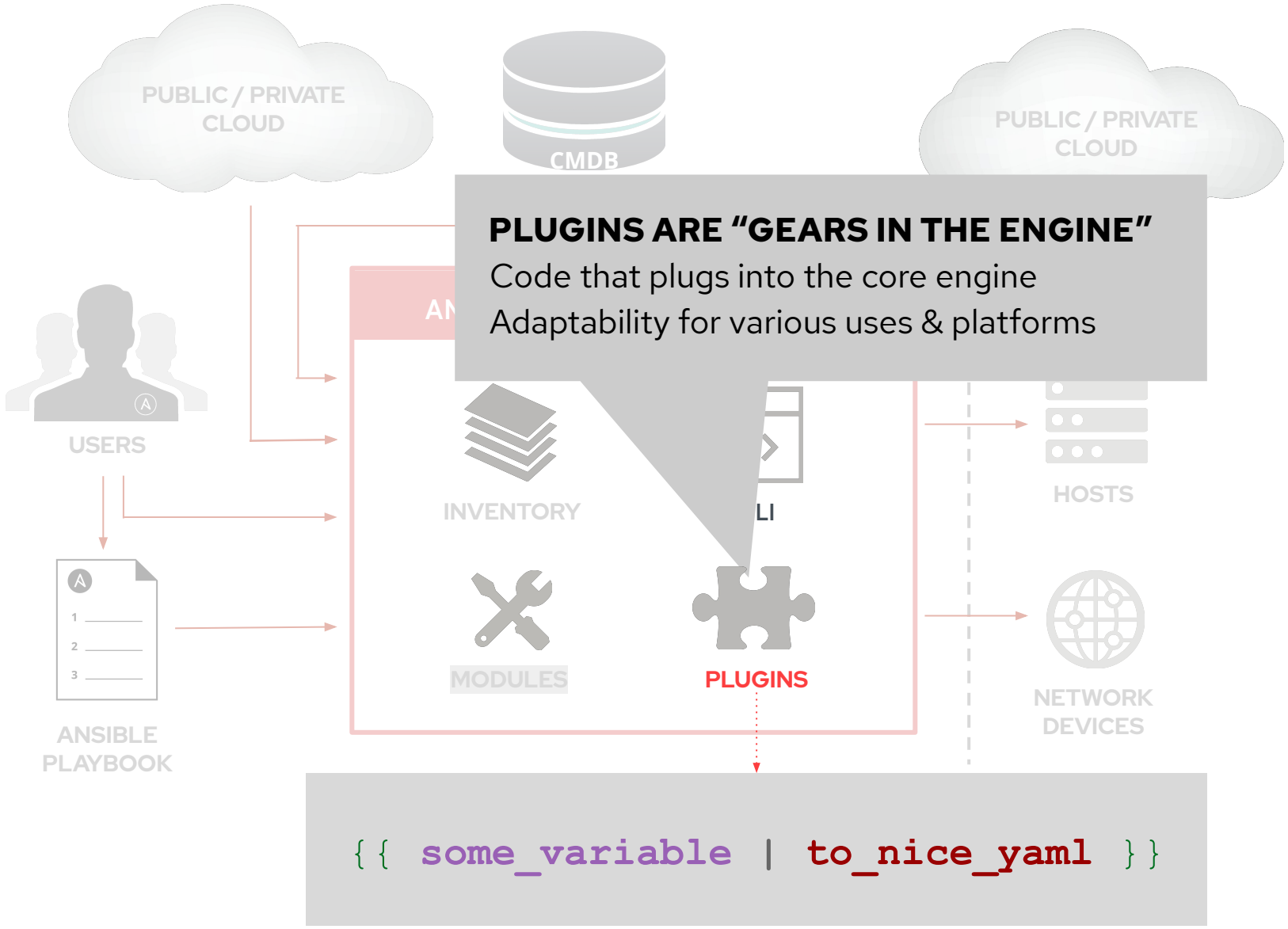


MODULES ARE "TOOLS IN THE TOOLKIT"

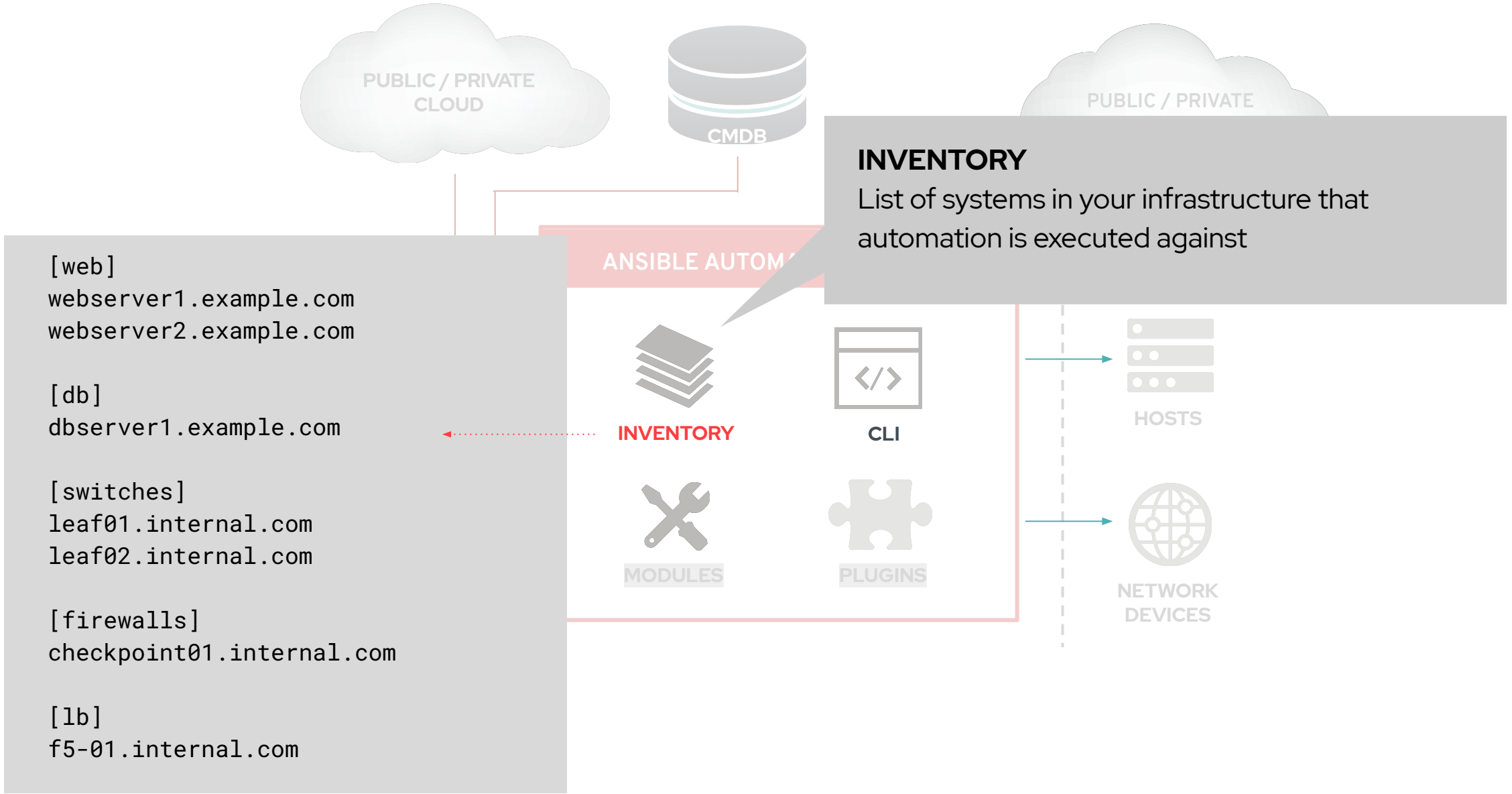
Python, Powershell, or any language

Extend Ansible simplicity to the entire stack

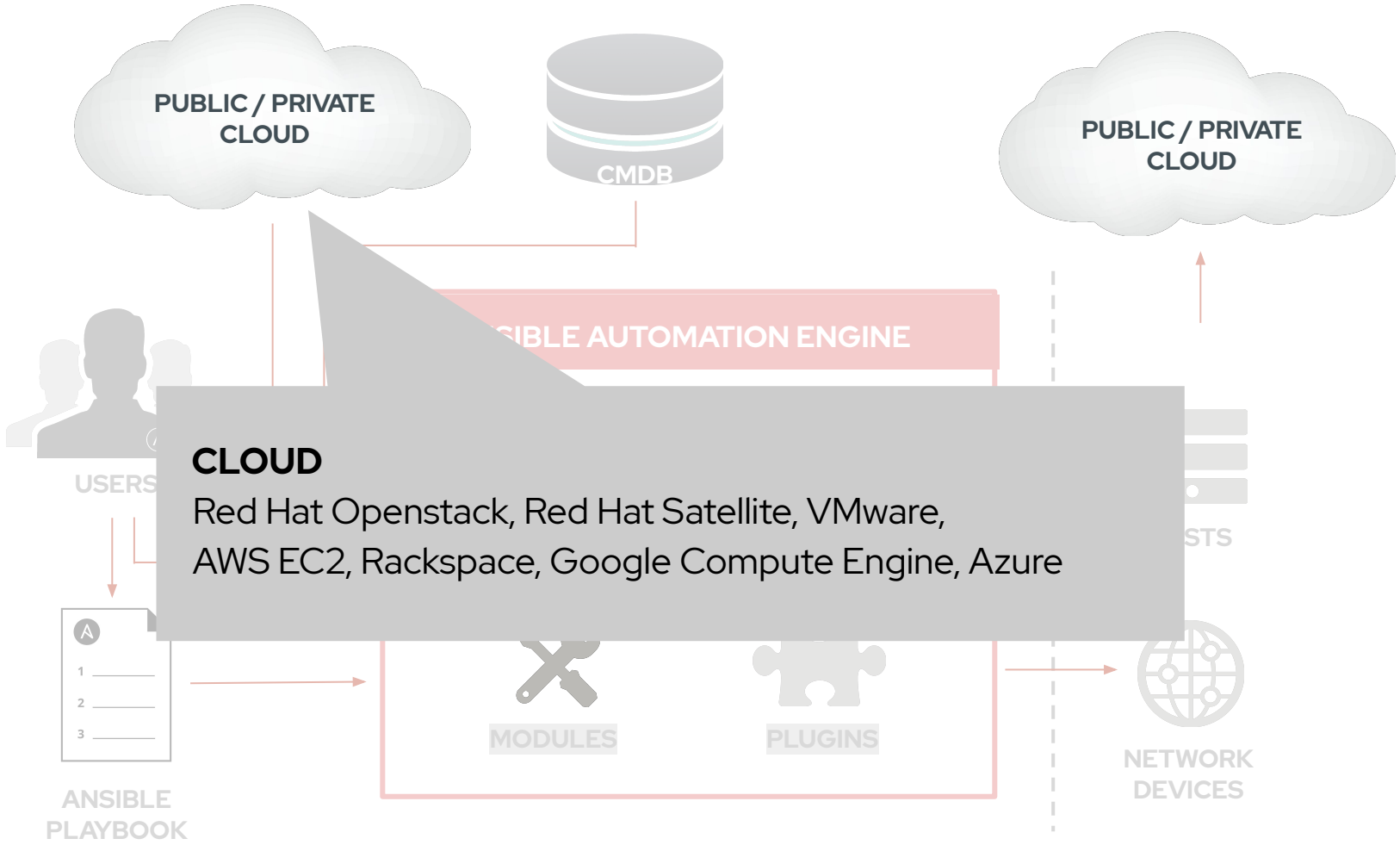
```
- name: latest index.html file is present
  template:
    src: files/index.html
    dest: /var/www/html/
```


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
PLUGINS ARE "GEARS IN THE ENGINE"
Code that plugs into the core engine
Adaptability for various uses & platforms
USERS
INVENTORY
HOSTS
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK
{{ some_variable | to_nice_yaml }}

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE
INVENTORY
List of systems in your infrastructure that automation is executed against
[web]
webserver1.example.com
webserver2.example.com
[db]
dbserver1.example.com
[switches]
leaf01.internal.com
leaf02.internal.com
[firewalls]
checkpoint01.internal.com
[lb]
f5-01.internal.com
ANSIBLE AUTOM
INVENTORY
CLI
HOSTS
MODULES
PLUGINS
NETWORK DEVICES

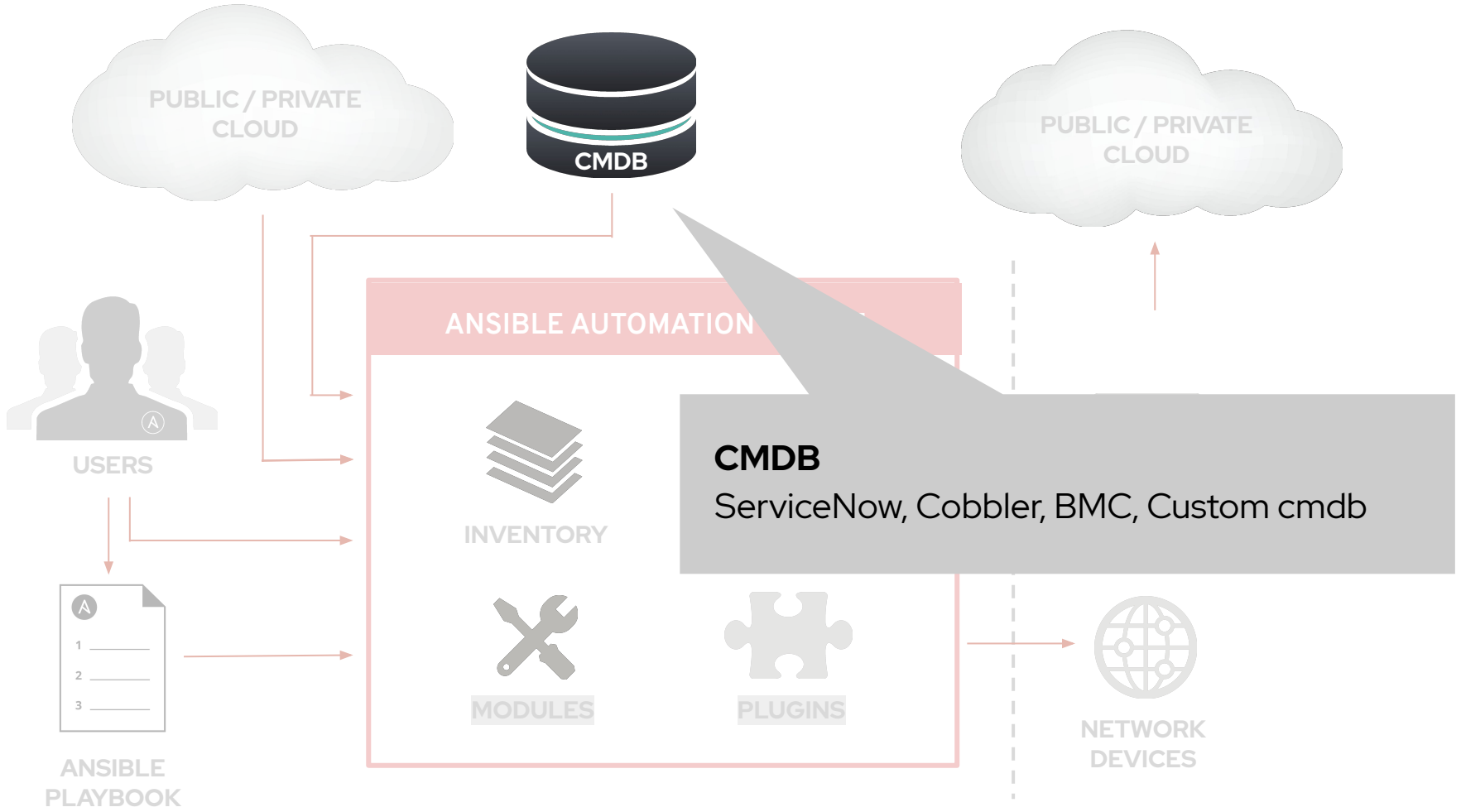
Red Hat



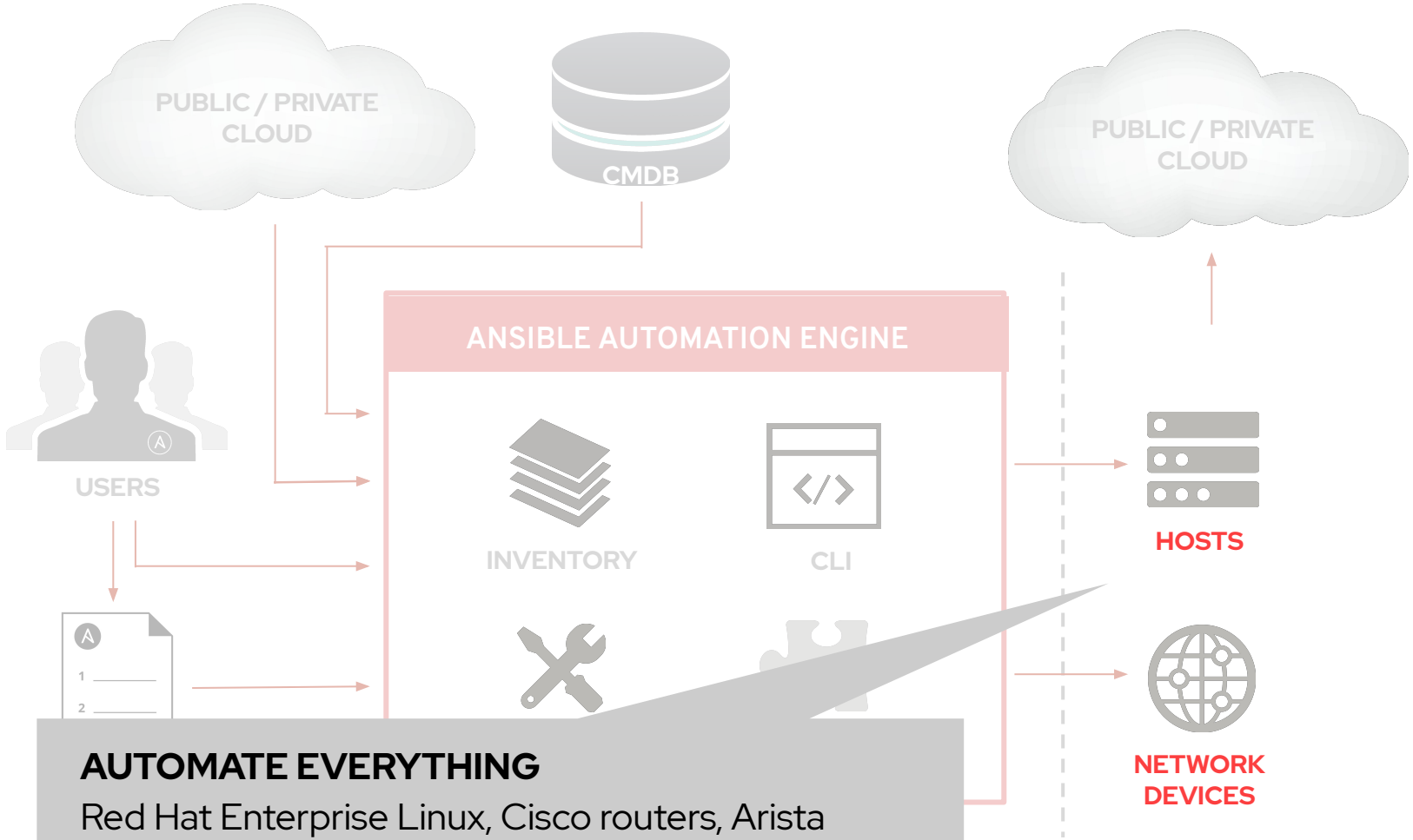
CLOUD

Red Hat Openstack, Red Hat Satellite, VMware,
AWS EC2, Rackspace, Google Compute Engine, Azure

Red Hat

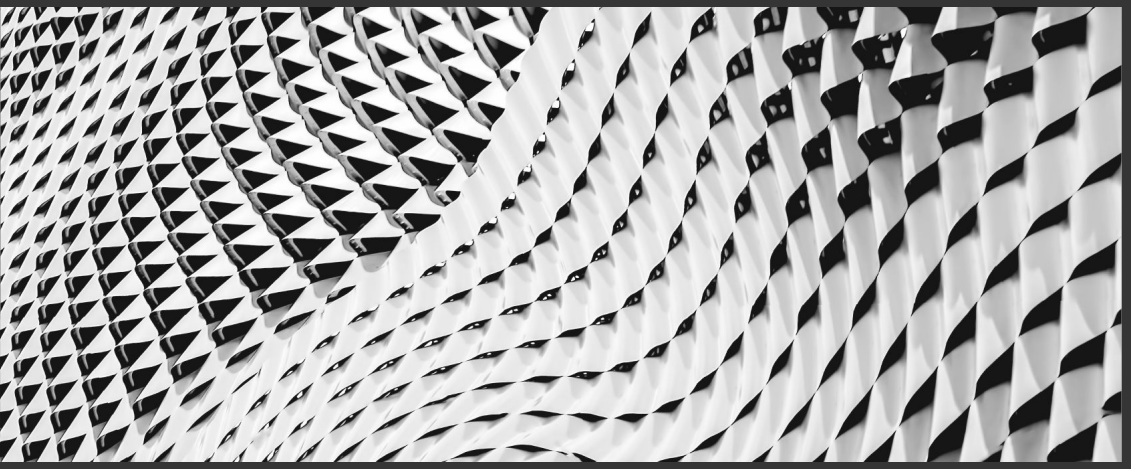

PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION
USERS
INVENTORY
CMDB
ServiceNow, Cobbler, BMC, Custom cmdb
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION ENGINE
USERS
INVENTORY
CLI
HOSTS
NETWORK DEVICES
AUTOMATE EVERYTHING
Red Hat Enterprise Linux, Cisco routers, Arista switches, Juniper routers, Windows hosts, Check Point firewalls, NetApp storage, F5 load balancers and more

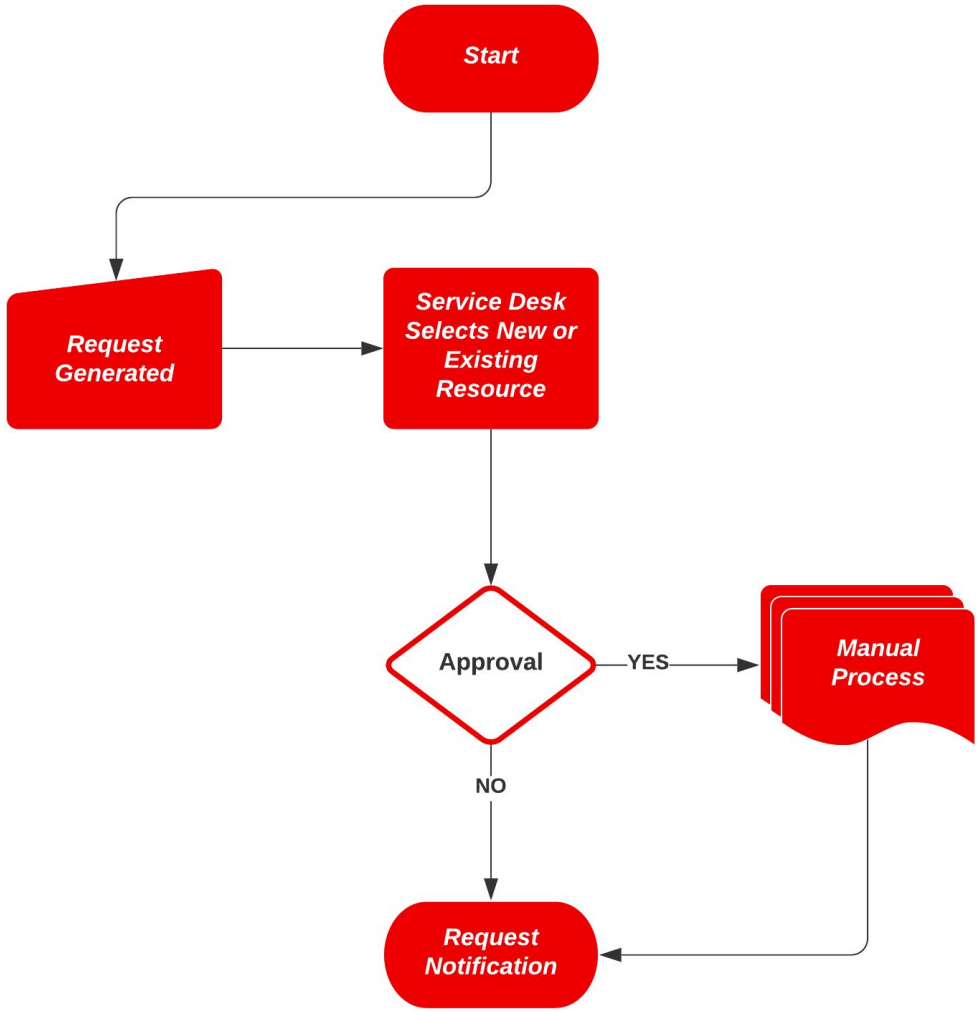
Red Hat

Automating Identity Management with Ansible

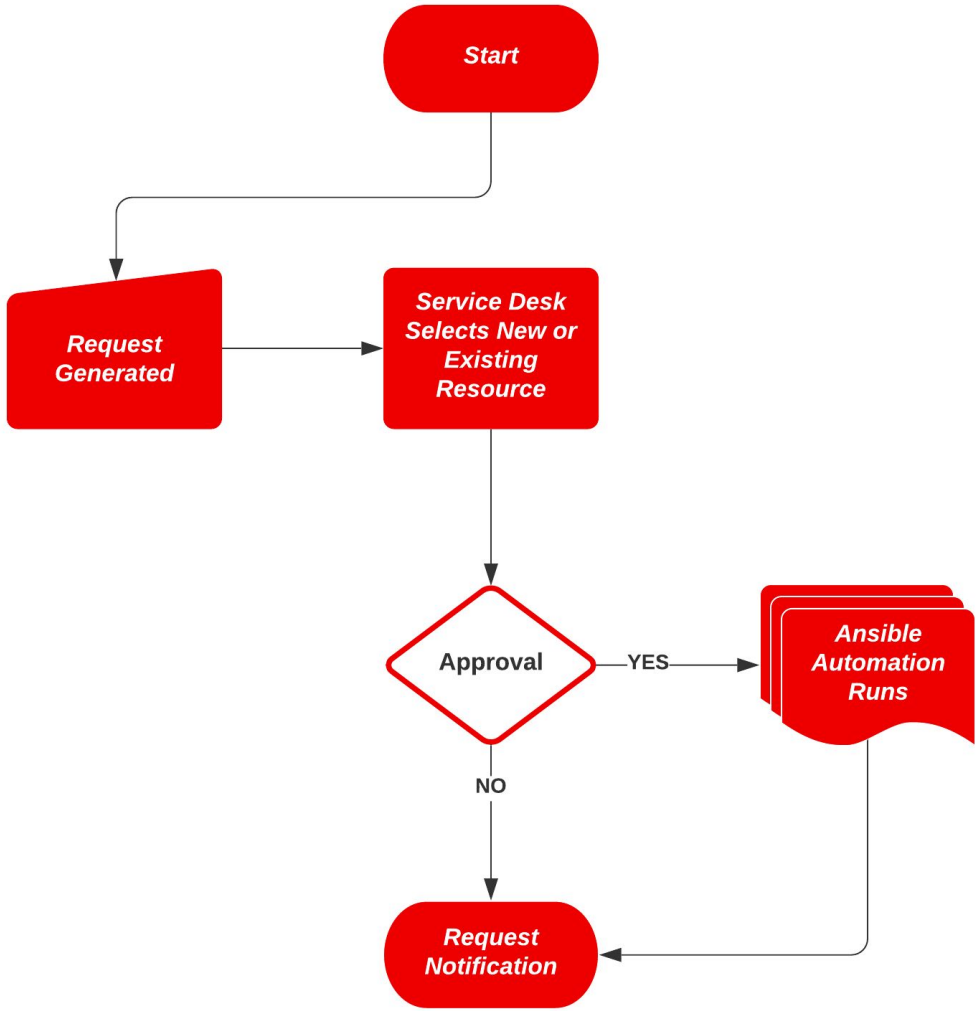


How do you make user, group, host based access control, and sudo rule management easier and allow a non-administrator to add, remove, or change identity resources?

Red Hat

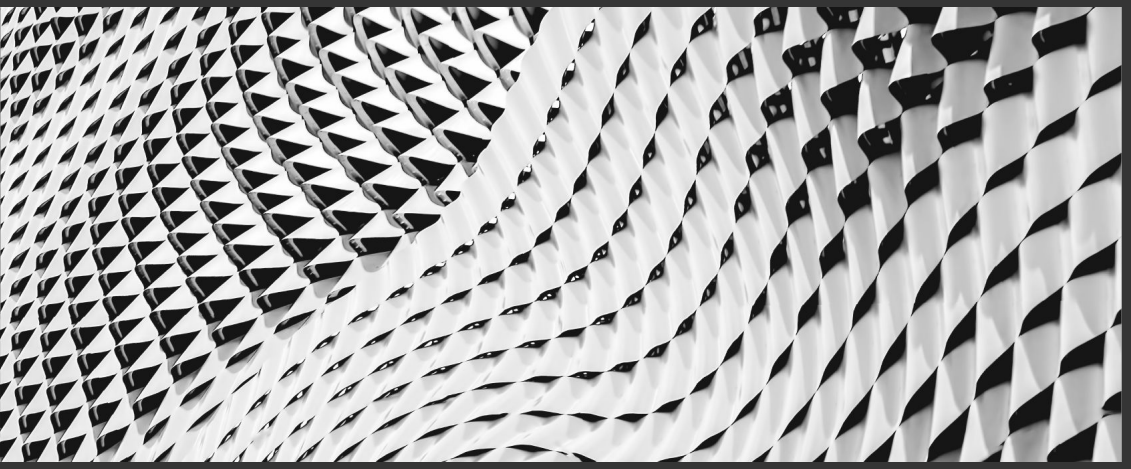


- Request is generated to ticketing system (Service Now, Remedy, etc)
- Service Desk Associate Selects an Existing resource from CMDB or enters new resource details
- Approval Process
- Manual Process if request is approved ***(could take hours or days)***
- Requester is notified of status later and might need to call/email back to get status.



- Request is generated to ticketing system (Service Now, Remedy, etc)
- Service Desk Associate Selects an Existing resource from CMDB or enters new resource details
- Approval Process
- Automation Runs if request is approved ***(COMPLETED IN SECONDS)***
- Requester is notified of status ***immediately*** after automation completes

Ansible Setup Considerations



What do I need to make this work?

Red Hat

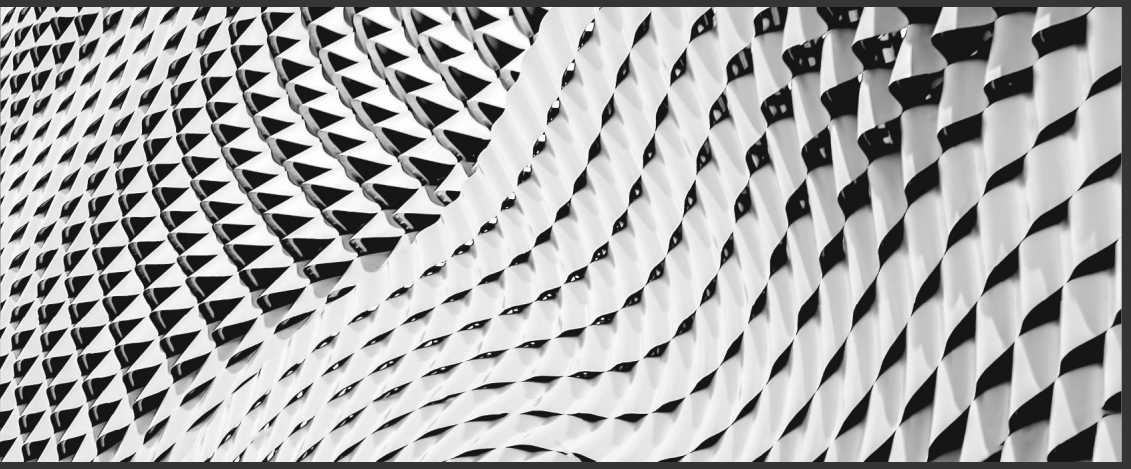
Considerations when using Ansible Engine

- Red Hat Identity Management Master Server in Ansible Inventory
  - To keep things simple, use the name “ipaserver”
- Credentials for IdM user with edit privileges to user/group/HBAC/sudo resources
  - Keep these credentials in a vaulted variable file in your project
    - ansible-vault encrypt ipa_admin_creds.yml
- Install the freeipa/ansible_freeipa collection from Ansible Galaxy
  - Can be installed from a requirements yaml file
    - ansible-galaxy install -r <requirements file>
- Install my bpkrumme/ipa_admin project (or fork it/create your own)
  - Includes requirements file for collections
  - Includes a template (unencrypted) for ipa_admin_creds.yml

Considerations when using Ansible Tower

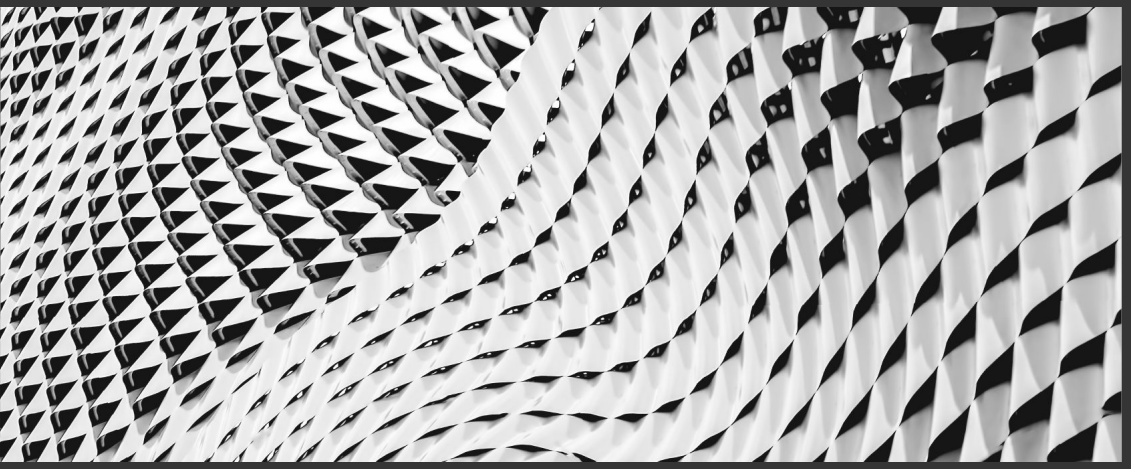
- Red Hat Identity Management Master Server in Ansible Inventory
- Install my bpkrumme/ipa_admin project (or fork it/create your own)
  - Includes requirements file for collections
  - Includes a template for ipa_admin_creds.yml
- Credentials for IdM user with edit privileges to user/group/HBAC/sudo resources
  - Keep these credentials in a vaulted variable file in your project
    - ansible-vault encrypt ipa_admin_creds.yml
- Credential in Ansible Tower to decrypt the vaulted variables
- Job Templates to run the automated tasks
  - Limit to IdM Master Server
  - Create Surveys for required variables

DEMO



Red Hat

Extra Resources



Red Hat

- freeipa/ansible_freeipa collection
  - https://galaxy.ansible.com/freeipa/ansible_freeipa
- My ipa_admin project
  - https://github.com/bpkrumme/ipa_admin
- Red Hat Identity Management Documentation
  - https://access.redhat.com/articles/1586893
- Ansible Documentation
  - https://docs.ansible.com/
- Ansible Tower API Guide
  - https://docs.ansible.com/ansible-tower/latest/html/towerapi/index.html

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat