

Управление платформой Red Hat Virtualization с помощью Ansible Tower

Игорь Малкин

Технический специалист

МОНТ

Всеволод Жмуров

Архитектор ПО

МОНТ

<https://t.me/redhatmont>

redhat@mont.com



MONT
Group of companies



Red Hat

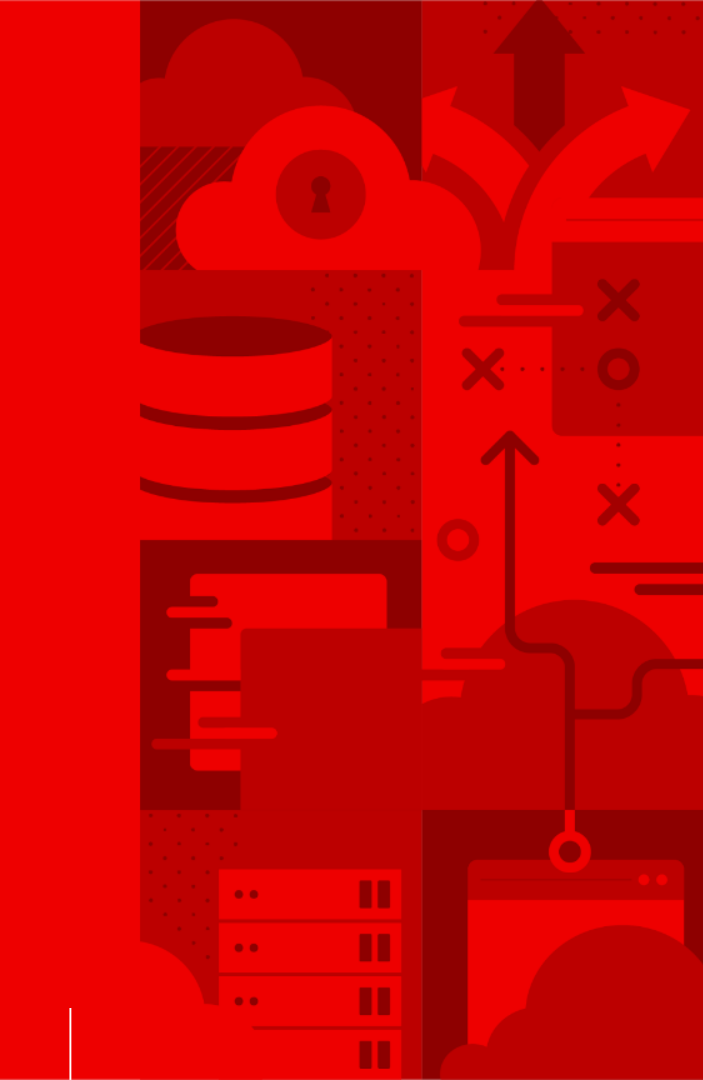
Содержание

1) Red Hat Virtualization

- Обзор продукта
- Что нового в последнем релизе?
- Roadmap - что будет дальше?
- Live Demo

1) Red Hat Ansible Automation

- Обзор продукта
- Зачем нужен Tower?
- Как это использовать?
- Live Demo



Red Hat Virtualization

RED HAT VIRTUALIZATION

Зрелый продукт с давней историей

RED HAT ENTERPRISE VIRTUALIZATION BEATS VMWARE
on the SPECvirt_sc2010 benchmark on both speed and scale

2010

RED HAT ENTERPRISE VIRTUALIZATION 3.1, 3.2
Windows guests NUMA collaboration with HP

2013

RED HAT ENTERPRISE VIRTUALIZATION 3.6
V-2-V migration tool

2015

RED HAT VIRTUALIZATION 4.1
Ansible integration
Native SDN

2017

RED HAT VIRTUALIZATION 4.3
RHEL 8 guest support
SDN compatible with OpenStack 10/13/14
IBM POWER9 support
Ansible integration for RHV Manager

2019

2009

QUMRANET ACQUISITION

2012

RED HAT ENTERPRISE VIRTUALIZATION 3.0
More solution partners
RESTful API
Memory overcommit

2014

RED HAT ENTERPRISE VIRTUALIZATION 3.3, 3.4
OpenStack Neutron integration
Hot Plug CPU
Affinity management
IBM POWER support

2016

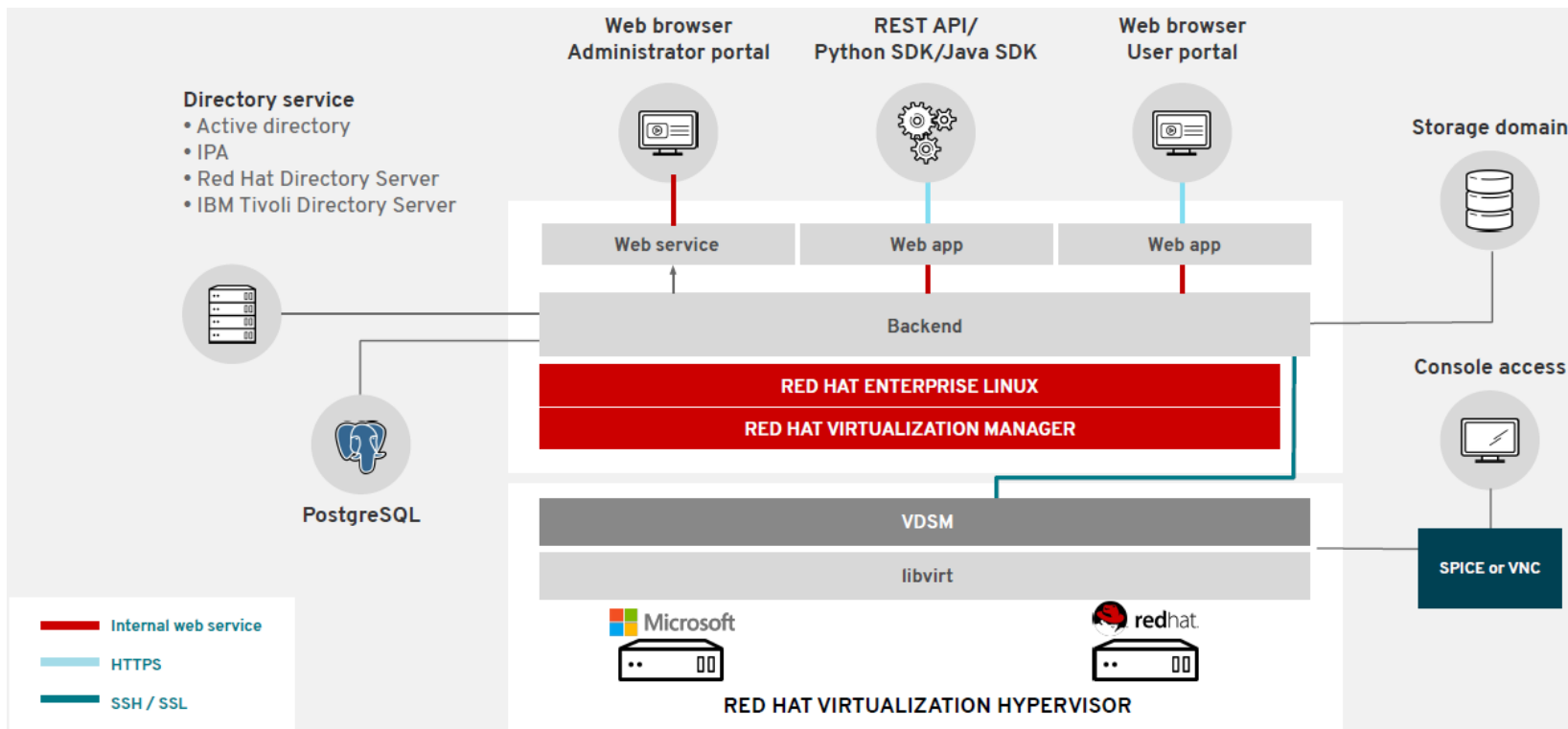
RED HAT VIRTUALIZATION 4.0
10th product release

2018

RED HAT VIRTUALIZATION 4.2
NVIDIA Grid vGPU support
Native DR
New metrics
Store new UI
Cisco ACI

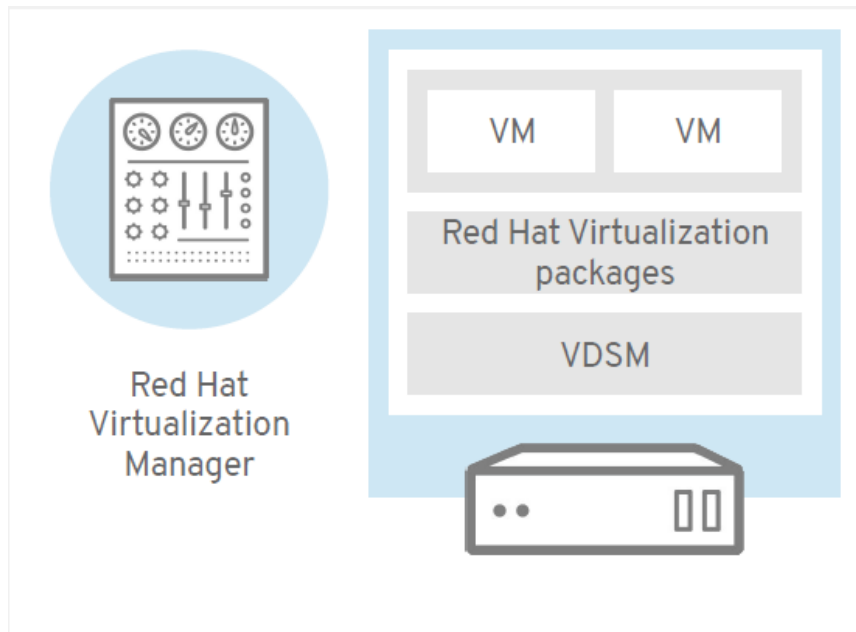
RED HAT VIRTUALIZATION

Архитектура



RED HAT VIRTUALIZATION

Гипервизор - Red Hat Virtualization Hypervisor



QEMU-KVM-RHEV

- **RHEL Co-Engineering** – наследует производительность, масштабируемость, безопасность, стабильность Red Hat Enterprise Linux
 - **Экосистема***: Делит с Red Hat Enterprise Linux экосистему* программных и аппаратных решений
 - **Хост**: 384 физических ядра CPU на гипервизор, 12TB RAM (64TB теоретический максимум)
 - **Гости (VM)**: 240 vCPU, 4TB RAM
 - **Дата-центр**: 200 хостов, неограниченное число VM
 - **RHV Manager**: несколько Дата-центров и кластеров
 - **Cross-Platform**: Microsoft-certified для Windows VM
- VDSM Hooks** - механизм запуска на хосте скриптов как реакции на события

RED HAT VIRTUALIZATION

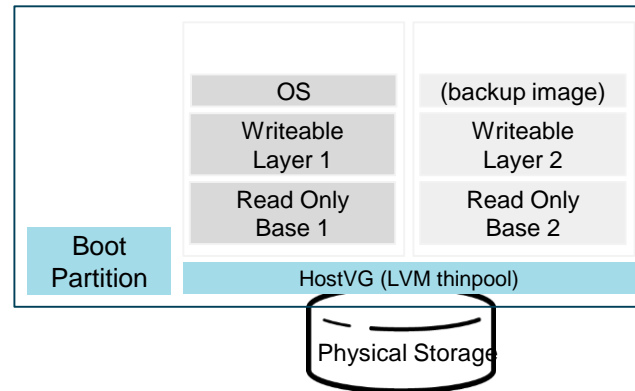
Гипервизор - Red Hat Virtualization Hypervisor

1) “Next Generation” Node

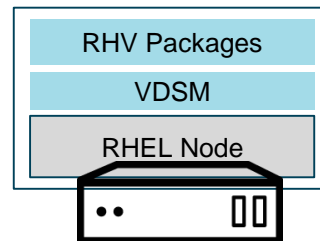
- RHV-H – версия RHEL, предназначенная быть гипервизором
- Развертывание с помощью ISO, PXE, USB, клонов,...
- Файловая система с возможностью записи (в отл. от RHEV-H)
- Оптимизированный установщик Anaconda
- “Cockpit” - административная GUI консоль - встроен
- Политики безопасности и сервисы оптимизированы для VM

2) “Thick (RHEL)” Node

- RHV 4 может использовать RHEL 7 как хост
- Большой размер хоста (HDD, RAM)
- QEMU-KVM заменяется QEMU-KVM-RHV
- RHV Manager конфигурирует политики безопасности и VDSM

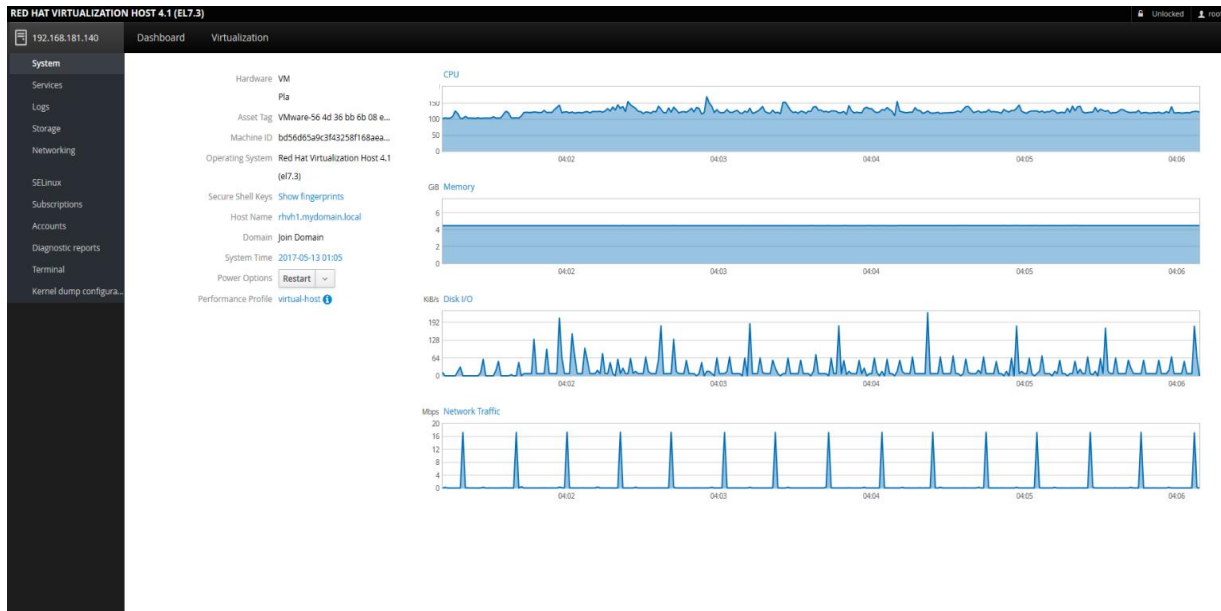


*RHV-H заменил RHEV-H в RHV 4.
Для RHV 3.6 доступен бэкпорт*



RED HAT VIRTUALIZATION

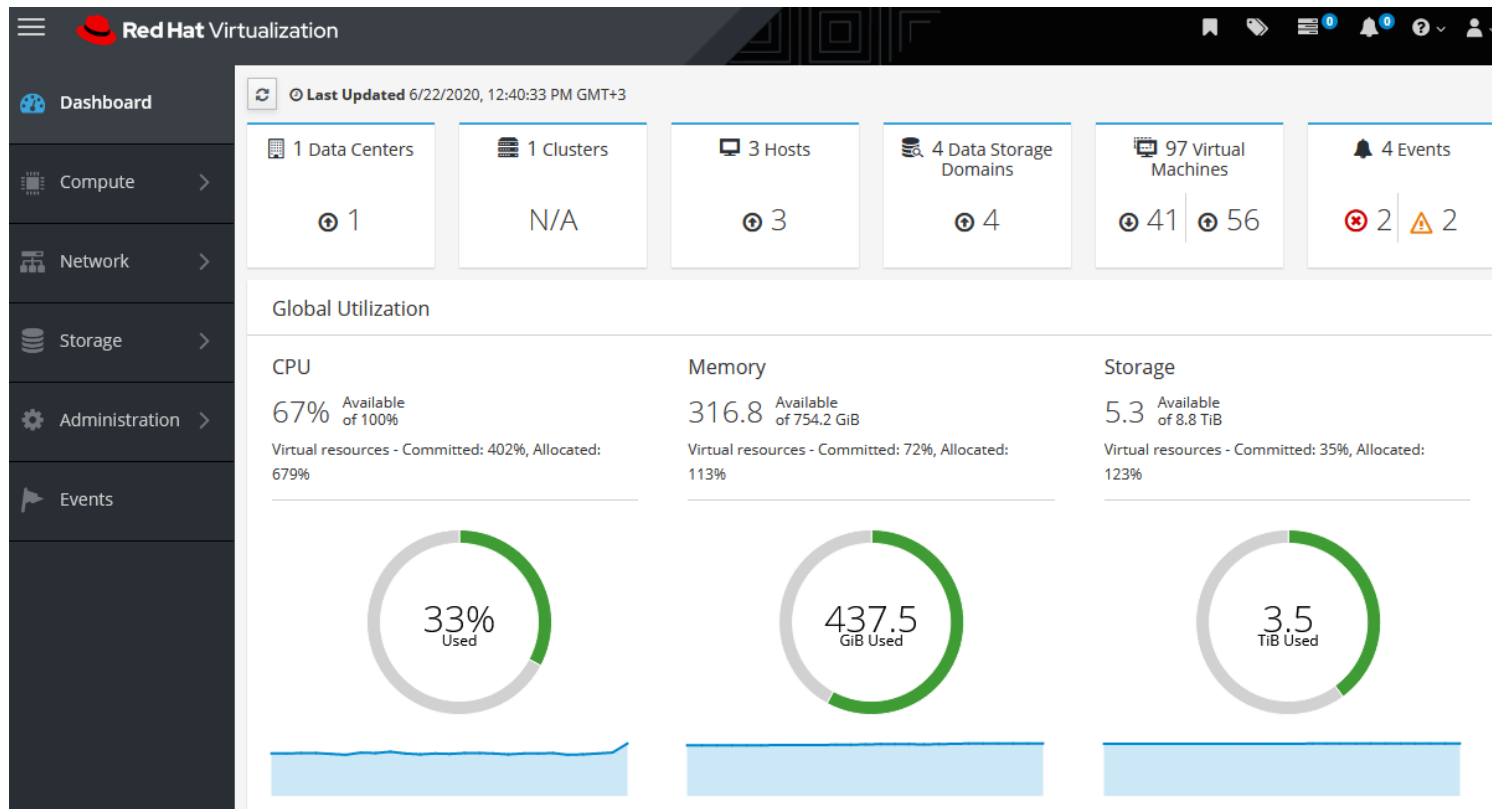
Панель управления Cockpit



- Включена “по умолчанию” в Red Hat Virtualization Host установочный образ, может быть добавлена на RHEL host
- Используется для настройки сетей, хранилища, активации тюнинг-профилей и подписок, и других задач. Также доступен CLI
- Позволяет просматривать метрики загрузки подсистем хоста
- Из общего веб-интерфейса можно провести развертывание RHV Manager как VM (Hosted Engine, в т.ч. с Gluster), с HA - в GUI визарде
- Доступ по HTTPS

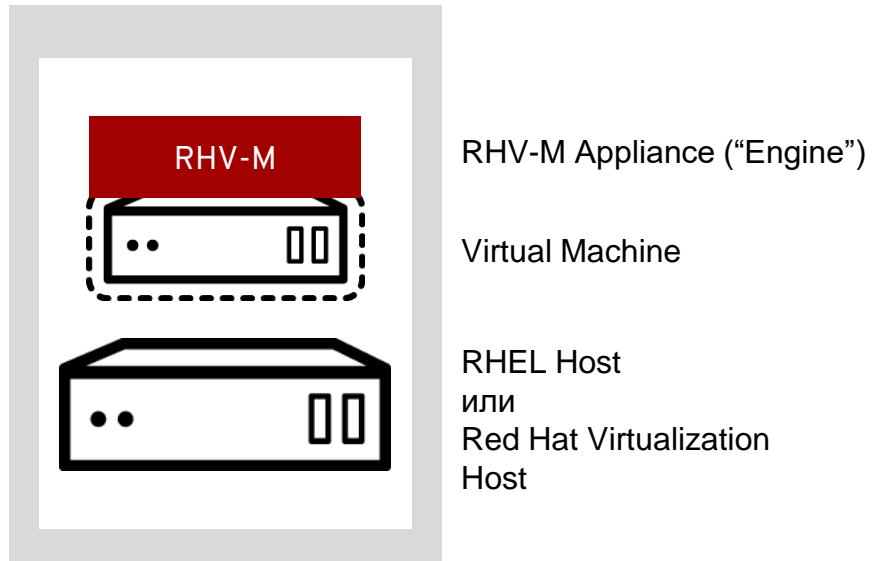
RED HAT VIRTUALIZATION

Менеджер управления



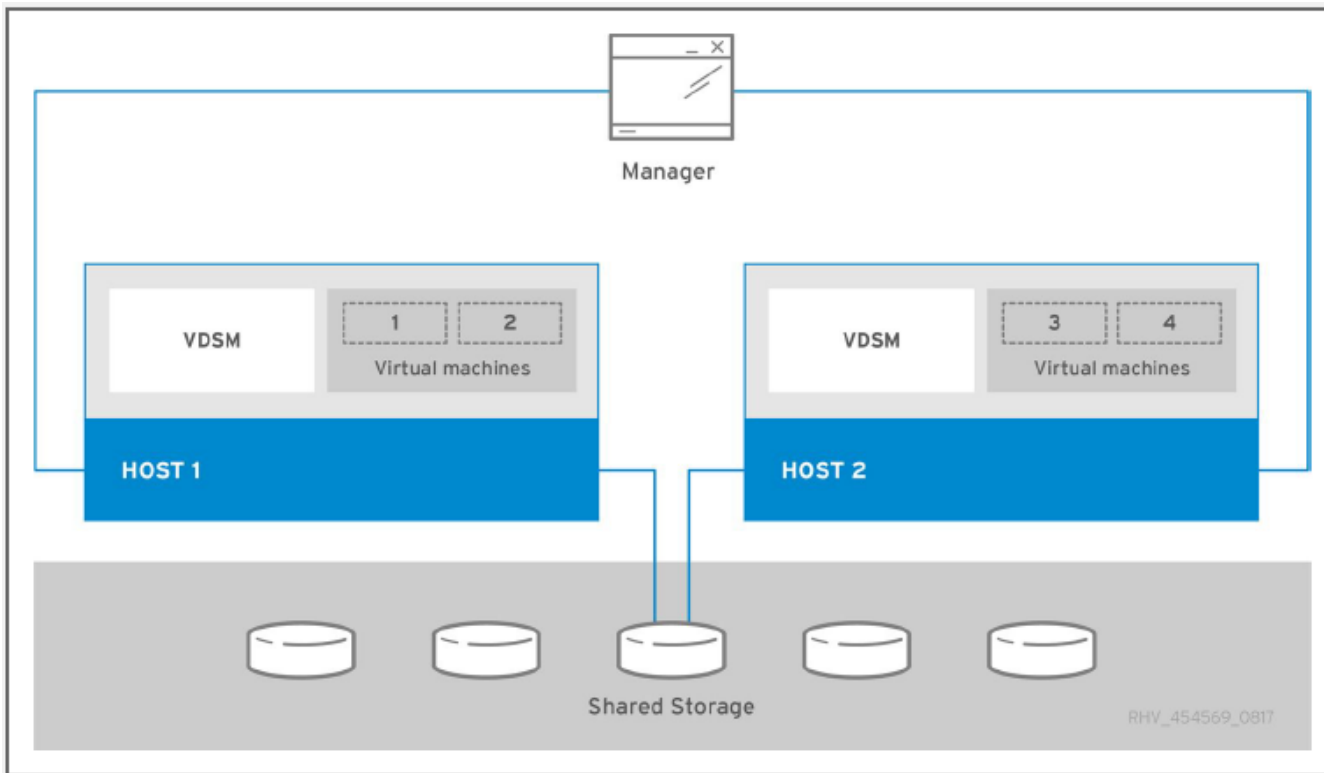
Варианты установки RHVM

- 3 основных варианта развертывания RHV:
 - Standard (non-HA)
 - Hosted Engine with RHEL
 - Hosted Engine with RHVH
- “Engine” - синоним Red Hat Virtualization Manager
- Self-Hosted Engine также обозначается как “Hosted Engine” или “HE”
- В вариантах с Hosted Engine RHV-M работает как виртуальный апплаенс
- Для RHV-M доступен готовый **.ova** образ, но его можно запустить только на **RHV**;
- Если надо разместить RHV-M на VMware - RHEL с “yum install rhevm” + “engine-setup”

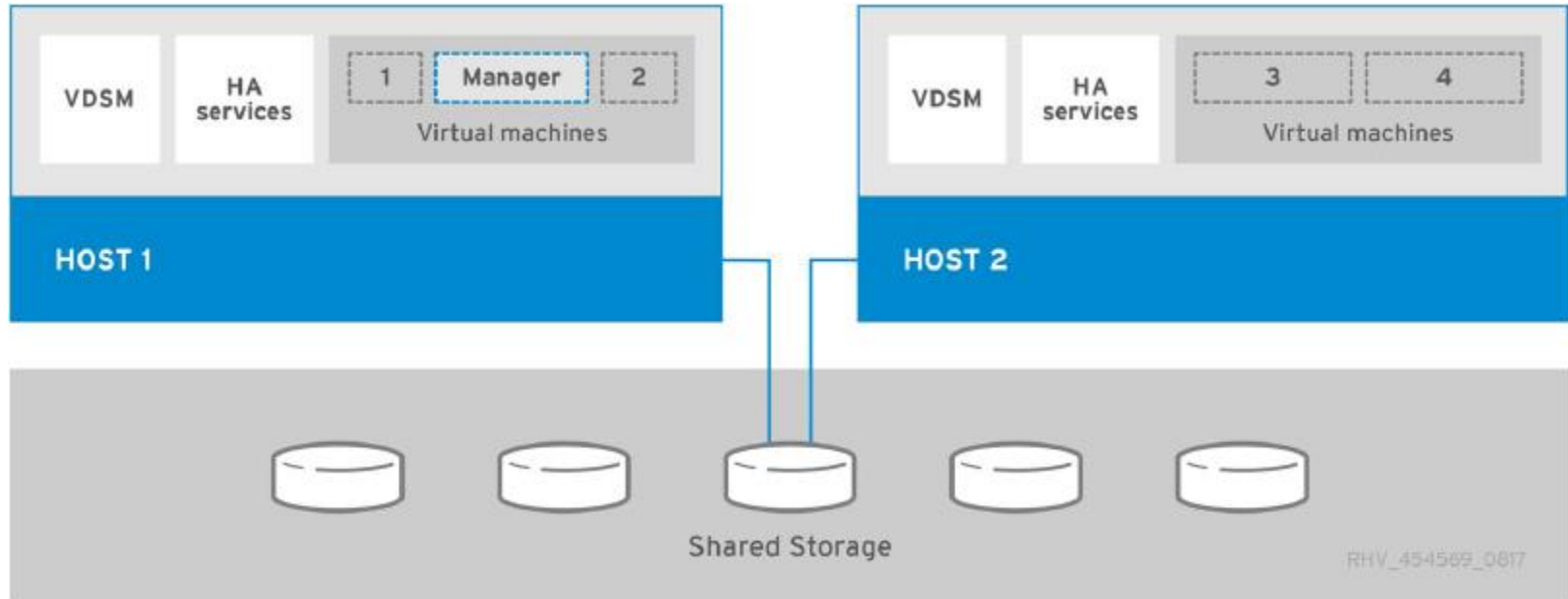


нужен DNS! forward+reverse, не hosts

Варианты установки RHV - Standard



Варианты установки RHV - Self-Hosted Engine



Важность RED HAT VIRTUALIZATION MANAGER

Что случится если RHV-M упадет?

RHV-M это мозг платформы - если он упадет, то:

- Не будет возможности управлять ресурсами (compute, network, storage, пользователи)
- Нет доступа к REST API (backup, recovery, reporting, automation)
- Нет сервисов для виртуальных ресурсов (HA, load balance, optimization, quotas, QoS)

Если какие-либо виртуальные ресурсы (compute, storage, network) работают, то они продолжат работать несмотря на недоступность RHV-M.

RED HAT VIRTUALIZATION

Основной функционал версии 4.3

Core	Live Migration	HA / DR	Affinity / Anti-Affinity	CPU Pinning
	NUMA Support	Resource Reservation	Large Page support	NVIDIA vGPU
	VM templates	Hot Add Memory & CPU	Migrate/Import VMs	Overcommit
Network	VLAN tagging	PCI Passthrough	Native SDN (OVS) / Openstack Neutron	Network QoS
	NIC bonding	Jumbo frames	IPV6 (guest)	Network labels
Storage	Storage Live Migration	Thin/Thick Provisioning	Live Snapshots/Merge	SCSI, NFS, FC, GlusterFS
Security	RBAC & Tiered Access	Firewall	sVirt	SELinux
Mgmt & APIs	Browser Based Mgmt	Python & Java SDKs	REST APIs	Backup API

Red Hat Virtualization 4.3

Что уже добавлено?

RED HAT VIRTUALIZATION 4.3

Единая экосистема решений Red Hat



Best for virtualized workloads that
require infrastructure to provide
SLAs



Best for private cloud deployment
for cloud-native apps



Best for cloud-native applications

RED HAT VIRTUALIZATION 4.3

Что уже есть сейчас?

- [SAP HANA certification](#)
- Полностью автоматизированный инсталлятор для OpenShift 4.4
- Интеграция с проактивным сервисом Red Hat Insights
- Поддержка MS Windows 2019
- AMD EPYC processor support
- Support for IBM POWER9 systems
- Поддержка OpenStack Controller Nodes
- “High performance” профиль для виртуальных машин
- **Nested virtualization (TECH PREVIEW)**
- **Import Debian and Ubuntu VMs from VMware and Xen (TECH PREVIEW)**
- **Mobile (Android) app: moVirt (TECH PREVIEW)**

Red Hat Virtualization 4.4 Beta Уже доступна!

RED HAT VIRTUALIZATION 4.4 Beta

Информация о релизе

- Red Hat Enterprise Linux 8 - базовая операционная система
- Cinderlib Integration - поддержка Ceph Storage
- Улучшены алгоритмы работы HA
- [Поддержка kubevirt в качестве External Provider](#)
- Changed Block Tracking (CBT): incremental backup без создания СНЕПШОТОВ

Red Hat Virtualization

Интеграция с Ansible Automation

RED HAT VIRTUALIZATION

Интеграция с Ansible Automation



EXTENDED AUTOMATION FUNCTIONALITY FOR RED HAT VIRTUALIZATION

› Red Hat Virtualization and Red Hat Ansible Automation are integrated in order to provide streamlined configuration for:

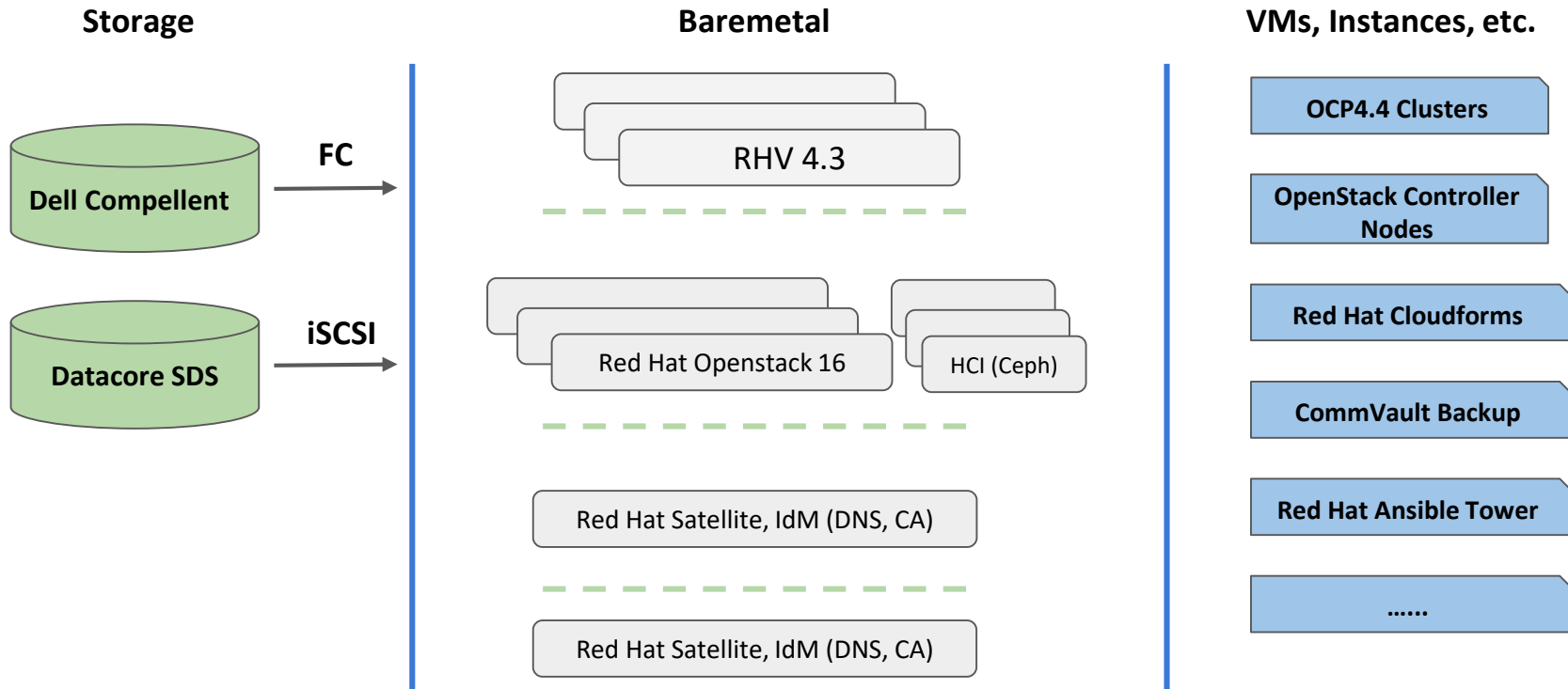
- Virtual machines, templates, and pools
- Networks, storage, hosts, and datacenters
- Red Hat Virtualization Manager
- Disaster recovery
- Updates

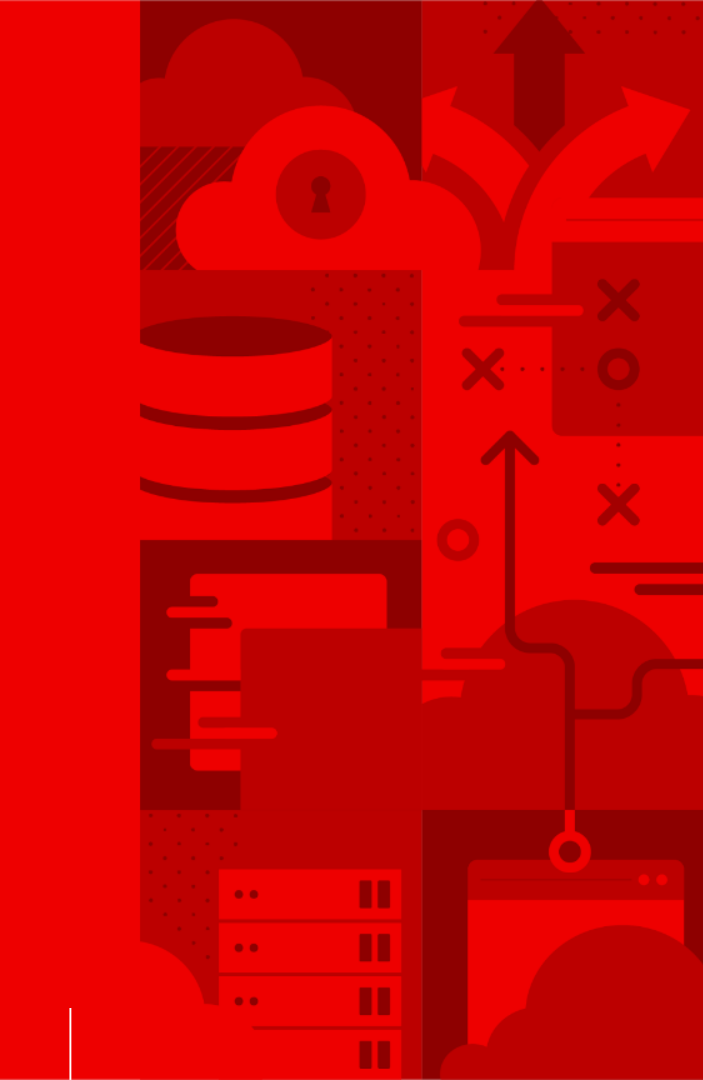
› Automation functionality:

- **Removes** manual steps from deployment and reconfiguration
- **Streamlines** operations, freeing up resources to focus on strategic initiatives
- **Provides** a single support stack for virtualization and automation
- **Includes** and supports Ansible roles for Red Hat Virtualization

DEMO

Архитектура Демо-стенда





Red Hat Ansible Automation

Что можно делать, используя Ansible?

Автоматизация, развертывание, управление различными IT структурами

Do this...

Orchestration

Configuration
Management

Application
Deployment

Provisioning

Continuous
Delivery

Security and
Compliance

On these...

Firewalls

Load Balancers

Applications

Containers

Clouds

Servers

Infrastructure

Storage

Network Devices

And more...

RED HAT ANSIBLE AUTOMATION

Основные преимущества



Просто

- Простой язык на основе YAML
- Не требует навыков программирования
- Последовательное выполнения задач
- Сценарий прост и понятен для других команд



Функционально

- Установка приложений
- Управление изменениями
- Автоматизация рабочих процессов
- Настройка активного сетевого оборудования



Безопасно

- Не требует агента на клиенте
- OpenSSH & WinRM в качестве транспорта
- Эскалация привилегий
- Проверка на соответствие стандартам компании

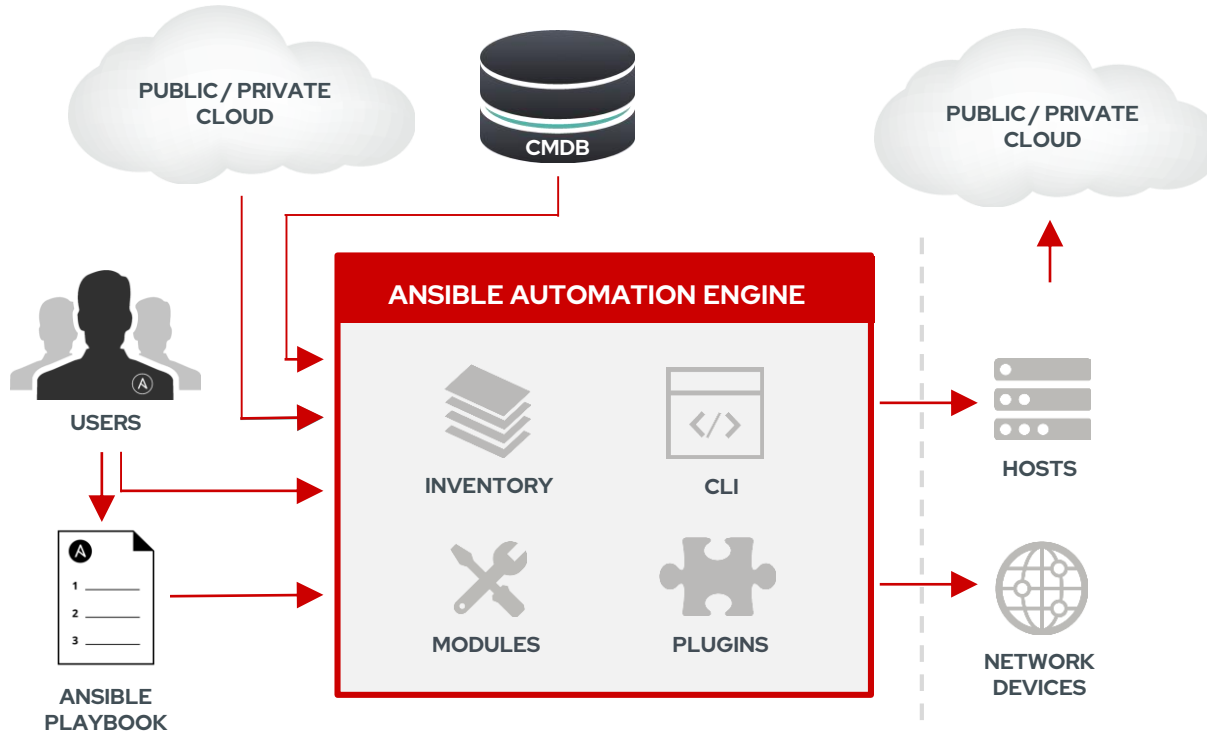
Ansible automates technologies you use

Time to automate is measured in minutes

Cloud	Virt & Container	Windows	Network	Security	Monitoring
AWS	Docker	ACLs	A10	Checkpoint	Dynatrace
Azure	VMware	Files	Arista	Cisco	Datadog
Digital Ocean	RHV	Packages	Aruba	CyberArk	LogicMonitor
Google	OpenStack	IIS	Cumulus	F5	New Relic
OpenStack	OpenShift	Regedits	Bigswitch	Fortinet	Sensu
Rackspace	+more	Shares	Cisco	Juniper	+more
+more		Services	Dell	IBM	
Operating Systems	Storage	Configs	Extreme	Palo Alto	Devops
RHEL	Netapp	Users	F5	Snort	Jira
Linux	Red Hat	Domains	Lenovo	+more	GitHub
Windows	Storage	+more	MikroTik		Vagrant
+more	Infinidat		Juniper		Jenkins
	+more		OpenSwitch		Slack
			+more		+more

RED HAT ANSIBLE ENGINE

Ахитектура



Пример плейбука

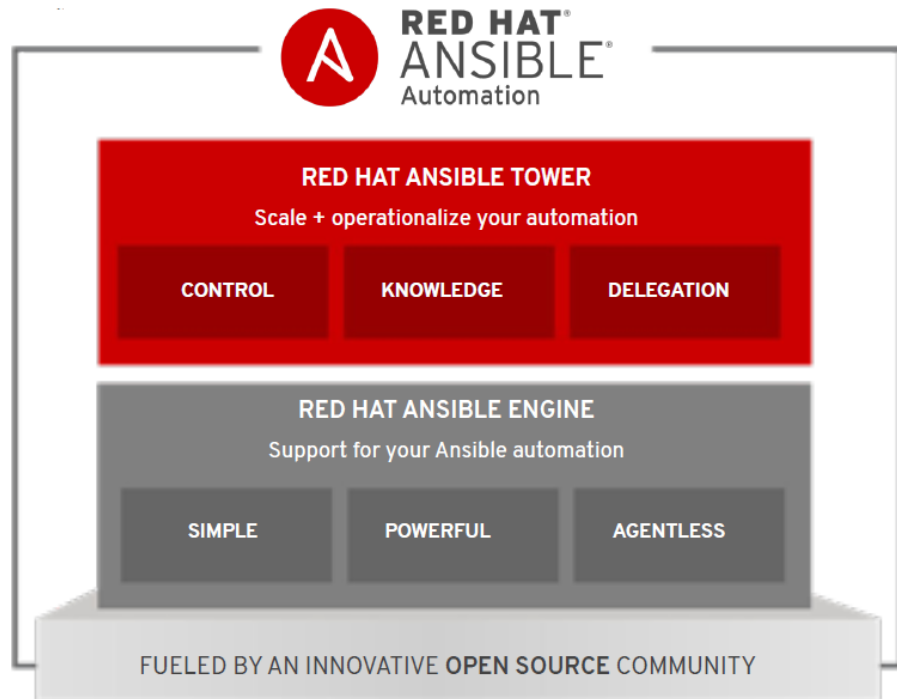
```
---  
- name: install and start apache  
  hosts: web  
  become: yes  
  
  tasks:  
    - name: httpd package is present  
      yum:  
        name: httpd  
        state: latest  
  
    - name: latest index.html file is present  
      template:  
        src: files/index.html  
        dest: /var/www/html/  
  
    - name: httpd is started  
      service:  
        name: httpd  
        state: started
```

RED HAT ANSIBLE AUTOMATION

Ansible Tower vs Ansible

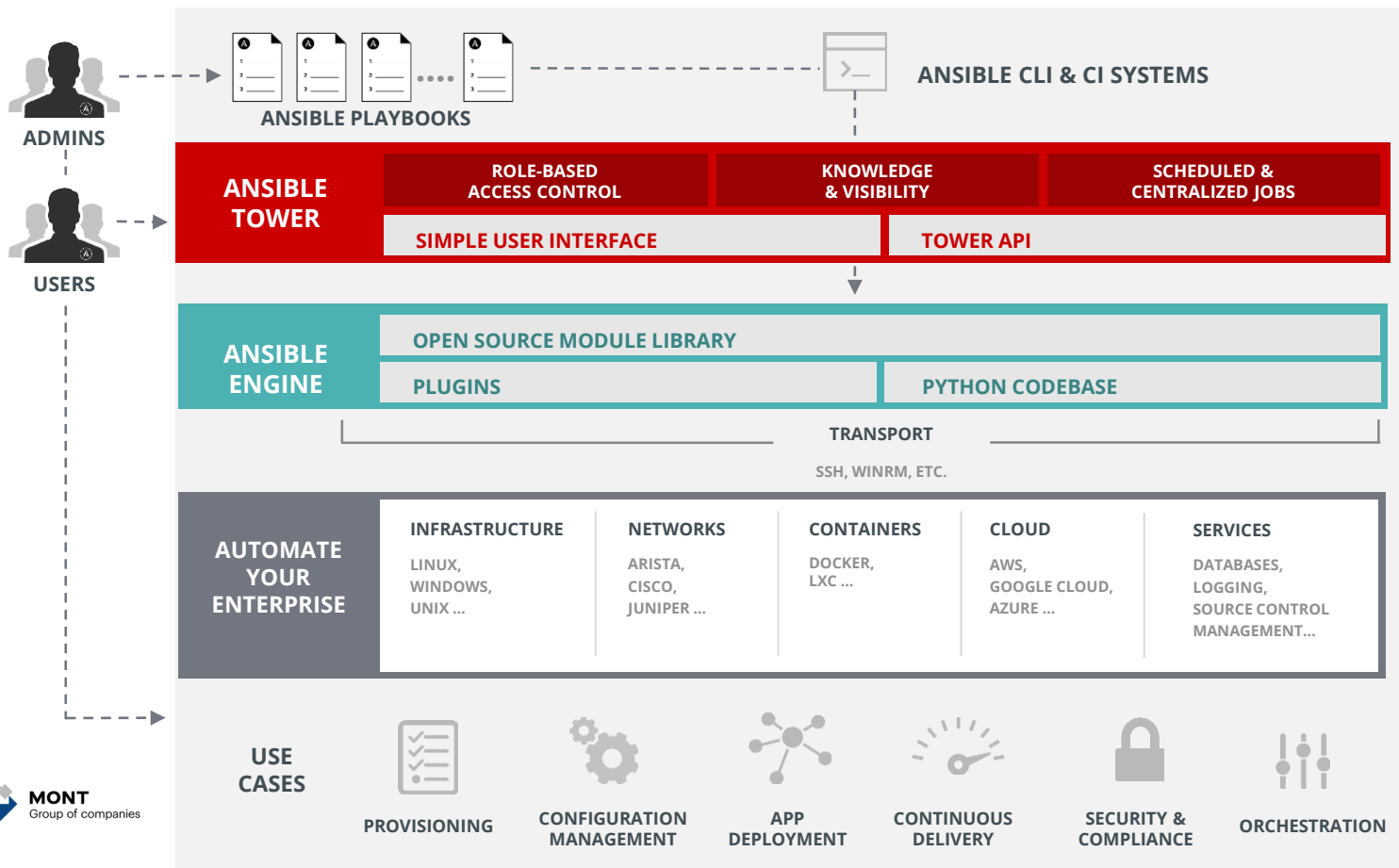
Ansible - проект сообщества, спонсируемый Red Hat. Это простой язык автоматизации, который описывает желаемое состояние инфраструктуры с помощью Ansible Playbooks.

Ansible Tower - это фреймворк корпоративного применения Ansible для контроля, управления и обеспечения безопасности автоматизации с функциями UI и RESTful API.



RED HAT ANSIBLE TOWER

Архитектура



Red Hat Ansible Tower

Push button

Любой пользователь может запустить выполнение задания по кнопке прямо сейчас, завтра, каждый вторник, одним словом - когда угодно.

Кластеризация

Подключите несколько узлов Ansible Tower в кластер, чтобы реализовать отказоустойчивость и увеличить производительность вашей платформы автоматизации.

RBAC

Создает необходимое разделение и изоляцию пользователей и ресурсов. Пользователи могут безопасно использовать Ansible Tower для работы только с теми системами и только в тех средах, к которым они имеют доступ.

Ad-Hoc

Запускайте задачи на любом хосте с помощью удаленного выполнения команд Ansible Tower. Быстрое добавление пользователей или групп, сброс паролей, перезапуск службы или сервера, исправление критической проблемы безопасности.

Activity Stream

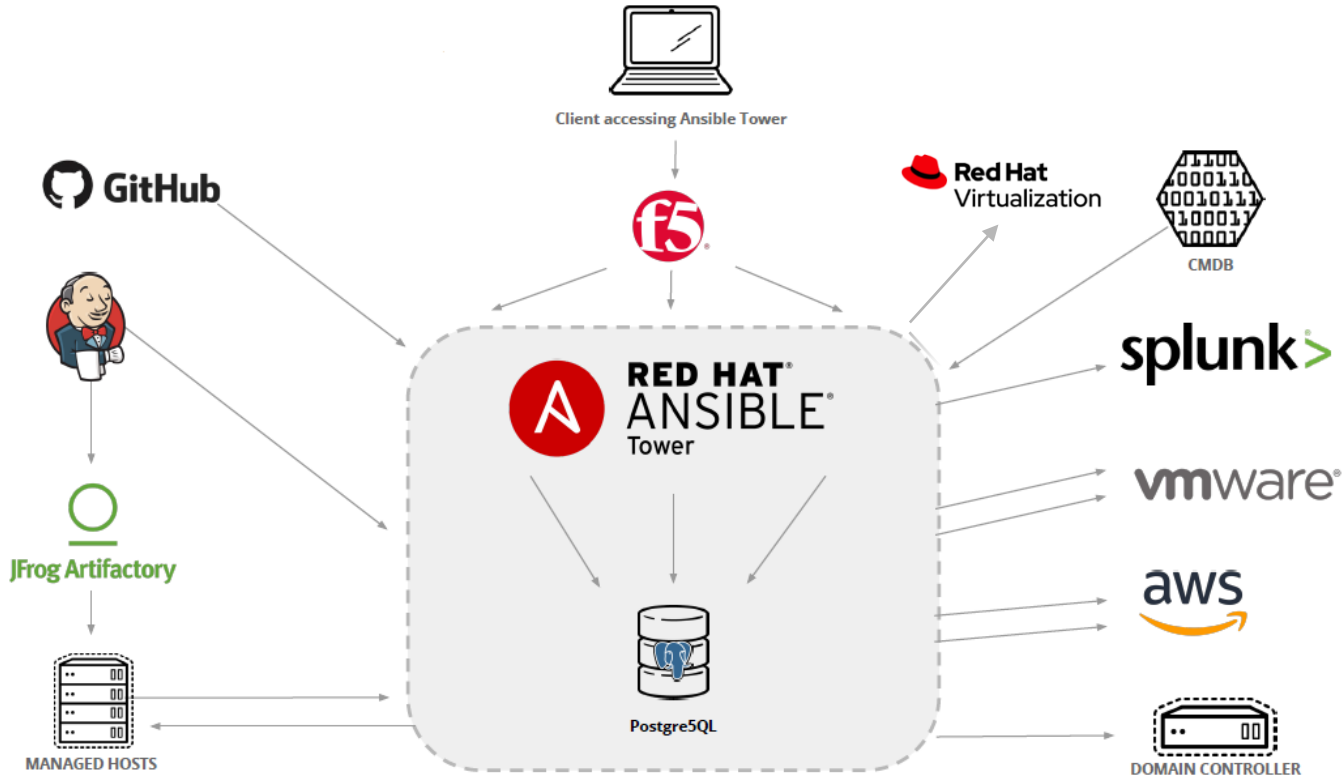
Безопасно хранит данные о каждом выполненном задании и позволяет вам просматривать их позже или экспортировать данные через API Tower.

Workflows

Объединяют любое количество Playbooks для создания единого рабочего процесса. Различные задания могут выполняться в зависимости от успеха или неудачи предыдущего Playbook.

RED HAT ANSIBLE TOWER

Возможности интеграции



RED HAT ANSIBLE TOWER

Интеграция со средствами ИБ



Security information and event management (SIEM)

- Threat analysis module
- High degree of customization



Intrusion detection system and intrusion prevention system (IDS/IPS)

- Most popular standalone IDS
- Integrated into many security products



Modern firewalls

- Leading firewall solution

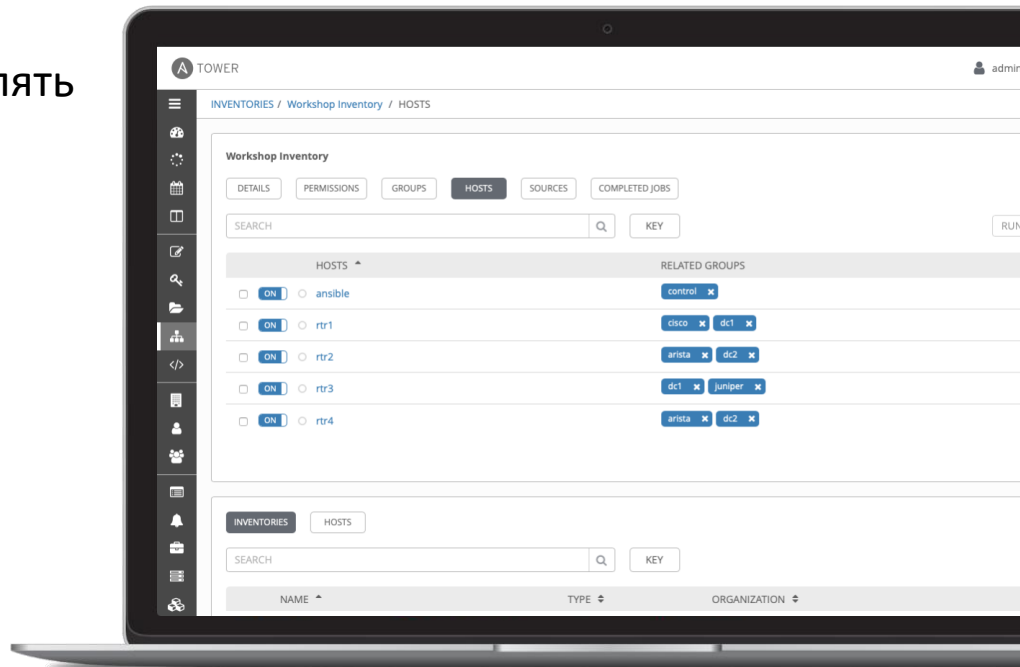
Red Hat Ansible Tower

Основные сущности

Inventory

Список хостов, которыми может управлять Tower и выполнять на них jobs.

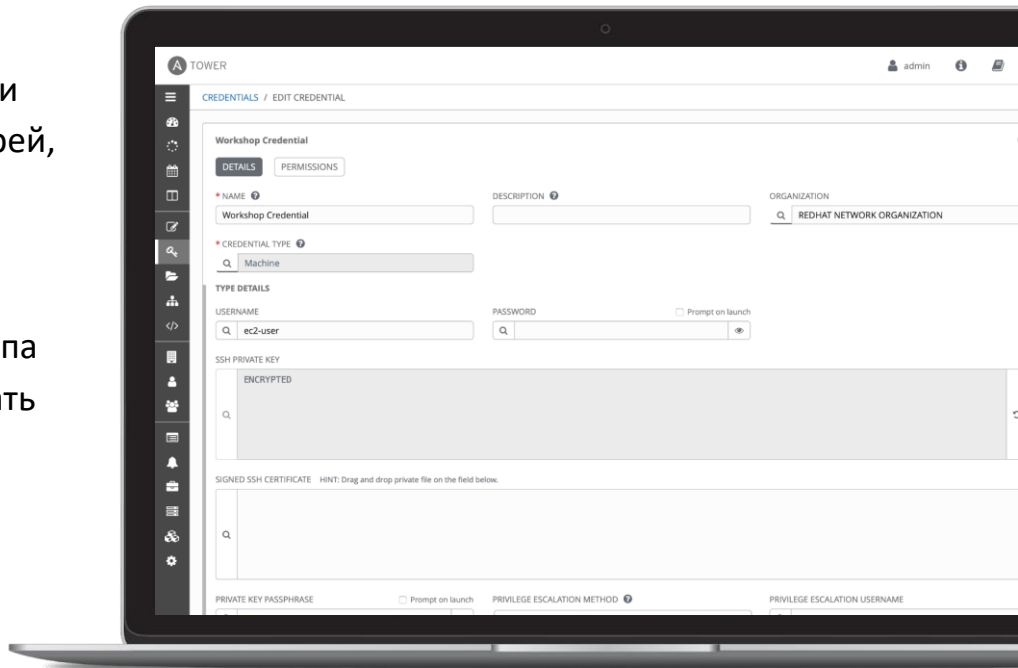
- Можно создавать группы
- Можно добавлять переменные
- Можно регулировать доступ для пользователей и команд
- Можно запускать ad-hoc команды
- Способы импортировать inventory
 - Через tower-manage
 - Через playbook (ansible_tower modules)
 - Через source для inventory



Credentials

Credentials используются для аутентификации при запуске job, а также для синхронизации инвентарей, импорта проектов и других моментов, где необходимо проводить аутентификацию

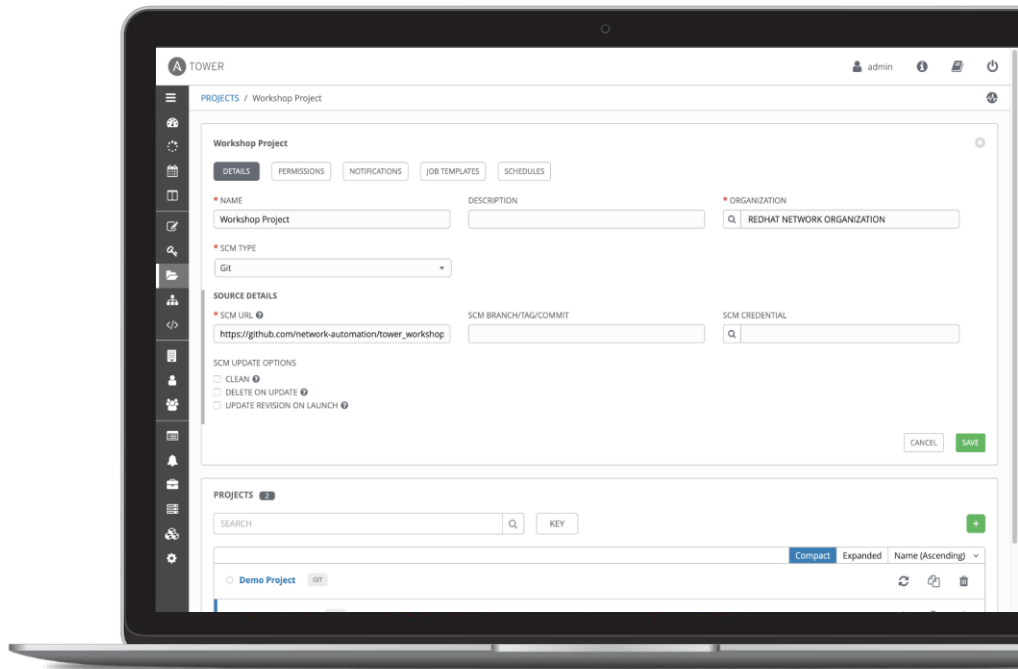
- На **Credentials** также можно давать права доступа
- Для разных сущностей необходимо использовать разные типы credential



Projects

Project - коллекция для playbook

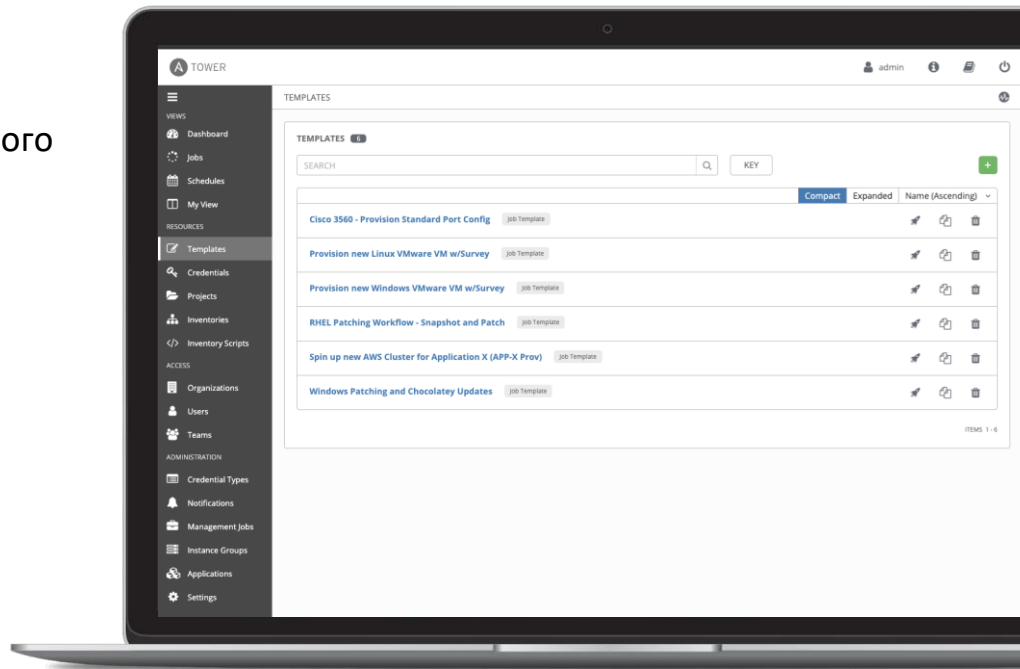
- Вы можете использовать разные типы хранения
- Git и Mercurial не поддерживают парольную аутентификацию
- На проекты также можно задавать свои права доступа



Job Templates

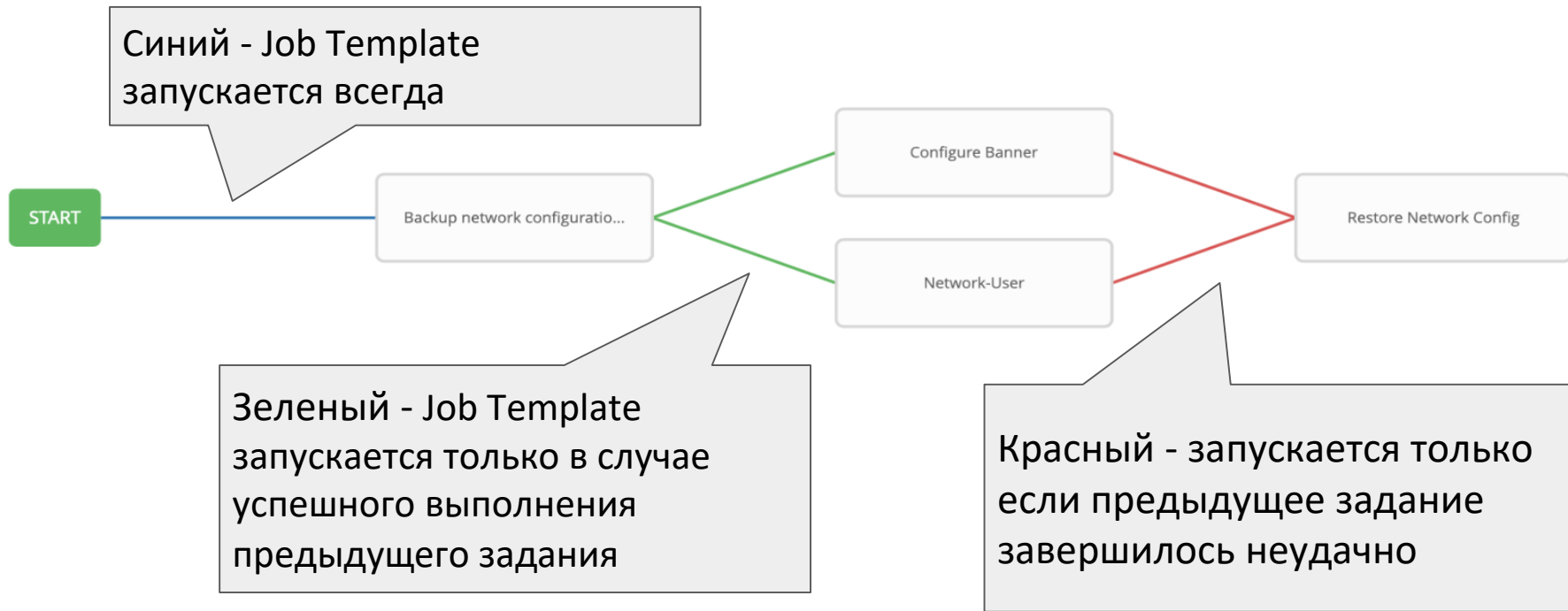
Template - набор параметров playbook для успешного запуска job. Шаблон состоит из:

- Inventory
- Project (содержит playbook)
- Credentials
- Survey or optional vars
- Job может быть запущен через GUI или API



Workflows

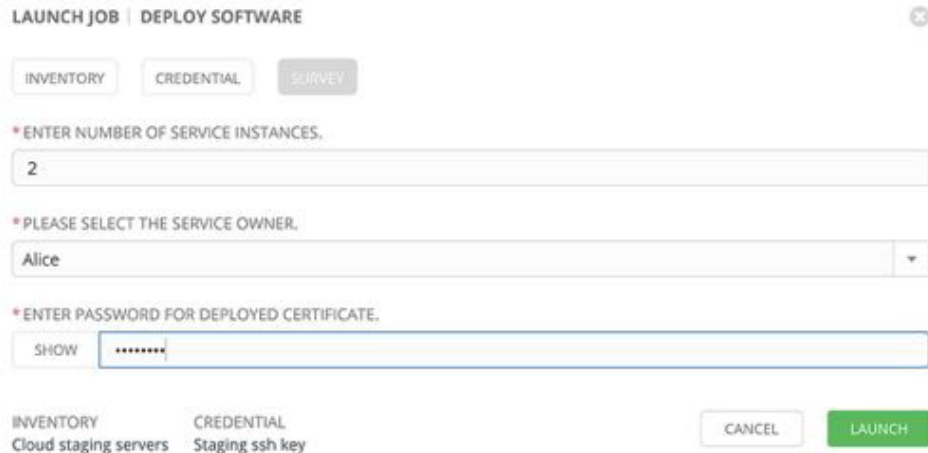
Возможность создавать цепочку событий с различными сценариями



Surveys

Tower surveys allow you to configure how a job runs via a series of questions, making it simple to customize your jobs in a user-friendly way.

An Ansible Tower survey is a simple question-and-answer form that allows users to customize their job runs. Combine that with Tower's role-based access control, and you can build simple, easy self-service for your users.



The screenshot shows the 'LAUNCH JOB | DEPLOY SOFTWARE' interface in Ansible Tower. At the top, there are three tabs: 'INVENTORY', 'CREDENTIAL', and 'SURVEY', with 'SURVEY' being the active tab. Below the tabs, there are three required fields:

- * ENTER NUMBER OF SERVICE INSTANCES. (Input: 2)
- * PLEASE SELECT THE SERVICE OWNER. (Dropdown menu: Alice)
- * ENTER PASSWORD FOR DEPLOYED CERTIFICATE. (Input: SHOW [password masked with dots])

At the bottom, there are two buttons: 'CANCEL' and 'LAUNCH'. Below the 'INVENTORY' and 'CREDENTIAL' tabs, there are labels for the selected inventory and credential: 'INVENTORY Cloud staging servers' and 'CREDENTIAL Staging ssh key'.

Red Hat Ansible Tower

Установка и требования

RED HAT ANSIBLE TOWER

Установка и требования

Supported Operating Systems:

- Red Hat Enterprise Linux 8.0 or later 64-bit (x86) (only Ansible Tower 3.5 and greater can be installed)
- Red Hat Enterprise Linux 7.4 or later 64-bit (x86)
- CentOS 7.4 or later 64-bit (x86)

Сценарии установки:

- Integrated installation
- Single machine with an external database
- High Availability Multi-Machine Cluster

Sizing:

- 2 CPU min
- 4 RAM min
- 20 GB Disk (150+ for database server)

Red Hat Ansible Tower

Интеграция с Red Hat Virtualization

RED HAT ANSIBLE TOWER

Интеграция с RHV



New integration support for RED HAT ANSIBLE ENGINE 2.7

- **Ansible modules and roles are fully supported**
- Red Hat Virtualization includes the downstream Ansible Engine

New roles include:

ovirt.shutdown-env - Performs a clean shutdown of the RHV environment. Useful for RHHI-V deployments.

ovirt.engine-setup - Automates the install and configuration of RHV-M in a standard (non-HE) deployment

ovirt.hosted-engine-setup - Automates the install and configuration of RHV-M in a hosted-engine deployment

ovirt.infra - Allows users to create and manage datacenters, clusters, hosts, networks, storage domains, authentication and authorization, and more

RED HAT ANSIBLE TOWER

Интеграция с RHV - Примеры

```
# Creates a new server rhel7 Virtual Machine from Blank template
# on brq01 cluster with 2GiB memory and 2 vcpu cores/sockets
# and attach bootable disk with name rhel7_disk and attach virtio
- ovirt_vm:
  state: present
  cluster: brq01
  name: myvm
  memory: 2GiB
  cpu_cores: 2
  cpu_sockets: 2
  cpu_shares: 1024
  type: server
  operating_system: rhel_7x64
  disks:
    - name: rhel7_disk
      bootable: True
  nics:
    - name: nic1
```

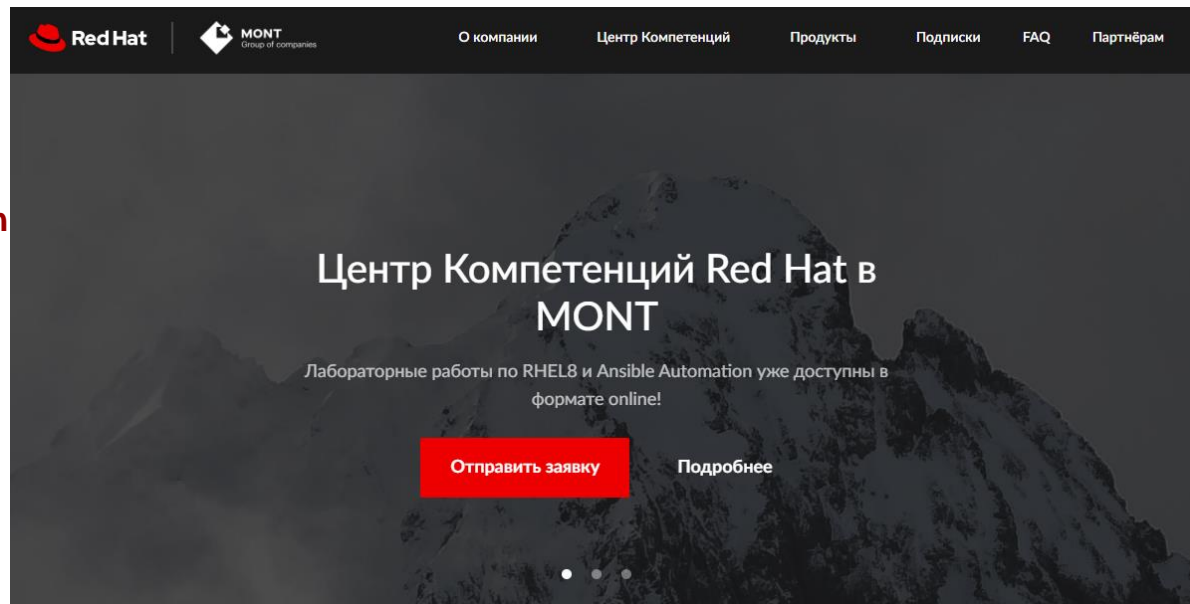
```
- name: Register VM with vnic profile mappings and reassign bad macs
  ovirt_vm:
    state: registered
    storage_domain: mystorage
    cluster: mycluster
    id: 1111-1111-1111-1111
    vnic_profile_mappings:
      - source_network_name: mynetwork
        source_profile_name: mynetwork
        target_profile_id: 3333-3333-3333-3333
      - source_network_name: mynetwork2
        source_profile_name: mynetwork2
        target_profile_id: 4444-4444-4444-4444
    reassign_bad_macs: "True"
```

DEMO

Центр Компетенций Red Hat

Центр Компетенций Red Hat в компании Mont

- Лабораторные работы
 - **RHEL 8**
 - **Red Hat Ansible Automation**
 - **RHV (ТВА)**
- Помощь и консультации
- База знаний
- Демо-стенд



СПАСИБО!

Мы в Telegram: <https://t.me/redhatmont>

Наша почта: redhat@mont.com

Наш сайт: <http://redhat.mont.com/>

