redhat.

Ansible. Автоматизация управления сетевой инфраструктурой

Александр Сафонов
Архитектор решений
asafonov@redhat.com

18 апреля 2018

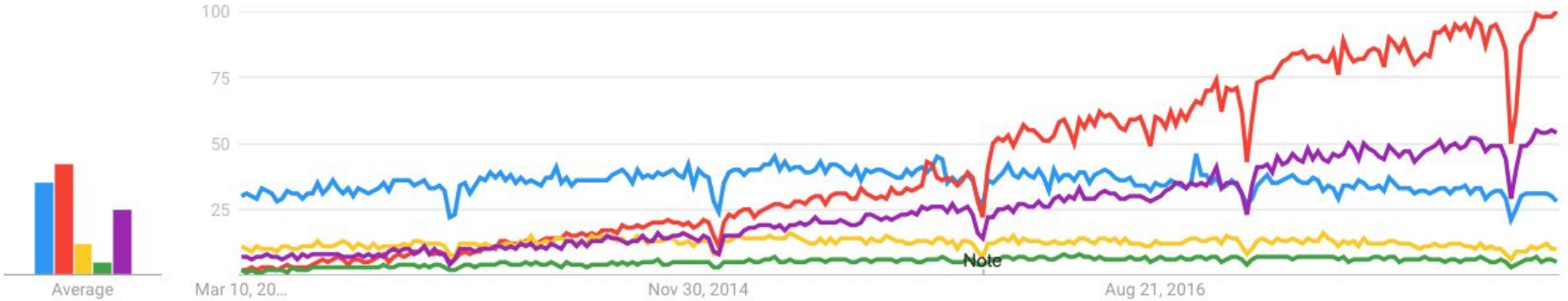

v1 - Set config file to use on boot
1. Write multiple configuration files
• For each environment/region
2. Inspect metadata on boot and use the matching config file
v1 - Set config file to use on boot
1. Write multiple configuration files
• For each environment/region
2. Inspect metadata on boot and use the matching config file
28,000+
stars on GitHub
1600+
Ansible modules
500,000+
downloads a month

2

ANSIBLE POPULARITY

Puppet	Ansible	Chef	Salt	DevOps
Software	Software	Topic	Software	Search term

Interest over time



redhat.

ANSIBLE - ОСНОВНЫЕ ПРЕИМУЩЕСТВА

ПРОСТОТА В ИСПОЛЬЗОВАНИИ

- Простой язык на основе YAML
- Не требует навыков программирования
- Последовательное выполнение задач
- Автоматизация для всех

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

- Развертывание приложений
- Управление изменениями
- Автоматизация рабочих процессов
- Оркестрация между различными платформами

БЕЗОПАСНОСТЬ

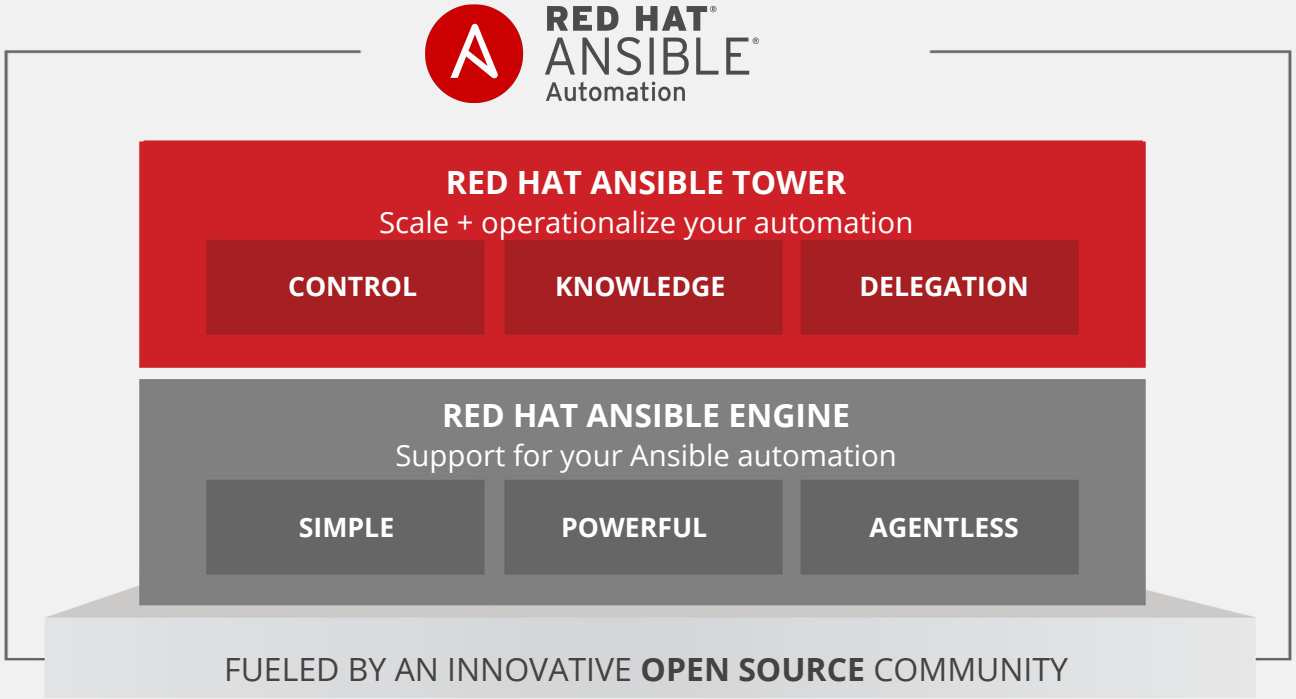
- Не требует агента на клиенте
- OpenSSH & WinRM в качестве транспорта
- Эскалация привилегий

ANSIBLE - THE MOST POPULAR OPEN SOURCE AUTOMATION PLATFORM

Goal: Unify provisioning, configuration, and application deployment

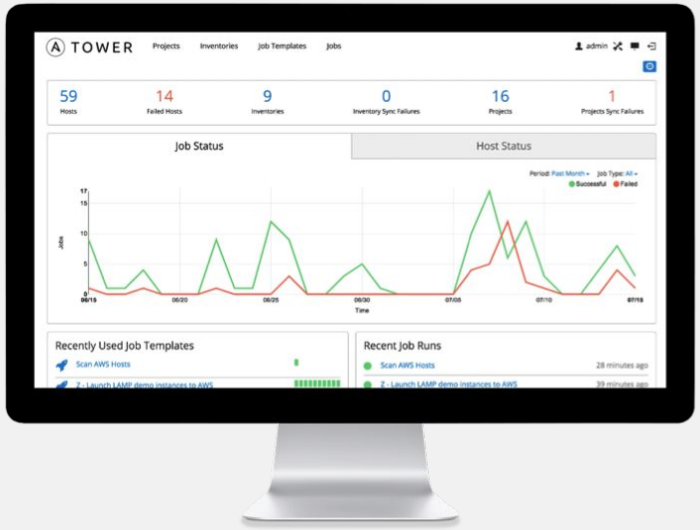
Result: Ansible. A python-based command line engine that interprets and executes YAML-based “Playbooks” that contain one or more “plays” or tasks.

RED HAT ANSIBLE AUTOMATION



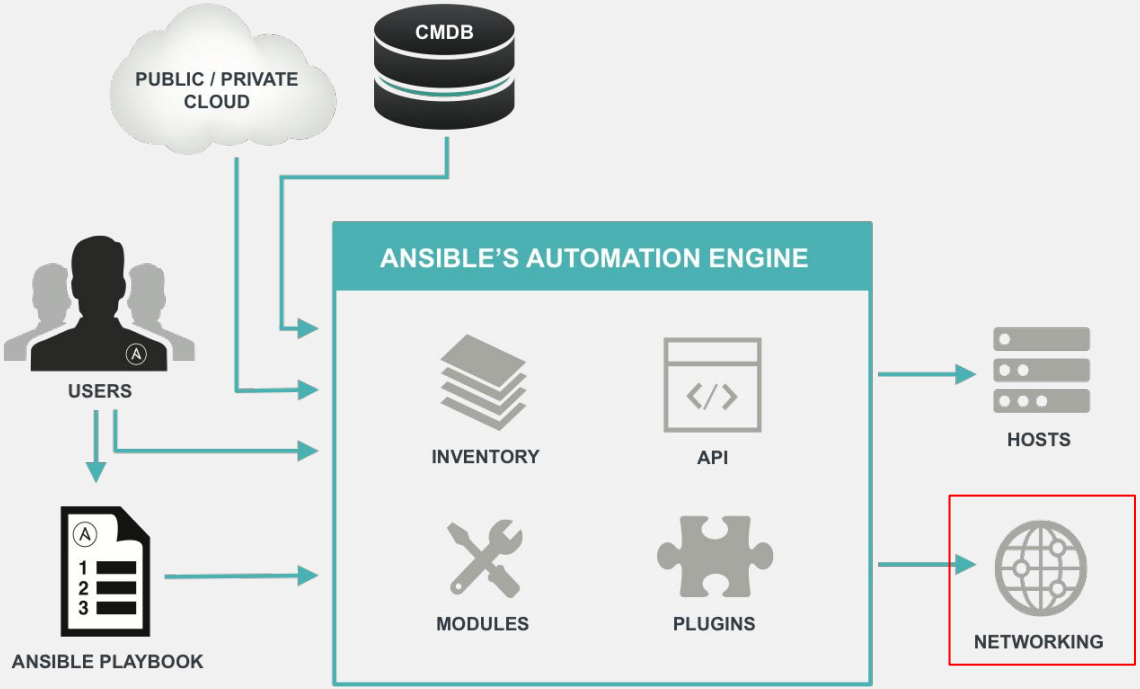
RED HAT ANSIBLE TOWER

Платформа для автоматизации, включающая в себя

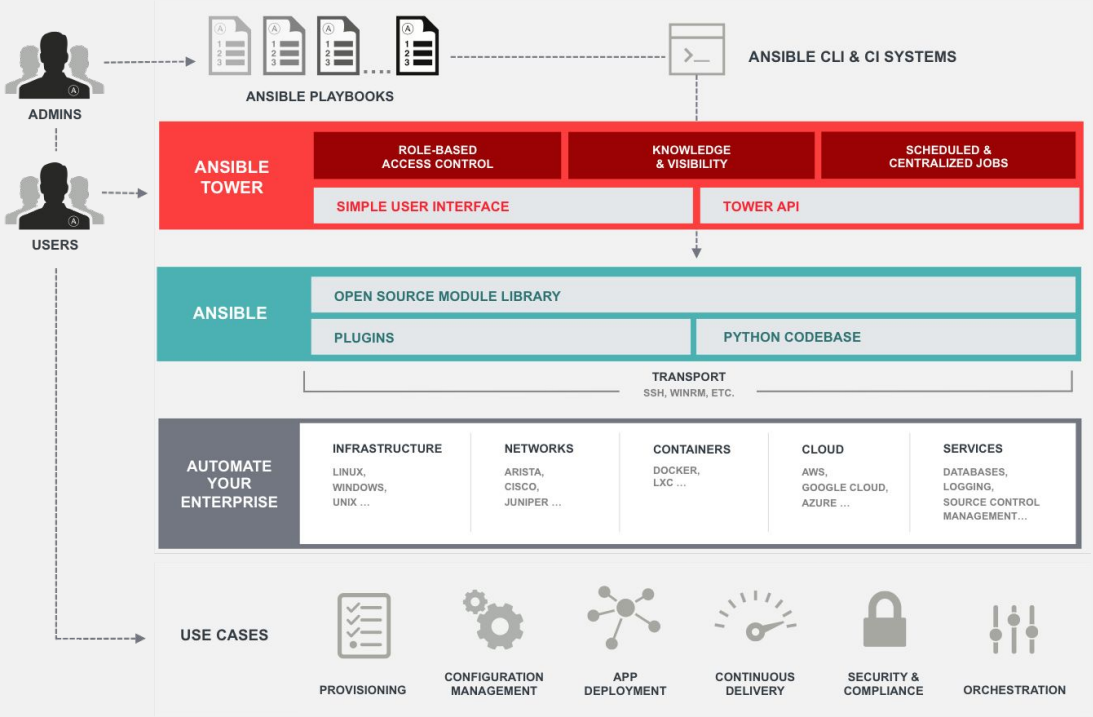


- **Язык** для автоматизации ИТ-инфраструктуры и приложений с помощью сценариев
- **Движок Ansible** для запуска и работы сценариев
- **Ansible Tower** предоставляет:
  - возможность автоматизировать рабочие процессы и определить взаимосвязь между сценариями
  - ролевая модель доступа для запуска сценариев
  - централизованное выполнение задач с регистрацией событий и их статусом
  - графический интерфейс и REST API

RED HAT ANSIBLE AUTOMATION ARCHITECTURE

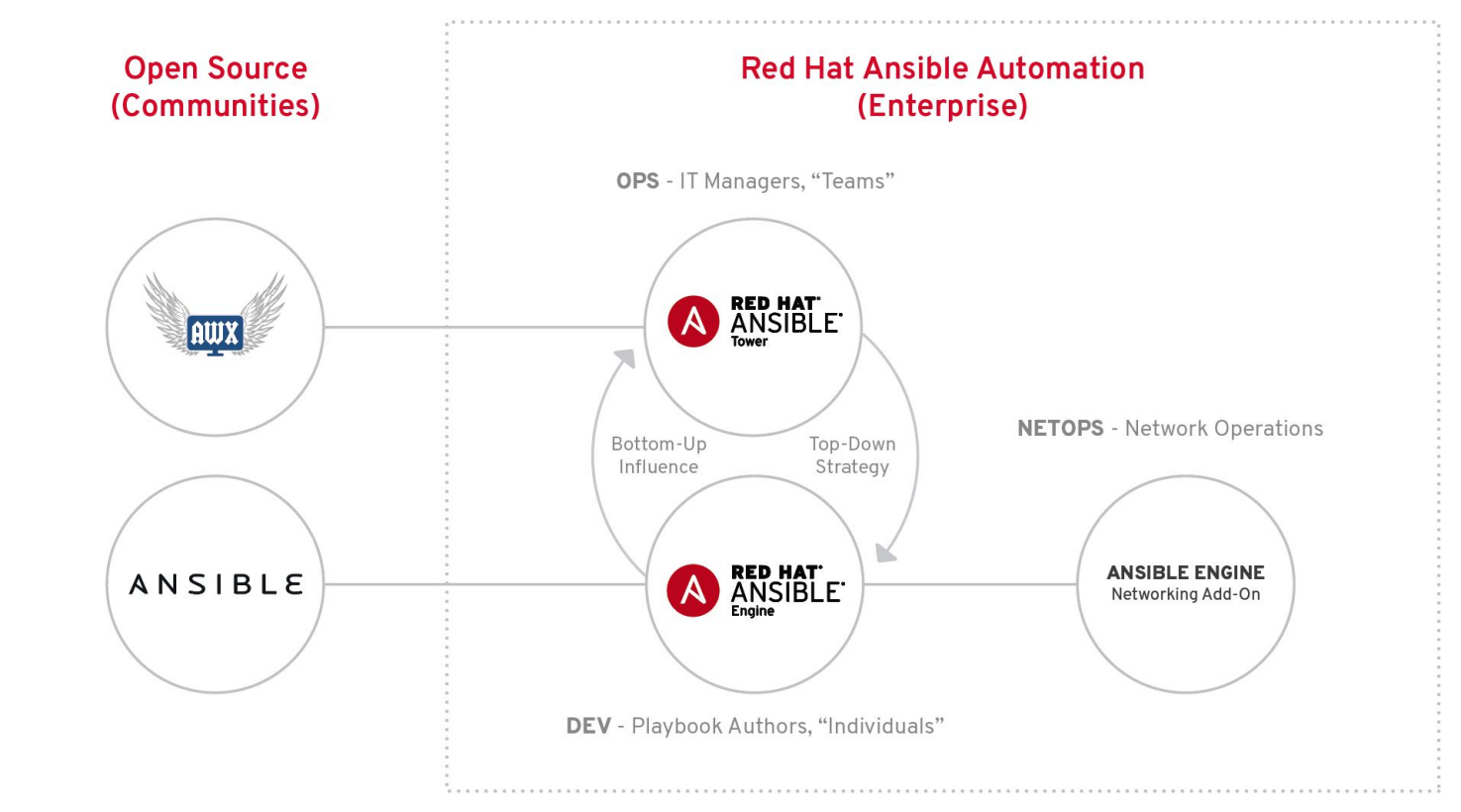


RED HAT ANSIBLE TOWER ARCHITECTURE



https://www.ansible.com/products/tower

ANSIBLE - PROJECT & PRODUCT

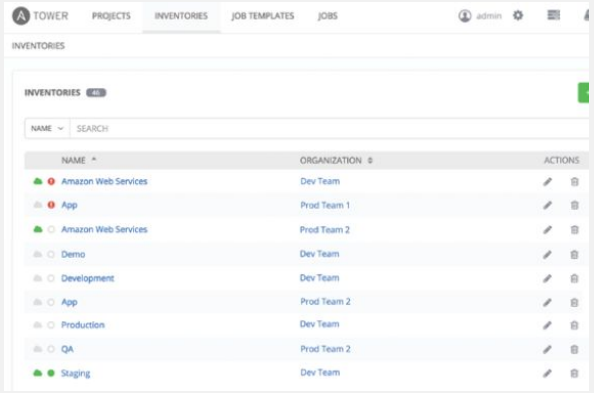


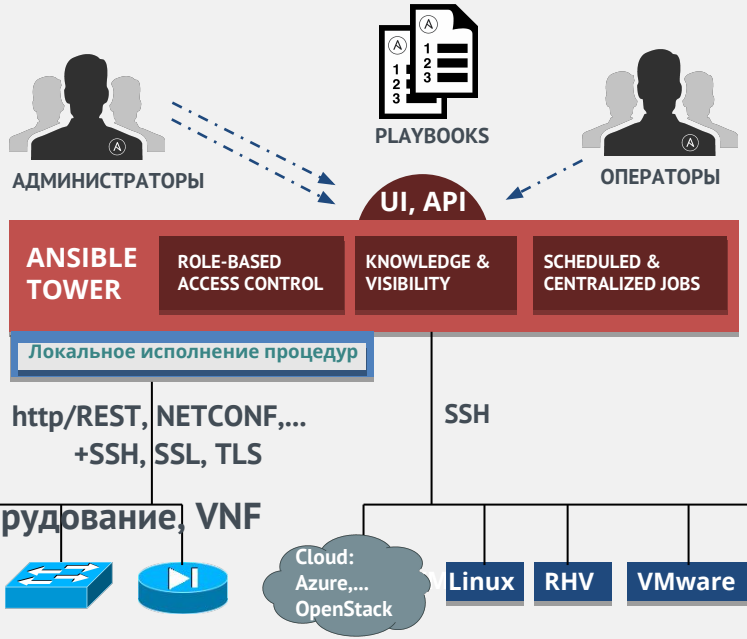
redhat.

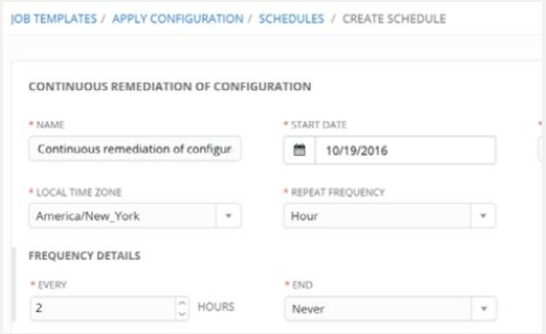
RED HAT ANSIBLE TOWER

RED HAT ANSIBLE TOWER

INFRASTRUCTURE-AS-A-CODE // УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ

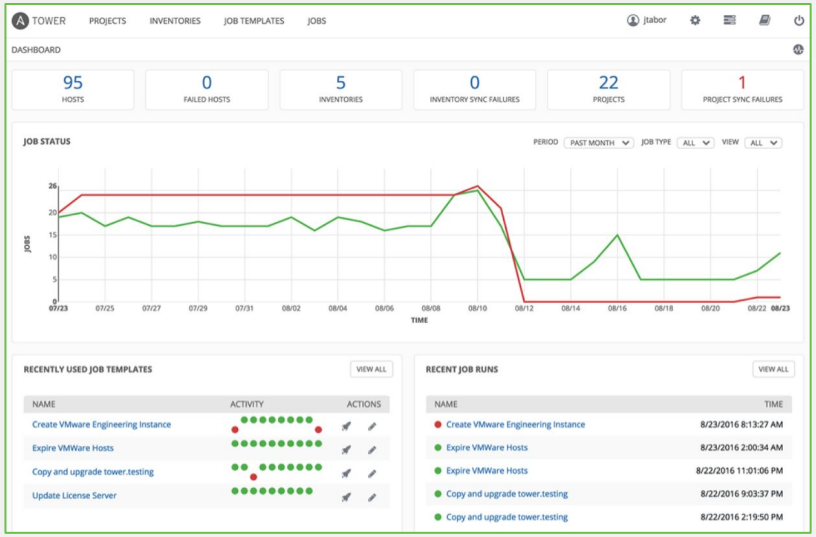


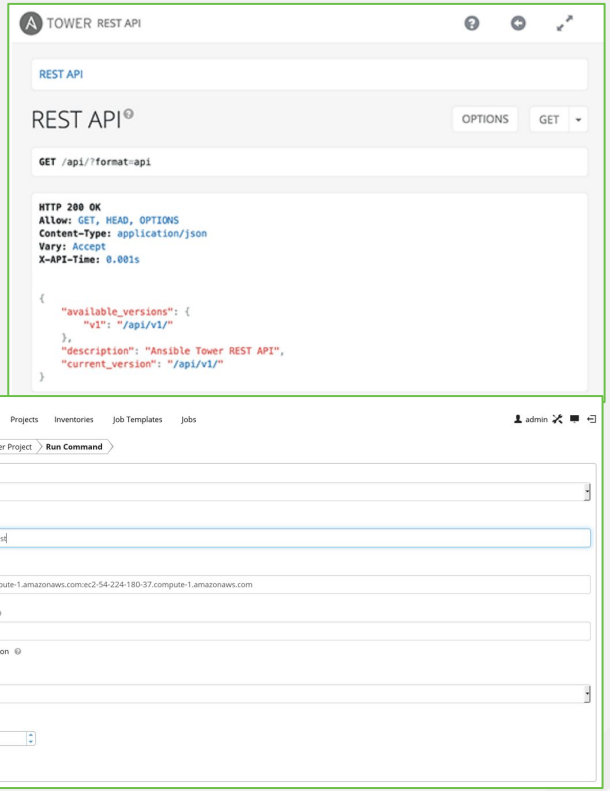




redhat.

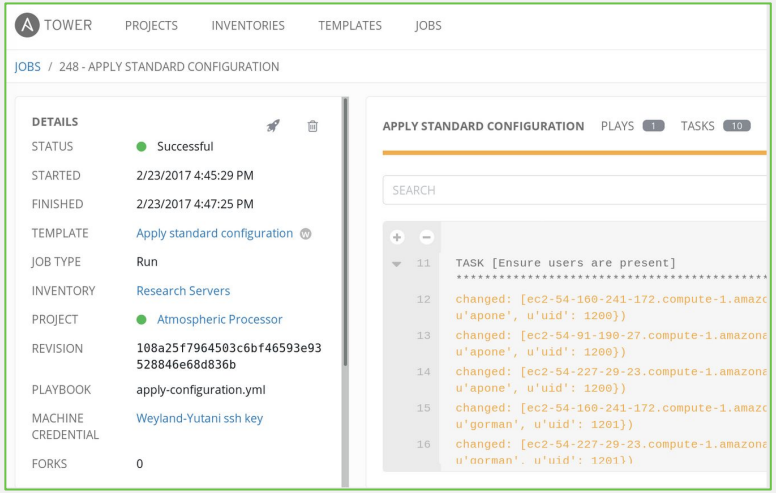
Ansible Tower - Автоматизация

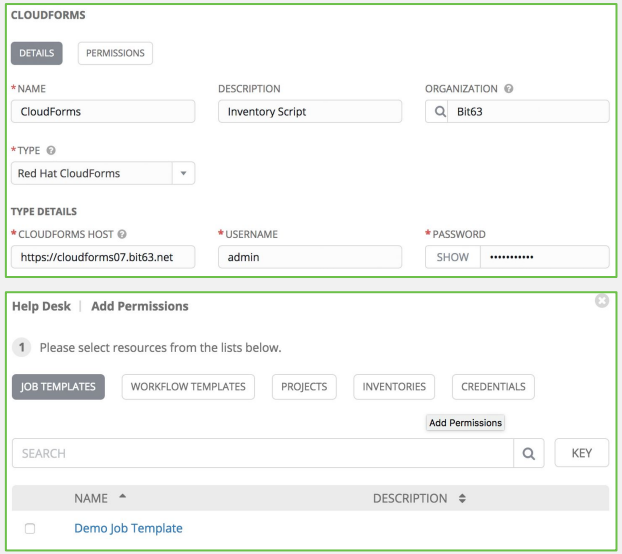




- Запуск сценариев нажатием одной кнопки
- Импорт сценариев из SCM
- CLI, REST API, remote execution, интеграции с CI/CD tools

Ansible Tower - Контроль и RBAC

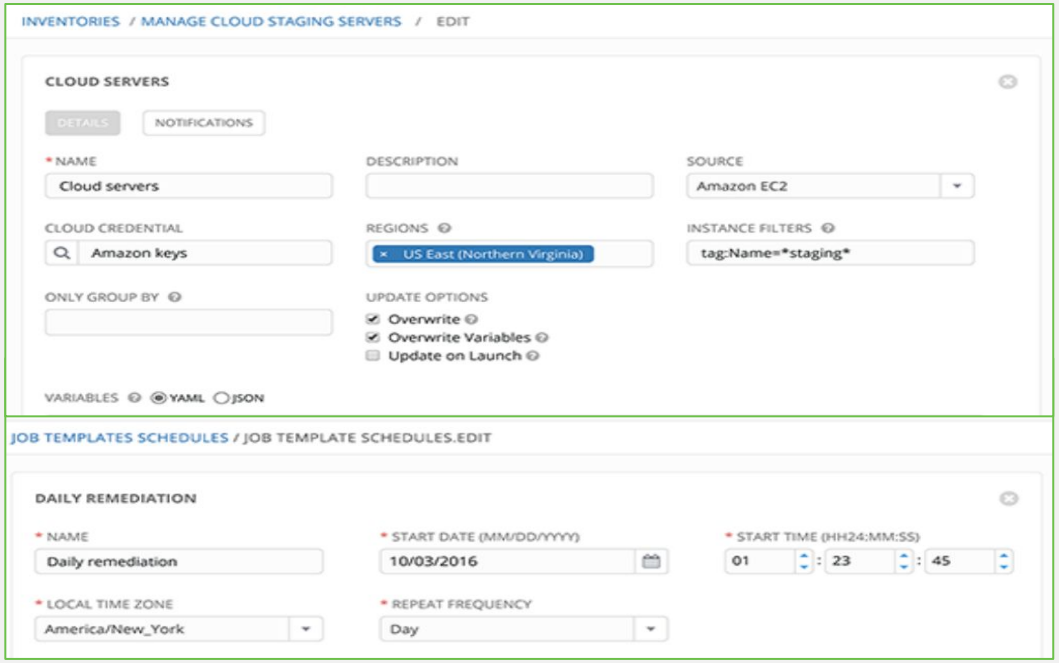


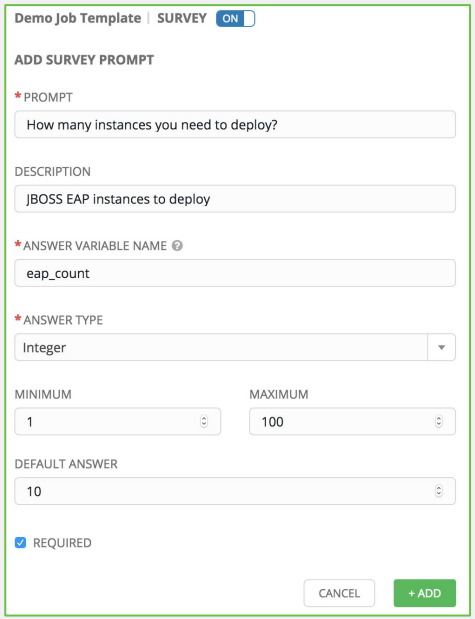


- Регистрация всех действия в БД
- Статус выполнения сценариев
- История выполненных задач

- Управление на уровне организаций, рабочих групп
- Хранение пользовательских данных в шифрованном виде
- Не надо иметь учетки на клиентах

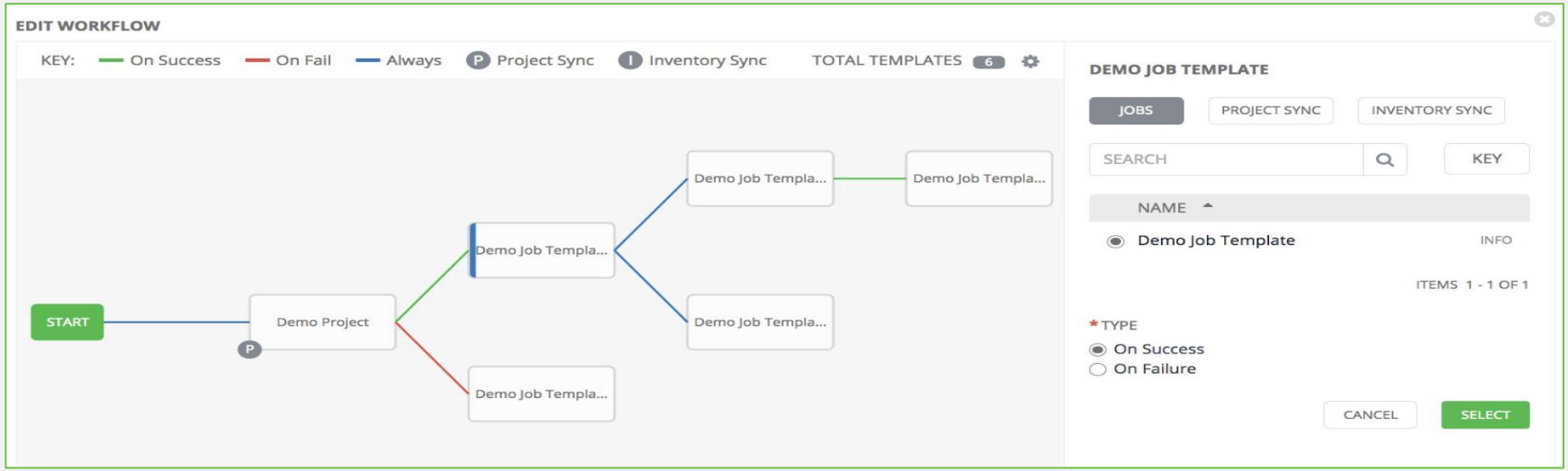
Ansible Tower - Управление





- Динамическая инвентаризация клиентов
- Запуск сценариев по расписанию
- Использование опросника для задания доп. параметров
- Уведомления в режиме реального времени

Ansible Tower - Управление ‘workflow’



Provision → Configure → Deploy → Scale

Build → Test → Promote → Verify → Deploy

Встроенный редактор рабочих процессов / workflow:

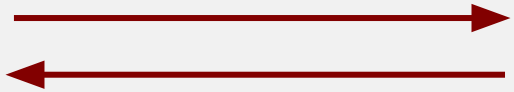
- Возможность группировать сценарии в зависимости от условий и результатов выполнения предыдущего
- Ролевая модель и результат выполнения задач

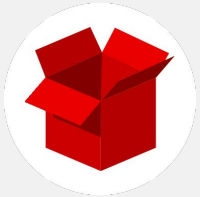
RED HAT ANSIBLE NETWORKING


MANAGING NETWORKS
HASN'T CHANGED
IN 30 YEARS.

WHY HASN'T NETWORKING CHANGED?

Networking vendors are the trusted advisors





PEOPLE

- Domain specific skill sets
- Vendor oriented experience
- Siloed organizations
- Legacy operational practices

PRODUCTS

- Infrastructure-focused features
- Baroque, CLI-based interfaces
- Siloed technologies
- Monolithic, proprietary platforms

WHAT IS THE PRIMARY METHOD OF MAKING NETWORK CHANGES IN YOUR ENVIRONMENT?

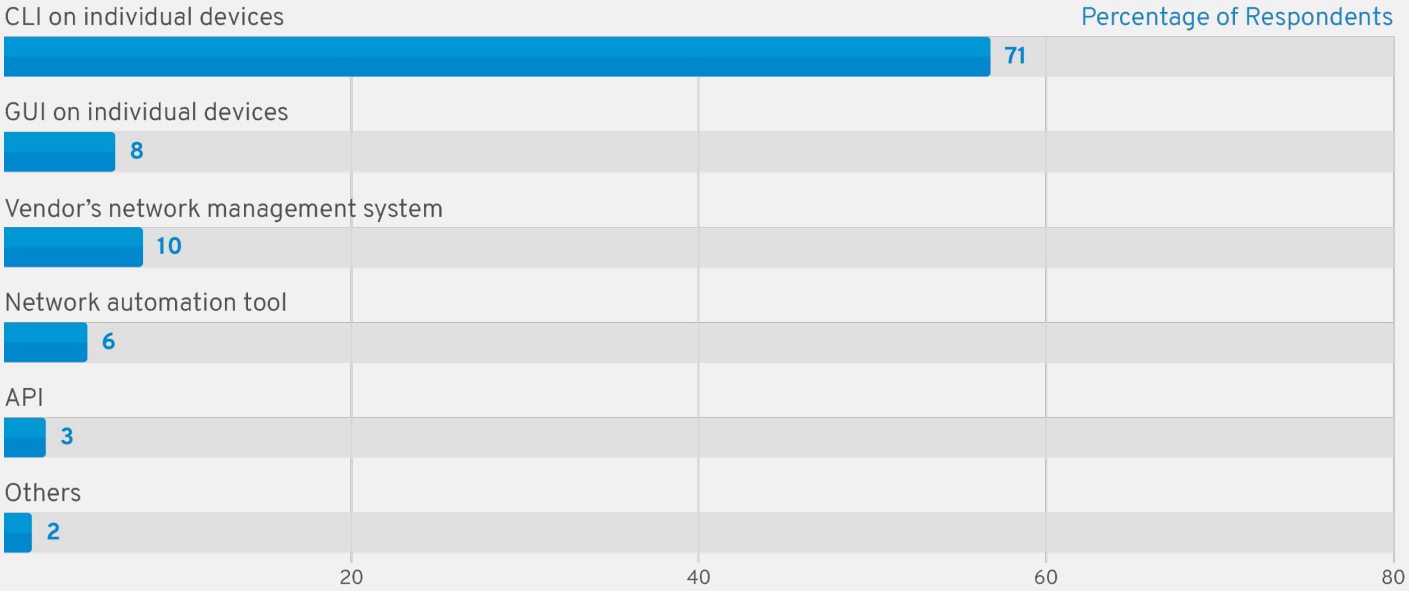


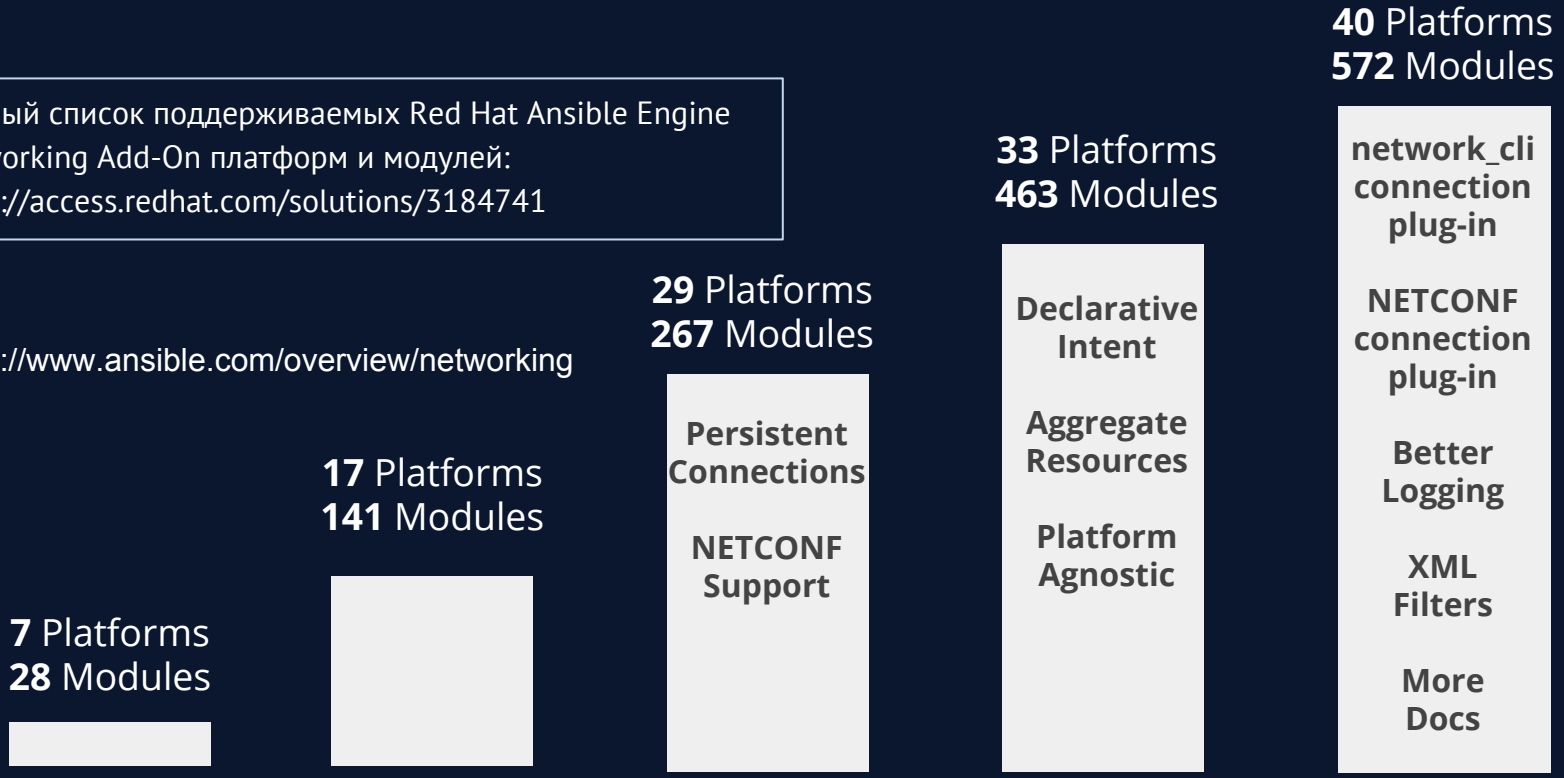
Figure 1
Primary Method for Making Network Changes

Source: Gartner, *Look Beyond Network Vendors for Network Innovation*, Andrew Lerner, 23 January 2018, ID: G00349636.

NETWORK AUTOMATION PROGRESS

Полный список поддерживаемых Red Hat Ansible Engine Networking Add-On платформ и модулей:
https://access.redhat.com/solutions/3184741

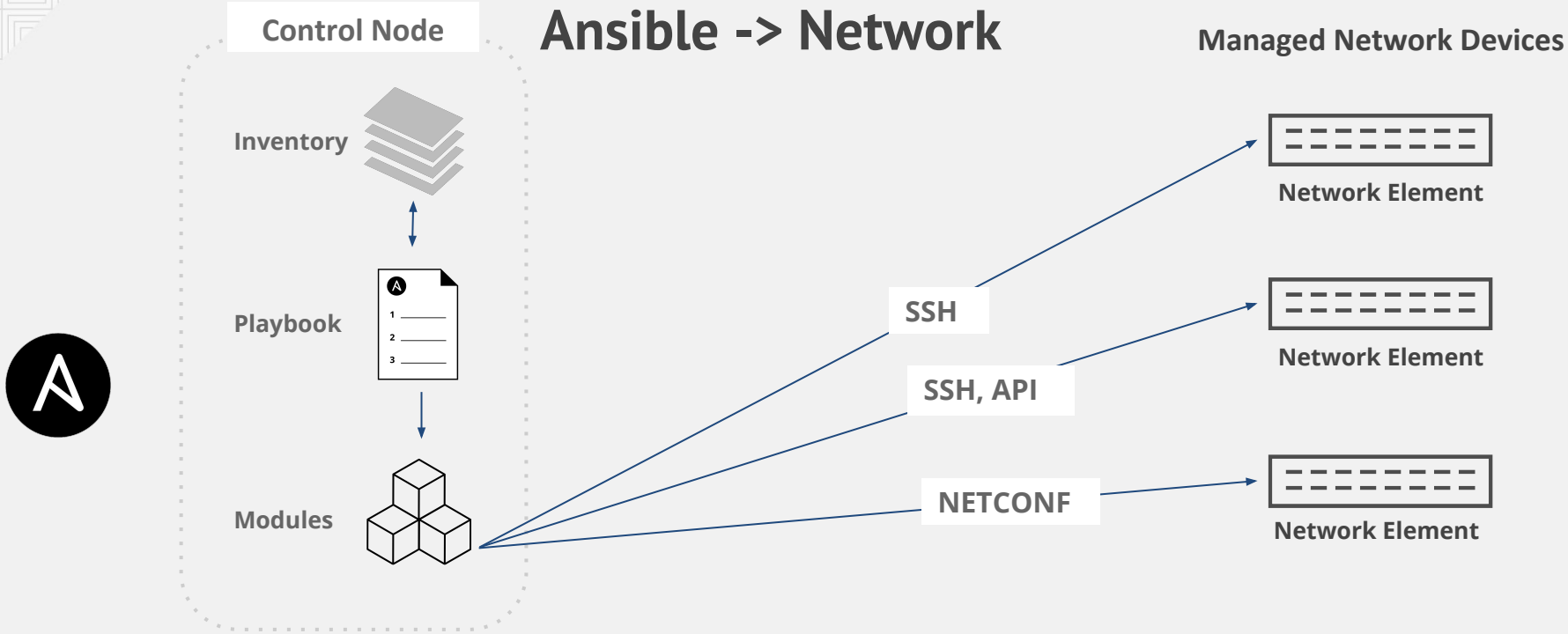
https://www.ansible.com/overview/networking



NETWORK MODULES: BUILT-IN DEVICE ENABLEMENT

- A10
- Apstra AOS
- Arista EOS (cli, eAPI), CVP
- Aruba Networks
- AVI Networks
- Big Switch Networks
- Brocade Ironware
- Cisco ACI, AireOS, ASA, IOS, IOS-XR, NSO, NX-OS
- Citrix Netscaler
- Cumulus Linux
- Dell OS6, OS9, OS10
- Exoscale
- F5 BIG-IP
- Fortinet FortIOS, FMGR
- Huawei
- Illumos
- Infoblox NIOS
- Juniper Junos
- Lenovo CNOS, ENOS
- Mellanox ONYX
- Ordnance
- NETCONF
- Netvisor
- Openswitch
- Open vSwitch (OVS)
- Palo Alto PAN-OS
- Nokia NetAct, SR OS
- VyOS

Ansible -> Network



Modules:
Handles execution of remote system commands

Control Node:
Any client system (server, laptop, VM) running Linux or Mac OSX

Managed Nodes (Inventory):
A collection of endpoints being managed via SSH or API.

Ansible - NETWORKING AUTOMATION

Configure, validate, & ensure continuous compliance for physical network devices

BUILD
with Red Hat Ansible Engine

- Get automating quickly
- Integrate multi-vendor configurations
- Ideal for both brownfield and greenfield

Automate discrete tasks

RED HAT® ANSIBLE® Engine

MANAGE
with Red Hat Ansible Engine

- Methodically track configuration drift.
- Make changes across any set of network devices.
- Validate that changes were successful.

Automate business processes

RED HAT® ANSIBLE® Engine

SCALE
with Red Hat Ansible Tower

- Ensure ongoing steadystate on a schedule.
- Use role-based access controls with specific teams.
- Integrate external third-party solutions with RESTful API.

Orchestrate & operationalize automation

RED HAT® ANSIBLE® Tower

NETWORK AUTOMATION WITH ANSIBLE

PLAN	BUILD	RUN
Ansible automation baked in as part of design and architecture	Build engineers use Ansible (jobs/playbooks) to set up new configurations across multi-vendor networking platform, operating systems, private and public cloud.	Network Operations use Ansible to run or schedule jobs for specific use cases eg. scan

Heterogenous mix of networking vendors

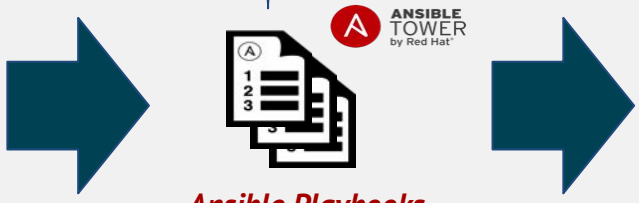
ARISTA · cisco · f5 · JUNIPER NETWORKS · cumulus networks · paloalto NETWORKS · CITRIX NetScaler

Decoupling the data model from the execution enables:

Multi-vendor orchestration

Enhanced network operational model through scalable, repeatable patterns

Integration into agile DevOps workflows



Ansible Playbooks

Define Intent, Policy, Architecture

Execution

Apply across device type, vendors

NETWORK SERVICE AUTOMATION EXAMPLE

Data Center and WAN Network Devices. > 10,000 Multi-vendor Devices – NXOS, JunOS, IOS-XR, EOS

Before Red Hat Automation Tools:

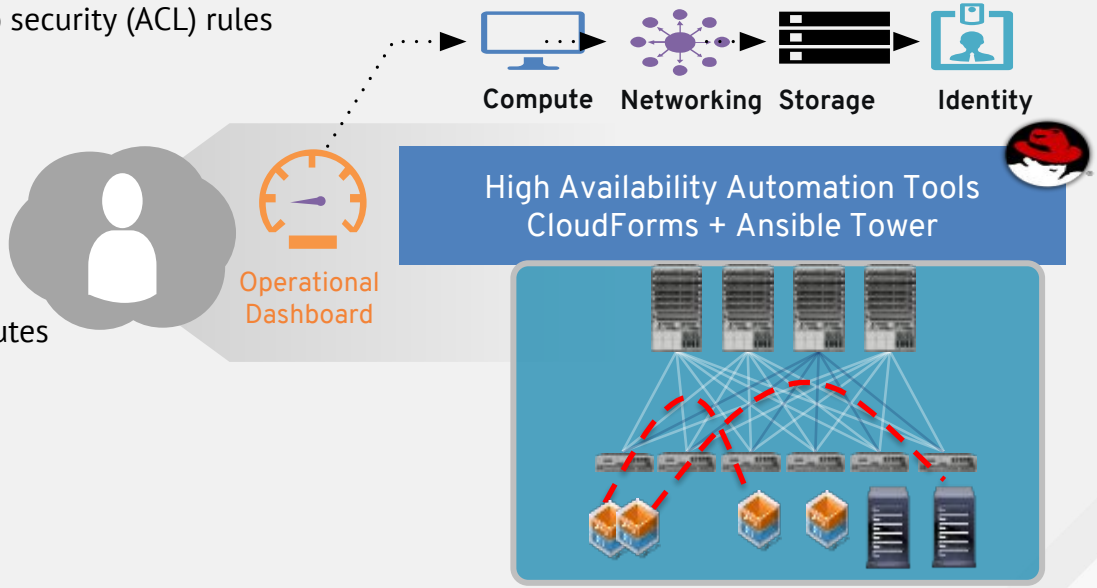
- Manual operator translation of daily changes to security (ACL) rules
- Not Compliant with Operational Business Rules

After:

- Ansible Tower + CloudForms
- Automated Rule Playbooks
- Daily Remediation of Business Rules
- Hours to Provision One Device Reduced to Minutes

Key Benefits:

- Fully Automated, Open, Secure
- Saves Time – More Productive Teams
- Fewer Mistakes / Errors
- Significant Reductions in Complexity
- Apply Across Other Service Deployments



Faster Deployments –> Lower Costs

SDN vs Automation (Ansible)

BENEFIT	SDN	AUTOMATION
Reconfigure the network from a central point	✔	✔
Reduced vendor lock in with commodity hardware	?	✔
Leverage existing infrastructure	✖	✔
Decouple control plane from data plane	✔	✔
Reduced opex/capex costs	?	✔

TRANSFORMING THE ENTERPRISE

PHYSICAL NETWORK STATE VALIDATION

DATA CENTER FABRIC AUTOMATION

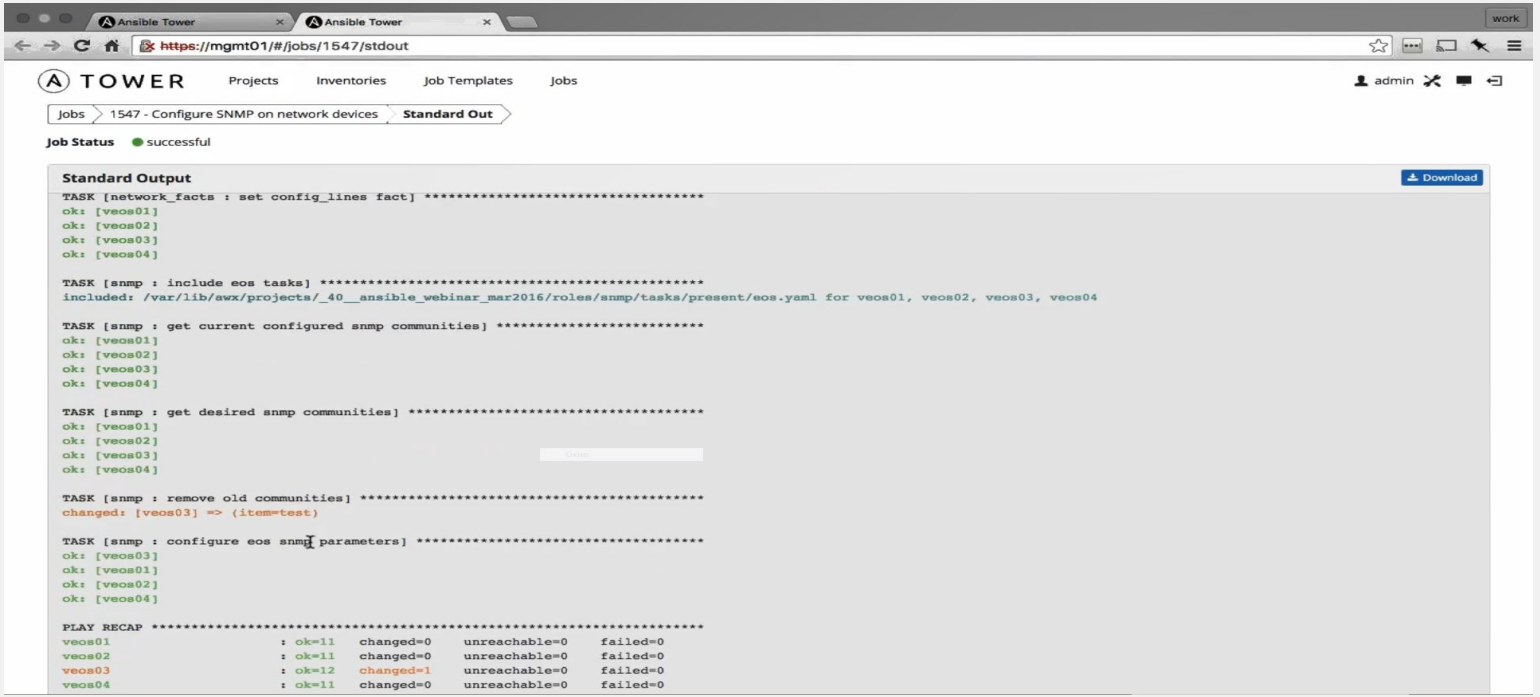
HYBRID CLOUD NETWORK INTERCONNECT

40 Networking platforms

570+ Networking modules

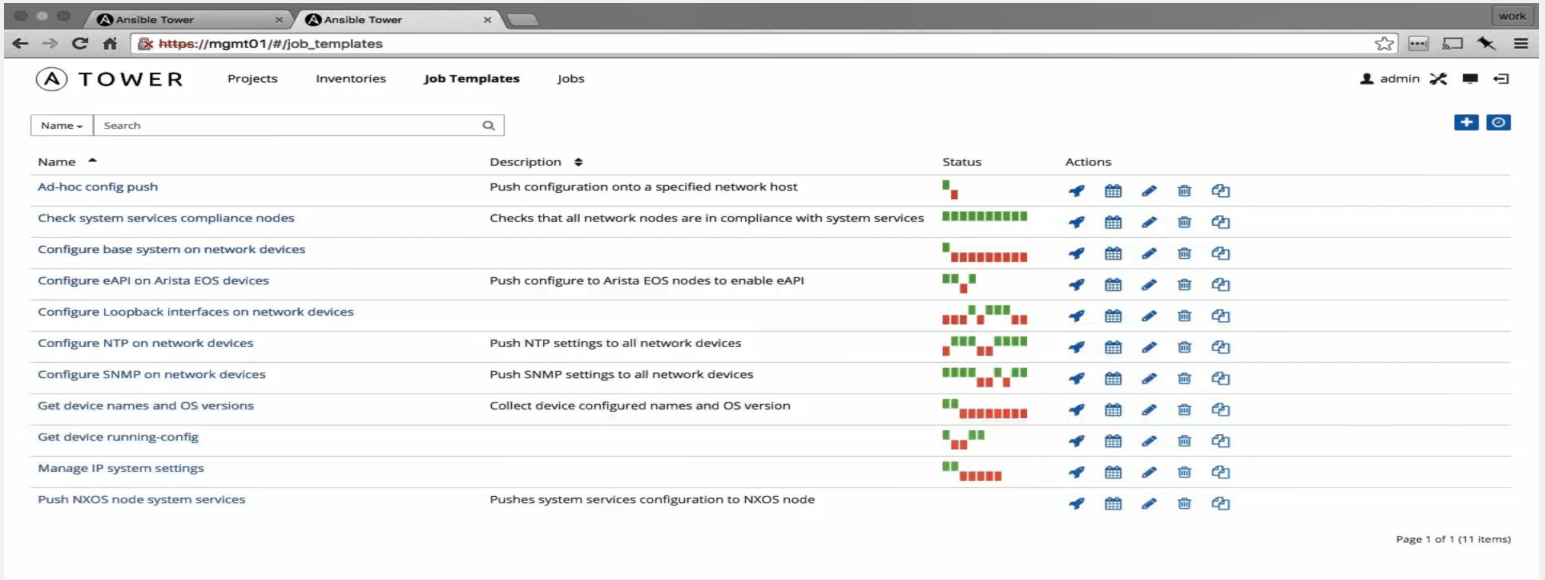
ansible.com/networking

Ansible Tower - UI



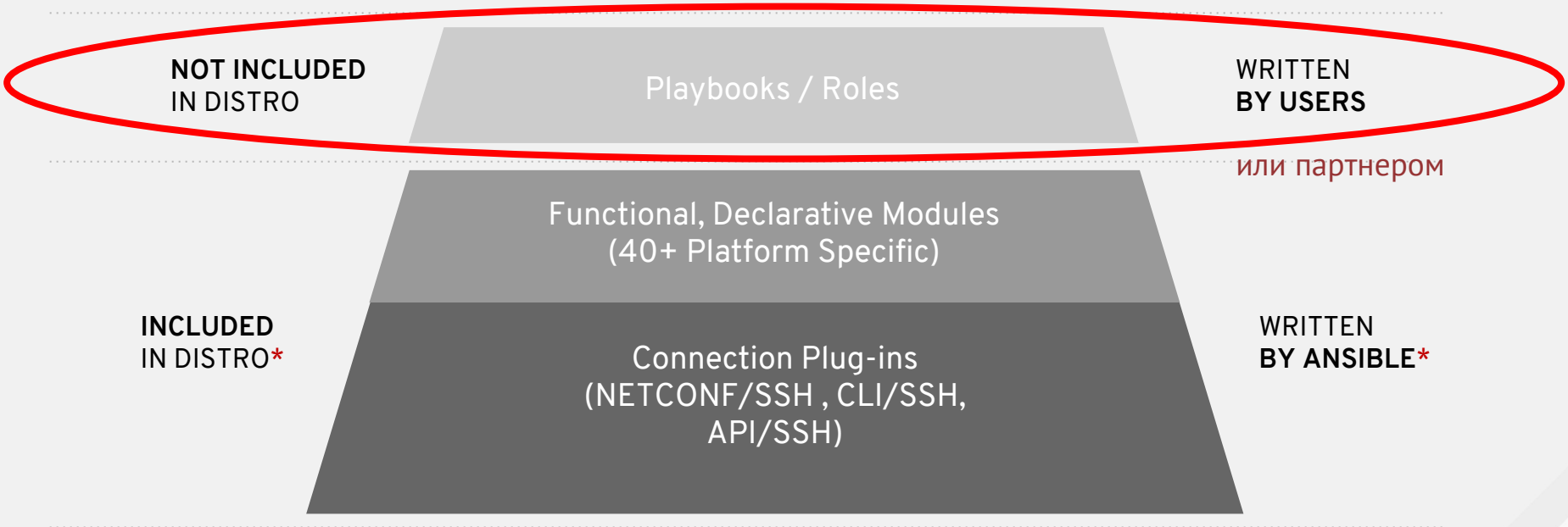
https://www.ansible.com/resources/webinars-training/automating-your-network

Ansible Tower - UI



https://www.ansible.com/resources/webinars-training/automating-your-network

Ansible for Networking



*Can also be created and maintained by the community

Ansible для Networks - Кому и зачем

- Часть DevOps и Трансформационной истории
  - Кроме контейнеров актуальна и автоматизация legacy, а Network - наиболее legacy
  - Можно дополнять Ansible для ИТ, реализовывать параллельно, или, наоборот, первым
- Альтернатива/дополнение к вендорским EMS/NMS
- Альтернатива вендорским SDN
  - Вместо закупки контроллера и доп.лицензий

Типовые сценарии применения

- Новые дата-центры и проекты модернизации существующих
- Территориально-распределенная инфраструктура с типовыми блоками устройств

Важно

- В конкурентах только ‘Do Nothing’ и DIY. Популярный для BM puppet несопоставим, различные SNMP средства удачно дополняются Ansible, начиная с настройки SNMP и агентов на устройстве
- Стоимость мала на фоне затрат на сетевое оборудование и обслуживающих его людей

Спасибо


plus.google.com/+RedHat


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHatNews


youtube.com/user/RedHatVideos