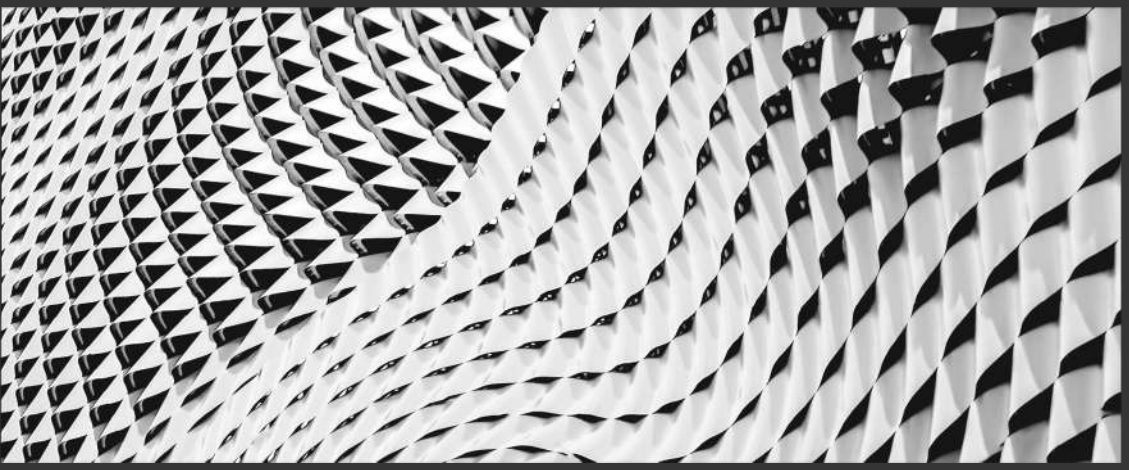
비즈니스 연속성을 위한 레드햇 자동화 플랫폼 활용

: 언택트 시대의 IT인프라 운영 방안

김득희 TL (Solution Architect Team)
dekim@redhat.com
한국 레드햇

Red Hat

COVID-19가 바꾸어 놓은 IT 환경



Red Hat

코로나19(COVID-19) 실시간 상황판

KR한국

마지막 업데이트: 2020. 7. 26. 오전 1:00:16

전 세계

16,055,228	644,808	9,813,539	4.02%
(+22,732)	(+532)	(+14,809)	
확진자	사망자	격리해제	치사율

대한민국

14,092	298	12,866	2.11%	1,518,634	19,681
(-)	(-)	(-)		(-)	(-)
확진자	사망자	격리해제	치사율	총검사자	검사중

ⓘ 용어 설명

*대한민국 수치는 질병관리본부 보도자료 기준

*대한민국 확진자 증감수치는 전일 발표 대비 변화량

WHO "전세계 일일 코로나 신규 환자 또 최고치"

이옥진 기자

입력 2020.07.25 11:11 | 수정 2020.07.25 11:15

미국·브라질·인도·남아공 심각, 유럽에서도 '2차 유행' 경고

24일(현지 시각) 멕시코 몬테레이의 한 공공병원에서 한 의료종사자가 방호복과 마스크, 고글을 착용하고 있다. /로이터 연합뉴스

Red Hat

전례없는 불확실성

"I don't have all the information I need to make the tough decisions between addressing cost pressure and planning for the future"

CIO의 긴급한 대응과 판단

"My immediate focus is on our people, but there is a backdrop of real fear for the business. I feel like everyone is looking to me"

일상에 대한 새로운 정의 – 뉴 노멀

"This situation is unprecedented. We are finding ourselves planning for things we have never done or even thought of before"

Source: Sector research; industry reports; BCG CIO engagements

[비즈톡톡] 포스트 코로나, 왜 '클라우드'에 주목하는가

조선비즈 | 황민규 기자

입력 2020.05.21 06:10

신종 코로나바이러스 감염증(코로나19) 이후 급격한 경제·산업 지형 변화와 관련해 빠짐없이 등장하는 키워드가 하나 있다면 바로 '클라우드'입니다. 윤성로 4차산업혁명위원회 위원장도 최근 조선비즈와 인터뷰에서 '포스트 코로나' 시대의 핵심 동력을 클라우드로 지목한 바 있습니다.

클라우드는 이미 수년에 걸쳐 미국의 IT 공룡 기업들을 중심으로 대규모 투자가 이뤄져왔습니다. 오래전부터 이들 기업은 클라우드가 인공지능(AI) 시대를 견인하는 핵심 인프라가 될 것이라는 점을 간파하고 있었던 것입니다.

정보통신산업진흥원(NIPA)은 최근 보고서에서 "코로나19 이후 가속화될 언택트(Untact) 시대에 클라우드는 공공, 기업, 사회 시스템의 연속성을 보장하는 효과적인 수단으로 재조명받고 있다"며 코로나19 이후 뉴노멀 변화의 핵심으로 클라우드를 꼽았습니다.

정보통신산업진흥원 제공

◇코로나19 이후 '선택'이 아닌 '필수' 요소로 자리매김

포스트 코로나와 클라우드

"공공, 기업, 사회 시스템의 연속성을 보장하는 효과적인 수단으로 재조명"

Red Hat

[기획] 코로나19 이후 온택트 시대, 네트워크 인프라 자동화가 중요해진 이유

이상일 기자 2020.05.22 10:04:08

가+ 가-

[기획/언택트 시대, 기업 모빌리티 혁신⑧] 언택트 넘어 연결 중심의 '온택트(Ontact)'사회를 대비

[디지털데일리 이상일기자] 코로나19가 사회 구조는 물론 기업의 경영환경도 바꾸고 있는 가운데 '초연결성'에 대한 논의가 새롭게 불거지고 있다. 기업에 있어 언제 어디서나 업무 프로세스가 유지될 수 있는 '모빌리티'가 중요해지고 있으며 이를 지원하기 위한 근간인 네트워크의 중요성도 다시 부각되고 있는 상황이다.

이에 업계에선 '언택트(Untact)'를 넘어 연결 중심의 '온택트(Ontact)'의 시대가 본격화될 것으로 전망하고 있다. 사회적으로 멀어진 거리가 온라인을 통해 연결되고 있는 것. 따라서 클라우드, 빅데이터, 그리고 업무 자동화를 뒷받침하기 위한 네트워크 인프라의 혁신이 요구되고 있는 상황이다.

"온택트(OnTact)의 시대로"

화장실 갈 시간도 줄일만큼 코로나로 더 바빠진

[중앙일보] 입력 2020.03.16 05:00 수정 2020.03.18 11:22

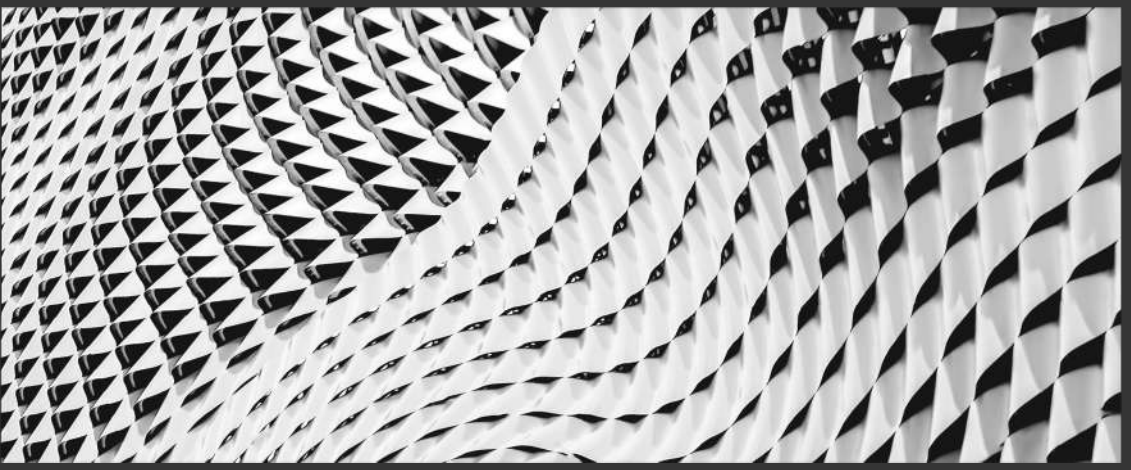
1000명 동시 접속→3000명 동시 접속

코오롱그룹은 최근 그룹 전반에 걸친 재택근무를 실시 중이다. 이에 대응해 기존 1000명의 유저가 동시에 접속해 사용할 수 있던 VPN 용량도 최근 3000 유저 수준으로 확장했다. 사실상 [illegible] 사무직 직원 대부분이 재택근무에 들어간 데 따른 조치다. 그 바람에 김 팀장과 그의 팀원 입장에선 업무량이 기존보다 3배 이상 늘었다. 외부에서 접속한 직원들에게 어느 수준의 업무까지 접근할 수 있을지 일일이 권한을 설정해주는 것은 기본이다.

"원격 접속을 위한 VPN 사용 증가"

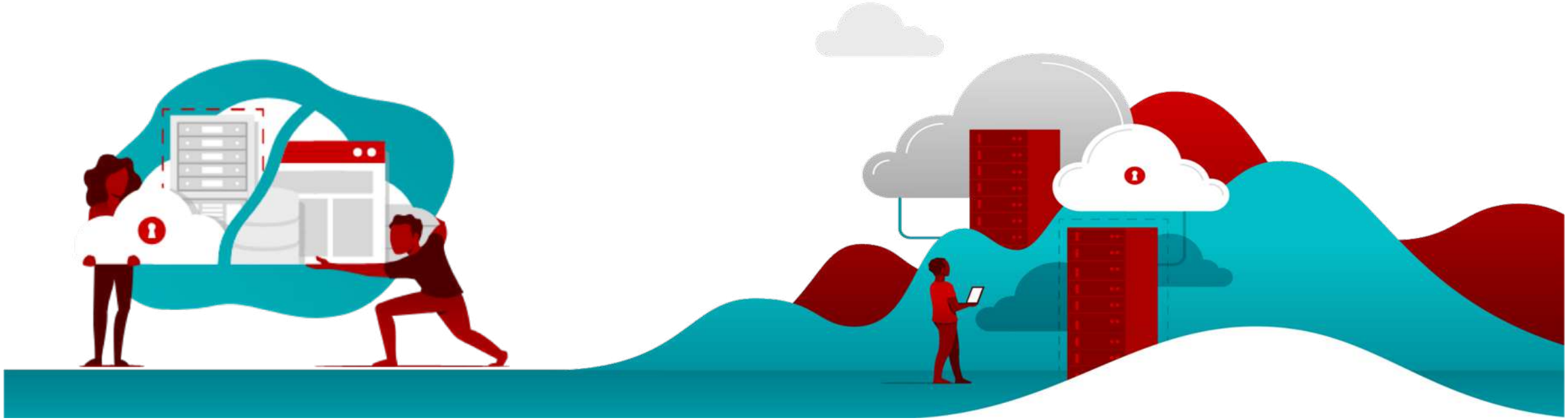
Red Hat

COVID-19에 대응하는 IT 자동화 전략



Red Hat

IT 자동화 전략의 방향성



(사용자 역할) (운영자 역할) (자동화 도구의 역할)

SELF-SERVICE → PROCESS →

- 반복작업
- 승인
- 모니터링
- 패치
- 보안점검
- etc

Red Hat

자동화 고려 사항

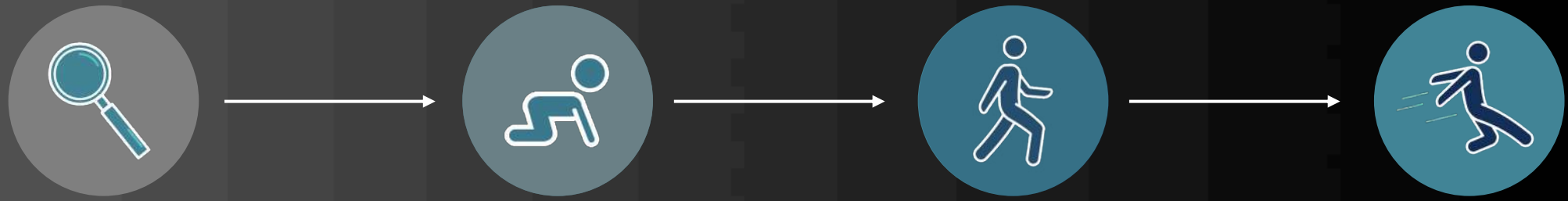
작고 자주 반복되는 것

다른 자동화 케이스를 참고

소프트웨어처럼 취급

사고의 틀을 깰 것

자동화 된 셀프서비스 – 단계별 접근 방법



Identify

- 수동 작업 식별
- 측정 가능한 대상 설정
- TF 팀 구성

Initial steps

- 소프트웨어 자동 배포
- 이벤트에 대한 자동 치료
- Read-only 작업에 대한 자동화

Gaining momentum

- Self-service, 운영 환경의 자동 장애 조치
- 패치 자동화
- 완성 단계의 자동화 TASK

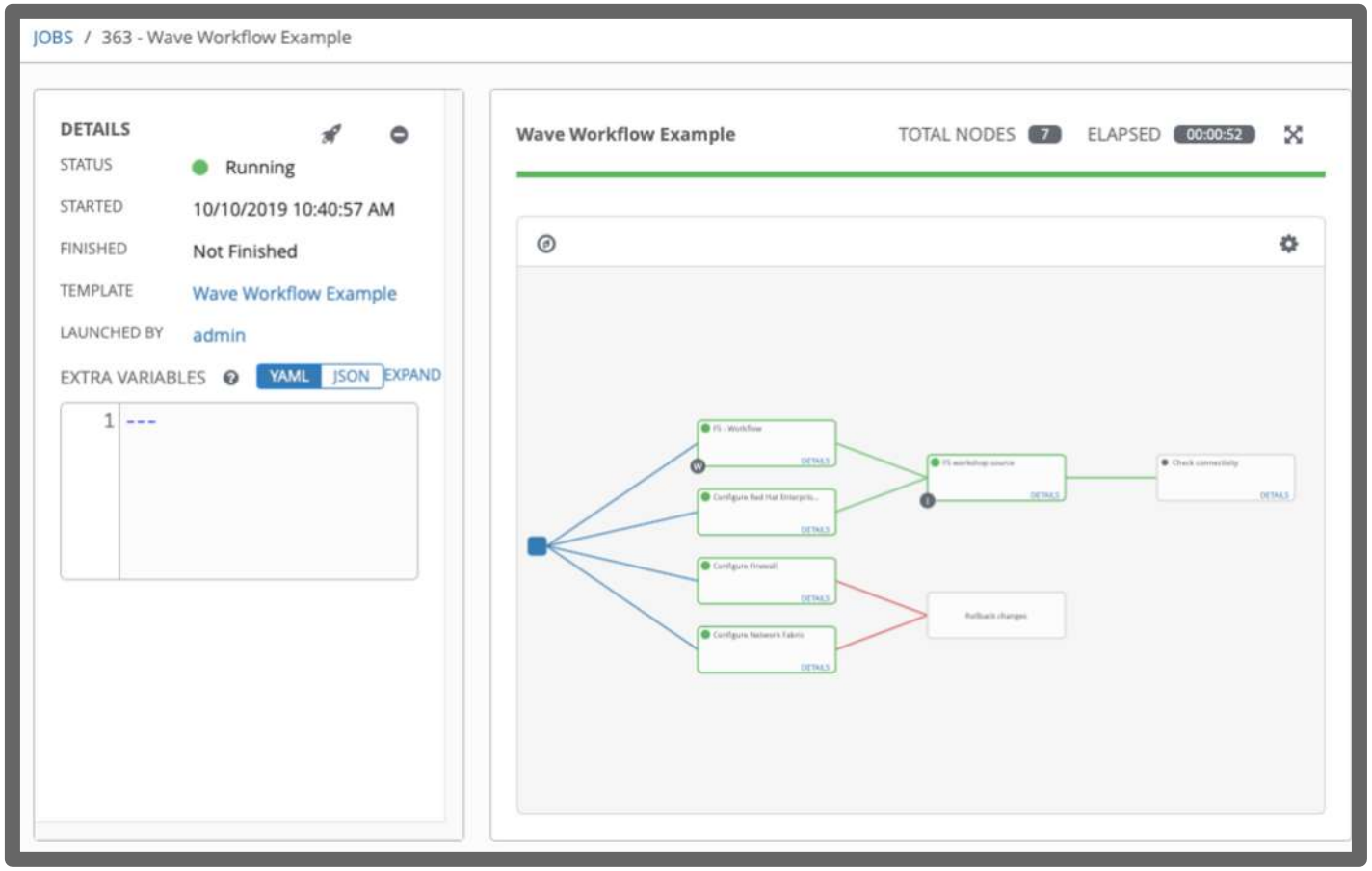
Fully self-service

- 수 초 안에 End-to-end 환경의 자동 배포
- 스토리지 확장, 데이터 관리, 사용자 운영 등을 위한 완벽한 셀프 서비스

Capability / Benefits

Ansible Tower의 워크플로우

- 자동화 단계를 플로우 형태로 구성하여 **전체 자동화 가능**
- **기존 구성 된 템플릿들의 연결**을 통해 손쉬운 워크플로우 생성 및 관리 가능
- 승인이 필요한 단계에서는 워크플로우가 일시 중지되며, **승인 완료를 대기**



Red Hat

Ansible Tower를 통한 셀프서비스 워크플로우

CI/CD Teams

Platforms Teams DB, Web, Middleware..

Application Teams

Security

Other

1.

SELF-SERVICE

주문형 셀프서비스를 이용한 프로비저닝 / 패치 요청
- 승인
- 제어 변경
- 비즈니스 프로세스

2.

프로세스 시작

- 설치 전, 사전 점검

3.

표준 운영 환경 (SOE) 기반의 배포

- VMware
- Cloud Instance templates (AMI, ARM..) Azure, GCP, AWS

4.

회사 표준 환경 구성 업데이트

- NTP, DNS
- Compliance & Security
- OpenSCAP, STIG, CIS
- Install Additional Software

5.

애플리케이션 빌드 및 설정 작업

- AppServers
- DBServers
- Middleware
- COTS applications

6.

기타 설정 작업 (i.e Network)

- Firewall, Ports
- VPC
- VLANs
- Access Control Lists

7.

포스트 점검 수행

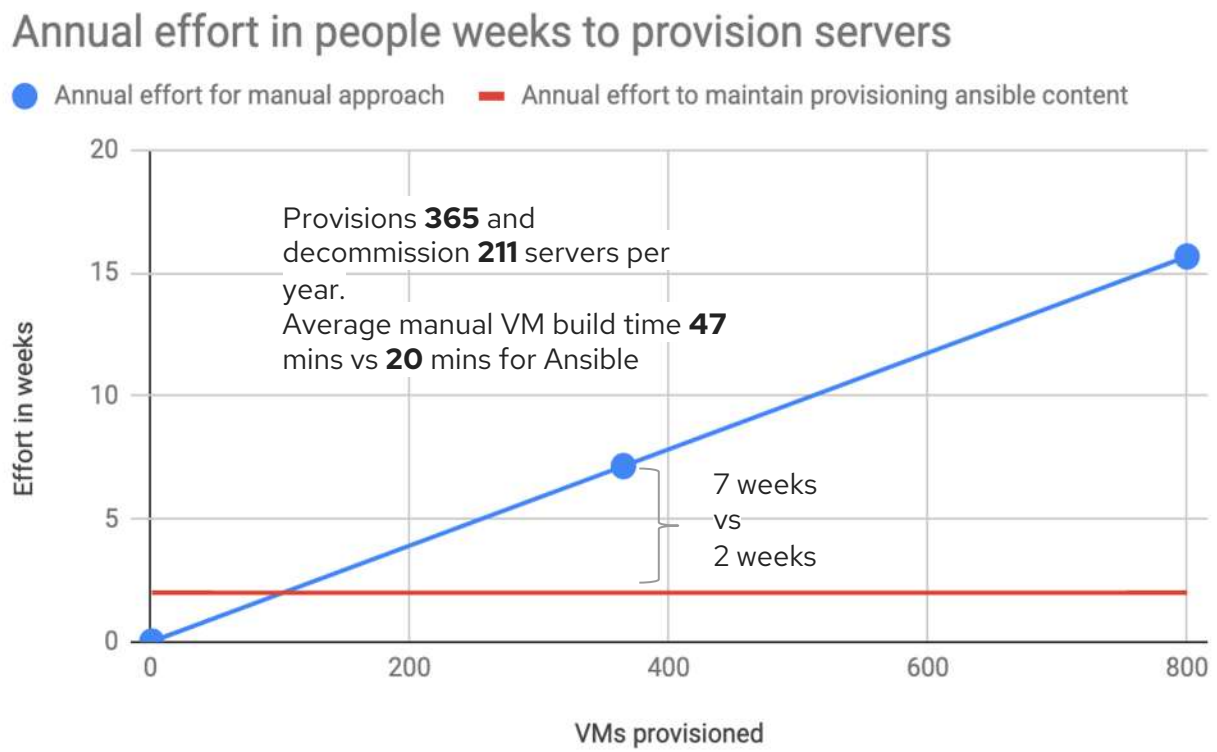
- 기본 검사
- 컴플라이언스 검사
- 서비스 테스트

8.

Application / Business Outcome

Red Hat

자동화 된 셀프서비스의 이점



Key benefits

- Self-Service 환경을 통해, **최소한의 대기 시간과 Linux 운영자 개입없이 서비스 가능**
- 프로비저닝 워크플로우에 통합 된 거버넌스, 규정 준수를 통해 **완벽한 보안 상태 유지**
- 프로비저닝 워크플로우 내에서 ServiceNow를 통합하여 **CMDB 일관성 유지**
- 클라우드 및 관리되지 않는 환경을 위한 **확장과 재사용 가능**한 프로비저닝 워크플로우

Source: Results shared by Red Hat customer in the Financial services

보안 & 컴플라이언스

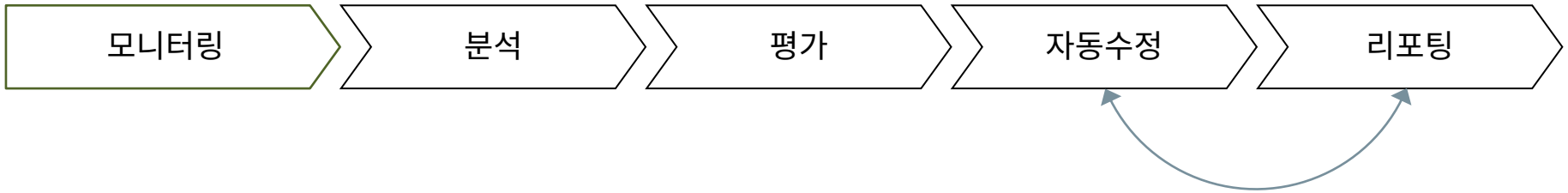
컴플라이언스 정책

조직 내에서 준수해야 하는 **가이드라인**
패스워드 정책 설정 (길이 / 주기 / 특수문자 여부)
필수 에이전트 설치

IT 환경 관리의 어려움

가상화 환경에서 관리해야 하는 가상머신의 수가 매우 많음
클라우드 기반의 인스턴스 생성 / 소멸이 매우 다변적
추적 및 모니터링

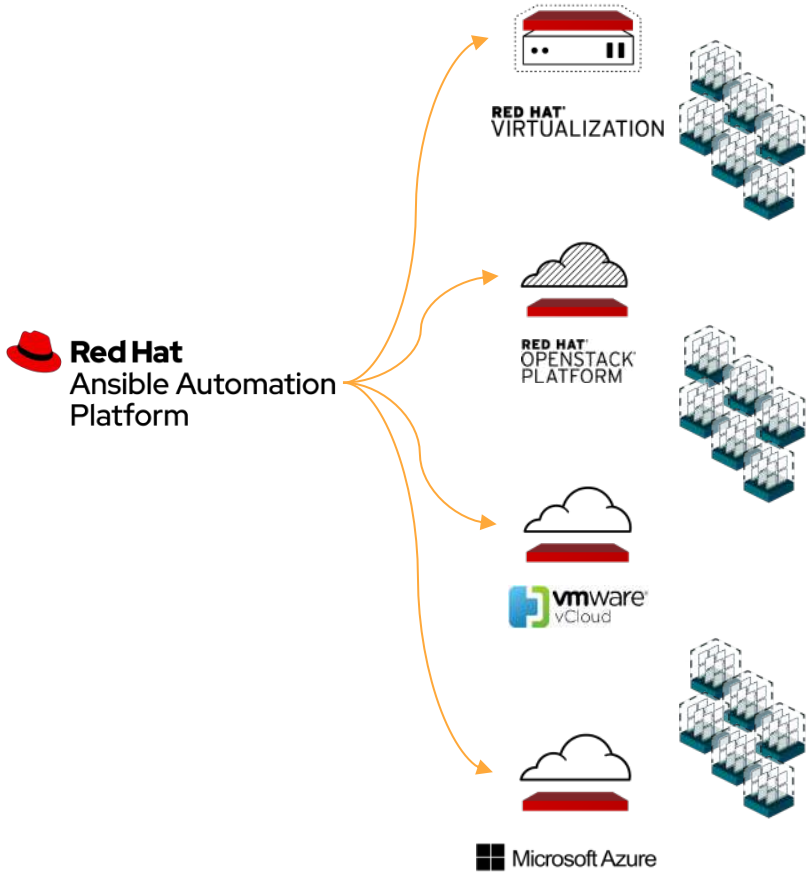
자동화 도구 및 **통합**



Red Hat

보안 & 컴플라이언스

모니터링 → 분석 → 평가



전용 분석 도구 이용

or

자동화 도구만을 이용

Disable tftp Service	pass
Install tcp_wrappers Package	pass
Disable xinetd Service	pass
Set Deny For Failed Password Attempts	fail
Set Password Minimum Length	fail
Set Password Strength Minimum Digit Characters	fail
Set Password Strength Minimum Lowercase Characters	fail
Set Password Strength Minimum Uppercase Characters	fail

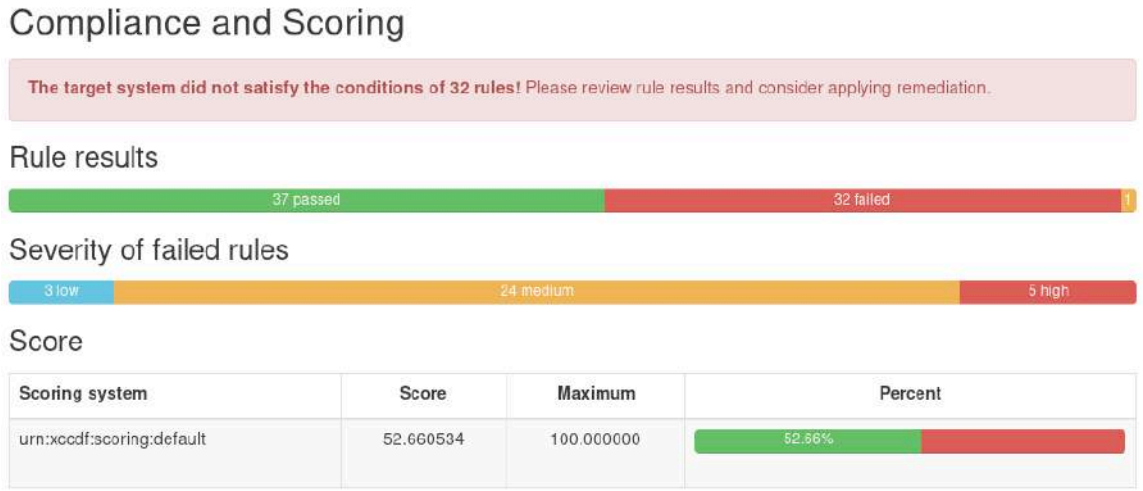
Red Hat

보안 & 컴플라이언스

자동수정 → 리포팅

```
- name: "Ensure SELinux State is Enforcing"
    lineinfile:
      path: /etc/sysconfig/selinux
      regexp: '^SELINUX='
      line: "SELINUX={{ var_selinux_state }}"
      create: yes

- name: "Set Password Minimum Length in login.defs"
    lineinfile:
      dest: /etc/login.defs
      regexp: "^PASS_MIN_LEN *[0-9]*"
      state: present
      line: "PASS_MIN_LEN -
            {{ var_accounts_password_minlen_login_defs }}"
```



Red Hat

Ansible Tower를 통한 보안 패치 워크플로우

CI/CD Teams

Platforms Teams DB, Web, Middleware..

Application Teams

Security

Other

1.

SELF-SERVICE

주문형 셀프서비스를 이용한 프로비저닝 / 패치 요청
- 승인
- 제어 변경
- 비즈니스 프로세스

2.

프로세스 시작

- 설치 전, 사전 점검

3.

OS 패치

-Satellite 또는 기존 패치 도구와 통합
-Ansible 패치 모듈 사용

4.

애플리케이션 패치 & 설정 변경

-AppServers
-DBServers
-Middleware
-COTS applications

5.

기타 설정 작업 (i.e Network)

- Firewall, Ports
- VPC
- VLANs
- Access Control Lists

6.

포스트 점검 수행

- 기본 검사
- 컴플라이언스 검사
- 서비스 테스트

7.

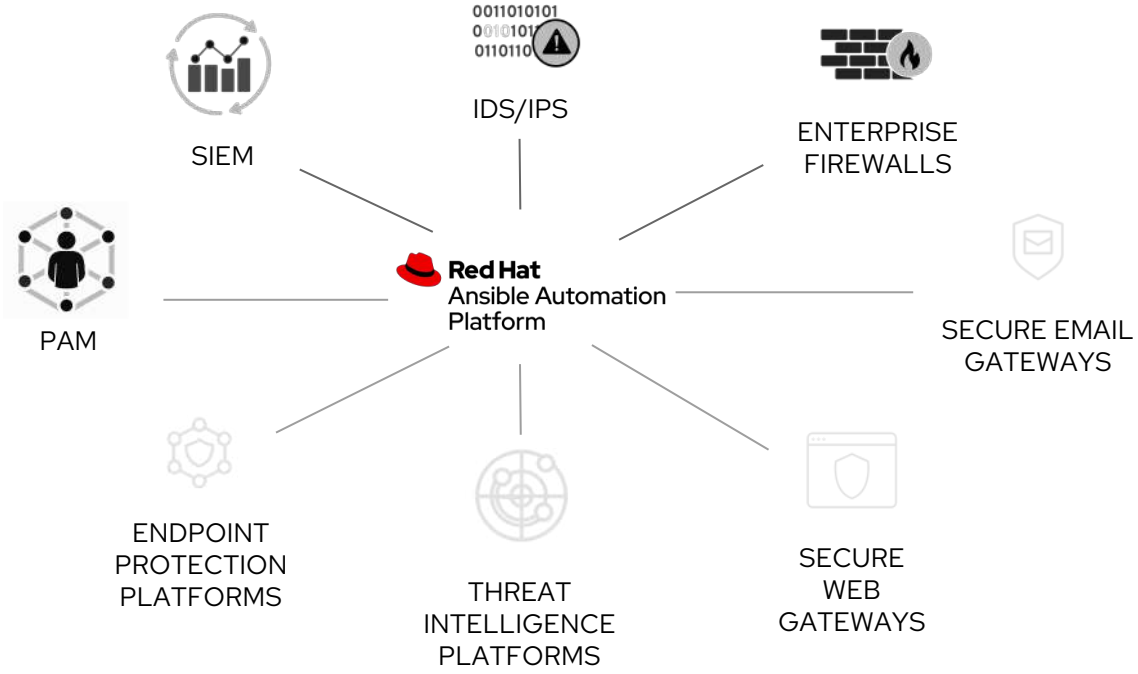
Application / Business Outcome

Red Hat

Ansible의 Security 솔루션 자동화

ORCHESTRATE THREAT RESPONSE ACROSS SECURITY DOMAINS

- 다양한 보안 솔루션 통합 및 오케스트레이션
- 보안 에코시스템들을 자동화하기 위한 다양한 모듈 / 플레이북 / 라이브러리 제공



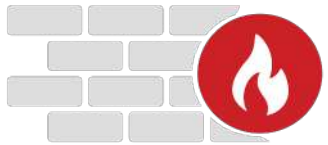
Red Hat

Ansible의 Security 파트너

Security Information & Events Management

splunk>

IBM



Enterprise Firewalls

Check Point SOFTWARE TECHNOLOGIES LTD

CISCO

f5

FORTINET

Intrusion Detection & Prevention Systems

SNORT

Check Point SOFTWARE TECHNOLOGIES LTD

FORTINET

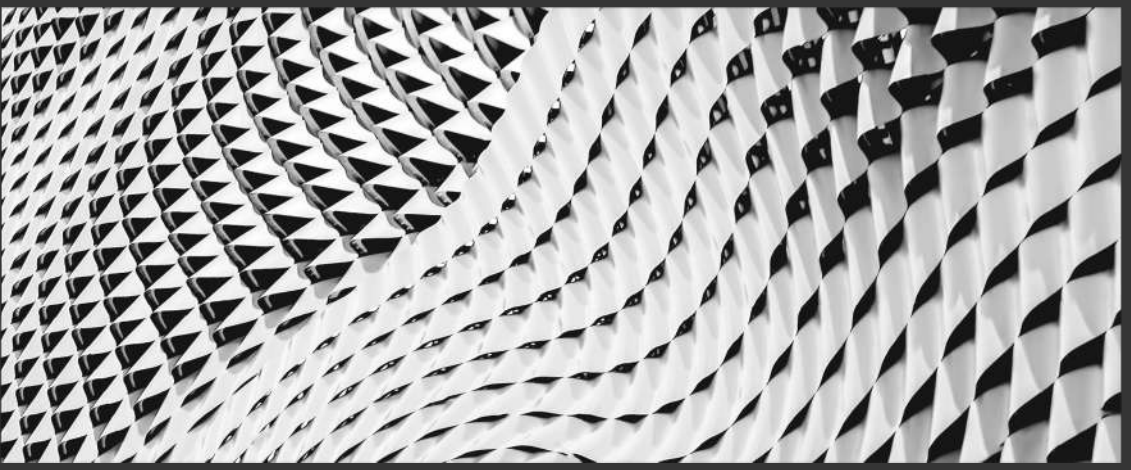
Privileged Access Management

CYBERARK

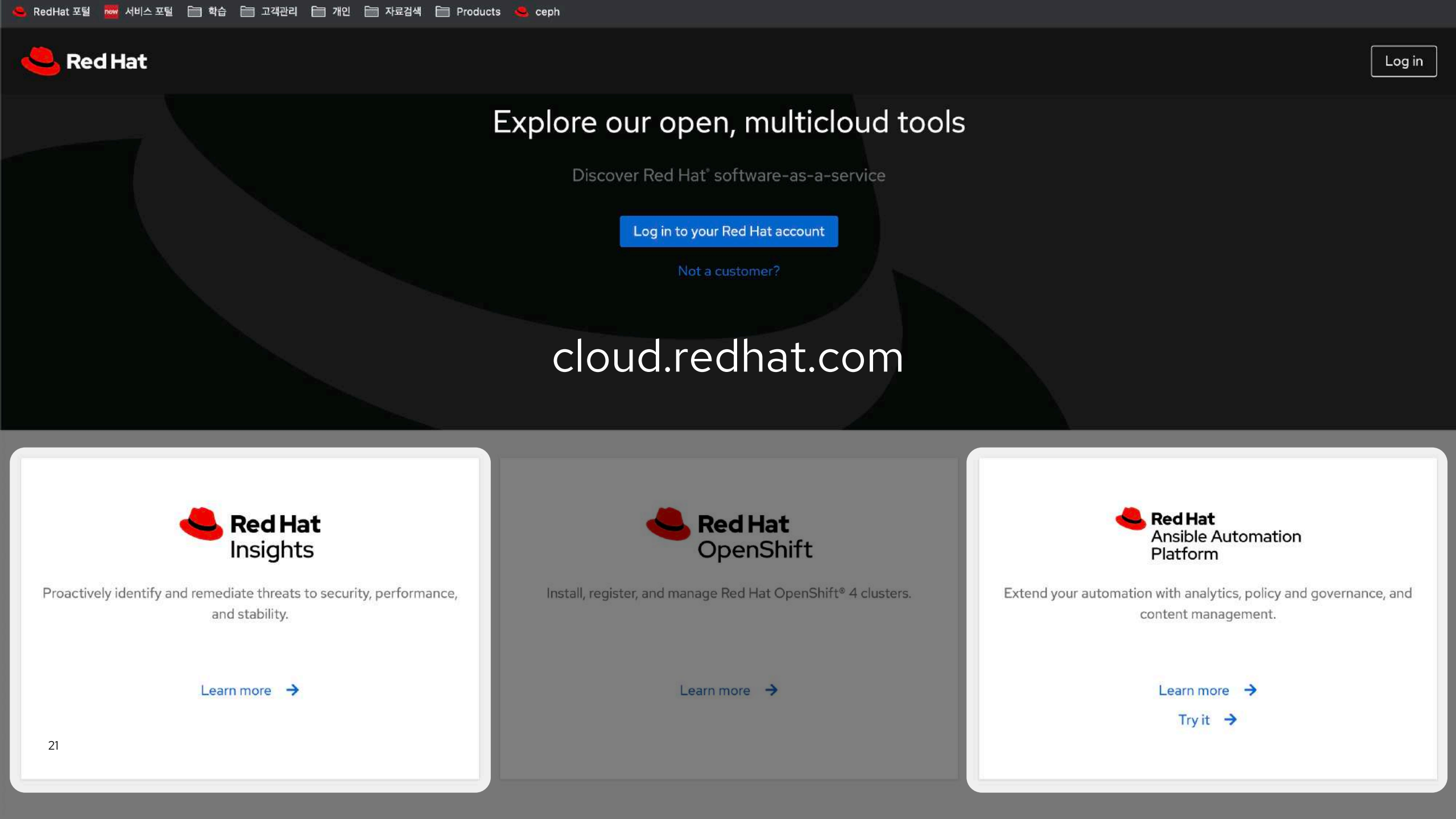
syncope

Red Hat

COVID-19에 대응하는 레드햇의 SaaS 서비스



Red Hat

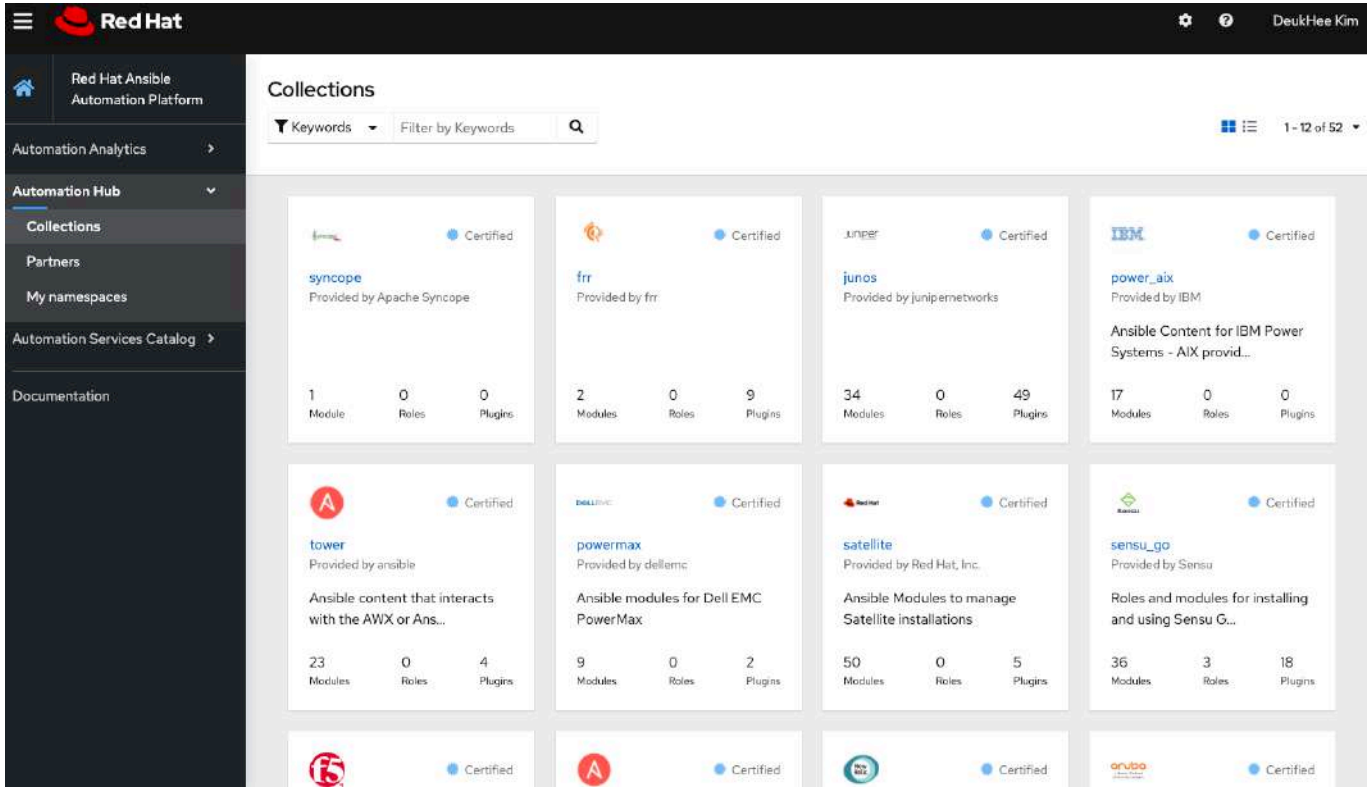

RedHat 포털
서비스 포털
학습
고객관리
개인
자료검색
Products
ceph
Red Hat
Log in
Explore our open, multicloud tools
Discover Red Hat® software-as-a-service
Log in to your Red Hat account
Not a customer?
cloud.redhat.com
Red Hat Insights
Proactively identify and remediate threats to security, performance, and stability.
Learn more
Red Hat OpenShift
Install, register, and manage Red Hat OpenShift® 4 clusters.
Learn more
Red Hat Ansible Automation Platform
Extend your automation with analytics, policy and governance, and content management.
Learn more
Try it

Ansible Content Collections

Discover, publish, and manage Collections

- 레드햇과 파트너를 통해 인증되고, 지원 가능한 SaaS 기반의 **앤서블 컨텐츠 저장소**
- 클라우드 프로바이더, 벤더 및 파트너를 통한 **검증 된 컨텐츠 제공**
- 프로덕션 환경에서의 리스크 최소화

cloud.redhat.com



Red Hat

Automation Hub의 지속적인 컨텐츠 추가

Cloud Activation	VPN Activation	Network Provisioning	Bare Metal Activation	
Azure, Google 및 AWS에서 워크로드를 신속하게 프로비저닝 및 구성	Ansible Automation을 사용하여 VPN 액세스 자동화 / Scale Up	ZTP(Zero Touch Provisioning)을 통해 네트워크 설정의 빠른 교체 및 동적 프로비저닝 제공	WTI Serial 콘솔을 통해 원격 노드 관리	

Red Hat Insights

Red Hat Insights

Red Hat Ansible Automation Platform

What happened?	Why did it happen?	What will happen?	What can we do about it?	How can we fix it?
DESCRIPTIVE ANALYTICS (묘사적 분석)	DIAGNOSTIC ANALYTICS (진단 분석)	PREDICTIVE ANALYTICS (예측 분석)	PRESCRIPTIVE ANALYTICS (처방 분석)	AUTOMATED REMEDIATION (자동 수정)

Never Mind...!!!

- 무엇을 수정해야 하는가?
- 어떻게 수정해야 하는가?
- 수정 대상은 얼마나 많은가?

Insights를 통해 진단받고

Red Hat

Why Red Hat Insights?

종합적인 분석
(w/ Red Hat의 전문 대응 팀)

지속적인
취약성 경고

보안 위험에 대한
가시성 향상

문제해결의
자동화

온 프레미스, 하이브리드 클라우드 및 퍼블릭 클라우드에서 일관된 단일 관리 솔루션

Red Hat

Why Red Hat Insights?

Operational Efficiency

종합적인 분석
(w/ Red Hat의 전문 대응 팀)

지속적인
취약성 경고

보안 위험에 대한
가시성 향상

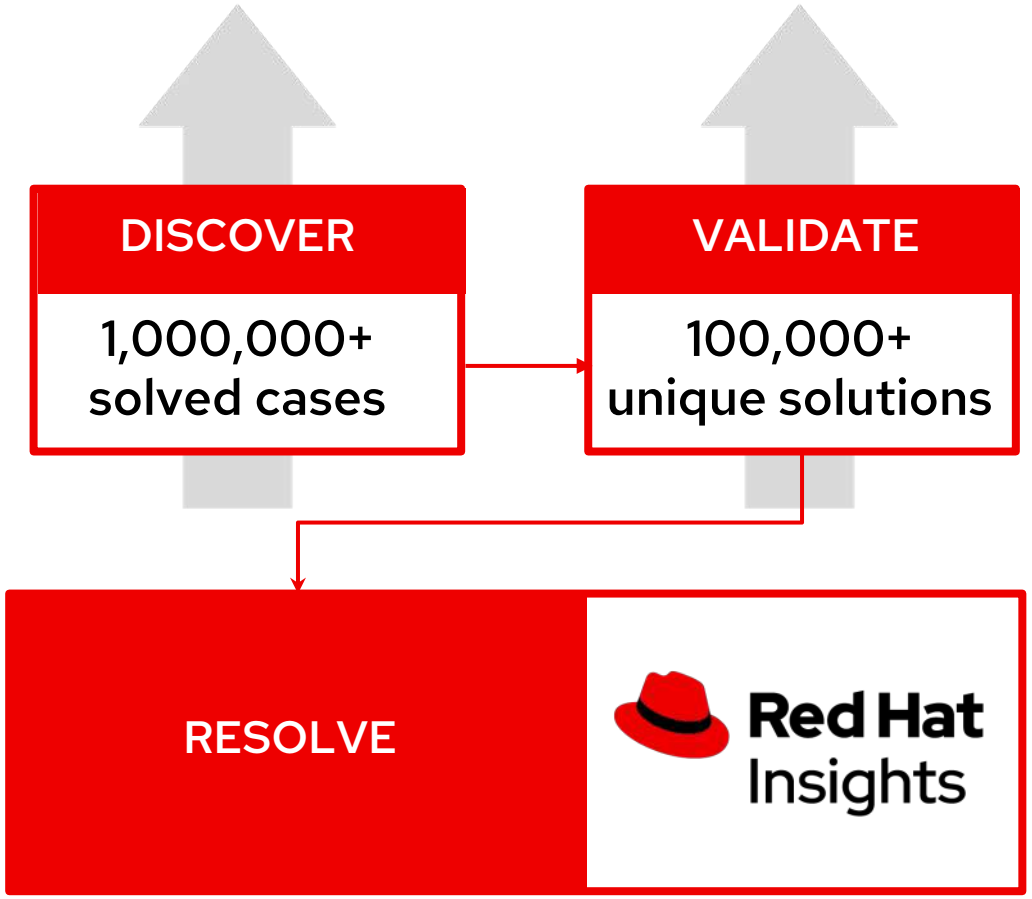
문제해결의
자동화

온 프레미스, 하이브리드 클라우드 및 퍼블릭 클라우드에서 일관된 단일 관리 솔루션

Security Risk Management

Red Hat

실제 경험 기반의 해결 가이드 제공



" Red Hat에 요청 된 85% 이상의 크리티컬한 이슈는 이미 Red Hat과 파트너에 알려진 이슈입니다."

– RED HAT GLOBAL SUPPORT SERVICES

- 전 세계 Red Hat 고객을 통한 20년 이상의 축적 데이터 기반
- 신규 리스크의 지속적인 파악
- 기업에서 수집 된 데이터와 레드햇 전문 대응팀의 실제 경험

Red Hat

Red Hat Insights

Dashboard
Advisor
Vulnerability
Compliance
Patch
Drift
Policies
Inventory
Remediations
Subscription Watch

Documentation

Dashboard

Insights system inventory

432 8% of total syste...
Systems running insights-client

81 stale systems
79 systems to be removed

Subscription Watch utilization summary

Red Hat Enterprise Linux 4%
Red Hat OpenShift 1%

Patch

395 systems affected

1227 security advisories
3084 bug fixes
602 enhancements

Advisor recommendations

9 Incidents detected

0 Critical 20 Important 70 Moderate 30 Low

120 Recommendations impacting 277 systems

Vulnerability

2648 CVEs impacting your systems

224 CVSS 8.0 - 10 2002 CVSS 4.0 - 7.9 422 CVSS 0.0 - 3.9

Compliance

DISA STIG for Red Hat Enterprise Linux 7
0 systems 0% passes

Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
0 systems 0% passes

Standard System Security Profile for Red Hat Enterprise Linux 7
9 systems 27% passes

10 more compliance policies

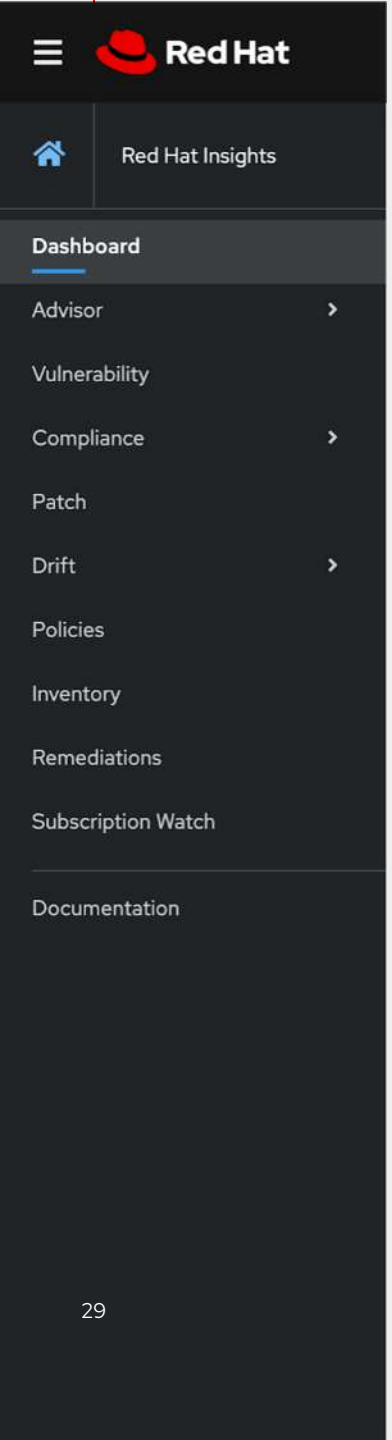
Remediations

Success elfutils
07 May 2020 17:25 UTC

Success Postfix_patch
07 May 2020 16:28 UTC

Success glibc_patch
07 May 2020 12:19 UTC

Success CC_SQL01



Overview of Red Hat Insights

Advisor
가용성, 성능 및 안정성 위험 분석

Vulnerability
Red Hat Enterprise Linux CVE 평가, 개선 및 보고

Compliance
OpenSCAP에 정의 된 규정 준수 평가 및 모니터링

Subscription Watch
Red Hat 서브스크립션 현황을 효율적이고 확실하게 관리

Drift
기준 프로파일과 비교 및 이전 상태와 비교하여 변경 내용 확인

Policies
자체 정책을 정의하고 모니터링하여 불일치 식별

Patch
최신 상태를 유지하기 위한 Red Hat 권고 적용 가능성 분석

Red Hat

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