Red Hat
Ansible Automation
Platform

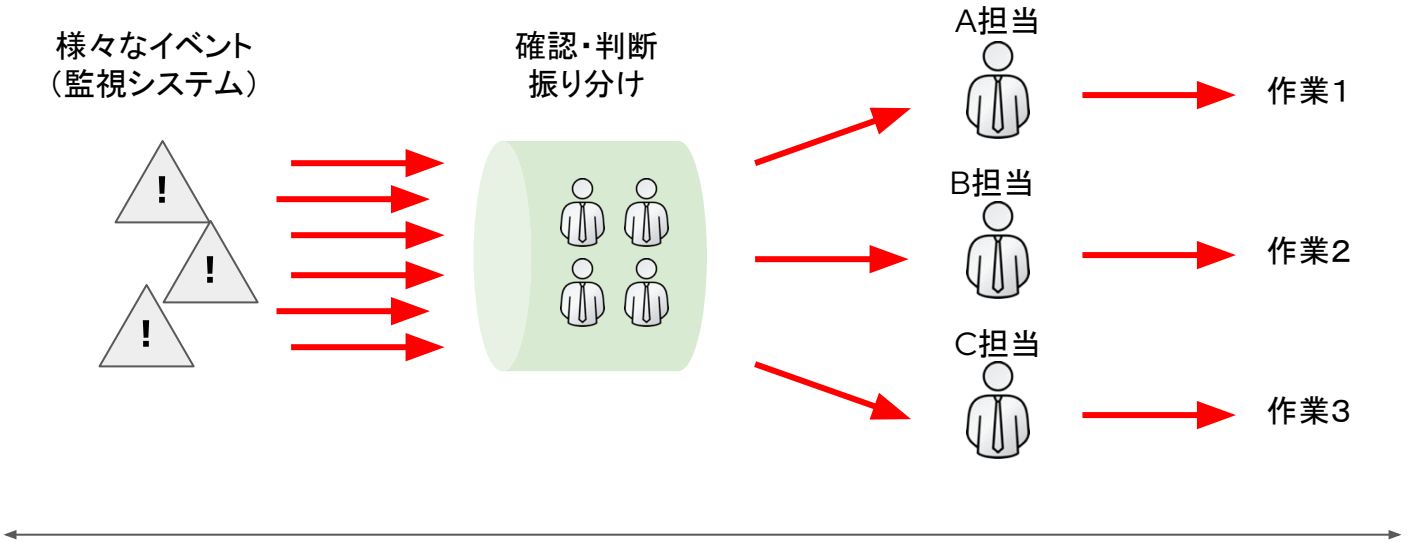
Zabbix x Ansible で実現する障害対応の自動化

Event-Driven Ansible による Zabbix イベント連携

2023-11-16

Tomoaki Nakajima
Red Hat

セッションの概要



ここに Zabbix x Ansible の組み合わせを導入する何がおきるのか？

Red Hat

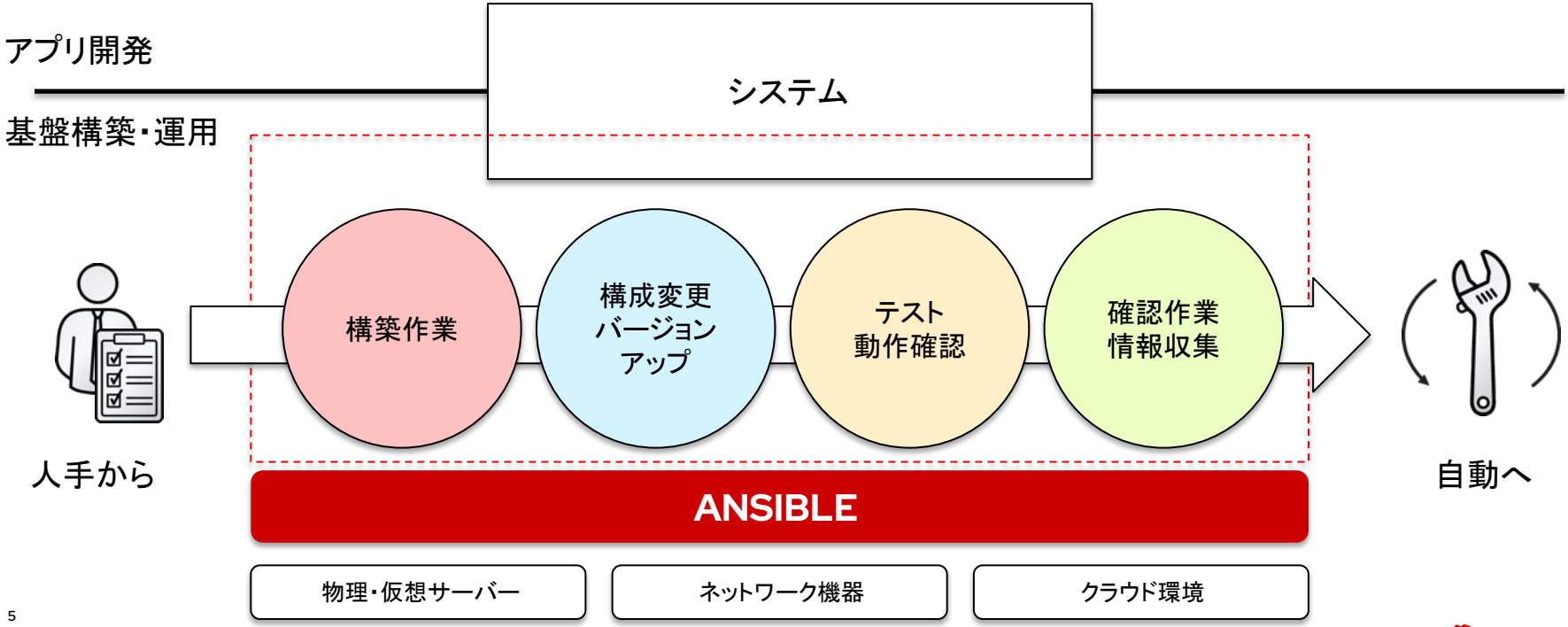
アジェンダ

- Ansibleの概要
- Event-Driven Ansible
- Zabbix x Ansible
- まとめ

Ansible の概要

Ansible とは

- IT基盤の構築や運用を自動化する「 IT Automation」を実現する。



Red Hat

Ansibleの特徴：多様なインフラ環境に対応

140+

Certified Content Collections

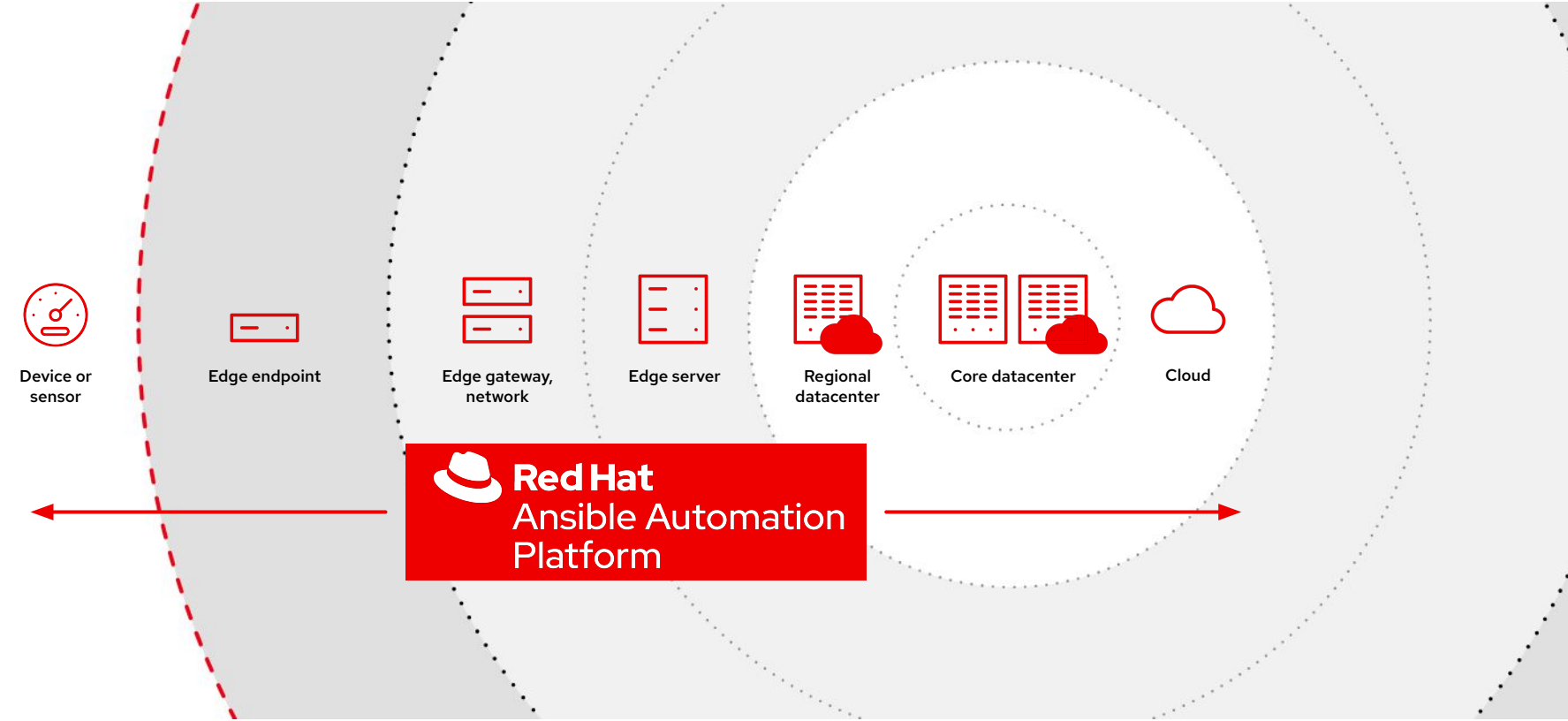
55+

Certified technology partners

Infrastructure Cloud Network Security Edge

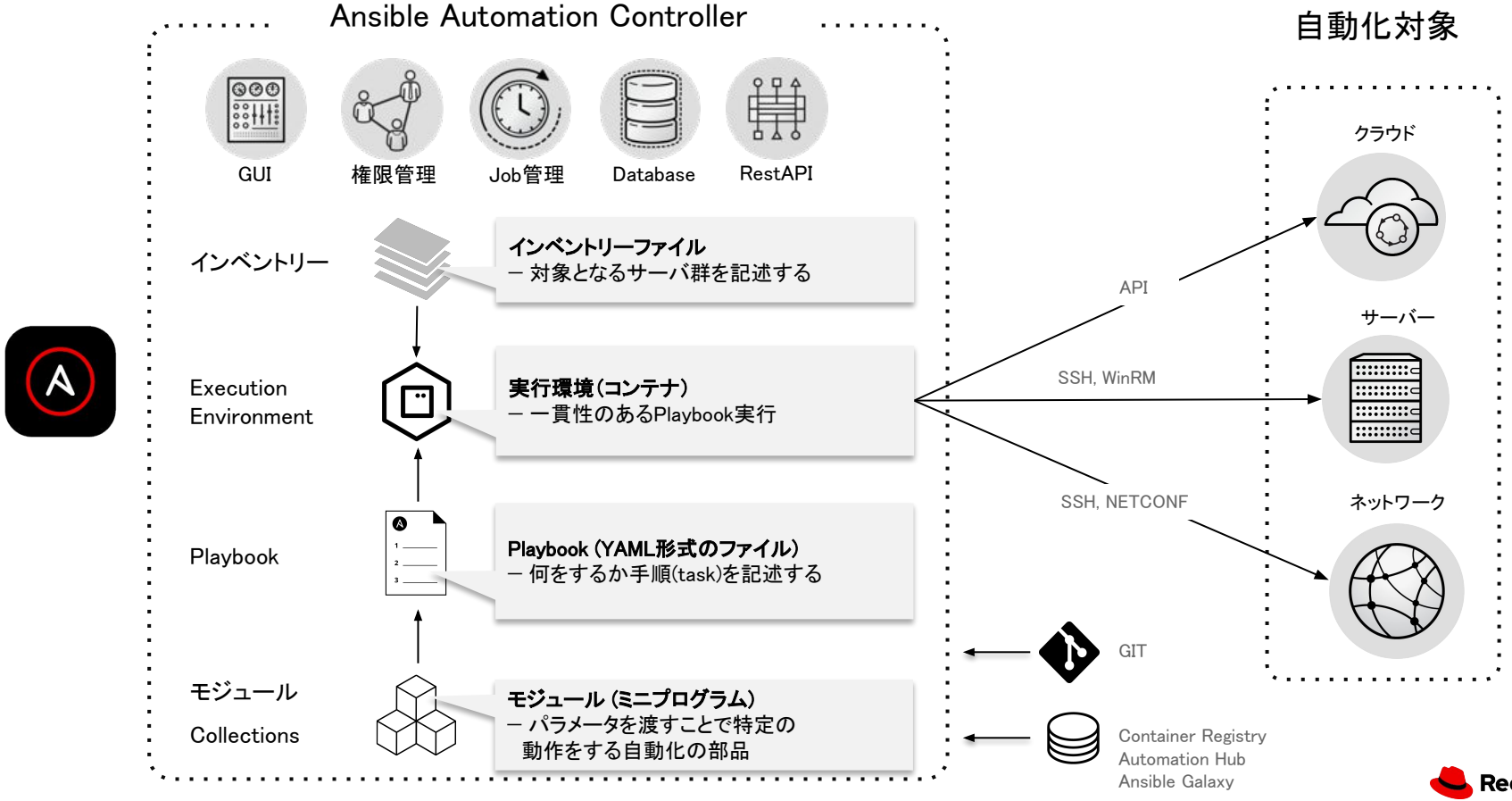
Red Hat

Ansibleの特徴：データセンターからエッジまで、統合された自動化環境を提供



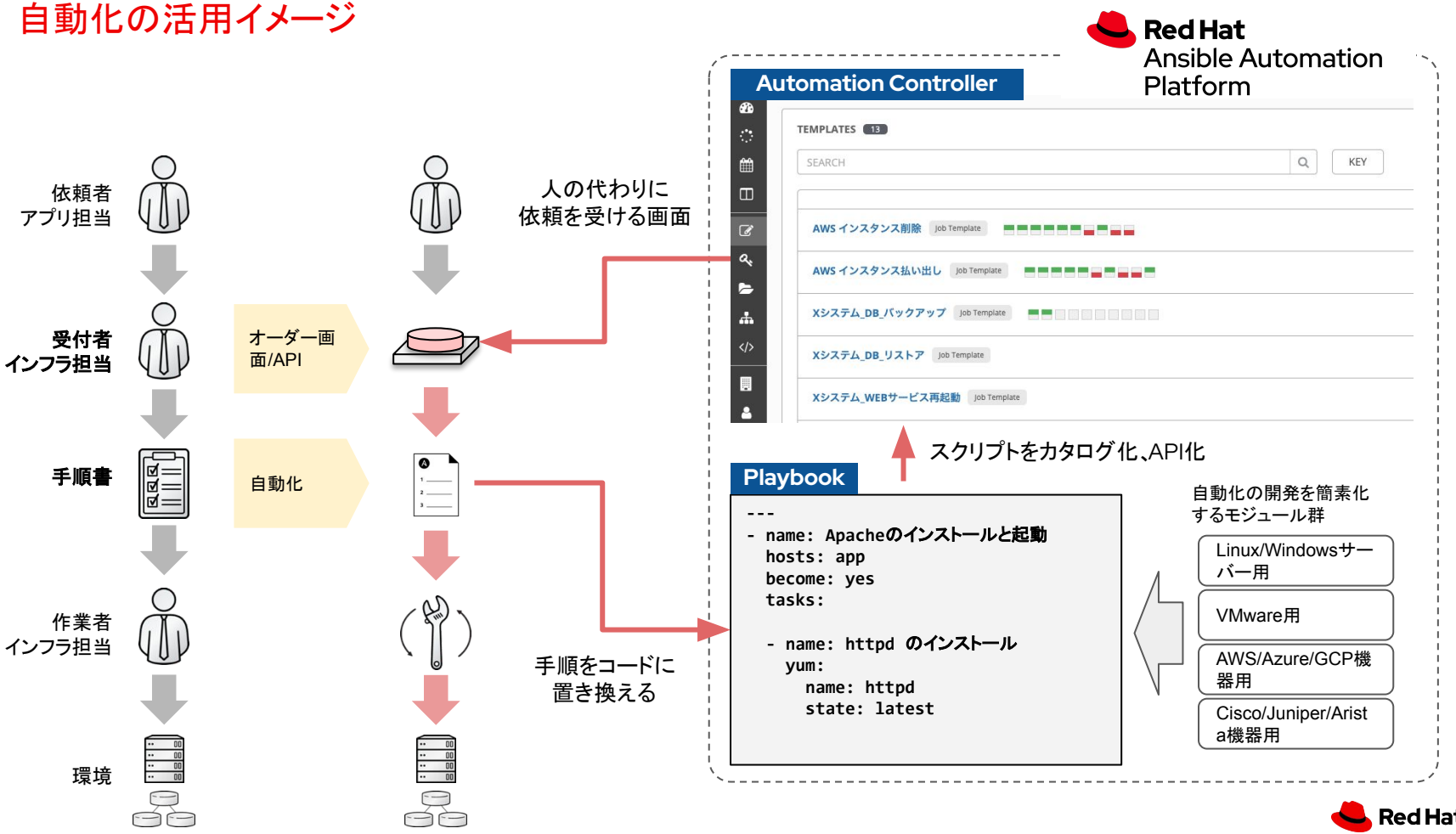
Red Hat

Ansible はサーバーにインストールして利用（Managed Service も利用可能）



Red Hat

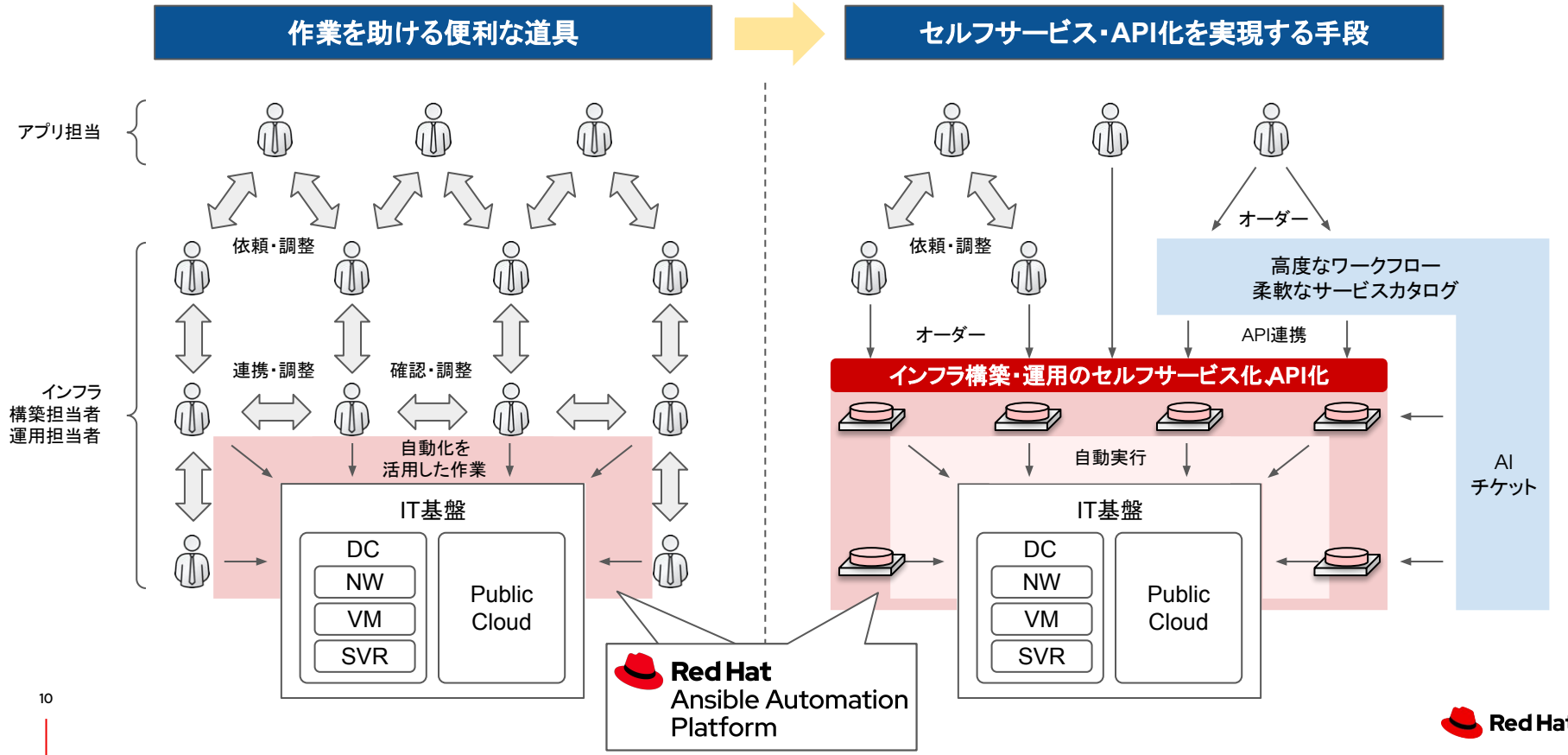
自動化の活用イメージ


Red Hat
Ansible Automation
Platform
Automation Controller
TEMPLATES 13
SEARCH
KEY
AWS インスタンス削除 Job Template
AWS インスタンス払い出し Job Template
Xシステム_DB_バックアップ Job Template
Xシステム_DB_リストア Job Template
Xシステム_WEBサービス再起動 Job Template
依頼者
アプリ担当
受付者
インフラ担当
作業者
インフラ担当
環境
オーダー画面/API
自動化
人の代わりに
依頼を受ける画面
スクリプトをカタログ化、API化
手順をコードに
置き換える
Playbook

- name: Apacheのインストールと起動
hosts: app
become: yes
tasks:
- name: httpd のインストール
yum:
name: httpd
state: latest
自動化の開発を簡素化
するモジュール群
Linux/Windowsサーバー用
VMware用
AWS/Azure/GCP機器用
Cisco/Juniper/Arista機器用

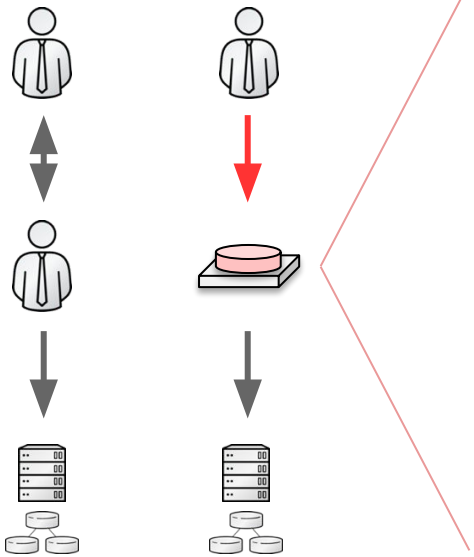
自動化トレンド：2つの自動化の考え方

こちらの使い方が急速に広がっている



Red Hat

セルフサービス化・API化される作業の例



サーバー関連
- ❑ 仮想サーバーの払い出し、削除
- ❑ 仮想サーバーの構成変更
- ❑ サーバーの再起動
- ❑ 作業前のバックアップ、リストア
- ❑ ログ取得
- ❑ パスワードリセット、変更
- ❑ ユーザー作成、削除

監視・運用関連
- ❑ 監視エージェント導入・設定
- ❑ 監視項目の追加
- ❑ 監視の一時停止、再開
- ❑ メンテナンスページの表示・非表示
- ❑ 障害の一次対応（情報取得など）

クラウド関連
- ❑ インスタンス払い出し
- ❑ インスタンスの再起動
- ❑ VPC/セキュリティグループ設定
- ❑ IAM設定、ユーザー作成

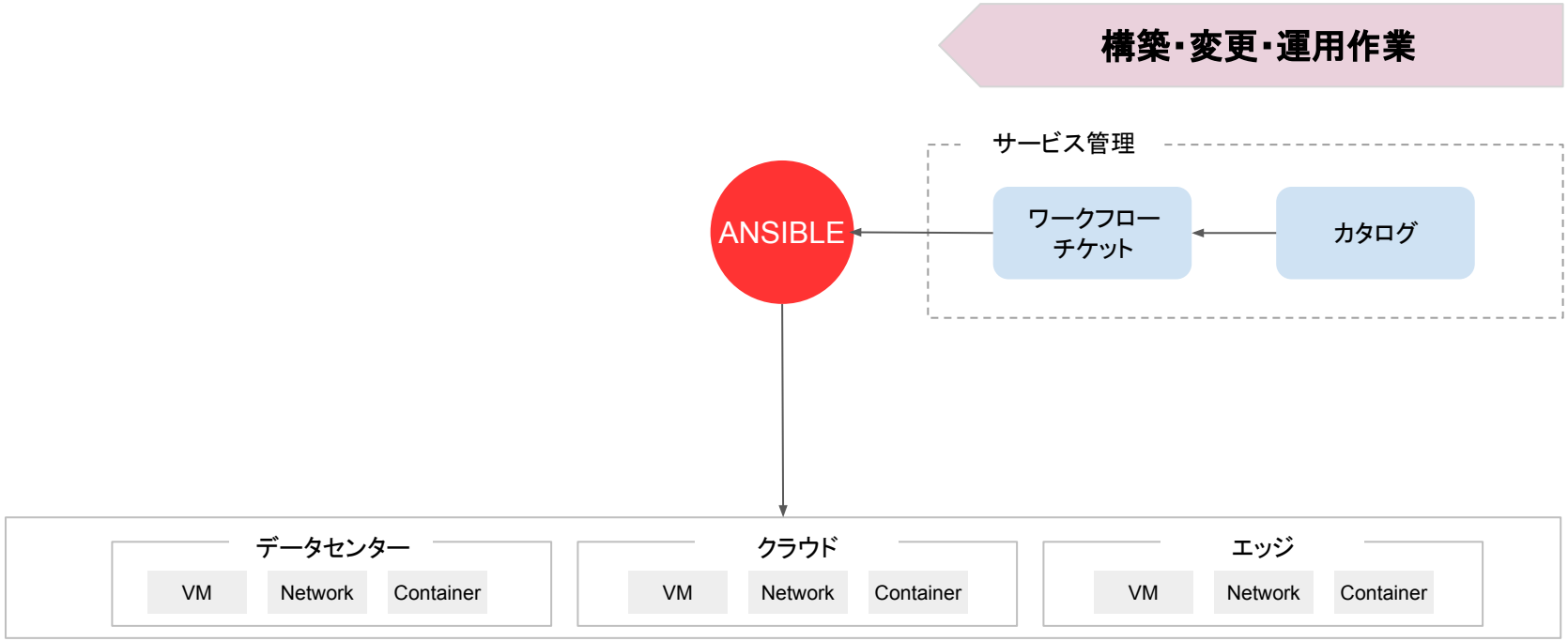
セキュリティ関連
- ❑ IDS/IPS エージェント配布と設定の強制
- ❑ FWルールの強制
- ❑ SIEM連携による自動防御

ネットワーク関連
- ❑ IPアドレスの払い出し
- ❑ ACL変更
- ❑ 最新コンフィグバックアップ
- ❑ ロードバランサーへのサーバー追加、削除
- ❑ FWのポート開け閉め
- ❑ DNSエントリー追加、削除
- ❑ E2E疎通確認

アプリケーション関連
- ❑ サービスの再起動
- ❑ DBバックアップ、リストア
- ❑ 開発環境の払い出し、削除
- ❑ 証明書の更新
- ❑ リリース作業

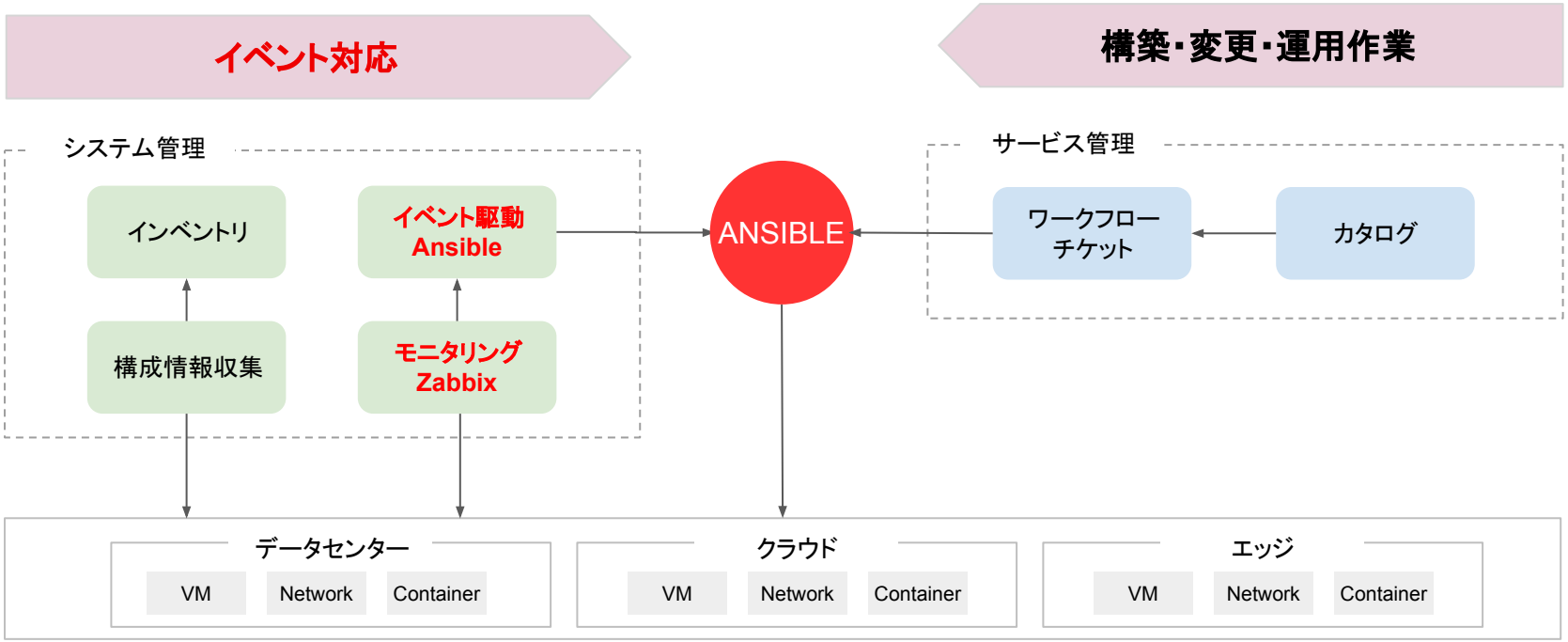
その他
- ❑ チケット更新(ServiceNow等)
- ❑ 最新設定情報の収集、CMDB構築
- ❑ 設定報告書の作成

Ansible を用いた構築・変更・運用作業のシステムイメージ



Red Hat

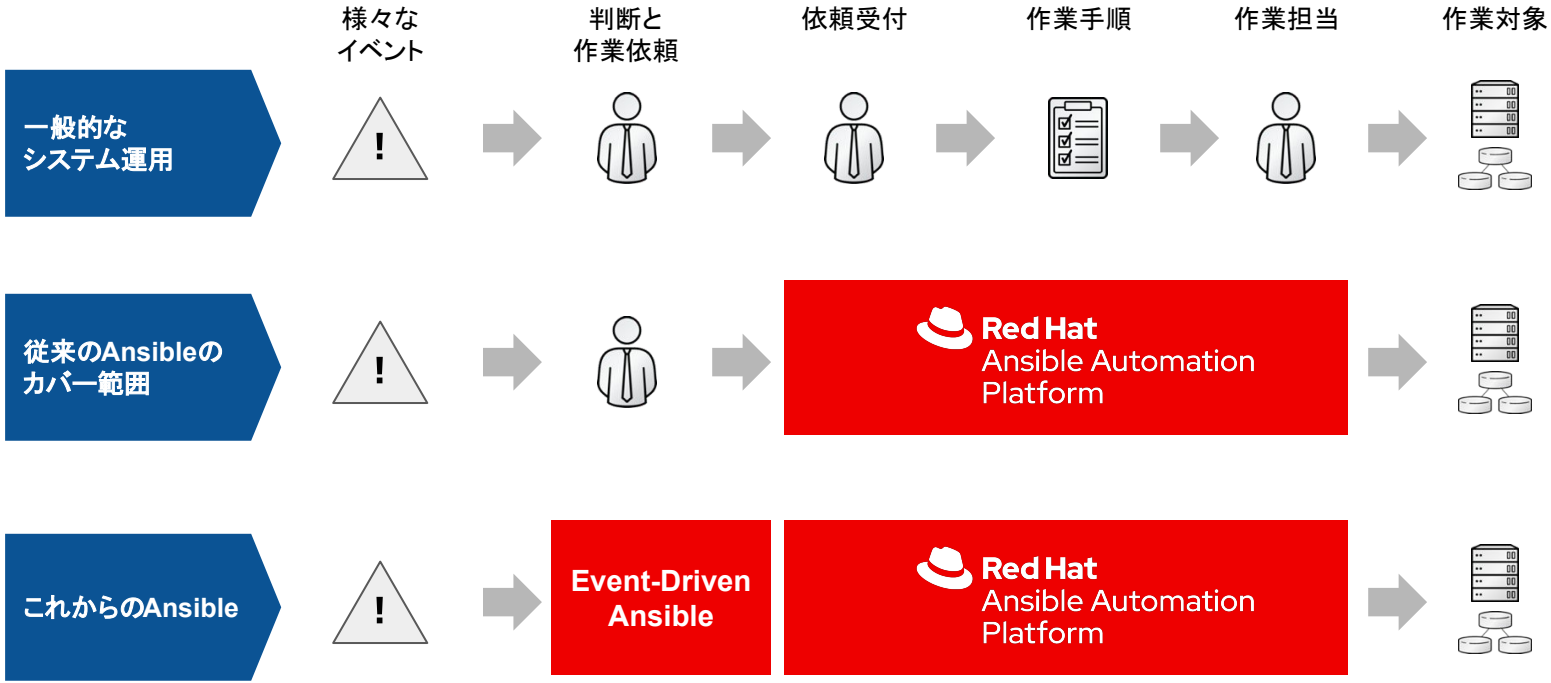
イベント対応の自動化（本日の主題）



Red Hat

Event-Driven Ansible

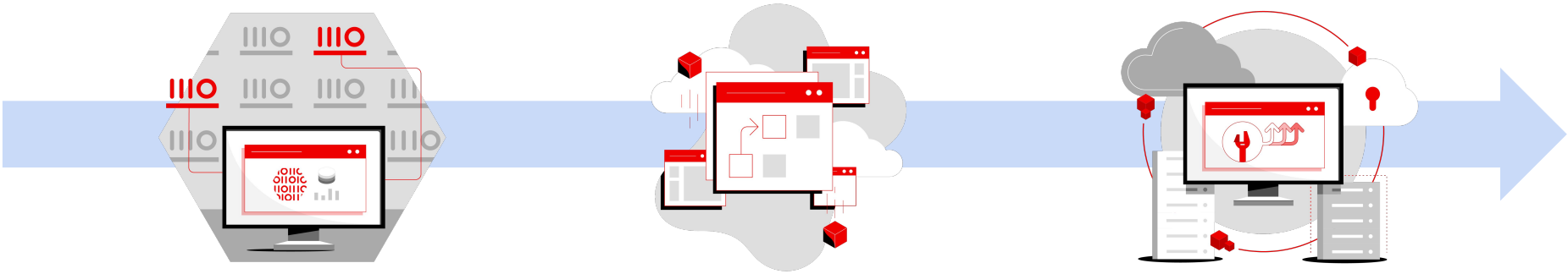
Event-Driven Ansible の位置づけ



Red Hat

Event-Driven Ansible の主要な構成要素

シンプル、パワフル、エージェントレス



ソース

使用するイベントデータの
全ソース

ルール

Event-Driven Ansible® を使用して
作成

アクション

条件またはイベントが一致すると、
Ansible の自動化が実行される

Ansible Rulebook には、受け取るイベントのソースと、特定の条件が満たされた場合に実行する自動化の指示が含まれており、柔軟に記述できます。

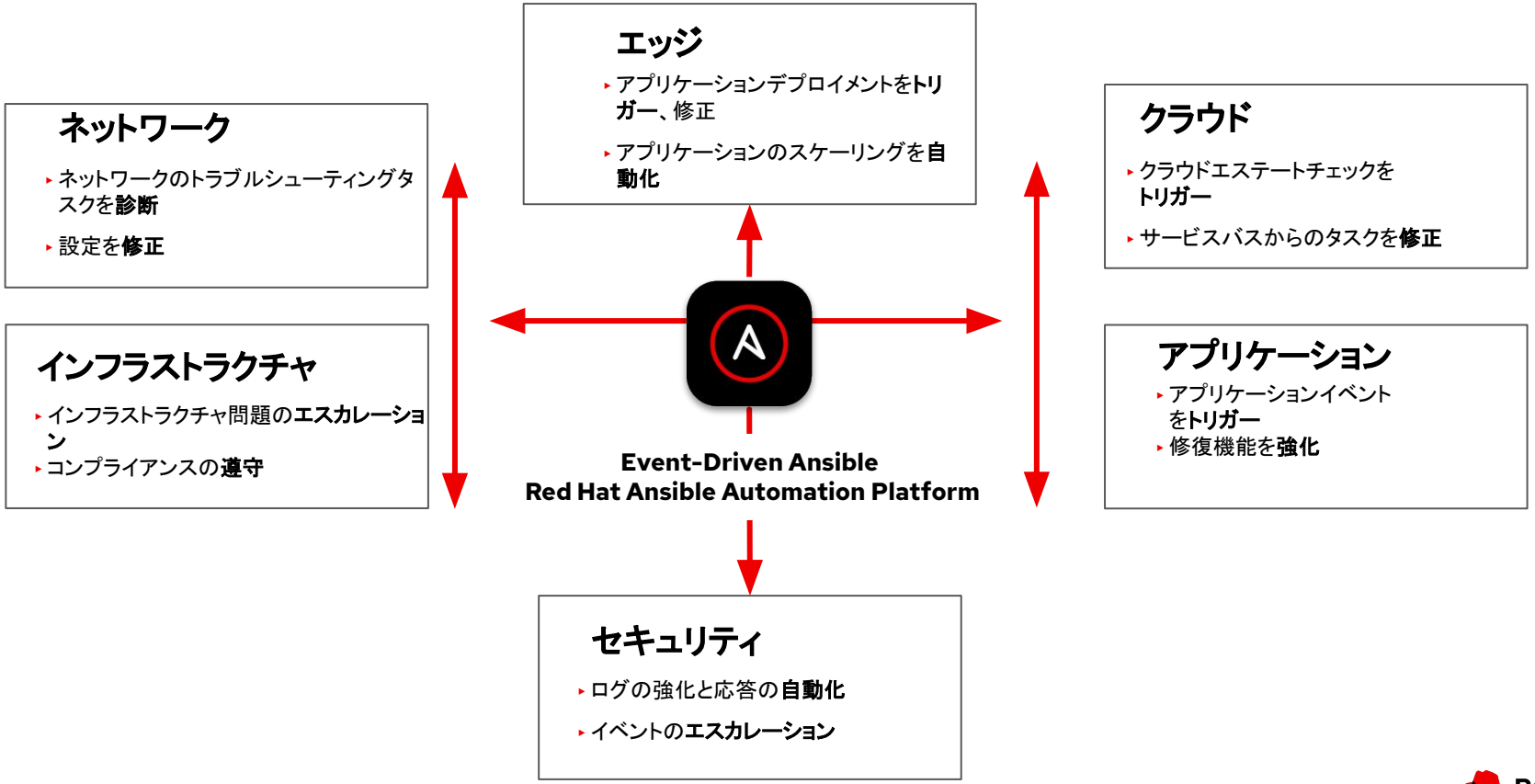
Ansible Rulebook

ルールを使用したシンプルな宣言型決定

- **ルールエンジンがイベントを処理**
  - ルールエンジンが、条件およびアクションに基づくルールトリガーを実行できる
  - ルールは Ansible Rulebooks に記述される
  - ルールを特定のホストやグループで発生するイベントに適用できる
- **イベントに対するアクションの条件付き管理**
  - 論理条件に対する単純な YAML 構造
  - イベントは各種アクションをトリガーできる
    - Ansible Playbook の実行
    - モジュールの実行
    - 新規イベントのイベントハンドラーへのポスト
- **YAML に類似した形式の使用**
  - 現在の Ansible ユーザーは、Rulebook の記述を短期間で学習して使用できる

```yaml
- name: Automatic Remediation of a web server
  hosts: all
  sources:
    - name: listen for alerts
      ansible.eda.alertmanager:
        host: 0.0.0.0
        port: 8000
  rules:
    - name: restart web server
      condition: event.alert.labels.job == "fastapi" and
event.alert.status == "firing"
      action:
        run_playbook:
            name: ansible.eda.start_app
```

イベント処理にAnsibleの自動化能力をそのまま転用可能



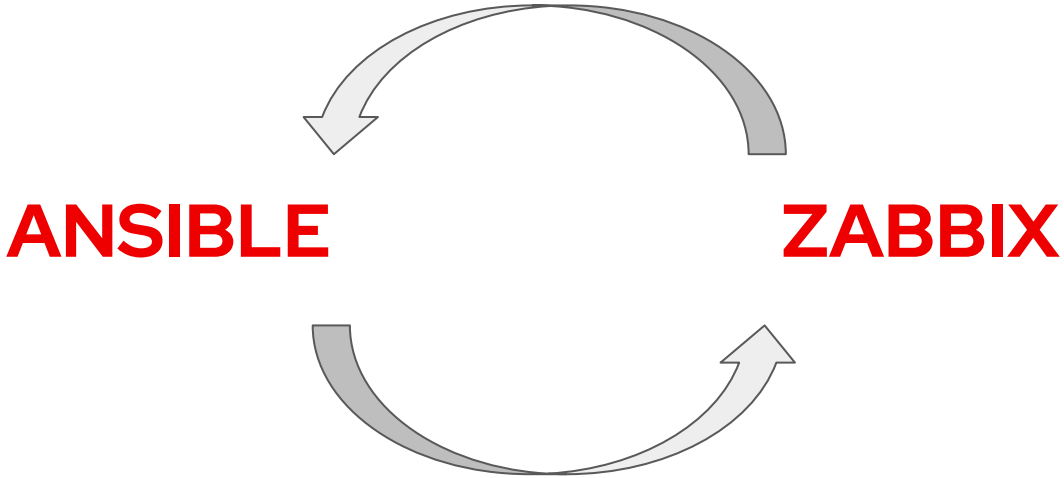
Red Hat

Zabbix x Ansible

AnsibleとZabbixの関係

Zabbix からイベントを発信し、そのイベントをEDAで判定して定義済みの自動化を実行する（こちらを取り上げます）

参考：https://www.zabbix.com/integrations/ansible



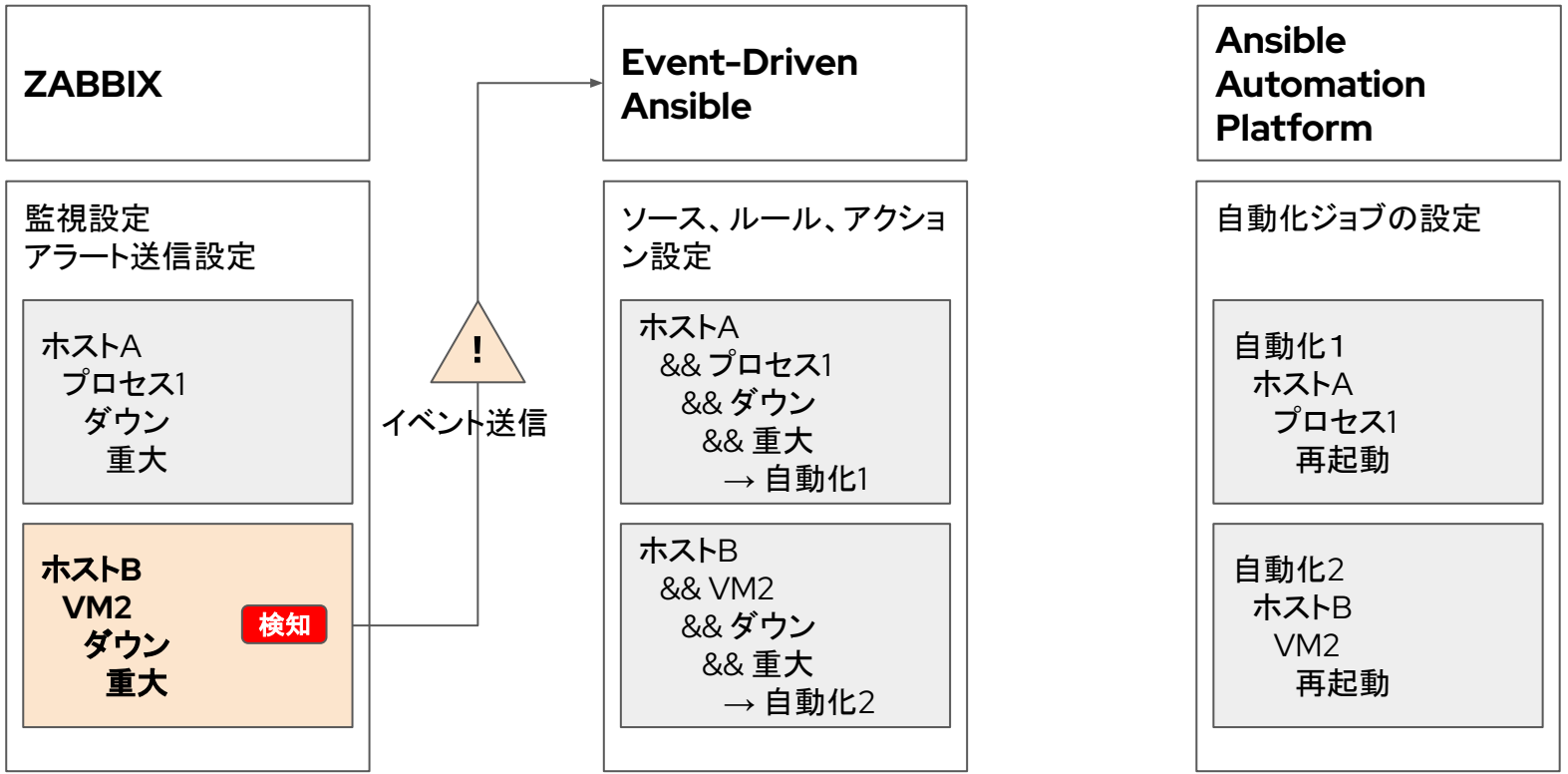
Zabbix上の監視設定をAnsible Playbook で自動化することが可能（今回は取り上げない）

参考：https://docs.ansible.com/ansible/latest/collections/community/zabbix/index.html

Red Hat

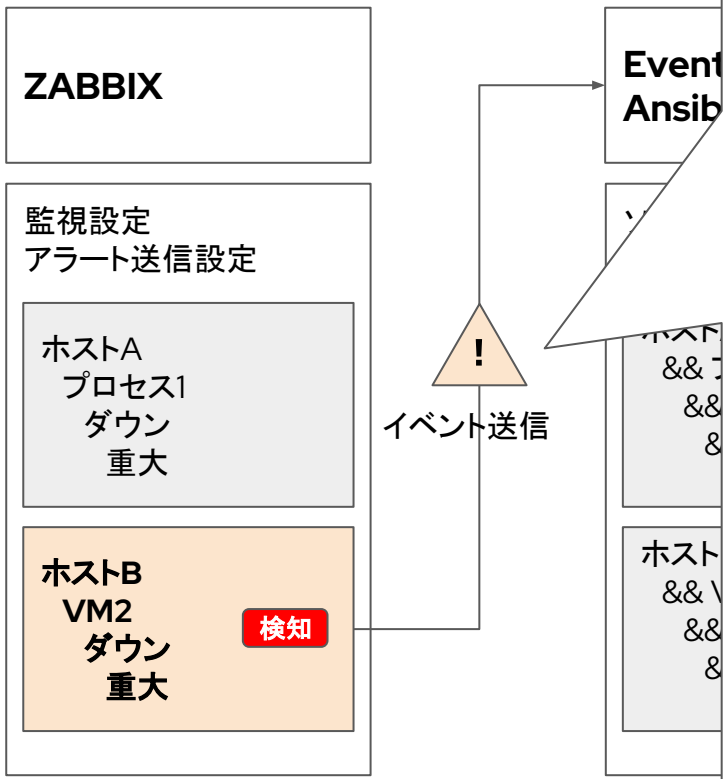
連携のイメージ（1）

連携のイメージ（2）



Red Hat

連携のイメージ（3）



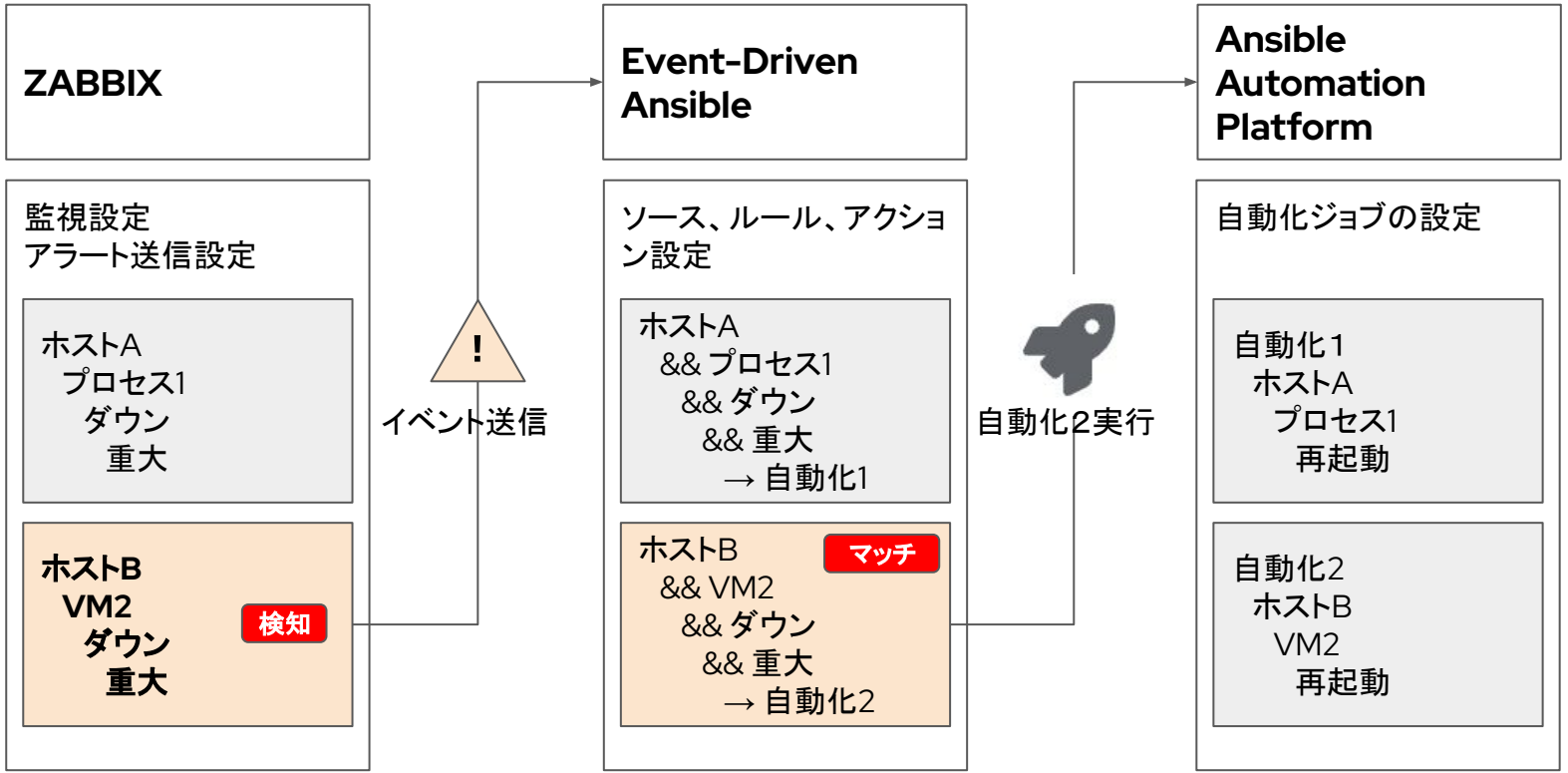
送信されるイベントデータサンプル


```
{'event': {'meta': {'endpoint': 'endpoint',
                    （省略）
                    'payload': {'HTTPProxy': '',
                                'acknowledged': 'No',
                                'endpoint': '/endpoint',
                                'event_date': '2023.10.26',
                                'event_datetime_timestamp': 1698281140,
                                'event_id': 35,
                                'event_name': 'VM2死活監視',
                                'event_nseverity': 4,
                                'event_object': 0,
                                'event_severity': 'High',
                                'event_source': 0,
                                'event_tags': {},
                                'event_time': '00:45:40',
                                'event_value': 1,
                                'host_groups': ['Linux servers'],
                                'host_host': 'demo-hostB',
                                'host_id': 10602,
                                'host_ip': '172.31.0.155',
                                'host_port': '10050',
                                'monitoring_source': 'Zabbix sever',
                                'operation_data': '0',
                                'send_to': '11.22.33.44:8888',
                                'subject': 'Event ID: 35, Host: '
                                           'demo-hostB, Problem: VM2死活監視',
                                'trigger_description': '',
                                'trigger_id': 23415,
                                'trigger_name': 'VM2死活監視エラー'}}}}
```

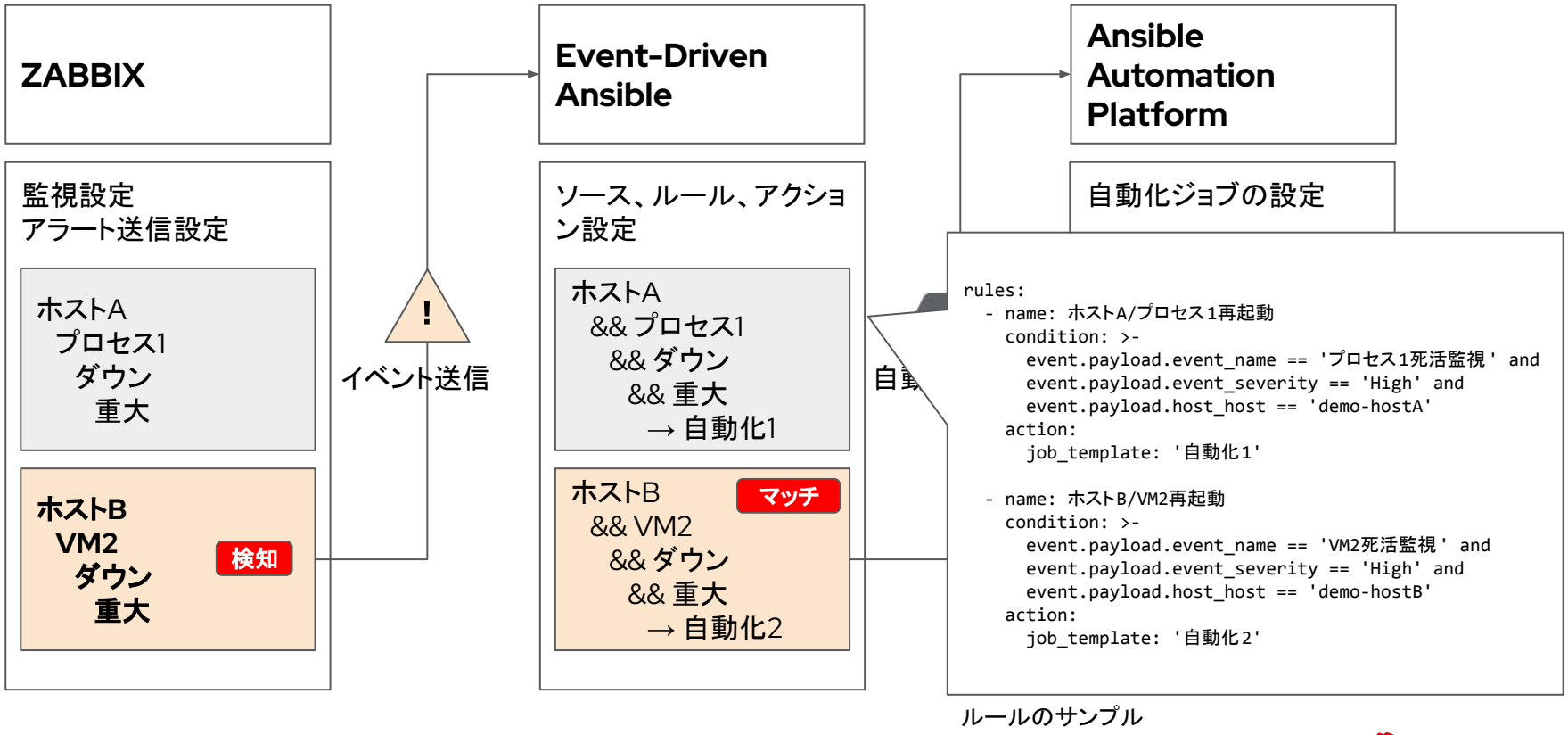

Red Hat

連携のイメージ（4）

送信されるイベントデータサンプル



連携のイメージ（5）

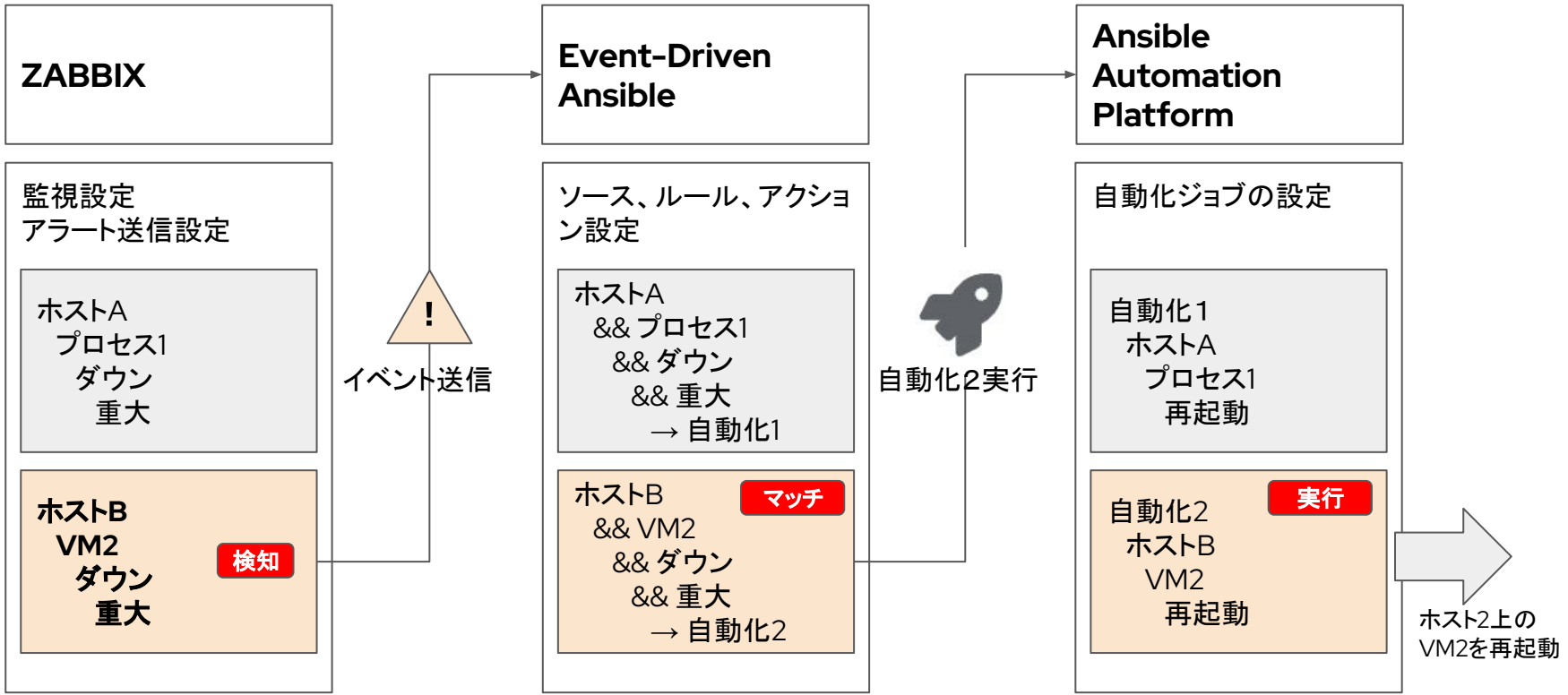


ルールのサンプル

Red Hat

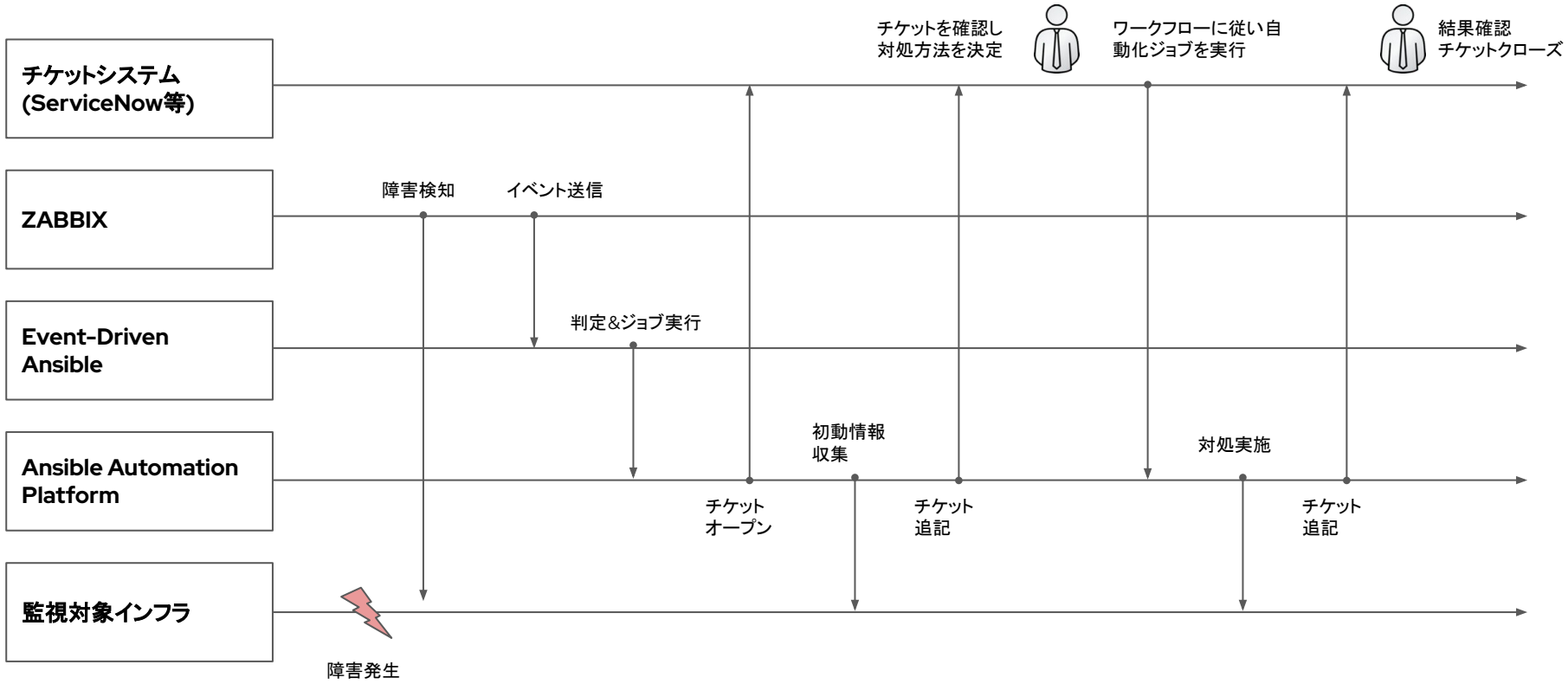
連携のイメージ（6）

送信されるイベントデータサンプル



Red Hat

複雑なケースへの適用

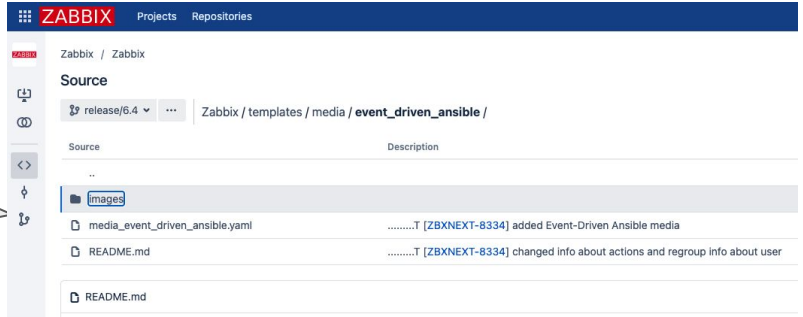


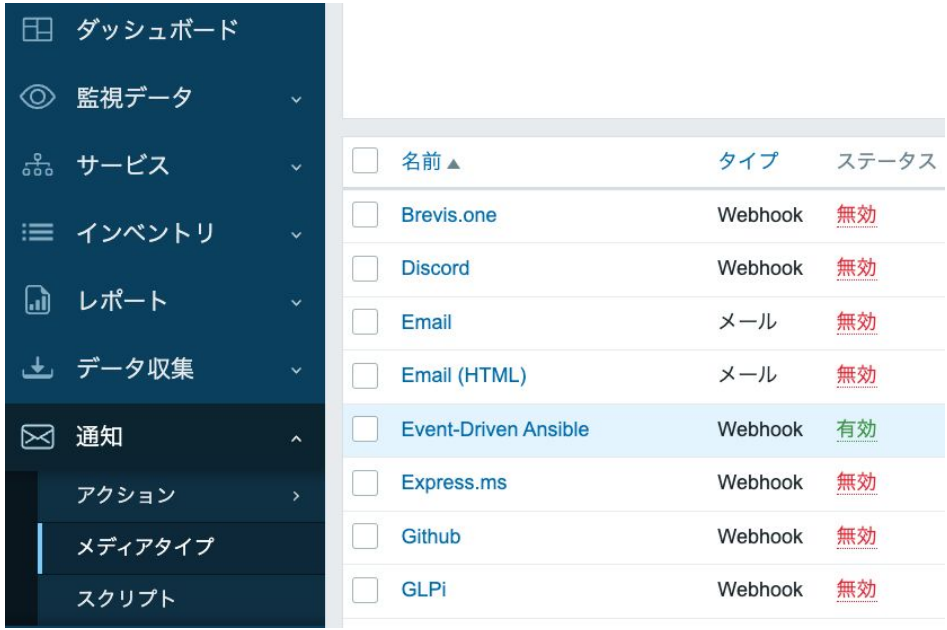
Red Hat

ZabbixとEDAの連携方法（1）

通常の監視設定（ホスト、アイテム、トリガー）を行う

公式サイトからEDA用のメディアテンプレートを取得（現在は6.0/6.4用が配布されています）





通知のメディアタイプからテンプレートをインポートして「有効」にする

詳細な手順に関しては公式サイトをご参照ください
https://www.zabbix.com/jp/integrations/ansible#event_driven_ansible

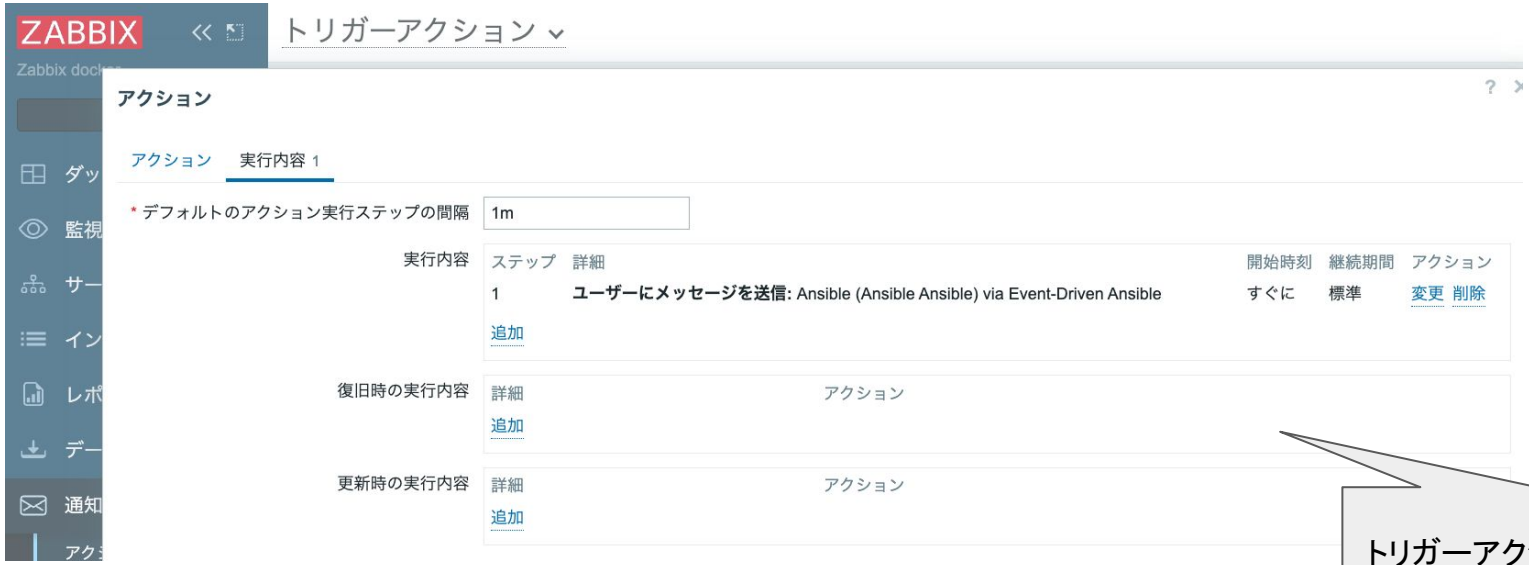
Red Hat

ZabbixとEDAの連携方法（2）

通知先のユーザーのメディアにEDAを追加し、送信先のEDAサーバーのアドレスを指定する

Red Hat

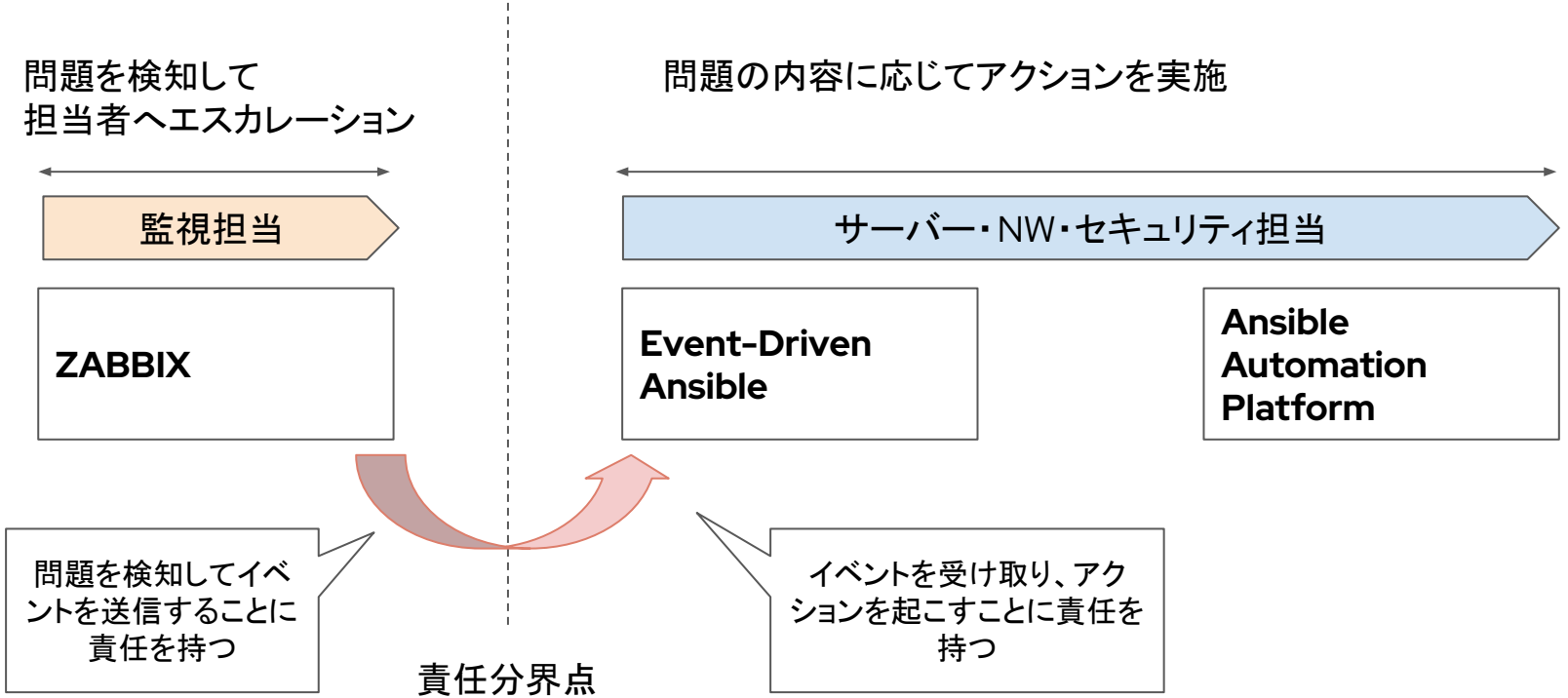
ZabbixとEDAの連携方法（3）



トリガーアクションを作成し、トリガー発生時にEDAに連携するユーザーへの通知を設定する

Red Hat

Zabbix x EDA 連携のメリット：現在の組織の責任範囲の中で活用可能



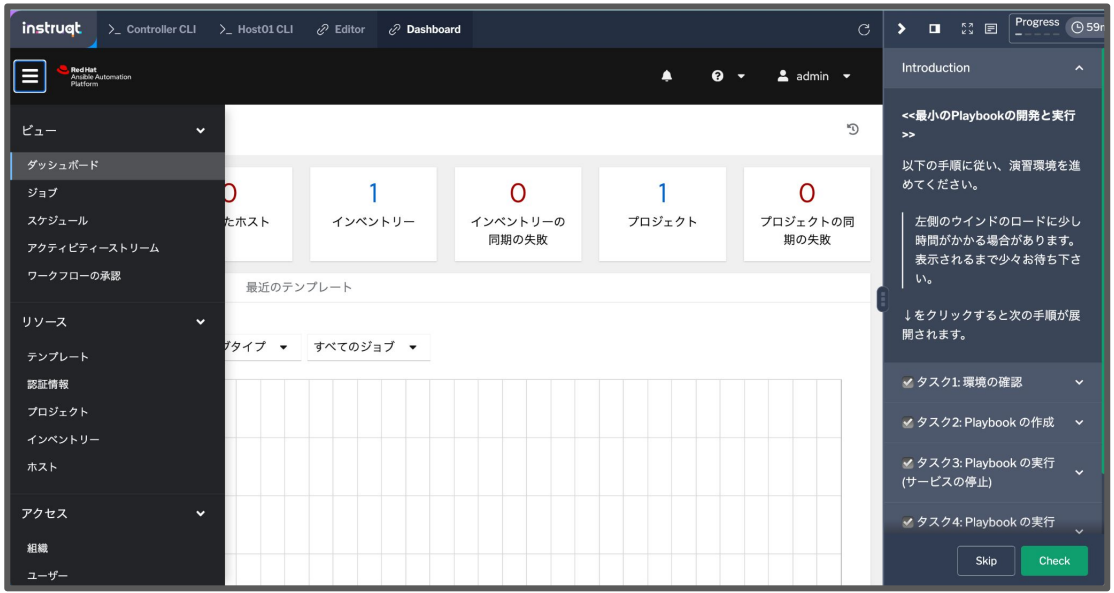
Red Hat

まとめ

まとめ

- Zabbix x Event-Driven Ansible(EDA) は認定済みのイベント連携が可能です。
- EDA を用いることで、Zabbix が発信するイベントに応じて、自動対処を行うことができます。
- EDA は Ansible のもつ強力な自動化機能を使うことが可能で、
  サーバー、ネットワーク、クラウド、セキュリティ、エッジ、アプリ等の
  多様なインフラ操作を自動化することが可能です。

Interactive Lab によるAnsible Automation Platform と新機能の体験



https://red.ht/rhja-lab

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