



Automating Disaster Recovery with Red Hat Ansible

Company: Bank of Ontario

Title: Disaster Recovery Automation Framework Using Ansible

Date: June 5, 2025

Author: Rohan Etemadi, Principal DevSecOps Engineer

Reviewed By: Dana Iqbal (DR Lead), Behnam Hajian (Solutions Architect)

1. Executive Overview

Disaster Recovery (DR) has traditionally been a complex, manual, and error-prone process requiring hours to restore services during outages. In 2025, **Bank of Ontario** implemented a **fully automated DR strategy using Red Hat Ansible Automation Platform**, significantly reducing Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) across critical systems.

This initiative, supported by Red Hat and Deloitte, automates **multi-site failover, infrastructure restoration, application configuration**, and **data verification**—delivering a repeatable, auditable, and rapid recovery process.

2. DR Automation Objectives

- Ensure **infra-to-app stack** recovery within SLA (<30 minutes RTO)
- Provide **playbook-driven failover** to DR region (AWS + on-prem)
- Automate **post-recovery validation** steps (DB health, service uptime, endpoint reachability)
- Integrate with **Ansible Tower** to orchestrate DR runbooks with approvals, scheduling, and reporting
- Eliminate manual dependencies in cloud and VM recovery workflows

3. Automated DR Scenarios

3.1 Cloud DR (AWS & Azure)

Trigger:

- Site failure at **Primary Region (Toronto)**

Ansible Actions:

- Launch DR-hosted EC2 instances from golden AMIs
- Bootstrap with cloud-init + Ansible for services (nginx, PostgreSQL, internal APIs)
- Reconfigure DNS failover using AWS Route53
- Validate app endpoints (`/health`, `/version`) and DB status

yaml

CopyEdit

```
- name: Launch DR EC2 Instances
  hosts: localhost
  tasks:
    - ec2:
        key_name: dr-key
        image: ami-0d54a4c0c7...
        instance_type: t3.medium
        wait: true
        region: ca-central-1
```

3.2 On-Prem DR (vSphere / OpenShift Virtualization)

Trigger:

- VM failure or site isolation detected via monitoring

Ansible Actions:

- Clone VMs from DR templates
 - Re-attach to DR VLAN
 - Restore last ZFS snapshot or volume
 - Re-join service discovery (Consul)
-

3.3 Application-Level Recovery

For stateful workloads (e.g., core banking apps), Ansible automates:

- Container rescheduling on DR OpenShift cluster
- DB failover and promotion using Patroni + Ansible PostgreSQL roles
- Rehydration from object storage (S3, MinIO)

yaml

CopyEdit

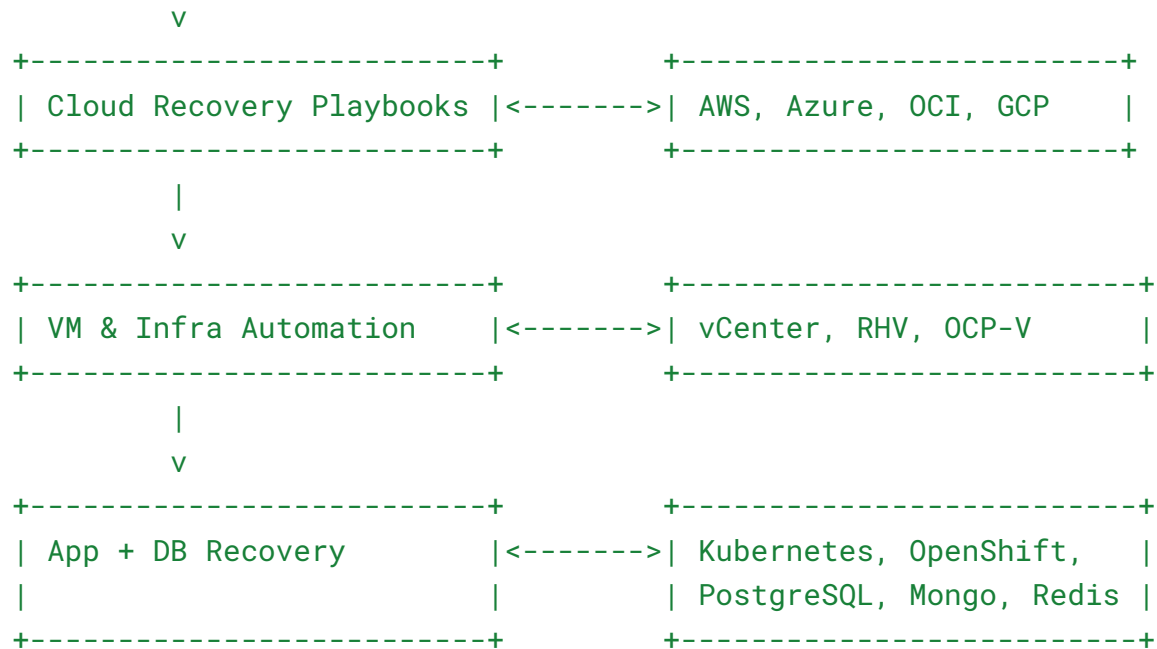
```
- name: Failover PostgreSQL to DR node
  include_role:
    name: ansible-postgresql
  vars:
    pg_action: promote
    target_node: dr-db01
```

4. Integration Architecture

lua

CopyEdit

```
+-----+
|  Ansible Tower  |
+-----+
|
```



5. Key Features

✓ Event-Driven DR

- DR runbooks triggered automatically by **Zabbix**, **ServiceNow**, or **Prometheus** events
- Example: VM heartbeat failure ⇒ auto-recover from template

✓ Approval & RBAC

- All DR actions gated through **Ansible Tower role-based workflows**
- Executives notified via Microsoft Teams with “Approve & Run” button

✓ Idempotent & Auditable

- Playbooks ensure repeatability (run X times = same result)
- Full logs stored in centralized Splunk instance

6. Benefits Realized

Metric	Before Automation	After Ansible DR	Delta
RTO (infra-level)	2–4 hours	20–30 minutes	✓ 85% faster
Full DR Test Duration	3 days	< 5 hours	✓ 93% faster
Compliance Readiness	Manual evidence	Auto-generated	✓ Continuous
Operational Staff Required	6–10 engineers	1–2 operators	✓ 80% less
SLA Violations (2024→2025)	3	0	✓ Eliminated

7. Cost Savings Estimate

Category	Cost Saved (Annualized)
DR Test Labor Reduction	CAD \$42,000
SLA Penalty Avoidance	CAD \$85,000
Faster Recovery = Business Uptime	CAD \$120,000
Paperwork & Compliance Overhead	CAD \$18,000
Total Savings	~CAD \$265,000/year

8. Next Steps

Initiative	Owner	Deadline
Migrate remaining playbooks to GitOps	Platform Team	July 2025
Add Ansible Lightspeed for AI-generated DR runbooks	R&D Ops	August 2025
Extend DR to hybrid SaaS apps (Workday, Salesforce)	Deloitte + Infra	Q4 2025

9. Conclusion

By implementing Red Hat Ansible for disaster recovery, **Bank of Ontario** transformed its DR practice from **reactive and manual** to **predictive and programmable**. This has dramatically improved resilience, reduced operational burdens, and aligned with regulatory expectations for business continuity.