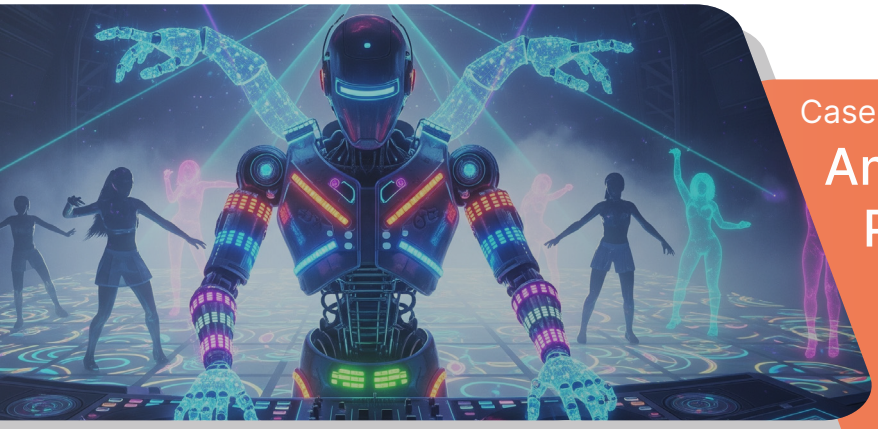

Case study

Ansible Automation Powered Client's Performance Exponentially!

Red Hat Ansible Automation Platform & Satellite

The Client

A leading U.S. public utility provider delivering electric and natural gas services across multiple states, powering millions of homes and businesses daily. Annual revenues exceeding $100 billion.

Client's Challenge

Client had, no, or minimal automation in place, relying heavily on individual bash scripts. There was no centralized automation platform resulting in manual configuration management and inconsistent VM deployments across environments.

Solution & Business Impact

Designed and implemented a suite of automation and compliance initiatives to reduce manual efforts and the many prones it exposes.

A standardized automation framework for regular operations across client's hybrid environments, strengthen system resilience, and ensuring continuous adherence to security and quality standards. Covered the full lifecycle—from provisioning and configuration to disaster recovery, patch management, and intelligent infrastructure optimization—delivering measurable efficiency, reliability, and governance improvements.

Technical Deliverables

- Post-Provisioning Automation for Hybrid Environments
- CI/CD and Code Quality Automation in Azure DevOps
- Intelligent Automation for VM & Infrastructure Management
- System Compliance, Reporting, and Hardening
- Intelligent Automation for VM & Infrastructure Management
- ServiceNow-Integrated Automation Workflows

Quantifiable Outcome

ROI and operational efficiency calculated!

SORINT utilized an effort-tracking mechanism, already in place by client's team, which captures key parameters of daily tasks and workflows through an integrated operational portal to help estimate key business outcomes in regards to time, effort, and cost saving. The figures below demonstrate the before and after of this automation initiatives:

+278
hours saved in operational tasks annually

+$1M
in cost savings

Near-0
manual intervention in provisioning, patching, DR testing, & reporting

Technical Activities

Post-Provisioning Automation for Hybrid Environments

Designed and implemented a comprehensive post-provisioning framework for Windows and Linux systems.
Deployed on Azure & on-premises infrastructure.

- Dynamic inventory generation
- Integration with "ServiceNow" for asset tracking,
- SSSD configuration for security compliance
- Automated application setups.

CI/CD and Code Quality Automation in Azure DevOps

- Enforced Ansible linting via CI/CD pipelines in Azure DevOps, to provide real-time feedback and policy compliance across playbooks and roles.
- Developed a templated Ansible project skeleton creator that auto-creates and checks in new roles/playbooks into ADO repositories, reducing ramp-up time for new automations.

Disaster Recovery and Patch Cycle Automation

DR test orchestration with dynamic inventory for:

- DR hosts
- LPAR power automation
- Storage app verification
- Agents health reporting
- Connectivity & NFS mounts

Automated creation and delivery of DR test results:

- Custom notifications via MS Teams
- Backup expiration adjustments

Compliance & Reporting

- Automated process for on-demand OpenSCAP reports to support security grading
- Delivered Satellite-based patching and hygiene routines, CVE remediation by ID, tuneD profile configurations, and GUI removal for RHEL hosts to align with hardened baselines

Intelligent Automation for VM and Infra Management

- Engineered dynamic and case-insensitive VM discovery roles, VM clone workflows, and safe-mode rebooting for Windows VMs

For resource optimization

- A VMware snapshot lifecycle automation to cleanup aged ones was developed

ServiceNow-Integrated Automation Workflows

Automated ServiceNow

- Ticket creation
- Application code pushes
- A decommissioning playbook integrated with ServiceNow change controls
- Inventory logic to filter out non-reportable servers in SNOW-based compliance jobs

Business Value

Operational Efficiency at Scale

Eliminated significant manual tasks &, maintenance-related activities, such as provisioning, patching, DR testing, and reporting processes.

Resilient and Scalable Infrastructure Management

DR automation, health checks, and snapshot hygiene routines, the implemented solutions improved infrastructure resilience and readiness, with no human intervention required.

Security and Compliance Readiness

Enabled proactive compliance by hardening automated reports, CVE remediation, & configuration enforcement. This contributes directly to audit readiness and reduced security risks.

Clarity, Collaboration & Visibility

Enabled cross-team collaboration & faster feedback. E.g., extending the capabilities of "ServiceNow" which empowered the various involved teams with related timely notifications & actionable reports.

Standardization and Code Quality

Instituted a consistent & reusable automation framework governed by CI/CD linting.
Leading to fewer errors & faster deployments.