Network Configuration Management

Network Management

Orchestral.ai
AI-Driven Orchestration

Situation: A Network Operator Makes a Change

- A network operator makes a change to the configuration of a network device but may not have thought to reflect that change in the configuration management database CMDB.

- A monitoring Syslog service like Solarwinds, ELK Stack or Splunk would capture and log the change but not perform any CMDB query to ensure consistency.

- Over a period of time a "Configuration Drift" will develop whereby the actual configuration of various network devices and the CMDB configuration data will differ.

- Ultimately, there are potentially serious security and compliance risks introduced by an accumulating "Configuration Drift" in the absence of a more automated approach to ensuring the actual and intended configurations are accurately reflected in the CMDB.

Composer Benefits

- **Increased network security**
  All network devices are automatically kept in compliance with security policies and best practices, reducing risks and costs while saving time.

- **Full audit visibility**
  The full scope of device config changes are captured along with operator interventions to ensure audit visibility and policy compliance.

- **Reduced troubleshooting time**
  With real-time awareness of changes in device configurations, operators no longer need to invest time searching for the source of config changes.
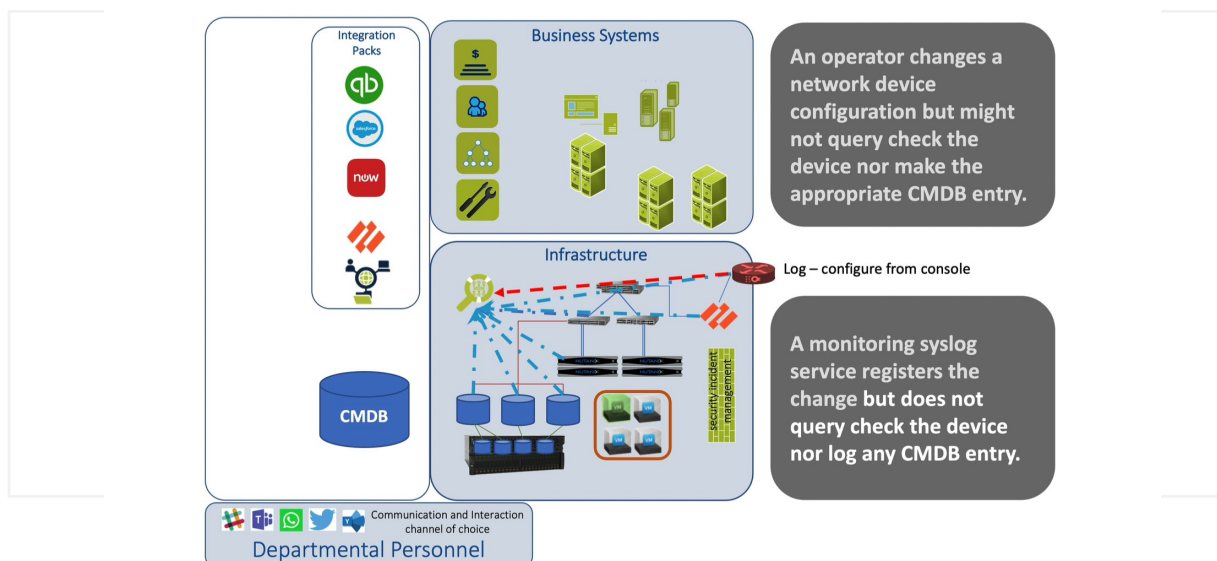
Manual Change Management

FIGURE 1: Manual Configuration Change Management

Orchestral.ai's Composer Solution

Orchestral.ai provides a completely automated solution to this problem. Orchestral Composer's event-driven architecture can automatically execute a "Configuration Drift" workflow in response to the "event" of a change in the configuration of a network device. Composer's event-driven architecture ensures that any configuration change is captured and synchronized with the Configuration Management Database (CMDB) upon operator approval and in accordance with applicable policies.
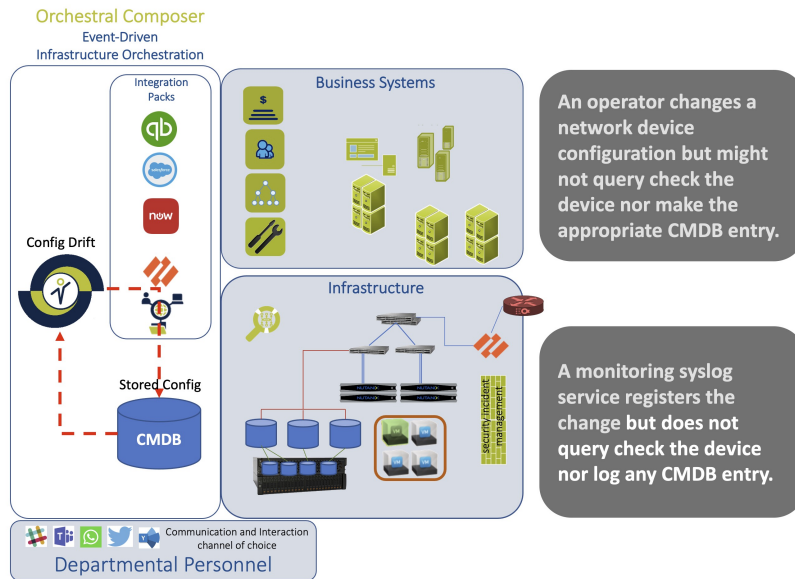
Automated Change Management

FIGURE 2: Automated Configuration Change Management with Orchestral Composer

Composer Automated Change Management

1. Composer monitors the Syslog service, such as SolarWinds, ELK Stack, Splunk or similar for the specific "event" of a configuration change.
2. Once a config change has been detected, Composer will initiate a "Config Drift" workflow that begins with a query check of the Configuration Management Database (CMDB).
3. Composer retrieves from the CMDB the stored configuration of the target (i.e changed) device and brings this data into the "Config Drift" workflow.
4. Leveraging the hundreds of available device integrations, Composer will then extract the running config of the target/ changed device.
5. Next, Composer performs a diff to compare the stored device configuration against the changed device configuration with the result captured for audit purposes.
6. Composer will then prompt the operations team via Chatops, email or similar alerting tool to make them aware of the change and provide them an opportunity to decide which config to retain.
7. Should the operations team choose to retain the CMDB config, then Composer will create an IT Service Management (ITSM) ticket with high priority to replace the running config with the stored CMDB config.
8. If the operations team chooses to retain the changed config, then Composer will update the CMDB with the changed config to ensure that the actual running config is correctly captured in the CMDB.
9. Finally, the audit trail of this operation is saved by Composer by opening an ITSM ticket and attaching the related data.

Orchestral.ai
AI-Driven Orchestration

Orchestral.ai is a team of like-minded technology professionals possessing a combined experience of over 100 years in the IT industry.

Contact Us
For more information, please contact our Client Development Team at **info@orchestral.ai**