Revised: August 19, 2025

SMA workflow framework

How the SMA workflow operates

The SMA workflow describes a centralized system for managing, monitoring, and acting upon events within an infrastructure, while also providing robust alerting capabilities. The key components involved in the process are:

Summary

- **SMA (System Management Agent):** A central management entity that provides a unified monitoring infrastructure, easy configuration options, and maintains a history of events.
- **Config Input:** The source for providing policy configurations to the SMA, typically through a Command Line Interface (CLI).
- **Monitor Clients (LC-SMA, Zone Server, FCNS, F-port Server):** Various systems or services that register with the SMA to receive configuration updates and send event triggers.
- **Action Clients (FPM, Port Manager):** Systems or modules that register with the SMA to receive and execute specific actions.
- **Alerting (Syslog, SNMP TRAP, OBFL):** External systems or protocols used by the SMA to send notifications for logging and alert generation.

Result

The SMA workflow provides a comprehensive and centralized approach to infrastructure management, enabling automated monitoring, dynamic configuration, proactive event handling, and efficient notification through various alerting mechanisms.

How SMA policy architecture works

Policy architecture provides a structured framework for defining and applying rules to manage system and network behavior. It organizes elements into logical groups and associates specific monitoring conditions with automated actions.

Summary

The key components involved in the process are:

- **Policy**: The overarching framework that defines rules and responses for managing system or network behavior.
- **Entity Group**: A logical collection of network elements or systems (for example: edge ports, core ports, system) to which specific monitoring and action rules are applied.
- **Monitor Group**: A set of predefined conditions or metrics that are continuously observed within an Entity Group to detect specific states or events (for example: slow-drain, link integrity, configuration scale, environment and so on).
- **Action Group**: A collection of automated responses or operations triggered when conditions defined by a Monitor Group are met (e.g., FPIN, Syslog, Port-Guard, Trap).

Result

The policy architecture enables a modular, scalable, and automated approach to managing and responding to events across various network and system entities, ensuring consistent application of rules and efficient operational control.