UAS IMPLEMENTATION WORKSHOP

Universal Alert Technology Add-On to Splunk®

Abstract

UAS Implementation Workshop Agenda and Output

Burilliance, LLC of Virginia

Table of Contents

Introduction

The purpose of this document is to outline the workshop to be conducted to plan for the implementation of the Universal Alert Script (UAS) technology add-on to Splunk. It documents the required attendees, the agenda, detailed workshop activities and the workshop output.

Required Attendees

The following job functions need to be represented during the workshop. Some of these roles may be one in the same depending on your enterprise:

- Splunk System Administration team member(s)
  - Those responsible for the administration of the Splunk software/system
- Splunk Architectural team member(s)
  - Those responsible for the current and future architecture of the Splunk system
- Alert Management System (AMS) system administrators/power users
  - Those responsible for the alert management system and it's capabilities
- Operations team member(s)
  - Those responsible for receiving and acting on alerts
- Alert Designer(s)
  - These may be various team members coming from operations and engineering and may span multiple disciplines including System Admins, Database Admins, Application Owners, and Network Admins

Agenda

- Overview Current/Planned Splunk System Architecture
    - Data Sources
    - Forwarders
    - Indexers
    - Search Heads
- Overview Current/Planned Splunk Usage
    - For what purposes is Splunk being used today
    - Are there any strategic plans for expanded usage
    - Are there any third party applications in use today
    - Is any Splunk Alert functionality being used today
        - If so, are any scripts currently in place and what do they do
- Overview Current/Planned Alert Management System
    - What is the current AMS
    - Is there a plan to keep the current alert methods, migrate these to Splunk, or maintain a hybrid
    - How do alerts currently get generated into the AMS
        - If not Syslog, is there a well-defined API
    - What are the mandatory and optional key/value pairs necessary to initiate an alert in the AMS
- Overview of UAS
    - How does it “connect” to Splunk
    - Alerting “methods”
    - Architecture overview
    - Use cases
    - Configuration overview
- UAS Implementation Planning
    - Alert methods
        - Is there any custom development required
        - Agreement on which methods will be used (current and future)
        - Gathering configuration items for each methods system interface
        - Determining if a default method will be used
    - Standard or customizable key/value pairs
        - Agreement on standards across all groups,
            - Using field aliasing, OR
        - Standards within groups, OR
        - Customized per alert
        - Implications on AMS interface
- Detailed configuration information gathering
    - Per script
    - Per alert method

Workshop Output

- AMS key/value pair mandatory and optional key/value pairs
- Alerting strategy: migration or hybrid
- AMS API (as required)
- Single or multiple scripts/configurations
- Alerting methods agreement
- Alert key/value pairs agreement
- Alert methods configuration(s)
- Script configuration(s)