



# Prognosis Labs

Alerting - Advanced

Wednesday, October 18, 2017

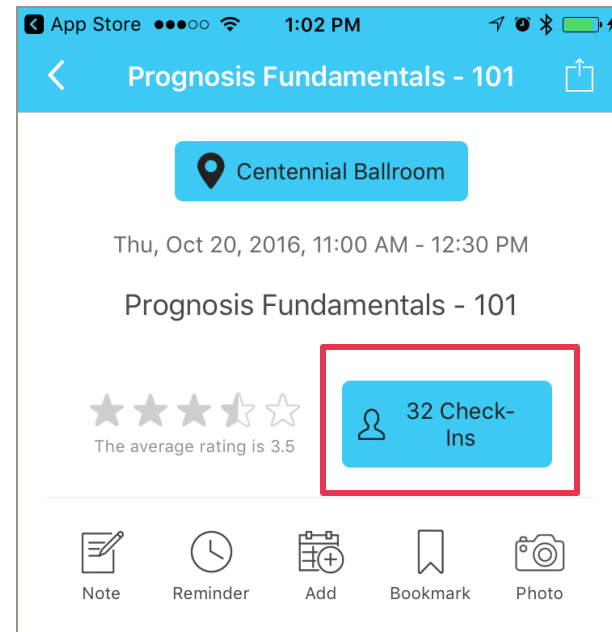
**Rick Scheidegger**





# Welcome!

Please check-in on the mobile app - see your class record, remember what tests to take, and help us improve





- **WiFi SSID:** IR Prognosis Summit
- **WiFi PW:** Summit17
- Download the Slides from  
Online.Prognosis.com(insert URL)
- Login to the Demo Instance (insert URL)



# Agenda

This Labs session will cover the following topics and have exercises to reinforce the topics

- New feature discussion
- Quick review of Prognosis threshold components
- Nodegroups and Nodes to monitor selection ?
- Command Destination
- Availability Destinations
- Sending SMS/MMS alerts



# Learning Objectives

- After completing this course you should:
  - Have a better understanding Prognosis threshold capabilities
  - Be able to build thresholds that utilize more advanced configurations
  - Understand how best to utilize thresholds to meet your operational needs



- Hands on Prognosis and threshold configurations
- Reinforce topics learned previously
- Discuss and use features to incite thought
- Prompt additional discussions



# Topic - Threshold Quick Review

- A Threshold is a Prognosis service that scans system data looking for predefined exception conditions.
- Once an exception is detected, the Threshold definition can send details via an event message to one or more of a variety of destinations such as; Events log, SNMP trap, Dispatch Manager, Commands etc.



# Threshold Components

The screenshot shows the configuration window for an Avaya Alert on a system named \CON-08R2-PROG10. The window has several tabs: General, Conditions, Default Destinations, Schedule, and Nodes to Run On. The 'Conditions' tab is active.

**Threshold Name:** The 'Unique Threshold Process Name' field is set to 'Avaya\_Alert'.

**Condition Name and Where Clause:** The 'Threshold Conditions' list includes several items. The 'Aura CPU Usage (OCTOTAL > 80)' condition is highlighted with a red box. Below it, the 'Problem Summary' and 'SNMP Trap' entries are also highlighted with a red box, showing their respective where clauses.

**Condition Destinations:** The 'Condition Destinations' field is partially visible at the bottom of the window, showing a configuration for a destination.

- Aura Avail Up (CURRSTAT = "UP" OR CURRSTAT = "DE")
- Aura CPU Usage (OCTOTAL > 80)**
- Problem Summary (1031: @AVSEMKPI.MGRTYPE@ Manager @AVSEMKPI.PNODE@ has CPU usage exceeding 80%)**
- Dispatch Manager (@AVSEMKPI.MGRTYPE@ Manager @AVSEMKPI.PNODE@ has CPU usage exceeding 80%)**
- SNMP Trap (1031: @AVSEMKPI.MGRTYPE@ Manager @AVSEMKPI.PNODE@ has CPU usage exceeding 80%)**
- Aura Degraded (CURRSTAT = "DE")
- Aura Down (CURRSTAT = "DN")
- Aura Memory Usage (MEMTOTAL > 85)
- Board Avail Up (( CURRSTAT = "UP" OR CURRSTAT = "DE" ) AND
- Board Degraded (CURRSTAT = "DE" AND BRDNUM MATCHES RE





# Threshold Conditions

- A condition uses “Where Clauses” to create a trigger to feed a condition destination
  - Condition Destinations will also need to be configured
    - Problem Summary – Internal Prognosis records
    - Dispatch Manager , DISPMAN, SMTP alert destination
    - SNMP trap out
    - Command – Can execute scripts on the Prognosis server
    - Others will be discussed



# Threshold Conditions-Visual

The screenshot shows the configuration window for an Avaya Alert on a system named \CON-08R2-PROG10. The window has several tabs: General, Conditions, Default Destinations, Schedule, and Nodes to Run On. The 'Conditions' tab is active.

Under the 'General' section, the 'Unique Threshold Process Name' is set to 'Avaya\_Alert'.

The 'Threshold Conditions' section is expanded, showing a list of conditions. The condition 'Aura CPU Usage (OCTOTAL > 80)' is highlighted with a red box. A callout box labeled 'Condition Name and Where Clause' points to this condition.

Below the highlighted condition, there is a 'Problem Summary' and three 'Destinations' (Dispatch Manager, SNMP Trap, and another SNMP Trap) all with the same summary text: 'Problem Summary (1031: @AVSEMKPI.MGRTYPE@ Manager @AVSEMKPI.PNODE@ has CPU usage exceeding 80%)'. A callout box labeled 'Condition Destinations' points to this summary text.

Other conditions listed include 'Aura Avail Up (CURRSTAT = "UP" OR CURRSTAT = "DE")', 'Aura Degraded (CURRSTAT = "DE")', 'Aura Down (CURRSTAT = "DN")', 'Aura Memory Usage (MEMTOTAL > 85)', 'Board Avail Up (( CURRSTAT = "UP" OR CURRSTAT = "DE" ) AND ...)', and 'Board Degraded (CURRSTAT = "DE" AND BRDNUM MATCHES RE...)'.



# Thresholds Best Practices

- Build a display using the record you will be alerting upon.
- Consider data field types when configuring Timing
  - CPU, Memory utilization spikes
- With “log” type data records, utilize timestamp fields within the Where clause
- Node group usage can simplify alerting



# Alerts - New Features

- Prognosis 11.2 introduced new Alert features of note. They are located in the “ALERTS” configuration
  - Preserve Alerts
  - Suppress Threshold



# Preserve Alerts

- Avoids Alert Floods during a Prognosis service restart or server restart
- Keeps a persistent file in the <drive> \Prognosis Server\Configuration\autoancache directory
- Disabled (commented out) by default



# Preserve Alerts configuration

- PRESERVE-ALERTS ( Y )
- ! The current alert state is saved to disk on an interval in seconds configurable below.
- CACHE-INTERVAL ( 30 )
- ! The alert state will be discarded if it is older than the configured value in seconds below.
- CACHE-TIMEOUT ( 86400 )
- ! This setting is used to suppress thresholds. In this mode, thresholds will not trigger events
- ! and will not dispatch any messages to destinations.



# Suppress Threshold

- The 'Alert Suppression' feature is used to turn off all Threshold processing on a Prognosis server. When activated, all Threshold processes running on the selected Prognosis server will temporarily stop receiving data for any triggered alerts. This feature will help to stop false alerts from being raised when they are expected, such as during routine maintenance.



# Suppress Threshold Configuration

- Commented out/disabled by default
- Configuration item
  - SUPPRESS-THRESHOLD()
  - Syntax is just as it is, just needs to be uncommented in the ALERTS configuration and start the configuration.





# Lab Exercises

- Exercise 1
  - Thresholds using timestamp fields and timing parameters
- Exercise 2
  - Creating custom node groups
- Exercise 3
  - Thresholds using command destinations – part 1
- Exercise 4
  - Threshold using bg command destination – part 2
- Exercise 5 ?



# Exercise 1 - Topics

- Identify Prognosis timestamp fields
- Discuss where clauses to utilize timing parameters
- Build a threshold condition to take advantage of timing parameters



# Exercise 1 - Specifics

- Build a single window display using the PrognosisErrorLog record
- Create a where clause to filter out date based on timing
- Apply the where clause to a threshold condition to create the desired “on” event.



# Exercise 2 - Topics

- How are Prognosis Node Groups are structured and built
  - Static creation
  - Dynamic creation
- How are node groups used in threshold conditions



## Exercise 2 - Specifics

- Create a new node group with nodes of choice
- Create a threshold condition to utilize the new node group
- Apply the where clause to a threshold condition to create an “on” event.



# Exercise 3 - Topics

- Prognosis Command Destinations
  - Common uses
    - MOM integrations
    - Dynamic testing based on other alerts
    - Processing data
  - Overview of configuration components
  - Viewing command results



## Exercise 3 - Specifics

- Create a threshold condition with a command destination
  - Will execute for “on event”
  - Type execute in the server shell
  - Will execute a ircnfutl.exe command
  - Will utilize “prognosis” key
  - Will be executed on the “CurrentNode”



# Exercise 4 - Topics

- Command Destinations Part 2
  - Using thresholds to aid in troubleshooting
    - Automatically execute commands within an existing alert to provide more information.
      - Ping
      - tracert
    - Have available output to see results





## Exercise 4 – Specifics

- Modify an existing threshold to add a command destination
  - Locate a threshold condition using a record with an IP address field
  - Add a command destination to either ping or traceroute the ip address of the device on an on event



# Topic - Alerting with SMS/MMS

- Prognosis can provide alerting to a Short Message Service (SMS) or Multimedia Message Service (MMS) device
  - Utilizes the Dispatch Manager destination
  - Requires knowledge of the end user device service provider
  - Quick and Simple!!!!



# Vendor Specific Information

- Most wireless phone providers have Simple Mail Transfer Protocol (SMTP) destinations for SMS/MMS devices
- Can be found by vendor and country on the internet, one example..
- <http://www.emailtextmessages.com/>



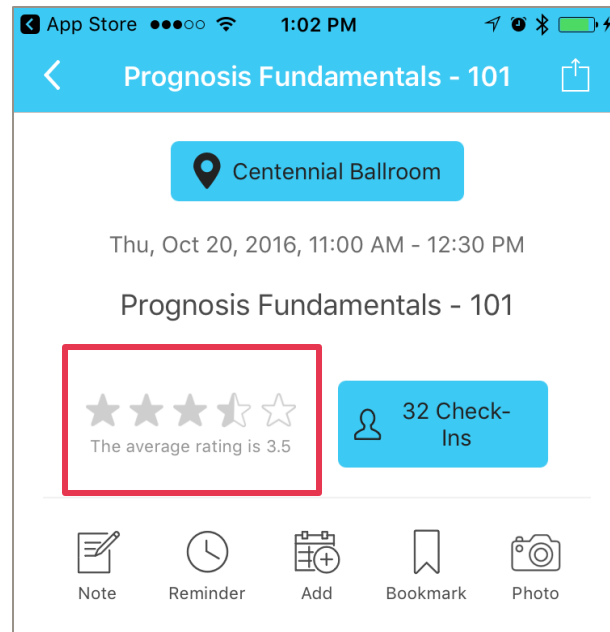
# Recap

- We've covered:
  - Prognosis Timestamp based alerting
  - Using Prognosis Nodegroups in thresholds
  - Using Prognosis Command destinations and multiple ways they can be used



# Next Steps

- **Please Rate the Class**
- **Take the Knowledge Reinforcement Test**
- **Log On to [Online.Prognosis.com](http://Online.Prognosis.com)** to download slides & ask questions
- *Every class rating gets you a chance to win prizes!*



# Questions?

