Skills 1st

Zenoss 4 Event Management Workshop Exercises

Version 1

January 2013

Jane Curry

Skills 1st Ltd

www.skills-1st.co.uk

Jane Curry
Skills 1st Ltd
2 Cedar Chase
Taplow
Maidenhead
SL6 0EU
01628 782565

jane.curry@skills-1st.co.uk

www.skills-1st.co.uk

Introduction

Workshop Aims

The purpose of this workshop is to demonstrate the underlying architecture of the Zenoss events subsystem, by completing a series of exercises covering many of the more subtle features of Zenoss. Logging and debugging techniques will also be discussed.

It is assumed that participants starts with at least an overview knowledge of Zenoss; by the end of the workshop, they should have a thorough understanding of Zenoss events and a large number of working examples.

This workshop is a companion to the "Event Management for Zenoss Core 4" paper which is freely available from http://www.skills-1st.co.uk/papers/jcurry.html . You should have a copy of the paper as you do the workshop exercises. There are exercises associated with each chapter of the paper.

The aim of the workshop is to spend 90% of the time working hands-on. **Brief** introduction sessions will be conducted for each unit and the instructor will be available throughout to assist and answer questions. The companion paper provides the in-depth information.

The exercises are not intended to be proscriptive; feel free to explore aspects further. If an area is irrelevant to you, feel free to skip it.

Workshop Environment

The exercises will use Zenoss 4.2.3 installed on a CentOS 6.3 system, *zen42.class.example.org*. There is also a Windows machine provided.

The Open Source package *Raddle* (available from SourceForge) is installed on the Zenoss server to provide an emulated network with three Cisco routers, two Cisco switches, an SNMP-capable Linux server, and a handful of ping-able devices.

The Zenoss server is running a DNS that resolves all names for the class environment.

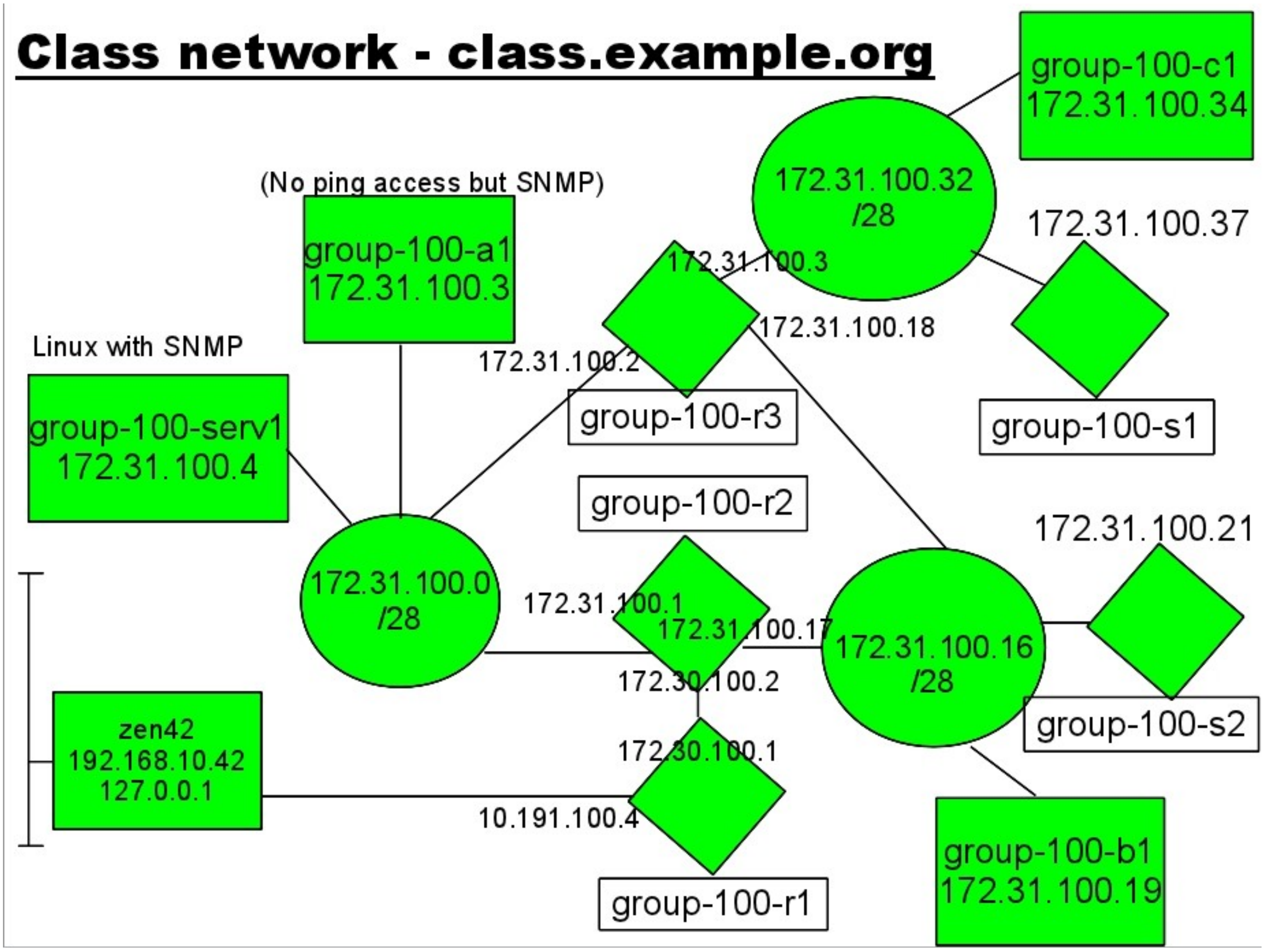

Illustration 1: Class network diagram

Notations

Throughout this exercise guide, text to be typed or menu options to be selected will be highlighted by *italics*. Important points to take note of will be shown in **bold.**

Points of particular note are highlighted by an icon.

Table of Contents

1 Exercises for Unit 1 – Introduction....10
  1.1 Introduction to the environment....10
2 Exercises for Unit 2 - Event Architecture....10
  2.1 Generating test events....10
    2.1.1 zensendevent in Zenoss 4.2.3....12
  2.2 Event Manager default configuration....13
  2.3 Exploring the MySQL database....13
    2.3.1 Optional exercises....14
  2.4 The RabbitMQ subsystem....14
  2.5 Queues and daemons....15
  2.6 Event context and eventState....18
  2.7 Fingerprints and de-duplication....18
  2.8 Resolution, Ageing and Archiving....19
    2.8.1 Optional exercises....21
  2.9 Zenoss log files....21
3 Exercises for Unit 3 - Events generated by Zenoss....22
  3.1 Node up / down events....22
  3.2 IP Service events....22
  3.3 Process events....23
  3.4 SNMP failure on a device....24
4 Exercises for Unit 4 - Generating syslog events....24
  4.1 Configuring syslog....25
  4.2 Configuring Zenoss for syslog....26
  4.3 Testing syslog with the logger command....26
  4.4 Inspecting syslog events at Zenoss....26
  4.5 Increasing debugging for zensyslog....27
  4.6 Optional exercise - Understanding the syslog parsing mechanism....28
5 Exercises for Unit 5 – Generating Windows Event Log events....36
  5.1 Configuring Zenoss to receive Windows Event Logs....36
  5.2 Generating Windows Logon Failure events....36
  5.3 Inspect event details for windows events....37
  5.4 Checking logfile entries for zeneventlog....37
  5.5 Optional exercises - Using syslog on a Windows system....38
6 Exercises for Unit 6 – Event Mappings....40
  6.1 Explore out-of-the-box event classes and mappings....40
  6.2 Creating a new event subclass....42
  6.3 Mapping incoming events to an event class....42
  6.4 Mapping using a simple Regex....43
  6.5 Mapping using a Python expression Rule....45
7 Exercises for Unit 7 - Event Transforms....47

7.1 Using a simple Transform in an event mapping....47
7.2 Mapping with a Regex and Transform....48
7.3 Applying event and device context in relation to transforms....50
7.4 Correlating events....53
7.5 Transforms at event level....54
7.6 defaultmapping eventClassKey....56
7.7 Optional exercises....57
7.7.1 Understanding fields available for event processing....57
8 Exercises for Unit 8 - Testing and debugging aids....58
8.1 Log files....58
8.1.1 zeneventd.log....58
8.1.2 zeneventserver.log....59
8.1.3 Other log files....59
8.2 Using zendmd to run Python commands....60
8.3 Using the Python debugger in transforms....61
8.3.1 Run limited Zenoss system for debugging....61
8.3.2 Run zeneventd in the foreground in debug mode....62
8.3.3 Modify an event transform to include a pdb breakpoint....62
8.3.4 Using pdb....62
9 Exercises for Unit 9 – SNMP event mappings....64
9.1 Understanding SNMP TRAP processing....64
9.2 SNMP on Windows systems....66
9.3 SNMP on Linux systems....67
9.3.1 Optional exercise - SNMP V3 for net-snmp agents....69
9.4 Understanding the net-snmp MIBs....70
9.5 Configuring Zenoss to understand SNMP TRAP OIDs....73
9.5.1 A few comments on importing MIBs with Zenoss....76
9.6 Optional exercise - Using the MIB Browser ZenPack....77
9.7 Mapping SNMP TRAPs to Zenoss events....80
9.8 Event Class mapping transforms for SNMP events....82
9.9 Mapping Rules for SNMP events....83
9.10 Optional exercise - More elegant transform....84
10 Exercises for Unit 10 – Triggers and Notifications....85
10.1 Defining a Trigger....85
10.2 Defining an email Notification....85
10.3 Defining a Command Notification....86
10.4 Defining a TRAP Notification....89
10.5 Understanding the Zenoss MIB....90
10.6 Optional exercise - fixing ZENOSS-MIB.txt....91
10.7 Notification Schedules....91
10.8 Running zenactiond in debug mode....92
10.9 Optional exercise - the effect of device Production State....93

11 Exercises for Unit 11 - Accessing events with the JSON API....94
11.1 Understanding the JSON API....95
11.2 Bash examples of using the JSON API....95
11.2.1 Optional exercise - bash example to retrieve trigger information....96
11.3 Python examples of using the JSON API....97
11.3.1 Optional exercise - python example to retrieve parameterised event records....98
12 Appendix A - Some solutions....99
12.1 JSON API bash example - zenoss_JSONAPI_curl_Triggers.sh....99
12.2 JSON API python example - get_events.py....100
13 References....106

About the author

Jane Curry has been a network and systems management technical consultant and trainer for 25 years. During her 11 years working for IBM she fulfilled both pre-sales and consultancy roles spanning the full range of IBM's SystemView products prior to 1996 and then, when IBM bought Tivoli, she specialised in the systems management products of Distributed Monitoring & IBM Tivoli Monitoring (ITM), the network management product, Tivoli NetView and the problem management product Tivoli Enterprise Console (TEC). All are based around the Tivoli Framework architecture.

Since 1997 Jane has been an independent businesswoman working with many companies, both large and small, commercial and public sector, delivering Tivoli consultancy and training. Over the last 5 years her work has been more involved with Open Source offerings, especially Zenoss.

She has developed a number of ZenPack add-ons to Zenoss Core and has a large number of local and remote consultancy clients for Zenoss customisation and development. She has also created several workshop offerings to augment Zenoss's own educational offerings. She is a frequent contributor to the Zenoss forums and IRC chat conversations and was made a Zenoss Master by Zenoss in February 2009.