



# Zenoss Event Management Workshop

*November 30th, 2008*

*Jane Curry*

*Skills 1st Ltd*

[www.skills-1st.co.uk](http://www.skills-1st.co.uk)

***DRAFT***

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

[jane.curry@skills-1st.co.uk](mailto:jane.curry@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 designed to demonstrate many of the more subtle features of Zenoss.

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

## Workshop Environment

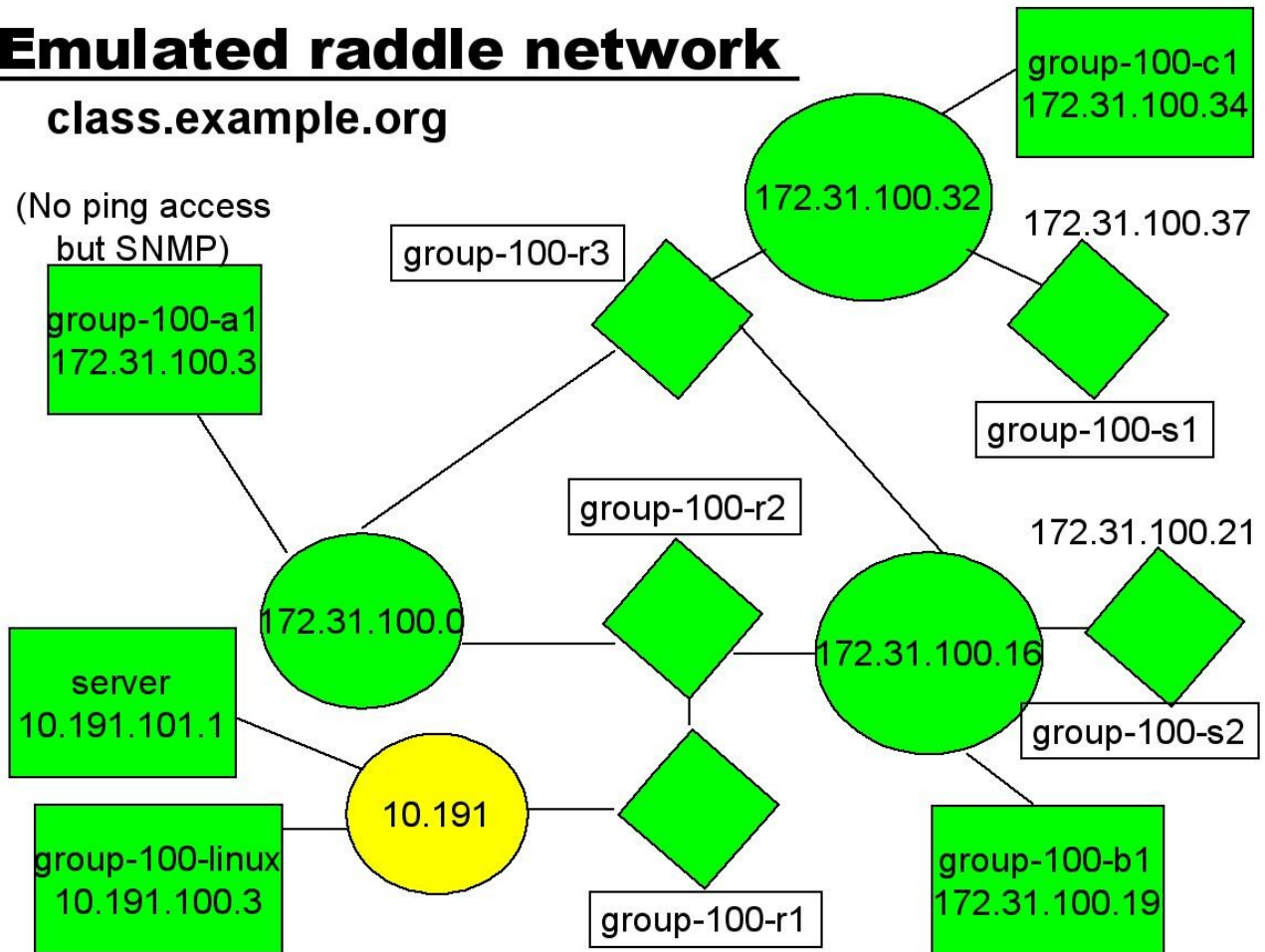
The exercises will use a variety of real systems and VMware machines. Zenoss 2.2.4 is installed on a SuSE 10.3 system. There should also be a Windows system (either real or a VM).

The Open Source package *Raddle* (available from Source Forge) is used to provide two VMs. *server.class.example.org* is the DNS system and default route for the rest of the Raddle environment. It will also be used as a system for testing various event scenarios. The base Operating System is Fedora Core 3 (FC3). The second Raddle system is *group-100-linux.class.example.org*. Also based on FC3, it runs an emulation of 3 Cisco routers, 2 Cisco switches and a handful of ping-able devices. Note that *group-100-linux* may well exhibit strange behaviour with regard to what it can ping and what it can access using SNMP – it is best left alone!

# Emulated riddle network

class.example.org

(No ping access  
but SNMP)



## 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**.

## Table of Contents

|      |   |    |
|------|---|----|
| 1    | Exercises for Unit 1 – Events generated by Zenoss.....              | 6  |
| 1.1  | Exercise 1 – Examine polling intervals for Collectors.....          | 6  |
| 1.2  | Exercise 2 – Examine defaults for the Event Manager.....            | 7  |
| 1.3  | Exercise 3 – Node up / down events.....                             | 8  |
| 1.4  | Exercise 4 – IP Service failures from Linux and Windows.....        | 8  |
| 1.5  | Exercise 5 – Service failure from Windows.....                      | 9  |
| 1.6  | Exercise 6 – Process failure from Linux.....                        | 10 |
| 1.7  | Exercise 7 – Process failure from Windows.....                      | 10 |
| 1.8  | Exercise 8 – SNMP failure on a device.....                          | 11 |
| 1.9  | Exercise 9 – IP failure on a device.....                            | 12 |
| 1.10 | Summary for Unit 1.....   | 13 |
| 2    | Exercises for Unit 2 - Generating syslog events.....                | 15 |
| 2.1  | Exercise 1 – Configuring syslog.....                                | 16 |
| 2.2  | Exercise 2 – Configuring Zenoss for syslog.....                     | 16 |
| 2.3  | Exercise 3 – Configuring syslog-ng.....                             | 16 |
| 2.4  | Exercise 4 - Testing syslog with the logger command.....            | 17 |
| 2.5  | Exercise 5 – Inspecting syslog events at Zenoss.....                | 17 |
| 2.6  | Exercise 6 – Increasing debugging for zensyslog.....                | 18 |
| 2.7  | Exercise 7 - Understanding the syslog parsing mechanism.....        | 19 |
| 2.8  | Summary for Unit 2.....   | 25 |
| 3    | Exercises for Unit 3 – Generating Windows Event Log events.....     | 26 |
| 3.1  | Exercise 1 - Configuring Zenoss to receive Windows Event Logs.....  | 26 |
| 3.2  | Exercise 2 – Generating Windows Logon Failure events.....           | 26 |
| 3.3  | Exercise 3 – Inspect event details for windows events.....          | 27 |
| 3.4  | Exercise 4 – Using syslog on a Windows system.....                  | 27 |
| 3.5  | Summary for Unit 3.....   | 28 |
| 4    | Exercises for Unit 4 – Event Mappings.....                          | 30 |
| 4.1  | Exercise 1 – Explore out-of-the-box event classes and mappings..... | 30 |
| 4.2  | Exercise 2 – Creating a new event subclass.....                     | 31 |
| 4.3  | Exercise 3 – Mapping incoming events to an event class.....         | 32 |
| 4.4  | Exercise 4 – Mapping using a simple Regex.....                      | 33 |
| 4.5  | Exercise 5 – Mapping using a Python expression Rule.....            | 34 |
| 4.6  | Exercise 6 – Using a simple Transform in an event mapping.....      | 36 |
| 4.7  | Exercise 7 – Mapping with a Regex and Transform.....                | 37 |
| 4.8  | Exercise 8 – Extracting device information in an event mapping..... | 39 |
| 4.9  | Exercise 9 – Applying event and device context.....                 | 39 |
| 4.10 | Exercise 10 – Correlating events.....                               | 41 |
| 4.11 | Exercise 11 – Transforms at event level.....                        | 42 |
| 4.12 | Summary for Unit 4.....   | 44 |
| 5    | Exercises for Unit 5 – SNMP event mappings.....                     | 48 |
| 5.1  | Exercise 1 – Understanding SNMP TRAP processing.....                | 48 |

|       |   |    |
|-------|---|----|
| 5.2   | Exercise 2 – SNMP on Windows systems.....                         | 49 |
| 5.3   | Exercise 3 – SNMP on Linux systems.....                           | 50 |
| 5.4   | Exercise 4 – Configuring Zenoss to understand SNMP TRAP OIDs..... | 52 |
| 5.4.1 | A few comments on importing MIBs with Zenoss.....                 | 55 |
| 5.5   | Exercise 5 – Mapping SNMP TRAPs to Zenoss events.....             | 59 |
| 5.6   | Exercise 6 – Event Class transforms for SNMP events.....          | 60 |
| 5.7   | Exercise 7 – Mapping Rules for SNMP events.....                   | 61 |
| 5.8   | Exercise 8 – Rules and transforms for SNMP events.....            | 62 |
| 5.9   | Summary for Unit 5.....   | 63 |
| 6     | Exercises for Unit 6 – Event Commands.....                        | 66 |
| 6.1   | Exercise 1 – Creating a simple event command.....                 | 66 |
| 6.2   | Exercise 2 – Combining event commands.....                        | 67 |
| 6.3   | Exercise 3 – Debugging event commands.....                        | 68 |
| 6.4   | Summary for Unit 6.....   | 72 |
| 7     | Exercises for Unit 7 – Events, Alerts & Production Status.....    | 73 |
| 7.1   | Exercise 1 – Configuring Zenoss for a mail server.....            | 73 |
| 7.2   | Exercise 2 – Configuring Zenoss users for email.....              | 73 |
| 7.3   | Exercise 3 – Configuring Alerting Rules.....                      | 74 |
| 7.4   | Exercise 4 – Other alerting mechanisms.....                       | 76 |
| 7.5   | Exercise 5 – Production Status.....                               | 78 |
| 7.6   | Summary for Unit 7.....   | 79 |
| 8     | Appendix A zendmd commands useful with events.....                | 80 |
| 9     | References.....   | 82 |