indeni network optimism

Netcool/OMNIbus Integration Module for indeni Security Operations Monitoring Solution

Release 1.0

indeni Inc.
1 Bridge Plaza, 2nd floor
Fort Lee, NJ, 07024 USA
Tel: +1-877-778-8991
E-mail: info@indeni.com

indeni Israel
14 Menachem Begin Rd.
Ramat Gan, 52700 Israel
Tel: +1-809-494-190
E-mail: info@indeni.com

indeni UK Limited
60 Goswell Road
London, EC1M7AD UK
Tel: +44-800-098-8972
Email: info@indeni.com

www.indeni.com

indeni network optimism

Table of Contents

indeni Inc.
1 Bridge Plaza, 2nd floor
Fort Lee, NJ, 07024 USA
Tel: +1-877-778-8991
E-mail: info@indeni.com

indeni Israel
14 Menachem Begin Rd.
Ramat Gan, 52700 Israel
Tel: +1-809-494-190
E-mail: info@indeni.com

indeni UK Limited
60 Goswell Road
London, EC1M7AD UK
Tel: +44-800-098-8972
Email: info@indeni.com

www.indeni.com

Introduction

This document describes the integration of the indeni security operations monitoring solution for firewalls with the real-time event and fault management solution, IBM Tivoli Netcool/OMNIbus.

This integration has been developed by the indeni team with the technical cooperation and assistance of the IBM Israel GTU team.

This document provides the following information:

- Description of the functionality of the integration
- Software prerequisites
- Release/version information
- Installation guide
- Screenshots of the fully configured integration

Netcool/OMNIbus Integration Module

Description

The Netcool/OMNIbus Integration Module for the indeni Security Operations Monitoring Solution for Firewalls (indeni) provides a SNMP trap-based integration between indeni and Netcool/OMNIbus. indeni SNMP traps are monitored by Netcool/OMNIbus via the SNMP probe and the associated configuration and rules file. indeni Security Operations Monitoring Solution will notify Netcool/OMNIbus of any alarms and events supported by indeni.

The indeni-Netcool/OMNIbus Integration Module provides the following functionality:

- Automated de-duplication of events and alarms in Netcool/OMNIbus
- Automated "Generic Clear" correlation of problem/resolution events
- Informative and descriptive event presentation in Netcool/OMNIbus

Netcool/OMNIbus Integration History

Release 1.0: May 31, 2011 based on the indeni/MIB version

Last-updated: May 31, 2011, 0000Z

Release 1.0 includes the following file:

- indeni.mttrapd.rules

Software Requirements and Dependencies

- Netcool/OMNIbus v7.x
- Netcool/OMNIbus SNMP Probe (nco_p_mttrapd v11)
- indeni Security Operations Monitoring Solution, indeni-MIB, last updated on May 31, 2011 at 0000Z

Installation of Probe Rules Files

Please note that it is assumed that $OMNIHOME is set to "/opt/netcool/omnibus". If a different path is used, replace all instances of "opt/netcool/omnibus" below with the appropriate path.

1. Create subdirectory "indeni" in the $OMNIHOME.probes/<arch> folder
2. Copy the following file to $OMNIHOME.probes/<arch>/indeni:
   - indeni.mttrapd.rules

3. This amendment should be made in $OMNIHOME/probes/<arch>/mttrapd.props: RulesFile:
   - "$OMNIHOME/probes/<arch>/indeni/indeni.mttrapd.rules"

4. Create a new class in the Netcool/OMNIbus Object Server:

   - In Netcool/OMNIbus Administrator -> ObjectServer Configuration -> Visual -> Classes add:
     Class Number = 5210
     Class Description = indeni Limited

   - Resync the Object Server Classes in your Netcool/OMNIbus EventList

5. Edit "deduplication" trigger in the Netcool/OMNIbus Object Server:

   - In Netcool/OMNIbus Administrator -> ObjectServer Configuration -> Automation -> Triggers, edit the *Deduplication* trigger, replacing

     set old.Summary = new.Summary;

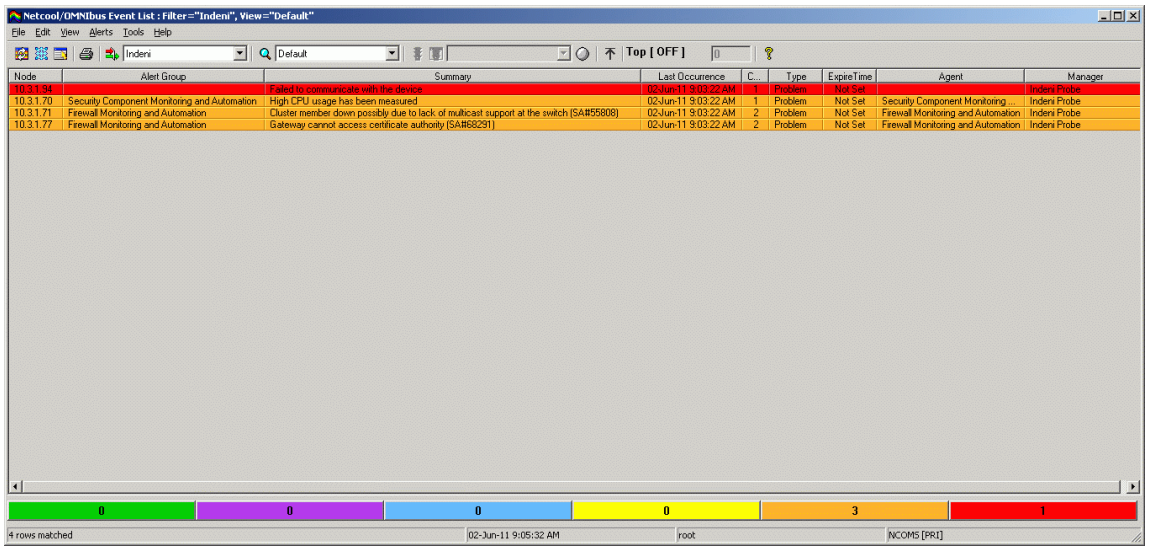
     with

     if ((old.Class = 5210) and (new.Type = 2))
     then
     set old.Summary = 'Resolution of: ' + old.Summary;
     else
     set old.Summary = new.Summary;
     end if;

6. Restart the SNMP Probe (nco_p_mttrapd).

Screenshots

The figures below show examples of a Netcool/OMNIbus EventList, populated with indeni Security Operations Monitoring Solution events:

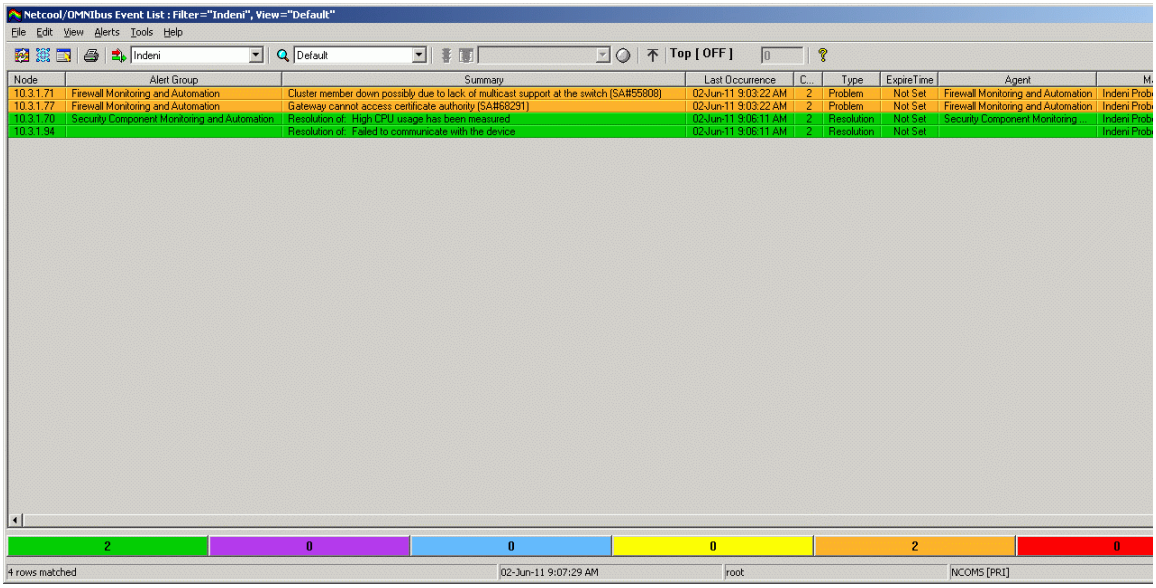


indeni Inc.
1 Bridge Plaza, 2nd floor
Fort Lee, NJ, 07024 USA
Tel: +1-877-778-8991
E-mail: info@indeni.com

indeni Israel
14 Menachem Begin Rd.
Ramat Gan, 52700 Israel
Tel: +1-809-494-190
E-mail: info@indeni.com

indeni UK Limited
60 Goswell Road
London, EC1M7AD UK
Tel: +44-800-098-8972
Email: info@indeni.com

www.indeni.com



Notes

<arch> is a variable that represents your operating system directory. For example, win32 for Windows.

References

1. Netcool/OMNIbus SNMP Probe Reference Guide April 30, 2009
2. Netcool/OMNIbus Version 7 Release 3 Probe and Gateway Guide
3. Netcool/OMNIbus Version 7 Release 3 Administration Guide

indeni Inc.
1 Bridge Plaza, 2nd floor
Fort Lee, NJ, 07024 USA
Tel: +1-877-778-8991
E-mail: info@indeni.com

indeni Israel
14 Menachem Begin Rd.
Ramat Gan, 52700 Israel
Tel: +1-809-494-190
E-mail: info@indeni.com

indeni UK Limited
60 Goswell Road
London, EC1M7AD UK
Tel: +44-800-098-8972
Email: info@indeni.com

www.indeni.com

indeni network optimism

About indeni

indeni is entrusted by enterprises around the globe to keep their networks running smoothly 24/7/365.

Founded in 2009 by a team of network security experts, indeni is reshaping the way complex networks are managed. Unlike standard up/down solutions, indeni is built on Dynamic Knowledge - giving enterprises a way to future-proof their ever-evolving network.

indeni lets you automate error checking, prevent configuration mistakes and pre-empt dormant issues months before they cause service disruption. The result: unprecedented network visibility, control and optimism.

Our game-changing Dynamic Knowledge solutions are rapidly winning the attention of Global and Fortune 100 companies - from Telco and Financial organizations to government agencies and SMBs. For more information about indeni, visit www.indeni.com or email us at sales@indeni.com.

indeni Inc.
1 Bridge Plaza, 2nd floor
Fort Lee, NJ, 07024 USA
Tel: +1-877-778-8991
E-mail: info@indeni.com

indeni Israel
14 Menachem Begin Rd.
Ramat Gan, 52700 Israel
Tel: +1-809-494-190
E-mail: info@indeni.com

indeni UK Limited
60 Goswell Road
London, EC1M7AD UK
Tel: +44-800-098-8972
Email: info@indeni.com

www.indeni.com