

An Event Connector Case Study: SolarWinds

Overview

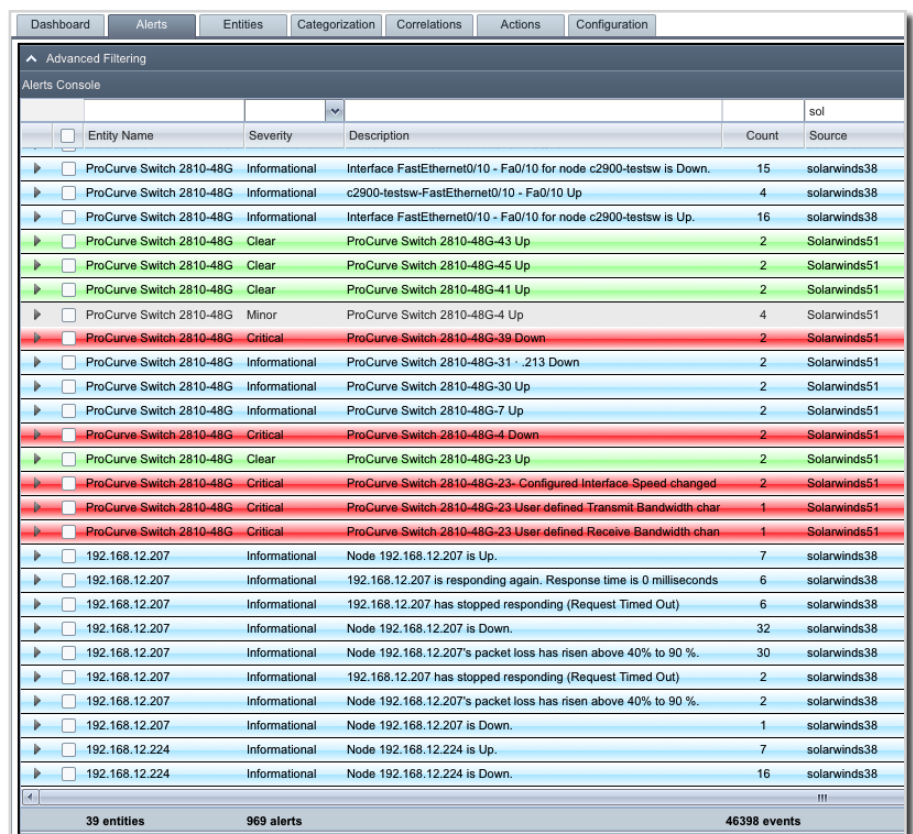
The SolarWinds Connector delivers out-of-the-box integration between SolarWinds Orion NPM and RightITnow ECM. This enables consolidation, correlation and reduction of a high volume of events and alerts from SolarWinds Orion NPM alongside other sources of IT events, via RightITnow ECM's real-time event correlation technology. IT Operations and Service Desk staff gain from a streamlined processing of events and alerts that they can remediate quickly and effectively. In addition, they can seamlessly integrate their Operations console with the Service Desk, through a close-loop incident management process not available in Orion NPM.

How It Works

The SolarWinds Connector imports all events, alerts, topology and entity information into the RightITnow ECM repository using the SolarWinds Interface Service (SWIS). It is designed to work against multiple instances of Orion NPM. The information collected includes:

- ▶ SolarWinds proprietary identifiers like Node and Interface ID's
- ▶ Device identifiers like IP address, community string, MAC address etc.
- ▶ Device status information like up or down, managed or unmanaged
- ▶ Business context data like location, contact, service name etc.

RightITnow ECM's event correlation engine then reduces the number of SolarWinds events and alerts into meaningful and service impacting RightITnow alerts. The correlation operates not only against the flow of events and alerts from SolarWinds, but any infrastructure event captured by RightITnow ECM as well - enabling advanced cross-domain correlation.



Entity Name	Severity	Description	Count	Source
ProCurve Switch 2810-48G	Informational	Interface FastEthernet0/10 - Fa0/10 for node c2900-testsw is Down.	15	solarwinds38
ProCurve Switch 2810-48G	Informational	c2900-testsw-FastEthernet0/10 - Fa0/10 Up	4	solarwinds38
ProCurve Switch 2810-48G	Informational	Interface FastEthernet0/10 - Fa0/10 for node c2900-testsw is Up.	16	solarwinds38
ProCurve Switch 2810-48G	Clear	ProCurve Switch 2810-48G-43 Up	2	Solarwinds51
ProCurve Switch 2810-48G	Clear	ProCurve Switch 2810-48G-45 Up	2	Solarwinds51
ProCurve Switch 2810-48G	Clear	ProCurve Switch 2810-48G-41 Up	2	Solarwinds51
ProCurve Switch 2810-48G	Minor	ProCurve Switch 2810-48G-4 Up	4	Solarwinds51
ProCurve Switch 2810-48G	Critical	ProCurve Switch 2810-48G-39 Down	2	Solarwinds51
ProCurve Switch 2810-48G	Informational	ProCurve Switch 2810-48G-31 - 213 Down	2	Solarwinds51
ProCurve Switch 2810-48G	Informational	ProCurve Switch 2810-48G-30 Up	2	Solarwinds51
ProCurve Switch 2810-48G	Informational	ProCurve Switch 2810-48G-7 Up	2	Solarwinds51
ProCurve Switch 2810-48G	Critical	ProCurve Switch 2810-48G-4 Down	2	Solarwinds51
ProCurve Switch 2810-48G	Clear	ProCurve Switch 2810-48G-23 Up	2	Solarwinds51
ProCurve Switch 2810-48G	Critical	ProCurve Switch 2810-48G-23 - Configured Interface Speed changed	2	Solarwinds51
ProCurve Switch 2810-48G	Critical	ProCurve Switch 2810-48G-23 User defined Transmit Bandwidth chan	1	Solarwinds51
ProCurve Switch 2810-48G	Critical	ProCurve Switch 2810-48G-23 User defined Receive Bandwidth chan	1	Solarwinds51
192.168.12.207	Informational	Node 192.168.12.207 is Up.	7	solarwinds38
192.168.12.207	Informational	192.168.12.207 is responding again. Response time is 0 milliseconds	6	solarwinds38
192.168.12.207	Informational	192.168.12.207 has stopped responding (Request Timed Out)	6	solarwinds38
192.168.12.207	Informational	Node 192.168.12.207 is Down.	32	solarwinds38
192.168.12.207	Informational	Node 192.168.12.207's packet loss has risen above 40% to 90 %.	30	solarwinds38
192.168.12.207	Informational	192.168.12.207 has stopped responding (Request Timed Out)	2	solarwinds38
192.168.12.207	Informational	Node 192.168.12.207's packet loss has risen above 40% to 90 %.	2	solarwinds38
192.168.12.207	Informational	Node 192.168.12.207 is Down.	1	solarwinds38
192.168.12.224	Informational	Node 192.168.12.224 is Up.	7	solarwinds38
192.168.12.224	Informational	Node 192.168.12.224 is Down.	16	solarwinds38

FIGURE 1: RightITnow ECM extracts alerts from multiple NPM instances, de-duplicates in real-time and enriches them with owner and service information.

An Event Connector Case Study : SolarWinds

With RightITnow ECM and the SolarWinds Connector, IT operations staff can then plan and execute appropriate operational response to these alerts using multiple paths:

- ▶ IT Operations staff can use a RightITnow ECM alert to access relevant SolarWinds reports, enabling them to understand why the events were generated and provide a head-start to problem resolution
- ▶ Operators can use RightITnow ECM to re-poll an interface or device via Orion NPM in order to verify their current status
- ▶ Operators can escalate alert to the Service Desk. Recorded incidents are enriched by connections to underlying events and contextual performance reports within Orion NPM - facilitating problem investigation and resolution
- ▶ IT Operator acknowledged alerts in RightITnow ECM, are also automatically acknowledged in the SolarWinds Orion alert list

To maintain data and event integrity, the SolarWinds Connector continuously updates RightITnow ECM by periodically checking and updating changes from the various instances of SolarWinds Orion NPM.

Why Try the Connector?

The SolarWinds Connector provides granular, proactive monitoring of IT infrastructure combining SolarWinds event streams with other event sources like SNMP traps, Windows Event and Syslog messages, VMWare infrastructure, and other monitoring tools.

In addition, it makes it easy to:

- ▶ Perform early diagnosis and resolution of infrastructure issues
- ▶ Achieve higher uptime and service levels
- ▶ Have a streamlined and automated operations process

System Specifications

The SolarWinds Connector works with SolarWinds Orion NPM v10.0 or later.

About RightITnow

RightITnow delivers real-time, cross-domain event correlation software that enables enterprises to optimize IT Operations processes so they can drive down costs, resolve problems faster and assure end user services. It achieves this by automating the event to alert to incident life cycle and bridging the gap between IT Operations center and the Service Desk – driving higher productivity and effectiveness.

Contact us at info@RightITnow.com

US Office 112 Bandol Court, San Ramon, CA 94582 USA +1 415 992 6390

The screenshot shows the 'Alerts Console' interface. At the top, there are tabs for 'Dashboard', 'Alerts', 'Entities', 'Categorization', 'Correlations', 'Actions', and 'Configuration'. Below the tabs is an 'Advanced Filtering' section. The main area is a table with columns: 'Entity Name', 'Severity', 'Description', 'Count', and 'Source'. The table contains several rows of alerts, mostly from 'solarwinds38'. A context menu is open over one of the rows, showing options like 'Change Severity', 'Assign To', 'Close Alert', 'Show alert details in SolarWinds', and 'Open a ticket in Service-Now'.

Entity Name	Severity	Description	Count	Source
RivermuseTC0	Minor	ProCurve Switch 2810-48G-36 Up	6	solarwinds38
RivermuseTC0	Minor	Interface 36 for node ProCurve Switch 2810-48G is Up.	24	solarwinds38
RivermuseTC0	Minor	Interface 12 for node ProCurve Switch 2810-48G is Down.	7	solarwinds38
RivermuseTC0	Minor	Interface 13 for node ProCurve Switch 2810-48G is Down.	12	solarwinds38
RivermuseTC0	Minor	Interface 17 for node ProCurve Switch 2810-48G is Down.	14	solarwinds38
RivermuseTC0	Minor	Interface 20 for node ProCurve Switch 2810-48G is Down.	8	solarwinds38
RivermuseTC0	Minor	Interface 23 for node ProCurve Switch 2810-48G is Down.	10	solarwinds38
RivermuseTC0	Minor	ProCurve Switch 2810-48G-36 Down	6	solarwinds38
RivermuseTC0	Minor	Interface 36 for node ProCurve Switch 2810-48G is Down.	8	solarwinds38
RivermuseTC0	Minor	Interface 25 : 213 Mirror for node		solarwinds38
RivermuseTC0	Informational	Interface 28 for node ProCurve Si		solarwinds38
RivermuseTC0	Informational	Interface 29 : ChrisDesk for node		solarwinds38
RivermuseTC0	Informational	Interface 32 for node ProCurve Si		solarwinds38
RivermuseTC0	Informational	Interface 35 for node ProCurve Si		solarwinds38
RivermuseTC0	Informational	Interface 37 for node ProCurve Si		solarwinds38
RivermuseTC0	Informational	Interface 38 for node ProCurve Si		solarwinds38
RivermuseTC0	Informational	Interface 40 for node ProCurve Si		solarwinds38
RivermuseTC0	Informational	Interface 42 for node ProCurve Si		solarwinds38
RivermuseTC0	Informational	Interface 46 for node ProCurve Switch 2810-48G is Down.	5	solarwinds38
RivermuseTC0	Informational	Interface 47 for node ProCurve Switch 2810-48G is Down.	13	solarwinds38
RivermuseTC0	Informational	Interface 3 for node ProCurve Switch 2810-48G is Down.	9	solarwinds38
RivermuseTC0	Informational	Interface 5 for node ProCurve Switch 2810-48G is Down.	9	solarwinds38
RivermuseTC0	Informational	Interface 9 for node ProCurve Switch 2810-48G is Down.	12	solarwinds38
192.168.12.23	Major	conn=72620 fd=44 ACCEPT from IP=127.0.0.1:32943 (IP=0.	1	syslog

FIGURE 2: Every RightITnow alert provides direct contextual access to the SolarWinds console