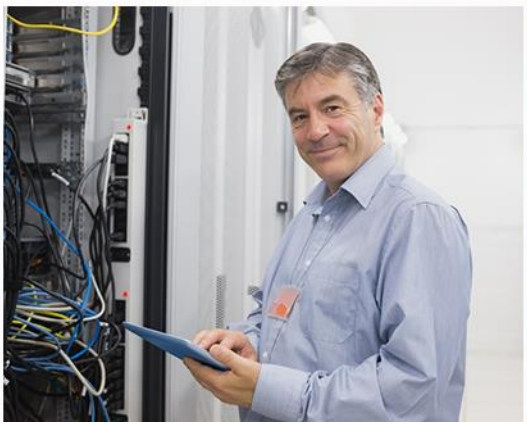
Enterprise Alert® 2015: Integration with SolarWinds Orion NPM



EnterpriseAlert® - Transforming critical incident communication


1 ABSTRACT 3

2 STEP 1 – CREATE A SOLARWINDS EVENT SOURCE IN ENTERPRISE ALERT® 4

3 STEP 2 – PREPARE AND CREATE AN ALERT ACTION IN SOLARWINDS 6

4 STEP 3 – CREATE ALERT POLICY AND RUN A TEST SCENARIO 8

5 CONTACT 9

5.1 Mailing Address 9

5.2 Hours of Operation 9

6 DISCLAIMER 10

PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM

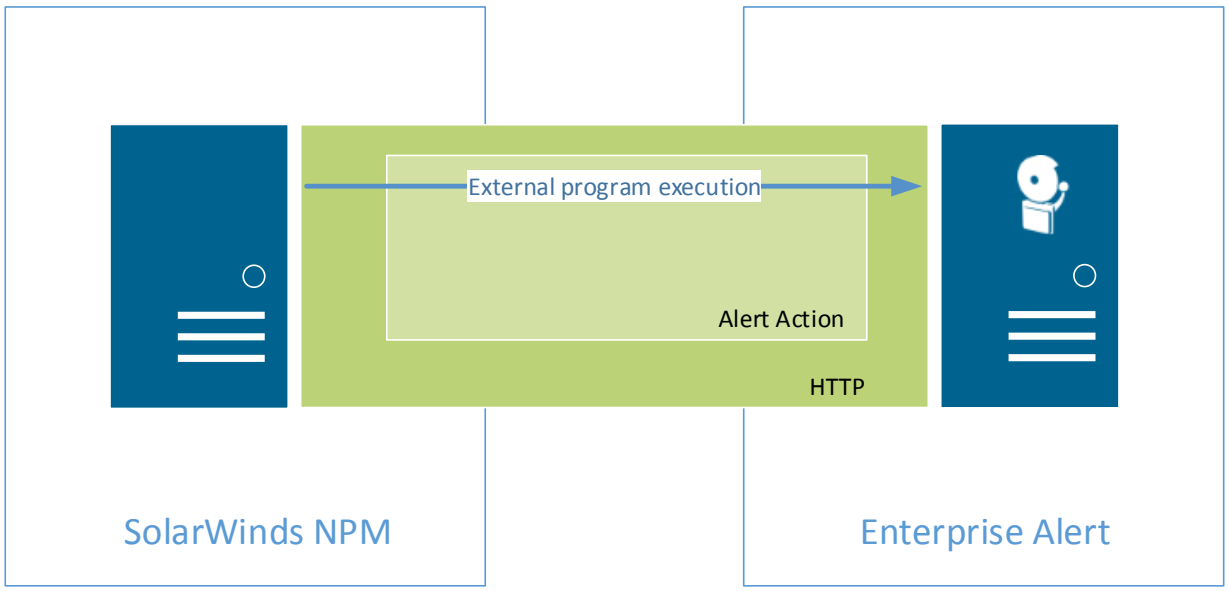
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

1 ABSTRACT

The integration between SolarWinds NPM and Enterprise Alert® is based on a Web Service (part of Enterprise Alert®) which is great for a cloud deployment of Enterprise Alert® while your SolarWinds system runs on your premises.

This document contains instructions and guidance about how Enterprise Alert® 2015 is integrated with SolarWinds Network Performance Monitor (NPM).

The basic architecture is displayed below:



2 STEP 1 – CREATE A SOLARWINDS EVENT SOURCE IN ENTERPRISE ALERT®

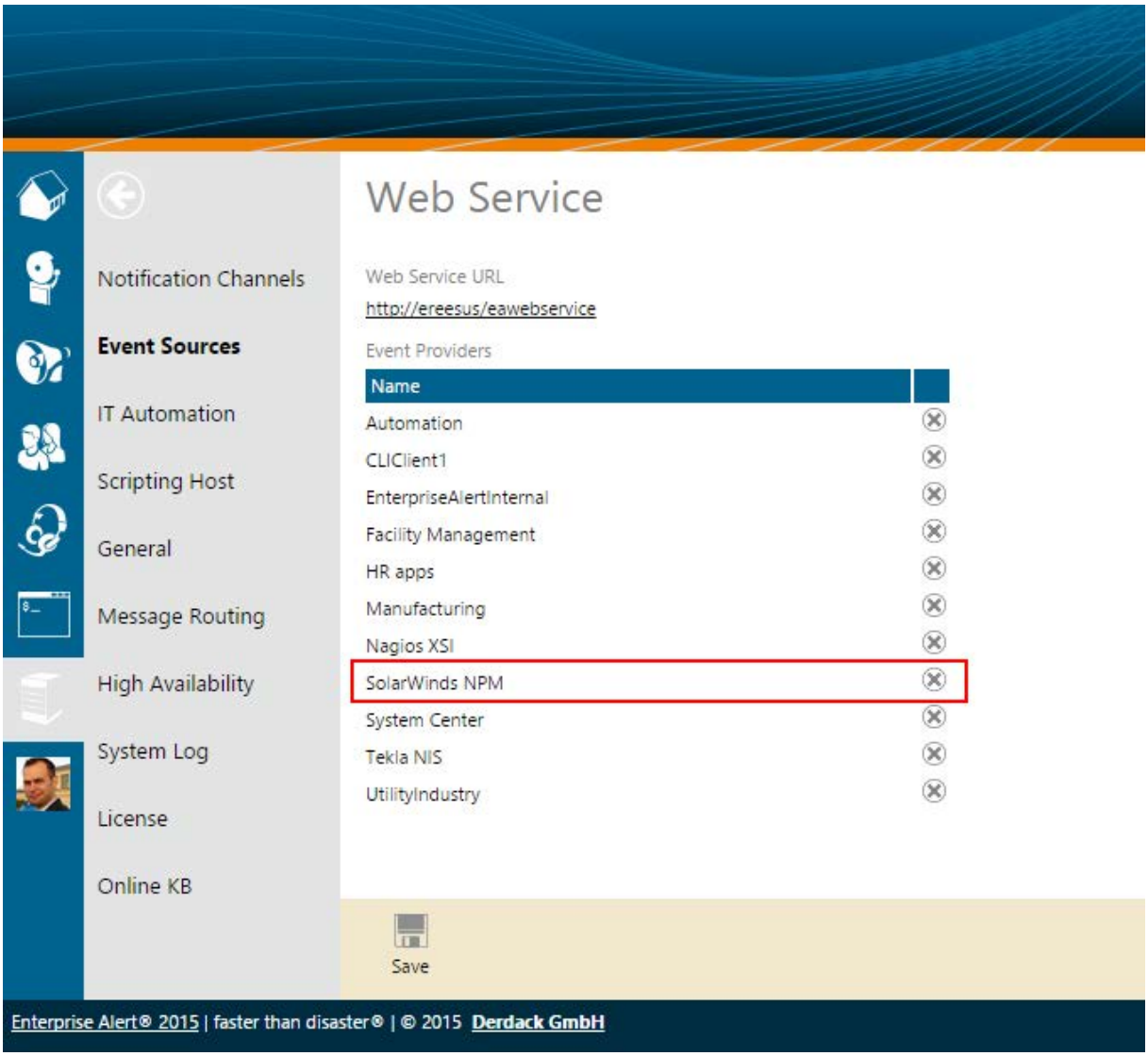
The first step is to create a new web service event source (also referred to as event provider) in Enterprise Alert® by performing the tasks below:

1) On the Enterprise Alert® machine browse to the web service command line client.
   By default it can be found here:
   %Program Files%\Enterprise Alert\CommandLine
2) Open the **RemoteCLI.exe.config** file in Notepad and
   a. Update the setting "EAWebServiceURL" with the FQDN of your Enterprise Alert® server
   b. Enter admin access credentials of Enterprise Alert® in the settings "UserName" and "Password"
   c. Save the file
3) Open a commend shell and execute the following command to register a SolarWinds NPM event source in Enterprise Alert®:
   RemoteCLI REGISTER /provider:"SolarWinds NPM" /params:"Acknowledged;AcknowledgedBy;AcknowledgedTime;AlertTriggerCount;AlertTriggerTime;Application;ObjectName;NodeID;Status;StatusDescription;NodeName;AvgResponseTime;Severity;GroupID;GroupName"

Please note, the parameters that are specified here are only a selection of available SolarWinds incident attributes. You may remove attributes or add others in the call above.

You can find all available attributes online in the SolarWinds help under http://www.solarwinds.com/documentation/en/flarehelp/orionplatform/default.htm#orioncoreagadvancedalertvariablesgeneral.htm%3FTocPath%3DOrion%2520Platform%2520Admin%2520Guide%7COrion%2520Variables%2520and%2520Examples%7CAdvanced%2520Alert%2520Engine%2520Variables%7C_____1

4) Log on to Enterprise Alert® and navigate to **System –> Event Sources**. Click on Web Service. You should see a new source having the name SolarWinds NPM:



3 STEP 2 – PREPARE AND CREATE AN ALERT ACTION IN SOLARWINDS

The second step is to prepare and configure an Alert Action in SolarWinds. When SolarWinds creates events it can perform actions such as sending emails or executing external applications. For the purpose of simply forwarding an event to Enterprise Alert® an external application execution action must be created. The external app will be the command line client of the Enterprise Alert® web service which is able to send incidents to Enterprise Alert®. Follow the steps below to create the alert action in SolarWinds:

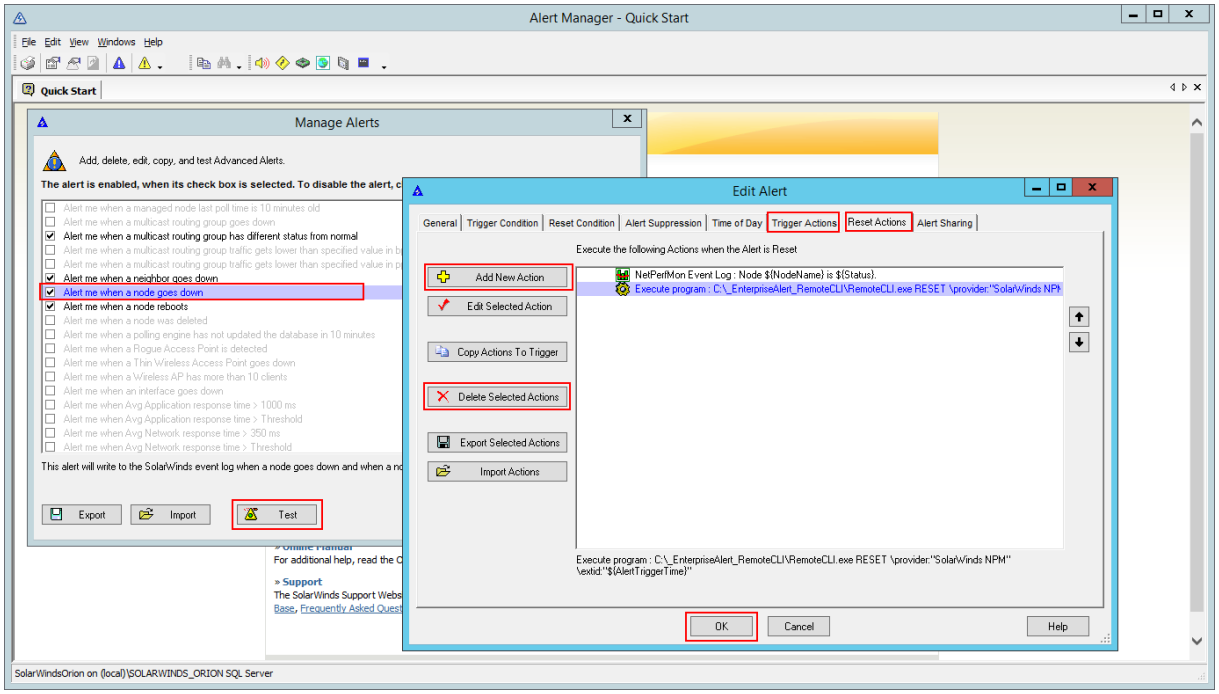
1) On the SolarWinds machine create a folder in which you can save the command line application of Enterprise Alert® (e.g. **C:\EA_RemoteCLI**)
2) Copy the file **RemoteCLI.exe** from the Enterprise Alert® machine into this folder
3) On the SolarWinds machine navigate to the folder **C:\Windows\System32** in Windows Explorer and copy the file **RemoteCLI.exe.config** from the Enterprise Alert® machine into this folder
4) On the SolarWinds machine open the "Advanced Alert Manager" of SolarWinds. A shortcut to it can be found here: **C:\ProgramData\Microsoft\Windows\Start Menu\Programs\SolarWinds Orion\Alerting, Reporting, and Mapping**
5) Click the "**Configure Alerts**" button.
6) Select the rule "**Alert me when a node goes down**" and click Edit
7) Click "**Trigger Actions**".
8) Remove the send email action if it is present
9) Click "**Add New Action**" and select "**Execute external program**"
10) In the textbox paste the following command line call which forwards the event in SolarWinds to Enterprise Alert®

    C:\EA_RemoteCLI\RemoteCLI.exe RAISE /provider:"SolarWinds NPM" /extid:"${AlertTriggerTime}" /params Acknowledged:"${Acknowledged}" AcknowledgedBy:"${AcknowledgedBy}" AcknowledgedTime:"${AcknowledgedTime}" AlertTriggerCount:"${AlertTriggerCount}" AlertTriggerTime:"${AlertTriggerTime}" Application:"${Application}" ObjectName:"${ObjectName}" NodeID:"${NodeID}" Status:"${Status}" StatusDescription:"${StatusDescription}" NodeName:"${NodeName}" AvgResponseTime:"${AvgResponseTime}" Severity:"${Severity}" GroupID:"${GroupID}" GroupName:"${GroupName}"

    The parameter "exid" is used to correlate event updates to initially received new incidents in Enterprise Alert®.
11) Click "**Reset Action**"
12) Again, remove the email action and add an external program execution action
13) In the textbox paste the following command line call which forwards an event in SolarWinds to Enterprise Alert®

    C:\EA_RemoteCLI\RemoteCLI.exe RESET /provider:"SolarWinds NPM" /extid:"${AlertTriggerTime}"

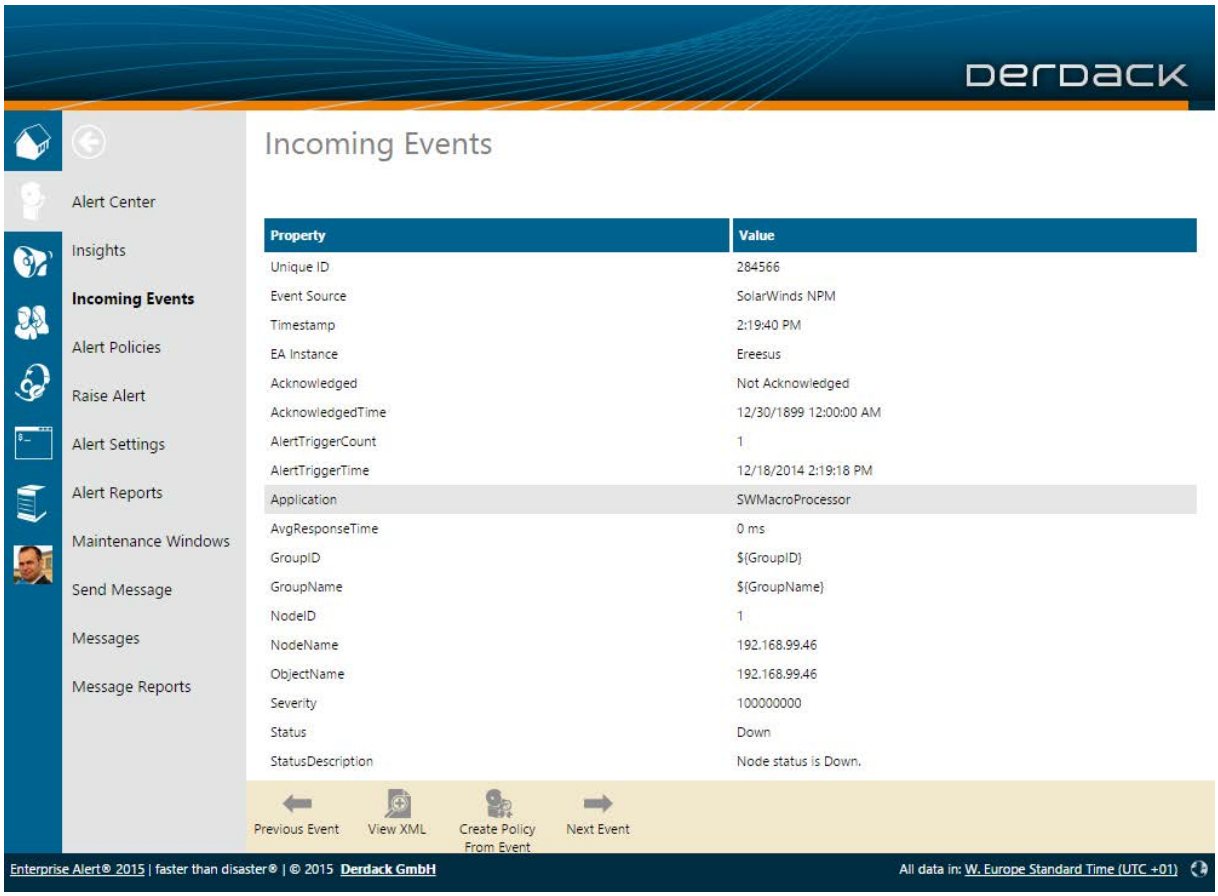
    Configuring the reset action in addition to the trigger action results in the effect that alerts in Enterprise Alert® will be automatically closed in case corresponding nodes in SolarWinds are no longer down.
14) Click OK to apply your changes. You can now click "Test" in order to create a test event and execute the trigger action. This should give you a new event from the SolarWinds NPM event source in the Incoming Events journal in Enterprise Alert® (**Alerts -> Incoming Events**)



PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585

4 STEP 3 – CREATE ALERT POLICY AND RUN A TEST SCENARIO

Once you receive your events in Enterprise Alert® you can create an Alert Policy for these events. With the policy you configure which team or on-call person is receiving a particular SolarWinds event. In the policy details you have access to all the event parameters of SolarWinds and with the policy conditions you can fetch events matching certain characteristics (e.g. belong to a specific application or group) in order to define responsibility and to be able to target your alerts to the right people in the policy (alert destination).



A zip file with the two external app execution actions from the SolarWinds Alert Manager for plug-and-play import can also be found here: http://1drv.ms/1zzTUaI

5 CONTACT

Please visit www.derdack.com for further information on Enterprise Alert® or contact us:

Germany: +49 (331) 29878-20 (German, English, Spanish), Fax: +49 (331) 29878-22

UK: +44 (20) 88167095

US: +1 (202) 4700885

Email: info@derdack.com

5.1 Mailing Address

Derdack GmbH
Wilhelmgalerie
Friedrich-Ebert-Strasse 8
14467 Potsdam
Germany

5.2 Hours of Operation

Monday – Friday 09:00 a.m. – 06:00 p.m. Central European Time (GMT+1)

Closed Saturday and Sunday and on German and local public holidays

6 DISCLAIMER

© DERDACK GMBH, WWW.DERDACK.COM
PHONE +49 331 29878-0 · FAX +49 331 29878-22 · WWW.DERDACK.COM
AMTSGERICHT POTSDAM, HRB 13071 · MANAGING DIRECTOR: MATTHES DERDACK · EU VAT ID: DE 812 810 585