



# **Creating Agent Health Alerts in Data Center Security**

August, 2015

## Summary

Many times, a Data Center Security (DCS) administrator needs to be notified when a critical system is offline. While it is possible to capture and alert on these events in the DCS console, it is not a default setting. In this article we will examine step-by-step the necessary settings that need to be configured, and a short tutorial on how to construct the alert.

### Items needed to complete this exercise:

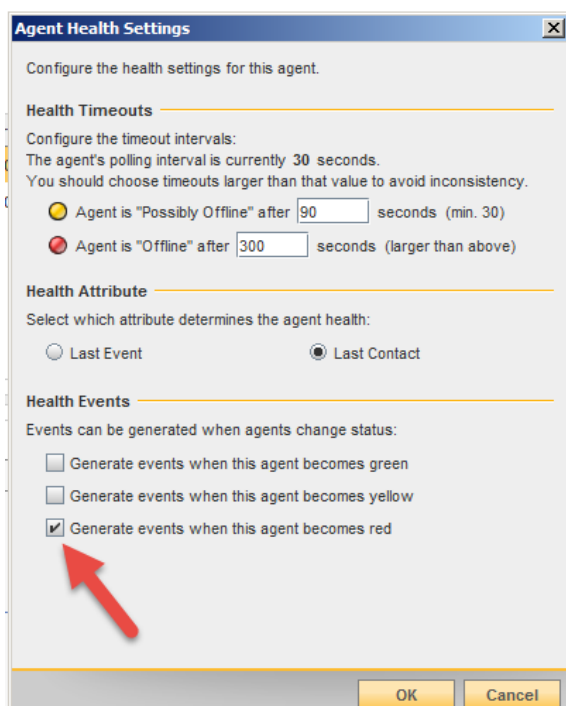
1. Access to the DCS console
2. Access to a test machine with the DCS agent installed that can be taken offline
3. A basic understanding of the DCS console, including how to navigate to different areas within the console and how to find the required information

### Step One:

#### Configuring DCS to generate events based on agent health

Alerts can be generated from any event that appears in the DCS console. The problem is that agent(s) going offline do not generate events by default. So, the first step is to configure DCS to generate events based on those criteria.

In the Assets view, highlight multiple assets, right click and choose *Properties*. Be sure to include the test machine. This will bring up the **Agent Health Settings** dialog window.



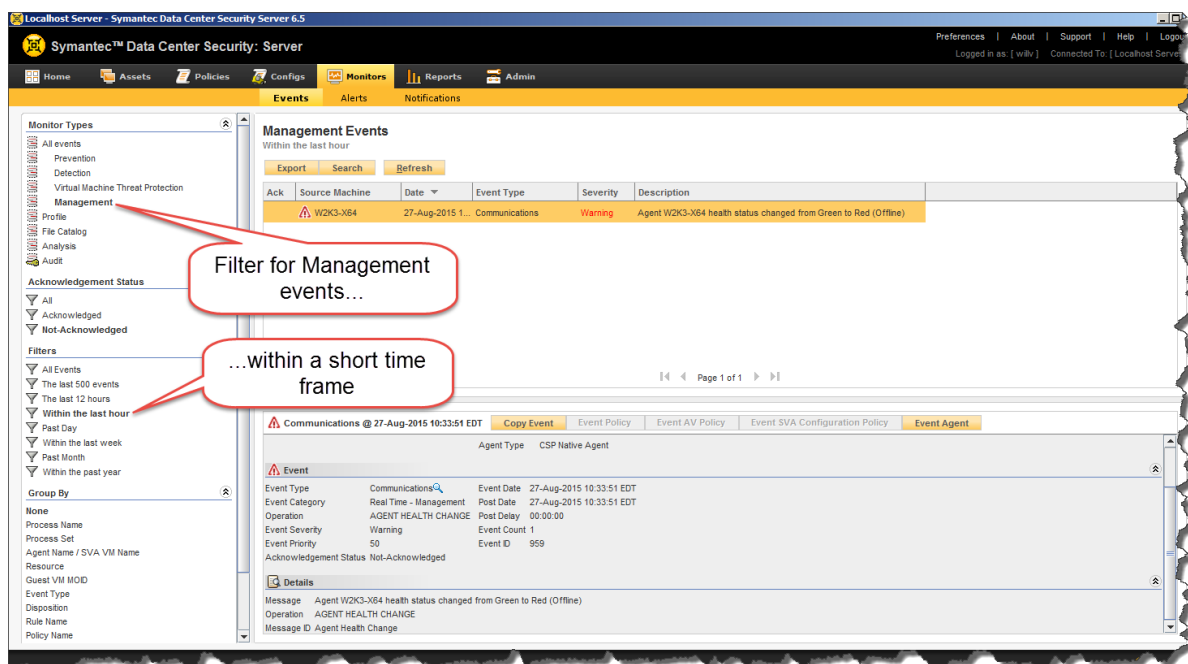
*Note:* If only one asset is chosen, the **Agent Health Settings** dialog window will be accessed from the **Configure Health** button found on the **General** tab.

In this window simple check boxes are displayed that enable (or, disable) events to be produced when an agents health status changes. In this example, an asset going offline (red) is the desired event to be generated.

Check the appropriate box, then click **OK**.

## Step Two: Configuring the alert

Before we can configure an appropriate alert, it is important to be able to identify the actual conditions that trigger the event. To do that, we will look at the details of the event that is generated by the agent going offline. To do that we will need to force an event generation. Take what ever steps are necessary to take the test machine offline. Allow the appropriate amount of time to elapse for an event to be generated. Review the agent health settings to determine the timeout settings for agent health. Once the timeout value has been exceeded, you will see a management event returned to the console and displayed in the *Events* view.

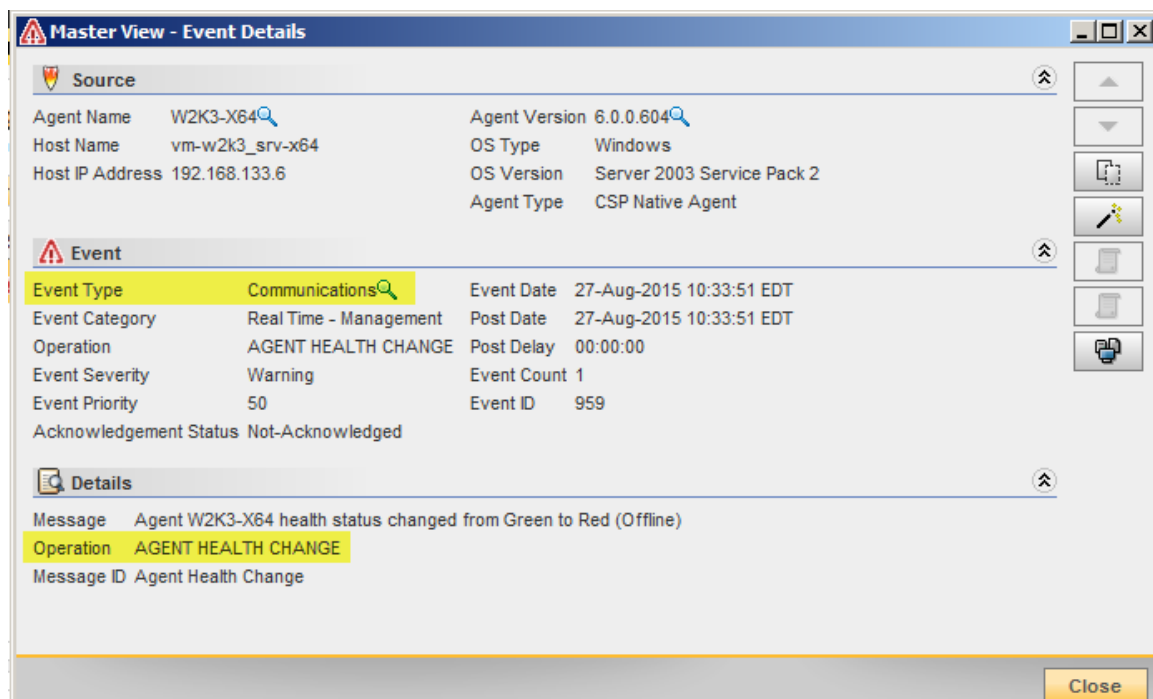


Filter for Management events...

...within a short time frame

Event Type	Event Category	Event Date	Event Policy	Event AV Policy	Event SVA Configuration Policy	Event Agent
Communications	Real Time - Management	27-Aug-2015 10:33:51 EDT	AGENT HEALTH CHANGE			

Examine the details of the event to get clues on how to construct the alert.



**Source**

Agent Name W2K3-X64 Agent Version 6.0.0.604  
 Host Name vm-w2k3\_srv-x64 OS Type Windows  
 Host IP Address 192.168.133.6 OS Version Server 2003 Service Pack 2  
 Agent Type CSP Native Agent

**Event**

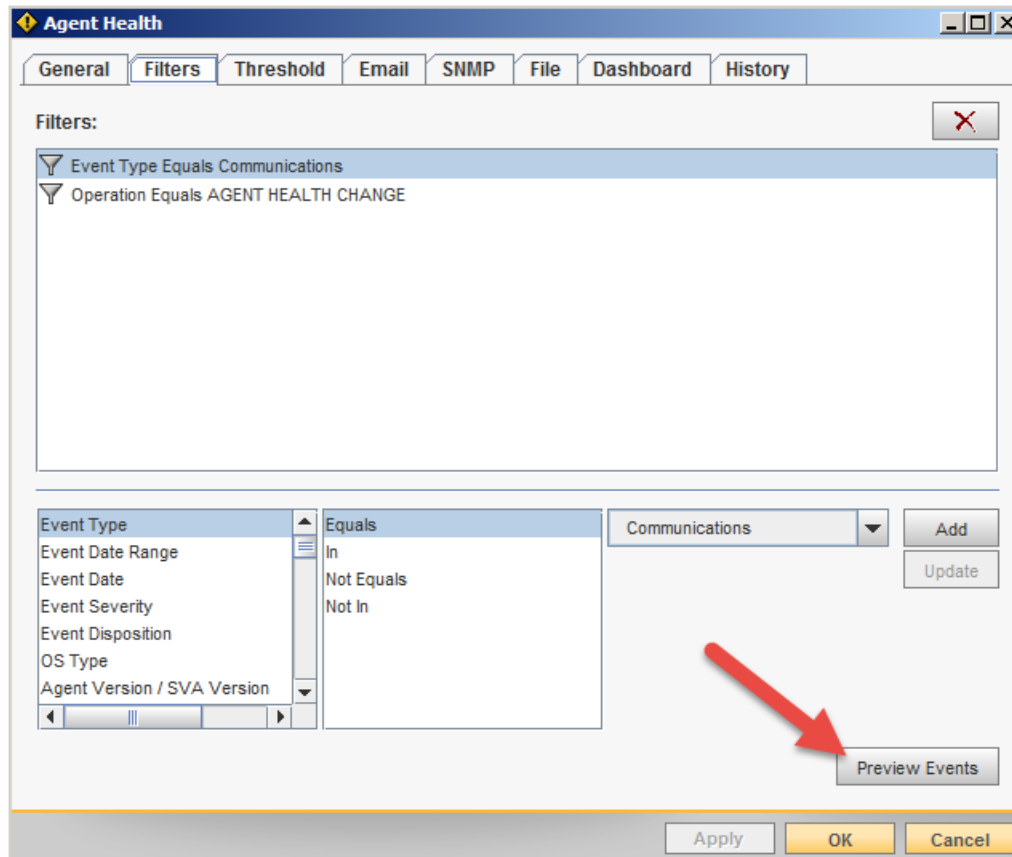
Event Type Communications Event Date 27-Aug-2015 10:33:51 EDT  
 Event Category Real Time - Management Post Date 27-Aug-2015 10:33:51 EDT  
 Operation AGENT HEALTH CHANGE Post Delay 00:00:00  
 Event Severity Warning Event Count 1  
 Event Priority 50 Event ID 959  
 Acknowledgement Status Not-Acknowledged

**Details**

Message Agent W2K3-X64 health status changed from Green to Red (Offline)  
 Operation AGENT HEALTH CHANGE  
 Message ID Agent Health Change

Close

It is important to capture enough information to be able to narrowly configure the alert filters. In the above example we will want to take advantage of the two entries in the *Event Details* highlighted in yellow.



Construct the filters as shown. Note: these filters are exactly as shown in the event details. Next, use the *Preview Events* button to ensure that the correct events will trigger the alert. Finally, configure the remainder of the alert settings (email, SNMP, or flat file) according to your needs.

### Step Three: TEST

As always, test your configurations. Remember to allow the timeout for the agent offline setting to expire. This is longer than the polling interval so patience is required. After the alert has been validated it is ready for use.