

### 5 Tips for Improving Alarm Efficiency

Alerts from syslog, SNMP and event log messaging can be overwhelming. Many network managers find that critical alerts get lost in the sea of notifications. The following five steps will improve your ability to spot real problems when they occur.

#### Tip 1: Clear Alarms Once They Are Resolved

An easy way to significantly improve alarm visibility is to clear alarms after a problem has been fixed. While alarm clearing may seem rudimentary, it will increase your ability to see critical alarms and eliminate a backlog in the alarm grid. Remember, not all alarm conditions auto-clear.

#### Tip 2: Adjust Alarm Severities

Many device vendors simply cry wolf and set too many alerts as “Critical,” which floods the alarm grid and hides truly critical problems. To prevent this, use a network management system that offers the ability to set or adjust the severity of an alert based on device type. For example, a major alarm is set to occur when key servers restart, but a less significant, informational alert is set to occur when access point switches restart. Properly setting the alert rule severity will save critical time when problems occur.

#### Tip 3: Set Appropriate Threshold Levels

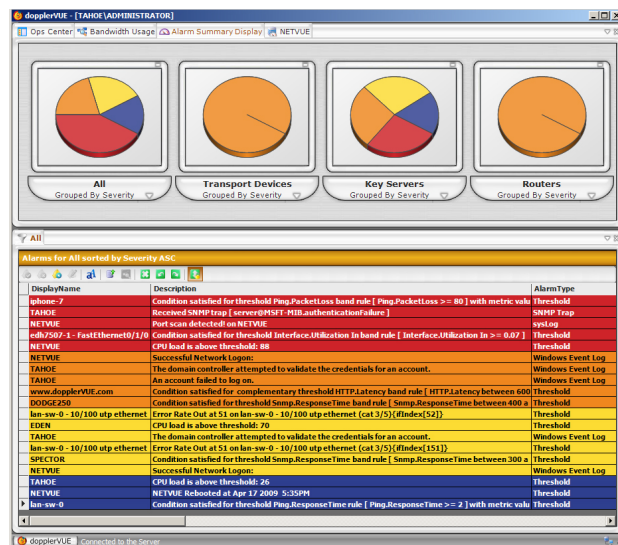
False positives can ruin the value of a performance polling system. Just as with alerts, many hardware vendors ship their products with default values for performance metrics that are designed to alert the user to any possible issue, which will cause a very large number of alarms. If you frequently get alerts that you never act on, it is time to make adjustments and set threshold levels to suit your environment.

Often this is best done by setting a sustained duration rate. For example, if the interface utilization stays above 80% for more than 30 minutes, then provide an alert. Using sustained duration will eliminate alerting on short term spikes in network conditions that you may not be able to fix quickly. The important question to ask yourself is “What would I do with this alert?” If the answer is to wait to see if it continues, then adjusting the duration before getting an alert is a good idea.

#### Tip 4: Create Custom Filters

Problems with devices that provide transport layer services will create a ripple effect on the network, causing many downstream devices to generate alerts as well. Avoid this problem by creating custom filters that only include these devices and sort them by severity. This will keep the problems most likely to cause damage on top of the alarm grid. You can extend this concept by setting specialized filters for your key servers and other high value devices. The main goal is to hide alerts on low level devices or those with low severities until they are needed.

Figure 1: dopplerVUE's alarm summary display, sorted by alarm severity.



## Tip 5: Consolidate Information

To visualize your network more efficiently, aggregate all network alerting into a single location. Having too little information is just as frustrating as too much information. In both cases, you simply end up not using the data. Manager-of-Manager systems (MOM's) provide an effective way to see your fault, performance and security alerts in a single screen sorted by severity. Looking at these alerts may not provide a true picture of the situation and can lead to data being ignored. Being able to see security attacks and performance or fault problems on a single screen provides the cause and effect. Turn on all of the alerting and use the sorting, filtering, and grouping capabilities of your NMS to get the big picture.

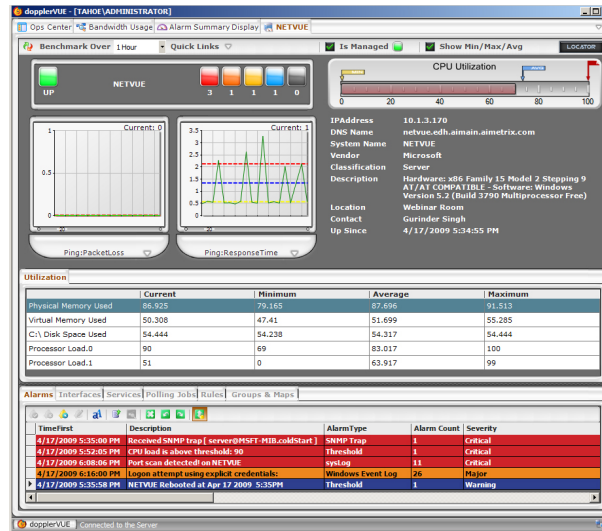


Figure 2: dopplerVUE's device view shows all alerts from any source.

## About dopplerVUE

dopplerVUE brings powerful network management features once available only in enterprise-grade solutions to networks of almost any size. **For more information about dopplerVUE visit [www.dopplerVUE.com](http://www.dopplerVUE.com) or call (888) 388-3669.**

© 2009 SYS Technologies. All Rights Reserved. All trade names referenced are the service mark, trademark or registered trademark of the respective manufacturer.