

Simple Network Management with Syslog

Staying on top of the overall health of your network is essential for maintaining optimal performance and availability. But how do you easily track thousands of network elements

and separate truly critical problems from ordinary network events? Automatically collecting event messages from network devices, rather than monitoring devices individually, is one common solution.


Over the years, the syslog protocol has evolved into an industry standard for creating, sending, and collecting event messages.

A standard syslog message includes the following information:

- Facility type (operating system, application, service, etc.) that originated the message.
- Severity level associated with the message (see Table 1).
- Date and time the message was sent.
- Hostname or IP address of the sending server or network device.
- Message text containing event description.

Want an easy-to-use syslog monitor for your desktop?

dVUE6 transforms syslog severity levels into visual alarms.



Operating systems, applications, and services continuously send these messages to centralized syslog servers. Depending on the capabilities of a particular syslog server, syslog messages can be sorted and viewed according to criteria such as message source, event severity, or key words in the message text. Additionally, the syslog server may filter syslog messages and raises alarms based on severity level. These alarms quickly draw your attention to unstable network elements, while the respective syslog messages provide the details you need to understand the source of the problem.

Table 1: Syslog Severity Levels

Code	Severity
0	Emergency: system is unusable
1	Alert: action must be take immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant
6	Informational: informational messages
7	Debug: debug-level messages

See Network Status at a Glance

dVUE6 is a graphical syslog server that allows you to easily monitor the status of key network devices from your desktop. Based on syslog severity codes, dVUE 6 displays availability and alarm indicators for the five most alarmed devices in your network.

When a device experiences a high number of alarm conditions, overall device availability is always a serious concern. For each displayed device, dVUE6 performs an ICMP ping every 15 seconds. You can periodically view ping response times to identify noticeable changes in device performance, which may imply potential problems.






Should a device fail to respond to a ping request, the availability indicator to the left of the device IP address changes from green to red, alerting you to a “down” device situation.

Meanwhile, at a glance, you can easily see the alarm status of the five most problematic devices in your network. As dVUE6 receives syslog messages, it:

- 1) Accumulates alarm counts for each device based on the syslog severity codes.
- 2) Displays the alarm status for the five most alarmed devices.
- 3) Illuminates all alarm indicators where one or more alarm counts exist (see Table 2).

In addition to monitoring increasing levels of alarm severity for a device, you can also view the number of alarm counts over time. If the alarm count starts to accelerate rapidly, particularly for critical or major alarms, the device may be on the verge of failing.

Table 2: dVUE6 Alarms

Alarm Indicator	Alarm Severity	Syslog Severity
Red 	Critical	Emergency (0) or Critical (1)
Orange 	Major	Alert (2)
Yellow 	Minor	Error (3)
Blue 	Warning	Warning (4)
Magenta 	Indeterminate	Notice (5), Informational (6), or Debug (7)

View Network Event Details

Because dVUE6 stores all syslog messages received from network devices, you can easily view the syslog message archive to see additional information regarding alarmed devices. Table 3 explains how to interpret a sample dVUE6 syslog message.

Table 3: dVUE6 Syslog Message

Message Field	Description
<code>Fri Dec 21 12:02:55 PST 2007</code>	Date and time at which dVUE5 received the message.
<code>Message : <188>171100: *Dec 21 11:45:56: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/0/0 (not half duplex), with lab-sw.aimetrix.com FastEthernet0/7 (half duplex).</code>	Message text explaining event or error (varies depending on device manufacturer).
<code>MessageDate : Dec 21 11:45:56</code>	Date and time message was sent.
<code>AgentAddress : 10.1.200.6</code>	Hostname or IP address of sending device.
<code>Facility : Local7</code>	Syslog facility.
<code>Severity : Warning</code>	Syslog severity level.
<code>ReceiverAddress : Civic[IPV4:514]</code>	Hostname or IP address of receiving device (dVUE5 computer).

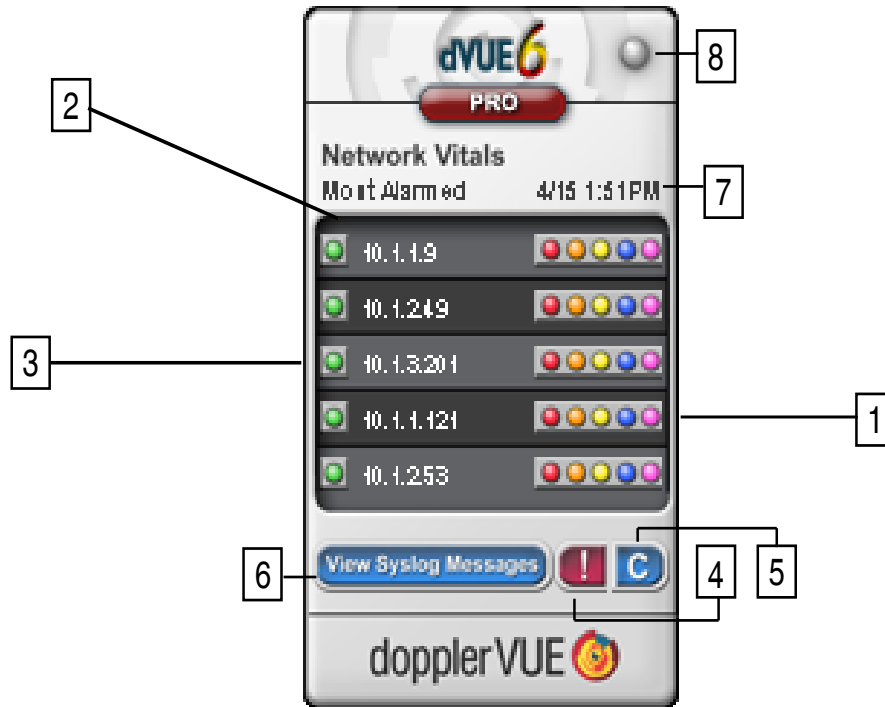
Set up dVUE6

Because dVUE6 is a Vista gadget, you simply add it to the Vista sidebar on your desktop. Or for any Windows system, unzip dVUE6x.zip and launch dVUE6x.exe. To receive syslog messages, be sure to add your computer’s IP address to the syslog configuration file of each device you wish to monitor (see the vendor documentation for instructions on how to add a syslog server, logger, or collector to the configuration file). Note that dVUE6 listens for syslog messages on port 514, which is the standard syslog port.

Using dVUE6

dVUE6 displays availability and alarm status for the five most alarmed devices at any given moment. That way, you always see the five devices in your network with the highest total alarm count. You can see additional details for a device by hovering over an availability or alarm severity indicator.

Note that closing dVUE6 (or restarting your computer) will suspend message collection and clear all alarm counts.



Code	Description
1	Alarm Severity Indicators alert you to alarm conditions (red/critical through magenta/indeterminate). Hover over an indicator to see alarm counts.
2	Status panel for each device shows availability, IP address, and alarm severity.
3	Availability Indicator tells you whether a device is up (green) or down (red). Hover over indicator to see ICMP ping messages for device.
4	Message Indicator illuminates whenever new syslog messages are received (click to reset).
5	Click to clear alarm counts. If you close dVUE6, alarm counts are not saved.
6	Click to view syslog messages (opens message archive in a Notepad window).
7	Timestamp shows when the list of Most Alarmed Devices was last updated.
8	When illuminated, signifies a new dVUE is available at www.dopplerVUE.com .

About dopplerVUE

dopplerVUE is a powerful yet easy to use network management solution for managing up to 5000 network elements. To see how dopplerVUE can solve your network management needs, visit to www.dopplerVUE.com. For more information call 888-dvue-now (888-388-3669).

© 2008 SYS Technologies. All Rights Reserved. All trade names referenced are the service mark, trademark or registered trademark of the respective manufacturer.