Type text to search here...
Home > Syslog Tutorial

Syslog Tutorial

May 22nd, 2014 Go to comments

As an administrator of a network, you have just completed all the configuration and they are working nicely. Now maybe the next thing you want to do is to set up something that can alert you when something goes wrong or down in your network. Syslog is an excellent tool for system monitoring and is almost always included in your distribution.

Places to store and display syslog messages

There are some places we can send syslog messages to:

Place to store syslog messages	Command to use
Internal buffer (inside a switch or router)	logging buffered [size]
Syslog server	logging
Flash memory	logging file flash:filename
Nonconsole terminal (VTY connection…)	terminal monitor
Console line	logging console

Note: If sent to a syslog server, messages are sent on UDP port 514.

By default, Cisco routers and switches send log messages to the console. We should use a syslog server to contain our logging messages with the logging command. Syslog server is the most popular place to store logging messages and administrators can easily monitor the wealth of their networks based on the received information.

Syslog syntax

A syslog message has the following format:

seq no:timestamp%FACILTY-SEVERITY-MNEMONIC: message text

Each portion of a syslog message has a specific meaning:
+ **Seq no**: a sequence number only if the service sequence-numbers global configuration command is configured
+ **Timestamp**: Date and time of the message or event. This information appears only if the service timestamps global configuration command is configured.
+ **FACILITY**: This tells the protocol, module, or process that generated the message. Some examples are SYS for the operating system, IF for an interface…
+ **SEVERITY**: A number from 0 to 7 designating the importance of the action reported.

The Syslog levels are:

Level	Keyword	Description
0	emergencies	System is unusable

1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Note: You can remember the order above with the sentence: “**E**ventually **A**ll **Critical Errors W**ill **N**ot **I**nvolve **D**amage”.

The highest level is level 0 (emergencies). The lowest level is level 7. To change the minimum severity level that is sent to syslog, use the logging trap *level* configuration command. If you specify a level, that level and all the higher levels will be displayed. For example, by using the logging console warnings command, all the logging of emergencies, alerts, critical, errors, warnings will be displayed. Levels 0 through 4 are for events that could seriously impact the device, whereas levels 5 through 7 are for less-important events. By default, syslog servers receive informational messages (level 6).

+ **MNEMONIC**: A code that identifies the action reported.
+ **message text**: A plain-text description of the event that triggered the syslog message.

Let’s see an example of the syslog message:

```
39345: May 22 13:56:35.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
```

+ **seq no**: 39345
+ **Timestamp**: May 22 13:56:35.811
+ **FACILTY**: LINEPROTO
+ **SEVERITY level**: 5 (notification)
+ **MNEMONIC**: UPDOWN
+ **message text**: Line protocol on Interface Serial0/0/1, changed state to down

Note: Facility levels and syslog levels are different. The facility represents the machine process that created the syslog event. Therefore the Facility value is a way of determining which process of the machine created the message. For example, is the event created by the kernel, by the mail system, by security/authorization processes, etc.

Facility	Description
Auth	Authorization system
Cron	Cron/at facility
Daemon	System daemons
Kern	Kernel
local0 to local7	Local use
Lpr	Line printer system
Mail	Mail system
News	USENET news
sys9 to sys14	System use
Syslog	Syslog itself
User	User process
Uucp	Unix-to-Unix copy system

The default syslog facility setting is local7.

Syslog Configuration

The following example tells the device to store syslog messages to a server on 10.10.10.150 and limit the messages for levels 4 and higher (0 through 4):

```
Router(config)#logging 10.10.10.150
Router(config)#logging trap 4
```

Of course on the server 10.10.10.150 we have to use a syslog software to capture the syslog messages sent to this server.

Comments (2) Comments

1. Mateo
   January 18th, 2020

   Thank you! well illustrated.

2. Subhojit
   August 17th, 2021

   Every Awesome Cisco Engineer Will Need Ice Cream Daily

Add a Comment

Name

Submit Comment

Subscribe to comments feed
Simple Network Management Protocol SNMP Tutorial Gateway Load Balancing Protocol GLBP Tutorial

Premium Member Zone

Welcome Gurjeet singh!

- Welcome Premium Member
- CCNA – New Questions Part 5
- CCNA – New Questions Part 6
- CCNA – New Questions Part 7
- CCNA – New Questions Part 8
- CCNA – New Questions Part 9
- Composite Quizzes

- Logout

CCNA 200-301

- Basic Questions
- Topology Architecture Questions
- Cloud & Virtualization Questions
- CDP & LLDP Questions
- Switch Questions
- VLAN & Trunking Questions
- VLAN & Trunking Questions 2
- STP & VTP Questions
- EtherChannel Questions
- TCP & UDP Questions
- IP Address & Subnetting Questions
- IP Routing Questions
- IP Routing Questions 2
- OSPF Questions
- OSPF Questions 2
- EIGRP Questions
- NAT Questions
- NTP Questions
- Syslog Questions
- HSRP Questions
- Access-list Questions
- AAA Questions
- Security Questions
- Security Questions 2
- DAI Questions
- IPv6 Questions
- DNS Questions
- QoS Questions
- Port Security Questions
- Wireless Questions
- Wireless Questions 2
- SDN Questions
- DNA Center Questions
- Drag Drop Questions
- Drag Drop Questions 2
- Drag Drop Questions 3
- VPN Questions
- DHCP Questions
- Automation Questions
- Miscellaneous Questions
- CCNA FAQs & Tips
- Share your new CCNA Experience

CCNA Self-Study

- Practice CCNA GNS3 Labs
- CCNA Knowledge
- CCNA Lab Challenges
- Puppet Tutorial
- Chef Tutorial
- Ansible Tutorial
- JSON Tutorial
- Layer 2 Threats and Security Features
- AAA TACACS+ and RADIUS Tutorial

- STP Root Port Election Tutorial
- GRE Tunnel Tutorial
- Basic MPLS Tutorial
- TCP and UDP Tutorial
- Border Gateway Protocol BGP Tutorial
- Point to Point Protocol (PPP) Tutorial
- WAN Tutorial
- DHCP Tutorial
- Simple Network Management Protocol SNMP Tutorial
- Syslog Tutorial
- Gateway Load Balancing Protocol GLBP Tutorial
- EtherChannel Tutorial
- Hot Standby Router Protocol HSRP Tutorial
- InterVLAN Routing Tutorial
- Cisco Command Line Interface CLI
- Cisco Router Boot Sequence Tutorial
- OSI Model Tutorial
- Subnetting Tutorial – Subnetting Made Easy
- Frame Relay Tutorial
- Wireless Tutorial
- Virtual Local Area Network VLAN Tutorial
- VLAN Trunking Protocol VTP Tutorial
- IPv6 Tutorial
- Rapid Spanning Tree Protocol RSTP Tutorial
- Spanning Tree Protocol STP Tutorial
- Network Address Translation NAT Tutorial
- Access List Tutorial
- RIP Tutorial
- EIGRP Tutorial
- OSPF Tutorial

Network Resources

- Free Router Simulators
  - CCNA Website
  - ENCOR Website
  - ENSDWI Website
  - ENARSI Website
  - DevNet Website
  - CCIE R&S Website
  - Security Website
  - Wireless Website
  - Design Website
  - Data Center Website
  - Service Provider Website
  - Collaboration Website

Top