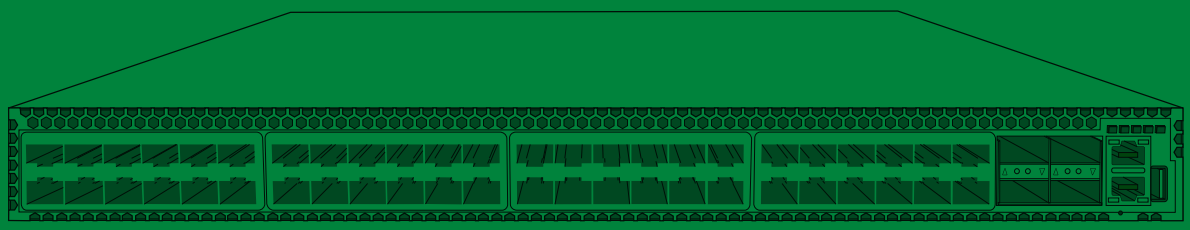
Securing Cumulus Linux

Security recommendations & best practices using Cumulus Linux



cumulus®

WHITE PAPER

Table of Contents

Introduction 1
Securely Configure and Operate a Cumulus Switch 2
- Securing the Administrative Interfaces 2
- Secure User Access Methods 5
- Setting up Accounts and Authentication 6
- Installing New Packages and Services 8
- Filtering and Protecting the Control Plane 9
- Secure Routing Methods 12

Monitoring the Switch 14
Installing Security Updates 16
Conclusion 17

Introduction

In order to protect the revenue and reputation of both a brand name and its customers, it is critical for any business to protect the reliability and integrity of their network and data. Deploying prudent security policies and practices can help prevent threats from entering and compromising your network, and thus protect your business from disruption or attack.

One of the key pieces to your security procedures is ensuring that your open source operating system, applications, and tools are properly configured and secured. Many networking products come with standard security features, but they lack the flexibility and accessibility to optimize your security features based on your organizational needs. In contrast, Cumulus Linux offers endless security options and resources.

As the leaders in Open Networking, Cumulus Networks offers unique insight into how to best protect your network. This white paper provides the security aspects of Cumulus Linux and recommends best practices for securely setting up, configuring, operating, and monitoring a data-center switch running Cumulus Linux.

Securely Configure and Operate a Cumulus Switch

Security is inherent in Cumulus Linux. Many security features are enabled by default, and Cumulus Networks provides others as recommendations and best practices. The first section of this white paper discusses the security aspects in the order that they are encountered as the switch is set up and configured. It includes the following topics:

- Securing the Administrative Interfaces
- System Imaging and Initial Configuration
- Secure User Access Methods
- Setting Up Accounts and Authentication
- Installing New Packages and Services
- Filtering and Protecting the Control Plane
- Secure Routing Methods

Securing the Administrative Interfaces

Securing the administrative interfaces is a best practice to prevent vulnerabilities during initial image load, to provide management access, and to maintain reachability to the switch during a failure scenario. As depicted in Figure 1, a typical data center switch contains two types of interfaces: switchport interfaces and administrative interfaces. The switchport interfaces (swp) are generally used for data and control plane traffic, while administrative interfaces are used to access and manage the switch.

Cumulus Networks recommends deploying a separate **out-of-band management network**. A separate out of band network provides separate management access and remote access to equipment during a primary network outage. It also provides security by separating management traffic from data traffic in a multi-tenant environment. The administrative interfaces (e.g. eth0) and any serial or console servers used to access the switch console port should be connected to the out-of-band management network.

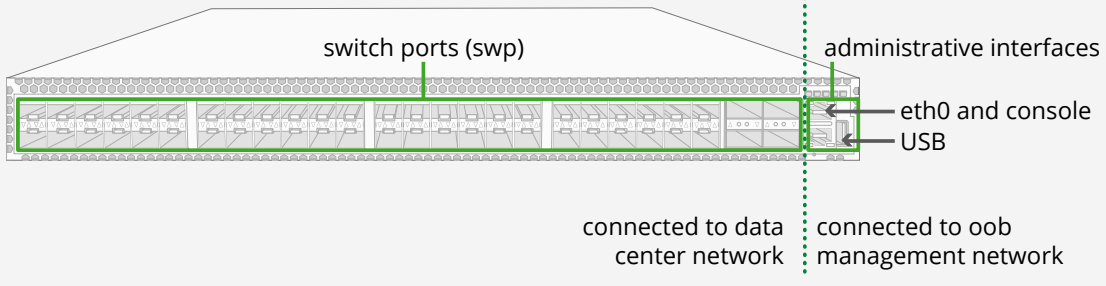


Figure 1 - Switch Port Types

As a security best practice, the **out-of-band management** network should always be isolated from the Internet to protect the out-of-band network and equipment from vulnerabilities. To do this, a firewall and a jump host are used between the out-of-band management network and the Internet. Figure 2 shows isolating the out-of-band management network from the Internet.

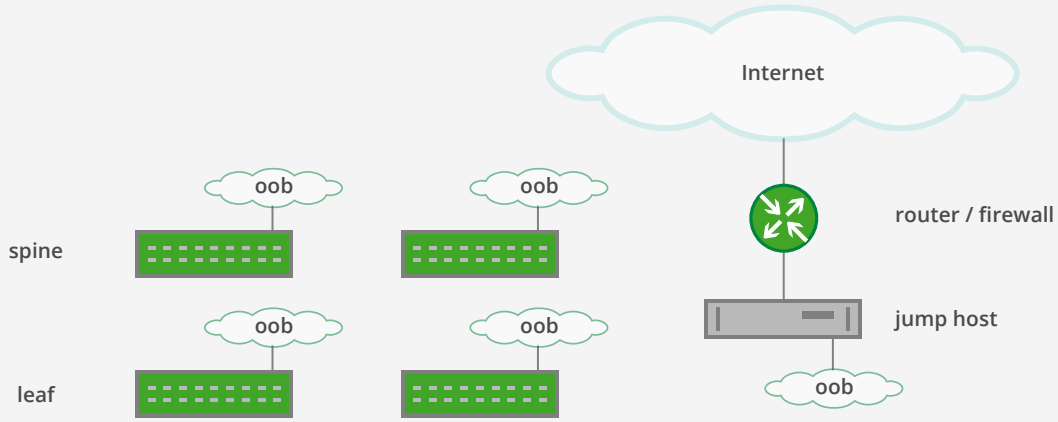


Figure 2 - Securing the Out-of-Band Management Network

The switches, any serial console servers, and the out-of-band management network, should always be stored in an area that is locked or secured in order to prevent unauthorized access.

To prevent packets traversing from the switchport interfaces to the out-of-band network, Cumulus Networks recommends the best practice of placing the switch's management interface(s) into the management **Virtual Routing and Forwarding** (VRF) instance, isolating it via layer 3.

System Imaging and Initial Configuration

If the switch did not come with Cumulus Linux pre-installed, the Open Network Install Environment (ONIE) is used for installing the Cumulus Linux operating system onto a bare-metal switch. Imaging of a bare-metal switch should occur via a secured out-of-band management network, using the switch's eth0. Procedures to install Cumulus Linux via ONIE are located in the **Installing a New Cumulus Linux Image** section of the User Guide.

After initial configuration, ZTP is disabled by default

After installation, initial switch provisioning should be done via **Zero Touch Provisioning** (ZTP) which should also occur over the out of band management network on eth0. ZTP can also be used to remove or modify the default users and/or passwords in Cumulus Linux and install ssh keys from a management server. More information utilizing ZTP can be found in the **Writing ZTP Scripts** part of the Zero Touch Provisioning User guide.

ZTP is disabled by default after the initial configuration process is complete.

The **Manually using the ZTP command** section within the Zero Touch Provisioning user guide describes more information on verifying and manually disabling ZTP, if necessary.

Secure User Access Methods

Cumulus Linux provides secure access to the switch via the industry-standard OpenSSH package. This provides customers with the most widely-vetted secure shell tool and allows any related Linux security updates to be immediately available in Cumulus Linux.

SSHv2 provides secure authentication and encryption, as well as scp and sftp applications, which can be used for securely transferring files. Telnet, ftp, tftp, and other less secure access methods are not enabled by default. Cumulus Networks recommends keeping less secure methods disabled.

Cumulus Linux uses the industry-standard OpenSSH application

Timing out idle SSHv2 sessions is a best practice to help prevent unauthorized access. For example, The following command times out the SSH session to 300 seconds:

```
cumulus@switch:~$ echo TMOUT=300 |sudo tee /etc/profile.d/session_timeout.sh
```

The timeout can be set for the amount appropriate for your business by changing the TMOUT value. The change will take effect upon next login to the switch.

When necessary, the console port can also be used to access the switch. By default, the switch console port is set to a 115200:8:N.

Setting up Accounts and Authentication

Cumulus Linux 3.x and newer releases ship with direct log into the root account disabled by default. Initially authenticate on the switch using the default username/password "*cumulus/CumulusLinux!*". **The password should be changed** as soon as possible, typically via the Zero Touch Provisioning process or via automation tools. If required, direct access to the root account can be enabled by generating a SSH key (see below) or setting a password. Procedures on how to enable the root account can be found in the **User Accounts** section of the Cumulus Linux User Guide.

Cumulus Networks recommends following Linux system administration best practices by creating individual accounts with sudo authentication to access privileged commands. Creating individual accounts helps track operator commands. The cumulus user that comes pre-defined after an image installation is a member of the sudo group; that user can be used to create appropriate users. To set this up, use the cumulus account with sudo privileges to access the visudo application. Visudo is used to configure the /etc/sudoers file to enable sudo permissions on any accounts. More information on adding permissions for specific users can be found in the **Using Sudo to Delegate Privileges** section of the User Guide.

Some organizations require use of a login banner which can be configured as a message of the day (motd). To configure a motd, edit the /etc/motd file with the appropriate information.

Cumulus Linux supports several authentication mechanisms

Cumulus Linux supports the following secure authentication mechanisms:

- **Public key authentication**
- **Local password and shadow files**
- **TACACS+ authentication**
- **Lightweight Directory Access Protocol (LDAP) authentication**

Cumulus Networks recommends using public key authentication as a best practice to authenticate users, as it prevents password/access information from traversing the network, and does not require user-created passwords. This process generally consists of generating a key set on the management station and copying the public key to the remote switch for authentication. More information on deploying this feature can be found in the **SSH For Remote Access** area of the User Guide.

If local passwords, TACACS+, or LDAP are required, Cumulus Linux authenticates using the Linux Pluggable Authentication Modules (PAM). PAM allows an additional layer of abstraction as different applications communicate an authentication request to PAM, and PAM will perform the authentication and return the response. This method allows a one-stop shop authentication mechanism for a variety of applications on the switch.

Strong password criteria should be defined by your organization's security policy. If local passwords are used, the obscure option is enabled by default which requires a password of at least 6 characters in length, requires complex passwords, and does not allow re-use or similarity of the old password for all non-root user accounts. See the section on obscure passwords in the pam_unix manual page on Cumulus Linux for more information on default password strengths. Root account does not require password complexity.

If desired, PAM can be used to increase the minimum length of the local password. To increase the minimum password length, add the keyword "minlen" to the last line of the /usr/share/pam-configs/unix file . Set the value to the minimum length desired. For example, the below line will change the minimum length of the password to 10 characters:

```
Password-Initial: [success=end default=ignore] pam _ unix.so obscure sha512 minlen=10
```

By default, passwords are required to be strong, however, if more specific password strengths are required to be enforced, packages such as the libpam_pwquality and pam_cracklib are available on the debian repository and can be used with Cumulus Linux.

Forgotten passwords can be recovered via the **boot recovery mode**.

For more information, refer to the **User Accounts** section of the Cumulus Linux User Guide.

Installing New Packages and Services

To limit vulnerability, external packages should be tested along with Cumulus Linux on a dedicated lab switch . Install new packages and updates using the "apt-get update" with the "apt-get install" or "apt-get upgrade" command. These commands will upgrade all packages.

If the package is a Cumulus package, Apt-get to a Cumulus repository can use https for secure transfer. To use https, change the /etc/apt/sources.list file from "http" to "https" to the repository if https is required. Also, all Cumulus Linux packages are GNU Privacy Guard (GPG) signed.

All Cumulus Linux packages in the Cumulus repository are GPG signed

When installing or enabling any new service or package, Cumulus recommends reviewing the network ports that are opened, and the accounts and programs that may be created during the installation process. To check the open ports, use the command:

```
cumulus@switch:~$sudo netstat -nlp -inet -inet6
```

More information about identifying the listening ports can be found in the **Identifying Active Listener Ports for IPv4 and IPv6** section of the documentation.

Cumulus Networks recommends the best practice of only opening the necessary ports, and leaving all others closed. By default, Cumulus Linux opens ports such as ssh, dhclient and ntp for both IPv4 and IPv6 upon bootup of the switch. If IPv6 or BGP unnumbered is not implemented, Cumulus Networks recommends disabling all IPv6 ports. For more detailed information on the Cumulus Linux default opened ports, refer to the **default open ports article**.

A port can be closed by disabling the service associated with the port. In Cumulus Linux 3.0 and above, stop or disable a service by using the following command:

```
cumulus@switch:~$systemctl [stop|disable] SERVICENAME.service
```

Refer to the **Managing Application Daemons** section of the user documentation for more information on stopping or disabling services.

Filtering and Protecting the Control Plane

It is crucial to also protect a switch's control plane to ensure the proper control plane applications have access to the switch's CPU. Failure to do so could increase vulnerabilities to a Denial of Service (DOS) attack. Cumulus provides control plane protection by default, as well as offers an additional method. This section covers:

- **Linux netfilter tools: iptables, ip6tables, and ebtables**
- **Hardware-based DDOS protection**

Linux Netfilter Tools: iptables, ip6tables, and ebtables

Iptables, ip6tables, and ebtables protect the switch's management, control, and data planes. These applications reside in the user space, and provide access to the **netfilter** framework in the kernel, allowing for the configuration of Access Control Lists (ACLs). ACLs control the type and quantity of traffic allowed into the management, control and/or data plane of the switch. IPtables, IP6tables, and ebtables control IPv4, IPv6, and layer 2 traffic, respectively.

Figure 3 depicts the default control plane prioritization and policing done in Cumulus Linux. The default filters are written directly into the hardware on the switchport interfaces, whether the protocol is active or not, and perform at line rate; no performance degradation occurs.

Traffic is policed to protect CPU resources, and prioritized to ensure mission critical traffic has first access to CPU resources during times of congestion. Coming from the switchport interfaces, OSPF, BGP, MLAG, BFD, BDPU and LACP are placed in class 7, a low latency queue, and policed to the CPU. Other control plane and management plane traffic, (e.g. ARP, LLDP, ICMP, IGMP, MLD, etc.) , are placed in remaining queues which are scheduled via weighted round robin and also policed towards the CPU. A general "catch all" policer is also enabled by default to catch other types of control/ management plane traffic headed towards the CPU and placed into class 0.

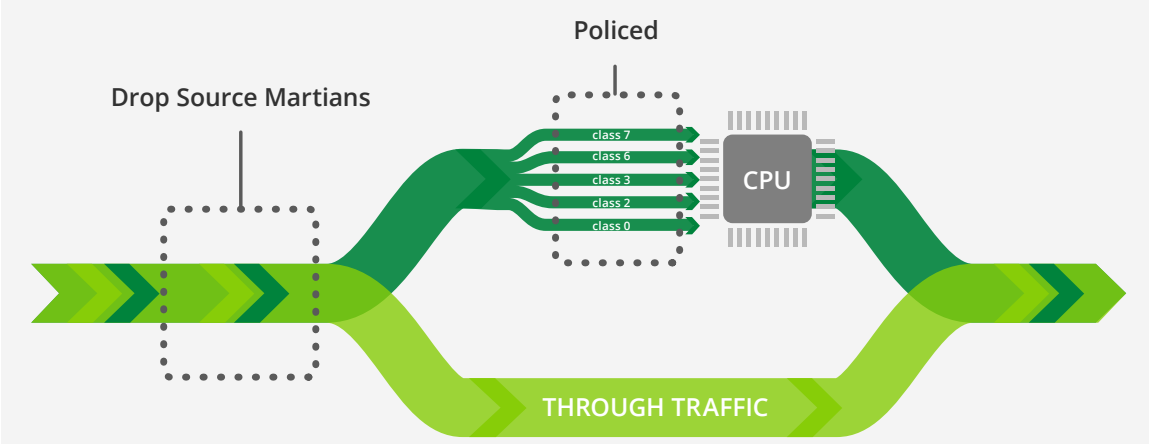


Figure 3 - Default Policing and Filtering in Cumulus Linux

Further, source address martians with any destination address are dropped.

More specifically, Cumulus Linux prioritizes and meters the following types of traffic destined to the switch CPU adding the catch all policer at the end:

- **IPv4 Protocols: BFD, BGP, BOOTP, ICMP, IGMP, LNV, MLAG, OSPF, IPROUTER*, Local****
- **IPv6 Protocols: BFD, BGP, DHCPv6, ICMPv6, MLD, OSPF, Local, IPROUTER*, Local****
- **Mac Layer Protocols: ARP, BDPU, CDP, LACP, LLDP, PDVT, Local****

Note: **IPROUTER is an unresolved address. This type of packet is sent to the CPU in order to ARP for the destination or any other packet that the hardware does not have enough information to forward.*

*** Local is all traffic with a MAC or IP address associated with an interface on the local switch.*

More detailed information on the exact policers and filters enabled in Cumulus Linux can be found in the **Default Filters Table**.

Cumulus Linux enables filters and policing to protect the management and control planes by default

---

The configuration files for the filters can be found in "/etc/cumulus/acl/policy.d" directory. The policy.d directory contains two files by default, 00control_plane.rules and 99control_plane_catch_all.rules. The policy files with a ".rules" suffix are executed in the order returned by "ls" of this directory.

It is important not to change or mis-configure the default filters unless it is imperative for business reasons and you are very familiar with the related protocols and iptables, ip6tables and/or ebtables applications.

Cumulus Linux also supports configuring additional filtering, policing, and re-marking packets on the data, control and management planes in hardware without any performance degradation. Cumulus Linux goes further than Debian Linux by supporting additional targets such as SPAN, police and tricolor police, which are covered in the **Supported Rule Types Section** of the **Netfilter - ACL documentation**.

To add additional filters in Cumulus Linux, create the new filter files with a .rules suffix in the /etc/cumulus/acl/policy.d" directory. Cumulus Linux uses the utility "cl-acltool" to check and write the filters from the files into hardware. Cl-acltool will alert you if a filter is not configured correctly, exceeds the hardware resources, or is unable to write into hardware for another reason. More information on cl-acltool can be found in the **Installing and Managing ACL Rules** section of the Netfilter-ACL documentation.

The filters enabled in Cumulus Linux, including default filters, can be found by issuing the following command at the bash prompt:

```
cumulus@switch:~$sudo cl-acltool -L all
```

Additional information on configuring control plane, management plane, and data plane rules can be found in the Netfilter-ACL documentation.

Hardware-Based DDOS Protection

Note: *Hardware-Based DDOS Protection is applicable only to switches with a Broadcom Trident, Trident II, or Tomahawk ASIC.*

The DDOS protection mechanism protects data, control, and management plane traffic in the switch. It drops any packets that match one or more of the following criteria while incurring no performance impact:

- Source IP address matches the destination address for IPv4 and IPv6 packets
- Source MAC address matches the destination MAC address
- Unfragmented or first fragment SYN packets with a source port of 0-1023
- TCP packets with control flags =0 and seq number == 0
- TCP packets with FIN, URG, and PSH bits set and seq number == 0
- TCP packets with both SYN and FIN bits set
- TCP source PORT matches the destination PORT
- UDP source PORT matches the destination PORT
- First TCP fragment with partial TCP header
- TCP header has fragment offset value of 1
- ICMPv6 ping packets payload larger than programmed value of ICMP max size
- ICMPv4 ping packets payload larger than programmed value of ICMP max size
- Fragmented ICMP packet
- IPv6 fragment lower than programmed minimum IPv6 packet size

Cumulus Networks recommends enabling this feature when deploying a switch with the above mentioned ASICs, as hardware-based DDOS protection is disabled by default. Although Cumulus recommends enabling all of the above criteria, they can be individually enabled if desired. More information on deploying this feature can be found in the Configuring Hardware-Based DDOS Protection section of the Cumulus Linux User Guide.

Secure Routing Methods

The last security item in configuration is to ensure you are using secure routing methods. Protecting the routing plane helps protect the integrity of the routing table. Without routing protection, packets could be sent to an unknown destination, an unknown neighbor could send a large number of routes utilizing all the switch's memory, or a router could become neighbors with an unknown router.

Therefore, if a layer 3 data center fabric is deployed, Cumulus Networks recommends use of the following methods to protect the integrity of the switch and the routing table from neighbors located across the switchport interfaces as a best practice.

Border Gateway Protocol (BGP)

- BGP unnumbered: Use of BGP unnumbered interfaces removes IPv4 and global IPv6 addresses from router interfaces, thus reducing the attack vector. If using BGP unnumbered is not possible, be sure to block internal link addresses from being advertised.
- MD5 authentication: Ensures the integrity of the BGP neighbors.
- Maximum prefixes: Allows the router to limit the number of prefixes accepted from a neighbor. Configuring this feature prevents memory overload.
- TTL security: Can help prevent the establishment of unknown neighbors from spoofing a known neighbors address with iBGP. Configure the neighbor to be the correct number of hops away.
- BFD maximum hop count: To help prevent spoofing, Cumulus Networks recommends configuring a maximum hop count for each BFD peer when using BFD multihop.
- Route/AS-path filtering: For eBGP, only advertise/accept routes and from ASes that are known and needed. The routes can be controlled by use of filter lists and/or prefix lists and route-maps.
- Neighbor verification with Prescriptive Topology Manager (PTM): For fabrics using BGP unnumbered links, Cumulus Networks recommends verifying the correct neighbor using PTM.

Cumulus Linux provides several methods to secure layer 3

Open Shortest Path First (OSPF)

- MD5 authentication: Ensures integrity of the OSPF neighbors.
- BFD maximum hop count: To help prevent spoofing, Cumulus Networks recommends configuring a maximum hop count for each BFD peer when using BFD multihop.
- Neighbor verification with the Prescriptive Topology Manager (PTM): For fabrics using OSPF unnumbered links, Cumulus Networks recommends verifying the correct neighbor using PTM.

Monitoring the Switch

Cumulus Networks recommends monitoring your switches regularly for security issues, configuration changes, and to investigate any unusual or suspicious messages. This section of the whitepaper details various techniques for effective monitoring.

All logging in Cumulus Linux is done via the rsyslog mechanism with high precision timestamp logging on by default. Logins and attempted logins are logged by default in /var/log/syslog. The file should be regularly reviewed on a regular basis, and issues should be promptly investigated.

For example, the following output shows an attempt to log in with an invalid account:

```
2016-07-12T19:40:06.083690+00:00 sw01 sshd[1234]: Invalid user admin from 192.168.2.201
2016-07-12T19:40:06.084711+00:00 sw01 sshd[1234]: input_userauth_request: invalid user admin [preauth]
2016-07-12T19:40:06.085598+00:00 sw01 sshd[1234]: pam_unix(sshd:auth): check pass; user unknown
2016-07-12T19:40:06.085706+00:00 sw01 sshd[1234]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.2.201
2016-07-12T19:40:07.952824+00:00 sw01 sshd[1234]: Failed password for invalid user admin from
192.168.2.201 port 55572 ssh2
```

When numerous log messages similar to this occur in a short period of time, it is typically a sign of an attempt to break into the switch. Multiple IP addresses and accounts are often attempted as well.

Since Cumulus Linux is based on Debian Linux, utilities such as denyhosts are available on the Debian repository to help prevent SSH attacks. Along with denyhosts, Cumulus Networks recommends setting up /etc/hosts. allow to guarantee access to wanted hosts.

Cumulus recommends logging to a central server across the out-of-band management network since secure protocols are not used to write the log files. Configure rsyslog to write the log files to the central server by creating a configuration file in the "/etc/rsyslog" directory and restarting ryslog. More information how to set this up can be found in the **Sending Log Files to a Syslog server** section of the **Monitoring and Troubleshooting User Guide**.

Logs can be examined with programs such as *logwatch,* while products such as Nagios are also useful for monitoring. Additionally, devops tools such as Ansible Tower, Puppet and Chef can watch configurations and identify if configuration changes have been made. For example, Puppet has an agent running on the switch that can notify you if a configuration change is made, and Ansible Tower constantly monitors for configuration changes.

Monitoring best practices section of the user guide gives additional information.

SNMP can also be used to manage the switch. Cumulus does not enable SNMP by default for security reasons. If SNMP is required, Cumulus recommends SNMPv3, as it can enable secure authentication and encryption. Using SNMPv3, an even more secure method is installing and using the libsnmp-dev package, which prevents the use of cleartext passwords. Configure SNMPv3 by editing the /etc/snmp/snmpd.conf file and restart the snmpd daemon. More information on configuring and enabling SNMPv3 can be found in the **SNMP chapter** of the User Guide. To configure SNMP to run in a management VRF, refer to the **Management VRF chapter**.

To increase security by default, Cumulus Linux versions 3.x and later only listen to SNMP traffic coming from the switch itself - accessing SNMP information from outside the box is disabled. Cumulus recommends performing the security configuration (e.g. users, etc) first, and then configuring to listen on a specific interface ip address, and then starting snmpd. Refer to the **Configuring Ports for SNMP to Listen for Requests** section of the User Guide for additional information. The configuration file is located at /etc/snmp/snmpd.conf.

Installing Security Updates

Cumulus Linux is based on the Debian Linux distribution. Since Debian is an open source operating system, a wide variety of developers and engineers in the industry have access to writing and reviewing the source code as well as testing the operating system. With such a wide community developing, testing, and supporting Debian, it makes it nearly impossible to code a backdoor as it will be caught by the industry. If a security threat is identified, it is fixed swiftly and an update that includes only a fix to that vulnerability is provided.

The final section of this white paper discusses how to ensure your network remains secure by being vigilant with security updates. Cumulus Networks believes in the Linux model of security through transparency. Security advisories are constantly monitored, and Cumulus will notify users, and provide updated packages, when major vulnerabilities affect Cumulus Linux. This turnaround time is often much faster than traditional vendors. Within a reasonable time frame, Cumulus Networks will address security problems in accordance with the **Debian security policies** that are in place.

Cumulus believes in the Linux model of Security through Transparency

---

Every Cumulus Linux release will include all applicable security patches available prior to the build date. Any new vulnerabilities listed by Debian after the release will be evaluated and may be made available as a package update through the **Cumulus Networks repository**. The **Security Responses and Updates** article provides more information on the security update process.

Cumulus Networks recommends subscribing to the **cumulus-security-announce** mailing list to receive notifications of any new security vulnerabilities and act upon the notifications.

To limit vulnerability, new security updates should be tested on a dedicated lab switch and installed promptly thereafter. Since the security updates are a Cumulus package available on the Cumulus repository, more information is described in the **"Installing New Packages and Services"** section of this paper.

Conclusion

Cumulus Linux enables many security features by default, including disabling insecure access, adding control plane policing, turning off SNMP, and requiring secure passwords if used. Combined with the additional elective features and best practices, these configurations can ensure a very secure network with Cumulus Linux and allow you to deploy a secure data center.

By monitoring the Debian community recommendations, Cumulus Networks ensures any unforeseen risks are dealt with as efficiently as possible. Meanwhile, the Debian community is active in pursuing, reviewing, and providing transparent security announcements.

Cumulus Linux is deployed at scale in production in some of the largest data centers in the world. By running Cumulus Linux and abiding by these best practices, you will be deploying a well prepared network to mitigate threats against your business.

About Cumulus Networks®

Cumulus Networks demystifies the complexity of networking and enables better, faster, easier networks to support your business. Our network operating system, Cumulus® Linux®, allows you to build and operate your network with the mindset of web-scale pioneers like Google and Amazon, radically reducing the costs and complexities of modern data center networks. More than 400 organizations, including some of the largest-scale data center operations in the world, run Cumulus Linux. Cumulus Networks has received venture funding from Andreessen Horowitz, Battery Ventures, Sequoia Capital, Peter Wagner and four of the original VMware founders.

For more information visit **cumulusnetworks.com** or follow **@cumulusnetworks**.

11072016