Pica8 Evaluation Guide | June 2022

Using AmpCon to Manage PicOS-V Switches - Evaluation Guide

Contents

VIDEO LINKS

PLAYLIST ON YOUTUBE ▸

Import PicOS-V Switches

Automate Configuration of MLAG Feature in PicOS-V Switches

Use Ansible Playbooks to Verify L2 or L3 Functionality

Day-to-day Policy Enforcement

Configuration Management

Audit and Operation Logs

Pica8 Solution and AmpCon

Pica8's solution consists of two components. First is the AmpCon network controller, the automation command center for your enterprise network. Second is the PicOS switch software, which turns your bare metal into an enterprise switch, automated by AmpCon.

AmpCon is an application developed by Pica8 to automate the deployment, provisioning, and lifecycle management of switches, both physical and virtual. AmpCon can be installed on a physical server or a virtual machine (VM), although the preferred and most straightforward approach is to install the OVA provided by Pica8.

Overview of Using AmpCon to Automate PicOS-V Switches

PicOS-V is a free **Virtual Machine (VM)** from Pica8 that can help you get familiar with PicOS Software Switches. PicOS-V is used for validating the configuration of PicOS and testing L2 and L3 features at your own pace, with no costs associated. PicOS-V runs on VMware, GNS3 and VirtualBox hypervisors, without the need for a bare-metal switch or specialized hardware.

AmpCon universally manages and automates PicOS Software switches, both physical and virtual alike. All automation use cases are applicable to both PicOS and PicOS-V switches, except Zero Touch Provisioning (ZTP). AmpCon does not currently support ZTP of a PicOS-V (virtual) switch.

This document explains how to test the following major automation use cases of PicOS-V switches:

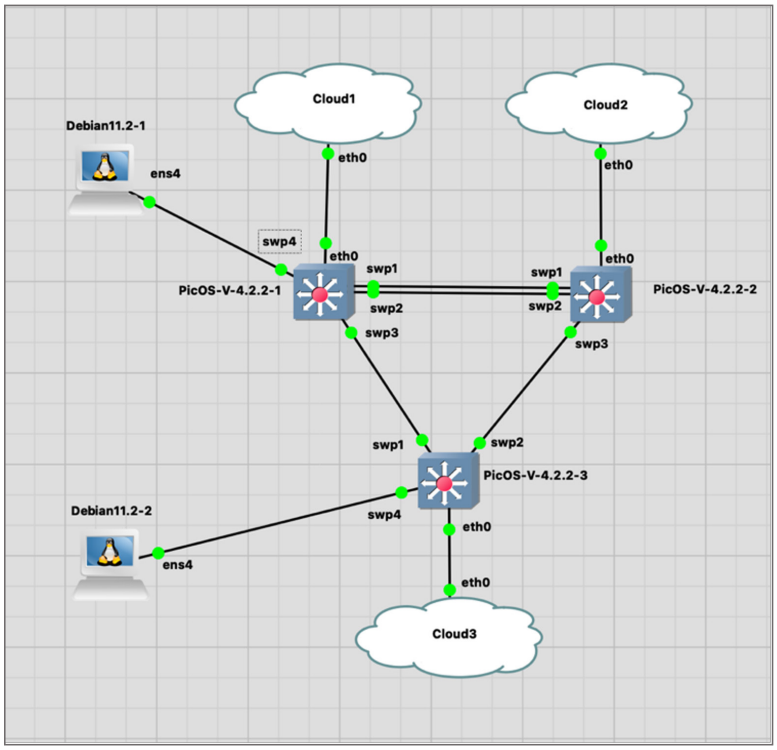
1. Import PicOS-V switches
2. Automate configuration of MLAG feature in PicOS-V switches
3. Use Ansible Playbooks to verify L2 or L3 functionality
4. Day-to-day Policy Enforcement
5. Configuration management
6. Audit and operation logs

Setup PicOS-V Testbed

Before you get started with AmpCon, setup a PicOS-V testbed following the steps given below:.

1. **Download PicOS-V:** Download PicOS-V using following link: https://www.pica8.com/picos-v/
2. **Setup PicOS-V** testbed in GNS3 environment: Download the following document: https://www.pica8.com/wp-content/uploads/Pica8-Pic0S-V-UserGuide.pdf and follow ***PicOS-V Installation, Setup and Testing*** in the ***GNS3*** section.

The following PicOS-V testbed topology was created in a GNS3 environment for testing and for the purpose of this use case. For more details on the GNS3 test environment setup, please refer to above PicOS-V User Guide.



Getting Started with AmpCon

Following are steps to install AmpCon:

1. **Download the AmpCon image:** https://www.pica8.com/ampcon-network-controller/
2. **Review AmpCon VM requirements:** For AmpCon Virtual Machine (VM) requirements please refer to AmpCon VM Requirements document. You do not need License for using PicOS-V.
3. **Install AmpCon:** Follow the AmpCon installation Guide document to install the AmpCon server in your Datacenter or Campus. AmpCon installation Guide document to this URL

AmpCon Automation Major Use Cases and Benefits

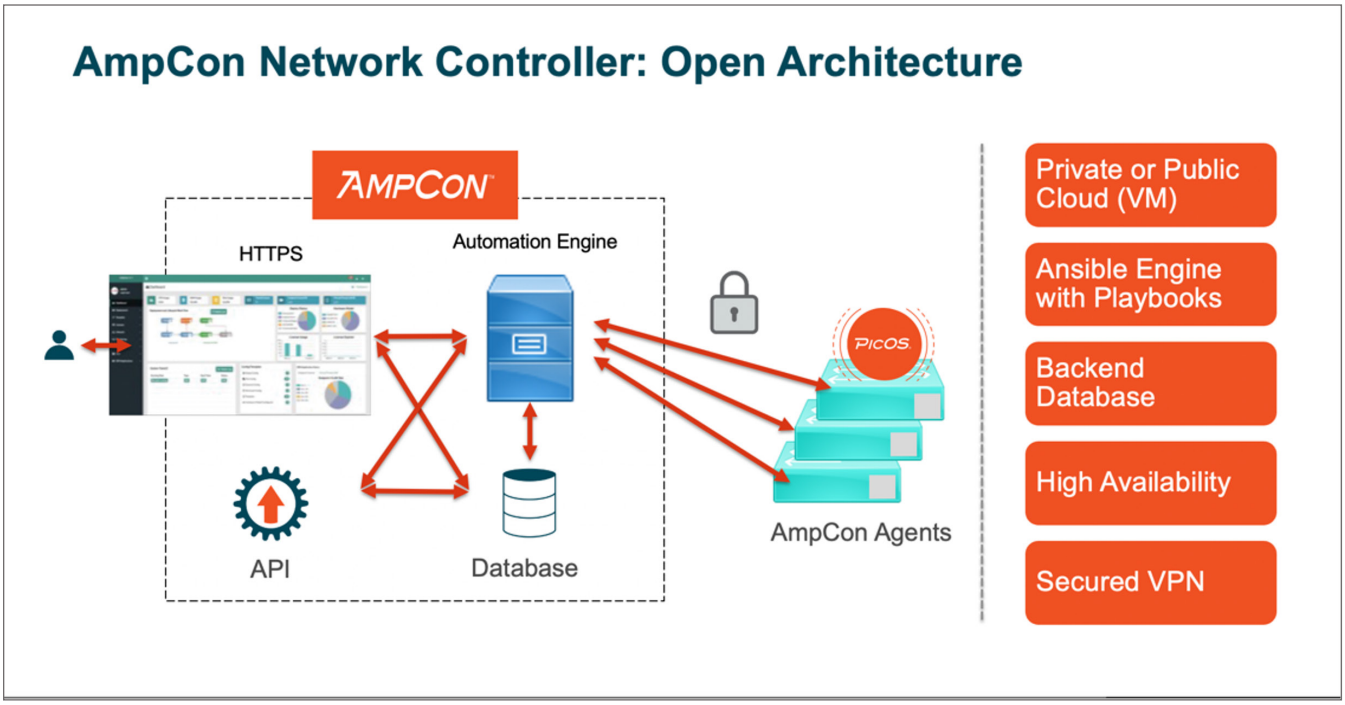
Following are AmpCon Automation major use cases:

1. **Switch Deployment:** Automate deployment of bare-metal switches to reduce cost and complexity.
2. **Security and Network Compliance:** Enforce day-to-day security and network compliance policies on groups of switches with ease.
3. **Scheduled backups and upgrades:** Leave long weeknight/weekend switch upgrades behind with automated upgrades and backups
4. **Customize your automation:** Use Ansible Playbooks to create custom workflows

AmpCon can be used to automate following business workflows to reduce operating expenses.

- ✔ Config Updates
- ✔ Config Backup/Rollback
- ✔ Compliance Management
- ✔ Scheduled Software Upgrades
- ✔ Switch Visibility (port stats, health check)
- ✔ Custom (user defined) Workflows
- ✔ RMA Replacements
- ✔ License Updates

AmpCon Architecture



AmpCon consists of the following components:

• Front-end web server

• Jinja2 point-and-click network template automation and creation

• Ansible playbook engine, a de facto automation standard, and

• Maria DB database

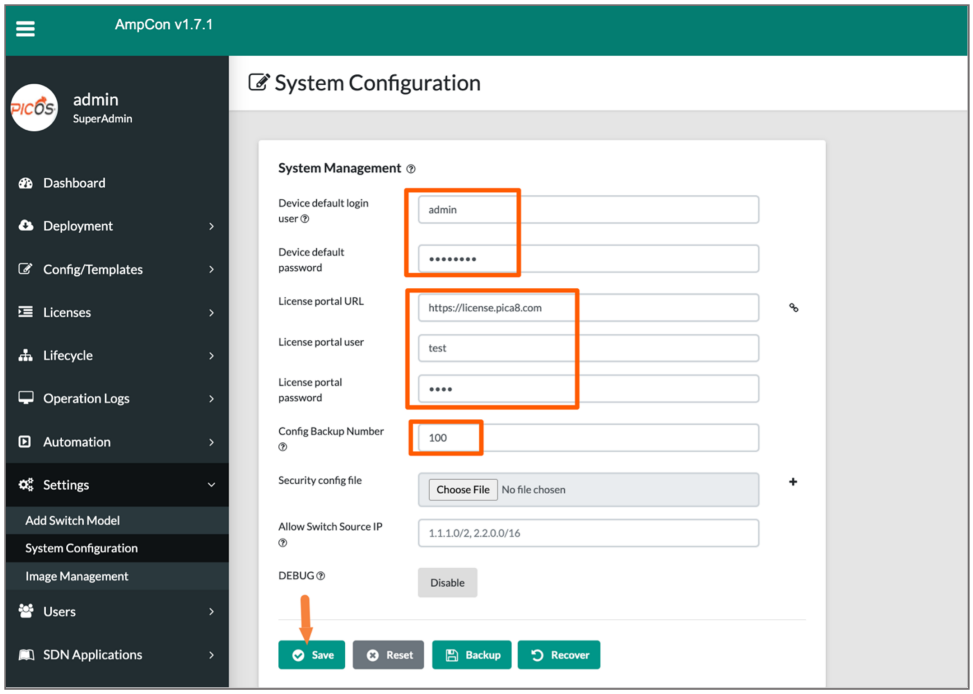
AmpCon communicates with AmpCon Automation Agent software running in the switches located in a remote campus or remote datacenter using a VPN. All communications between the AmpCon server and AmpCon Agent running in the switch are encrypted. The AmpCon Agent is only functional during Zero Touch Provisioning and Import process of a switch.

AmpCon provides a simple UI driven application to automate initial configuration, provisioning and deployment, as well as ongoing lifecycle management functions. It has significant impact on reducing operating expenses.

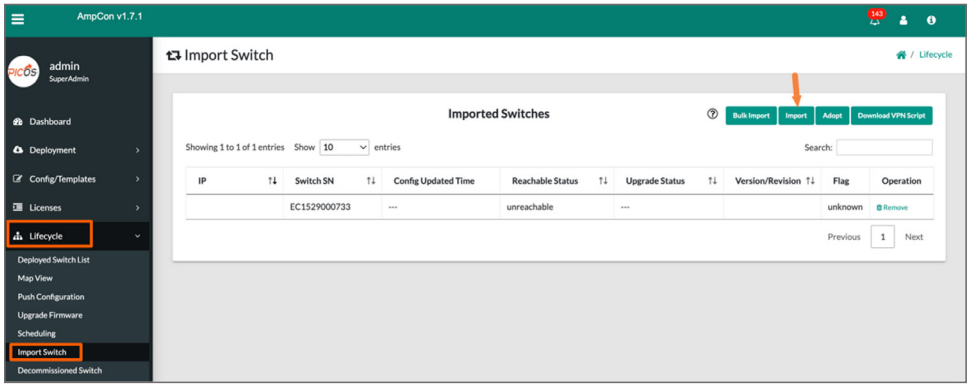
Import PicOS-V Switches VIDEO GUIDE

Import PicOS-V switch using following steps:

1. **Setup System Configuration:** Log into AmpCon UI using default credentials admin/admin. Select Settings > System Configuration as shown below:
   a. Enter the login credentials for PicOS-V switch. Enter admin as the username and enter password you have setup for the PicOS-V switch (default is “pica8”).
   b. Enter License Portal related information: URL is https://license.pica8.com, username is test and password is test. Please note these credentials will not be used since we will not be testing any License Portal related use case.
   c. Enter 100 for Config Backup number.
   d. Click ***Save***



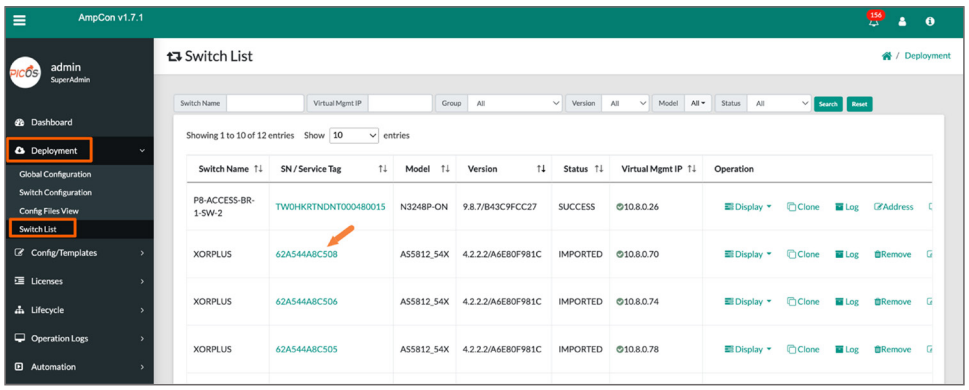
2. **Import a PicOS-V switch:** Select ***Lifecycle > Import Switch*** and click ***Import*** as shown below. Enter the management IP of the first PicoS-V switch and click ***Save***. It will take few minutes to import the switch.



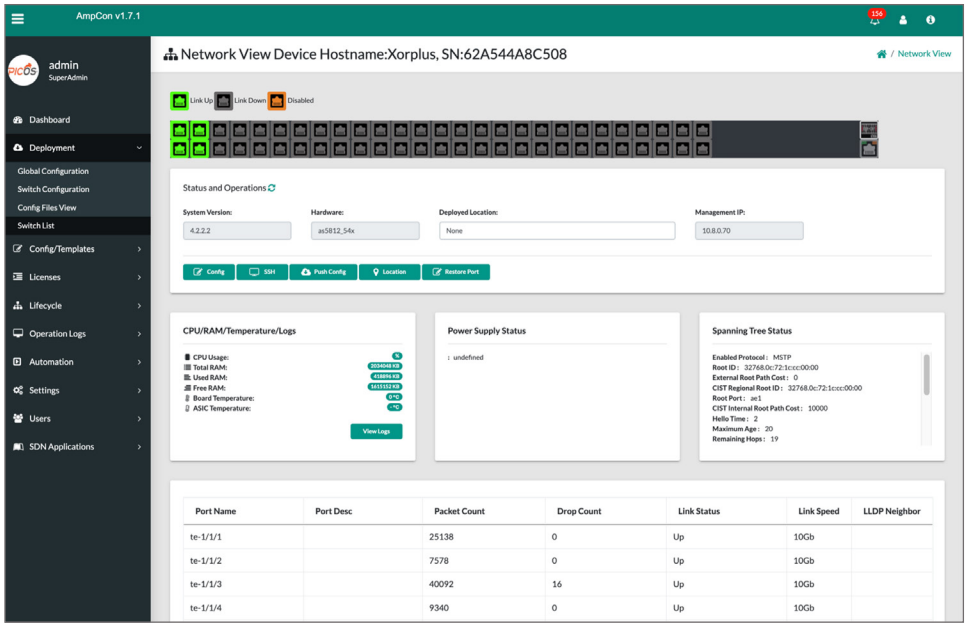
Verify whether the PicOS-V switch is successfully imported by selecting ***Deployment > Switch List*** menu. You will see the PicOS-V switch's Serial Number with Imported status.

3. Similarly import other two PicOS-V switches.

To look at the high-level health view of a specific imported switch, select Deployment > Switch List and click on the Serial Number of one of the switches we imported in this section as shown below.



You will see details on ports active, software version, hardware model, resource utilization info on CPU, and RAM. It also shows temperature, power status and snapshot of traffic status on active ports at the time of UI invocation. All the above are high-level health details of the switch. It does not replace Network Management.



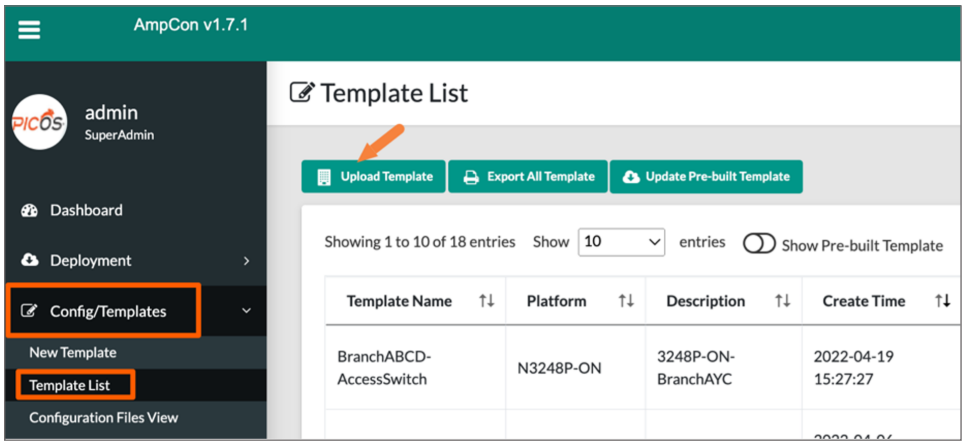
Automate Configuration of MLAG Feature in PicOS-V Switches VIDEO GUIDE

We will use AmpCon to automate configuration of MLAG feature in a spine and leaf cluster of PicOS-V switches.

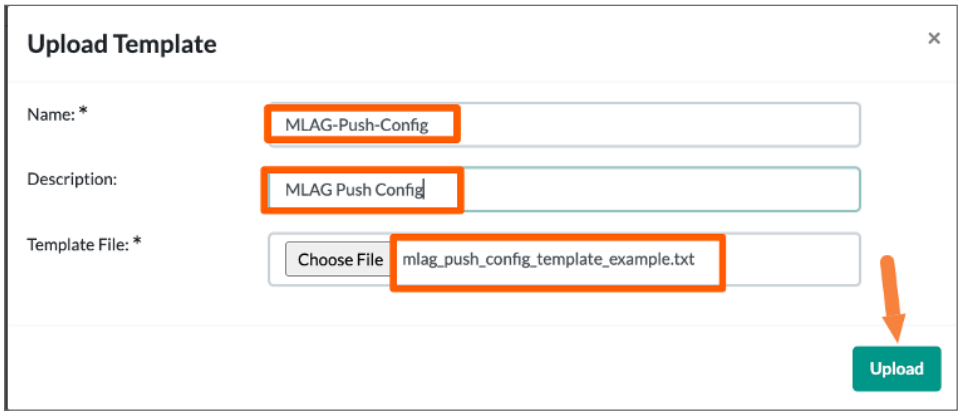
Automate Configuration of MLAG Feature in Spine Switches

We will use a Jinja2 Template to generate MLAG configuration for both spine switches. Jinja2 is one of the most used templating engines for Python. It is easy to use Jinja2 templates for config generation for a group of switches. We will examine the Jinja2 template mechanism more closely later in this section.
Automate configuring the first PicOS-V Spine switch with MLAG configuration by using the following steps:

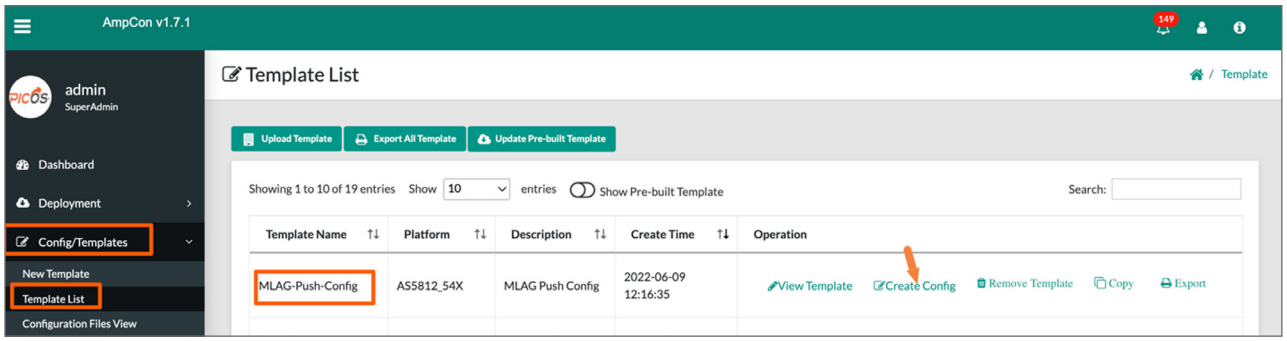
1. **Upload Template for MLAG configuration:** Select ***Config Templates > Template List*** and click ***Upload Template*** as shown below:



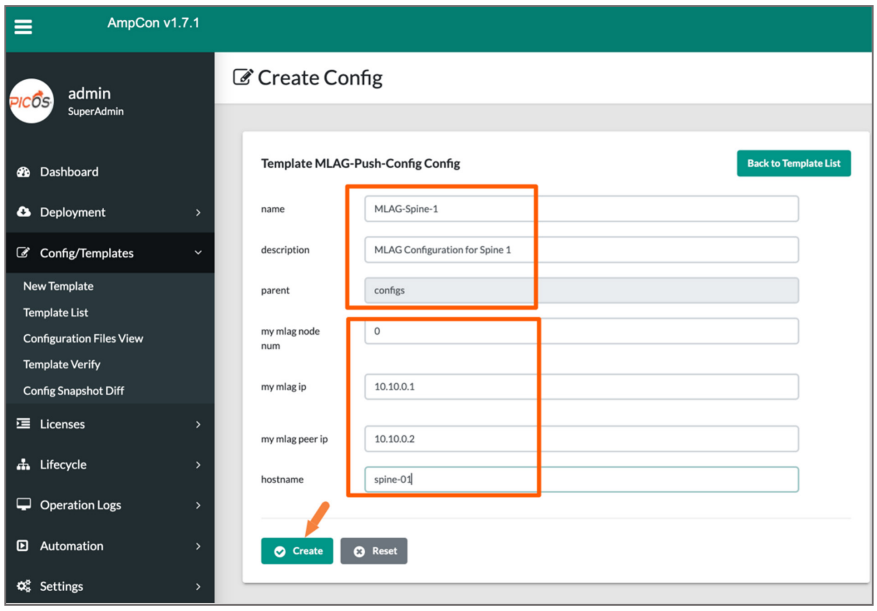
Enter the ***Name***, and ***Description*** as shown below. Select ***MLAG-Push-Config.txt*** Template file given in the Appendix A and click ***Upload*** as shown below.



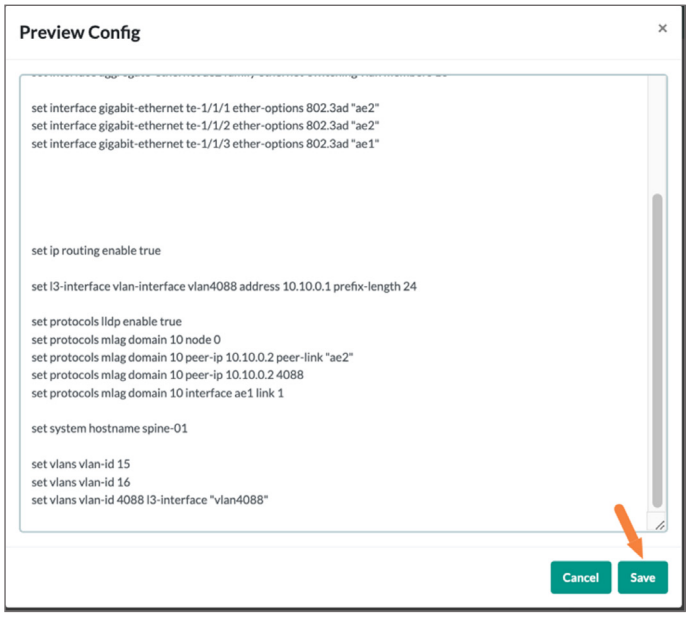
2. Select ***Config Templates > Template List > MLAG-Push-Config*** and click ***Create Config*** as shown below:



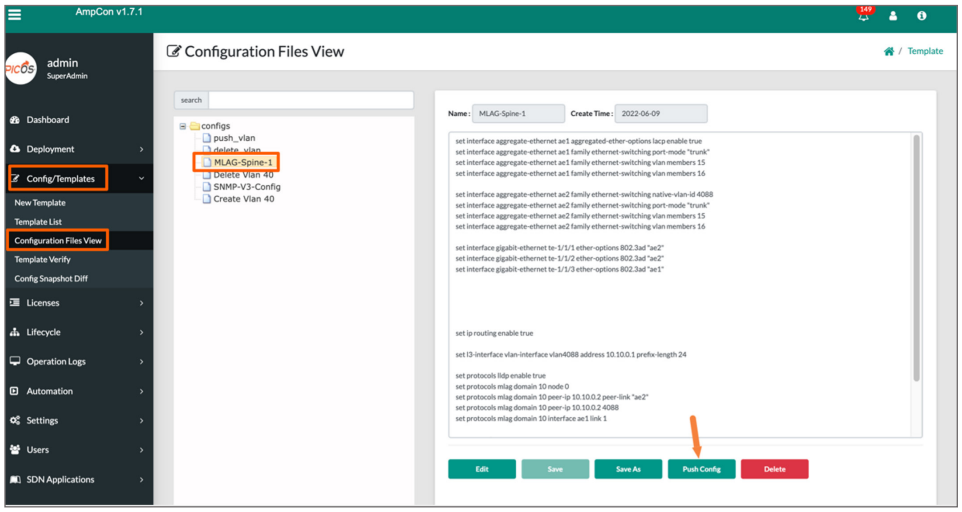
Enter the ***Name***, ***Description, parent, my mlag node num, my mlag ip, my mlag peer ip and hostname*** fields as shown below and click ***Create***:



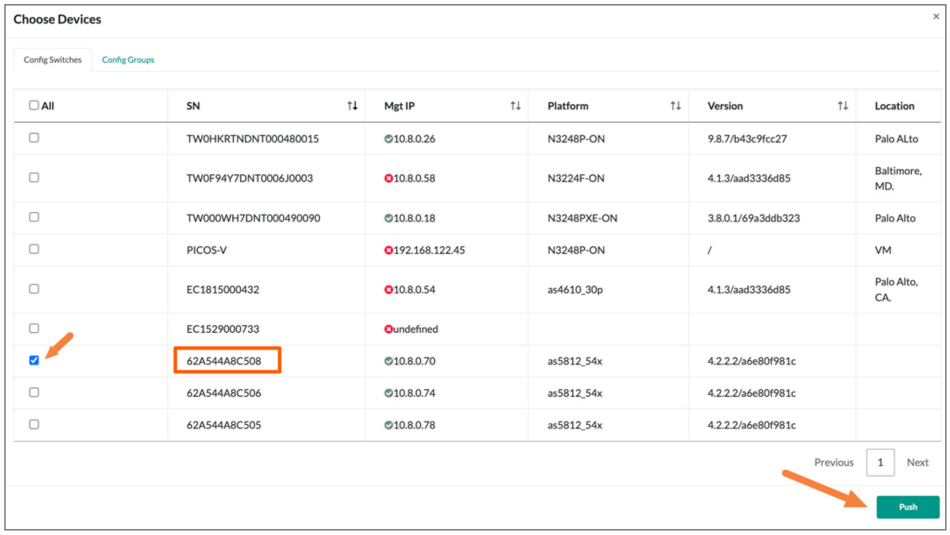
Review the config shown below and click ***Save***.



Select ***Config/Templates > Configuration Files > MLAG-Spine-1*** under configs and click ***Push Config***.

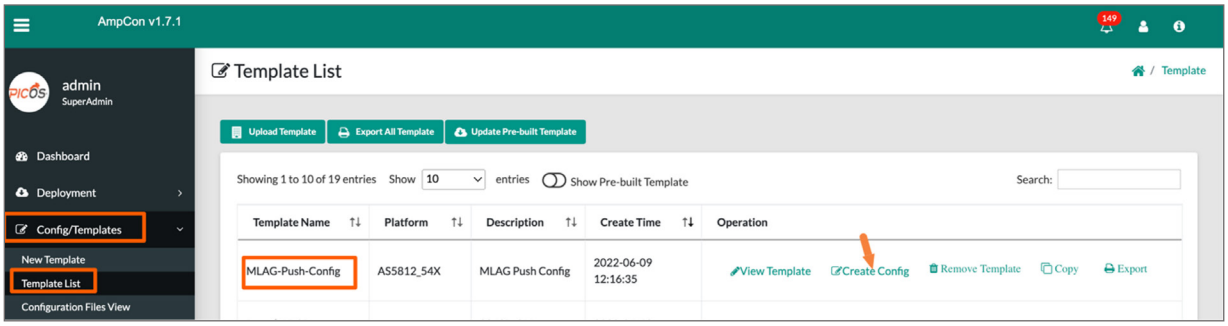


Select the PicOS-V switch with ***Serial Number*** that corresponds to the first PicOS-V spine switch in your GNS3 environment and click ***Push*** as shown below. Now first PicOS-V switch is fully configured with the MLAG configuration.

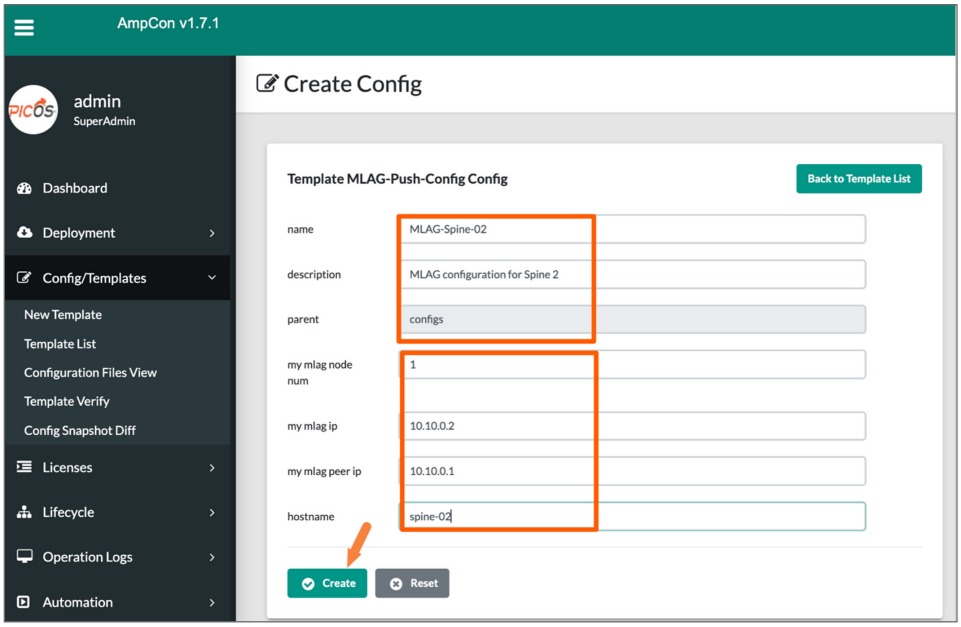


Automate configuring the second PicOS-V Spine switch with MLAG configuration by using the following steps:

1. Select ***Config Templates > Template List > MLAG-Push-Config*** and click ***Create Config*** as shown below:

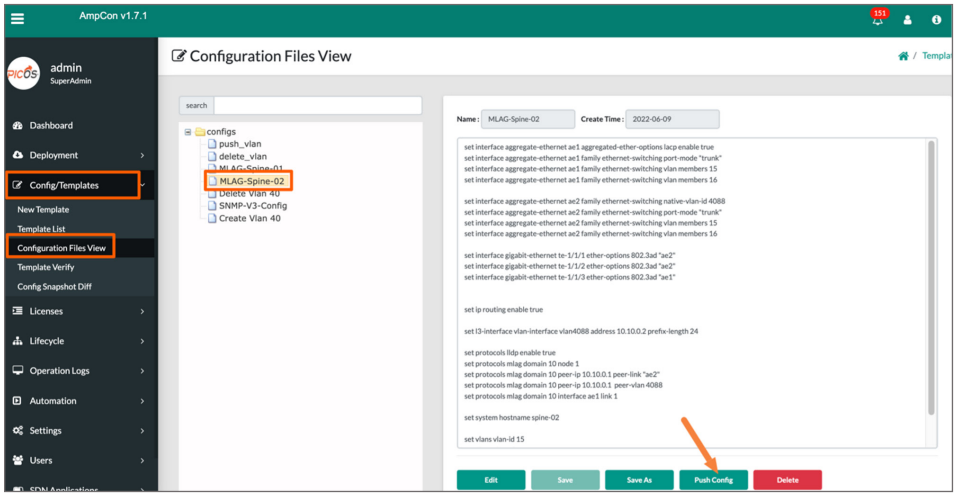


Enter the name, description, parent, my mlag node num, my mlag ip, my mlag peer ip and hostname fields as shown below and click ***Create***:

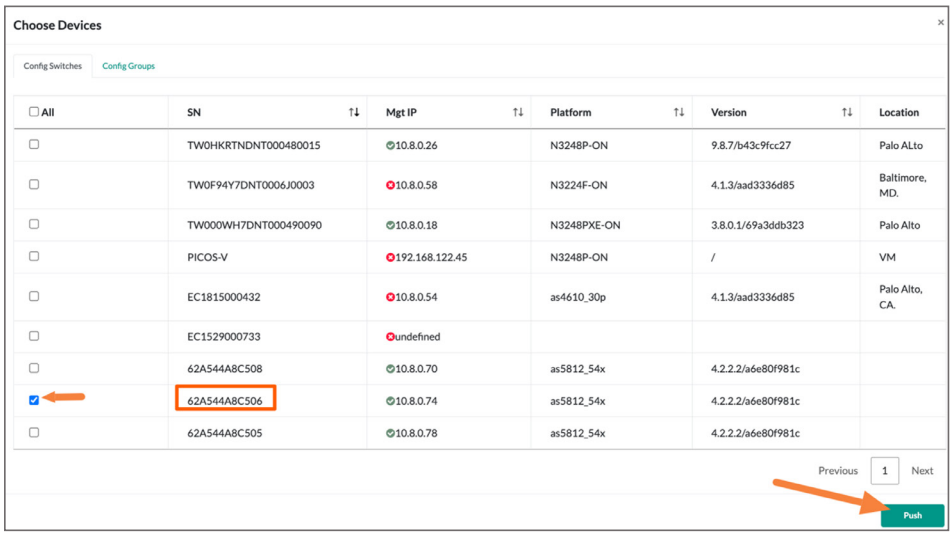


Review the config shown below and click ***Save***.

Select ***Config/Templates > Configuration Files > MLAG-Spine-2*** under configs and click ***Push Config***.



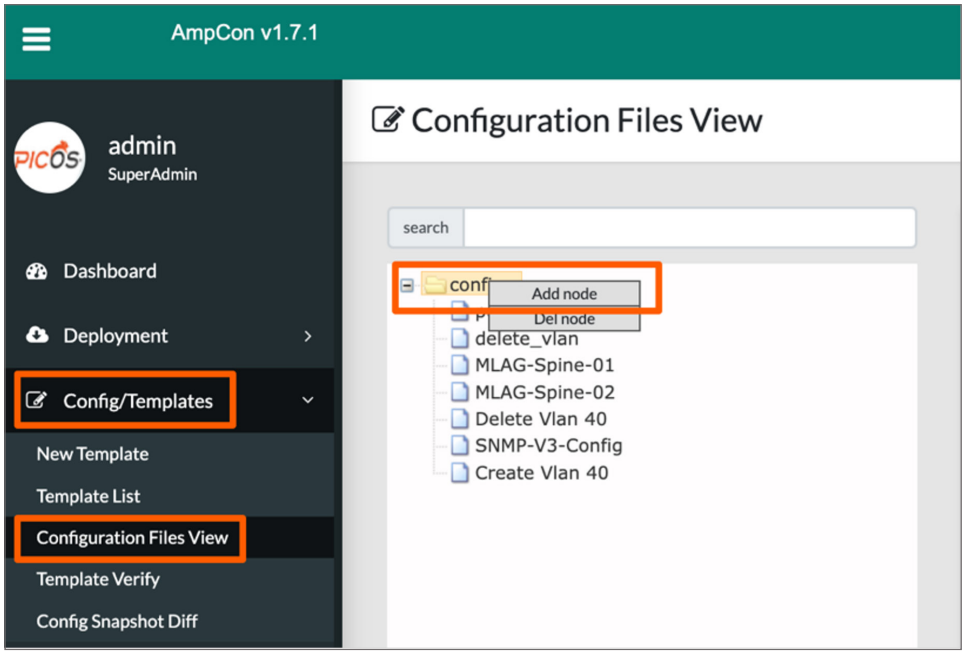
Select the PicOS-V switch with Serial Number that corresponds to the second PicOS-V spine switch in your GNS3 environment and click Push as shown below. Now second PicOS-V switch is fully configured with the MLAG configuration.



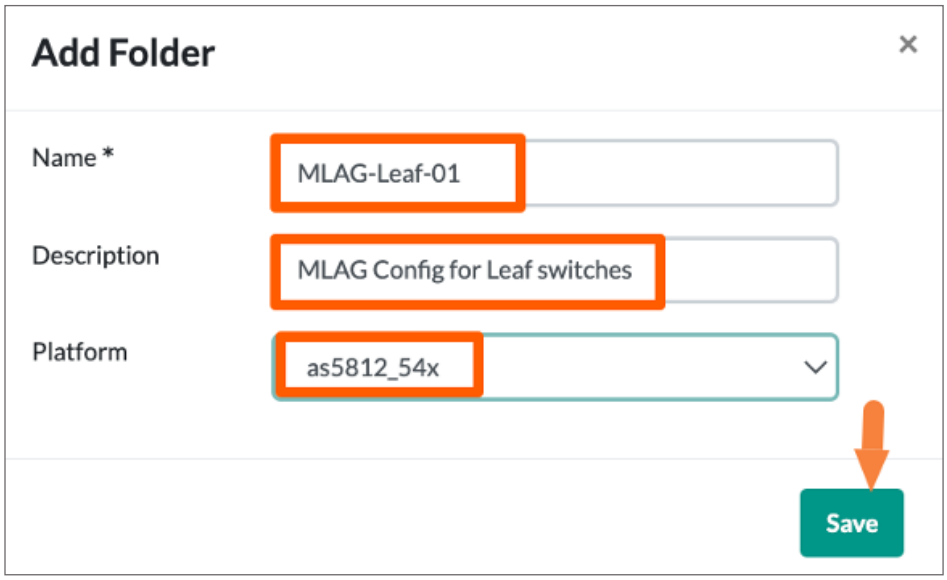
Automate Configuration of MLAG Feature in Leaf Switch

Automate configuring the first PicOS-V Leaf switch with MLAG configuration by using the following steps:

1. Select ***Config Templates > Configuration Files View*** and right click ***configs*** and select ***Add node*** as shown below.

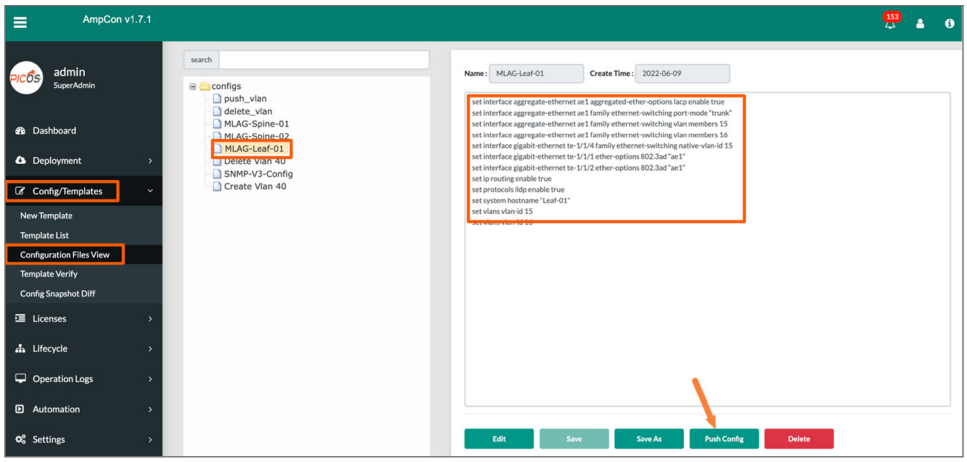


Enter ***Name***, ***Description*** and select the ***Platform*** as as5812_54x as shown below and click ***Save***.

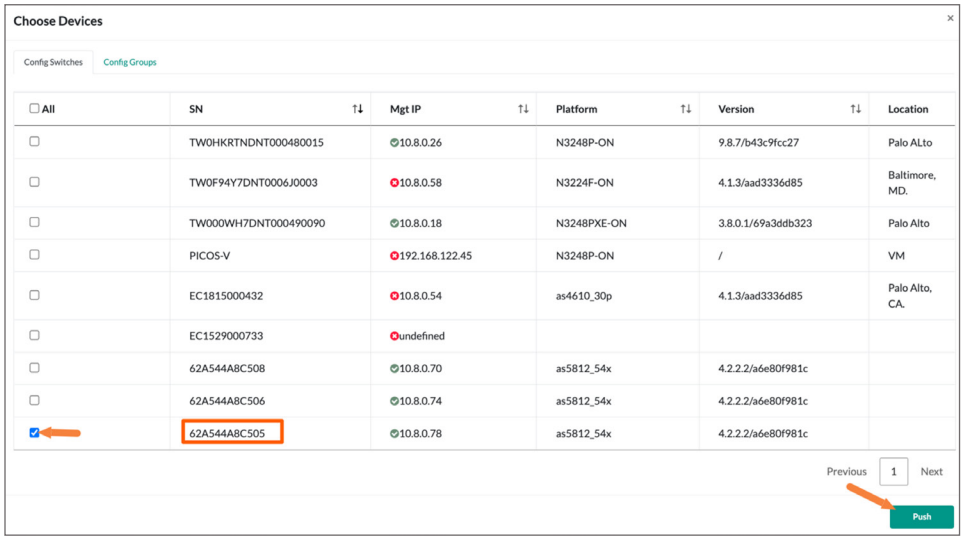


2. Select ***Config Templates > Configuration Files View > MLAG-Leaf-01*** and click ***Edit*** and paste the Leaf-01 PicOS-V switch configuration from PicOS-V User Guide and click ***Save***.

   Select ***Config Templates > Configuration Files View > MLAG-Leaf-01*** click ***Push Config*** as shown below.



   Select the PicOS-V switch with ***Serial Number*** that corresponds to the PicOS-V leaf switch in your GNS3 environment and click ***Push*** as shown below. Now the PicOS-V leaf switch is fully configured with the MLAG configuration.



Use Ansible Playbooks to Verify L2 or L3 Functionality VIDEO GUIDE ▸

In this example we will verify MLAG functionality using Ansible Playbooks.

In AmpCon you can use the Ansible Playbook UI to create custom workflows. Following are some examples:

1. **Security and Network Compliance:** Enforce day-to-day security and network compliance policies on groups of switches with ease.

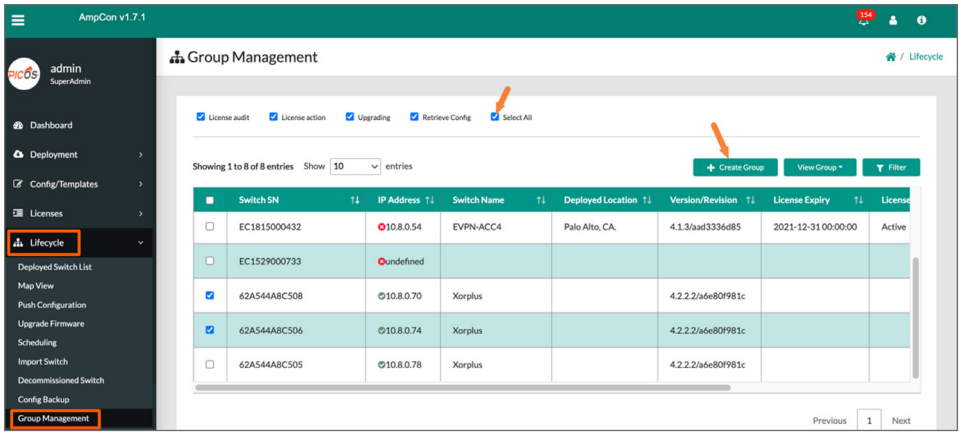
2. **Customize your automation:** Use Ansible Playbooks to create custom workflows. For example, using automation, you can check whether NAC policies are enforced on each access ports. If it detects NAC policies are not enforced on specific port, it will report and enable NAC policies back on the port.
3. **Check real-time status of the network:** You can run Ansible Playbooks to get real-time status of the network using L2 or L3 CLI commands.

In the previous section we have configured MLAG in two spines and one leaf PicOS-V switches. Let us verify whether MLAG is setup correctly in the spine switches by using the Ansible Playbook mechanism in AmpCon.

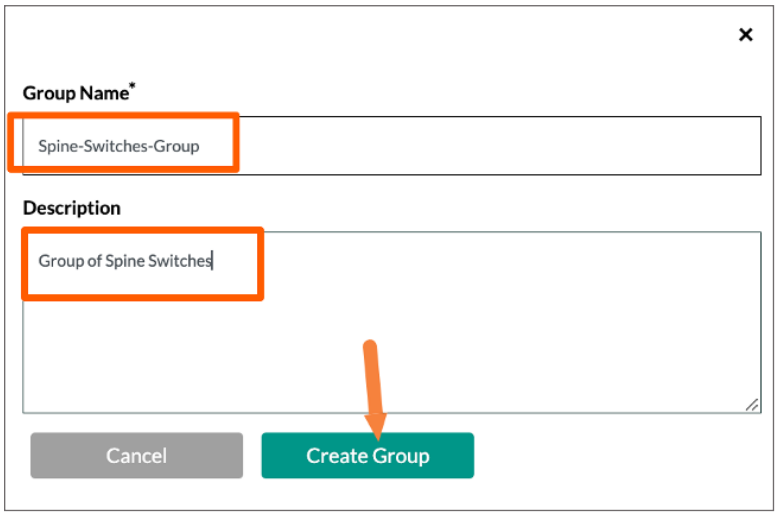
Following are the steps to do this using the Ansible Playbook mechanism in AmpCon:

1. **Create group of spine switches:** Before running an Ansible Playbook, we need to create a group of switches against which we run the Ansible Playbook. In our example we have two Spine switches. Hence, we will create a group of switches called ***Spine-Switches-Group*** and include the two PicOS-V Spine switches.

   From the UI do the following:
   • Select Lifecycle > Group Management menu
   • Click Select all button on the top
   • Select both Spine Switches identified by the Serial Number of the switch
   • and click Create Group as shown below

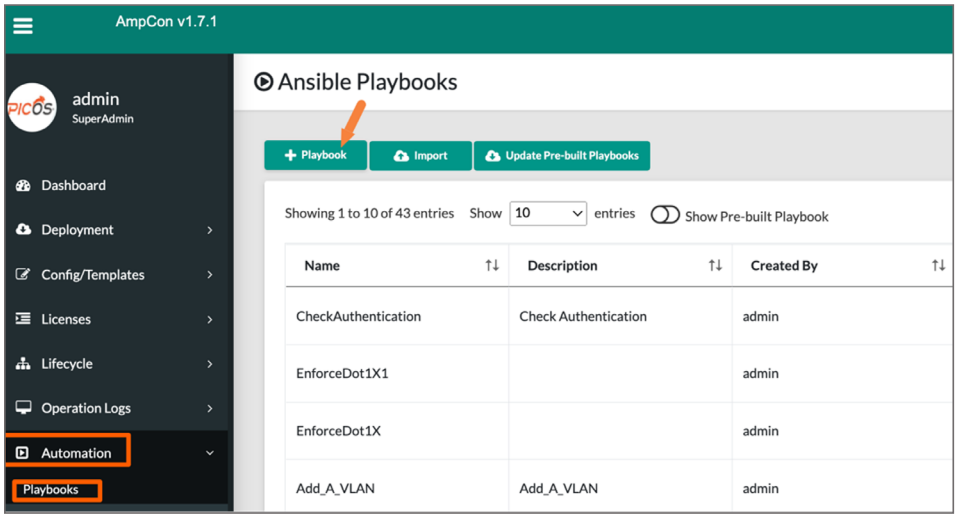


Enter the values for ***Group Name*** and ***Description*** fields as shown below and click ***Create Group***.



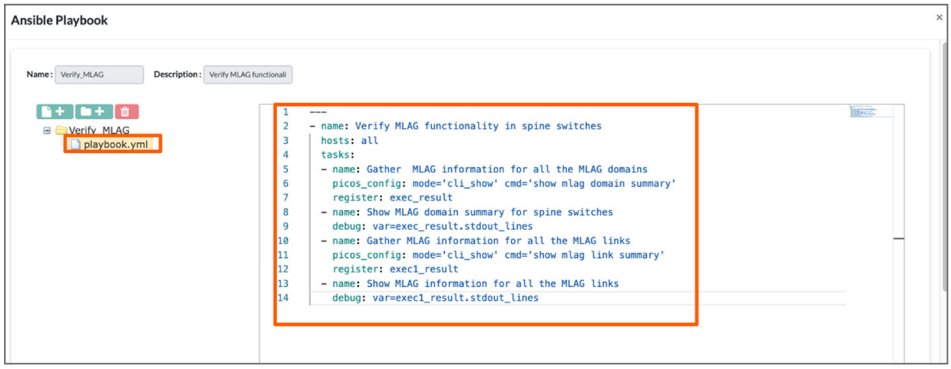
2. **Create and run Ansible Playbook to verify MLAG functionality in Spine Switches:**
   Following are steps:

   To create an Ansible Playbook in AmpCon, select ***Automation > Playbooks*** and click ***+ Playbook*** as shown below:

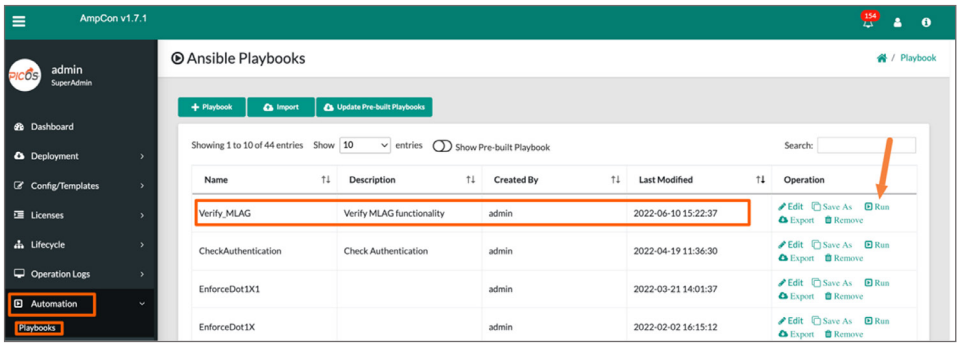


   Enter values from ***Name*** and ***Description*** fields as shown below and click ***Next***.

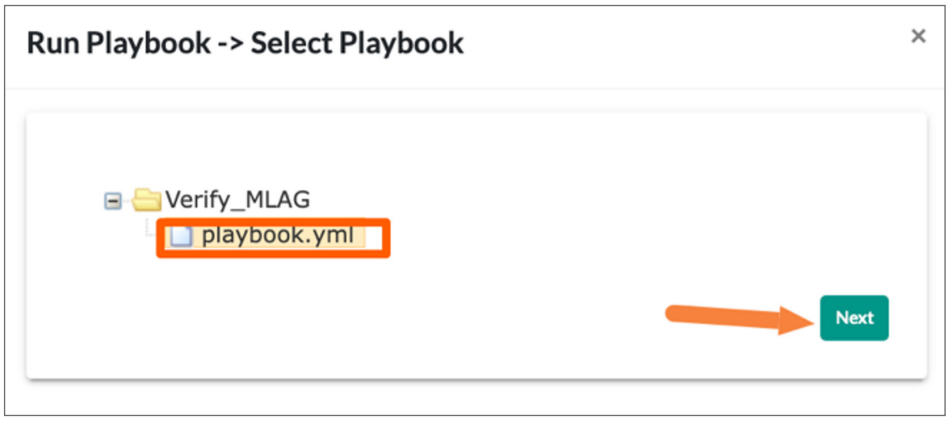
   Copy the Ansible Playbook given in Appendix B as shown below and click ***Save All***.



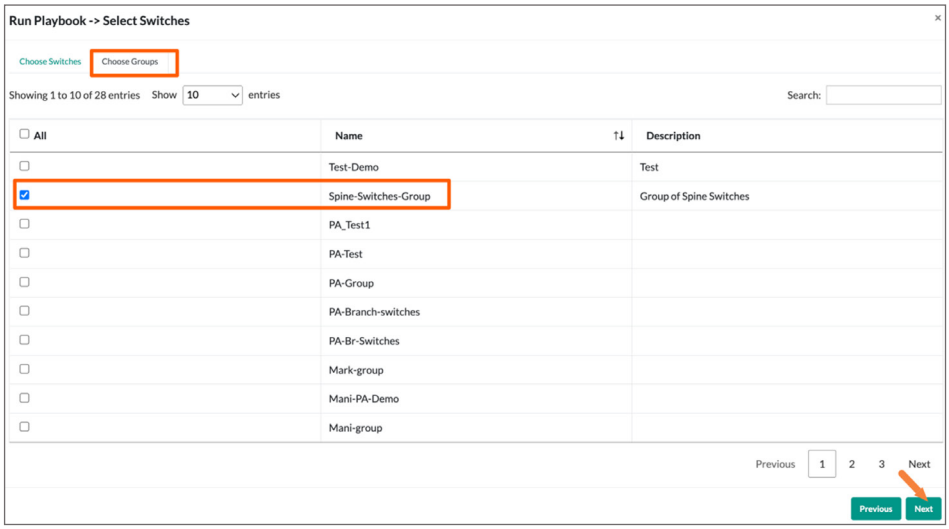
Select ***Automation > Playbooks*** menu and click ***Run*** icon associated with ***Verify_MLAG*** Ansible Playbook as shown below.



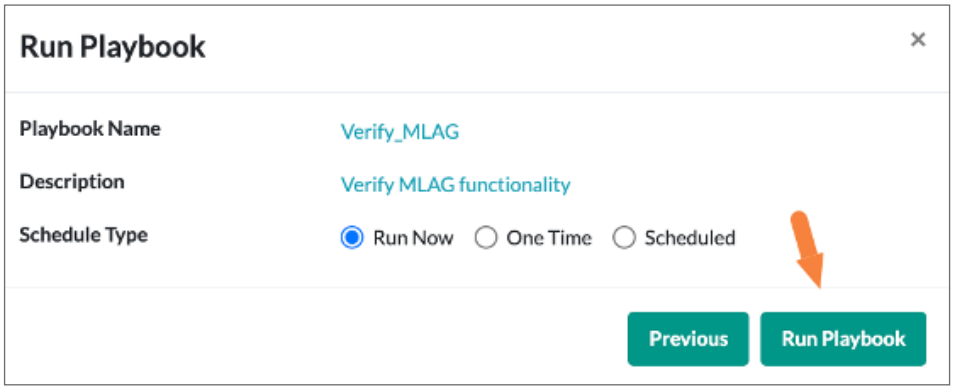
Select ***playbook.yml*** and click ***Next*** as shown below:



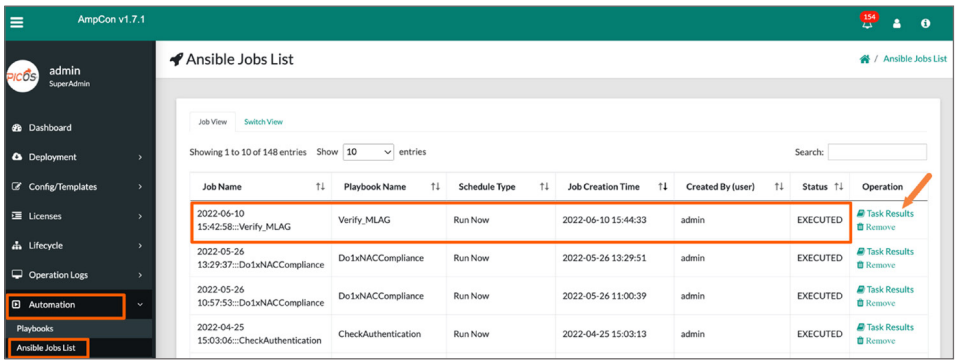
Select ***Choose Groups*** tab on the top and select ***Spine-Switches-Group*** as shown below and click ***Next*** two times.



Click ***Run Playbook*** as shown below:



3. **Verify MLAG functionality in Spine switches from the Ansible Playbook output:** Select ***Automation > Ansible Jobs List*** menu and click ***Task Results*** corresponding to Verify_MLAG Ansible Playbook as shown below:



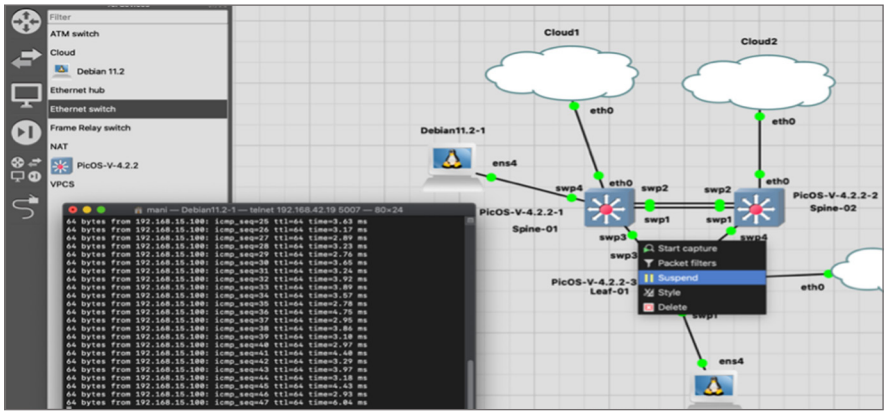
Select ***Result Output*** tab at the top as shown below. Here you will see outputs for the MLAG Domain and Link summaries for both Spine-01 and Spine-02 PicOS-V switches.

Verify MLAG Functionality with Traffic Test

Log into the console of the ***Debian11.2-1*** Server from the GNS3 client Application and execute the following Linux shell command to send ***100 packets from*** the ***Debian11.2-1 Server*** connected to the Spine-01 switch to the ***Debian11.2-2 Server*** connected to the Leaf-01 switch.

```
debian@debian:~$ ping -c 100 192.168.15.100
PING 192.168.15.100 (192.168.15.100) 56(84) bytes of data.
64 bytes from 192.168.15.100: icmp_seq=1 ttl=64 time=6.73 ms
64 bytes from 192.168.15.100: icmp_seq=2 ttl=64 time=40.9 ms
64 bytes from 192.168.15.100: icmp_seq=3 ttl=64 time=3.06 ms
```

When the ICMP traffic is flowing, right click on the link between the ***Spine-01*** and the ***Leaf-01***. Select ***Suspend*** to stop the traffic flowing through that link as shown below. MLAG will make the traffic flow ***from*** the ***Spine-01*** switch to the ***Leaf-01*** switch via the ***Spine-02*** switch.



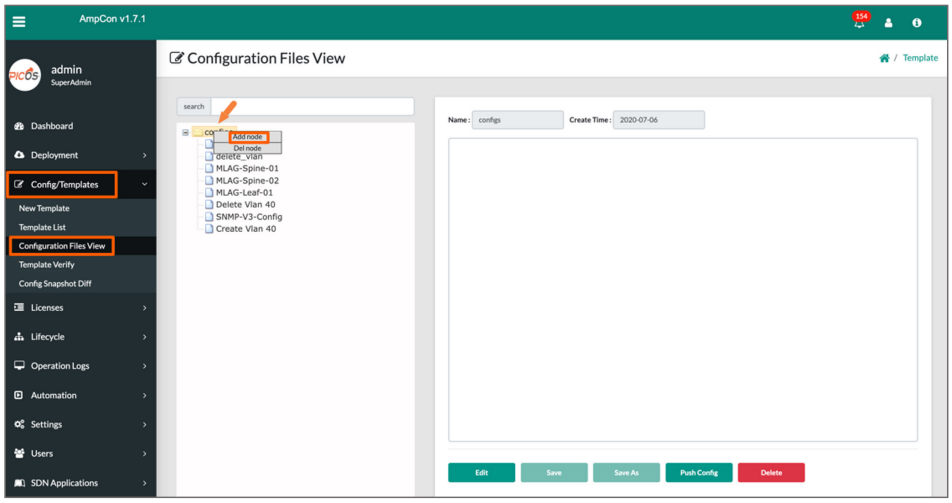
The output of ping traffic verifies that there is no packet loss when the link between Spine-01 and Leaf-01 goes down. This verifies MLAG functionality.

```
<… output suppressed …>
64 bytes from 192.168.15.100: icmp_seq=97 ttl=64 time=4.52 ms
64 bytes from 192.168.15.100: icmp_seq=98 ttl=64 time=4.55 ms
64 bytes from 192.168.15.100: icmp_seq=99 ttl=64 time=4.14 ms 64 bytes from 192.168.15.100: icmp_
   seq=100 ttl=64 time=4.22 ms
--- 192.168.15.100 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99912ms
rtt min/avg/max/mdev = 2.761/4.428/40.906/3.756 ms
```

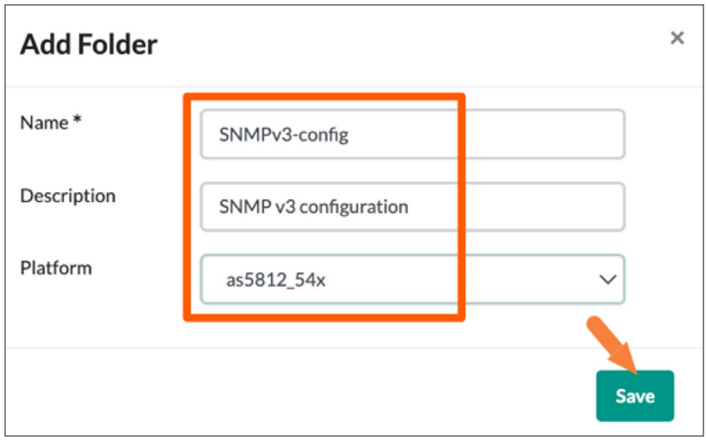
Day-to-day Policy Enforcement VIDEO GUIDE ▸

AmpCon can be used for automating day-to-day policy enforcement in a group of switches. As an example, let us say we need to integrate PicOS-V Spine switches with a Network Management server using SNMP v3. Following are steps to enable SNMPv3:

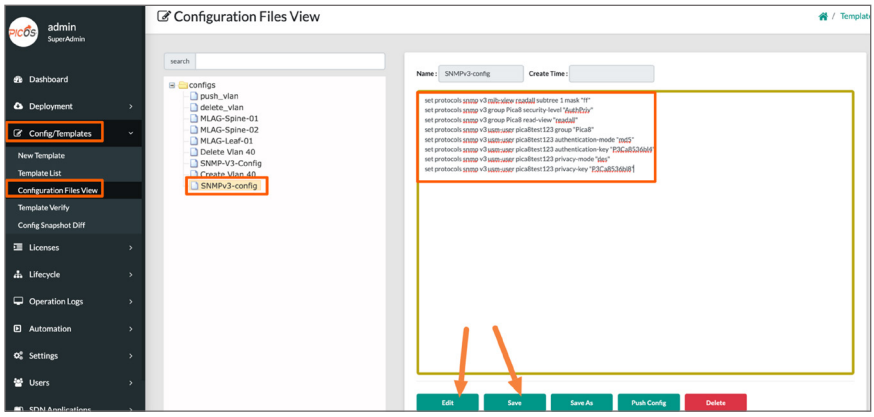
1. Log into AmpCon UI. Select ***Config Templates > Configuration Files View*** and right click on ***configs*** and select ***Add node*** as shown below:



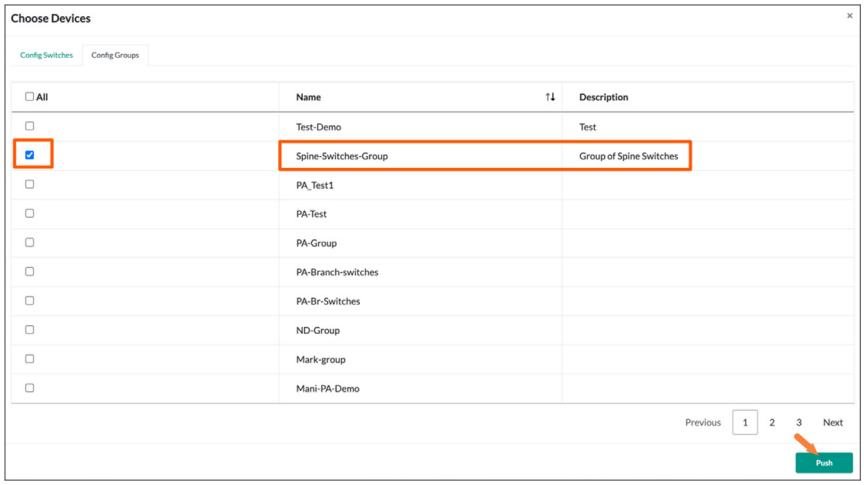
2. Enter ***Name***, ***Description***, and ***Platform*** as shown below and click ***Save***.



3. Select ***Config/Templates > Configuration Files View > SNMPv3-config*** and click ***Edit***. Copy the SNMP v3 configuration given in Appendix C and paste it to the right side window as shown below. Click ***Save*** as shown below. “Are you sure?” dialog box will appear. Click ***Yes***.



4. Select ***Config/Templates > Configuration Files View > SNMPv3-config*** and click ***Push Config***. Select ***Spine-Switches-Group*** as show below and click ***Push***.



5. Verify whether SNMP v3 configuration is properly configured in the spine switches by running the following Linux command in the Network Management Linux server. It queries the Spine-01 switch with management IP address 192.168.42.10 to provide its Hardware Model using the MIB 1.3.6.1.4.1.35098.1.13.0

```
root@zabbix-77:~# snmpwalk -v3 -u pica8test123 -l AuthPriv -a md5  -A P3Ca8536bl4 -x des  -X
P3Ca8536bl8 192.168.42.10 1.3.6.1.4.1.35098.1.13.0
SNMPv2-SMI::enterprises.35098.1.13.0 = STRING: "AS5812_54X"
```

The above command output verifies PicOS-V switch is properly integrated with Network Management server using SNMP v3.

Configuration Management VIDEO GUIDE

Following are four major Configuration management use cases in AmpCon.

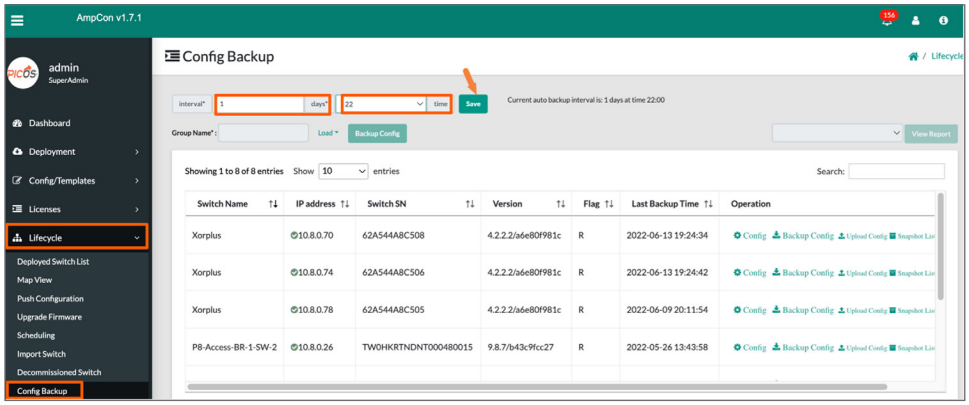
1. Automatic backup of configuration of all switches
2. Manual backup of configuration of a PicOS switch
3. Restore configuration of a switch from backup
4. Compare two configurations and identify the difference between them

Automatic Backup of Configuration of all Switches

You can enable automatic backup of the configuration of all deployed switches at a specific interval.

Select ***Lifecycle -> Config Backup*** menu and do the following as shown below:

1. Enter ***days*** with a value, for example set it to value 1 for daily configuration backup.
2. Enter ***Interval time*** in hours in timezone set in the AmpCon server. Daily backup of configuration will be done at the specific time entered in this step. In this example daily backup will be done at 11 PM UTC time daily.
3. Click ***Save***.

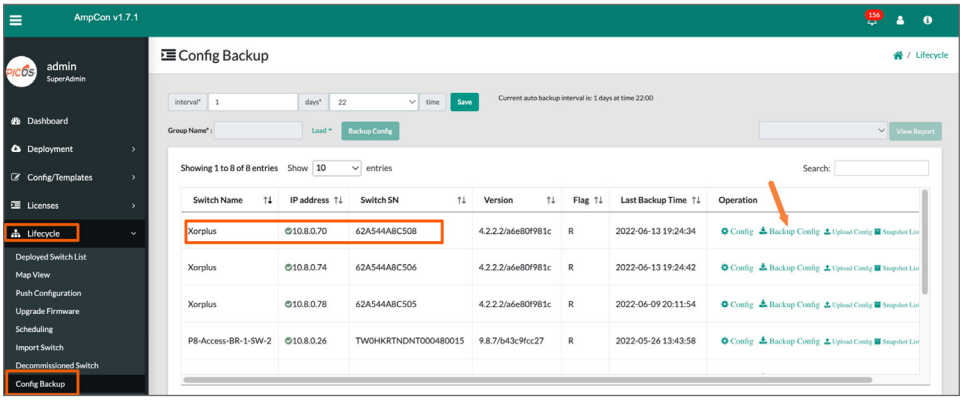


In the above example, configuration of all switches will be backed up in AmpCon at 11 PM daily.

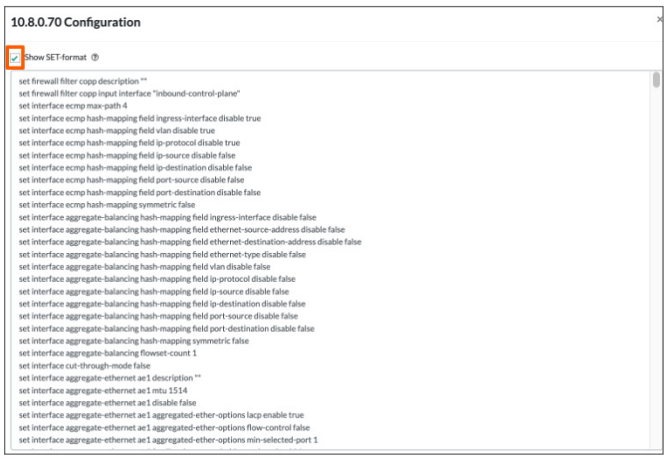
Manual Backup of Configuration of a PicOS Switch

A manual backup of a specific switch configuration can be initiated by the user at any time. Backup or snapshot of switch configurations is stored in the database.

To make a manual backup of a specific switch configuration, select Lifecycle > Config Backup, select the switch and click Backup Config as shown below.



To view the manual snapshot of config, select ***Lifecycle > Config Backup***, select the switch and click ***Config*** and click ***Show SET-format*** as shown below:



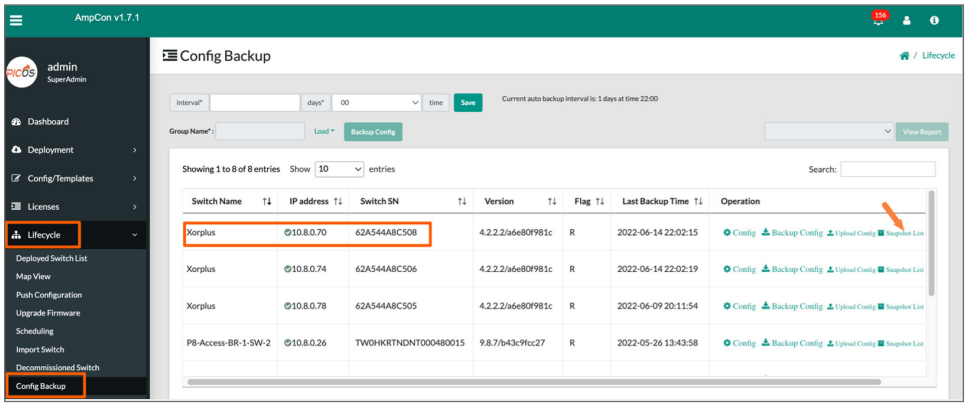
Restore Configuration of a PicOS Switch from Backup Saved in AmpCon

Log into the console of Spine-01 PicOS-V switch in GNS3 environment and execute the following:

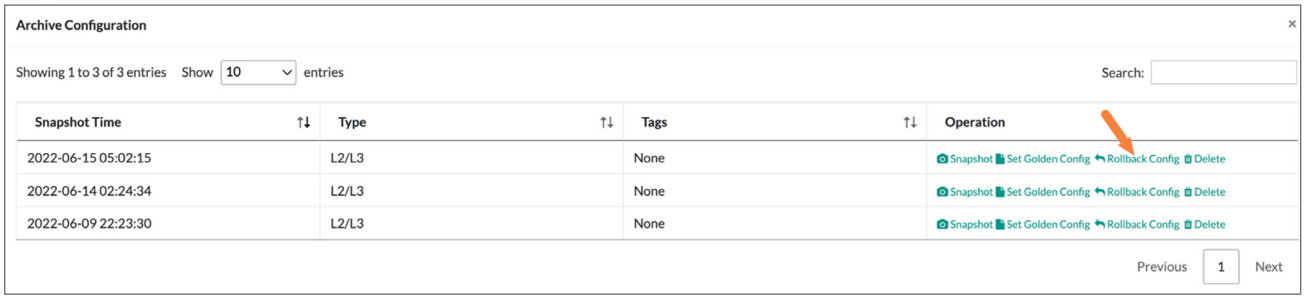
```
admin@spine-01> show system name
spine-01
admin@spine-01> configure t
Entering configuration mode.
There are no other users in configuration mode.
admin@spine-01# set system hostname foobar
admin@spine-01# commit
Commit OK.
Save done.
```

In the above example we accidentally changed the host name from ***spine-01*** to ***foobar***.

Select ***Lifecycle > Config Backup*** and select the row of PicOS-V switch with ***Serial Number*** that corresponds to ***spine-01*** switch and click ***Snapshot List*** as shown below.



Click ***Rollback Config*** as shown below and Rollback.



Check spine-01 PicOS-V console in GNS3 environment. You will see the following output.

```
admin@foobar# The configuration has been changed by user admin
DELTAS:
    system {
        hostname: "spine-01"
    }
```

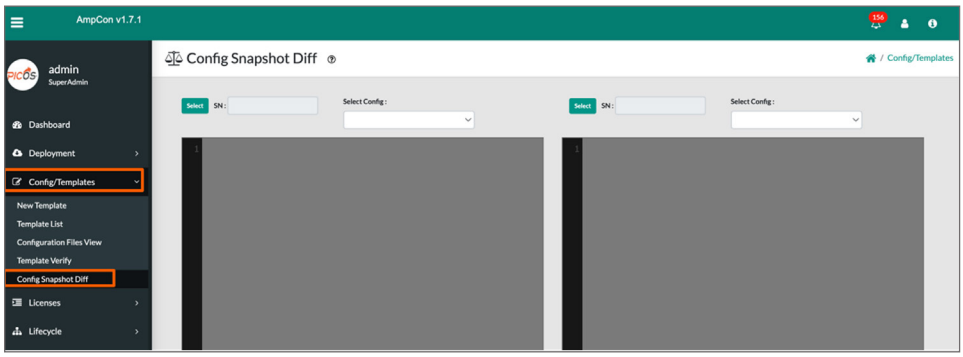
Run the following CLI to verify hostname of the switch is restored to spine-01 from foobar.

```
admin@spine-01# run show system name
spine-01
```

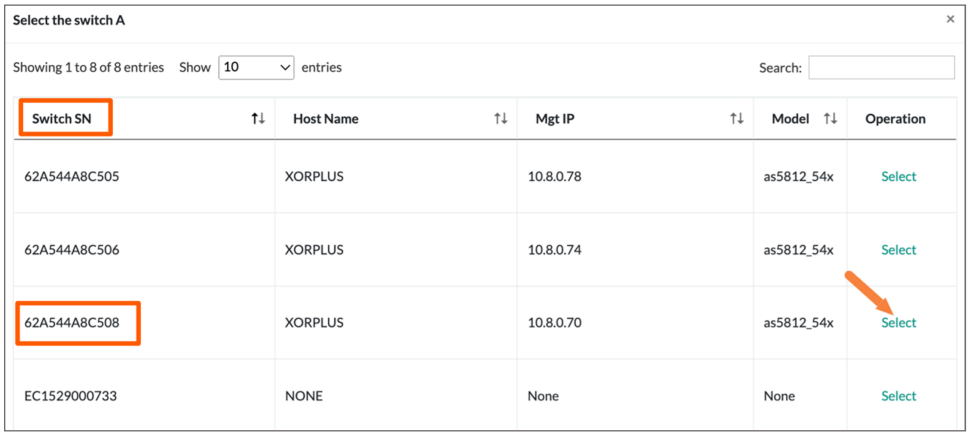
Compare Two Configurations and Identify the Differences Between Them

Let us compare the configuration of PicOS-V ***spine-01*** switch before and after ***SNMP v3*** configuration is applied as performed in the earlier section.

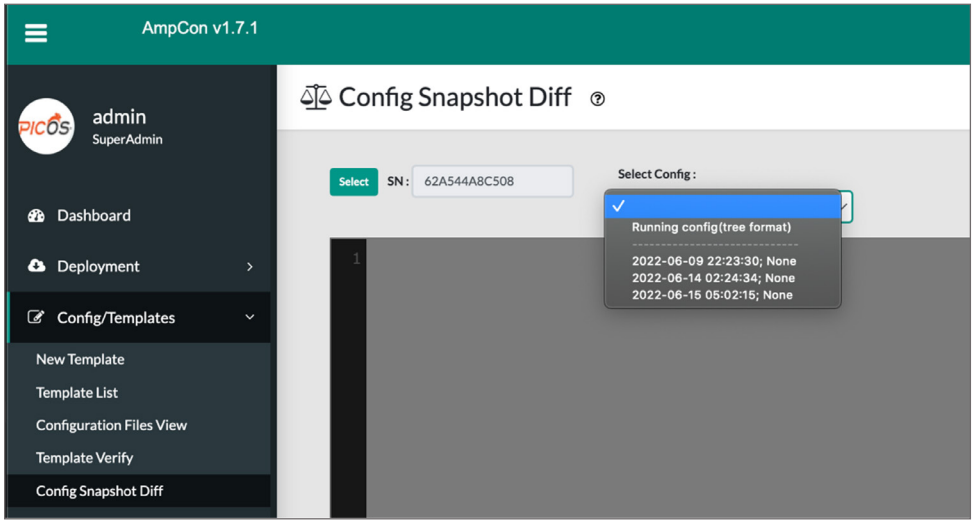
Select ***Config Templates > Config Snapshot Diff*** as shown below.



In the left pane click ***Select SN*** and click ***Select*** that corresponds to the ***Serial Number*** of the ***spine-01*** switch.

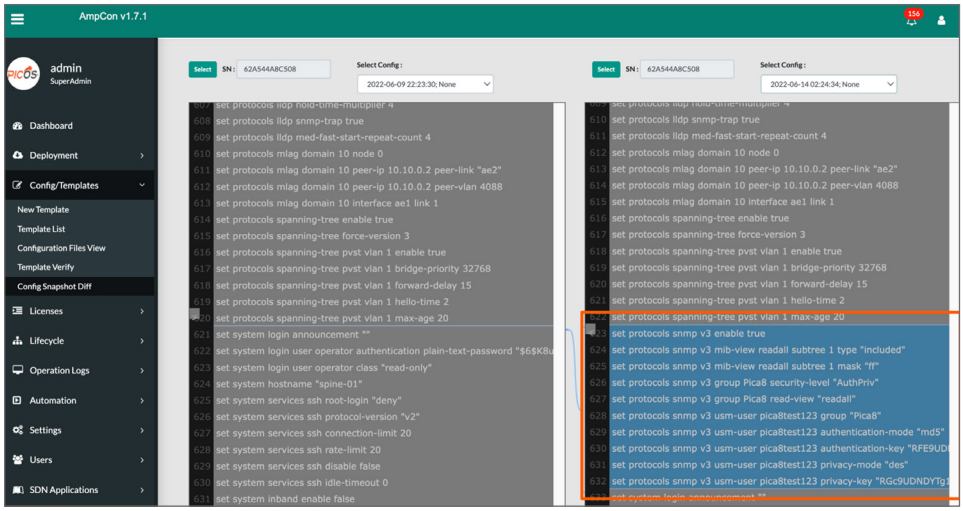


Select the oldest ***timestamp*** from the list as shown below.



In the right pane click ***Select SN*** and click ***Select*** that corresponds to the ***Serial Number*** of the spine-01 switch and select the ***newest timestamp*** from the list.

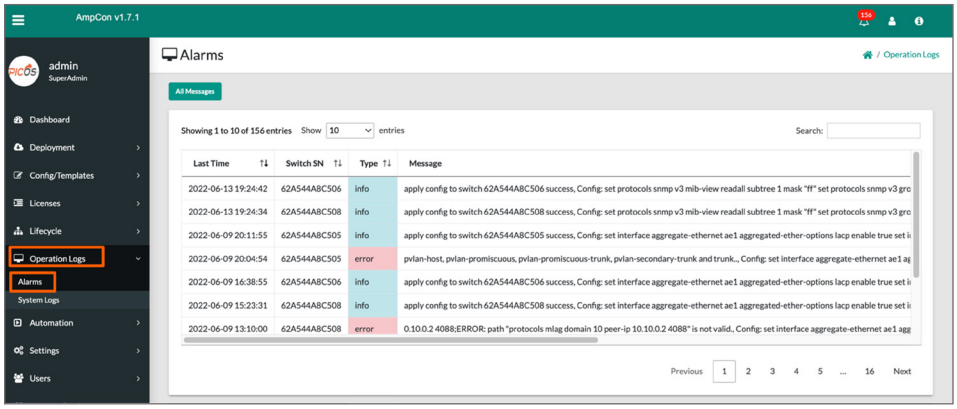
Scroll down the config on the right pane to see difference between these two configuration as highlighted in blue colors shown below.



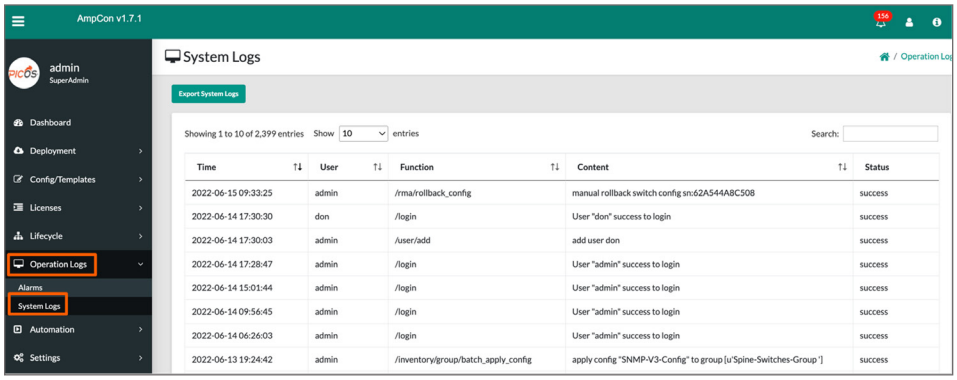
Audit and Operation Logs VIDEO GUIDE

Select Operation Logs > Alarms to view AmpCon operation errors and alerts.
Alerts are color coded as follows:

- **Red** – needs action
- **Yellow** – you might to want to look at it
- **Green** - good



Select ***Operation Logs > System Logs*** to view AmpCon audit logs as shown below. Audit logs provide info on who did what and when.



For troubleshooting purposes, the Backend Log will be very useful. To download Backend Log, click Export System Logs button in the above UI.

Reference

PicOS

The following are reference materials related to PicOS:
• PicOS Routing and Switching Configuration Guide

PicOS-V

The following are reference materials related to PicOS-V:
• PicOS-V Eval Guide

AmpCon

The following are reference materials related to AmpCon:
• AmpCon Network Controller Deployment and User Guide

Appendix-A – Jinja2 Template to Configure MLAG in Spine PicOS-V Switches

The following is contents of Jinja2 Template with file name ***MLAG-Push-Config.txt***. It is used for configuring the MLAG feature in spine switches.

```
name: MLAG-Push-Config
description: MLAG Push Config
platform: AS5812_54X
content_start:
set interface aggregate-ethernet ae1 aggregated-ether-options lacp enable true
set interface aggregate-ethernet ae1 family ethernet-switching port-mode “trunk”
set interface aggregate-ethernet ae1 family ethernet-switching vlan members 15
set interface aggregate-ethernet ae1 family ethernet-switching vlan members 16

set interface aggregate-ethernet ae2 family ethernet-switching native-vlan-id 4088
set interface aggregate-ethernet ae2 family ethernet-switching port-mode “trunk”
set interface aggregate-ethernet ae2 family ethernet-switching vlan members 15
set interface aggregate-ethernet ae2 family ethernet-switching vlan members 16

set interface gigabit-ethernet te-1/1/1 ether-options 802.3ad “ae2”
set interface gigabit-ethernet te-1/1/2 ether-options 802.3ad “ae2”
set interface gigabit-ethernet te-1/1/3 ether-options 802.3ad “ae1”

{% if my_mlag_node_num == “0” %}
set interface gigabit-ethernet te-1/1/4 family ethernet-switching native-vlan-id 15
{% endif %}

set ip routing enable true

set l3-interface vlan-interface vlan4088 address {{my_mlag_ip}} prefix-length 24

set protocols lldp enable true
set protocols mlag domain 10 node {{my_mlag_node_num}}
set protocols mlag domain 10 peer-ip {{my_mlag_peer_ip}} peer-link “ae2”
set protocols mlag domain 10 peer-ip {{my_mlag_peer_ip}}  peer-vlan 4088
set protocols mlag domain 10 interface ae1 link 1

set system hostname {{hostname}}

set vlans vlan-id 15
set vlans vlan-id 16
set vlans vlan-id 4088 l3-interface “vlan4088”

content_end$
```

```
param_start:
{
“my_mlag_node_num”: {
“param_default”: “”,
“type”: “uint”,
“required”: “required”,
“description”: “mlag-node-num [0,1]”,
“param_check”: “”
},
“my_mlag_ip”: {
“param_default”: “”,
“type”: “text”,
“required”: “required”,
“description”: “my_mlag_ip, e.g 192.168.42.1”,
“param_check”: “”
},
“my_mlag_peer_ip”: {
“param_default”: “”,
“type”: “text”,
“required”: “required”,
“description”: “my_mlag_peer_ip, e.g 192.168.42.1”,
“param_check”: “”
},
“hostname”: {
“param_default”: “”,
“type”: “text”,
“required”: “required”,
“description”: “hostname of switch, e.g. 10”,
“param_check”: “”
}
}

param_end$
```

Appendix-B – Ansible Playbook for Verifying MLAG Functionality

Following is content for the Ansbile Playbook called ***Verify_MLAG.yml*** to verify the MLAG functionality.

```
---
- name: Verify MLAG functionality in spine switches
  hosts: all
  tasks:
  - name: Gather  MLAG information for all the MLAG domains
    picos_config: mode='cli_show' cmd='show mlag domain summary'
    register: exec_result
  - name: Show MLAG domain summary for spine switches
    debug: var=exec_result.stdout_lines
  - name: Gather MLAG information for all the MLAG links
    picos_config: mode='cli_show' cmd='show mlag link summary'
```

```
    register: exec1_result
  - name: Show MLAG information for all the MLAG links
    debug: var=exec1_result.stdout_lines
```

Appendix-C – SNMP v3 Configuration

Following is SNMP v3 related configuration for PicOS-V switch:

```
set protocols snmp v3 mib-view readall subtree 1 mask “ff”
set protocols snmp v3 group Pica8 security-level “AuthPriv”
set protocols snmp v3 group Pica8 read-view “readall”
set protocols snmp v3 usm-user pica8test123 group “Pica8”
set protocols snmp v3 usm-user pica8test123 authentication-mode “md5”
set protocols snmp v3 usm-user pica8test123 authentication-key “P3Ca8536bl4”
set protocols snmp v3 usm-user pica8test123 privacy-mode “des”
set protocols snmp v3 usm-user pica8test123 privacy-key “P3Ca8536bl8”
```

