

NetMRI Policy Deployment Guide

Table of Contents

| Introduction | 2 |
|---|----|
| Prerequisites | 2 |
| PCI compliance | 2 |
| DISA-STIG Compliance | 13 |
| Auto Device Remediation | 19 |
| Testing the triggered job by changing a device configuration manually | 29 |
| Device CVE/PSIRT - Advisor | 35 |
| Device Life Cycle Management | 44 |

Introduction

This deployment guide will show you how to use the NetMRI policy feature to analyze the discovered intermediary device (ie routers, switches, firewalls, etc) configurations for any policy violations like PCI (payment card industry), DISA STIG (Defense Information Systems Agency Security Technical Information Guides), and CVE/PSIRT (Common Vulnerabilities and Exposures/Product Security Incident Response Team) violations. In addition, this deployment guide will show how to configure NetMRI to auto remediate any misconfigurations and provide life cycle management information on the discovered devices.

Rules and Policy

The NetMRI Policy Design Center provides you with the ability to test the configuration of devices in your network against a specific set of rules and identify where the device does not comply with those rules. **Rules** are the individual tests and are grouped into a set called a **Policy.** Policies are deployed to analyze one or more Device Groups in the NetMRI system (see the topic "Introducing Device Groups" in the Infoblox NetMRI Administrator Guide, Part 3 Device and Network Exploration, Devices & Interfaces for more information on Device Groups.)

Rules are written in one of three forms: A Simple Rule looks for configuration statements that are required to be present and/or are required to be absent in the device's configuration. A Rule Logic Builder rule combines several tests and combines their evaluation with logical operators like AND, OR, NOT, etc. These two rule types are stored internally as XML documents, so the third way to write rules is directly in XML. Consult the Infoblox NetMRI Administrator Guide, Part 5 Network Compliance for more details.

Prerequisites

- The NetMRI appliance must be configured to discover the required devices.
- The discovered devices have been placed into the default device groups or user-created device groups.
- Mail server settings are configured.
- The NetMRI appliance must have a backup of the discovered devices' configuration files.
- In the deployment sections, lab devices are used as examples to illustrate the features

PCI compliance

If you have an enterprise network where credit card information traffic flows through it, then you must adhere to a version of the PCI DSS standards. NetMRI has built-in policies for PCI DSS compliance. The following instructions show you how to implement PCI policies. The predefined policies are examples built mainly for Cisco and Juniper. For other vendors you may need to create additional rules following the given examples.

1. Navigate to Config Management → Policy Design Center → Policies → PCI DSS 3.0 IOS/NX-OS.

| Dashboard Network Analysis | Network Explorer Config Man | egoment Reports | | A 4 |
|---|---------------------------------------|--|--------------|---------|
| Config Archive Config | Search Job Management Policy I | Design Center | | |
| ummary Rules Policies Policy Deployment | | | | |
| udd Delete Copy Import Export Print | | | | Default |
| Policies | Policy Name: | Rules in this Policy | | |
| Search | FG10333.0103/14x-03 | Name | Severity | |
| E IAVA 2009-A-0022 | Short Name: PCI 3.0 | PCI 3.0 IOS/NX-OS Two Factor Authentication | error | |
| 2 Advisories | | TI PCI 30 IOS BOOTP Server disable | error | |
| E DISA v7, r1.9 JUNOS | Infobiox, Inc. | H PCI 3 0 IOS CDP Service | info | |
| DISA v7, r1.9 Cisco Infrastructure Router | Description: | | ino | |
| DISA v7, r1.9 Cisco Infrastructure Switch | This policy is provided to the user a | IS PCI 3.0 NX-OS COP Service | into | |
| DISA v7. r1.9 Cisco Perimeter Router | is, and is meant as a general | al PCI 3.0 IOS Console Exec 15 Minute Timeout | error | |
| DISA v7, r1.9 Cisco Perimeter Switch | interpretation of the POLDS | B PCI 3.0 NX-OS Console Exec 15 Minute Timeout | error | |
| E DISA v8, r11 STIG Firewall | View Policy Properties | PCI 3.0 IOS Console Local or AAA Login | error | |
| DISA v8, r11 STIG Infrastructure Layer 2 Switch | Read Only | B PCI 3.0 NX-OS Console Local or AAA Login | error | |
| DISA v8, r11 STIG Infrastructure Layer 3 Switch | Device Filter for Policy | B PCI 3.0 IOS Enable Secret | error | |
| NSA 1 to IOS | View filter | B PCI 3.0 IOS Finger Service (11.2-) | error | |
| DISA v8, r11 STIG Network Devices | | H PCI 3.0 /OS Einner Service (11.3-12.0) | 9/0/ | |
| PCI DSS 2.0 IOS | | | and a second | |
| E PCI DSS 3.0 IOS/NX-OS | | B PCI 3.0 IOS Finger Service (12.1+) | error | |
| E PCI DSS 1.2 IOS | | H PCI 3.0 NX-OS HTTP Server | error | |
| DISA v8, r11 STIG Perimeter L3 Switch | | B PCI 3.0 IOS HTTP Server | error | |
| S PANE IOP | | B PCI 3.0 IOS Identid Service | error | |

2. Make sure the PCI 3.0 policy is highlighted. Click on the Copy button to copy this default policy to a user created policy. Fill out the Policy Name, Short Name (max Short Name length is 12 characters), and Author. Click Save.

| Policy Name: | PCI Policy | | | |
|--------------|------------|--|--|--|
| Short Name: | PCI Policy | | | |
| Author: | TME | | | |
| Description: | | | | |
| | | | | |

3. Highlight the newly created policy called PCI Policy.

| Config Archive Config | Search Job Management Policy De | sign Center | | N W |
|---|--|---|----------|------------------|
| mmary Rules Policies Policy Deployment | | | | |
| dd Delete Copy Import Export Print | | | | Default Statu |
| Policies | Policy Name: | Rules in this Policy | | |
| earch | PCI Policy | Name | Severtty | |
| E IAVA 2009-A-0022 | Short Name: PCLDSS 3.0 | H PCI 2.0 (DS NV OS Two Factor Authentication | arror . | |
| Advisories | 1010000.0 | POLICIA DO DOTO Parente disable | and . | |
| DISA v7, r1.9 JUNOS | Author: Thomas Lee | Poi so los doorn sever deale | BIO | |
| DISA v7, r1.9 Cisco Infrastructure Router | | G PCI 3.0 IOS CDP Service | into | |
| DISA v7, r1.9 Cisco Infrastructure Switch | This policy is provided to the user as | Del 3.0 IOS Console Exec 15 Minute Timeout | error | |
| DISA v7, r1 9 Cisco Perimeter Bouter | is, and is meant as a general | PCI 3.0 IOS Console Local or AAA Login | error | |
| DISA v7. r1.9 Cisco Perimeter Switch | interpretation of the PGI DS | b PCI 3.0 IOS Enable Secret | error | |
| DISA v8, r11 STIG Firewall | Edit Policy Properties | B PCI 3.0 IOS Timestamps Logging | error | |
| DISA v8, r11 STIG Infrastructure Layer 2 Switch | | B PCI 3.0 IOS Disable MOP | warning | |
| DISA v8, r11 STIG Infrastructure Layer 3 Switch | Device Filter for Policy | B PCI 3.0 IOS Disable NTP | warning | |
| I DISA V6, F11 S FIG Intrastructure Router | Choc.9, mat. | PCI 30 IOS PAD Service | ettor | |
| DISA v8, r11 STIG Network Devices | | H RCI 3.0 IOS Render Confe | allow - | |
| PCI DSS 2.0 IOS | | | | |
| PCI DSS 3.0 IOS/NX-OS | | Di PCI 3.0 IOS/NA-OS IP Source Route | error | |
| PCI DSS 1.2 IOS | | di PCI 3.0 IOS/NX-OS VTY Access Class Inbound | error | |
| DISA v8, r11 STIG Perimeter Router | | B PCI 3.0 IOS VTY Transport Input SSH | error | |
| SANS IOS | | B PCI 3.0 IOS VTY AAA Login | error | |
| PCI Pallcy | | B PCI 3.0 IOS/NX-OS User Secrets | error | |
| | | H PCI 3.0 IOS SNMP v1 and v2 obsolete | error | |
| | | B PCI 3.0 IOS/NX-OS SNMP v1 and v2 obsolete | error | |
| | | PCI 3.0 IOS Min Password Length 7 characters policy | error | |
| | | # PCI 3.0 IOS Min Password Length 7 characters | arror | |
| | | H PCI 3.0 IOS Parenword must contain ourmain and anhabatic characters | | |
| | | | | |
| | | | | Test Policy Edit |

4. Click on the Edit button on the lower right corner of the screen to edit this policy and the following screen appears:

| Select Rules | \boxtimes |
|---|------------------|
| Please select the rules you would like to add | |
| Search | |
| PCI 3.0 IOS BOOTP Server disable | |
| PCI 3.0 IOS CDP Service | |
| PCI 3.0 IOS Console Exec 15 Minute Timeout | |
| PCI 3.0 IOS Console Local or AAA Login | |
| PCI 3.0 IOS Disable MOP | |
| PCI 3.0 IOS Disable NTP | |
| PCI 3.0 IOS Enable Secret | |
| PCI 3.0 IOS Finger Service (11.2-) | |
| PCI 3.0 IOS Finger Service (11.3-12.0) | |
| PCI 3.0 IOS Finger Service (12.1+) | |
| PCI 3.0 IOS HTTP Server | |
| PCI 3.0 IOS Identd Service | |
| PCI 3.0 IOS Min Password Length 7 characters | |
| PCI 3.0 IOS Min Password Length 7 characters policy | |
| Save | Cancel Clear All |

- Select the rules that you want to add or not by clicking on the check box. Click Save. Note: To familiarize yourself with this feature, you can choose any number of the rules below for your Cisco IOS devices:
 - a. PCI 3.0 IOS BOOTP Server disable
 - b. PCI 3.0 IOS CDP Service
 - c. PCI 3.0 IOS HTTP Server
 - d. PCI 3.0 IOS Min Password Length 7 characters

If you have Cisco NX-OS devices, you can choose any number of the rules below:

- a. PCI 3.0 IOS/NX-OS SNMP v1 and v2 obsolete
- b. PCI 3.0 NX-OS CDP Service
- c. PCI 3.0 NX-OS Disable NTP
- d. PCI 3.0 NX-OS HTTP Server

| Ple | ase select the rules you would like to add |
|-----|---|
| | PCI 3.0 IOS BOOTP Server disable |
| | PCI 3.0 IOS CDP Service |
| - | PCI 3.0 IOS Console Exec 15 Minute Timeout |
| | PCI 3.0 IOS Console Local or AAA Login |
| | PCI 3.0 IOS Disable MOP |
| | PCI 3.0 IOS Disable NTP |
| | PCI 3.0 IOS Enable Secret |
| | PCI 3.0 IOS Finger Service (11.2-) |
| | PCI 3.0 IOS Finger Service (11.3-12.0) |
| | PCI 3.0 IOS Finger Service (12.1+) |
| | PCI 3.0 IOS HTTP Server |
| 0 | PCI 3.0 IOS Identd Service |
| | PCI 3.0 IOS Min Password Length 7 characters |
| | PCI 3.0 IOS Min Password Length 7 characters policy |
| | PCI 3.0 IOS PAD Service |
| | Save Cancel Clear All |

 Click on the Policy Deployment tab to deploy the policy to the chosen device group. Notice the LabCore device group is selected. The LabCore device group is a user-defined device group and is used as an example. The Save button will be ungrayed when a change is detected. Click Save if needed.



7. Navigate to Network Analysis → Policy Compliance. By default, all deployed policies will be displayed for the selected device group. The status on the Policy Compliance screen will be 'Deployed' after initially deploying a policy and the status will only update when analysis is complete. It may take a few minutes before the newly created policy returns data.

| | talabeta Crist | | inpliance renound | | | | | | | | | - |
|-----------------------|----------------|-------------|-------------------|-----|------------|--------------|--------------|--------------|--------------|-----------------|----------------|---------------------------|
| LabCore 2017-04-05 | | | | | | | | | | | 3 | Search |
| earch | | | | | | | | | | Views · Filters | Policies 🔹 🎜 💐 | App Servers (16) |
| - | IP Address | 2009-A-0022 | 2009-A-0026 | ADV | DISA-JUNOS | DSA-CIRv7r19 | DSA-CISv7r19 | DSA-CL2SW1.9 | DSA-CPRv7r19 | DSA-CPSv7r19 | FWBR11 IL28 | IT Services (4) |
| ore-6506 | 10.60.0.1 | X | 2 | 1 | 12 | 2 | X | 7 | 2 | X | | LabCore (14) |
| ne-3560-48-p2r3-25.m | 10.60.0.11 | | | | 12 | 2 | x | 12 | 2 | × | | Network Management (3) |
| ne-3750-48-p4r1-22.m | 10.60.0.12 | 121 | 2 | 2 | 2 | 2 | 181 | × | 12 | 121 | | Network Pending (5) |
| 4r2-n3k.m | 10.60.0.13 | 8 | 2 | 2 | 12 | 2 | 12 | 12 | 12 | 2 | | NIOS (34) |
| 3750-vlan-patch.m | 10.60.0.31 | | 2 | 2 | 2 | 2 | 12 | × | 2 | 2 | X | Routing (12) |
| omp3750 | 10.60.3.34 | | 2 | 1 | 2 | 2 | × | | 2 | × | X | Security (3) |
| adev-c2960.m | 10.60.14.252 | 2 | 2 | 2 | 2 | 191 | 2 | 2 | 2 | | | UNKNOWN (150) |
| witchf804b7 | 10.60.18.237 | 2 | 2 | 8 | 12 | 2 | [2] | 2 | 1921 | 122 | | Workstations w/o SNMP (32 |
| ack2.acme.com | 10 60 30.53 | 12 | | 2 | 121 | 12 | × | [2] | | × | X | |
| et-ewitch | 10.60.30.253 | | 2 | 1 | 2 | 2 | × | 2 | 12 | × | X | |
| KO13-kc | 10.60.30.254 | 2 | 2 | 2 | 2 | 192 | × | 12 | 2 | × | X | |
| sco-p4r3-34 | 10.60.136.31 | | 2 | 1 | 12 | 12 | × | 12 | 8 | × | X | |
| 4r3-31.kkptj-labs.com | 10.60.192.250 | | 12 | 2 | 2 | 19 | 2 | × | 2 | 12 | X | |
| sco-p4r1-29 | 10.60.192.253 | | 2 | 1 | 2 | 2 | X | 12 | 12 | X | X | |
| | | | | | | | | | | | | |

- Infoblox 💸 Dash 4 4 0 Select Device Group F - 🍓 All Devices (421) Search es • 2 A Views · Filt Name 7/19 IP Add <u>10.60.0.1</u> 10.60.0.11 core-6506 ? 1 0 0 0 ? IAVA 2009-A-0022 X 2 2 2 × × ? tme-3560-48-p2r3-25.m nt (3) IAVA 2009-A-0026 tme-3750-48-p4r1-22.m p4r2-n3k.m 2 2 × Advisories DISA v7, r1.9 JUNOS 10.60.0.12 (17) 10.60.0.13 ? ? cj3750-vlan-p comp3750 10.60.0.31 1 ? x ? DISA v7, r1.9 Cisco Infr 8 10.60.3.34 2 2 2 DISA v7, r1.9 Cisco Infr ure Switch DISA v7, r1.9 Cisco L2 Switch DISA v7, r1.9 Cisco Perimeter Ro sedev-c2960.n 10.60.14.252 2 NMP (32) 2 2 2 2 switchf804b7 10.60.18.237 3 2 2 2 DISA v7, r1.9 Cisco Perimeter Switch DISA v8, r11 STIG Firewall stack2.acme 10.60.30.53 12 2 × 2 x x x x tost-switch 10.60 30.253 1 2 2 2 X X X 2 2 2 2 2 2 2 DISA v8, r11 STIG Infrastructure Layer 2 Switch DISA v8, r11 STIG Infrastructure Layer 3 Switch SKO13-kc ? 10.60.30.254 ? ? 2 2 csco-p4r3-34 10.60.136.31 DISA v8, r11 STIG Infrastructure Router × p4r3-31.kkptj-labs.com 10.60,192,250 1 ? 2 ? ? × NSA 1.1c IOS osco-p4r1-29 10.60.192.253 1 1 DISA v8, r11 STIG Network Devices PCI DSS 1.2 10S PCI DSS 2.0 105 PCI DSS 3.0 IOS/NX-OS PCI Policy 1 of 1 | | | | Displaying 1 - 14 of 14 I Page //10.60.16.9 2017-04-05 15:15
- 8. Click on the Policies drop down menu to select the PCI Policy.

9. The following should appear.

| Andrew Control Brance Transmitt Brance Transmitt Brance Transmitt Andrew Transmitt A | LabCore 2017-04-05 | | | | | | | | | | | 0 | 3001.31 |
|---|--|---|---|--|---|--|--|---|---|---|---|--|---|
| each Ivines Falles Addserved Name Nam | olicy: PCI Policy escription: This policy is reated. You should use th bund at: https://www.pcise | provided to the user s policy without modi curitystandards.org/ | as is, and is meant as a fication only after you h | a general interpretat ave reviewed it and | ion of the PCI DSS 3 determined that it de | 0.0 framework. The fu bes or does not apply | nction of this policy is to your specific nee | s to provide the user ds. For further refere | with a starting point nce to more detailed | from which a more de PCI compliance requ | stailed and specific or iroments, please che | Return to Policy View impliance effort can be ck PCI documentation | - SAII Devices (421) App Servers (16) IT Services (4) |
| min P Address 054AA-03 054C0+031 054C0+031 054C0+031 054C0+031 054BAD-031 054TP-031 054T | iearch | | | | | | | | | | Views • Filters | Policies 🔹 🎜 🦂 | NAME ONLY (137) |
| 9x9-500 950-01 92 | lamo | IP Address | 105-000-033 | IOS-BTP-031 | IOS-CDP-031 | IOS-CON-035 | IOS-CON-036 | IOS-ENA-031 | 108-LOG-032 | IOS-NMOP-031 | IOS-NTP-039 | IOS-PAD-031 IOS-S | Network Management (3) |
| wo390-49-02-32.m 19.502.0.11 2 | ore-6506 | 10.60.0.1 | X | X | X | 1 | X | X | 1 | 8 | 8 | | Network w/o SNMP (17) |
| e 3750 445 pert 22.m 10.802.12 22 23 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | e-3560-48-p2r3-25.m | 10.60.0.11 | × | X | X | 1 | × | × | 1 | 8 | 53 | | NIOS (34) |
| 10.20.2.1 X | e-3750-48-p4r1-22.m | 10.60.0.12 | × | × | x | 1 | x | x | 1 | 5× | 583 | | Security (3) |
| mg3730 10.802.24 24 24 24 24 24 24 24 24 24 24 24 24 2 | 750-vlan-patch.m | 10 60 0 31 | × | × | × | I | × | 1 | 1 | X | 1 | | Switching (19) |
| 10.20.20:23 2 <td< td=""><td>mp3750</td><td>10.60.3.34</td><td>×</td><td>×</td><td>X</td><td>2</td><td>×</td><td>×</td><td>1</td><td>1</td><td>28</td><td></td><td>Workstations w/o SNMP (32</td></td<> | mp3750 | 10.60.3.34 | × | × | X | 2 | × | × | 1 | 1 | 28 | | Workstations w/o SNMP (32 |
| 10.60.00.253 X X X Y X X Y X Y X Y <t< td=""><td>ack2.acme.com</td><td>10.60.30.53</td><td>X</td><td>X</td><td>X</td><td>1</td><td>X</td><td>1</td><td>1</td><td></td><td></td><td></td><td> (at</td></t<> | ack2.acme.com | 10.60.30.53 | X | X | X | 1 | X | 1 | 1 | | | | (at |
| CO13-kc 10.50.202.54 X | st-switch | 10 60 30 253 | × | × | × | 1 | × | X | 1 | 583 | 1 | | |
| so p4/1-34 10.80.152.21 21 22 23 24 24 24 25 27 | 013-kc | 10 60 30 254 | × | × | × | 2 | × | × | I | × | × | | |
| rs 31 Abrij-bale com 10.80.192.253 20 20 20 20 20 20 20 20 20 20 20 20 20 | co-p4r3-34 | 10 60.136.31 | 2 | × | × | 1 | × | | 1 | | | | |
| 00-941-23 10.50.192.253 🕢 🕅 🕅 🕅 🕅 🕅 🗭 🗭 🚺 | r3-31.kkptj-labs.com | 10.60.192.250 | X | X | X | | X | X | | | 1 | | |
| | ico-p4r1-29 | 10.60.192.253 | | X | X | 1 | X | | 1 | 1533 | 1538 | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

- 10. You can move the mouse over to any of the colored boxes to get detailed information of the policy analysis or you can click on any of the boxes to get more detail in a new window. Here is a legend of the various colored boxes:
 - a. Red X: Error
 - b. Blue X: Info
 - c. Yellow X: Warning
 - d. Green √: Pass
- 11. To run a report navigate to Reports → Report Gallery and move the mouse pointer over the Policy Compliance Summary report.



12. Click on the 'Run' link. Select the device group and then click on the 'Next' button.

| Policy Compliance | Summary Repo | t | | | | \mathbf{x} |
|--|--------------------|---|------------------|----------------|--------------|--------------|
| A constraint of the second sec | | | Step 1 of 2: Sel | lect Time Vari | ables and De | vice Groups |
| Date: | 10/20/2020 | 8 | | | | |
| Period: | Daily | | | | | |
| Device Groups | Devices | | | | | |
| Search | | | | | | |
| - SAII Devices (8 | 9) | | | | | |
| aazhar (1 | 4) | | | | | |
| – 🍓 All Cisco | Gear (44) | | | | | |
| Cisco | _Switch_Demo (6) | | | | | |
| PGrac | ia (0) | | | | | |
| Sif (8) | | | | | | |
| | (8) | | | | | |
| App Serv | ers (8) | | | | | |
| Basic Roy | ers w/o SNMP (2) | | | | | |
| Branch Si | witches (8) | | | | | |
| Building | 708 (15) | | | | | |
| Cisco AP | s (0) | | | | | |
| Cisco IO | S (25) | | | | | |
| | | | | | | |
| Company | / 1 (0) | | | | | |
| End of Su | pport Devices (11) | | | | | |
| Firewall (| 6) | | | | | |
| fl switches | s (6) | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | < Previous | Next > | Cancel |

13. Select the policies that you want to run by highlighting the selected policy and clicking on the right arrow. Click on the 'Run' button.

| 1 Transmission Section Section Section 1 Section Section Section Section 1 Section Section Section Section 2 Section Section Section Section 3 Section Section Section Section | | | Step 2 of 2: Select Polici |
|--|----|--|----------------------------|
| Policies DISA v7, r1.9 JUNOS DISA v8, r20 STIG Firewall DISA v8, r20 STIG Infrastructure Layer 2 Switch DISA v8, r20 STIG Network Devices DISA v8, r21 STIG Infrastructure Layer 3 Switch DISA v8, r21 STIG Infrastructure Router DISA v8, r23 STIG Perimeter L3 Switch DISA v8, r23 STIG Perimeter Router DTS Operations Policy DTS PCI Security Policy DTS Sample Rules enable External Logging Global Policy Grego HoR IOS Blocked End Host Hostname policy bdb IAVA 2009-A-0022 IAVA 2009-A-0026 IB_10127 High CVE-2018-5743 IB_10472 High CVE-2019-1477 IB_10622 Med CVE-2019-11478 | 00 | Selected Policies DTS PCI Security Policy | Clear |

14. The report will show on the screen. At the upper left of the screen, you can choose to download the report in PDF, Excel, or MS Word format in addition to printing the report.



15. Click on the schedule button under the Polcy Comp[lance Summary report to schedule the report. Select the device group. Click Next.

| Policy Compliance | Summary Report | 8 | (|
|---|---|---|----|
| | Bit (Amp) Bi | Step 1 of 4: Select Time Variables and Device Group | os |
| Date: Period: | 10/20/2020 | | |
| Device Groups | Devices | | |
| Search | | | - |
| - All Devices (8 aazhar (1 - All Cisco Cisco Cisco Sif (8) Sif (8) App Serv Basic Rou Branch Su Branch Su | 9) 4) Gear (44) _Switch_Demo (6) iia (0) (8) (8) (7) (7) (7) (7) (7) (7) (7) (7 | | |
| Cisco AP | 's (0) S (25) | | |
| Cloud (0) Company End of Su Firewall (| y 1 (0) upport Devices (11) 6) s (6) | | |
| | | < Previous Next > Cancel |) |

16. Select the policies that you want to run by highlighting the selected policy and clicking on the right arrow. Click on the 'Next' button.

| Policy Compliance Summary Report | | | | × |
|---|----|--|----------------|-----------------|
| | | | Step 2 of 4: S | Select Policies |
| Policies DISA v7, r1.9 JUNOS DISA v8, r20 STIG Firewall DISA v8, r20 STIG Infrastructure Layer 2 Switch DISA v8, r20 STIG Network Devices DISA v8, r21 STIG Infrastructure Layer 3 Switch DISA v8, r21 STIG Infrastructure Router DISA v8, r23 STIG Perimeter L3 Switch DISA v8, r23 STIG Perimeter Router | | Selected Policies DTS PCI Security Policy | | Clear |
| DTS Operations Policy DTS PCI Security Policy DTS Sample Rules enable External Logging Global Policy Grego HoR IOS Blocked End Host Hostname policy bdb | 00 | | | |
| IAVA 2009-A-0022 IAVA 2009-A-0026 IB_10127 High CVE-2018-5743 IB_10472 High CVE-2018-10239 IB_10531 Low CVE-2019-6469 IB_10622 High CVE-2019-11477 IB_10622 Med CVE-2019-11478 | | | | _ |
| | | < Previous | Next > | Cancel |

17. Enter the email address of the destination of this report. Click Next.

| Policy Compliance Sum | mary Report | \mathbf{X} |
|--|--|---------------------------------------|
| Antipation of the second second | | Step 3 of 4: Select Report Scheduling |
| Report Name: | Policy Compliance Summary | |
| To Emails: | | |
| To Users: | InfobloxTest InfobloxTest () Japan tokyo () MohammadTest MohammadTest () NETMRISPT-4456 NETMRISPT-4456 () Ahmad Abou Zaher (aabouzaher@infoblox.com) | |
| Output Format: | pdf | * |
| Recurrence Pattern: | Weekly | |
| Execution Time: | 6:00 AM | |
| Sunday | Tuesday 🔲 Thursday 🔲 Saturday | |
| Monday 🔲 | Wednesday 🔲 Friday | |
| | | |
| | | < Previous Next > Cancel |

18. Verify the settings of the scheduled report. If configurations are correct, click Schedule.

| Policy Compliance Su | mmary Report | 8 |
|----------------------|-----------------------------|--|
| | | Step 4 of 4: Summary of Scheduled Report |
| Report Name: | Policy Compliance Summary | |
| Date: | 10/20/2020 | |
| Period: | Daily | |
| Device Groups: | Cisco IOS | |
| Devices: | | |
| Policies: | DTS PCI Security Policy | |
| To Emails: | | |
| To Users: | 715 | |
| Schedule: | Weekly - Monday at 06:00 AM | |
| | | |
| | | < Previous Schedule Cancel |

DISA-STIG Compliance

STIGs are nothing more than alternate configurations that make commonly used applications more secure. All DoD IT assets must meet STIG compliance in some fashion before they are allowed to operate on DoD networks. In the example below, we use a DISA STIG policy for layer 2 switches. The following instructions will show you how to implement DISA STIGs compliance:

1. Navigate to Config Management → Policy Design Center → Policies → DISA v8,rll STIG Infrastructure Layer 2 Switch.

| Oblox 💸 Dashboard Network Analysis | s Network Explorer Config Man | agement Reports | | A 🕸 |
|---|---|---|----------|-----|
| Config Archive Confi | ig Search Job Management Policy I | Design Center | | |
| | 4 | | | 3 |
| Add Delete Coov Import Export Print | | Default Statu | | |
| Policies | Compared and the second s | | | |
| Search | Layer 2 Switch | Name | Severity | |
| E IAVA 2009-A-0026 | Short Name: | B DISA v8, r11 NET0230 - Network element is not password protected | error | |
| Advisories | IL2Sw8R11 | DISA v8. r11 NET0433 - The device is not authenticated using an AAA server. | error | |
| DISA v7, r1.9 JUNOS | Author: | B DISA v6, r11 NET0700 - Operating system is not at a current release level - Error | error | |
| DISA V7, r1.9 Cisco Infrastructure Router | Infobiox, Inc. | T DISA v8 r11 NET0600 - Passwords are viewable when displaying the config | ermr | |
| DISA v7, r1.9 Cisco L2 Switch | Description: | DIGA VE rt1 NET0740. LTTP reserve is not disabled | arror | |
| DISA v7, r1.9 Cisco Perimeter Router | Implementation Guide Version: 8 | | eitu | |
| DISA v7, r1.9 Cisco Perimeter Switch | Release: 11 Date: 27 Jul 2012 | DISA v8, r11 NET0812 - Two NTP servers are not used to synchronize time. | error | |
| E DISA v8, r11 STIG Firewall | View Policy Properties | DISA v8, r11 NET0813 - NTP messages are not authenticated. | error | |
| E DISA v8, r11 STIG Infrastructure Layer 2 Switch | Read Only | B DISA v8, r11 NET0820 - DNS servers must be defined for client resolver. | error | |
| DISA v8, r11 STIG Infrastructure Layer 3 Switch | | B DISA v8. r11 NET0890 - SNMP access is not restricted by IP address. | error | |
| NSA 1.1c IOS | Device Filter for Policy | B DISA v8, r11 NET0894 - Network element must only allow SNMP read access | error | |
| DISA v8, r11 STIG Network Devices | 1: (devicevendor = 'Cisco') | B DISA v8, r11 NET0991 - The OOBM interface not configured correctly. | info | |
| PCI DSS 2.0 IOS | 2: (devicevendor = 'Juniper') | | | |

2. Make sure the selected DISA STIG policy is highlighted. Click on the Copy button to copy this default policy to a user created policy. Fill out the Policy Name, Short Name (Short Name is limited to 12 characters), and Author. Click Save.

| Policy Name: | STIG Policy | | |
|--|-------------------------------------|-----|--|
| Short Name: | STIG Policy | | |
| Author: | тме | | |
| Description: | | | |
| Lujei L Owneen | security recrimed implementation of | luc | |
| Version: 8 Release: 11 Date: 27 Jul 20 | 12 | | |

3. Highlight the newly created policy called STIG Policy.

| Config Archive Config | Search Job Management Policy D | esign Center | | |
|--|--|---|----------|------------|
| mary Rules Policies Policy Deployment | | | | |
| Delete Copy Import Export Print | _ | | | Default St |
| licies | STIG Policy | Rules in this Policy | | |
| 1AVA 2009-A-0022 | Short Name: | Name | Severity | |
| IAVA 2009-A-0026 | STIG Policy | BISA v8, r11 NET0230 - Network element is not password protected | error | |
| Advisories | Author: | B DISA v8, r11 NET0433 - The device is not authenticated using an AAA server. | error | |
| DISA v7, r1.9 JUNOS DISA v7, r1.9 Cisco Infrastructure Router | TME | II DISA v8, r11 NET0700 - Operating system is not at a current release level - Error | error | |
| DISA v7, r1.9 Cisco Infrastructure Switch | Description: | B DISA v8, r11 NET0600 - Passwords are viewable when displaying the config | error | |
| DISA v7, r1.9 Cisco L2 Switch | Layer 2 Switch Security Technical Implementation Guide Version: 8 | B DISA v8, r11 NET0740 - HTTP server is not disabled | error | |
| DISA v7, r1.9 Cisco Perimeter Router | Release: 11 Date: 27 Jul 2012 Edit Policy Properties | B DISA v8, r11 NET0812 - Two NTP servers are not used to synchronize time. | error | |
| DISA v8, r11 STIG Firewall | | DISA v8, r11 NET0813 - NTP messages are not authenticated. | error | |
| DISA v8, r11 STIG Infrastructure Layer 2 Switch | | II DISA v8. r11 NET0820 - DNS servers must be defined for client resolver. | error | |
| DISA v8, r11 STIG Infrastructure Layer 3 Switch | Device Filter for Policy | I DISA v8. r11 NET0890 - SNMP access is not restricted by IP address. | error | |
| IDISA V6, F11 S FIG Intrastructure Router | 1000.101.5 | DISA v8. r11 NET0894 - Network element must only allow SNMP read access | error | |
| DISA v8, r11 STIG Network Devices | 1: (devicevendor = 'Cisco') 2: (devicevendor = 'Juniper') | DISA v8. r11 NET0991 - The QOBM interface not configured correctly. | info | |
| PCI DSS 2.0 IOS | | 1 DISA v8 r11 NET1823 - There is no authentication required for cooscie access | error | |
| PCI DSS 3.0 IOS/NX-OS | | 1 DISA v8 r11 NET1824 . The console part does not limaged after 10 minutes | arror | |
| DISA v6, r11 STIG Perimeter L3 Switch | | DISA ve rt1 NET1820. The content of an electric and deabled. Error | arror | |
| DISA v8, r11 STIG Perimeter Router | | DISA v8 r11 NET1845 - SSM assessor timeout is out 60 accords or lass - Error | arror | |
| SANS IOS | | DISA V8 r11 NET1635 - Management connections must applied these * Error | 9777 | |
| STIG Policy | | DISA v8 r11 NET0340 - Looin hanner is non-avietant or not OOD approval | APPO | |
| | | H DISA v9 v11 NET1927 Assessment exceptions are not restricted | ana. | |
| | | DIDA 20, 111 No. 1 1037 * Weinegeneens Connections are not restricted. DIDA 20, 111 No. 1 1037 * Weinegeneens Connections are not restricted. | uno. | |
| | | Drok vo, r11 Nc 11040 - Son login exempts value is greater than 3 - Error | error | |
| | | DISA V9, F11 NE 11947 - The network element must not allow SSH Version 1 | error | |
| | | DISA V6, F11 NE11660 - An insecure version of SNMP is being used. | error | |

4. Click on the Edit button on the lower right corner of the screen to edit this policy and the following screen appears:

| Select Rules |
|---|
| Please select the rules you would like to add |
| DISA v8, r11 NET-VLAN-005 - VLAN 1 traffic traverses across unnecessary trunk - Error |
| DISA v8, r11 NET-VLAN-005 - VLAN 1 traffic traverses across unnecessary trunk - Info |
| DISA v8, r11 NET-VLAN-006 - The VLAN1 is being used for management traffic. |
| DISA v8, r11 NET-VLAN-007 - Ensure trunking is disabled on all access ports. |
| DISA v8, r11 NET-VLAN-008 - A dedicated VLAN is required for all trunk ports. |
| DISA v8, r11 NET-VLAN-009 - Access switchports are assigned to the native VLAN - Er |
| DISA v8, r11 NET-VLAN-009 - Access switchports are assigned to the native VLAN - Info |
| DISA v8, r11 NET-VLAN-023 - NET-VLAN-023 |
| DISA v8, r11 NET-VLAN-024- Upstream access not restricted for non-802.1x VLAN |
| DISA v8, r11 NET0162- AG ingress ACL is not configured to secure enclave. |
| DISA v8, r11 NET0164 - AG router has a routing protocol to the enclave. |
| DISA v8, r11 NET0166 - AG Network IP adresses are advertised in enclave |
| DISA v8, r11 NET0167 - AG must adhere to PPS boundary 12 and 14 policies |
| DISA v8, r11 NET0190 - LAN addresses are not protected from the public. |
| UISA v8, r11 NET0230 - Network element is not password protected |
| Save Cancel Clear All |
| Save Cancel Clear All |

- Select the rules that you want to add by clicking on the check box. Click Save Note: To familiarize yourself with this feature, you can choose any number of the rules below for your Cisco IOS devices:
 - a. DISA v8, r11 NET0230 Network element is not password protected
 - b. DISA v8, r11 NET0600-Passwords are viewable when displaying the config
 - c. DISA v8, r11 NET0710-The Cisco discovery protocol (CDP) is not disabled
 - d. DISA v8, r11 NET0740-HTTP server is not disabled

| Se | lect Rules | × |
|-----|---|---|
| Ple | ase select the rules you would like to add | |
| 1 | DISA v8, r11 NET-VLAN-005 - VLAN 1 traffic traverses across unnecessary trunk - Error | |
| | DISA v8, r11 NET-VLAN-005 - VLAN 1 traffic traverses across unnecessary trunk - Info | |
| | DISA v8, r11 NET-VLAN-006 - The VLAN1 is being used for management traffic. | |
| | DISA v8, r11 NET-VLAN-007 - Ensure trunking is disabled on all access ports. | |
| | DISA v8, r11 NET-VLAN-008 - A dedicated VLAN is required for all trunk ports. | |
| | DISA v8, r11 NET-VLAN-009 - Access switchports are assigned to the native VLAN - Er. | |
| | DISA v8, r11 NET-VLAN-009 - Access switchports are assigned to the native VLAN - Info | |
| | DISA v8, r11 NET-VLAN-023 - NET-VLAN-023 | |
| | DISA v8, r11 NET-VLAN-024- Upstream access not restricted for non-802.1x VLAN | |
| | DISA v8, r11 NET0162- AG ingress ACL is not configured to secure enclave. | |
| | DISA v8, r11 NET0164 - AG router has a routing protocol to the enclave. | |
| | DISA v8, r11 NET0166 - AG Network IP adresses are advertised in enclave | |
| | DISA v8, r11 NET0167 - AG must adhere to PPS boundary 12 and 14 policies | |
| | DISA v8, r11 NET0190 - LAN addresses are not protected from the public. | |
| | DISA v8, r11 NET0230 - Network element is not password protected | |
| | Save Cancel Clear A | 1 |

 Click on the Policy Deployment tab to deploy the policy to the chosen device group. Notice the LabCore device group is selected. The Save button will be ungrayed when a change is detected. Click Save if needed.

| -Lab | Update Available: 1 HotFix(es) | FindIT Q User: admit |
|---|--|--|
| Oblox 😵 Dashboard Network Analysis | Network Explorer Config Management Reports | A & |
| Config Archive Config S | earch Job Management Policy Design Center | |
| | | |
| Dates Deliver Deliver Deliver Destaurant | | |
| mary Rules Policies Policy Deployment | | |
| Policies | Policy: STIG Policy | |
| Search | Description: Layer 2 Switch Security Technical Implementation Guide Version: 8 Release: 11 Date: 27 Jul 20 Device Filter Price 1 or 2 | 012 |
| E IAVA 2009-A-0022 | Device Finer, Role, 1 or 2 | |
| E IAVA 2009-A-0026 | 1: (devicevendor = 'Cisco') 2: (devicevendor = 'Lucioo') | |
| Advisories | 2. (ocaricaterioni - aniiher) | |
| DISA v7. r1.9 Cisco Infrastructure Router | | |
| DISA v7, r1.9 Cisco Infrastructure Switch | | |
| E DISA v7, r1.9 Cisco L2 Switch | Search | |
| DISA v7, r1.9 Cisco Perimeter Router | Name | Count |
| DISA v7, r1.9 Cisco Perimeter Switch | 3 Al Devices | |
| DISA v8, r11 STIG Infrastructure Laver 2 Switch | App Servers | 1 |
| DISA v8, r11 STIG Infrastructure Layer 3 Switch | App Servers w/o SNMP | |
| DISA v8, r11 STIG Infrastructure Router | IT Services | |
| NSA 1.1c IOS | TT Services w/o SNMP | |
| DISA v8, r11 STIG Network Devices | V LabCore | |
| PCI DSS 2.0 IOS | NAME ONLY | 1 |
| PCI DSS 1.2 IOS | Network Low-Level | |
| DISA v8, r11 STIG Perimeter L3 Switch | Network Management | |
| DISA v8, r11 STIG Perimeter Router | Network Pending | |
| SANS IOS | Network w/o SNMP | 1 |
| PCI Policy | E NIOS | |
| Es all's Policy | Dopumizers | |
| | E south | |
| | Security Control | |
| | - Switching | 1 |
| | I UNKNOWN | 14 |
| | | Dente de Constante de Constan |

7. After waiting 10 minutes or more for processing, navigate to Network Analysis → Policy Compliance. By default, all deployed policies will be displayed for the selected device group.

8. Click on the Policies drop down menu to select the STIG Policy.

| LabCore 2017-04-07 Versi - Filters Policies Search Name IP Address IL25w6R11 IRoudiR11 IRoudiR11 PL3sw6R11 StriG Policy Image: Address and Address | Starth Starth <t< th=""><th></th><th>Issues Ch</th><th>anges Policy Co</th><th>mpliance Perfor</th><th>mance</th><th></th><th></th><th></th><th></th><th></th><th>Select Device Group</th></t<> | | Issues Ch | anges Policy Co | mpliance Perfor | mance | | | | | | Select Device Group |
|--|---|-----------------------|---------------|-----------------|-----------------|-----------|-----------|-----------|-------------|-----------------|----------------------|-----------------------------|
| Name IP Address L35w8R11 Rout8R11 PL3sw8R11 PL3sw8R11 PL3sw8R11 PL3sw8R11 STG Policy I A I Name ID 50.0.1 X <th>Vence Filters Policie </th> <th>LabCore 2017-04-07</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>0</th> <th>Search</th> | Vence Filters Policie | LabCore 2017-04-07 | | | | | | | | | 0 | Search |
| PAddress B_159wBR11 B_05WBR11 PR0vBW11 STIS Policy PA corre-6005 1040.0.1 X | IL3.SwdR11 IROudB11 PL3.SwdR11 PROudB111 STIG Policy Ø IS IS IS IS IS IS IS IS IS IS < | Search | | | | | | | | Views • Filters | Policies • 2 3 | - GAI Devices (419) |
| ore-8001 10.80.0.11 IM | X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X | lame | IP Address | IL2Sw6R11 | IL3Sw6R11 | IRout8R11 | PL3Sw8R11 | PRout8V11 | STIG Policy | | IA 💟 | |
| ne 3560-48-p24-32.5.m 10.60.0.12 C C C C C C C C C C C C C C C C C C C | Image: Section of the section of t | ore-6506 | 10.60.0.1 | × | × | × | × | × | × | | DISA v8, r11 STIG In | frastructure Layer 2 Switch |
| ne-3730-48-p4r1-32.m 10.60.0.12 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X X | ne-3560-48-p2r3-25.m | 10.60.0.11 | × | × | X | X | x | × | | DISA v8, r11 STIG In | frastructure Layer 3 Switch |
| 3750-4an-patch.m 10.62 0.21 X X X X X X X Importance DISA V8, r11 STIG Perimeter 13 SM Importance Importance Importance DISA V8, r11 STIG Perimeter 13 SM Importance Importan | Image: Constraint of the constr | ne-3750-48-p4r1-22.m | 10.60.0.12 | × | × | × | × | × | × | | DISA v8, r11 STIG In | frastructure Router |
| smp3750 10.60.3.24 K <td>Image: Constraint of the constr</td> <td>3750-vlan-patch.m</td> <td>10.60.0.31</td> <td>×</td> <td>×</td> <td>×</td> <td>×</td> <td>×</td> <td>×</td> <td></td> <td>DISA v8, r11 STIG P</td> <td>rimeter L3 Switch</td> | Image: Constraint of the constr | 3750-vlan-patch.m | 10.60.0.31 | × | × | × | × | × | × | | DISA v8, r11 STIG P | rimeter L3 Switch |
| ack2 arms com 10.60.20.25 X < | Image: Constraint of the constr | omp3750 | 10.60.3.34 | × | × | × | × | × | × | | DISA v8, r11 STIG P | rimeter Router |
| st-switch 10.60.30.253 X | X | tack2.acme.com | 10.60.30.53 | × | × | X | × | × | × | | STIG Policy | |
| K013-4c 10.60.30.254 K | X | est-switch | 10.60.30.253 | × | × | × | × | × | × | | | UNKNOWN (1- |
| Scorp47-3-4 10.60.136.3.1 X X X X X X 4G-31.4kgt/sebs.com 10.60.192.250 X X X X X X scorp4r1-29 10.60.192.253 X X X X X X | | KO13-kc | 10.60.30.254 | × | × | X | × | × | × | | | Workstations |
| Kr3-31.Megi-labs.com 10.60.192.250 K <thk< th=""> <!--</td--><td></td><td>sco-p4r3-34</td><td>10.60.136.31</td><td>×</td><td>×</td><td>X</td><td>×</td><td>×</td><td>×</td><td></td><td></td><td></td></thk<> | | sco-p4r3-34 | 10.60.136.31 | × | × | X | × | × | × | | | |
| soo-p4r1-29 10.60.192.253 🗙 🔀 🕅 🕅 | | 4r3-31.kkptj-labs.com | 10.60.192.250 | × | x | X | × | × | × | | | |
| | | sco-p4r1-29 | 10.60.192.253 | X | × | x | × | x | × | | | |
| | | | | | | | _ | _ | _ | | | |

9. The following should appear.

| Policy: STIG Policy Description: Infrastructure L3 Swite Search | tch Security Technical Implement | tation Guide Version: 8 F | | | | | | | 82.0 |
|---|----------------------------------|---------------------------|----------------------|----------|---------|---------|---------|------------------------------------|-------------------|
| Search | tch Security Technical Implemen | tation Guide Version: 8) | | | | | | Ret | um to Policy View |
| Name IP Ac | | | Release: 11 Date: 27 | Jul 2012 | | | | | |
| lame IP Ac | | | | | | | Views | Filters Polici | - 2 A |
| lantan lataan | Address NET0230 | NET0433 | NET0700E | NET0600 | NET0740 | NET0812 | NET0813 | NET0820a | NET0890a |
| ore-6506 <u>10.66</u> | 60.0.1 × | × | × | × | | × | × | × | × |
| ne-3560-48-p2r3-25.m 10.6 | 60.0.11 | × | × | × | | × | × | × | × |
| ne-3750-48-p4r1-22.m 10.6 | 60.0.12 | × | × | × | × | × | × | × | × |
| 3750-vlan-patch.m 10.6 | 60.0.31 | × | × | | I | × | × | × | × |
| pmp3750 <u>10.6</u> | 60.3.34 | × | × | × | | × | × | × | × |
| tack2.acme.com 10.6 | 60.30.53 | × | 1 | × | × | × | × | × | × |
| st-switch 10.6 | 60.30.253 | × | × | × | × | × | × | × | × |
| KO13-kc 10.64 | 50.30.254 X | × | 1 | × | × | × | × | × | × |
| sco-p4r3-34 10.6 | 60.136.31 | × | × | × | 1 | × | × | × | × |
| 4r3-31.kkptj-labs.com 10.6 | 60.192.250 | × | × | × | 2 | × | × | × | × |
| sco-p4r1-29 10.64 | 60.192.253 | × | × | × | 1 | × | × | X | × |

- 10. You can move the mouse over to any of the colored boxes to get detailed information of the policy analysis or you can also click any of the boxes to get details in a new window. Here is a legend of the various colored boxes:
 - a. Red X: Error
 - b. Blue X: Info
 - c. Yellow X: Warning
 - d. Green √: Pass

11. To run the Compliance Summary report, navigate to Reports \rightarrow Report Gallery and move mouse pointer to the Policy Compliance Summary.

| ∃ Compliance | | | | | | |
|---|--|--|--|---|---|------------------------|
| Default Credentials Report The most list retreet devices that is a second with the most list retreet devices that is a second with the most list retreet devices that is a second with the most list retreet devices a specific line priod. | Display Display Image: State of the state of t | PC P | Representation of the second s | ance Details des a drailed and policy rg, and the for policy Run, Schedule | Policy Compliance Summary This report provides an overview of the policy compliance situs for all policies and the network devices against which they are deployed. | PSIRT Report - Updated |

12. Click on the 'Run' button.

| | | Step 1 of 2: Select Time Variables and Device Group |
|--|--|---|
| Date: | 04/28/2017 | |
| eriod: | Daily 🎽 | |
| Device Groups | Devices | |
| Search | | |
| End of S G IT Servic LabCore NAME C Network Network NOS (3) Coptimizz Security Security Security | upport Davices (0) tes (4) tes wio SNMP (0) (1) NLY (143) Low-Lovel (0) Management (3) Pending (5) wio SNMP (15) 5) trans (0) (12) (4) to control (0) | |
| Switchin | ng (18) | |

13. The report will show on the screen. At the upper left of the screen, you can choose to download the report in PDF, Excel, or MS Word in addition to printing the report.

| Showing page 1 o | 11 | | | | | | | | | 41.4 | B De Go to page: | - |
|--|--|---|---|---|--|--|---|---|--|---|--|---|
| Policy Compliance Summary hate Range: 2017-04-07 00:00:00 to 2017-04-07 23:59:59 here Groups: LabCore here: | | | | | | | | | | | | |
| Policy | Complia | ince By | Device | | Policy | Comp | liance | By R | ule | | | |
| Error: 79.00% —— | | | - Warning: 0.00% Jnknown: 21.00% | Int | D: 27.42% | | | — Error. — Warn — Unknc | 32.73% ling: 0.57% wwn: 11.449 | 6 | | |
| Overall Status | | Overall | ISS: 0.00% b: 0.00% Number of Device | 6 | Pass: 27,84% - | | | | | | | |
| Overall Status Name STIG Policy | | Overall Status | Iss: 0.00% | 5 | Pass: 27.84% - | |), a | | | | | |
| Overall Status Name STIG Policy | e | Overall Status | Iss: 0.00% b: 0.00% Number of Device | 8 | Pass: 27.84% - | | ä | | | | | |
| Overall Status Name STIG Policy | e unkno | Overall Status mor X | ss: 0.09% (b: 0.00%) Number of Device | 8 | Pass 27.84% - | | 4 | | | | | |
| Overall Status Name STIG Policy Compliance By | e Iunkno Policy | Overall Status mor X wm 2 | ss: 0.09% b: 0.00% Number of Device 11 3 | 5 | Pass: 27.84% - | Passad | E-mar Md | seelee | lais Ci | innad | | |
| Overall Status lame STIG Policy Compliance By lame | e Wunkno Policy IP Address | Overall Status mor X xwm 2 Vendor | ss: 0.09% b: 0.00% Number of Device 11 3 Model | 5 | Pass 27.84% - | Passed | Error Wa | ıming | Info Si | ipped | Unknown | |
| Overall Status Iame STIG Policy Compliance By Iame TIG Policy cj3750-4an- patch.m | e unkno Policy IP Address 10.60.0.31 | Overall Status mor X own 2 Vendor Cisco | Number of Device Number of Device II 3 Model catalyst37xxStack | 5 | Pass 27.84% - Statue error | Passed 44 | Error Wa 55 | ıming 1 | Info Sł 38 | ipped 7 | Unknown 0 | |
| Dverall Status Iame TIG Policy Compliance By Iama TIG Policy cj3750-vlan- pat2-n3k.m | e unkno Policy IP Address 10.60.0.31 10.60.0.13 | Overall Status mor X wm 2 Vendor Cisco Cisco | ss: 0.00% b: 0.00% Number of Device 11. 3 Model catalyst37x/Stack | 5 | Pass: 27.84% - Status error unknown | Passed 44 21 | Error We 55 5 | ıming 1 | Info \$1 38 38 | lipped 7 7 | Unknown 0 74 | |
| Dverall Status fame STIG Policy Compliance By Anne Compliance By Anne pat2-n3k.m p4t2-n3k.m p4t2-n3k.m | e unkno POlicy IP Address 10.60.0.31 10.60.192.250 | Overall Status mor X Cisco Cisco Cisco | Number of Device II 3 Model catalyst37xxStack catalyst37xxStack | s × × | Pass: 27.84% - Statue error unknown error | Passed 44 21 40 | Error Wa 55 5 5 9 | arning 1 0 1 | Info \$# 38 38 38 | lipped 7 7 7 7 | Unknown 0 74 0 | |
| Dverall Status lame STIG Policy Compliance By clama ris Policy rights.m p47-31.kept- labs.com sedev-2960.m | e unkno IP Address 10.60.0.31 10.60.013 10.60.14.252 10.60.14.252 | Overall Status mor Xvm 2 Cisco Cisco Cisco Cisco Cisco | ess 0.00% b: 0.00% Number of Device 11 3 Model catalyst37xcStack catalyst37xcStack catalyst37xcStack | s X X X | Pass: 27.84% - Status error unknown error unknown | Passed 44 21 40 22 | Error Wa 55 5 59 4 | ıming 1 0 1 | Info \$¥ 38 38 38 38 38 | iipped 7 7 7 7 | Unknown 0 74 0 74 | |
| Overall Status eams THG Policy Ame THG Policy G3750-Van- patch.m p4/2-n3k.m p4/2-n3k.kgl- labs.com sedev-c2680.m switchR0457 | e unkno IP Address 10.60.0.31 10.60.19.2.50 10.60.14.252 10.60.14.252 | Overall Status mor X wm X Cisco Cisco Cisco Cisco Cisco Cisco Cisco | Aumber of Device Number of Device 11 3 Model catalyst37xStack catalyst37xStack | | Pass: 27.84% - Statue error unknown error unknown unknown | Passed 44 21 40 22 21 | Error Wa 55 59 4 5 | uming 1 0 1 0 0 | Info 54 38 38 38 38 38 38 38 38 | lipped 7 7 7 7 7 7 | Unknown 0 74 0 74 74 | |
| Overall Status Name STIG Policy Compliance By Name STIG Policy q3750-Van- patch.m p4f2-735.km p4f2-735.km p4f2-735.km sedev-c2960.m switch180457 tms-3750-48- p4f-22.m | e unkno Policy IP Address 10.60.0.31 10.60.19.2.25(10.60.19.2.25(10.60.14.252 10.60.14.252 10.60.14.252 | Overall Status mor K wh C Cisco Cisco Cisco Cisco Cisco Cisco Cisco Cisco Cisco | Aumber of Device Number of Device 11 3 Model catalyst37xStack catalyst37xStack catalyst37xStack | s (X) (Y) (Y) (Y) (Y) (Y) (Y) (Y) (Y) (Y) (Y | Pass: 27.64% - Statue error unknown error unknown error | Passed 44 21 40 22 21 43 | Error Wa 55 59 4 5 56 | 1 0 1 0 0 1 | Info SI 38 38 38 38 38 38 38 38 | ipped 7 7 7 7 7 7 7 | Unknown 0 74 0 74 74 0 | |
| Dvorall Status Name STIG Policy Compliance By Name STIG Policy (3750-Man- patch.m p4r2-n3k.m p4r2-n3k.m p4r2-n3k.m sedev-c2960.m sedev-c2960.m sedev-c2960.m sedev-c2960.m sedev-c2960.m sedev-c2960.m | e unknow Policy IP Address 10.60.013 10.60.14.252 10.60.14.252 10.60.14.252 10.60.14.252 10.60.3254 | Overall Status mor X mor Z Vendor Cisco Cisco Cisco Cisco Cisco Cisco Cisco Cisco Cisco Cisco Cisco Cisco | Asso 0.00%. b: 0.00% Number of Device 11 3 Model catalyst37xxStack catalyst37xxStack catalyst37xxStack catalyst37xxStack catalyst37xxStack catalyst37xxStack | | Pass: 27.94% - Status error unknown error unknown error error | Passod 44 21 40 22 21 43 42 | Error Wa 55 5 5 9 4 5 5 6 5 8 | 1 0 1 0 1 0 1 1 1 | Info \$8 38 38 38 38 38 38 38 38 38 38 | lppad 7 7 7 7 7 7 7 7 7 8 | Unknown 0 74 0 74 74 0 0 0 | |

14. Click on the schedule button under the Compliance Summary Report description. Select the device group. Click Next.

| Date: 04/05/2017 Period: Daily Device Groups Devices Search • • All Devices (421) App Servers (16) App Servers (16) T Services (4) IT Services (4) • NAME ONLY (137) Network Pending (5) Network Pending (5) NOS (34) Optimizers (0) • Rowing (12) | ⊠ |
|--|----------------------------|
| Date: 04/05/2017 3 Period: Daily Device Groups Devices Search - SAI Devices (421) App Servers (16) App Servers (16) App Servers (16) T Services (4) T Services (4) T Services (4) T Services (5) NAME ONLY (137) NAME ONLY (137) Network Management (3) Network Management (3) Network Management (3) Network Management (3) Network Management (3) Not Not (4) Potimizers (0) Potimizers (0) Potimizers (0) Potimizers (0) | ariables and Device Groups |
| Period: Daily v Period: Daily v Period: Devices Search | |
| Devices Devices Search - | |
| Search | |
| | 1 |
| Security (3) Security Control (0) Switching (19) UNKNOWN (150) Video (0) | |

15. Enter the email address of the destination of this report. Click Next.

| | | Step 3 of 4: Select Report Scheduli |
|--------------------|---|-------------------------------------|
| Report Name: | Policy Compliance Summary | |
| To Emails: | management@xyzcorp.com | |
| To Users: | NetMRI Admin () dave signori () support support () tac tac () Thomas Lee (thomasl@infoblox.com) | |
| Output Format: | pdf | ~ |
| ecurrence Pattern: | Weekly | |
| Execution Time: | 6:00 AM 👻 | |
| Sunday | Tuesday 🔲 Thursday 🔲 Saturday | у |
| Monday E | Wednesday 🔲 Friday | |
| | | |

16. Verify the settings of the scheduled report. If configurations are correct, click Schedule. At this time this report will be run and sent out to the email address on the date below and the time below.

| Report Name: Pol | 1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1. | Show A of A. Summany of Schoduled Dane |
|--------------------|--|--|
| Report Name: Pol | | Step 4 or 4: Summary of Scheduled Repo |
| | icy Compliance Summary | |
| Date: 04/ | 07/2017 | |
| Period: Dai | ily | |
| Device Groups: Lab | Core | |
| Devices: | | |
| Policies: STIC | 3 Policy | |
| To Emails: ma | nagement@xyzcorp.com | |
| To Users: | | |
| Schedule: We | ekly - Monday at 06:00 AM | |

Auto Device Remediation

NetMRI triggered jobs allow a script or template with predefined or custom variables to execute against a device when a "triggering source event" occurs. Triggering sources consist of the following:

- Policy rule violations.
- Custom and standard Issues.

Note: In order for the auto device remediation to work as quickly as possible, the device must be configured to send syslog data to the NetMRI appliance. Otherwise, NetMRI will detect the change on the next change detection interval. For example, in Cisco IOS, the configuration statement is 'logging <IP address of syslog server>'.

In this example, we create a triggered script to delete any instances of SNMP community name public or private as a community string in any configuration of the devices. In this exercise, we're going to create a rule to test for the presence of the SNMP community string and test it against a device along with a script to delete the public and/or private SNMP community string.

- 1. Navigate to Config Management → Policy Design Center → Rules and look for the rule called IOS SNMP Community Strings.
- 2. Here is that rule:

| Rule Name: | Ru | le Logic Builder | | | | |
|--|-----|---|-----------------|----------------------|---|--|
| OS Sinnie Community Strings | Enf | force This Rule: If (1) | then 2 | 1 | 0 | |
| Short Name: IOS-SNMP-001 | | # Туре | | Note | | |
| Author: Infoblox, Inc. | 9 | 1 Config File Mate | ch | | | |
| Severity is error | | Must Contain AT LEA | AST ON | NE of These Lines | | |
| Description: | | ^snmp-server | | | | |
| f using SNMP, do not use default community strings. References: | Ξ | 2 Config File Mate May Not Contain Any | ch ly of Thi | ese Lines | | |
| | | ^snmp-server co | ommuni | ity (public private) | | |
| Remediation: | | | | | | |
| community strings for SNMP. | | | | | | |
| /iew Rule Properties | | | | | | |
| Read Only | | | | | | |
| Device Filter for Rule: | | | | | | |
| Rule: 1 and 2 and 3 | | | | | | |
| 2: (devicesysdescr contains 'IOS') | | | | | | |
| 3: devicetype in (Router, Switch- | | | | | | |
| (outer, owner) | | | | | | |
| | | | | | | |
| Used in these policies: NSA 1.1c IOS | | | | | | |
| SANS IOS | | | | | | |
| | | | | | | |
| | | | | | | |

Now, we're going to create a policy using that rule and test it against the devices. At this point, the rule should pass.

1. Navigate to Config Management → Policy Design Center → Policies and create a policy that uses the IOS SNMP Community String rule.

2. Click on the 'Add' button and you should see the following screen:

| Config Archive Conf | lg Search Job Management | olicy Design Center | | 0 |
|--|---|----------------------|--|--------------|
| Rules Rules Rules Rules Rules Add Delake Cary Import Export Barden Barden Barden Barden Barden Barden Barden Barden Barden Barden Barden Barden Barden Barden Barden Barden Diskov, ri rid Javodi Barden Barden Barden Diskov, ri rid Javodi Barden Barden Barden Diskov, ri rid Javodi Barden Barden Barden Diskov, ri rid Store Ortherson Barden Barden Barden Barden Diskov, ri rid Store Ortherson Barden Barden Barden Barden Diskov, ri rid Tori Imagenetic Marten Barden Barden Barden Diskov, ri rid Tori Imagenetic Marten Barden Barden Barden Diskov, ri rid Tori Imagenetic Marten Barden Barden Barden Diskov, ri rid Tori Imagenetic Marten Barden Barden Barden Diskov, ri rid Stor Perimager | Policy Name: LAA 2003-6022 Such Anno: Such Anno: Hobbox, Inc. Description: This policy processor is acceled policy and witchine is acceled policy And Such Anno Anno Anno Anno Anno Anno Anno Anno | Rules in this Policy | Exercity arror error error error error error error error error error | Defask State |

3. Enter the Policy Name, Short Name, Author, and description. Click 'Save' afterwards.

| Add Policy | | | × |
|--------------|---------------------|------|--------|
| Policy Name: | SNMP public private | | |
| Short Name: | SNMP public | | |
| Author: | tme | | |
| Description: | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | Save | Cancel |

4. Highlight the newly created policy and you should see a blank rules screen:

| Config Archive Cor | ifig Search Job Management Policy | y Design Center | | |
|---|---|----------------------|-----------|------------|
| nmary Rules Policies Policy Deployment | | | | |
| id Delete Copy Import Export Print | | | | Default St |
| arch | Policy Name: SNMP public | Rules in this Policy | | |
| [JMA 2009-A022 [JAN0009-A022 [Anisotes [DISAV, r1 9 Class Infrastructure Route [DISAV, r1 9 Class Devineter Route [DISAV, r1 9 TOR Devinetor, Lyne 2 Bench [DISAV, r1 9 TOR Devinetor, Lyne [DISAV, r1 9 TOR Devineto | Broot Name: SNMP public Title Description: Party to be some Party to be some Party to be some Party to be some Party of the some Party of the some Party of the some Control Name Party of the some Party of the s | | Saverity. | |
| | | | | |

5. Click on the Edit button in the lower right corner of the screen. A small screen will appear.

| Select Rules | \boxtimes |
|--|-------------|
| Please select the rules you would like to add | - |
| Cisco IPSec IKE Vulnerability (PIX) | |
| Cisco IPSec IKE Vulnerability (Router and Switches) | |
| Cisco IPSec IKE Vulnerability (VPN) | |
| DISA v7, r1.9 AAA Method list is not applied or implemented | |
| DISA v7, r1.9 An Infinite Lifetime key has not been implemented | |
| DISA v7, r1.9 An insecure version of SNMP is being used | |
| DISA v7, r1.9 Authentication traffic does not use loopback | |
| DISA v7, r1.9 BSD commands are not disabled | |
| DISA v7, r1.9 Configuration auto-loading must be disabled | |
| DISA v7, r1.9 Console port is not configured to timeout-10 min | |
| DISA v7, r1.9 Device must log severity levels 0 through 6 | |
| DISA v7, r1.9 Devices are not password protected for out-of-band | |
| DISA v7, r1.9 DHCP service is not disabled on premise | |
| DISA v7, r1.9 DNS servers must be defined for client resolver | |
| DISA v7, r1.9 Emergency account privilege level is not set | |
| Save Cancel Clear Al | |

6. Scroll down and click on the IOS SNMP Community Strings rule and then click Save.

| Select Rules |
|---|
| Please select the rules you would like to add |
| IOS Single Helper Address |
| IOS Single Loopback Interface |
| IOS SNMP Community Strings |
| IOS SNMP Hosts |
| IOS SNMP Loopback Source |
| IOS SNMP RW Communities |
| IOS SNTP Client |
| IOS SNTP Server |
| IOS SSH Retries |
| IOS SSH Timeout |
| IOS TCP Keepalives In |
| IOS TCP Keepalives Out |
| IOS TCP Small-Servers (11.2-) |
| IOS TCP Small-Servers (11.3+) |
| IOS TCP SYN Wait |
| Save Cancel Clear All |

7. The following screen appears:

| Infobiox 😵 Dashboard Network Analysis | Network Explorer Config M | Reports | | × \$ |
|--|--|--|----------------|------------------|
| Config Active Config Summary Rules Policies Policy Deployment Add Delete Cary Import Export Print Policies Search Edu An 2009 A 0022 Edu An 2009 A 0025 | 3 Search Job Management Police Policy Name: SNMP public SNMP public SNMP public | Nutes in this Policy Nutes in this Policy Nutes State Stat | Breadly and | Default Status |
| Andrones Disk v7, 11 a JUNO5 Disk v7, 11 a Guo J Steland Disk v7, 11 a Guo Parmite Route Disk v7, 11 a Guo Parmi | Autor: TWE Description: Policy to tea MAMP community string public. Bit Deface room teams Data Enter Device Filter for Policy Add a filter | | | |
| | | | | Test Policy Edit |

8. Test the policy against a device configuration. Click on the 'Test Policy' button on the lower right corner of the previous screen. The following small screen appears.

| Test Policy | | | | | × |
|---|--|--------------------------------|-----------------|--------------------|----------------|
| Test Against E | xisting Device | Test Against Attributes/Config | File Test Again | st Template | |
| Search | | | | | |
| All Devices App Se App Se IT Serv IT Serv LabCot | (421) rvers (16) rvers w/o SNMP (0 ices (4) ices w/o SNMP (0) • (14) DNLY (143) | 3 | | | |
| Search | E | | | | 2 |
| IP Address 🔺 | Device Name | Device Type | Device Vendor | Device Model | Device Version |
| 10.60.30.254 | SKO13-kc | Switch-Router | Cisco | catalyst37xxStack | 15.0(2)SE6 |
| 10.60.136.31 | csco-p4r3-34 | Switch-Router | Cisco | catalyst3560v248ps | 12.2(50)SE5 |
| 10.60.192.250 | p4r3-31.kkptj-lab | s.com Switch | Cisco | catalyst37xxStack | 12.2(55)SE3 |
| 10.60.192.253 | csco-p4r1-29 | Switch-Router | Cisco | catalyst37xxStack | 12.2(53)SE2 |
| 🚺 🖣 Page | 2 of 2 🕨 🕅 | Displaying 11 - 14 of 14 | Cancel | | |

9. For this example, we selected the device group 'LabCore' and then the switch with the IP address of 10.60.30.254. Click on the 'Test' button. The following screen will appear:

| Infoblo |)x 途 | Configuration Policy Test Results | |
|--|--|---|--|
| CONTROL YOUR NETW | IORK | 2017-04-17 18:02:41 | |
| Policy SNMP pu | blic | | |
| Policy to test for | the SNMP community s | tring public | |
| Pass | | | |
| Policy Summary | r | | |
| Pase | 1 (100 00%) | 1 | |
| Fail | 0 (0 00%) | | |
| Error | 0 (0.00%) | | |
| Warning | 0 (0.00%) | | |
| Info | 0 (0.00%) | | |
| Skin | 0 (0.00%) | | |
| Unknown | 0 (0.00%) | • | |
| Checked | 1 (100.00%) | • | |
| Rules Summary | : | 1 | |
| IOS SNMP Cor | mmunity Strings:IOS-SN | IMP-001 | Pass |
| IP: 10.60.30.2 Model: catalys Version: 15.0 Last Check: 2 Rule IOS SNMM If using SNMP, as a general in which a more i reviewed it and Filter: Rule: 1 and 1: (devices; 2: (devices; 3: devicet; Pass | 54 137xxStack 13 | munity strings. References: NSA; SANS 5.7.2, 5.7.3 This rule is provided to th 1.1c and SANS frameworks. The function of this rule is to provide the user wit npliance effort can be created. You should use this rule without modification of a or does not apply to your specific needs.) Router, Switch) | he user as is, and is mear th a starting point from nly after you have |
| Remediation: Do not use Logic: Running cc ^snmg Running cc ^snmg | default well-known co onfig file contains so >-server onfig file does not co -server comunity (pp | mmunity strings for SNMP. me: mtain any: blio[private) | |
| | | | |

- 10. We want to be sure that **the policy passes on this device** before deploying.
- 11. Highlight and deploy the SNMP public private policy against the LabCore device group, by checking the box next to the LabCore device group in the Policy Deployment tab, and click Save.

| Config Archive Config Se | arch Job Management Policy Design Center | |
|---|--|--------------------------------|
| nary Rules Policies Policy Deployment | | |
| 17.5.5 19 WM 2006 A 0022 20 MM 2006 A 0022 21 AAkontes 20 ISA V7, 19 JUNOS 20 ISA V7, 19 JUNOS 20 ISA V7, 19 Coco Infrastructure Bouter 20 ISA V7, 19 Coco Infrastructure Switch | Policy: SNMP public private Description: Policy to test for the SNMP community string public or private Device Filter: | |
| DISA v7, r1.9 Cisco L2 Switch | Search | |
| DISA V7, n.9 Usco Perimeter Router | Name | Cou |
| DISA v6, r11 STIG Firewall DISA v6, r11 STIG Infrastructure Layer 2 Switch DISA v6, r11 STIG Infrastructure Layer 3 Switch DISA v6, r11 STIG Infrastructure Router NSA 1.1c IOS | App Schwars App Schwars App Schwars w/o SMMP Ti Services Ti Services w/o SMMP | |
| DISA v8, r11 STIG Network Devices | V LabCore | |
| JPCI DSS 20 IGS JPCI DSS 30 (OSNX-OS PCI DSS 12 IOS DISA %, r11 STIG Perimeter L3 Switch DISA %, r11 STIG Perimeter Router SANS IOS DPC pelies | KANE ONLY Retwork Kanagement Network Rending Retwork Kensing | |
| PCI Policy | Colimbus | |
| s SMMP public private | Security Control | |
| | | Disable All Enable All Save Ca |

12. Wait for your deployed policy to pass for all devices in the LabCore device group.

| ME-Lab | | | INFOBLOX_INT | ERNAL. | | | |
|--|------------------------------|-----------------------------|-------------------|---------|-----------------|-------------|------------|
| nfoblox 💸 🛛 📭 🔤 | shboard Network | nalysis Network Explore | Config Management | Reports | | | |
| | Issues Cha | nges Policy Compliance | Performance | | | | |
| LabCore 2017-04-18 | | | | | | | 0 |
| Policy: SNMP public prive Description: Policy to test | ate for the SNMP communit | ty string public or private | | | | Return to F | Policy Vie |
| Search | | y using public or private | | | Views • Filters | Policies - | 2.8 |
| Name | IP Address | los anmo | | | | | C 4. |
| core-6506 | 10.60.0.1 | | | | | | |
| tme-3560-48-p2r3-25.m | 10.60.0.11 | | | | | | |
| tme-3750-48-p4r1-22.m | 10.60.0.12 | | | | | | |
| cj3750-vlan-patch.m | 10.60.0.31 | | | | | | |
| comp3750 | 10.60.3.34 | | | | | | |
| stack2.acme.com | 10.60.30.53 | | | | | | |
| est-switch | 10.60.30.253 | | | | | | |
| SKO13-kc | 10.60.30.254 | | | | | | |
| csco-p4r3-34 | 10.60.136.31 | | | | | | |
| p4r3-31.kkptj-labs.com | 10.60.192.250 | | | | | | |
| csco-p4r1-29 | 10.60.192.253 | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Page 1 of 1 | Displaying | 1 - 11 of 11 | | | | | |

13. Create a script to delete the SNMP public and/or private community strings. Navigate to Config Management → Job Management → Scripts. Click on the '+' button to add a script.

| Config Archive Config Search | Job Manager | ment Polic | y Design Center | ; | | |
|---|--------------|-------------|-----------------|------------|---------------------|-----------------------|
| Library Config Templates Lists Scheduled Jobs | Triggered Jo | xbs Job His | tory Custom 1 | ssues | | |
| n | | | | | | Views - Filters 🕂 🍁 🕍 |
| Name . | Language | Run Level | Created By | Updated By | Updated On Last Run | |
| 2009 Extended DST Compliance | CCS | High | admin | admin | 2017-03-13 16:15:18 | |
| Ad Hoc Command Batch | CCS | High | admin | admin | 2017-03-13 16:15:17 | |
| Assign Port to VLAN | Perl | High | admin | admin | 2017-03-13 16:15:29 | |
| Catalyst 3750 Bad Stack Switch | CCS | High | admin | admin | 2017-03-13 16:15:18 | |
| Catalyst Port ErrDisabled | CCS | High | admin | admin | 2017-03-13 16:15:18 | |
| Example 1 - Cisco Set User Password | CCS | High | admin | admin | 2017-03-13 16:15:18 | |
| Example 1 - Cisco Set User Password (Perl) | Perl | High | admin | admin | 2017-03-13 16:15:19 | |
| Example 2 - Multi-Vendor Set User Password | CCS | High | admin | admin | 2017-03-13 16:15:19 | |
| Example 2 - Multi-Vendor Set User Password (Perl) | Perl | High | admin | admin | 2017-03-13 16:15:19 | |
| Example 3 - Cisco Set Existing User Password | CCS | High | admin | admin | 2017-03-13 16:15:19 | |
| Example 3 - Cisco Set Existing User Password (Perl) | Peri | High | admin | admin | 2017-03-13 16:15:19 | |
| Example 4 - Cisco Set Duplex | CCS | High | admin | admin | 2017-03-13 16:15:20 | |
| Example 4 - Cisco Set Duplex (Perl) | Peri | High | admin | admin | 2017-03-13 16:15:20 | |
| Example 5 - Cisco Set Duplex Redux | CCS | High | admin | admin | 2017-03-13 16:15:20 | |
| Example 5 - Cisco Set Duplex Redux (Perl) | Ped | High | admin | admin | 2017-03-13 16:15:20 | |
| Example 6 - Cisco Set Port Fast | CCS | High | admin | admin | 2017-03-13 16:15:20 | |
| Example 6 - Cisco Set Port Fast (Perl) | Perl | High | admin | admin | 2017-03-13 16:15:21 | |
| Example 7 - Cisco Set Port Fast Redux | CCS | High | admin | admin | 2017-03-13 16:15:21 | |
| Example 7 - Cisco Set Port Fast Redux (Perl) | Perl | High | admin | admin | 2017-03-13 16:15:21 | |
| HTTP Server Running On Switch or Server | CCS | High | admin | admin | 2017-03-13 16:15:30 | |
| Invalid User Account Issue | CCS | High | admin | admin | 2017-03-13 16:15:21 | |
| IOS ACL Archive | CCS | High | admin | admin | 2017-03-13 16:15:22 | |

14. Enter the name of the script, run level of high, description, and the script itself. When finished, click on the 'Save & Close' button.

| dd New Scrip | ŧ | | 8 |
|--|--|--------------|--------------------|
| Tip: use the Re | equiar Expression Test page to check trigger variable and trigger te | nplates. | |
| Name: | Remove SNMP Community string public private | E3 | |
| Run Level: | High | | |
| Category: | | | |
| Description: | removes SNMP public and/or private community strings | | |
| Language: | CCS 🗸 | | |
| # Remove ######### Action: Remo Action-Comm Config 1 no som no som no som end write m | a the SNMP community string public #################################### | | |
| **** | ******* | | |
| | | Save & Close | Save Export Cancel |

15. Navigate to Config Management --> Job Management --> Triggered Jobs and click the + sign in the upper right-hand corner to add a Triggered Job.

| TME-Lab | | | NFOBLOX_INTERNAL | | | | FindIT | Q User: admin Logo |
|-----------|--|-----------------------|--------------------------------|--------------------------------------|---------------|--------------|---------------------|------------------------|
| Infoble | 🗙 😵 Dashboard Network Analysis Netwo | ork Explorer Config I | Management Reports | | | | | 4 4 0 |
| | Config Archive Config Search | Job Management | licy Design Center | | | | | |
| (| | | | | | | | |
| Serietz | Likrany Config Templater, Liste, School and Jobs | Trippered John John | History Custom Issuer | | | | | |
| Juniper | billing compared and a stream and | inggered sous | inter production of the second | | | | - | |
| Search | | | | | | | | Views • 🔶 🎜 |
| Actions | Name | Level . Enabled | Active Window Trigger Type | Trigger Event | Device Groups | Action | Created On | Updated On |
| \$ | IOS SSH Settings | High No | 24/7 Policy Rule | IOS SSH Retries | All | Schedule Job | 2015-12-10 16:49:11 | 2015-12-10 16:41 |
| \$ | Isolate Rogue DHCP Server | High Yes | 24/7 Issue | Rogue DHCP Server Located (Devices) | All | Schedule Job | 2017-03-13 16:15:38 | 2017-03-13 16:11 |
| \$ | Locate Rogue DHCP Server | High Yes | 24/7 Issue | Rogue DHCP Server Detected (Devices) | All | Auto-Run | 2017-03-13 18:15:44 | 2017-03-13 16:11 |
| - | Provision Bare Metal Device | High Yes | 24/7 Issue | Bare Metal Device Found (Devices) | Ali | Schedule Job | 2017-03-13 16:15:51 | 2017-03-13 16:11 |
| | | | | | | | | |
| 14 -4 | Page 1 of 1 🔄 🕅 Displaying 1 - 4 of 4 | | | | | | Updated | at 2017-04-18 10:46:15 |

16. Select "Policy Rule" as the Trigger Source from the drop down and select the IOS SNMP Public Private rule within the Policy Rule Selection box, and click Next.



17. Select the "LabCore" group and make sure that the "Active Time Window" indicates 24/7, and click Next.

| Triggered Job Wizard | | \mathbf{x} |
|----------------------|---|--------------------------|
| Trigger Filters | | ? |
| Device Groups: | All Devices (421) App Servers (16) IT Services (4) LabCore (11) NAME ONLY (144) | |
| Active Time Window: | 24/7 | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | < Previous Next > Cancel |

18. In the "Define Job" pane, you can add details like a custom name and a description. However, make sure that the "Enabled" box **is** checked and that you have selected script created in step 2. Click Next.

| Denne Job | | | | |
|--|----------------------------|--------------------------------|-----------------------------|------------|
| Job Name: (| Use Custom Name: | Deleting SNMP Community strin | C Use Script Name | Enabled: 🔽 |
| Job Description: | Deletes public and/or | private SNMP community strings | | |
| Scripts Templates | | Remove SNMP Communit | y string public and private | |
| earch | | | | |
| cript Name | | | | |
| rovision Bare Metal Devi | се | No input required | | |
| rovision Network | | | | |
| uarantine Device | | | | |
| darantine Device | ty string public and priva | | | |
| emove SNMP Communi | | | | |
| emove SNMP Communi eset Logging | | | | |
| emove SNMP Communi eset Logging et Interface Description | | | | |

19. From the "Schedule Job Execution" pane, make sure that you select "Run Job Immediately" from the "Trigger Action" drop down, and click Next.

| Triggered Job Wizar | rd | \times |
|---------------------|---|----------|
| 15 Schedule Job E | Execution | ? |
| Trigger Action: | Execution Run Job Immediately | • |
| | < Previous Next > | Cancel |

20. Review the properties of the job and click Save.



Testing the triggered job by changing a device configuration manually

You will log into a device via telnet and issue a couple of commands to change the configuration. The steps below would also cause a configuration backup to occur. NetMRI will not backup configurations if no changes have occurred.

- 1. Open up a terminal window on your PC.
- Telnet to a switch in the device group. In this example the switch is called SKO13-kc and the IP address is 10.60.30.254.
- 3. The username is admin and the password is 'infoblox'.
- If necessary, go into enable mode by entering "enable" at the prompt. The enable password is "infoblox".
- 5. Type "config t" at the prompt to configure the device.
- Enter the following command to add the SNMP public community string: SKO13-kc(config)# snmp-server community public ro
- 7. Exit config mode and issue a "write mem" command.

8. Leave the terminal session open, and issue a "term mon" command.



This will show you when NetMRI logs into the device and removes the SNMP statement. This should occur about 15 minutes after the change.

9. Navigate to Config Management → Config Archive and look for your configuration change.

| | Dashboard Network | k Analysis Network Ex | plorer Config Management Reports | |
|---------------|------------------------|-----------------------|--|--|
| 2 | Config Archiv | e Config Search Job | Management Policy Design Center | |
| | | | | |
| Dan ion Comun | | « | | |
| Counce Choop | | | | |
| Search | s (42E) | | | |
| App S | iervers (16) | | Config Archive | |
| IT Ser | vices (4) | | Select a Device Group Filter and Device from the list to the left | |
| LabCo | ore (11) | | Note: devices only annear in this list if config collection is enabled for | |
| NAME | ork Management (3) | | this device and a successful configuration collection has occurred. | |
| Netwo | ork Pending (5) | | | |
| Netwo | ork w/o SNMP (15) | | | |
| Routin | (35) ng (12) | | | |
| Secur | ity (4) | | | |
| earch | | 2 | | |
| Address | Device Name 🔺 | Device Type | | |
| 0.60.0.31 | cj3750-vlan-patch.m | Switch (99%) | | |
| 0.60.3.34 | comp3750 | Switch-Router (99%) | | |
| 0.60.0.1 | core-6506 | Switch-Router (99%) | | |
| 0.60.192.253 | csco-p4r1-29 | Switch-Router (99%) | | |
| 0.60.136.31 | csco-p4r3-34 | Switch-Router (99%) | | |
| 0.60.192.250 | p4r3-31.kkptj-labs.com | Switch (99%) | | |
| 0.60.30.254 | SKO13-kc | Switch-Router (99%) | | |
| 0.60.30.53 | stack2.acme.com | Switch-Router (99%) | | |
| 0.60.30.253 | test-switch | Switch-Router (99%) | | |
| 0.000.44 | tme-3560-48-p2r3-25.m | Switch-Router (99%) | | |
| 0.00.0.11 | | | | |
| 0.60.0.12 | tme-3750-48-p4r1-22.m | Switch (99%) | | |

10. Select the switch that was modified. In our example that is SKO13-kc.

| 47405 YOLH H47WOHL | Config Archive | e Config Search Ja | ob Man | agement | Policy Desi | gn Center | | | | | | |
|--------------------|---|---------------------|--------|-----------|-------------|-------------|-----------------------|-----------------------|--------------|------------------|---------------------|--|
| | | | | | | | | | | | | |
| Device Group | | | < 10. | 60.30.254 | SKO13-kc | Cisco Las | t Checked: 2017-04-18 | 8 14:00:29 Get Config | | | | |
| Contra Group | | | Ru | nning Co | nfig Saved? | Yes | | Files Archived: | 86 | Dates Back To: 2 | 2015-12-13 18:13:03 | |
| Search | | | | Actions | BL Status | Config Type | First Seen | Last Collected - | Edited By | | | |
| All Devices | (426) | | m | ö | Current | Running | 2017-04-18 13:57 | 2017-04-18 13:57 | admin | | | |
| IT Serv | ices (4) | | 177 | 8 | Current | Saved | 2017-04-18 13:57 | 2017-04-18 13:57 | admin | | | |
| LabCo | re (11) | | | * | Archived | Running | 2017-04-18 13:52 | 2017-04-18 13:52 | admin | | | |
| NAME | ONLY (148) | | PT | 45 | Archived | Saved | 2017-04-18 13:52 | 2017-04-18 13:52 | admin | | | |
| Networ | k Pending (5) | | F | ä | Archived | Running | 2017-04-18 12 23 | 2017-04-18 12 23 | admin | | | |
| Networ | es Group th All Davices (25) App Services (4) T Services (4) NARCONY (148) Network Nendrig (5) Notices Ne | | 100 | * | Archived | Saved | 2017-04-18 12 23 | 2017-04-18 12:23 | admin | | | |
| NIOS (3 | 35) | | | * | Archived | Running | 2017-04-18 12-17 | 2017-04-18 12:17 | admin | | | |
| Securit | g (12) tv (4) | | 271 | * | Archived | Sound | 2017-04-18 12-17 | 2017.04.18 12:17 | admin | | | |
| earch | | 3 | | ** | Archived | Runcica | 2017-04-18 11-33-15 | 2017-04-18 11:33-15 | admin | | | |
| our office | and the second se | L | 1 | * | Archived | Sound | 2017-04-18 11-33-15 | 2017-04-18 11-33-15 | admin | | | |
| Address | Device Name A | Device Type | R | * | Archived | Running | 2017-04-18 11-26-15 | 2017.04.18 11:26:15 | admin | | | |
| 0.60.0.31 | cj3750-vlan-patch.m | Switch (99%) | 100 | * | Archived | Savad | 2017-04-18 11-26-15 | 2017-04-18 11-28-15 | admin | | | |
| .60.3.34 | comp3750 | Switch-Router (99%) | E | * | Archived | Running | 2017-04-17 20-02 | 2017-04-17 20-02 | admin | | | |
| /.60.0.1 | core-6506 | Switch-Router (99%) | - | * | Archived | Saund | 2017-04-17 20:02 | 2017-04-17 20:02 | admin | | | |
| 60.192.253 | csco-p4r1-29 | Switch-Router (99%) | 100 | ** | Archived | Duraliza | 2017-04-17 20:02 | 2017-04-17 20:02 | aumen | | | |
| 0.60.136.31 | csco-p4r3-34 | Switch-Router (99%) | 1 | * | Archived | Running | 2017-04-17 19:49 | 2017-04-17 19:49 | thomasi | | | |
| .60.192.250 | p4r3-31.kkptj-labs.com | Switch (99%) | 100 | \$2 | Archived | Saved | 2017-04-17 19:49 | 2017-04-17 19:49 | thomasi | | | |
| .60.30.254 | SKO13-ko | Switch-Router (99%) | 불 | \$2 | Archived | Running | 2017-04-17 18:02 | 2017-04-17 18:02 | thomasi | | | |
| 0.60.30.53 | stack2.acme.com | Switch-Router (99%) | 12 | 54 | Archived | Saved | 2017-04-17 18:02: | 2017-04-17 18:02: | thomasi | | | |
| 0.60.30.253 | test-switch | Switch-Router (99%) | 12 | - | Archived | Running | 2017-04-17 17:57 | 2017-04-17 18:00: | thomasi | | | |
| 0.60.0.11 | tme-3560-48-p2r3-25.m | Switch-Router (99%) | 12 | - | Archived | Saved | 2017-04-17 17:57 | 2017-04-17 18:00: | thomasl | | | |
| 0.60.0.12 | tme-3750-48-p4r1-22.m | Switch (99%) | 12 | 4 | Archived | Running | 2017-04-17 17:18 | 2017-04-17 17:18 | thomasl | | | |
| Page | 1 of 1 P P Displaying | g 1 - 11 of 11 | 14 | Page | 1 of 2 | ▶ ▶ Disp | olaying 1 - 50 of 86 | | | | | |
| | | | | | | | | | Compare Sero | ad Davice | | |

11. Select the configuration files to compare.

| | | | | 50.30.254 S | KO13-kc | Cisco Last | Checked: 2017-04-18 | 14:00:29 Get Config | 0 | | |
|---|-------------------------|---------------------|--------------|-----------------|-----------|-------------|---------------------|---------------------|-----------|------------------------------------|--|
| vevice Group | | | Ru | nning Conf | ig Saved? | Yes | | Files Archived: | 86 | Dates Back To: 2015-12-13 18:13:03 | |
| earch | | | E | Actions BL | Status | Config Type | First Seen | Last Collected - | Edited By | | |
| All Devices | (426) | | | * | Current | Pussien | 2017-04-18 13-57 | 2017-04-18 13-57 | admin | | |
| App Se | irvers (16) ices (4) | | - | ** | Current | Cound | 2017-04-10 13.07 | 2017-04-18 13:57 | admin | | |
| Dashboard Network Analysis Config Search Inf and Concept Inf and Concept | | | | 34 | Current | Daved | 2017-04-18 13.57 | 2017-04-18 13:57 | admin | | |
| NAME | ONLY (148) | | | ** | Archived | Running | 2017-04-16 13:52 | 2017-04-18 13:52 | aomin | | |
| Networ | rk Management (3) | | | \$¥ | Archived | Savec | 2017-04-18 13:52 | 2017-04-18 13:52 | aomin | | |
| Networ | k w/o SNMP (15) | | 121 | \$ 2 | Archived | Running | 2017-04-18 12:23 | 2017-04-18 12:23 | admin | | |
| NIOS (3 | 35) | | (A 1 | \$ | Archived | Saved | 2017-04-18 12:23: | 2017-04-18 12:23: | admin | | |
| Routin | g (12) | | | * | Archived | Running | 2017-04-18 12:17: | 2017-04-18 12:17: | admin | | |
| - M Securit | (y (4) | (| | \$ | Archived | Saved | 2017-04-18 12:17: | 2017-04-18 12:17: | admin | | |
| arch | | 2 | | \$ | Archived | Running | 2017-04-18 11:33:15 | 2017-04-18 11:33:15 | i admin | | |
| ddress | Device Name 🔺 | Device Type | | \$ | Archived | Saved | 2017-04-18 11:33:15 | 2017-04-18 11:33:15 | i admin | | |
| 0.0.31 | cj3750-vlan-patch.m | Switch (99%) | | \$ | Archived | Running | 2017-04-18 11:26:15 | 2017-04-18 11:26:15 | i admin | | |
| 0.3.34 | comp3750 | Switch-Router (99%) | 0 | • | Archived | Saved | 2017-04-18 11:26:15 | 2017-04-18 11:26:15 | i admin | | |
| 90.0.1 | core-6506 | Switch-Router (99%) | | - | Archived | Running | 2017-04-17 20:02: | 2017-04-17 20:02 | admin | | |
| 30.192.253 | csco-p4r1-29 | Switch-Router (99%) | | \$ | Archived | Saved | 2017-04-17 20:02: | 2017-04-17 20:02: | admin | | |
| 50.136.31 | csco-p4r3-34 | Switch-Router (99%) | | \$ | Archived | Running | 2017-04-17 19:49: | 2017-04-17 19:49: | thomasi | | |
| 0.192.250 | p4r3-31.kkptj-labs.com | Switch (99%) | | ₽ | Archived | Saved | 2017-04-17 19:49 | 2017-04-17 19:49: | thomasl | | |
| 0 30 254 | SKO13-kc | Switch-Router (99%) | 12 | 孕 | Archived | Running | 2017-04-17 18:02 | 2017-04-17 18:02: | thomasl | | |
| 30.30.53 | stack2.acme.com | Switch-Router (99%) | E | \$ | Archived | Saved | 2017-04-17 18:02 | 2017-04-17 18:02: | thomasi | | |
| 0.30.253 | test-switch | Switch-Router (99%) | 12 | 牵 | Archived | Running | 2017-04-17 17:57 | 2017-04-17 18:00: | thomasl | | |
| 50.0.11 | tme-3560-48-p2r3-25.m | Switch-Router (99%) | E | ₽ | Archived | Saved | 2017-04-17 17:57: | 2017-04-17 18:00: | thomasi | | |
| 60.0.12 | tme-3750-48-p4r1-22.m | Switch (99%) | | 夺 | Archived | Running | 2017-04-17 17:18: | 2017-04-17 17:18: | thomasl | | |
| 4 Page | 1 of 1 k k Displayin | 1 - 11 of 11 | H | 4 Page | 1 of 2 | Displ | laving 1 - 50 of 86 | | | | |

12. Click on the 'Compare' button. Notice the change?

| Com | paring Configuration Files | |
|-------|---|---|
| Sele | cted Files | |
| | Host Device: 10.60.30.254(SKQ13-kc) File Status: Archived Saved Last Modified: 2017-04-18 12.23.01 by admin | Host Device: 10.60.30.254(SKO13-kc) File Status: Archived Saved Last Modified: 2017-04-18 13:52:09 by admin |
| Find: | view * action * Changes: 0 | Removals: 0 Additions: 1 |
| 1 | version 15.0 | 1 version 15.0 |
| 2 | no service pad | 2 no service pad |
| 3 | service timestamps debug datetime msec | 3 service timestamps debug datetime msec |
| 4 | service timestamps log datetime msee | 4 service timestamps log datetime msec |
| 5 | no service password-encryption | 5 no service password-encryption |
| | Skipping to line 374 | Skipping to line 374 |
| 374 | ip sla enable reaction-alerts | 374 ip sla enable reaction-alerts |
| 375 | logging trap debugging | 375 logging trap debugging |
| 376 | logging host 10.60.16.96 | 376 logging host 10.60.16.96 |
| 377 | 4 | 377 1 |
| 378 | snmp-server community infoblox RO | 378 snmp-server community infobiox RO |
| | | 379 snmp-server community public RO |
| 379 | a | 380 1 |
| 380 | 3 | 381 ! |
| 381 | line con 0 | 382 line con 0 |
| 382 | line vty 0 4 | 383 line vty 0.4 |
| 383 | exec-timeout 30 0 | 384 exec-timeout 30 0 |

 After this change occurred, you can navigate to Network Analysis → Policy Compliance to look for the indication of a policy compliance issue. You may need to refresh the screen until the red 'X' appears. This may take about 5 minutes.



14. Click on the red X and you get an explanation of the violation.

| | policy_status: compliance_results |
|--|---|
| Not Secure | https://10.60.16.96/webui/policy_status/compliance_results?report_type=by_device_for_rule&id=4. |
| ofoblo | v 🐟 Configuration Policy Analysis |
| NTROL YOUR NETW | харана 2017-04-18 13:54:56 |
| vice SKO13-k : 10.60.30.254 odel: catalyst3 ersion: 15.0(2) | 7xxStack SE6 7.4.10 19:64 56 |
| tule los enimp if using SNMP, and is meant a with a starting | public privato do not use default community atrings. References: NSA: SANS 5.7.2, 5.7.3 This rule is provided to the user as is a general interpretation of the NSA 1.1.c and SANS frameworks. The function of this rule is to provide the user soint from which a more detailed and specific compliance effort can be created. You should use this rule without |
| nouncation or | ly after you have reviewed it and determined that it does or does not apply to your specific needs. |
| Filter: | |
| Filter: Rule: 1 and 3 1: (devicev 2: (devices) 3: devicety) | and 3 ndor matches 'Cisco') #descr contains '105') e in (Nouter, Switch-Router, Switch) |
| Filter: Rule: 1 and : 1: (devices: 2: (devices: 3: devicety) Error Message: | : and 3 ndor matches 'Cisco') deser contair 'OS') e in (Nouter, Switch-Router, Switch) |
| Filter: Rule: 1 and 3 1: (devicev) 2: (devices) 3: devicety] Error Message: Line 379 m | and 3 naor matches 'Cisco') sedecr contains 'JOB') e in (Nouter, Switch-Mouter, Switch) e in (Nouter, Switch-Mouter, Switch) atches expression '^snmp-server community (public private)'. |
| Filter: Rule: 1 and : 1: (devices: 2: (devices: 3: devicety) Error Message: Line 379 m Remediation: | and 3 ndor matches 'Cisco') deser contais 'JSS') e in (Nouter, Switch-Router, Switch) atches expression '^snmp-server community (public (private)'. |
| Filter: Rule: 1 and : 1: (devices) 2: (devices) 3: devicety Error Message: Line 379 m Remediation: Do not use | and 3 ndor matches 'Cisco') se in (Nouter, Switch-Router, Switch) atches expression '^snmp-server community (public private)'. default well-Known community strings for SNMP. |
| Filter: Rule: 1 and 1: (devices) 2: (devices) 3: devicety Error Message: Line 379 m Remediation: Do not use Logic: | <pre>i and 3 indor matches 'Cisco') addeer contains 'OS') e in (Nouter, Switch-Router, Switch) atches expression '^snmp-server community (public private)'. default well-known community strings for SNMP.</pre> |

15. The triggered jobs process may take a few minutes to revert your changes to that specific device. Navigate to Network Analysis → Changes to view changes. Also, this change will trigger a configuration backup.

| Lai | Core 2017-04-18 / Dail | 1 | | | | | | | | 10 |
|---------|------------------------|----------------------------------|----------------------------|--------|-------------------|---------------------|-------------|---------------|--------------------------------|-------------------------------|
| Search | | _ | _ | | - | | | | Views • Filters Disp | alay · 🎝 Z |
| Ictions | Change Window - | IP Address | Name | Vendor | Model | Device Type | User | Change Method | Change Type | Confi |
| \$ | 2017-04-18 13:57:09 | 10.60.30.254 | SKO13-kc | Cisco | catalyst37xxStack | Switch-Router (99%) | admin | Syslog.Config | Admin | Runni |
| 尊 | 2017-04-18 13:51:49 | 10.60.30.254 | SKO13-kc | Cisco | catalyst37xxStack | Switch-Router (99%) | admin | Syslog,Config | Admin | Runni |
| Ф | 2017-04-18 12:22:14 | 10.60.30,254 | SKO13-kc | Cisco | catalyst37xxStack | Switch-Router (99%) | admin | Syslog,Config | Admin | Runni |
| \$ | 2017-04-18 12:16:53 | 10.60.30,254 | SKO13-kc | Cisco | catalyst37xxStack | Switch-Router (99%) | admin | Syslog,Config | Admin | Runni |
| \$ | 2017-04-18 11:32:16 | 10.60.30.254 | SKO13-kc | Cisco | catalyst37xxStack | Switch-Router (99%) | admin | Syslog,Config | Admin | Runni |
| 亞 | 2017-04-18 11:25:37 | 10.60.30.254 | SKO13-kc | Cisco | catalyst37xxStack | Switch-Router (99%) | admin | Syslog.Config | Admin | Runni |
| | | | | | | | | | | |
| 4 | Page 1 of 1 | 바를 Displaying 1 | 1 - 6 of 6 | | | | | | Updated at 20 | 017-04-18 14:13:08 |
| 4 4 | Page 1 of 1 🖗 | P Displaying 1 | 1 - 6 of 6 | | | | | | Updated at 20 |)17-04-18 14:13:08 © |
| 4 4 | Page 1 of 1 🖗 | P Displaying 1 | 1 - 6 of 6 tected Chang | e | | | | Most Cha | Updated at 20 Inged Devices | 017-04-18 14:13:08 ¥ |
| 4 4 | Page 1 of 1 # | Displaying 1 | 1 - 6 of 6 tected Chang | e | | | | Most Cha | Updated at 20 anged Devices |)17-04-18 14:13:08 ⊗ |
| 4 4 | Page 1 of 1 # | Displaying 1 Def | 1 - 6 of 6 tected Chang | e | | | | Most Cha | Updated at 20 inged Devices | 017-04-18 14:13:08 ≚ |
| 4 4 | Page 1 of 1 # | ▶ Displaying 1 | 1 - 6 of 6 tected Chang | e | | | | Most Cha | Updated at 20 | 317-04-18 14:13:08 © |
| 14 - 4 | Page 1 of 1 > | ₽ Displaying 1 | 1 - 6 of 6 tected Chang | e | | | 10.60.30.25 | Most Cha | Updated at 20 | 017-04-18 14:13:08 ≆ |
| 14 4 | Page 1 of 1 # | P Displaying 1 | 1 - 6 of 6 tected Chang | e | | | 10.60.30.25 | Most Cha | Updated at 20 | 017-04-18 14:13:08 ≆ |
| 14 - 4 | Page 1 of 1 P | P Displaying 1 | 1 - 6 of 6 tected Chang | e | | | 10.60.30.25 | Most Cha | Updated at 26 | 017-04-18 14:13:08 ⊗ |
| 4 4 | Page 1 of 1 >> | ▶ Displaying 1 | 1 - 6 of 6 tected Chang | je | | | 10.60.30.25 | Most Cha | Updated at 20 Inged Devices | 017-04-18 14:13:08 |
| 4 4 | Page 1 of 1 >> | ₽↓ Displaying 1 Def | 1 - 6 of 6 tected Chang | 2 | | | 10.60.30.25 | Most Cha | Updeted as 20 Inged Devices | 117-04-18 14:13:0 1 6 7 |

16. Click on the wheel of the latest change and select 'View Saved Configuration Difference'. You see the SNMP public community string command is removed per the policy and triggered job.

| mparing C | Configuration Files | | | | | | |
|------------------|--|--|-------------|--|----|--|-----|
| elected Files | Host Device: File Status: Last Modified: | 10.60.30.254(5KO13-kc) Archived Saved 2017-04-18 13:52:09 by admin | | Host Device: File Status: Last Modified: | 1 | 10.60.30.254(SKC)13-kc) Current Saved 2017-04-18 13:57:26 by admin | |
| Find: | view T action T | Changes: 0 | Removals: 1 |). | 00 | Additions: 0 | 0 0 |
| 1 version 15. | D | | 1 ve | sion 15.0 | | | |
| 2 no service j | ad . | | 2 по | service pad | | | |
| 3 service time | estamps debag datetime macc | | 3 ма | vice timestamps debug datetime resec | | | |
| 4 service time | estamps log datetime msec | | 4 se | vice timestamps log datetime miec | | | |
| 5 so service ; | aussword-encryption | | 5 no | service password-encryption | | | |
| Skipping to | line 374 | | Sk | pping to line 374 | | | |
| 374 ip sta enabl | e reaction-alerts | | 374 ip | la enable reaction-alerts | | | |
| 375 logging ma | p debugging | | 375 loj | ging trap debugging | | | |
| 376 logging hos | at 10.60.16.96 | | 376 loj | ging bost 10.60,16.96 | | | |
| 377 : | | | 377 1 | | | | |
| 378 samp-serve | r community infobios RO | | 378 sm | np-server community infoblox RO | | | |
| 379 simp-serve | er contrastily public KO | | 379 | | | | |
| 380 1 | | | 380 1 | | | | |
| 381 1 | | | 381 1 | | | | |
| 382 line con 0 | | | 382 lin | com 0 | | | |
| 383 Time vty 0.4 | | | 383 lin | r viy 0.4 | | | |
| 384 exec-times | nat 30 0 | | 384 # | cc-timeout 30 0 | | | |

17. You can see a record of the triggered job being run to fix the SNMP misconfiguration. Navigate to Config Management → Job Management → Job History.

| Search | | | | | | | | | Views • Filters |
|--------|----------|--|---|--------------|-------------|---------------------|---------------------|---|-----------------|
| tatus | Job ID 🔻 | Name | Script | Initiated By | Approved By | Start Time | End Time | Summary Count | |
| ок | 4 | Doleting SNMP Community string (Triggered Jobil/Run Now) | Remove SNMP Community string public and private | admin | admin | 2017-04-18 13:57:00 | 2017-04-18 13:57:21 | Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0 | |
| ок | 3 | Deleting SNMP Community string (Triggered Job)[Run Now] | Remove SNMP Community string public and private | admin | admin | 2017-04-18 12:22:00 | 2017-04-18 12:22:23 | Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0 | |
| ок | 2 | Deleting SNMP Community string [Triggered Job][Run Now] | Remove SNMP Community string public and private | admin | admin | 2017-04-18 11:32:00 | 2017-04-18 11:32:26 | Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0 | |
| OK | 1 | Remove SNMP Community string public and private [Triggered Job][Run Now] | Remove SNMP Community string public and private | admin | admin | 2017-04-17 20:02:00 | 2017-04-17 20:02:25 | Total: 1, Pending: 0, OK: 1, Error: 0, Other: 0 | |

18. Click on the name of the latest job. The following screen appears:



19. Click on the 'OK' link. The following screen appears:



20. The screen above shows NetMRI logging in and running the script. You can click on the Script tab, Status Log tab, Custom Log tab, Session Log tab, and Files tab to see the details of each.

Device CVE/PSIRT - Advisor

Network vendors provide Security Advisory information with increasing cadence and complexity. Your team needs to make sense of this data, determine which vulnerabilities impact your network's security posture, and take timely action to keep your network secure. For many, internal and external compliance requirements make this challenge even more complex. Empowered*Advisor*[™] from Empowered Networks for NetMRI helps you ensure your network is secure & compliant, with Always-On Analysis, Alerts & Advice, based on Security Advisories.

After installation of the EmpoweredAdvisor, you can do the following to gather the PSIRT information on your devices. In this example, we are using the LabCore device group and assigning the PSIRT policies to view any device vulnerabilities, but you can assign the PSIRT policies to any or all of the device groups in your NetMRI.

1. Navigate to Config Management → Policy Design Center. Make sure the left pane is viewing By Device Groups.

| v Rules Policies Policy Deploym | rent . | | | |
|---------------------------------|--|----------------|---------------------|--|
| a demonstration and a second | | | | |
| ice Groups | Device Group: LabCore | | | |
| ch | Member Count: 11 Criteria: STyne in ("Switch" "Switch-Router") and Stiendor = "Cisco" | | | |
| App Servers (16) | enterial erge in Content, enterination para evolution - elece | | | |
| App Servers w/o SNMP (0) | | | | |
| End of Support Devices (0) | | | | |
| IT Services (4) | | | | |
| LabCore (11) | | | | |
| NAME ONLY (147) | | | | |
| Network Low-Level (0) | Search | | | |
| Network Management (3) | | - | | |
| Network w/o SNMP (15) | Name A Short Name | Author | Last Change Data | |
| NIOS (35) | B CI DSS 3.0 IOS/NX-OS PCI 3.0 | Infoblox, Inc. | 2017-03-13 15:52:07 | |
| Optimizers (0) | E PCI Policy PCI DSS 3.0 | Thomas Lee | 2017-04-05 15:00:31 | |
| Routing (12) | | PSIRT Advisory | 2017-04-18 08:57:22 | |
| Security Control (0) | ∃ V PSIRT Crit cisco-sa-20120328-pal CV1248184366 | PSIRT Advisory | 2017-04-18 08:57:28 | |
| Switching (18) | | PSIRT Advisory | 2017-04-18 08:57:18 | |
| UNKNOWN (145) | PSIRT Crit cisco-sa-20170317-cmp CV3096274358 | PSIRT Advisory | 2017-04-18 08:57:24 | |
| Video (0) | H POIDT High cares as 20120328.lks CV/2681898831 | PSIRT Advisory | 2017.04.18.09.57.58 | |
| Wireless (0) | # DOIDT High sizes as 20100229 and CH4101022795 | DPIDT Advisory | 2017 04 10 09:59 47 | |
| Workstations (0) | Peter High decose 2012020-801a CV4191023700 | PSIRI Advisory | 2017-04-10 00.00.97 | |
| Workstations w/o SNMP (33) | CV3702241036 | PSIRT Advisory | 2011-04-10.0033[23] | |
| | PSIKI High cisco-sa-20120926-ios-ips CV608615420 | PSIRT Advisory | 2017-04-18 08:59:18 | |
| | # PSIRT High cisco-sa-20120926-nat CV3571247085 | PSIRT Advisory | 2017-04-18 08:58:11 | |
| | B PSIRT High cisco-sa-20130327-pt CV1911329901 | PSIRT Advisory | 2017-04-18 08:59:23 | |
| | | | | |

- 2. From the screen shot above, highlight the device group and then scroll down on the right pane to the PSIRT section. Click on each PSIRT policy that you want to evaluate. Click Save when it becomes ungrayed.
- 3. After about 10 minutes or more depending upon the size of the device group and/or number of PSIRT policies enabled, navigate to Network Analysis → Issues to view Issues.

| Infoblox | 😵 Dashboard | Network Analysia Network Explore | Config | Management F | Reports | | | | 2 | A 🖗 | 0 |
|------------|---|--|-------------|----------------|------------|-------|-----------|--------------|--------------------------------|--|------|
| | Issu | es - Changes Policy Compliance | Performance | | | | | | | Select Device Group | 35 @ |
| LabCorr | Varning 6 2017-04-19 / Daily Warning 6 Error Count 6 Routina Security 6 Security | Charges Policy Compliance | Performance | | | | | | • | Search Search Search Search Application (427) Application (427) Application (417) AnAME Only (146) AnAME Only (146) Network with SMMP (15) Network with SMMP (15) Reading (12) Search (41) Reading (12) R | |
| Search | is Subnets | WITHESS | | | | | | | Views * Filters Display * 🗸 2 | Switching (18) UNKNOWN (146) Workstations w/o SNMP (34) | |
| Severity . | Last Seen | Title | Status | Component | # Affected | # New | # Cleared | # Suppressed | | | |
| Error | 2017-04-19 13:44:33 | Router Interface Down | Current | Interfaces | 4 | 0 | .0 | 0 | | | |
| Creat | 2017-04-19 13:26:10 | Policy Violation: PSIRT High cisco-sa-20 | Current | Configurations | 1 | 1 | 0 | 0 | | | |
| Error | 2017-04-19 12:08:32 | VLAN Member Phoney | Current | VLANS | 22 | 0 | 0 | 0 | | | |
| Error | 2017-04-19 12:08:22 | Device leave Limit Exceeded | Current | Devices | 7 | 0 | 0 | 0 | | | |
| Crist | 2017-04-19 12:06:53 | Access Port With Portliner Disabled | Current | Interfaces | | 0 | 0 | 0 | | | |
| Error | 2017-04-19 09:11:05 | Policy Violation: PSIRT Crit cisco. sa 201 | Current | Configurations | 8 | 0 | 0 | 0 | | | |
| Error | 2017-04-19 09:11:06 | Policy Violation: PSIRT Crit cisco-sa-200 | Current | Configurations | 1 | 0 | 0 | 0 | | | |
| Error | 2017-04-19 09:11:06 | Policy Violation: PSIRT Crit cisco-sa-201 | Current | Configurations | 10 | 0 | 0 | 0 | | | |
| Error | 2017-04-19 09:11:06 | Policy Violation: PSIRT Crit cisco-sa-201 | Current | Configurations | 2 | 0 | 0 | 0 | | | |
| Error | 2017-04-19 05:16:11 | VLAN Topology Change | Current | VLANs | з | 0 | 0 | 0 | | | |
| 💧 Warning | 2017-04-19 13:48:10 | Cisco Buffer Misses High | Current | Devices | 1 | 0 | 0 | 0 | | | |
| 🔥 Warning | 2017-04-19 13:38:42 | Interface Congested | Current | Interfaces | 4 | 2 | 0 | 0 | | | |
| 14 4 Pag | ie 1 of 2 🕨 🔰 | Displaying 1 - 15 of 25 | | | _ | | | | Updated at 2017-04-19 13:55:17 | | |

4. Click on the Views pull-down menu and select PSIRT Violations. This will show only the PSIRT violations.

| Infoblox | 😵 Dashboard | Network Analysis Network Explorer | Config | Management F | leports | | | | | 4 4 0 |
|--|--|---|-------------|----------------|------------|-------|-----------|--------------|---------------------------------|---|
| | Issu | les + Changes Policy Compliance | Performance | | | | | | | Select Device Group |
| LabCon | e 2017-04-19 / Daily | | | | | | | | 0 | Search |
| info Count 8 Scontigue Devices | Waming Count 6 rations 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 | Versall Score | | | | | | | | AD Devices (427) App Servers (16) T Services (4) Marke ONLY (146) NAME ONLY (146) Notwork Management (3) Notwork wid SMMP (15) Note (32) Routing (12) Security (4) Switching (18) Wurkerbang (18) |
| Search | The second se | No. | 1 | | | 1000 | | 1000 C | Views 🔹 Filters Display 🔹 🖓 🔁 | Workstations w/o SNMP (34) |
| Severity * | Last Seen | Title | Status | Component | # Affected | # New | # Cleared | # Suppressed | Add view | |
| W Error | 2017-04-19 13:44:33 | Router Interface Down | Current | Interfaces | 4 | 0 | 0 | 0 | Manage views | |
| Error | 2017-04-19 13:26:10 | Policy Violation: PSIRT High cisco-sa-20 | Current | Configurations | 1 | 1 | 0 | 0 | Standard view | |
| Error | 2017-04-19 12:08:32 | VLAN Member Priority | Current | VLANs | 22 | 0 | 0 | 0 | PSIRT Violations | |
| Error | 2017-04-19 12:08:22 | VLAN Member Minimum Priority | Current | VLANs | 22 | 0 | 0 | 0 | | |
| Error | 2017-04-19 12:08:12 | Device Issue Limit Exceeded | Current | Devices | 7 | 0 | 0 | 0 | | |
| Error | 2017-04-19 12:06:53 | Access Port With PortFast Disabled | Current | Interfaces | 8 | 0 | 0 | 0 | | |
| Error | 2017-04-19 09:11:06 | Policy Violation: PSIRT Crit cisco-sa-201 | Current | Configurations | 8 | 0 | 0 | 0 | | |
| Error | 2017-04-19 09:11:06 | Policy Violation: PSIRT Crit cisco-sa-200 | Current | Configurations | 1 | 0 | 0 | 0 | | |
| Error | 2017-04-19 09:11:06 | Policy Violation: PSIRT Crit cisco-sa-201 | Current | Configurations | 10 | 0 | 0 | 0 | | |
| Error | 2017-04-19 09:11:06 | Policy Violation: PSIRT Crit cisco-sa-201 | Current | Configurations | 2 | 0 | 0 | 0 | | |
| Error | 2017-04-19 05:16:11 | VLAN Topology Change | Current | VLANs | 3 | 0 | 0 | 0 | | |
| A Warning | 2017-04-19 13:48:10 | Cisco Buffer Misses High | Current | Devices | 1 | 0 | 0 | 0 | | |
| A Warning | 2017-04-19 13:38:42 | Interface Congested | Current | Interfaces | 4 | 2 | 0 | 0 | | |
| 14 4 Pag | ge 1 of 2 ▶ ▶] | Displaying 1 - 15 of 25 | | | | | | | Updated at 2017-04-19 13:55:17 | |

5. After selecting the PSIRT view, you will see the following:

| Infoblo | X 💸 Dashboard | Network Analysis Network Explore | r Config | Management F | leports | | | | | × \$ | 0 |
|--|---|---|------------------------------|---|--------------------------|--------|--------------------------|---|-------------------------------|--|-----|
| | Issu | ies • Changes Policy Compliance | Performance | | | | | | | Select Device Group | > 0 |
| LabCe | 2017-04-19 / Daily | | | | | | | | | Search | |
| C LabCo Info Count B Contor Data Contor B Contor Cont | ve 2017-04-19 / Daiy Verming Court 6 11 12 12 13 14 15 15 15 15 15 15 15 15 15 15 | Overall Score J. J. J. J. J. Alts J. Alts J. Matter Writess | Status Current Current | Component Configurations Configurations | #Affected 1 8 2 | 0 0 | # Cleared 0 0 0 | # Suppressed 0.00000000000000000000000000000000000 | Views * Filters Display * 💐 🐉 | Search - Search - Search (27) A polyces (427) T Services (4) - Search (11) Network Management (3) Network was SNMP (15) Notice Panding (12) Search (11) Notice Panding (12) Search (11) Search (12) Search (13) Search (146) Workstations w/o SNMP (34) | |
| Error | 2017-04-19 09:11:06 | Policy Violation: PSIRT Crit cisco-sa-201 | Current | Configurations | 10 | 0 | 0 | 0 | | | |
| Error | 2017-04-19 13:26:10 | Policy Violation: PS/RT High cisco-sa-20 | Current | Configurations | 1 | 1 | 0 | 0 | | | |
| | | | | | | | | | | | |

6. Click on one of the links to view the affected devices.

| omponent: Configurations everity: Error ast Seen: 2017-04-19 09:11:06 | Correctness: -2.0 Stability: 0.0 6 | | | | | | | | | | | | | | | |
|---|--|-----------------------------------|---------------|-------|--------|-------|---------|------|---------|---------------------|---------|---------|---------|-------|-----------------|---------|
| n Device Group | Components Affected by Iss | ve (Current) | | | | | | | | | | | | | | |
| irch | Search | | | | _ | | _ | | | | Views - | Filters | Display | | | 312 |
| All Devices (427) | Device Name | Device Type | IP Address | Rules | Passed | Error | Warning | Info | Details | Last Seen | DIIT S | up7 | | | | |
| LabCore (11) | me-3750-48-p4r1-22.m | Switch (99%) | 10.60.0.12 | 5 | 4 | 1 | 0 | 0 | View | 2017-04-19 09:11:06 | Same | | | | | _ |
| Switching (18) | tme-3560-48-p2r3-25.m | Switch-Router (99%) | 10.60.0.11 | 5 | 4 | 1 | 0 | 0 | View | 2017-04-19 09:11:06 | Same | | | | | |
| | D p4r3-31.kkpti-labs.com | Switch (99%) | 10 60 192 250 | 5 | 4 | 1 | 0 | 0 | View | 2017-04-19 09:11:06 | Seme | | | | | |
| | El comp3750 | Switch-Router (99%) | 10.60.3.34 | 5 | 4 | 1 | 0 | 0 | View | 2017-04-19 09:11:06 | Same | | | | | |
| | m test-switch | Switch-Router (99%) | 10 60 30 253 | 5 | 4 | 1 | 0 | 0 | View | 2017-04-19 09:11:06 | Same | | | | | |
| | C csco-p4r1-29 | Switch-Router (99%) | 10.60.192.253 | 5 | 4 | 1 | 0 | 0 | View | 2017-04-19 09:11:06 | Same | | | | | |
| | El <u>caco-p4r3-34</u> | Switch-Router (99%) | 10.60 136.31 | 5 | .4 | 1 | 0 | 0 | View | 2017-04-19 09:11:06 | Same | | | | | |
| | Ci3750-vian-patch m | Switch (99%) | 10.60.0.31 | 5 | 4 | 1 | 0 | 0 | View | 2017-04-19 09:11:06 | Same | | | | | |
| | H 4 Page 1 of 1 | P ₂ Displaying 1 - 8 | of 8 | | | | | | | | | | | Updat | sd at 2017-04-1 | 19 14:0 |
| | 8 - 6 - 4 - | | | | | | | | | | | | | | | |

7. Click on one of the View links under the Details column.

| Infoblox 🐟 | Configuration Policy Analysis | | |
|--|--|-------|-----|
| | 2017-04-19 09:11:06 | | |
| olicy PSIRT Crit claco-sa-20120328-pai | | | |
| Cisco IOS Software Command Authorization Bypass CVEs included in this Ce | sto Security Advisory CVE-2012-0384: Cisco IOS Software Command Authorization Bypass Vulnerability | | |
| Filter: | | | |
| Role: 1 1: (devicewendor matches 'Claco') | | | |
| Error | | | |
| Last Check: 2017-04-19 09:10:58 | | | |
| Policy Summary: | | | |
| Pass 4 (80 00%) | | | |
| Fall 1 (20.00%) | | | |
| Error 1 (20.00%) | | | |
| Warning 0 (0.00%) | | | |
| Info 0 (0.00%) | | | |
| Skip 0 (0.00%) | | | |
| Chacked 5/100.0050 | | | |
| Rules Summary: | | | |
| PSIRT cisco-sa-20120328-oal Rule 1:CV1251609925 | | Pasa | 100 |
| PSIRT cisco-sa-20120328-pai Rule 2:CV1545163038 | | Pass | 1 |
| PSIRT cisco-sa-20120328-pai Rule 3:CV4109462364 | | Pass | 123 |
| PSIRT cisco-sa-20120328-pai Rule 4 CV957321223 | | Pass | 2 |
| PS/RT cisco-sa-20120328-pai Rule 5 CV1624568525 | | Error | × |
| Device cl3750-vian-catch.m | | | |
| IP: 10.60.0.31 | | | |
| Model: catalyst37xxStack | | | |
| Last Chack: 2017-04-19 14:07-21 | | | |
| | | | |
| Rule PSIRT cisco-sa-20120328-pail Rule 1 | | | |
| Cisco IOS Software Command Authorization Bypass | | | |
| Filter: | | | |
| Sule: 1 1) (devicevendor matches 'Cisco') | | | |
| 20 D | | | |

8. Scroll down the screen if necessary to view the error details. This screen shows the title of the PSIRT, filter used to choose the device to evaluate, the remediation link, and the logic for evaluating the filtered device.

| Rule PSIRT clscx-ss-2012022b-pail Rule 5 |
|--|
| Cisco IOS Software Command Authorization Bypass |
| Filter: |
| Rules 1 11 (deriverender statutes "Cisto") |
| I Error |
| Remediation: |
| http://tools.clson.com/security/center/content/Clsoolecuritybundle/clsoo-ao-20120328-bundle |
| Logic: |
| (derinspekter in "Lies 18 Setues, CFSHE Setues (CFSHE-SETUESBANG-SE, Version 12.1(5)18). SEtURE ESTENCE (CE) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (CE) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (CE) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (tc) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (tc) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (tc) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (tc) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (tc) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (tc) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (tc) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Compiled the S-Sequent 21.1(5)180. SetURE ESTENCE (tc) Technical Sequent: http://www.sissuess/undrugget Cogyright (s) 186-5111 by Ease Systems, Inc. Cogyright (s) 186-5111 by Ease Systems |
| |

- 9. Copy and paste the remediation URL. In this case it is: <u>http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20120328-bundle</u>
- 10. Here is the result of the URL:

| | | | | | Worldw | vide [change] Welcome, Ac | count Log Out My Cisco |
|-------------------------------|-------------|---|---|--|--|--|--------------------------|
| CI | sco | Products & Services | Support Ho | ow to Buy | Training & Events | Partners | Q |
| Home | e / Cisco | o Security / Security Advisories | | | | | |
| Cis Cis | co S SCO | Security Security Advis | ories | | | | |
| Vuln | nerabili | ties Filter By Product | | | | | |
| Qui | ck Sea | arch Q | | | | | × |
| | Advan | ced Search | | | | | |
| | ADVIS | | | | | | |
| | | DRY | | | CVE | LAST UPDATED | VERSION |
| | Searc | DRY h Advisory Name | | IMPACT ≡ ₀ | CVE Search CVE | Most Recent | VERSION |
| • | Searc | Advisory Name Cisco IOS XR Software Cisco D Vulnerability | viscovery Protocol Format S | IMPACT =₀ All tring High | CVE Search CVE CVE-2020-31 | LAST UPDATED Most Recent 18 2020 Oct 20 | VERSION |
| • | Searci | RY h Advisory Name Cisco IOS XR Software Cisco I Vulnerability Cisco Webex Teams Client for Vulnerability | ilscovery Protocol Format S Windows DLL Hijacking | IMPACT ≡₀ All tring ● High | CVE Search CVE CVE-2020-31 CVE-2020-35 | LAST UPDATED Most Recent 18 2020 Oct 20 35 2020 Oct 07 | VERSION |
| ▲▲ | Searc | RY h Advisory Name Cisco IOS XR Software Cisco I Vulnerability Cisco Webex Teams Client for Vulnerability Cisco Identity Services Engine Vulnerability | iscovery Protocol Format S Windows DLL Hijacking Authorization Bypass | IMPACT II) | CVE Search CVE CVE-2020-31 CVE-2020-35 CVE-2020-34 | LAST UPDATED Most Recent 18 2020 Oct 07 35 2020 Oct 07 67 2020 Oct 07 | VERSION |
| | Searco | Advisory Name Clasco IOS XR Software Clasco IC Vulnerability Clasco Webex Teams Client for Vulnerability Clasco Identity Services Engine. Vulnerability Clasco Video Surveillance 8000 Discovery Protocol Remote Co Service Vulnerability | liscovery Protocol Format S Windows DLL Hijacking Authorization Bypass Series IP Cameras Cisco Je Execution and Denial of | IMPACT II) | CVE Search CVE CVE-2020-31 CVE-2020-35 CVE-2020-34 CVE-2020-35 | LAST UPDATED Most Recent 18 2020 Oct 07 35 2020 Oct 07 67 2020 Oct 07 44 2020 Oct 07 | VERSION |

- 11. From this screen, you can find out details of the vulnerability and fix for the vulnerability.
- 12. In addition, you can run a Policy Compliance Summary report to show the number of devices in a device group that have vulnerabilities. Navigate to Reports → Report Gallery. Move the mouse pointer to the Policy Compliance Summary report.

| (conpliance | | | | | | | | | | |
|--|--|---|--|--|--|--|-------------|---|--|------------------------|
| Debut Credentials Report This report has been on the second participation of the accessing with the second participation of the second participation whether default credentials a specific time period. | Arrow Contraction of the second secon | ISO 27002 This report documents compliance with certain network aspects of the ISO 27002-2005 standard, commonly used as best practices goldlines for Sahanes-Oxley, HPAA and GLBA compliance. | | PCI This report documents compliance with certain network aspects of the Phymeric Card Industry Data Security Standard Version 3.0. | And Annual Annua | Policy Compliance Details This report provides a detailed list of all policies and policy rules, along with the devices passing and failing, and the specific reasons for policy violations. | Rec Schools | Policy Compliance Summary This report provides an overview of the policy compliance situs for all policies and the network devices against which they are deployed. | | PSIRT Report - Updated |

13. Click on the 'Next' link.

| Policy Compliance | a Summary Report | × |
|---|--|--|
| | | Step 1 of 2: Select Time Variables and Device Groups |
| Date: | 04/28/2017 | |
| Period: | Daily | |
| Device Groups | Devices | |
| Search | | |
| App Service App Service End of St T Service T Service LubCore AAME O Network Network Network Network Network Not S(35 Optimize Paulino, Service Network | vers (16) vers wio SNMP (0) upport Devices (0) es (4) es wio SNMP (0) (11) NLY (143) Low-Level (0) Management (3) Pending (5) w/o SNMP (15)) rs (0) (12) | |
| Security Security Switchin UNKNOV | (4) Control (0) g (18) VN (138) | |
| | | < Previous Next > Cancel |

14. Select the PSIRTs that were used in the screen shot in step 1 as an example



15. Click on the 'Run' button. The following screen appears. At the upper left of the screen, you can choose to download the report in PDF, Excel, or MS Word in addition to printing the report.

| Showing page 1 of 3 | | VI V 🕨 🕪 Go to page: |
|--|---|---|
| Policy Compliance Date Range: 2017-04-19 00:00:00 to 2017-04 Device Groups: LabCore Devices: | Summary 19 23:59:59 | |
| Policy Compliance By | Device Policy C | Compliance By Rule |
| Int: 0.00% | – Warning: 0.00% – Unknown: 0.00% – Pass: 88.80% – | Into: 0.00% Enor: 11.11% Warning: 0.00% Unknown: 0.00% |
| Pass: 60.00%/ | | |
| Pass: 00.00% | Number of Devices | _ |
| Pass: 60.00% | Number of Devices | |
| Pass: 00.00% Dverall Status Same Situr Si | Number of Devices | _ |
| Pass: 60.00% Dverall Status SIRT Crit cisco-sa-20080610-annov3 error R pass 20080610-annov3 error R pass 20080610-annov3 | Number of Devices | |
| Pass: 60.00% | Number of Davloes | |
| Pas:: 60.00% Deverall Status Istime Overall SIRT Crit clisco-sa-2016061 (1-annova pass) SIRT Crit clisco-sa-20120328-bai error X pass) | Number of Devices | |
| Pase: 60.00% | Number of Devices 1 10 8 3 | |
| Pass: 80.00% | Number of Devices | |
| Pass: 60.00% Pass: 60.00% Pa | Number of Devices 1 10 8 3 2 9 | |
| Pass: 00.00% Server all Status Server all Status | Number of Devices | |
| Pas: 60.00% Series 20060610-ampv3 PSIRT Crit cisco-sa-20160610-ampv3 SIRT Crit cisco-sa-201203245 PSIRT Crit cisco-sa-20140605-openasi error ≥ PSIRT Crit cisco-sa-20140605-openasi error ≥ PSIRT Crit cisco-sa-2017037-orm error ≥ | Number of Devices 1 1 10 8 3 2 9 10 | |
| Pass: 60.00% | Number of Davices 1 1 0 8 3 2 9 10 10 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | |
| Pass: 60.00% Proventil Status | Number of Devices 1 1 0 8 3 2 9 10 10 1 | |
| Pass: 60.00% | Number of Davices 1 1 1 0 8 3 2 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | |

16. You can have the report scheduled to be sent out via email. Highlight the PSIRT Report and click on the schedule button.

| | Report Gallery School | tuled Reports Report M | eneger | | | | | | |
|---|---|--|---|--|---|---------|--|---|---|
| unander Wagnerel Station Antonio Contraction Antonio Contractio Antonio Contractio Antonio Contractio Anto | Configuration Management Summary of the network devices meeting specific group criteria for which the system is managing configurations. | | test Report all the configuration changes that have taken place in the last 24 hours. (Only shows the Running configuration) | | | | | | |
| Compliance | Default Credentials Report This report lists network devices | 100 0102 State and an and a state and a s | 150 27002 This report documents compliance with certain network | PD Monte State St | PCI This report documents compliance with certain network | | Policy Compliance Details This report provides a detailed list of all policies and policy | Table Segment Jonney Ministration and and a segment of the second | Policy Compliance Summary This report provides an overview |
| | found to be accessible using vendor default credentials during a specific time period. | Internet and Annual State (Second State (Seco | sepects of the ISO 27002-2005 standard, commonly used as best practices guidelines for Sarbanes-Ordey, HIPAA and GLBA compliance. | Construction of the second seco | sepects of the Payment Card Industry Data Security Standard Version 3.0. | Linuta. | rules, along with the devices passing and failing, and the specific reasons for policy violations. | = 1 | of the policy compliance status for all policies and the network devices against which they are deployed |
| un, Schedule, Eds. sport, Delete | PSIRT Report - Updated | | | | | | | | |
| Health | | | | | | | | | |
| Ec | Example: Issues for today A report of only today's issues | | Issue Details This report provides a listing of the issues reported by a group of network devices over a specific time period. | | Network Health This report provides a summary of key health metrics for a group of network devices over a specific time period. | | Network History This report provides a summary of key stiributes for the entire network over a specific time period. | | Network Performance This report provides a summery of key performance metrics for group of network devices over a specific time period. |

17. Select the device group. Click Schedule.

| Policy Compliance | e Summary Re | sport | 🛛 |
|--|---|------------|--|
| | | | Step 1 of 4: Select Time Variables and Device Groups |
| Date: | 04/19/2017 | | |
| Device Groups | Devices | | |
| Search | 10 | | |
| App Sen End of Su T Servic End T Servic End T Servic LabCom | vers w/o SNMP upport Devices ces (4) ces w/o SNMP (11) NLY (146) | (0) (0) | |
| Network Network Network NIOS (35 | Management (Pending (5) w/o SNMP (15 i) ers (0) | 3) | |
| Routing Security Security Switchin | (12) (4) Control (0) g (18) | | |
| | VN (146) | | < Previous Next > Cancel |

18. Select the PSIRT policies and click Next.

| | | Step 2 of | 4: Select Polic |
|--|---|---------------------------------------|-----------------|
| licies | | Selected Policies | Clear |
| IB_6112 Med CVE-2016-9131 | | PSIRT Crit circo.co. 20080610.compu/2 | |
| JN Crit CVE-2013-6618 | | PSIRT Crit cisco-sa-20080010-simpv3 | |
| IN High CVE-2014-3818 | | PSIRT Crit cisco-sa-20120520-pai | |
| IN Med CVE-2013-7313 | | PSIRT Crit cisco-sa-20170317-cmp | |
| NSA 1.1c IOS | | PSIRT Citt Cisco-sa-20170317-Citip | |
| PCI USS 1.2 IOS | | 1 51KT HIGH 6500 38-20120320-IKC | |
| PCI DSS 2.0 IOS | | | |
| PCI DSS 3.0 IOS/NX-OS | | | |
| PCI Policy | | | |
| PSIRT Crit cisco-sa-20080610-snmpv3 | | | |
| PSIRT Crit cisco-sa-20120328-pai pount o it is a solution of the solution o | 0 | | |
| PSIRT Criticisco-sa-20140605-openssi PDUDT Officience 20170017 | 9 | | |
| PSIRT Crit cisco-sa-20170317-cmp | G | | |
| PSIRT High cisco-sa-20120328-ike | - | | |
| PSIRT High cisco-sa-20120328-smartinstall POUDT US + Size - 20120328 - smartinstall | | | |
| PSIRT High cisco-sa-20120926-dncpv6 | | | |
| Point Migh cisco-sa-20120926-los-lps | | | |
| PSIKI High cisco-sa-20120926-nat | | | |
| PSIKI High cisco-sa-20130327-pt | | | |
| PSIKT High cisco-sa-20130327-smartinstall DOUDT Life cisco-sa-20120207 | | | |
| Point righ cisco-sa-20130925-cce DOIDT Lich sizes as 20130925-cce | | | |
| Point righ cisco-sa-20130925-dhcp Doubt line cisco-sa-20130925-dhcp | | | |
| PSIRI High cisco-sa-20130925-ipv6vfr DSIRI High cisco-sa-20130925-ipv6vfr | | | |
| PSIKI High cisco-sa-20130925-nat | | | |

19. Enter the email address, output format, recurrence pattern, execution time, and day of week. Click Next.

| | | 5 | Step 3 of 4: Select Report Schedu |
|--------------------|--|----------|-----------------------------------|
| Report Name: | Policy Compliance Summary | | |
| To Emails: | management@xyzcorp.com | | |
| To Users: | NetMRI Admin () dave signori () psirt psirt () support support () tao tao () | | |
| Output Format: | pdf | | • |
| ecurrence Pattern: | Weekly | 1 | |
| Execution Time: | 6:00 AM | • | |
| Sunday | Tuesday 🔲 Thursday 🔲 : | Saturday | |
| i⊠ Monday E | weonesoay 🗀 Fnday | | |
| | | | |

20. Verify the settings are correct. Click Schedule.

| cy Compliance Su | immary Report |
|------------------|---|
| | Step 4 of 4: Summary of Scheduled Repo |
| Report Name: | Policy Compliance Summary |
| Date: | 04/19/2017 |
| Period: | Daily |
| Device Groups: | LabCore |
| Devices: | |
| Policies: | PSIRT Crit cisco-sa-20080610-snmpv3,PSIRT Crit cisco-sa-20120328-pai,PSIRT Crit cisco- sa-20140605-openssl,PSIRT Crit cisco-sa-20170317-cmp,PSIRT High cisco-sa-20120328-ike |
| To Emails: | management@xyzcorp.com |
| To Users: | |
| Schedule: | Weekly - Monday at 06:00 AM |
| | |
| | < Previous Schedule Cancel |

Device Life Cycle Management

After installation of the Empowered Networks' Empowered Advisor, you can do the following to gather the Life Cycle information on your devices. In this example, we are using the LabCore device group.

| | rk Analusia Naturali | Explorer Coolin Nanan | ment Reports | | | | 3 | | |
|------------------------|----------------------|---|---------------------|--------|----------------------|---------------------|---|-----------------|----|
| Inventory | Summaries Topology | Discovery Switch Port | Management | | | | Select Device Group | • × | |
| LabCore 2017-04-19 | | | | | | 0 | Search | | |
| Devices | All Devices | | | - | | | - SAll Devices (427) App Servers (16 | 9 | |
| Infrastructure Devices | Search | | 1. | heren | l | Views 🔹 Filters 🖉 😴 | LabCore (11) | | |
| Device Components | IP Address - | Device Name | Туре | Vendor | Model | | NAME ONLY (14 | 6) ement (3) | |
| Connected IP Phones | 10.60.0.1 | core-6506 | Switch-Router (99%) | Cisco | cat6506 | | Network Pendin | g (5) | |
| All Devices | 10.60.0.11 | tme-3560-48-p2r3-25.m | Switch-Router (99%) | Cisco | cat3560x48 | | Network w/o SN | MP (15) | |
| | 10.60.0.12 | tme-3750-48-p4r1-22.m | Switch (99%) | Cisco | catalyst37xxStack | | NIOS (35) | | |
| | 10.60.0.31 | cj3750-vlan-patch.m | Switch (99%) | Cisco | catalyst37xxStack | | Security (4) | | |
| | 10.60.3.34 | comp3750 | Switch-Router (99%) | Cisco | catalyst37xxStack | | Switching (18) | | |
| | 10.60.30.53 | 10.60.30.53 stack2.acme.com Switch-Router (99%) Cisco cat29xxSt | cat29xxStack | | Workstations w/o SNM | | | | |
| | 10.60.30.253 | test-switch | Switch-Router (99%) | Cisco | cat29xxStack | | Workstations w/o SNM | | 9) |
| | 10.60.30.254 | SKO13-kc | Switch-Router (99%) | Cisco | catalyst37xxStack | | | | |
| | 10.60.136.31 | csco-p4r3-34 | Switch-Router (99%) | Cisco | catalyst3560v248ps | | | | |
| | 10.60.192.250 | p4r3-31.kkptj-labs.com | Switch (99%) | Cisco | catalyst37xxStack | | | | |
| | 10.60.192.25 | csco-p4r1-29 | Switch-Router (99%) | Cisco | catalyst37xxStack | | | | |
| Virtual Devices | * | | | | | | | | |
| Interfaces | + | | | | | | | | |
| DSs | + | | | | | | | | |
| Models | + 14 4 1 Pro | a tlaft h hi Diraha | 200 1 11 al 11 | | | | | | |

1. Navigate to Network Explorer → Inventory. Select the device group and then select All Devices.

2. Click on the Views drop down menu and select EoX Lifecycle Announcements view.

| Inventory | Summaries Topology | Discovery Switch Port | Management | | | | Select Device Group |
|---------------------|--------------------|------------------------|---------------------|--------|--------------------|-----------------------------|--------------------------|
| LabCore 2017-04-19 | | | | | | 0 | Search |
| | All Devices | | | | | Ĩ | - 🍪 All Devices (427) |
| evices | Search | | | | | Views 🔻 Filters 🖉 🖉 | IT Services (4) |
| Device Components | IP Address | Device Name | Type | Vendor | Model | Add view | NAME ONLY (146) |
| Connected End Hosts | 10.60.0.1 | core-6506 | Switch-Router (99%) | Cisco | cat6506 | Manage views | Network Management (3) |
| Connected IP Phones | 10.60.0.11 | tme-3560-48-p2r3-25.m | Switch-Router (99%) | Cisco | cat3560x48 | Standard view | Network Pending (5) |
| | 10.60.0.12 | tme-3750-48-p4r1-22.m | Switch (99%) | Cisco | catalyst37xxStack | | NIOS (35) |
| | 10 60 0.31 | cj3750-vlan-patch.m | Switch (99%) | Cisco | catalyst37xxStack | EoX Lifecycle Announcements | Routing (12) |
| | 10.60.3.34 | comp3750 | Switch-Router (99%) | Cisco | catalyst37xxStack | | Security (4) |
| | 10.60.30.53 | stack2.acme.com | Switch-Router (99%) | Cisco | cat29xxStack | | UNKNOWN (146) |
| | 10.60.30.253 | test-switch | Switch-Router (99%) | Cisco | cat29xxStack | | Workstations w/o SNMP (3 |
| | 10.60.30.254 | SKO13-kc | Switch-Router (99%) | Cisco | catalyst37xxStack | | |
| | 10.60.136.31 | csco-p4r3-34 | Switch-Router (99%) | Cisco | catalyst3560v248ps | | |
| | 10.60.192.250 | p4r3-31.kkptj-labs.com | Switch (99%) | Cisco | catalyst37xxStack | | |
| | 10.60.192 253 | csco-p4r1-29 | Switch-Router (99%) | Cisco | catalyst37xxStack | | |
| | | | | | | | |
| tual Devices | + | | | | | | |
| erfaces | + | | | | | | |
| \$ | + | | | | | | |

3. Here are the results. In this device group, all of the devices are end-of-sale. The end-of-sale date is listed along with the end-of-support date. This information will allow you to plan a budget to replace the affected switches.

| Inventory | Summaries Topology | Discovery Switch P | ort Management | | | | | | Select Device Group |
|--|--------------------|--------------------------|-----------------------|--------|--------------------|------------------------|-----------------------|--------------------------|-------------------------|
| bCore 2017-04-19 | | | | | | | | (8) | Search |
| | All Devices - | eX Liferacia Association | unite | | | | | Ĭ | - GAI Devices (427) |
| ces | - County | ox checycle Announcem | unus - | | | | | Store & Ohne 1 R. W. | T Services (4) |
| nfrastructure Devices | len e co | | 1. | lu | la co | land the second second | | views · rates · · | LabCore (11) |
| levice Components Connected End Hosts | IP Address A | Device Name | туре | Vendor | Model | EOX_Status (Devices) | End_of_Sale (Devices) | End_of_Support (Devices) | Network Management (3) |
| onnected IP Phones | 10.60.0.11 | tme-3560-48-p2r3-25.m | Switch-Router (99%) | Cisco | c8:3560x48 | End of Sale | 2016-10-30 | 2021-10-31 | Network Pending (5) |
| 8 Devices | 10.60.0.12 | ome-3750-48-p4r1-22.m | Switch (99%) | Cisco | catalyst3/xxStack | End of sale | 2016-10-30 | 2021-10-31 | Network w/o SNMP (15) |
| | 10.60.0.31 | cj3750-vian-patch.m | Switch (99%) | Cisco | catalyst37xx5tack | End of Sale | 2016-10-30 | 2021-10-31 | Routing (12) |
| | 10.00.3.34 | comp3750 | Switch-Houter (3976) | Cisco | cataryst3/xxStack | End of Sale | 2016-10-30 | 2021-10-31 | Security (4) |
| | 10 60 30 254 | SKO13-RE | Switch-Router (99%) | Cisco | catalyst37xxStack | End of Sale | 2016-10-30 | 2021-10-31 | Switching (18) |
| | 10.60.136.31 | csco-p4r3-34 | Switch-Router (99%) | Cisco | catalyst3560v248ps | End of Sale | 2016-05-14 | 2021-05-31 | Workstations w/o SNMP (|
| | 10.00.192.200 | p4r3-31.xxpq-labs.com | Switch (9976) | Cisco | catalyst37xx5tack | End of Sale | 2016-10-30 | 2021-10-31 | |
| | 10.00.102.203 | caco-peri-za. | Switch-Roonter (save) | Cieco | cataryst3/kkstack | End or pare | 2010-10-30 | 202110/01 | |
| | | | | | | | | | |
| al Devices | + | | | | | | | | |
| faces | + | | | | | | | | |
| | + | | | | | | | | |
| da | The second second | ALTEL & BLIME | | | | | | | |

4. You can run a report on the end-of-life devices. Navigate to Reports → Report Gallery → Asset → List EoX Cisco Devices.

| CON HIS YOUR ALTRON | Report Gallery Sched | uled Reports Report M | anager | | | | | |
|--|---|--|--|---|--|---|---------|---|
| | | | | | | | Add Cus | tom Report Import Custom Report |
| | Asset Inventory This report lists the devices meeting specific group criteria found to be on the network during a specific time period. | | Chassis Inventory This report provides a listing of physical components of devices found on the network during a specific time period. | Discovery Status This report provides details on network discovery status. | | Example: 100/Helf Interfaces Shows all the 100Mbps Interfaces running in half duplex mode. | 5 | Life Cycle Management This report shows the life cycle of each device |
| Run, Schedule, Eds, Export, Delete | List EoX Cisco Devices | The second secon | Managed Devices This report summarizes and lists the network devices managed by the system during a specific time period. | Virtual Asset Inventory This report lists the virtual devices contexts and their hosts NetMNI found on the network during a specific time period. | ************************************** | VLAN Interface Summary This report provides a summary of all VLANs found to be on the network during a specific time period. | | VRF Configuration Summary This report lists the VRF aware devices. |
| ∃ Change & Config | | | | | | | | |
| | Daily Config Changes Details Report all the configuration changes that have taken place in the last 24 hours. (Only shows the Running configuration) | Company Sales | Change Audit Summary This report provides a summary of the changes made to a group of network devices over a specific time period. | Config Change Audit Details This report lists the config changes made to a group of network devices over a specific time period. | | Config Change Audit Summary This report provides a summary of the config changes made to a group of network devices over a specific time period. | | Config Diff - Test |
| Configuration Management Configuration Management Sector Configuration Configu | Configuration Management Summary of the network devices a summary of the network devices meeting specific group criteria for which the system is managing configurations. | E | test Report all the configuration changes that have taken place in the last 24 hours. (Only shows the Running configuration) | | | | | |

5. Click on the Run button in the screen above. Select the device group and then click on the Run button.



6. The following screen appears.

| earch | | | | | | | | Mana Eller |
|-----------------------|---|---------------------------|-------------------|----------------------------|-------------|-----------------------------|---------------------------|--------------------|
| | and the second se | Concernence of the second | Call Sciences and | Construction of the second | - | Party and the second second | Constant Property and the | views · riders · · |
| amo | Model | Туре | Vendor | SNMP SysLocation | EOX_Status | End_of_Sale | End_of_Support | |
| ne-3750-48-p4r1-22.m | catalyst37xxStack | Switch | Cisco | | End of Sale | 2016-10-30 | 2021-10-31 | |
| ne-3560-48-p2r3-25.m | cat3560x48 | Switch-Router | Cisco | | End of Sale | 2016-10-30 | 2021-10-31 | |
| 4r3-31.kkptj-labs.com | catalyst37xxStack | Switch | Cisco | | End of Sale | 2016-10-30 | 2021-10-31 | |
| KO13-kc | catalyst37xxStack | Switch-Router | Cisco | | End of Sale | 2016-10-30 | 2021-10-31 | |
| omp3750 | catalyst37xxStack | Switch-Router | Cisco | Lab | End of Sale | 2016-10-30 | 2021-10-31 | |
| sco-p4r1-29 | catalyst37xxStack | Switch-Router | Cisco | | End of Sale | 2016-10-30 | 2021-10-31 | |
| 3750-vlan-patch.m | catalyst37xxStack | Switch | Cisco | | End of Sale | 2016-10-30 | 2021-10-31 | |
| sco-p4r3-34 | catalyst3560v248ps | Switch-Router | Cisco | | End of Sale | 2016-05-14 | 2021-05-31 | |
| | | | | | | | | |

7. This report can also be scheduled and sent to an email address on a periodic basis. Highlight the List EoX Cisco Devices report and click on the Schedule button.

| Infoblox 😵 🛛 | Dashboard Network Analysis | Network Explorer | Config Management Report | ts | | | | 4 4 0 |
|---|--|--|--|----|--|---|---------|---|
| CONTROL YOUN PALINGH | Report Gallery Sched | tuled Reports Report M | lanager | | | | | |
| | | | | | | | | 0 |
| | | | | | | | Add Cus | tom Report Import Custom Report |
| I Asset | | | | | | | | |
| | Asset Inventory This report lists the devices meeting specific group oriteria found to be on the network during a specific time period. | | Chassis Inventory This report provides a listing of physical components of devices found on the network during a specific time period. | | Discovery Status This report provides details on network discovery status. | Example: 100/Half Interfaces Shows all the 100Mbps Interfaces running in half duplex mode. | - | Life Cycle Management This report shows the life cycle of each device |
| Run, Schedule, Edit, Export, Délete | List EoX Cisco Devices | | Managed Devices This report summarizes and lists the network devices managed by the system during a specific time period. | | Virtual Asset Inventory This report lists the virtual devices contexts and their hosts NetfMRI found on the network during a specific time period. | VLAN Interface Summary This report provides a summary of all VLANs found to be on the network during a specific time period. | - | VRF Configuration Summary This report lists the VRF aware devices. |
| ∃ Change & Config | | | | | | | | |
| | Daily Config Changes Details Report all the configuration changes that have taken place in the last 24 hours. (Only shows the Running configuration) | A second se | Change Audit Summary This report provides a summary of the changes made to a group of network devices over a specific time period. | | Config Change Audit Details This report lists the config changes made to a group of network devices over a specific time period. | Config Change Audit Summary This report provides a summary of the config changes made to a group of network devices over a specific time period. | | Config Diff - Test |
| Andread of Management States of the Annual States | Configuration Management Summary This report provides a summary of the notwork devices meeting specific group: orthers for which the system is managing configurations | | test Report all the configuration changes that have taken place in the last 24 hours. (Only shows the Running configuration) | | | | | |

8. Select the Device Group and click Next.

| Date: 04/19/ Period: Daily Device Groups Device Search - All Devices (427) App Servers wio End of Support De It Services (4) It Services (4) Searchart Services (4) App Servers wio End of Support De All Devices (427) App Servers wio End of Support De It Services (4) MAME ONLY (146 | SNMP (0) vices (0) NMP (0) | Step 1 of 3: Select Time Variables and Device Groups |
|--|---------------------------------------|--|
| Date: 04/19/ Period: Daily Device Groups Device Search - App Servers (16) App Servers w/o End of Support De IT Services (4) IT Services (4) IT Services (11) AAME ONLY (145 | SNMP (0) vices (0) NMP (0) | |
| Period: Daily Device Groups Device Search - All Devices (427) App Servers w/o End of Support De IT Services (4) IT Services (4) Services (1) AME ONLY (146 | s SNMP (0) vices (0) NMP (0) | |
| Device Groups Device Search - Sall Devices (427) App Servers vio End of Support De IT Services (4) IT Services (4) IT Services (4) AME ONLY (145 AME ONLY (145 | s SNMP (0) vices (0) NMP (0) | |
| Search | SNMP (0) vices (0) VMP (0) | |
| All Devices (427) App Servers vio End of Support De IT Services (4) IT Services (4) IT Services (4) IT Services (4) NAME ONLY (146 Network Low-Ley | SNMP (0) vices (0) NMP (0) | |
| Network Manage Network Pending Network wio SNN NIOS (35) Optimizers (0) Routing (12) Security (4) Security (4) Security Control Switching (18) UNKNOWN (146) | ol (0) oleent (3) (5) P (15) | |

9. Type in the email address and select the recurrence pattern, execution time, and day. Click Next.

| List EoX Cisco Devices | Report | × |
|------------------------|--|---------------------------------------|
| | | Step 2 of 3: Select Report Scheduling |
| Report Name: | List EoX Cisco Devices | |
| To Emails: | management@xyzcorp.com | |
| To Users: | NetMRI Admin () dave signori () psirt psirt () support support () too tao () | |
| Output Format: | CSV | |
| Recurrence Pattern: | Weekly | |
| Execution Time: | 6:00 AM | |
| Sunday | Tuesday Thursday Saturday | |
| V Monday | Wednesday 🔲 Friday | |
| | | < Previous Next > Cancel |

10. Verify the settings are correct. Click Schedule.

| List EoX Cisco Device | s Report | 8 |
|-----------------------|-----------------------------|--|
| | | Step 3 of 3: Summary of Scheduled Report |
| Report Name: | List EoX Cisco Devices | |
| Date: | 04/19/2017 | |
| Period: | Daily | |
| Device Groups: | LabCore | |
| Devices: | | |
| To Emails: | management@xyzcorp.com | |
| To Users: | | |
| Schedule: | Weekly - Monday at 06:00 AM | |
| | | |
| | | < Previous Schedule Cancel |



in

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054 +1.408.986.4000 | info@infoblox.com | www.infoblox.com

© 2021 Infobiox, Inc. All rights reserved. Infobiox logo, and other marks appearing herein are property of Infobiox, Inc. All other marks are the property of their respective owner(s).