Analysis Use Cases in Network Automation

Overview

Device analysis allows you to determine if problems need to be addressed quickly or wait for a network change window. Heading off potential problems save time and money in the long run.

Current Situation

Without a product like Network Automation, you may never know about
- Device configuration changes and how often they occurred.
- Device compliance until the next analysis is done.
- Configuration issues.

Our Value

Without Network Automation, you may not know about a network problem until a call from a user is received. Network Automation provides you with the following screens for network analysis:

- Dashboard Views
    - Timeline Status Summary
    - Issue Summary
    - Change Summary
- Network Analysis
    - Issues by Type with Score Card
    - Issues by Type
    - Issues by Device
    - Changes
    - Policy Compliance
    - Performance

All of the views described below have the following in common
- Information can be view in the following timelines:
    - Daily: Select a single date in the currently shown calendar month.
    - Weekly: Sunday to Saturday seven-day period containing the selected date.
    - Monthly: Entire calendar month containing the selected date.
    - 7-Day: Seven days ending with the selected date.
    - 30-Day: Thirty days ending with the selected date.
    - The timelines can be selected by clicking on the little clock just below the Infoblox logo
- Information can be categorized by device groups. Device groups are a Network Automation organizational unit that gathers devices in related groups. A discovered device will be placed into one or more device groups based upon the criteria of each device group. The device groups are displayed on the right side of each view. Please refer to the administrator guide for more information.

Dashboard Views

Timeline Status Summary

This is the Timeline Status Summary. You can see the devices with the most changes over the past month in the upper left corner of the screen. Depending upon the location and use of these devices, this could be a normal or abnormal. You can click on the individual graph to drill down for details on the changes. The change graph on the bottom of the screen shows when changes occurred. This allows you to determine if the spike in changes correlates to a network event.

The pie chart shows policy compliance percentages. You can click on any part of the pie chart to drill down to the details of the policy compliance. The recommendation is to focus on the info, warnings, and error portions of the pie chart.

The Percentage Policy Compliance graph shows the passed percentage over time. A good trend is increasing percentage of compliance over time.

The middle graph is the issue variation graph. This graph tells the score for that day, the delta (more or less issues from the previous day) of issues. A good trend is a decreasing issue variation.

The middle section shows the overall score, info count, warning count, and error count. The issues can be narrowed down by the nine categories below. The overall score is based upon stability and correctness. The number itself is less important than the trend of that number over time; if the score decreases over time, then there may be issues of network stability. If the score increases over time, then network stability is improving.

Issue Summary
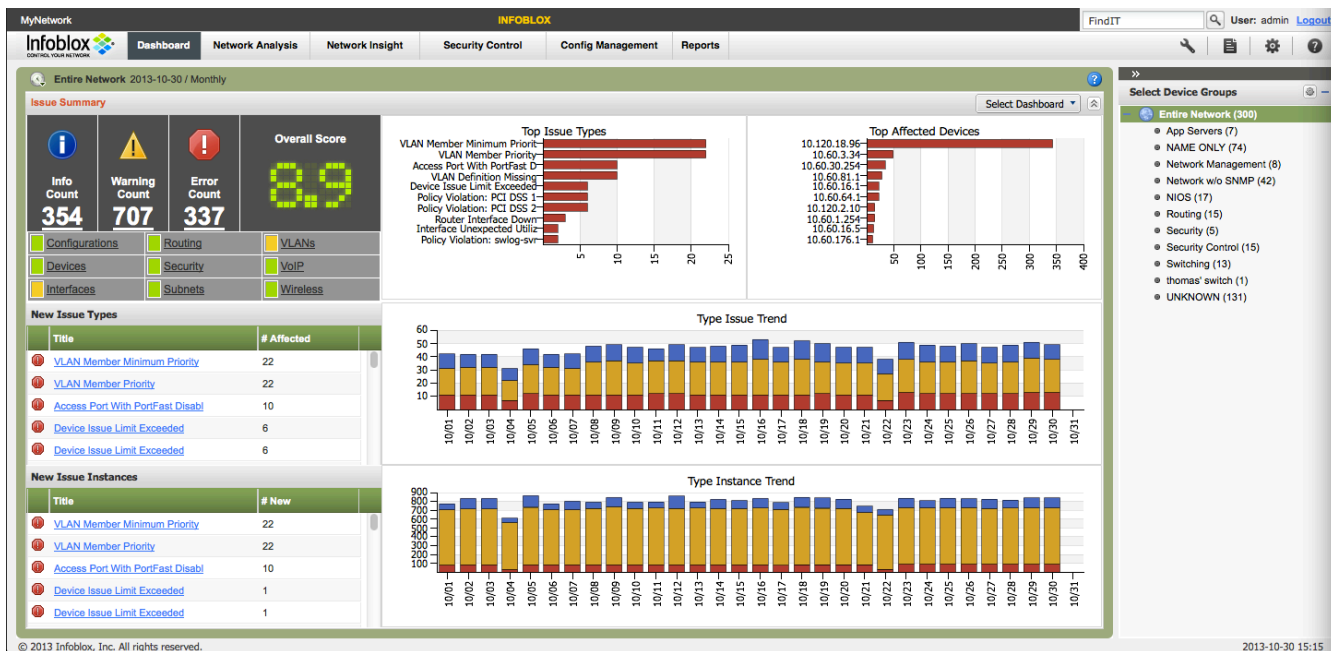
The issue summary dashboard shows:
- Network Score Card – the score is an indication of correctness based upon issues discovered. The less issues, the greater the score. The more issue, the lesser the score.
- Lists new issue types and instances. New issue types are issues that have occurred on other devices, but that are recently detected on the devices. New issue instances are new issues that have occurred
- Type issue trend
- Type instance trend
- Top affected devices
- Top issue types

The two most important graphs to analyze are the top issue types and top affected devices. This will point you to what issues need addressing the most on the devices that are most affected. This allows you to address the issue before they become noticeable by the user community.

Change Summary
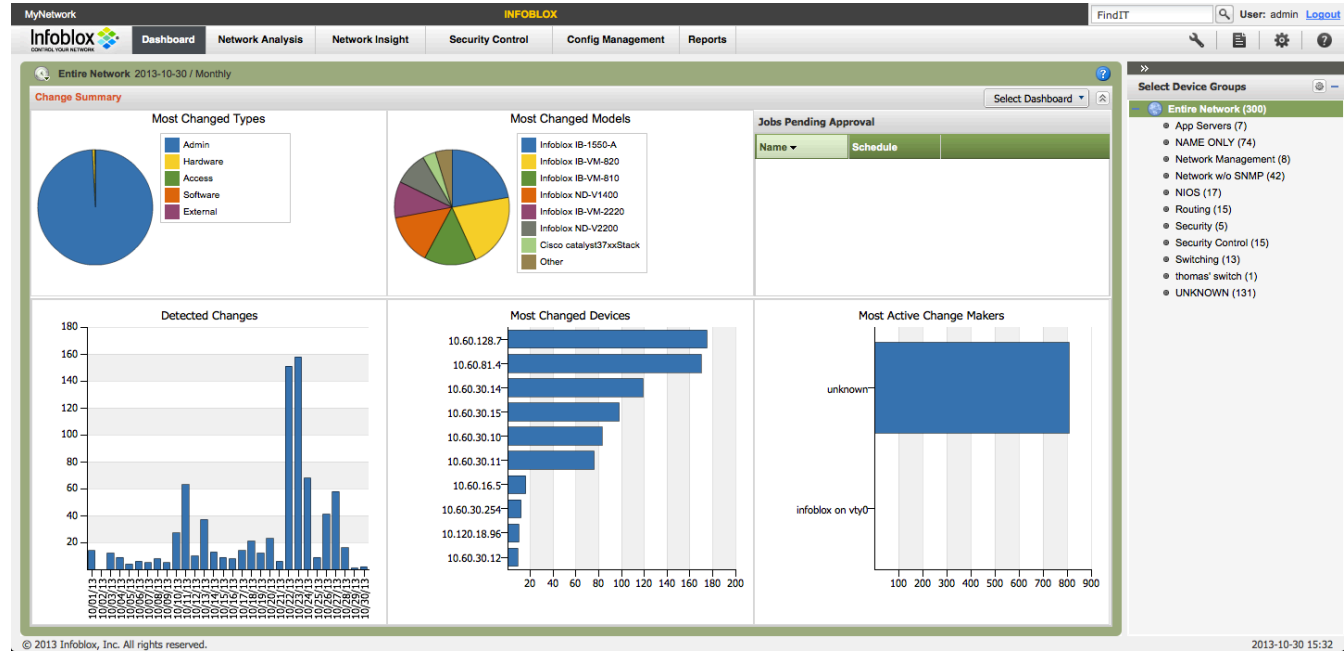
The change summary screen shows device configuration changes in the following manner:
- Most Changed Types. The following are definitions for each category:
    - Admin: changes to the actual configuration files on the device(s);
    - External: changes to the devices in the notification that are carried out by an external source, such as a change to the DNS record on a device;
    - Hardware: notification of a change in a device's hardware configuration, such as the removal or addition of a network module or line card;
    - Software: notification of a change in the device's software/OS version.
- Most Changed Models. Shows the type of devices that incurred the most changes.
- Detected Changes. Shows the amount of changes that occur on each day.
- Most Changed Devices – Shows the IP address of the devices that had the most changes.
- Most Active Change Makers – Show the username that was making those changes.

All parts of the summary page are clickable to drill down for more details. The graphs that are most important to notice are detected changes and most changed devices. Do the detected changes correspond to a day whereby many changes were taking place or were the amount of changes were unusual for that day? Is the most changed device(s) considered normal for those devices or is this something that is abnormal?

Network Analysis

Issues by type with score card

This is the main screen that you see when you log into Network Automation. From here, you can look at the issues are displayed and click to drill down on any one of them for more information. The issues can be group by any one of the nine categories.

When you click on a bar on the bar graph, you will see issues for that day.

Issues by type

This screen is shows all of the issues found within the last month. You can click on any of them to get a list of devices that are affected by this issue. This serves as a launch point towards troubleshooting and resolving the

issue with the network device(s). The screen can be modified to show issues on a daily, weekly, monthly, 7-day, or 30-day basis.

Issues by device with historic chart
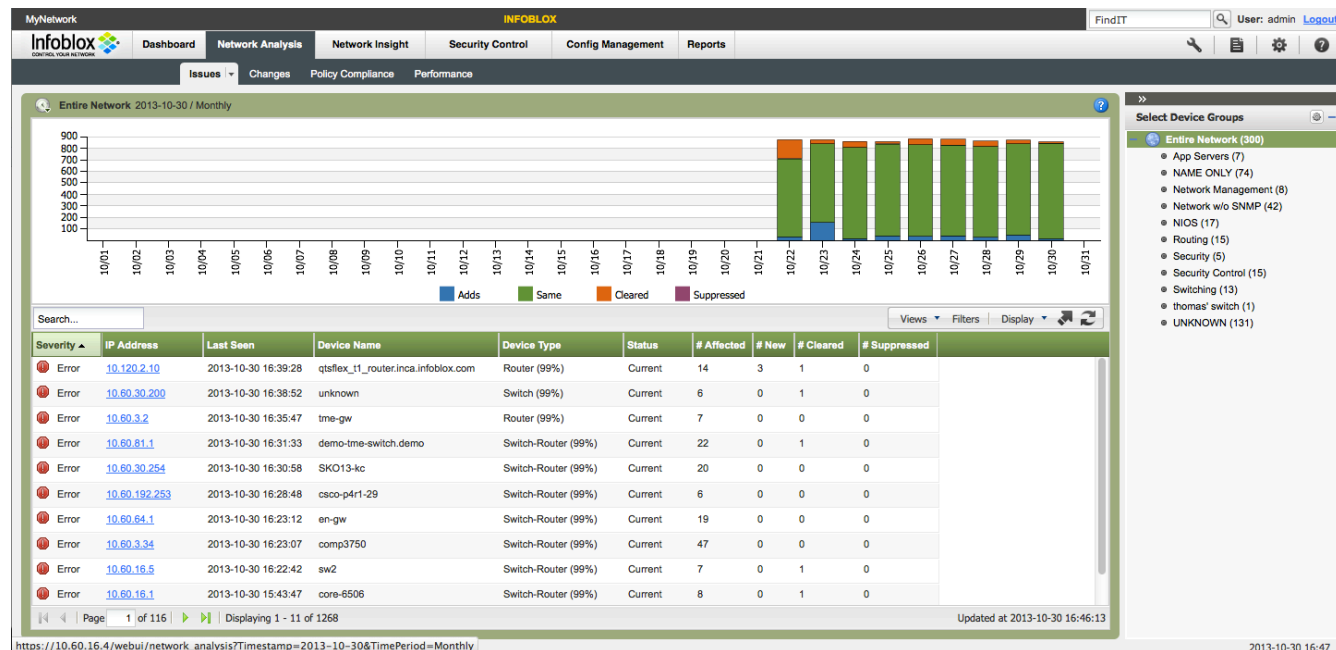
This chart shows the devices that have issues detected. You can drill down the IP address to see what issues were detected on the device. The Historic chart displays up to four data sets:

- Adds, indicating the quantity of new Issues for each time period.
- Same, indicating Issues the time period that remain from the preceding time period.
- Cleared, indicating Issues that have been cleared from the system due to administrative remediation or other causes.
- Suppressed, which shows the relative quantity of Issues that have been suppressed due to admin configuration of Issues that may be deemed to produce excessive notifications in each time period.

Issue counts for each time increment appear as stacked bars in the chart. Move the mouse over any colored bar section to view the count for that Issue type.

Issues by Device

The issue by device summary shows the same information, but without the historical graph. You can drill down on the IP address to see what issues need to be addressed with the device.
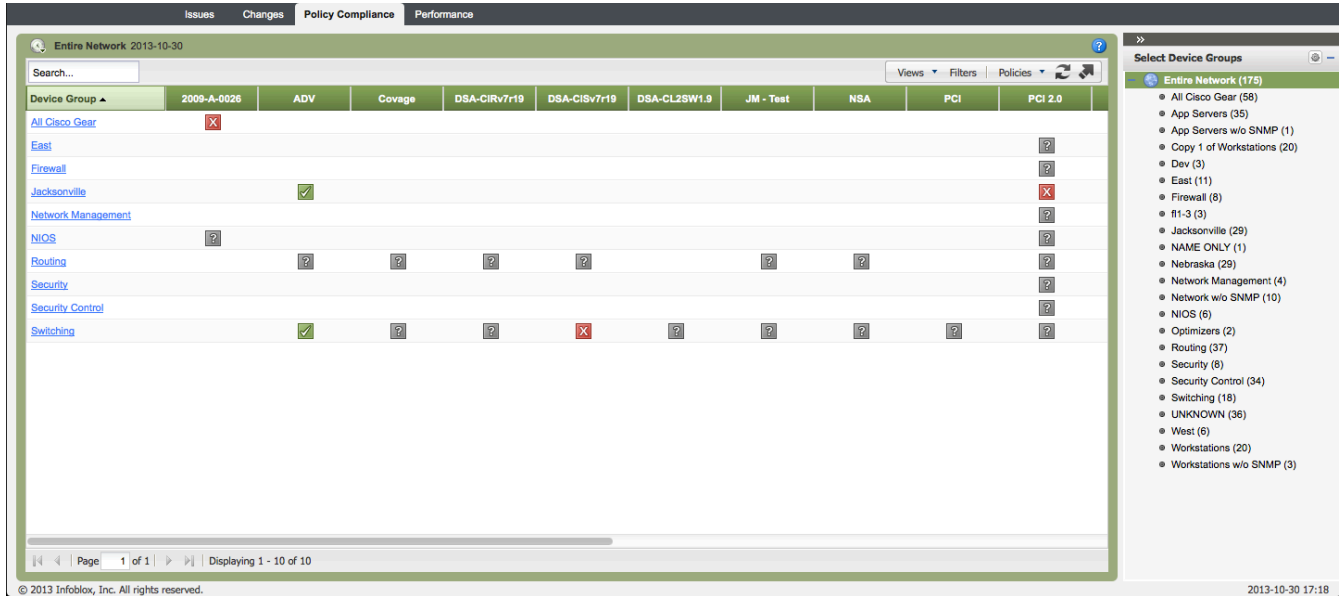
Changes

The Network Analysis Changes screen shows the devices that had changes within the last time period (ie daily, weekly, monthly, 7-day, or 30-day). The changes can be view by click on the Actions wheel. This allows you to see what changes occurred. You can also click on any of the bars in the bar graphs to get more detail on the changes too.

Policy Compliance Tab

The Policy Compliance tab shows the status of compliance for each device group if entire network is selected or for each device within a device group. You can click or hover on the boxes to get compliance details or compliance statistics respectively. Xs mean the device group or device did not pass compliance for that compliance policy. Check mark means the device group or device passed for that compliance policy. ? means policy status was skipped, unknown, or invalid for that compliance policy. Xs or ?s are worth investigating for non-compliance.

Network Analysis Performance tab
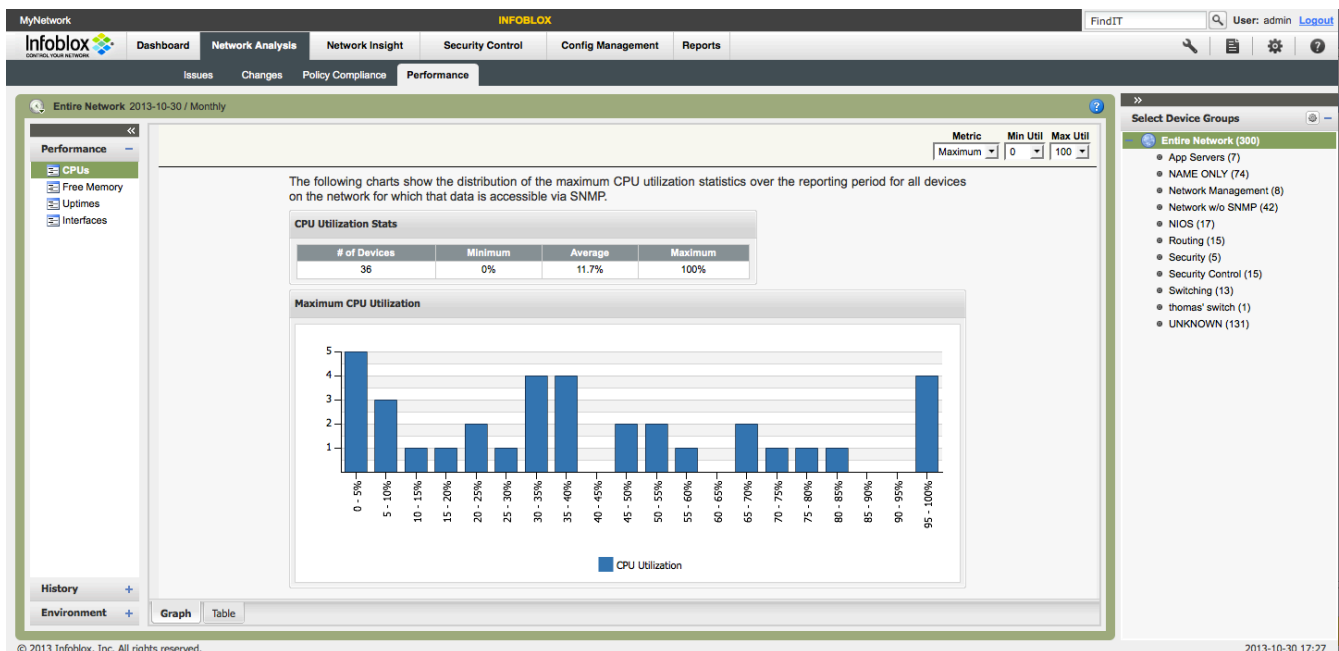
The Network Analysis Performance tab shows the following:

- Performance
    - CPU- is the CPU of the devices all running within normal range for your network?
    - Free Memory-is the memory utilization for each device normal for your network?
    - Uptimes-is the uptime correct for each device
    - Interfaces-is the interface utilization correct for each device?
- History
    - Devices-charts the number of devices discovered for the entire network or device group.
    - HSRP/VRRP groups - charts the number of HSRP/VRRP groups discovered for the entire network or device group.
    - Issues-charts, issue history, and issue differences.
    - Reboots-charts the number of reboots for the entire network or device group.
    - Routes- charts the number of routes discovery for the entire network or device group.
    - Subnets - charts summarize the types of subnets discovered on the network being analyzed.
    - VLANs - chart shows the number of distinct VLANs discovered on the network being analyzed.
- Environment – shows the voltage, temperature, power supply presence, and fan status.