Procedure - Completing a Network Assessment Using Auvik

Intent of this document

This document is intended to guide you through a complete network assessment as part of a regular or requested review for a site or location. A network assessment can also be used to benchmark a new site that's being onboarded, such as during an acquisition. It's highly recommended you run Auvik on a site for at least a week before completing the assessment report so you can collect a good set of data and spot trends.

Pre-requisites

Before starting a network assessment at a new site, make sure you have:

- Login credentials for the site's firewall, switches, and access points (see <Password Manager Tool>). If you're adding WMI or VMware for the site, grab those credentials as well.
- SNMP read-only community strings for all network devices, if SNMP is already enabled
- Domain administrator credentials for Windows Remote Management (WinRM) setup
- Access to a Windows server to deploy the Auvik Windows collector OR access to an ESXi host to deploy the Auvik OVA collector
- All data from <toolsets> being pushed to <documentation tool>
- A new network assessment report document set up from the template and ready to go

1/ Deploy Auvik

Follow the steps in the SOP called **Deploying Auvik on a New Network Site** to get Auvik installed. If you've already deployed Auvik, make sure the collector is on and running.

If you're going to review traffic as part of the network assessment, make sure NetFlow is on and is being pushed to the Auvik collector so traffic patterns are viewable in Auvik TrafficInsights.

2/ Grab a week's worth of data from the network

It's always good to parallelize tasks if you can. A large part of the work in a network assessment is gathering data about site infrastructure and how that infrastructure performs over a set period of time.

1) Open the site in Auvik.
2) Go to the home dashboard and select a date range of at least one week. (If you're assessing an existing site, you can load more than a week's data if you think it will prove helpful.)
3) Click the Export button.

4) Continue to step 3 while the data downloads. Check back on it once step 3 is complete.

3/ Filter the network map and export

The easiest way to communicate about the network to non-technical stakeholders is to provide highly visual and easy-to-read network maps. Auvik makes such maps easily shareable.

1) On the Auvik map for the site, apply the Network Elements Only filter. Export the map in SVG format.
2) Create any other map filters we commonly use that you think would provide insight into the site's network infrastructure and potential future improvements. Focus on things that would have a significant positive impact to the users. Export any resulting map views in SVG format.
3) Add the maps in the appropriate spaces in the assessment report.
4) Write descriptions of what each map shows so the reader can understand what they're looking at if you're not there.

4/ Grab the network device inventory

Focus on the network devices to highlight the underlying network infrastructure powering the site.

1) Go to the Network Elements tab in the Microsoft Excel file downloaded in the data export in step 2.
2) Sort the list by Type. Remove the columns you don't need for your report, such as Status, Network(s), and Connected To.
3) Optionally, add a column called Notes for any additional comments. For example, you may want to note that a device should be replaced or needs to be reconfigured.
4) Take a screenshot of your inventory list and put it in the appropriate space in the report <or embed the sheet in the network assessment report if you're using tools that allow it>.
5) Write a description of what the inventory shows and what it means. If you can easily do so, make connections from the inventory description to the map so the reader gains new context for both sections.

5/ Identify improvement opportunities for firmware and software versions and warranty coverage

Get a list of software and firmware versions for key devices

1) Go to the Devices tab of the data spreadsheet you downloaded in step 2.
2) Filter the list to focus only on network devices.
3) Remove unnecessary columns, such as device name andstatus.
4) Optionally, copy the Recommended Software Versions column from the Recommended Versions tab of the spreadsheet.

5) Optionally, add a column called Notes for any additional comments. For example, you may want to note a known security vulnerability with a listed software or firmware version that has since been fixed by an update.
6) Pull the list of software and firmware versions into your report in the appropriate section.
7) Write up a description for the information.
8) In the recommendations session at the end of the report, add any recommendations or items that need updating as soon as possible.
9) If there are updates you can make without taking the device down and you know these would delight the stakeholder, make those updates.

Get warranty coverage information for key devices

1) Go to the Warranty Status tab of the data spreadsheet you downloaded in step 2.
2) Optionally, add any notes you have about the warranty coverage.
3) Pull the warranty status list into your report in the appropriate section.
4) Write up a description for the information. You'll likely want to go into detail about why warranty and service coverage is important.
5) In the recommendations section at the end of the report, add any recommendations or items that need updating as soon as possible.

6/ Identify how the network is being used

A network assessment isn't just about the nuts and bolts of the hardware, but also about who's using the network and how. We need to make sure the infrastructure that's in place meets the needs of those using it and will fit the site's needs as the business grows and their needs change.

Look at WAN interface utilization

1) From the home dashboard in Auvik, take a screenshot of the All Internet Connections widget.
2) Pull the screenshot into your report in the appropriate section.
3) Write up a description for the information. Make sure to list the dedicated bandwidth that's part of this site's internet package. The data here may illustrate if a service upgrade is needed.

Assess quality of internet service

1) In Auvik, open the Internet Connection Check.
2) Set the time frame to the last week.
3) Check to see if the round-trip time or packet loss has been good for the past week.
   a) If there were any spikes or patterns that are cause for concern (meaning the internet wasn't performing as expected) include this information in your write-up and what it means from a user perspective.
4) Take a screenshot of the round-trip time and packet loss graphs. Include them in the report and write a small description of what these graphs mean and what they show.

Top devices consuming network resources

1) In Auvik, take a screenshot of the Top Devices by Utilization report for the last week.
2) Pull the screenshot into your report in the appropriate section.
3) Open Auvik TrafficInsights for the site and load a week's worth of data. (Skip this step if the site doesn't have NetFlow performance monitoring through TrafficInsights enabled.)
4) Dig into any traffic spikes during the week to see what applications made up the spike.
   a) If it wasn't legitimate business traffic, isolate it and take a screenshot to include in your report. Find out who the top talkers are for this application and make a note for yourself about whether it's on an end-user machine.
   b) If it's legitimate business traffic, isolate it and take a screenshot to include in your report. Find out who the top talkers are to see if there's a server or service running when it might not need to. Otherwise, check to see if the traffic is pushing the limits of the current internet package. If so, include your findings in your report.
5) Remove any traffic or time filters in TrafficInsights and switch to the geolocation area to see if there's high source or destination traffic to any unapproved countries.
   a) If yes, take a screenshot and include it in your report. You can also isolate traffic data by clicking on a country. Feel free to include a country-focused screenshot if you think it will provide additional insight.
6) Summarize all the information you learned about the site and its users in your report.

7/ Audit site credentials

With security top of mind these days, the credentials audit is an opportunity to uncover what's already in place and good, or what can be improved. Most users don't think about what vulnerabilities could exist within the network architecture itself.

See what credentials are being used and where

1) In Auvik, go to Manage Credentials <or password management tool/database>.
2) See how many devices are using the same set of credentials.
3) If any devices are using default credentials (for SNMP: private or public / for login: admin or cisco) add a recommendation in the report to update them.
4) Take a screenshot of both the SNMP and login credentials screens and include them in your report.
5) Write a description to support the screenshots. Focus on the importance of including network infrastructure in any security strategy. If a number of devices use the same credentials, be sure to point this out.

8/ Audit open issues (situational)

In this audit, we're looking for current issues that may be negatively affecting the site. The goal is to identify these issues so they can be resolved.

Review alerting trends

1) <In Auvik, go to the All Alerts dashboard or go to the board in your ticketing system> and review the tickets created for the site over the past week.
2) Look for trends, like the same device triggering a number of alerts or the same alert firing consistently around the same time of day. If you find something, dig a bit deeper

to see if you can identify the root cause of the alerts being triggered. If you don’t find anything, you can omit this section from your final report.

a) If you find something, include relevant information and screenshots in the report as to what you found and its impact. Be sure to add the solution to your list of recommendations at the end of the report.

9/ Develop the action plan

Throughout this assessment, you’ve been adding actions and strategies to the list of recommendations at the end of the report. Now it’s time to summarize all the information.

Include a list of actions you’ve already taken

If you made any changes to the network because of information uncovered during the assessment, note them. If reasonable, also include why the changes you made were positive and necessary.

Create and sort your list of recommended changes

1) Compile your list of recommended changes in rough somewhere separate.
2) Assign a severity level to each item. (High, medium, low is fine.)
3) Assign each item an estimated dollar amount based on how much the solution will cost to implement.
4) Sort the list in order of severity, from high to low. If you think two items have the same severity level, put the less costly one to implement first.
5) Put the list of ordered recommendations back into your report. If there are costs associated with a recommendation, include that information if it will be valuable to the reader.

10/ Finalize your network assessment report and send it to relevant stakeholders

Review the report from top to bottom, making sure there aren’t any typos, missing images, or incomplete sections. Once you’re happy with it, send it to the relevant stakeholder(s).