Domotz Pro Evaluation

In an attempt to troubleshoot a complex network issue with limited visibility, Domotz Professional was one solution to enable monitoring of the network remotely. This solution is available on a variety of platforms including AWS, Docker, Netgear ReadyNAS, QNAP, Synology, VirtualBox, or as a hardware appliance. As I have a Synology, so I'll be using that for the test.

Installation -

Installing the package on Synology is super simple as it is available in the Package Center. Once installed, open the Domotz Hub and it bring you to the Domotz page to sign in or create an account. The 14-day trial does not require a credit card. Once entering name, phone number, etc. you'll need to set up the first agent which requires a unique name.

Initial Scan -

Upon activating the trial, a scan of the network is conducted. In my lab which is fairly complex this took less than 2 minutes to complete. The scan establishes a link to the account, creates the database for the agent, discovers and classifies network devices, scans for open ports, looks for network infrastructure, and validates data in the database.

After the scan completed the dashboard discovered 20 devices and identified a partner integration with my network equipment.

Review of initial information -

Without changing any information the partner integration correctly identified the five pieces of UniFi networking gear. For some reason the UDM was not detected as part of the list. This integration allows for data from the controller to be fed into Domotz including ports, usage, and connected devices. Domotz Ubiquiti UniFi Integration - Setting up Domotz with Ubiquiti UniFi

The additional lab VLAN configured was not detected but no configuration was done.

Six devices were flagged as Important. The logic should be researched as it did flag the NAS, switch, and server but also flagged the printer and streaming media devices as important.

Within a few minutes of the initial scan a decent network diagram was generated. Some data was missing but I also didn't follow the guide to configure SNMP. I did validate in the UniFI controller SNMP was not turned on so the overview is pretty decent. The topology map can be searched and filtered. Network Topology - Domotz Help Center

Ports that are can create a encrypted overlay network to allow remote access to systems through https, ssh, rdp, and others. as well as an OpenVPN configuration that can be used through Tunelblick or OpenVPN. Access is logged and data transmitted is capped based on subscription.

Secure Remote Connection (domotz.com) and VPN on Demand - Domotz Help Center

Network Troubleshooting -

The Network Performance node shows basic information about the network including public IP, ISP name, gateway address, and DNS/DHCP information. The route analysis let's you test connectivity from the agent > router > ISP > and a 3rd party service including a custom URL. The details shows an average of loss and latency between each hop with the raw data showing data from MTR (combined traceroute and ping info). Any downtime is tracked (which could include the agent going offline). Alerts can be set up to send SMS or email alerts or the team can be alerted. The speed test shows averages over time (default scan is every 6 hours).

Powerful tools to give a boost to your network troubleshooting (domotz.com)

Logging and Reporting -

Reports can be generated and emailed including agent information, connection history, WAN performance, speedtest charts, device info, etc. Devices on the network can also be exported and sent via email.

Revision #1
Created 9 April 2024 02:18:26 by Matthew B.
Updated 9 April 2024 03:28:09 by Matthew B.