Foreman - Feature #25158

Sniff DHCP and TFTP network traffic and add them into audit

10/09/2018 12:54 PM - Lukas Zapletal

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Audit Log		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Interesting idea which is done by MaaS is to sniff network traffic (we would do this via proxy) and report it back as events. This can be then nicely presented in the Host - Audit page. A host requested DHCP IP address, requested TFTP file etc. This can be extended to more services etc.

- https://github.com/maas/maas/blob/master/scripts/dhcp-monitor
- https://github.com/maas/maas/blob/master/scripts/network-monitor
- https://github.com/maas/maas/blob/master/scripts/beacon-monitor

Related issues:

Related to Foreman - Tracker #25156: Ideas from MaaS	**New**

History

#1 - 10/09/2018 12:54 PM - Lukas Zapletal

- Related to Tracker #25156: Ideas from MaaS added

#2 - 10/09/2018 01:01 PM - Marek Hulán

By audit you mean log right? not the audits we display in UI or is that the goal?

#3 - 10/11/2018 09:34 AM - Lukas Zapletal

In MaaS you really see it in a host detail (node detail) on events page (we have audits for the same). So I was really thinking Foreman audits table, with host associated records so we can show them easily per-host.

I still think that all audits are subject of storing outside of RDBM, I know there is some extra work around associations but we have grown by far out of scope of the audited gem. But this is a different topic :-)

#4 - 10/15/2018 11:06 AM - Lukas Zapletal

- Triaged changed from No to Yes

#5 - 10/15/2018 11:11 AM - Timo Goebel

I love this feature, would really help to see what happens under the hood. Ideally, we could also enrich this data with access to templates, e.g. what https://github.com/ShimShtein/foreman_build_history does.

We actually don't need to sniff network packets to get the dhcp information. dhcpd can call scripts when certain events happen.