VOLTHA Security
VOL-278 Validate Least Privilege Permissions

2Q18 VOLTHA TST
4/10/2018

Tom Moore
tm9646@att.com

© 2017 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners. AT&T Proprietary (Internal Use Only). Not for use or disclosure outside the AT&T companies except under written agreement.

VOLTHA Security - Least Privilege Permissions

- Purpose – Verify User Story
- https://jira.opencord.org/browse/VOL-278 (Validate Least Privilege Permissions)
- As an Operator….
  I need to validate least privilege access on vOLTHA instances so that centralized NFV cloud resources maintain security compliance.
- I need to ensure privilege access for vOLTHA maintenance can not be elevated, so that NFV cloud resources in a multi-tenant environment maintain security compliance

- References for addressing concept of Least Privilege (limitation of Access Rights to a minimum level)
  - https://wiki.opencord.org/display/CORD/Security+in+CORD
  - "voltha-discuss" group

- Thoughts to Verify -
- What is the Role-based access definition for VOLTHA?
  - What roles are applicable in VOLTHA from CORD security? Including global (root) operators, infrastructure-specific operators, service-specific operators, service developers, and service tenants (including both end-users and other services)?
- vOLTHA instance deployment process
  - "voltha-discuss" includes discussion of privilege escalation policy used by the installer scripts to setup the cluster
    - Per the discussion, the installation process includes Ansible playbooks and uses escalation to 'sudo'
      - Sergio Slobodrian from Ciena responded that this would eventually change
        - ***Should involve a role-based security mechanism from an Ansible controller (for vOLTHA instance)? And/or from the Kubernetes orchestrator (for vOLTHA containers)?***

VOLTHA Security – Open in JIRA

Audit JIRA for other security functions - Searched “Security”, open items

- VOL-60 (**Execute a nessus scan on a running voltha cluster)**
- VOL-73 (**All servers in a voltha cluster must be secured)**
- VOL-262 (**SB Communication with the volha suite must be secure)**
  - VOL-266 , VOL-278, VOL-279

- Questions for other areas of Security (including but not limited to) –
  - Should we create a User Story companion to VOL-60 to analyze security perimeter of VOLTHA architecture?
  - Does VOLTHA need Identity and Access Management (IDAM) requirements?
  - For example - “audit trail logging” – do we need a User Story?
    - Is there a concept of a “transaction ID” (passed in API or from operator GUI/CLI) for tracking create/update/delete management actions in VOLTHA? The purpose of “transaction ID” is to support Logging for a historical view of “who did what and when”
    - Audit trail log only available to administrators
    - The transaction ID enables an operator to trace and correlate in a Northbound system
  - Are there other security functions we should capture in User Stories?

VOLTHA Security – Completed in JIRA

Audit JIRA for other security functions - Searched “Security”, closed items

- VOL-45 (**Secure East-west Inter Container communications between all voltha components/containers**)
- VOL-46 (**Secure East-west Inter Container communications between all voltha components/containers**)
- VOL-154 (**Consul Container comes up with Self-Signed Certificate/Key and SSL Config Files)**
- VOL-155 (**Registrator Container comes up with Self-Signed Certificate/Key)**
- VOL-209 (**Build Voltha/Consul Container with its own file system)**
- VOL-210 (**Build Voltha/Registrator Container with its own file system)**
- VOL-218 (**Secure Communication between Chameleon and vOLTHA Core)**
- VOL-219 (**Secure Communication between OF-Agent to vOLTHA Core)**
- VOL-264 (**REST Channel (External REST Client <==> Chameleon) needs to be Secured)**
- VOL-265 (**NETCONF Channel to vOLTHA in its North Bound needs to be Secured)**
- VOL-267 (**Calix Adapter to Calix OLT Communication needs to be Secured)**
- VOL-274 (**PONSIM Adapter to PONSIM OLT Communication needs to be Secured)**