Security Monitoring in a Nagios world

Chistos Triantafyllidis

OSCT F2F meeting

Overview

- Changes from SAM to Nagios
- Requirements from OSCT side
- Work roadmap
- Missing parts

From SAM to Nagios

- **SAM infrastructure**
  - SAM UI
    - Job submits / SE probes
    - Monitor probe results
      - *Feeding SAM DB*
  - SAM DB
    - Keeps result information for all probes
  - SAM web interface / PI
    - Read only access to the results or the monitored topology

From SAM to Nagios

- **Nagios infrastructure**
  - Nagios UI
    - Can be the same as the Nagios BOX
    - Job submits / SE probes
    - Monitor probe results
      - *Local Metric Store DB*
      - *Message broker network*
  - MyEGEE
    - Read only access to the results or the monitored topology

Changes in new infrastructure

- **Multi-level monitoring model**
  - Project level (to be deprecated)
    - Hosted at CERN
    - “lcgadmin” role for tests
  - ROC/NGI level
    - Hosted at ROCs/NGIs
    - Validation procedure
    - NGI/ROC VO groups
  - Site level (optional)
    - Hosted at sites

- **Results are published to the MQ for consumers**
  - Central DB
  - Web interface(?)

Changes in new infrastructure

- **Flexibility**
  - Nagios probes can be easily added/removed
    - At any level
    - No SAM validation
  - MDDB
    - Can deploy probe configuration at any level
- **Message Broker Network**
  - Allows the aggregation of results from any level to any level
  - Used for integration with other tools
    - GGUS
    - Operations Portal

Requirements from OSCT side

- **Secure transfer of results**
  - From probed node to the Nagios instance
  - From Nagios instance to any other consumer
- **Restricted ACLs for Nagios**
  - ROC / NGI Security officers
  - Site administrators
- **Ability to enforce new checks**
  - Without time consuming validations
  - Easily deployed

Work roadmap

- **Secure transfer of results**
  - ActiveMQ DOES support SSL encryption for connections
  - But this is not enforced for EVERY connection
  - Thus weaker side defines the system's security

- **Long discussions with both OSCT and OAT**
  - Decided encryption on message level
  - Results
    - encrypted on the probed node (WN)
    - decrypted on the probing node (Nagios)
    - Never being transferred un-encrypted over network

Work roadmap

- **Worked close with Emir (OAT)**
  - Nagios's host certificate is sent to the WNs
  - A simple shell wrapper is encrypting the result
    - Use of basic OpenSSL commands
  - The results are marked as being "encrypted"
    - Special handler at Nagios side
      - *Decryption*
      - *Non republished back to MQ*

- **Created a prototype**
  - Relies on the latest org.sam probes
  - Included at the latest org.sam.sec probes
    - Only a pakiti probe is included

Work roadmap

- **ACLs for Nagios**
  - In principal Nagios supports ACLs
  - Not clear if ACLs can be used for some services only
    - This an AP for OAT side
  - Proposed work-around scenarios
    - A dummy host per site
      - *GR-01-AUTH-secured*
    - A dummy host per host with security monitoring probes
      - *ce01.grid.auth.gr-secured*
      - *cream-ce01.grid.auth.gr-secured*

Work roadmap

- **Ability to enforce new probes**
  - New probes need definition in the MDDB
    - Should be easy via web interface
  - And the probe code deployed at the Nagios intances
    - Source of security monitoring probes managed by OSCT
    - Currently developed/used by AUTH (OSCT activity)
    - Separate package
    - Will be built centrally as all other OAT packages
      - *Source is available*
      - *Koji package to be built*
    - Jobs are submitted seperately of the normal CE probes
      - *We can't break their stuff*
      - *They can't break our stuff*
      - *No hard validation needed*

Missing parts

- **Secure transfer of results**
  - From probed node to the Nagios instance
    - Done
  - From Nagios instance to any other consumer
    - MyEGEE uses local DB connection
    - No other consumers are used
- **Restricted ACLs for Nagios**
  - This is an AP for OAT
- **Ability to enforce new checks**
  - Theoretical in place
  - Not ever used for our probes

Missing parts

- **Transition of current SAM probes**
  - There are 3 SAM probes currently
    - SW check
      - *Pakiti*
      - *Done*
    - Permissions check
      - *Done but not committed yet ☹*
      - *Depends on the ACLs issue*
    - CA/CRL check
      - *Code is almost migrated*
      - *Depends on the ACLs issue*

Missing parts

- **Alerting**
  - Do we need special alerting function?
  - No discussion for this yet
    - Probably this is a good place to do this
- **Management of ACLs**
  - Currently done via GOCDB
    - Is this sufficient?
    - Do we need another source?
- **Secure publish of results to MQ**
  - Central DB
  - Web front-end (?)

Questions?

Thank you…