Internal Auditing of Grid Operations Center Machines and Services

Presented here is an overview of a plan to verify the configuration of all GOC servers. Each section below gives a description of some part of that plan.

1 Cron auditing

Many GOC services depend on the periodic execution of scripts. One method to implement this is via and entry in a users (or roots) linux crontab. This method is volatile in that if a machine must be restarted or rebuilt the corntab must be re-installed. To avoid this all such periodic processes are specified by files in /etc/cron.d. A manual scan of all GOC machines has been completed and it has been verified there are no entries in crontab for any machine. Manual examination of /etc/cron.d has been completed and it has been verified that all existing files are appropriate. An automated version of the manual scan is being developed and will run periodically.

2 Firewall auditing

An automated method to determine the correctness of the firewall rules on all GOC machines will be developed.

3 File permission auditing

(under consideration)

4 Password auditing

(under consideration)

5 Backup auditing

An automated method to determine the existence of recent backups of all files associated with a GOC service will be developed. The manual scan referred to in section 1 showed many services were being backed up correctly.

6 Security patch update auditing

All GOC machines run RedHat Enterprise Linux 5. As of 25-Aug-2010 all machines (except the BDII servers) have the latest available RHEL5 update packages. On the second ITB release date in a month, any new updates will be applied to all ITB service instances. If no problems are detected, the same set of updates will be applied to production machines. Packages that become available between the ITB update and the production update will be considered untested and not installed on the production machines until the following update opportunity. This procedure keeps the operating systems within one month of the most current version.

7 Single point of failure analysis

Some components of the GOC infrastructure have been identified as a possible single point of failure. Among these are TWiki and OIM (single instance of each) and the VPN server in Indianapolis (single machine serving many servers). It is intended to systematically map out the dependencies of all services and servers to identify any other such possibilities

8 Service Logs and Alerts

Some failures are identified by sending mail to root on the host machine. Currently, these massages are forwarded to the system administrator and appended to a file on a single machine. Additionally, messages are piped to a script as they are received. It is intended that this script will contain heuristics to determine what level of action should be taken in response to a given message. It is currently being "trained", that is, filters to ignore routine events are being implemented.

9 Hardware and Network Auditing

Munin based monitoring is currently implemented on all machines. It is capable of generating alarms when a measured property of a machine exceeds tolerance. The tolerances are currently being tuned.

10 External Security Scan

The Indiana University Office of IT Security offers to scan any computer on the IU network for possible security problems. An initial scan has been completed and no significant issues were detected. It is anticipated this scan will be repeated every 3 months.

11 Recovery Procedure Auditing

When a service fails a procedure to recover should be followed. Currently, all services (except BDII) run on virtual machines and if a service fails, typically the virtual machine is rebuilt by an existing install script. A program to test these scripts has been initiated. The ITB instances of all services will be rebuilt periodically on ITB release days. It is anticipated that a few machines will be rebuilt per release day and the entire set of ITB VMs rebuilt in approximately 3 months.