

Configuration Baseline Variance Request for minosgpvm02
CD/SCP/REX Arthur Kreymer
01/31/2012

Background:

The MINOS experiment completed its offline migration to SLF 5 on Jan 19 2012, well before the end of SLF4 support at the end of February 2012. However, it would like to keep one system at SLF4 in case problems arise that require building software under SLF4 for comparison or debugging.

System function:

System minosgpvm02 is a virtual server. It currently allows interactive logins to all MINOS members, but it will be changed to allow connections using only one service, sshd, and from only one node, minos50.fnal.gov.

Access Enumeration:

Users: Minos NIS users

Access from: minos50.fnal.gov only

Services: sshd only

Variance Request:

The request is to keep minosgpvm02 at SLF 4 for up to six months beyond the February 29 end of support, i.e., no later than August 31, 2012.

Variance Remediation:

- Access is granted to Minos NIS users, and only by ssh from minos50.
- Iptables will be implemented to DROP all traffic EXCEPT:
 - o ssh/22 to/from minos50
 - o Bluearc and AFS file access
- Full logging and auditing are enabled and logs forwarded to clogger.fnal.gov
- Unneeded services (all but sshd) are disabled.
- The system will be shut down immediately if remotely exploitable security issues arise

Variance Impact:

If a variance is not granted, minosgpvm02 will be shut down. Possible impact to MINOS data analysis if problems arise that could have been diagnosed under SLF 4.

Variance Targets:

Minosgpvm02.fnal.gov

Variance Expiration:

No later than August 31, 2012.

Risks:

Obsolete OS no longer has vendor support or patches.

Proposed Mitigations:

See above under Variance Remediation. In addition,

- All machines have up to date MISCOMP and SysadminDB registrations
- System and service logs are forwarded to the Computer Security logging service
- Unneeded services will be disabled
- Positive network controls are implemented to limit connectivity between minosgpvm02.fnal.gov and minos50.fnal.gov for ssh with all other communications denied.