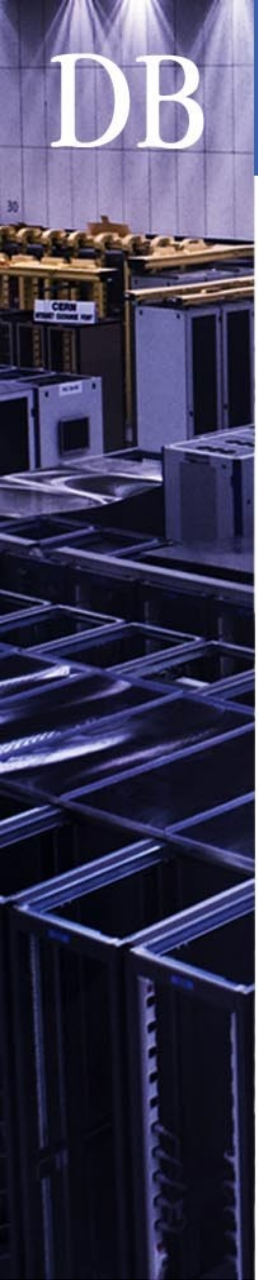
Tier1s open ports discussion

Distributed Database Operations Workshop
CERN, 16th November 2010

Dawid Wójcik

Tier1s open ports discussion

- All Sites’ replies visible here:
  - https://twiki.cern.ch/twiki/bin/view/PDBService/OpenPortsAtTier1s
- ASGC
  - no 3D DB at the moment
- BNL
  - no opinion
- CNAF
  - We have now opened LHCb to "any", but we'd like to restrict access to the Oracle ports to a list of reasonably known and safe networks, avoiding scans from the rest of the world.
- GridKa/DE-KIT
  - a few specific ports are open to the world (e.g. listener ports). Our preference is to allow a selected list of (safe) networks.



Tier1s open ports discussion

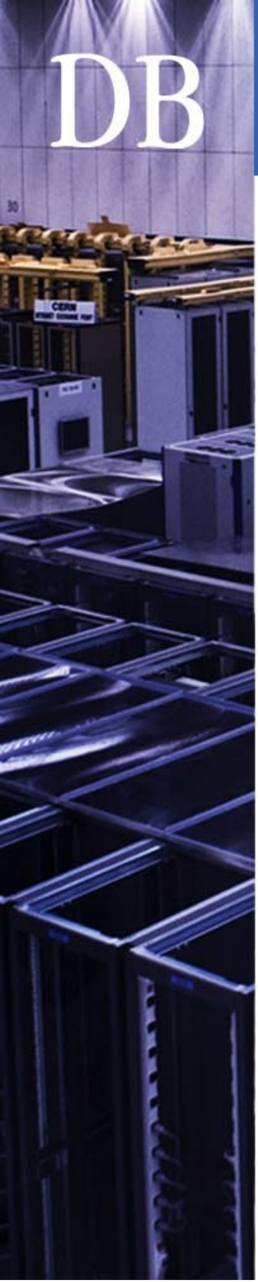
- IN2P3
  - there is no address-based filtering and for my part I think it would be fine to limit accesses. However, we should pay close attention to all possibilities and be aware of all consequences.
- NDGF
  - The 3D database servers at NDGF have the Oracle listener port open to the world. Access restrictions based on IP addresses/subnets would be welcome. We are only running ATLAS, not LHCb.
- PIC
  - We've opened listener ports to all the world, and oem agent's ports for oem server at CERN. It would be fine filtering connections to a restricted networks.

Tier1s open ports discussion

- RAL
  - I don't recall any special treatment for the DB systems other than to specifically open ports 1521,2121, 1830 and 5000-5002 inbound. There is no address-based filtering for inbound traffic specific to the nodes (other than the usual all-site-all-nodes restrictions). So access is generally blocked except for those ports. In terms of policy descriptions the closest is open-on-request. I expect we would prefer to allow any host access to appropriate ports at the firewall and implement host based blocking on the actual nodes.

Tier1s open ports discussion

- SARA
  - LHCb wants us to open our 3D oracle instance to the universe to enable them to access it from WNs on other T1s. We do not want to do this at SARA. However, we can make an opening for the WNs at T1s. Could you tell me in what subnets your WNs are so that we can open our firewall for them.
- TRIUMF
  - The only port that is globally open is 1521. Port 1830 is open to CERN (xxx.xxx.80.0 subdomain only) on our Oracle 3D ATLAS RAC.



Tier1s open ports discussion

- All sites share the idea of limiting listeners' ports access only to limited number of networks
- Possible scenarios:
  - Filtering on listener level
    - ☹ Unreliable (may hang listener startup if specified host does not exist)
    - ☹ Not possible to specify network ranges (must list all allowed hosts)
  - Filtering in iptables
    - ☺ Reliable
    - ☺ Possible to specify network ranges allowed or rejected
    - ☹ If filtering rules are changed, iptables restart may hang some connections in waiting state – tests required

Tier1s open ports discussion

- Regardless of filtering option chosen
  - Creating and maintaining list of allowed networks is time consuming
  - List of allowed networks may be site-dependant (?)
- Survey

Site	Has external conn.	Est. no. of networks	List highly dynamic	Accessed by Tier2
CERN	Y	120	N	Y/N
ASGC	-	-	-	-
BNL				
CNAF				
KIT				
IN2P3				
NDGF				
PIC				
RAL				
SARA				
TRIUMF