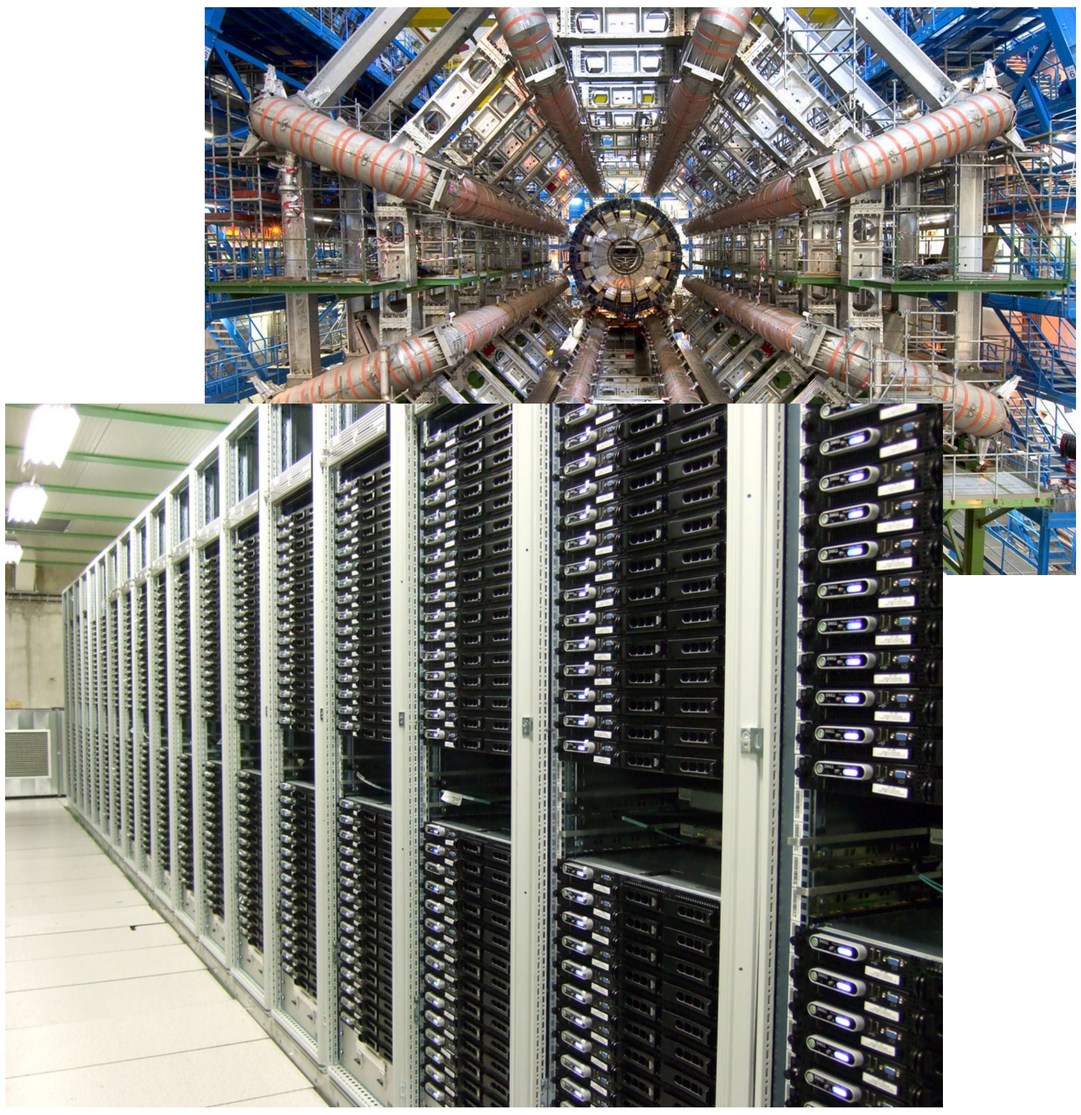
ATLAS TDAQ application gateway upgrade during LS1

S. Ballestrero, A. Bogdanchikov , F. Brasolin, A. C. Contescu, S. Dubrov, M. Hafeez, A. Korol , C. J. Lee, D. A. Scannicchio, M. Twomey, A. Voronkov, A. Zaytsev

Introduction

ATLAS is a particle physics experiment at the CERN Large Hadron Collider for studying data from proton and heavy ion collisions with energies per nucleon at the TeV scale. The ATLAS Technical Control Network (ATCN) connects the ATLAS online farm used for ATLAS Operations and data taking, including the ATLAS TDAQ (Trigger and Data Aquisition) and DCS (Detector Control System) nodes. The ATLAS Gateway service is a set of dedicated computers which provides a fine-grained access control between CERN General Public Network (GPN) and ATCN. From 2013 until the end of 2014 the LHC and the experiments are in the first Long Shutdown (LS1) state; this gave us a perfect opportunity to upgrade control software and configuration on the Gateway service.



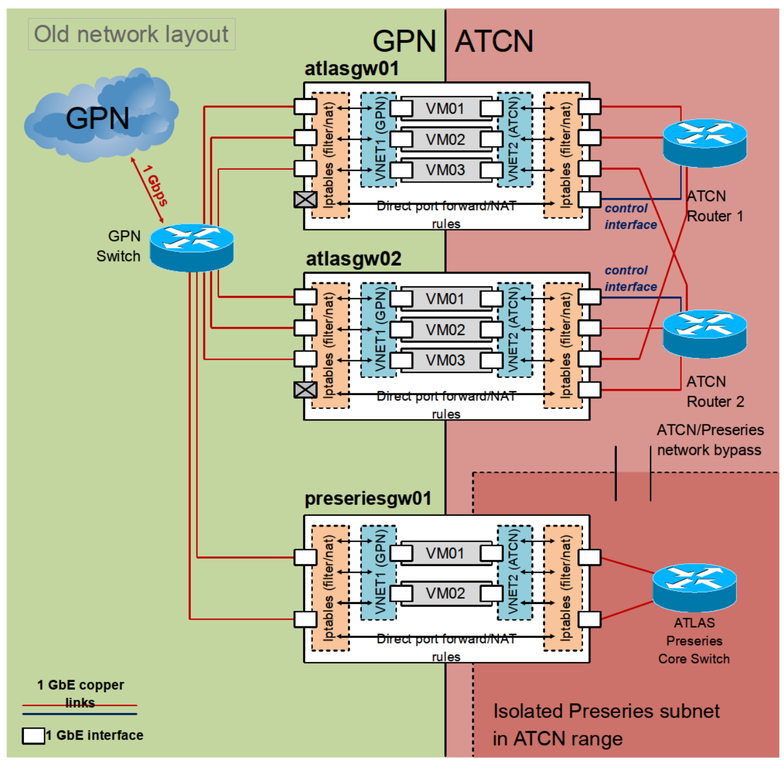
ATLAS Gateway functions

- SSH access from GPN to the TDAQ Linux based TDAQ hosts in ATCN.
- Remote desktop access from GPN to the DCS MS Windows hosts in ATCN.
- SCP/SFTP access to user (home) and detector (shared) data.
- Restricted HTTP proxy in both directions.
- Mail relay for ATCN hosts.
- Network Address Translation (NAT) for restricted set of TCP/IP connections from GPN to ATCN and from the special isolated test subnet of ATCN (preseries) to ATCN and GPN.
- Intrusion monitoring and prevention system.

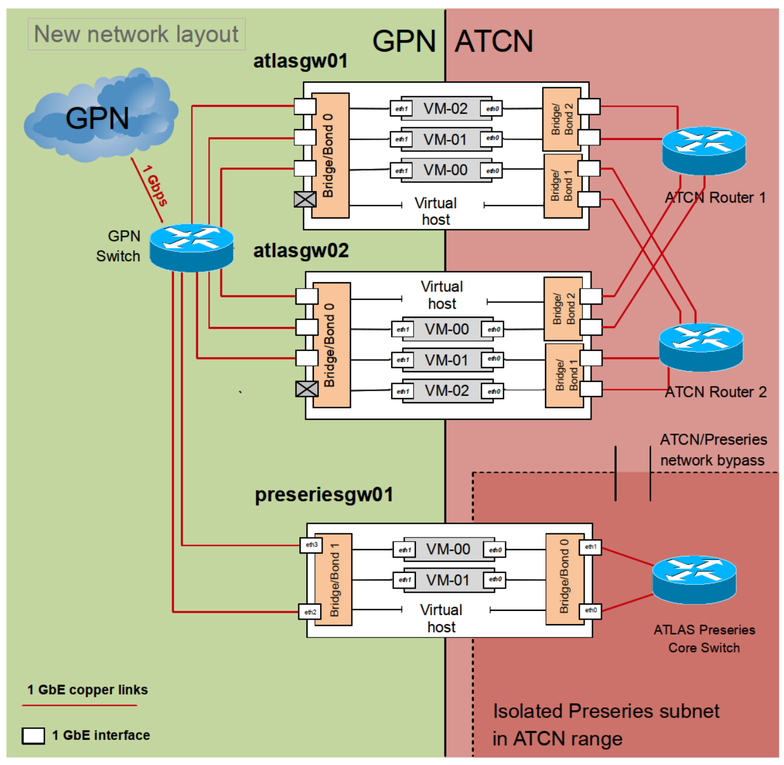
Old system architecture

Before this upgrade, each host system setup was based on one physical host using Scientific Linux CERN 5 (SLC5) and hosting several virtual machines (VM), using Xen v3 para-virtualization technology. The VMs were connected to two internal virtual networks. The iptables of the physical host provided a NAT for packets transfers from these internal networks to the actual ATCN and GPN connections. It also provided all dedicated, direct NAT transfers for ATCN and GPN hosts.

System architecture upgrade



- **Operating system** has been upgraded from **SLC5** to **SLC6** major release, which is now the recommended release for CERN and ATLAS experiment.
- **Virtualization technology** has been updated from **Xen** para-virtualization to **KVM** hardware-supported virtualization.
- **Internal networks** layers has been **removed**. Now the virtual machines are treated as independent hosts in the CERN network database[1] (LanDB) and are visible in the real networks (GPN and ATCN) through the **software bridge** and bonded physical channels. This greatly reduces the NAT rules and firewall configuration complexity. It will also allow the live migration of VMs to other hosts, in case of hardware issues.
- **All services**, including restricted GPN-ATCN NAT channels, are concentrated **on the VMs**. This makes the setup of the physical host as minimal as possible, providing only the virtualization service.
- The physical host and VMs are **configured** with **central Puppet**[2] configuration management system. Complex configuration items, like iptables and HTTP proxy configuration, are generated from templates. This greatly reduces the need for manual configuration and avoids misalignments of the configurations shared by all these VMs.



Implementation details of the current ATLAS Gateway

Intrusion detection and prevention

- **Samhain**[3] intrusion detection and report package.
- **RKHunter**[4] rootkit scanner package.
- **Fail2Ban**[5] intrusion prevention package.
- **Iptables** whitelist firewall rules.

HTTP proxy

- **Squid** proxy server package.
- **Samba**/**WinBind** server and ntlm helper for NTLM authorization.
- **Apache** web server package to distribute custom HTTP proxy autoconfiguration javascript file (proxy.pac).

Mail relay

- **Postfix** MTA package with rather straightforward network whitelist configuration.

SSH, SCP/SFTP and Remote Desktop access

- Login (SSHv2 protocol) to the Gateway host uses the **OpenSSH** package, patched to allow access restrictions according to LDAP netgroups.
- Privilege checks and further connections are made by the custom bash/perl set of scripts.
- The privilege check is done against the dedicated TDAQ Access Manager (AM), a Role Based Access Control (RBAC) system.
- Microsoft Remote Terminal access to DCS servers is implemented by the RDesktop package.

Network Address Translation

Iptables rules generated with the Puppet template from description, for example, this configuration line for the VM atlasgw01-01:

cname,host1,port1,host2,port2

will generate the following iptables rules:

-A BACKDOOR-POST-cname -s host1 -d host2 -p tcp -m tcp --dport port2 -j SNAT --to-source atlasgw01-01
-A BACKDOOR-PRE-cname -s host1 -p tcp -m tcp --dport port1 -j DNAT --to-destination host2:port2
-A BACKDOOR-FORWARD-cname -s host1 -p tcp -m tcp --dport port1 -m state --state NEW -j ACCEPT

Conclusions

During the LHC Long Shutdown 1 we performed a thorough upgrade of the ATLAS Gateway system. It included the transition to the last production release of the CERN Linux distribution (SLC6), the migration to a centralized configuration management system (Puppet) and the redesign of the internal system and network architecture. This upgrade has reduced the complexity of the system configuration and the risk of operational errors. By February 2014 the upgrade is fully completed.

[1] http://it-cs.web.cern.ch/it-cs/services/default.asp
[2] http://puppetlabs.com/puppet/puppet-open-source
[3] http://www.la-samhna.de/samhain/
[4] http://rkhunter.sourceforge.net
[5] http://www.fail2ban.org