Table of Contents

new LHCONE Acceptable Use Policy (AUP) -- still under construction (2020/02/17)

As agreed upon by the participants LHCOPN-ONE meeting on 2015/02/10. The final deadline for comments was 2015/02/27.

Preamble

The LHCONE is a dedicated network architecture inter-connecting participating HEP Sites and allowing those sites to pool their computing resources for a more efficient distribution, storage, processing and analysis of HEP data.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Definitions

- **HEP Site**: a high energy physics laboratory or university participating in and formally tied to one or more of the participating Collaborations listed in the next chapter;
- **HEP Service**: a computing resource primarily used to distribute, store, process and analyse the data generated by HEP Sites
- **LHCONE Site**: a HEP Site connected to the LHCONE L3VPN service;
- **LHCONE Prefix**: an IP subnet announced by a LHCOPN Site to the LHCONE L3VPN;
- **LHCONE Node**: a device using an IP address from a LHCONE Prefix to source or receive data;
- **LHCONE Traffic**: IP data traffic carried by the LHCONE L3VPN network, i.e. data traffic generated by a LHCONE Node and sent to another LHCONE Node;
- **LHCONE Provider**: National or International Network Service Provider (NSP) which provides network resources for the LHCONE L3VPN service;
- **WLCG Management Board**: the WLCG Management Board is responsible for LHCONE; all of the collaborations listed in the next section has to accept WLCG Management Board decissions.

Participating Collaborations and related information

The following Collaborations are currently participating in using the LHCONE:

WLCG

- The WLCG collaboration is documented on the web site http://wlcg.web.cern.ch/
- The WLCG collaboration is managed by the WLCG Management Board
- WLCG sites are listed on this web page
- WLCG Security Policies: WLCG Security Policies
- Additional information can be asked to wlcg.office@cernNOSPAMPLEASE.ch

Belle II

- The Belle II collaboration is documented on the web site http://belle2.kek.jp/
- The Belle II Computing Resources are managed by the Belle II Computing Steering Group (B2CSG)
- Belle II sites are listed in the Belle II MoU

- Belle II Security Policies: Belle II MoU. KEK is a member of EGI, thus compliant with WLCG security policies
- Additional information can be asked to belle2-wan-networking@belle2NOSPAMPLEASE.kek.jp

U.S. ATLAS

- The U.S. Atlas collaboration is documented on the web site http://www.usatlas.bnl.gov/
- The U.S. Atlas collaboration is managed by the U.S. ATLAS Operations Program Management Team
- The U.S. Atlas sites are listed on this web page: http://www.usatlas.bnl.gov/USATLAS_TEST/institutes,%20reps,%20emails.htm
- U.S. Atlas Security Policies: https://twiki.grid.iu.edu/bin/view/Documentation/PoliciesProcedures
- Additional information can be asked to U.S. ATLAS Computing usatlas-grid-l@listsNOSPAMPLEASE.bnl.gov

U.S. CMS

- The U.S. CMS collaboration is documented on the web site http://uscms.org
- The U.S. CMS collaboration is managed by the U.S. CMS Operations Program Management Team
- The U.S. CMS sites are listed on this web page: http://uscms.org/public_2/about/univs_labs.shtml
- U.S. CMS Security Policies: https://twiki.grid.iu.edu/bin/view/Documentation/PoliciesProcedures
- Additional information can be requested from the U.S. CMS Software and Computing Program Execution Team uscms-pet@uscmsNOSPAMPLEASE.org

Pierre Auger Observatory

- The Pierre Auger Observatory collaboration is documented on the web site https://www.auger.org/
- The Pierre Auger Observatory collaboration is managed by the Spokeperson
- Pierre Auger Observatory sites are listed in this web page
- Pierre Auger Observatory Security Policies based on EGI AUP
- Additional information can be asked to auger-distributed-computing@augerNOSPAMPLEASE.unam.mx and Jiri.Chudoba@cernNOSPAMPLEASE.ch

NOvA

- The NOvA collaboration is documented on the website http://www-nova.fnal.gov/.
- The NOvA collaboration is managed by the spokespeople
- The NOvA computing sites (both dedicated and opportunistic) are listed in this web page
- The NOvA collaboration security policies are based on the OSG Security Policies, including AUP
- Contacts for the NOvA experiment are Alex Himmel <ahimmel@fnal.gov> and Andrew Norman <anorman@fnal.gov>

XENON

- The XENON collaboration is documented on the website http://xenon1t.org/
- The XENON collaboration is managed according to this organization chart
- The XENON computing sites are listed in this web page
- The XENON computing security policies are described in this document
- Contacts for the XENON experiment are Luca Grandi <lgrandi@uchicago.edu> and Rob Gardner <rwg@uchicago.edu>

Process to include additional collaborations to LHCONE

Any scientific collaboration wishing to use the LHCONE services can ask to participate. The admission process is the following:

1. The collaboration presents itself, its computing model and network requirements to the community during a LHCONE meeting
2. The collaboration produces this information
    1. link to collaboration's description and documentation
    2. link to management board
    3. list of participating sites
    4. documentation of security policies
    5. - email address(es) of contact people
3. The LHCONE community accepts or rejects based on the impact on the LHCONE. Among criteria to be used in the evaluation:
    1. the collaboration must be related to Particle Physics
    2. a major fraction of the sites and collaboration s resources (CPUs and storage) must be already connected to LHCONE
    3. commitment to meet the technical and security requirements listed at the next point
    4. the bandwidth demand shouldn t have a significant impact on existing LHCONE data transfers
    5. commitment to participating and contributing to LHCONE meetings
4. Requirements to fulfil:
    1. comply with the WLCG security policies
    2. comply with the technical specifications of the LHCONE AUP concerning Announcement of IP Prefixes (LHCONE Prefixes) and Authorized source and destinations nodes (LHCONE Nodes)
    3. acknowledge the LHCONE AUP
5. The LHCONE community chairman informs the WLCG Management Board and WLCG Overview Board of the request and the decision
    - WLCG Management Board
    - WLCG Overview Board

Scope

This AUP is a set of policy requirements that applies to all LHCONE Sites. Its purpose is to define:

- which IP Prefixes must be announced for LHCONE Traffic;
- which nodes can be LHCONE Nodes;
- which HEP sites can be LHCONE Sites;
- consequences for non-compliance with this AUP.

LHCONE L3VPN Acceptable Use Policy (AUP)

Security incident reporting

A security incident is the act of violating an explicit or implied security policy. In line with WLCG Security policies requirements, LHCONE Sites MUST report suspected security incident as described in the WLCG Security Incident Response procedures.

Announcement of IP Prefixes for LHCONE Traffic (LHCONE Prefix)

A LHCONE Site announces to the LHCONE Provider's router a limited amount of IP prefixes (subnets) from its own public address range (see here for instructions on how to connect to LHCONE). These prefixes are called *LHCONE Prefixes*.

All LHCONE Traffic is subject to the following conditions:

- Traffic injected into the LHCONE can be originated only from addresses that belong to a LHCONE Prefix;
- Traffic injected into the LHCONE can be sent only to addresses that belong to a LHCONE Prefix.

This is essential to ensure traffic symmetry through any stateful firewall, i.e. enabling a proper TCP handshake. In addition, some sites might use the announced LHCONE Prefixes for traffic filtering in their stateful or stateless firewalls. Alternatively, LHCONE Sites can decide independently whether the LHCONE Traffic is allowed to bypass their own perimeter firewall or not.

Authorized source and destinations nodes (LHCONE Nodes)

IP addresses from the LHCONE Prefixes must be assigned to *LHCONE Nodes*, i.e. only to

- Nodes that are currently and primarily used to distribute, store, process and analyse the data generated by HEP Sites;
- Routers and switches for routing such data;
- perfSONAR probes and correspondent management infrastructure used for LHCONE.

The following devices must not be LHCONE Nodes:

- Generic campus devices (desktop and portable computers, wireless devices, printers, VOIP phones....).

Currently the following devices are tolerated as LHCONE Nodes:

- Computing nodes, storage elements and web servers not related with HEP computing services as long as they are managed according to the security policies agreed by each participating Collaboration. Relevant security policies documents are listed in the related section.

This exception is subject for later review.

Eligibility for Becoming a LHCONE Site

- Only HEP sites of one of the participating Collaborations can be connected to the LHCONE. Membership with a Collaboration can be verified by asking the contact emails provided in the related section;
- In order to be allowed to connect to the LHCONE L3VPN, a candidate site has to acknowledge this AUP. To acknowledge the AUP, a site representative has to
    - join the mailing list lhcone-operations@cernNOSPAMPLEASE.ch (https://e-groups.cern.ch/e-groups/EgroupsSubscription.do?egroupName=lhcone-operations)
    - send an email to the mailing list lhcone-operations@cernNOSPAMPLEASE.ch writing that the site acknowledges the AUP

Security incidents response and Non-compliance with the AUP

Policy violations and non-compliance issues MUST be reported to lhcone-operations@cernNOSPAMPLEASE.ch. Violations impacting the operational security of LHCONE MUST be reported as described in the WLCG Security Incident Response procedures. Severe or repeated violations MAY be escalated to *the WLCG Management Board and the offending LHCONE Site MAY be disconnected from LHCONE.

In addition, when confronted to policy violations or suspected security incidents, a LHCONE Site is allowed to drop the prefixes announced by the offending LHCONE Site at any time, disconnect itself from the LHCONE, as long as the changes are announced to the mailing list lhcone-operations@cernNOSPAMPLEASE.ch. The 65010:ASN LHCONE BGP community can be used to ensure symmetry.

Roles and Responsibilities

LHCONE Sites

- MUST abide by this AUP and all others applicable WLCG Security Policies;
- MAY define their own local security requirements with regard to traffic arriving from the LHCONE;
- MAY decide independently if the LHCONE traffic can bypass their own perimeter firewall or not.

LHCONE Providers

- MUST make sure that they connect to the LHCONE L3VPN only sites that are approved LHCONE Sites, that have also agreed to comply this AUP;
- MUST announce to the lhcone-operations@cernNOSPAMPLEASE.ch mailing list whenever a new site get connected to the LHCONE;
- MUST implement disconnection requests made by the WLCG Management Board;
- MUST implement BGP filtering based on LHCONE BGP communities.

the WLCG Management Board

- The WLGC Management Board

Related documents

- Grid Policy Documents;
- How to manage the routing for a Site connected to the L3VPN;
- [How to manage the routing for a Site connected to the L3VPN with SDN.

This topic: LHCONE > NewLhcOneAup
Topic revision: r4 - 2020-09-07 - BrunoHoeft