

Table of Contents

LHCONE Acceptable Use Policy (AUP)	1
Preamble.....	1
Definitions.....	1
Participating Collaborations and related information.....	1
Process to include additional collaborations to LHCONE.....	3
Scope.....	4
LHCONE L3VPN Acceptable Use Policy (AUP).....	4
Eligibility for becoming a LHCONE Site.....	4
Announcement of IP Prefixes for LHCONE Traffic (LHCONE Prefix).....	4
Authorized source and destinations nodes (LHCONE Nodes).....	4
Security incident reporting.....	5
Violations and non-compliance with the AUP.....	5
Roles and Responsibilities.....	5
Related documents.....	6

LHCONE Acceptable Use Policy (AUP)

As agreed upon by the participants LHCOPN-ONE meeting [↗](#) on 2021/03/23.

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. This AUP is to ensure an appropriate secure scientific use of the overlay network and to protect the connected sites.

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;
- **LHCONE Prefixes Database:** database of all the LHCONE prefixes being allowed in the LHCONE. The description of the Database and how to access it can be found at [this link](#)
- **WLCG Management Board:** the WLCG Management Board ensures it always has appropriate representation from all the LHCONE stakeholders, and thus the body responsible for LHCONE, in particular escalation of potential issues requiring arbitration; all of the collaborations listed in the next section agree to accept the WLCG Management Board decisions regarding the connectivity and security of LHCONE.
- **LHCONE Manager:** appointed by the LHCONE community and approved by the WLCG Management Board, is responsible for overseeing LHCONE in the respect of planning, maintaining and further development as well as administrative matters, and notably for maintaining a list of the sites that may connect to the LHCONE network.

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 obtained from wlcg.office@cernNOSPAMPLEASENOSPAMPLEASE.ch, or wlcg-security-officer@cernNOSPAMPLEASENOSPAMPLEASE.ch for security-specific questions.

Belle II

- The Belle II collaboration is documented on the web site <https://www.belle2.org/>
- 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 obtained from takanori.hara@kekNOSPAMPLEASENOSPAMPLEASE.jp and spardi@naNOSPAMPLEASE.infnNOSPAMPLEASE.it

U.S. ATLAS

- The U.S. Atlas collaboration is documented on the web site <https://po.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: <https://po.usatlas.bnl.gov/programoffice/institutes.php>
- U.S. Atlas security policies: <https://opensciencegrid.org/security/OSGSecurityPolicies/>
- Additional information can be obtained from U.S. ATLAS Computing usatlas-grid-1@listsNOSPAMPLEASENOSPAMPLEASE.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://opensciencegrid.org/security/OSGSecurityPolicies/>
- Additional information can be obtained from the U.S. CMS software and computing program execution team uscms-pet@uscmsNOSPAMPLEASENOSPAMPLEASE.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 spokesperson
- Pierre Auger Observatory sites are listed in this web page
- Pierre Auger Observatory security policies based on EGI AUP
- Additional information can be obtained from auger-distributed-computing@augerNOSPAMPLEASENOSPAMPLEASE.unam.mx and Jiri.Chudoba@cernNOSPAMPLEASENOSPAMPLEASE.ch

NOvA

- The NOvA collaboration is documented on the website <https://novaexperiment.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 Gavin Davies <gsd Davies@olemissNOSPAMPLEASE.edu>, Alex Himmel <ahimmel@fnalNOSPAMPLEASE.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@NOSPAMPLEASEuchicago.edu>

and Rob Gardner <rwg@NOSPAMPLEASEuchicago.edu>

JUNO

- The JUNO collaboration is documented on the website <http://juno.ihep.cas.cn/>
- The JUNO collaboration is managed by the project management
- The JUNO computing sites are listed in this web page
- All the JUNO sites connected to LHCONE are also WLCG sites and they agreed to adopt WLCG security policies
- Contacts for the JUNO experiment are:
 - ◆ Weidong Li, liwd@ihepNOSPAMPLEASENOSPAMPLEASE.ac.cn (JUNO offline L2)
 - ◆ Giuseppe Andronico, giuseppe.andronico@ctNOSPAMPLEASENOSPAMPLEASE.infn.it (JUNO offline L2)
 - ◆ Fazhi Qi, qfz@ihepNOSPAMPLEASENOSPAMPLEASE.ac.cn (part of IHEP network group)
 - ◆ Xiaomei Zhang, zhangxm@ihepNOSPAMPLEASENOSPAMPLEASE.ac.cn (JUNO DCI L3)
 - ◆ juno-lhcone@maillistNOSPAMPLEASENOSPAMPLEASE.ihep.ac.cn, mailing list grouping all the previous people

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
 - ◆ link to collaboration's description and documentation
 - ◆ link to management board
 - ◆ list of participating sites
 - ◆ documentation of security policies
 - ◆ 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:
 - ◆ the collaboration must be related to Particle Physics
 - ◆ a major fraction of the sites and collaboration's resources (CPUs and storage) must be already connected to LHCONE
 - ◆ commitment to meet the technical and security requirements listed at the next point
 - ◆ the bandwidth demand shouldn't have a significant impact on existing LHCONE data transfers
 - ◆ commitment to participating and contributing to LHCONE meetings
4. Requirements to fulfil:
 - ◆ comply with the WLCG security policies
 - ◆ comply with the technical specifications of the LHCONE AUP concerning announcement of IP Prefixes (LHCONE Prefixes) and authorized source and destinations nodes (LHCONE Nodes)
 - ◆ 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)

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 Participating Collaborations section;
- In order to be allowed to connect to the LHCONE L3VPN, a candidate site has to acknowledge this AUP. To confirm they read, understand and commit to abide to the AUP, the designated 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
- Once the two items above are confirmed, the LHCONE Manager will reply to the acknowledgement with the authorization to connect.

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 must originate only from addresses that belong to a LHCONE prefix;
- Traffic injected into the LHCONE must send 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.

All LHCONE prefixes must be declared in the LHCONE prefixes database

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;
- perSONAR 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....).

For sites which cannot segregate their networks, the following devices are tolerated:

- 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. The number of such devices shall be kept to a minimum. Relevant security policy documents are listed in the related section. related section.

Security incident reporting

Any violation of an explicit or implied security policy is termed a security incident. In line with WLCG security policies requirements, in addition to following local procedures, LHCONE sites must report suspected security incidents to wlcg-security-officer@cernNOSPAMPLEASENOSPAMPLEASE.ch and follow the WLCG security incident response procedures [☞](#).

Violations and non-compliance with the AUP

LHCONE participants are encouraged to resolve possible policy violations and non-compliance issues with one another, for instance via lhcone-operations@cernNOSPAMPLEASENOSPAMPLEASE.ch. Severe or repeated violations may be escalated to *the WLCG Management Board and the offending LHCONE site may be disconnected temporarily or indefinitely 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;
- Must connect only resources relevant to fulfilling the PREAMBLE of this AUP;
- May define (in addition to the WLCG security policies) 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;
- Must declare the list of their own LHCONE prefixes in the [\[https://twiki.cern.ch/twiki/bin/view/LHCONE/LhcOneVRF#LHCONE_Prefixes_Database\]](https://twiki.cern.ch/twiki/bin/view/LHCONE/LhcOneVRF#LHCONE_Prefixes_Database)[LHCONE Prefixes Database] and keep their entries up to date.

LHCONE Providers

- Agrees to only connect to LHCONE, organizations and/or route prefixes that the LHCONE Manager has agreed to accept.
- Agrees to announce any newly connected sites or prefixes to the lhcone-operations@cernNOSPAMPLEASENOSPAMPLEASE.ch mailing list
- Agrees to honor any written LHCONE disconnection requests from the WLCG Management Board for any organization that provider connects to LHCONE

- Agrees to implement BGP filtering based on LHCONE BGP communities.

Management Board

- Each Management Board of any LHCONE collaboration can request the disconnection from LHCONE of any LHCONE site which is not compliant with this AUP. In case of disputes, the ultimate and authoritative request must come from the WLCG Management Board
- The WLCG Management Board has the final and ultimate jurisdiction on its affiliated HEP/LHCONE sites and collaboration and the authority to withdraw a collaboration or ask a site to get disconnected

End Note: [1]: For reference: the key words MAY , "MUST", "MUST NOT" ,, "SHOULD", "SHOULD NOT" in this document are to be interpreted as described in RFC 2119

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 > LhcOneAup

Topic revision: r49 - 2022-02-09 - EdoardoMARTELLI



Copyright &© 2008-2022 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.

or Ideas, requests, problems regarding TWiki? use Discourse or Send feedback