CERN Firewall Closure

Introduction

"In order to better protect devices connected to the CERN network from the regular attacks initiated from off-site, direct connections to TCP and UDP ports of all devices will be blocked in the CERN firewall **by default**. Users can initiate client applications but not expose server processes. The default firewall functionality for the whole site will be equivalent to that currently available on the wireless network. Specific exceptions will need to be approved before server ports can be directly exposed to the Internet." CERN Firewall Closures Plan

Please note:

- 128.142.0.0 is not affected (already firewalled)
- 172.17.0.0 is not affected (no external access available)

The closure schedule is available from here.

Contact: Romain Wartel.

Firewall Closure annoucements

Annoucements will be posted here and to it-dep-gd@cern.ch.

MySQL Servers - Firewall Authorisation Required

GridFTP - Firewall Authorisation Required

From 13 JUNE 2006, prior firewall authorization will be required for servers to be reached from off-site on the following port number:

- TCP/2811 (GridFTP server)

From 20 JUNE 2006, the CERN firewall will not permit external access to unregistered CERN machines on the following port number:

- TCP/3306 (MySQL server)

The only GD nodes that have been identified as requiring their MySQL service to be available from the outside are the SFT (from RAL and IN2P3) and the RB nodes (from IC).

If you manage a service that also requires MySQL access from outside CERN, please contact Romain Wartel as soon as possible.

Plans for GD

GD has number of machines, and many of them are running Grid middleware. In order to understand exactly what ports need to be opened for the middleware to work **in practice**, a local firewall is being deployed on all the production nodes.

The deployment effort of this firewall and the discovery of potential issues is based on the LCG Nodes Status page. Please make sure it is kept up-to-date.

The list of machines that are using the local firewall is available here. **If any of your machine needs to provide a network service on a port >1024, you need to register it on this page by contacting Romain Wartel**.

Main cluster managers are being contacted to discuss their requirements regarding the opening of ports in the firewall.

The production machines are a priority, but other clusters **could** also be affected by the closure, hence system managers are advised to:

- Maintain the LCG Node Status page up-to-date
- Understand what network services are running on their machines
- Understand the firewall requirements of these network services

Support to handle the firewall closure (analysis of the affected systems, definition of the service requirements, implementation of a local firewall, gradual enforcement etc.) is offered for Prod, PPS and TB. Other services may benefit of some limited support, but unless it is agreed otherwise, they are expected to produce their own requirements.

Current Status (13 June 2006)

Production machines

The Prod machines have been firewalled.

PPS

The PPS has been firewalled.

TB

The TB has been firewalled.

Service Challenges

Not affected, except: lxgate22, lxgate24, lxgate26.

Others

Cluster managers are being contacted.

-- Romain Wartel - 20 Apr 2006

This topic: LCG > CernFirewallClosure
Topic revision: r7 - 2006-06-13 - RomainWartel