perfSONAR-PS Security Guidelines

**perfSONAR-PS Version:** 3.2

These guidelines are recommended in order to protect the LHCOPN from security holes currently existing in the perfSONAR-PS tool. Most of the LHCOPN perfSONAR-PS servers are reachable from outside the LHCOPN, and some security failures revealed by a security audit made on a typical perfSONAR-PS setup could present backdoors for hackers.

LHCOPN is not intended to be a public network and must be protected as best as possible. Simple changes to the perfSONAR-PS configuration and minor code modifications can avoid most of the security holes found during the audit.

**HTTPD server settings**

**In the /etc/httpd/conf.d/apache-toolkit_web_gui.conf**

Note: Changes made are in green bold:

```plaintext
# if the user is doing administrative tasks and didn't come in via HTTPS,
# redirect them for ALL pages
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/toolkit/.* https://%{SERVER_NAME}%{REQUEST_URI} [R,L]

Alias /toolkit /opt/perfsonar_ps/toolkit/web/root
<Directory "/opt/perfsonar_ps/toolkit/web/root">
  Options -Indexes FollowSymLinks +ExecCGI
  DirectoryIndex index.cgi index.php index.html
  AddHandler cgi-script .cgi
  AllowOverride All
  Order deny,allow
  Deny from all
  Allow from all
</Directory>

<Directory "/opt/perfsonar_ps/toolkit/web/root/*/*/etc">
  Options None
  AllowOverride All
  Order deny,allow
  Deny from all
  Allow from all
</Directory>
```

Virginie Longo – CERN 9-Dec-11
<Directory "/opt/perfsonar_ps/toolkit/web/root/*//*/templates">
  Options None
  AllowOverride All
  Order deny,allow
  Deny from all
</Directory>

<Directory "/opt/perfsonar_ps/toolkit/web/root/admin">
  Options -Indexes FollowSymLinks MultiViews +ExecCGI
  DirectoryIndex index.cgi index.php index.html
  AddHandler cgi-script .cgi
  AllowOverride All
  Order deny,allow
  Deny from all
  *  Allow from .localdomain.domain
  AuthShadow on
  AuthType Basic
  AuthName "Password Required"
  Require group wheel admin
</Directory>

*: Put your own domain

How to implement SSL certificates with grid user certificate support.

1. **Configure your server to apply the local CA host certificate**

Create a new certificate for your host and apply your local certification authority on this certificate.

   a. First add the real server name in httpd.conf to avoid some errors during the SSL verification.

   ```
   # vim /etc/httpd/conf/httpd.conf
   ServerName perfsonar-ps.cern.ch
   # service httpd restart
   ```

   b. **Generate certificate**

   ```
   # cd /root/
   #openssl req -new -out perfsonar.csr -nodes -sha1
   # ls -l
   ```

   c. **Then have this certificate approved by your certification authority.**

   Once you have your private key and your certificate, modify your ssl.conf file to apply the new certificate. Note that lines below have been changed to fit with CERN certificate. You may need to change only SSLCertificate lines - and “chain” is not mandatory.
# vim ssl.conf
AddType application/x-x509-ca-cert .crt .pem
AddType application/x-pkcs7-crl .crl
AddType application/pkix-cert .cer
SSLProtocol all -SSLv2
SSLCertificateFile /etc/pki/tls/certs/perfsonar-ca.cer
SSLCertificateKeyFile /etc/pki/tls/private/perfsonar-priv.pem
SSLCertificateChainFile /etc/pki/tls/certs/perfsonar-chain.cer
SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
# service httpd restart

Now, on the webpage, the site certificate should be CA trusted.

2. Configure server to authorize only Grid user certificates

# cd /tmp
# wget --no-check-certificate https://dist.eugridpma.info/distribution/igtf/current/igtf-policy-installation-bundle-1.43.tar.gz
# tar xzvf igtf-policy-installation-bundle-1.43.tar.gz
# cd igtf-policy-installation-bundle-1.43
# ./configure --with-profile=classic && make && make install
# ls -l /etc/grid-security/certificates/
You should find your local CA certificate in this folder (last command above) Then, uncomment and change these settings:

# vim /etc/httpd/conf.d/ssl.conf
SSLVerifyClient require
SSLCertCheck = 10
SSLCertificatePath /etc/grid-security/certificates/
# service httpd restart

If you refresh your webpage, the website should ask for your user certificate.

MYSQL server settings

Run $MYSQLPATH/mysql_secure_installation
It will remove test DB, anonymous user and ask you to setup a password for the root user.

PERFSONAR-PS tools settings.
Here is the most sensitive part of the subject, as it will touch the tool itself.
The first point is only an update to avoid XSS

**Avoid XSS**
As PHP has its htmlentities() function, a CGI script can use the “HTML::Entities” module to print GET/POST parameter values;

Here is an example of the change made to the $PERFPATH/toolkit/web/root/gui/perfAdmin/cgi script:

```perl
# grep HTML::Entities delayGraph.cgi
use HTML::Entities;
$title = "Source: " . HTML::Entities::encode($cgi->param('shost'));
$title .= " (" . HTML::Entities::encode($cgi->param('src')) . ") " if $shost;
$title .= " -- Destination: " . HTML::Entities::encode($cgi->param('dhost'));
$title .= " (" . HTML::Entities::encode($cgi->param('dst')) . ") " if $dhost;
```

```perl
# grep HTML::Entities serviceTest.cgi
use HTML::Entities;
my $html = errorPage("Unrecognized eventType: " . HTML::Entities::encode($eventType) . ".");
my $html = errorPage("Unrecognized eventType: " . HTML::Entities::encode($eventType) . ".");
```

**Restricting reverse ping and traceroute destination to client**

Another point to notice is the ability for anyone who accesses perfSONAR-PS reverse traceroute/ping tools to change the destination.
This field is visible only when you have done one time the traceroute/ping or by setting information in the URL (GET method).
By allowing users to change destination, you can potentially expose your internal routing paths.
Unless you trust all GRID users and you put in place the user certificate authentication, you may want to remove the possibility to set the end destination.

To do this, part of the code in the reverse_traceroute.cgi has been commented:

```perl
#"<small>To perform a
#   <!-- a href='http://boardwatch.internet.com/mag/96/dec/bwm38.html' -->
#   traceroute
#   from $ENV{SERVER_NAME},
```

Virginie Longo – CERN 9-Dec-11
At the same time you can remove size and probe options if you want:

```perl
if($name eq "function") {
  if($value eq "ping") {
    $function=$value;
  } elsif($value =~ /synack/) {
    if($hostname eq "www8.slac.stanford.edu") {
      $function=$value;
    } else {
      $err .= "Only SLAC supports synack function.<br>";
    }
  } elsif($name eq "debug") {
    $debug=$value;
  } elsif($name eq "size") {
    $ping_size=$value;
  } elsif($name eq "probe") {
    if($value=="ICMP") {
      $probe="-I"; #OK for Linux & Solaris
    }
  }
  if($ping_size eq ") {
    $ping_size=56;
  } elsif (!($ping_size =~ /^\d+/)) {
    $err .= "Size must be positive integer.<br>";
  } elsif (($ping_size < 56) || ($ping_size > 1400)) {
    $err .= "Size must be >= 56 & <= 1400.<br>";
  }
}

Disabling Jowping
Again this tool lets you configure ping size and count without any limit. This feature shouldn’t be allowed to the outside world. If user grid authentication cannot be set on your server, it may useful to disable this tool.