## Contents

1 Argus Release notes  
1.1 Argus 1.7.2 (01-08-2017) .................................................. 3  
1.2 Argus 1.7.1 (05-05-2017) .................................................. 4  
1.3 Argus 1.7.0 (09-02-2016) .................................................. 5  

2 Argus Authorization Service  
2.1 Summary ................................................................. 7  
2.2 Argus Service Installation ............................................. 7  
2.3 Service Components .................................................. 8  
2.4 Enabled Applications ............................................... 9  
2.5 Support and Monitoring .......................................... 9  
2.6 Development Information ..................................... 10  
2.7 Additional Support ............................................... 11  
2.8 About the name Argus ...................... .......................... 11  

3 Argus Concepts  
3.1 Argus Introduction ............................................... 13  
3.2 Attribute Based Descriptions .................................. 13  
3.3 Identifiers within Argus ......................................... 16  
3.4 Resource ID .......................................................... 16  
3.5 Conclusion ............................................................ 17  

4 Argus: Policy Administration Point (PAP)  
4.1 Summary ............................................................. 19  

5 Argus: Policy Decision Point (PDP)  
5.1 Summary ............................................................. 41  

6 Argus: Policy Enforcement Point Daemon (PEP)  
6.1 Summary ............................................................. 49  

7 Argus Monitoring  
7.1 Nagios Probes for Argus (UMD) ................................. 91  

8 Argus Quick Start Guide  
8.1 Argus Quick Start: Site Policy Setup ......................... 103  

9 Example of Authorization Requests and Policies  


9.1 User Based Authorization .............................................................. 107
9.2 Per-VO Pilot Job Authorization Policy ........................................... 108

10 Argus Service Reference Card ....................................................... 111
10.1 Definitions .................................................................................. 111
10.2 Service Reference Card ............................................................... 111

11 Argus Service Deployment for 1.7 version ......................................... 115
11.1 Requirements ............................................................................. 115
11.2 Installation with YUM ................................................................. 115
11.3 Update with YUM ..................................................................... 116
11.4 Configuration ............................................................................ 116

12 Nagios Probes for Argus ................................................................ 117

13 EMIR Publisher for Argus 1.6 (EMI-3) .............................................. 119

14 Known Issues ................................................................................. 121

15 Manual configuration ..................................................................... 123
15.1 Requirements ............................................................................. 123
15.2 PAP ......................................................................................... 123
15.3 PDP ......................................................................................... 124
15.4 PEP ......................................................................................... 124
15.5 Grid Mapping ........................................................................... 124
15.6 VOMS configuration ................................................................. 125
15.7 Restart services ........................................................................ 125
15.8 BDII configuration .................................................................... 125

16 Configuration with YAIM ................................................................. 127
16.1 Argus YAIM Configuration Variables .......................................... 127
16.2 Mandatory YAIM Variables ....................................................... 127
16.3 Argus site-info.def Configuration ............................................ 128
16.4 Generate Argus Configuration .................................................. 128

17 Authorization Service: Grid Map File Syntax .................................... 129
17.1 Description .............................................................................. 129
17.2 File Syntax .............................................................................. 129
17.3 Subject Keys .......................................................................... 129
17.4 Map Targets ........................................................................... 130

18 Argus YAIM Configuration for EMI ............................................... 131
18.1 YAIM Configuration for ARGUS_server .................................... 131

19 Known Issues for older version ....................................................... 133
19.1 Timeouts for certificates from CAs that use OCSP .......................... 133
19.2 Performance issue with Argus PEP Server (EMI-2, EMI-3, all versions) .. 133
19.3 Problem the EMI-3 update and Argus PEP Server v.1.6.1 .............. 134
19.4 Problem with Argus 1.6 (EMI-3) and fetch-crl .......................... 134
19.5 Problem with Nagios plugins for Argus and TMP directory permission ... 135
19.6 Problem with Argus 1.5 (EMI-2) and CREAM ............................ 135
19.7 Problem with upgrade from Argus 1.4 (EMI-1) to Argus 1.5 (EMI-2) .. 136

20 Legacy Pages from Twiki site .......................................................... 137
20.1 Argus EMIR Publisher Configuration (EMI-3) ............................. 137
20.2 Argus Services Fine Tuning ........................................................ 138
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.3 Argus Development Tools</td>
<td>140</td>
</tr>
<tr>
<td>20.4 GGUS User Support for Argus</td>
<td>141</td>
</tr>
<tr>
<td>20.5 Authorization Service: Load and Lifetime Testing</td>
<td>142</td>
</tr>
<tr>
<td>20.6 Authorization Services Testing Summary</td>
<td>145</td>
</tr>
<tr>
<td>20.7 Authorization Services Testing Summary</td>
<td>149</td>
</tr>
<tr>
<td>20.8 Authorization Services Testing Summary</td>
<td>153</td>
</tr>
<tr>
<td>20.9 Argus: Quick Start: Manual Installation</td>
<td>156</td>
</tr>
<tr>
<td>20.10 Argus: Quick Start: Manual Configuration</td>
<td>157</td>
</tr>
<tr>
<td>20.11 Quick Start: glite 3.2 Argus Installation</td>
<td>157</td>
</tr>
</tbody>
</table>

21 Indices and tables                                           161
Contents:
Argus Release notes

Latest release:

1.1 Argus 1.7.2 (01-08-2017)

The Argus 1.7.2 release provides a fix for an X.509 DN parsing problem in the PAP service.

1.1.1 Updated components

This release provides the following updated components:

- Argus PAP service version 1.7.2

1.1.2 Packages

Packages for this release can be obtained from the Argus product team package repository:

http://argus-authz.github.io/repo

Note that EL5/CENTOS5 packages are no longer provided (CENTOS5 is now out of support).

Upgrade procedure

To install Argus 1.7.2:

1. Update the packages.
2. Restart the Argus PAP service.
1.1.3 Main fixes

argus-pap-1.7.2

- PAP permissions don’t allow colon character in an X.509 subject principal [pap-16].

Older releases:

1.2 Argus 1.7.1 (05-05-2017)

The Argus 1.7.1 release introduces support for different X.509 CA Authentication profiles via the new Authentication Profile Policy Information Point (PIP).

With this support, it is possible to define which authentication profiles are enabled at the VO level, and for any trusted X.509 certificate. This first level of authorization is implemented at the PEP server, that uses a special policy file, called VO-CA-AP file, to determine which authentication profiles are enabled.

Further, finer grained authorization can then be implemented as usual with policies defined in the PAP using the newly introduced x509-authn-profile attribute, in order to have differentiated access within resources of the same VO.

In summary, the highlights of this release are:

- The new Authentication Profile PIP, which provides support for different CA authentication profiles in Argus;
- The new x509-authn-profile XACML attribute, that allows to write level-of-assurance aware policies, in case you need more flexibility than what is allowed by the VO-CA-AP file first level of authorization implemented in the PEP server;
- The new x509-subject-issuer XACML attribute, which was introduced to simplify the development of the Authentication Profile PIP.

1.2.1 Packages

Packages for this release can be obtained from the Argus product team package repository:

http://argus-authz.github.io/repo

Note that EL5/CENTOS5 packages are no longer provided (CENTOS5 is now out of support).

1.2.2 Service configuration

Instructions on how to configure the Authentication Profile PIP are provided in the following section:

- Authentication Profile PIP configuration

Upgrade procedure

To install Argus 1.7.1 and obtain a system with the same behavior of the former releases:

1. Update the packages.
2. Reconfigure the services, manually or with a configuration management system (such as Puppet, Ansible or Quattor).
3. Restart the services.
Argus 1.7.1 comes with a default configuration that grants the access to resources only to certificates issued by CAs in the *classic*, *scls* and *mics* IGTF profiles.

To enable IOTA CA support for selected VOs, you’ll need to:

1. Install the IOTA CA RPM, that provides the IOTA CA certificates and the policy info files;
2. Customize a VO-CA-AP policy file which states which authentication profiles are enabled for VOs and trusted certificates. This file can be provided by an RPM, such as `lcmaps-plugins-vo-ca-ap` package, or written manually by the system administrator, with the syntax described here.
3. Edit the Argus PEP server configuration file (`/etc/argus/pepd/pepd.ini`) to point the VO-CA-AP policy file, setting the `authenticationProfilePolicyFile` property with the `vo-ca-ap-file` absolute path.
   
   For example:
   ```
   authenticationProfilePolicyFile = /etc/grid-security/vo-ca-ap-file
   ```
4. Restart the services.

### 1.2.3 Main fixes

**PEP Server**

Milestone argus-pep-server-1.7.1:

- Introduce support for Authentication Profiles in Argus [pep-21].
- Introduce new `x.509-subject-issuer` and `x.509-authn-profile` attributes [pep-22].

**PAP**

Milestone argus-pap-1.7.1:

- Introduce new `x.509-subject-issuer` and `x.509-authn-profile` attributes [pap-14], [pap-15].

### 1.3 Argus 1.7.0 (09-02-2016)

The Argus 1.7.0 release provides fixes for some outstanding bugs and introduces support for Centos 7. The highlights of this release are:

- Centos7 support
- Argus services now require Java 8
- Upgraded core dependencies to latest versions:
  - Jetty upgraded to version 9.2.13.v20150730
  - VOMS upgraded to version 3.1
  - CANL upgraded to version 2.2.0
  - OpenSAML upgraded to version 2.6.4
- Introduced a load testing test suite based on Grinder
- Introduced an integration test suite based on Robot Framework
- Documentation has been migrated to ReadTheDocs
1.3.1 Packages

Packages for this release can be obtained from the Argus product team package repository:
http://argus-authz.github.io/repo

1.3.2 Service configuration

Instructions on how to configure and run the services are provided in the following documentation sections:

- Manual configuration
- YAIM configuration

Configuration for the services has not changed, so existing SL6 installation can upgrade and reconfigure services as usual (YAIM on SL6 is still supported).

YAIM configuration support is not provided on CENTOS 7; sites are free to use their favourite configuration management tool (Ansible, Puppet, Quattor) to manage the Argus services.

Changes in the mapping logic behaviour (pap-7, pap-11), and in particular in the handling of secondary group names, could produce different mappings for user jobs, so it’s safer to drain the site before upgrading the Argus services to version 1.7.0 if you want to avoid potential job failures due to the upgrade.

1.3.3 Main fixes

PDP-PEP-COMMON

- Update to CANL 2.2.0 to get more scalable certificate validation [pdp-pep-common-11].

PEP Server

- Improper synchronization may lead to corrupted mappings in the Gridmapdir [pep-3].
- Incorrect mapping for secondary group names [pep-7], [pep-11].
- Incorrect handling of CNs with internal slash characters [pep-9].

PAP

- Init script fails if shutdown command is changed in configuration [pap-7].
- BDII for Argus cannot check service status [pap-8].
- Prevent to creation of policy rules with empty subject [pap-6].
2.1 Summary

The Argus Authorization Service renders consistent authorization decisions for distributed services (e.g., user interfaces, portals, computing elements, storage elements). The service is based on the XACML standard, and uses authorization policies to determine if a user is allowed or denied to perform a certain action on a particular service.

The Argus Authorization Service is composed of three main components:

- The Policy Administration Point (PAP) provides the tools to author authorization policies, organize them in the local repository and configure policy distribution among remote PAPs.
- The Policy Decision Point (PDP) implements the authorization engine, and is responsible for the evaluation of the authorization requests against the XACML policies retrieved from the PAP.
- The Policy Enforcement Point Server (PEP Server) ensures the integrity and consistency of the authorization requests received from the PEP clients. Lightweight PEP client libraries are also provided to ease the integration and interoperability with other EMI services or components.

The following graphic shows the interaction between the components of the service:

**Note:** In Argus, the PEP is separated in a client/server architecture. The PEP Server handles the lightweight PEP client requests, and runs on the Argus node.

2.2 Argus Service Installation

The following section provides instructions for setting up an Argus environment quickly. It does not provide an exhaustive description of every possible deployment model or configuration option, that can be found in the following Service Components and Enabled Applications sections.

Before you continue it is recommend that you read this introduction to the Argus system. This will provide you with a better understanding of how the components work together, what information passes between the components and how policies are formed.
2.2.1 Argus Deployment

The Argus Service is installed with YUM. For the version 1.7, there isn’t an automatic configuration tool. Older version are configured with YAIM.

Please follow the Argus Deployment for version 1.7 documentation.

2.2.2 gLExec Worker Node with Argus Deployment

To install and configure an Argus compatible gLExec worker node, follow these GLExec Argus Quick Installation Guide

2.3 Service Components

If you are beginning to install the authorization service from scratch, you should install the components in the order listed here; PAP, then PDP, then PEPd. You don’t have to, but it makes the most sense for most use cases.

2.3.1 PAP: Policy Administration Point

The Policy Administration Point (PAP) provides three major functions:

- Provide the tools for authoring policies
- Store and manage authored policies
- Provide managed policies to other authorization service components

Fig. 1: Argus service components
2.3.2 PDP: Policy Decision Point

The Policy Decision Point (PDP) is a policy evaluation engine. The PDP receives authorization requests from Policy Enforcement Points and evaluates these requests against authorization policies retrieved from the PAP.

2.3.3 PEP: Policy Enforcement Point

The Policy Enforcement Point (PEP) is the client to the authorization service. It gathers information relevant to an authorization request (e.g. who the user, what action they are attempting to perform, which service they are attempting to perform the action on, etc.) and sends the request to the PDP for evaluation. The PEP then acts upon returned result by allowing the request to proceed (in the case a positive authorization decision) or by denying the action (in the event of a negative decision).

In Argus, the PEP itself has a client/server architecture
- The PEP Server handles the lightweight PEP client requests, and runs on the Argus node.
- Lightweight PEP client libraries are available to authorize requests from the application side, and to enforce decision locally. There are two variants available:
  - PEP Client C API: Programming Interface (API)
  - PEP Client Java API: Programming Interface (API)

PEP command-line clients are also available

2.4 Enabled Applications

The following applications contain an Argus PEP client and can make authorization requests to the Argus service.

Table 1: Argus-enabled Applications

<table>
<thead>
<tr>
<th>GSI PEP Callout</th>
<th>Introduction</th>
<th>Installation</th>
<th>Configuration</th>
<th>Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>gLExec with PEP Plugin</td>
<td>Introduction</td>
<td>Installation</td>
<td>Configuration</td>
<td>Troubleshooting</td>
</tr>
</tbody>
</table>

2.5 Support and Monitoring

2.5.1 GGUS Support

General support (installation, site administrator) for Argus is available through GGUS

2.5.2 Argus Support Mailing List

Argus specific (developer, site administrator) questions can be sent directly to the argus-support@googlegroups.com mailing list. You don’t need a Google email address or a Google account to send or receive emails from this mailing list.
2.5.3 Nagios Monitoring

Nagios plugins are available to monitor an Argus server.

- UMD: Argus Nagios Probes Documentation

2.6 Development Information

Argus is an open-source product hosted on GitHub. In addition to this user-oriented documentation, you can find a description of Argus architecture and main components at Argus main site.

2.6.1 Specifications

- XACML 2.0 Specifications eXtensible Access Control Markup Language (XACML) Version 2.0
- SAML 2.0 Profile of XACML, Version 2 (Working Draft 5)
- XACML Profile for the gLite WN XACML Grid Worker Node Authorization Profile (v. 1.0)
- XACML Profile for the gLite CE XACML Grid Computing Element Authorization Profile (v. 1.0)
- XACML Authorization Profile for EMI Common XACML Authorization Profile (v. 1.1)

2.6.2 Requirements

- Requirements Document (EDMS document 944192)
- Testing Plan (EDMS document 986067)

2.6.3 Presentations

- Argus – EMI Authorization Service (EGI UF 2011, 12 April 2011, Vilnus)
- General introduction to the authorization service
- Introduction to Argus for ROD (EGI ROD Workshop, 2 June 2010, Amsterdam)

2.6.4 Source Code Information

The Argus source code is on GitHub.

- Argus Authorization Service: https://github.com/argus-authz
2.6.5 Development Tools

The Argus PT uses the following development tools.
For performance and load testing we use the following testing suite.

2.6.6 Argus Production Settings and Optimization

Production sites can optimize the Argus Service settings to their specific needs. Please have a look at the Argus Service Fine Tuning documentation.

2.6.7 Performance and Load Testing

Argus provides a load testsuite, based on Grinder framework.
More information can be found on Argus load testsuite.

2.7 Additional Support

- HERAS-AF project has supported the project by providing a good XACML policy engine and excellent, ongoing, support of their code.
- YourKit is kindly supporting this open source projects with its full-featured Java Profiler. YourKit, LLC is the creator of innovative and intelligent tools for profiling Java and .NET applications. Take a look at YourKit’s leading software products: YourKit Java Profiler and YourKit .NET Profiler.
- This product includes software developed by the Caucho Technology.

2.8 About the name Argus

In Greek mythology Argus was a 100-eyed giant that was meant to watch and protect various things and people including the Goddess Io. He was slain by Hermes but the gods chose to preserve his hundred eyes and affix them to the tail-feathers of a brilliantly colored bird, the peacock, in homage. The peacock logo is provided by the royalty free clip art site clker.com.
3.1 Argus Introduction

The Argus authorization service is designed to answer questions in the form of *Can user X perform action Y on resource Z at this time?* Not surprisingly, two pieces of information are required to answer this question; the request that describes X, Y, and Z and the policy against which the request is evaluated. The purpose of this introduction is to provide an understanding of the logical contents of the request and the policy. Such an understanding will help in creating appropriate access control policies for a service. This introduction does not cover the command line tools, simple policy language, or underlying XACML policies used by the authorization service. That information can be found in the Policy Administration Point documentation.

3.2 Attribute Based Descriptions

Before discussing the request and response it is important to understand how users, actions, and resources are identified. Most grid deployers will be familiar with X.509 subject distinguished names (DNs) based access control. Access control systems which render authorization decisions based only on an identifier, like a subject DN, are known as identity-based access control systems. However, an application usually knows more about a user than simply their identifier. It may know for which organization the user works, or groups and professional organizations to which the user belongs. An access control system which can render a decision based on a set of attributes describing the users/resources/actions is known as an attribute-based access control system. Note, an attribute-based access control system where policies are only based on an identifier attribute is functionally equivalent to an identity-based access control system.

Argus is an attribute-based system. It uses attributes to identify the user attempting to perform an action, the resource on which the action is to be performed, the action itself, and other environmental information. Within the system an attribute is made of 4 pieces of information: a unique identifier/name, one or more values for the attribute, the data type of the attribute values (e.g. a string, an integer, an email address), and an optional identifier for the issuer of the attribute. The following are examples of attribute based descriptions.

In an identity based system a user (more properly known as a subject) might have the identity ‘jsmith’. In an attribute based system the subject might be identified by the following attributes:
<table>
<thead>
<tr>
<th>id</th>
<th>datatype</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>subject-id</td>
<td>string</td>
<td>jsmith</td>
</tr>
<tr>
<td>org</td>
<td>string</td>
<td>CERN</td>
</tr>
<tr>
<td>affiliation</td>
<td>string</td>
<td>emplyee</td>
</tr>
<tr>
<td>vo</td>
<td>string</td>
<td>lhcb, cms, atlas</td>
</tr>
</tbody>
</table>

In another example an action in an identity based access control system might be identified by the string ‘submit-job’. In an attribute based system the action might be identified with the following attributes:

<table>
<thead>
<tr>
<th>id</th>
<th>datatype</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>action-id</td>
<td>string</td>
<td>submit-job</td>
</tr>
<tr>
<td>pilot-job</td>
<td>boolean</td>
<td>false</td>
</tr>
<tr>
<td>executable</td>
<td>string</td>
<td>/usr/bin/myexec</td>
</tr>
<tr>
<td>expected-execution-duration</td>
<td>integer</td>
<td>10</td>
</tr>
</tbody>
</table>

The exact attributes available within a request are determined by the application seeking an authorization decision. Obviously each unique application will have different actions it wishes to protect, a different means of describing itself, and possibly different information about the subject. Also, as can be seen by these examples, the amount of information upon which a decision could be based is larger within an attribute based access control system than an identity based system. As demonstrated, the single piece of identity data used in an identity based system can also be used within an attribute based one.

### 3.2.1 The Request

An authorization decision request is simply a set of four different attributes collections. The four collections are:

- **subject** - contains attribute describing user who is trying to perform an action
- **action** - contains attributes describing the action the subject is attempting to perform
- **resource** - contains attributes describing the program within which the subject is attempting to perform the action
- **environment** - contains attributes relevant to the decision but not part of the previous three collection (e.g. time/date of the request, machine used by the subject, etc.).

A request must contain at least one attribute in each of the **subject**, **action**, and **resource** sets but it is common for there to be no environment attributes.

### 3.2.2 The Policy

A policy is a collection of rules that are evaluated to determine the result of an authorization request. The result of a policy evaluation may be:

- **permit** - indicates the subject is permitted to perform the action on the resource
- **deny** - indicates the subject is not permitted to perform the action on the resource
- **not applicable** - indicates no policy applied to the request and so no decision could be reached
- **indeterminate** - indicates there was an error evaluating the policy

In order to determine whether a rule is met each rule contains a **target**. The target defines one or more combination of attribute which trigger the rule. When more than one combination is listed any one may trigger the rule. For example, the target of a rule may stipulate the following combination:
• subject attribute vo has a value of atlas and the id of the action is job-submit and the id of the resource is cern-ce

• subject attribute id has a value of john and the id of the action is job-submit and the id of the resource is cern-ce

• subject attribute id has a value of jane and the id of the action is job-submit and the id of the resource is cern-ce

As you can see, each combination of attributes within the target needs to be complete (that is they need to describe the whole situation that would trigger a rule), there is no mechanism for expressing logical operations like AND, OR, NOT. As you can imagine this could lead to a lot of repeated information. To help alleviate this, policies, the container of rules, can also contain targets. Therefore the previous rule target could be written as follows:

• A policy with target: the id of the action is job-submit and the id of the resource is cern-ce

• A permit rule with the target combination:
  – subject attribute vo has a value of atlas
  – subject attribute id has a value of john
  – subject attribute id has a value of jane

You can also have multiple rules within a single policy, for example:

• A policy with target: the id of the action is job-submit and the id of the resource is cern-ce

• A permit rule with the target combinations:
  – subject attribute vo has a value of atlas
  – subject attribute id has a value of john
  – subject attribute id has a value of jane

• A deny rule with the target combinations:
  – subject attribute id has a value of christoph

In fact, policies can even contain other policies which helps in the case where you may want a policy about a resource which in turn contains a policy about actions (at that resource) and finally rules for that action. For example:

• A policy with target: id of the resource is cern-ce contains:
  – A policy with target: the id of the action is job-submit
    – A permit rule with the target combination:
      * subject attribute vo has a value of atlas
    – A deny rule with the target combination:
      * subject attribute id has a value of christoph
  – A policy with target: the id of the action is job-manage
    – A permit rule with the target combination:
      * subject attribute id has a value of john
      * subject attribute id has a value of jane
3.2.3 Not Applicable and Indeterminate Results

In some cases, either because no policy applied to the request or because there was an internal error evaluating a policy, a decision other than permit or deny is returned. In the event that a result of not applicable or indeterminate is returned Argus will treat this as a deny. Thus Argus is said to be a deny biased system.

3.2.4 Example Requests and Policies

Look at the dedicated page for request and policy examples.

3.3 Identifiers within Argus

Argus makes use of various identifiers for attribute identifiers and values. The identifiers must by URIs (URNs or URLs). The responsibility for defining such identifiers falls to different individuals, depending on the expected scope of use of the identifiers.

3.3.1 Entity ID

For those familiar with other grid services one of the first differences that you will encounter when setting up Argus is the requirement to provide entity IDs for the service components. These IDs provide a way of uniquely identify a logical service component. We use the term “logical service component” because each service component may be clustered. So the logical instance is the set containing all the physical instances participating in the cluster.

It is the deployer of service component that determines this identifier. The identifier may be any URI for which the deployer is authoritative. That is, it must come from a domain (in the case of a URL) or namespace (in the case of a URN) that the deployer controls. The following formula is a reasonable means for generating these identifiers:

\[
\text{http://}\{\text{authz\_domain}\}/\{\text{service\_component\_identifier}\}
\]

The domain should be a domain name that is not linked to any particular server's hostname but is instead related to the service (e.g. authz.example.org). The component identifier should be \text{pap}, \text{pdp}, or \text{pepd} depending on which component is being installed.

If an organization runs more than one component an additional qualifier may be added to appended to the path of the URL identifier. For example an organization that runs a different PEPd for each computer cluster they operate might choose the entity IDs \text{http://authz.example.org/pepd/cluster1} and \text{http://authz.example.org/pepd/cluster2}.

3.4 Resource ID

The resource identifier used to identify the resource being protected by the authorization service (e.g. a compute cluster, a portal). This identifier is specific to a given instance of the resource. If an organization runs two different portals each portal receives a different ID. These identifiers may then be used within a policy in order to indicate policies that apply to the specific resource (i.e. policy A applies to portal 1 and policy B applies to portal 2).

The resource identifier is selected by the deployer of the resource. Two reasonable ways for generating this identifier are:

- if the resource has a natural URI identifier associated with it (e.g. the main page of the portal) that may be used
- if the resource does not have a natural URI identifier a synthetic one may be created with the following formula:

\[
\text{http://}\{\text{authz\_domain}\}/\text{resource/}\{\text{resource\_identifier}\}
\]

The \text{authz\_domain} should be a domain name that is not linked to any particular server’s hostname but is instead related to the authorization...
service (e.g. authz.example.org). The resource identifier is simply a unique string for the protected resource. A human intelligible string is best (e.g. sequencingPortal).

### 3.4.1 Action ID

The action identifier is used to identify the action for which the resource is requesting authorization. This action identifier is specific to a given piece of software but all instances of that application use the same identifier for a given action, it is not deployment specific.

The action identifier is selected by the developer of the application. The identifier may be generated in one of two ways:

- If the application is widely used a request could be made to a standards body, such as IANA, for an unique identifier for each action of the application. This way all implementations of the specification will likely use the same identifier and thus make it a bit easier for policy writers.

- The application developer may generate an identifier. A reasonable formula for such an identifier is: http://{application_domain_name}/{application_name}/action/{action_id} where the domain name is the domain component of the application’s website and the action ID is a human readable string for the action (e.g. readFile, addUser)

### 3.4.2 Attribute ID

The attributes produced by an application identify bits of information that the application was able to gather and make available for an authorization request. The identifiers are specific to a given piece of software but all instances of that application use the same identifier for a given attribute, it is not deployment specific.

The attribute identifier is selected by the developer of the application. The identifier may be generated in a couple of ways:

- If the attribute is already defined by an existing standard (the LDAP schema standards are a great place to start looking) the identifier from that standard may be used. In the case of the LDAP schema the URN urn:oid:{ldap_attribute_oid} can be used.

- If the attribute is likely to be widely used a request could be made to a standards body, such as IANA, for an unique identifier for this attribute. This way all implementations of the specification will likely use the same identifier and thus make it a bit easier for policy writers.

- The application developer may generate an identifier. A reasonable formula for such an identifier is: http://{application_domain_name}/{application_name}/attribute/{attribute_id} where the domain name is the domain component of the application’s website and the attribute ID is a human readable string for the attribute (e.g. username, entitlements)

In general, application developers should prefer already defined attributes over creating their own.

### 3.5 Conclusion

At this point you should understand what an attribute is, that a request is a made of subject, action, resource, and environment attributes, what a rule is and that policies are a collection of rules. You should also understand that a policy or rule is triggered if any one of the combination of attribute/values listed within its target is present within the request.
CHAPTER 4

Argus: Policy Administration Point (PAP)

The Policy Administration Point (PAP) provides three major functions:

- Provide the tools for authoring policies
- Store and manage authored policies
- Provide managed policies to other authorization service components

4.1 Summary

4.1.1 Argus Policy Administration Point (PAP) Installation

To deploy the Argus PAP service, please follow the documentation Argus Deployment.

4.1.2 Argus Policy Administration Point (PAP): Configuration

Configuration Files

The PAP is configured through the use of two files: pap_configuration.ini and pap_authorization.ini, located in the /etc/argus/pap directory. Most of the information contained in these files can also be set through the command line interface (which is the recommended way to do configuration on the PAP).

There is also an environment file, located in /etc/sysconfig/argus-pap, that contains environment variables used by the init script that manage the service.

Service configuration file

The service is primarily configured through the pap_configuration.ini configuration file. This file is a standard INI file with five defined sections.
Section: [paps]

This section contains configuration about PAPs. The information in this section should be set via the PAP CLI.

A PAPs can be defined by providing the following information (the R value in the Required? column indicates information that is required only for remote PAPs):

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias.type</td>
<td>Defines a PAP as local or remote.</td>
<td>Y</td>
<td>None</td>
</tr>
<tr>
<td>alias.public</td>
<td>Visibility of the PAP: true or false. If false its policies are not sent to other PAPs.</td>
<td>N</td>
<td>false</td>
</tr>
<tr>
<td>alias.enabled</td>
<td>true or false. If false its policies are not sent to PDPs.</td>
<td>N</td>
<td>false</td>
</tr>
<tr>
<td>alias.dn</td>
<td>DN of the PAP to get policies from.</td>
<td>R</td>
<td>None</td>
</tr>
<tr>
<td>alias.hostname</td>
<td>Hostname of the PAP to get policies from.</td>
<td>R</td>
<td>None</td>
</tr>
<tr>
<td>alias.port</td>
<td>Port of the PAP to get policies from.</td>
<td>N</td>
<td>8150</td>
</tr>
<tr>
<td>alias.path</td>
<td>Path of the services exposed by the PAP to get policies from.</td>
<td>N</td>
<td>/pap/services</td>
</tr>
<tr>
<td>alias.protocol</td>
<td>Protocol to use to contact the remote PAP.</td>
<td>N</td>
<td>https</td>
</tr>
</tbody>
</table>

Section: [paps:properties]

This section contains information about policy distribution and PAP ordering.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>poll_interval</td>
<td>The polling interval (in seconds) for retrieving remote policies.</td>
<td>Y</td>
<td>None. Recommended value is 14400 (4 hours).</td>
</tr>
<tr>
<td>ordering</td>
<td>Comma separated list of PAP aliases. Example: alias-1, alias-2, ..., alias-n. Defines the order of evaluation of the policies of the PAPs, that means that the policies of PAP “alias-1” are evaluated for first, then the policies of PAP “alias-2” and so on.</td>
<td>N</td>
<td>If not specified the default pap is always the first one.</td>
</tr>
</tbody>
</table>

Section: [repository]

This section contains information about the PAP policy repository.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Path to the repository directory.</td>
<td>N</td>
<td>$PAP_HOME/repository</td>
</tr>
<tr>
<td>consistency_check</td>
<td>Forces a consistency check of the repository at startup.</td>
<td>N</td>
<td>false</td>
</tr>
<tr>
<td>consistency_check.repair</td>
<td>if set to true automatically fixes problems detected by the consistency check (usually means deleting the corrupted policies).</td>
<td>N</td>
<td>false</td>
</tr>
</tbody>
</table>
Section: [standalone-service]

This section contains information about the PAP standalone service.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-name</td>
<td>The hostname or IP address the service will bind to</td>
<td>N</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>port</td>
<td>The service port number</td>
<td>N</td>
<td>8150</td>
</tr>
<tr>
<td>shutdown</td>
<td>The service shutdown port number</td>
<td>N</td>
<td>8151</td>
</tr>
<tr>
<td>shutdown</td>
<td>The command string that must be received on the shutdown port in order to</td>
<td>N</td>
<td>shutdown</td>
</tr>
<tr>
<td></td>
<td>shutdown the service. The command is needed in order to prevent unauthorized</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>shutdown commands coming from localhost. This is effective only if the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>pap_configuration.ini file is not world-readable. If the option is not</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>present in configuration, no check on the command will be made.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>entity_id</td>
<td>This is a unique identifier for the PAP. It must be a URI (URL or URN). If</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a URL is used it need not resolve to any specific webpage.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Section: [security]

This sections contains information about PAP security configuration.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate</td>
<td>The X.509 pem-econded service certificate</td>
<td>Y</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td>private_key</td>
<td>The unencrypted private key bound to the certificate</td>
<td>Y</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td>trust_store_dir</td>
<td>The directory where CA files and CRL are looked for</td>
<td>N</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td>crl_update_interval</td>
<td>How frequently the PAP should update CRLs, CAs and namespaces from the filesystem. The interval is defined as a string with the following format: (N {s, m, h, d}) where N in the number of either (s=seconds, m=minutes, h=hours, d=days).</td>
<td>N</td>
<td>30m</td>
</tr>
</tbody>
</table>

Service Access Control

Access control rules are configured through the pap_authorization.ini configuration file. Authorization is based on off of the Subject DN or VOMS attribute within the client certificate used to authenticate to the PAP.
PAP permissions

The authorization layer is based on an Access Control List (ACL), composed of several Access Control Entries (ACEs). Each ACE defines the actions that an administrator is allowed to execute on the PAP. Administrators’ privileges are defined in terms of PAP permission flags, whose meaning is described in the table below:

<table>
<thead>
<tr>
<th>Permission Flag</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>POLICY_READ_LOCAL</td>
<td>Allows read access to locally defined policies</td>
</tr>
<tr>
<td>POLICY_READ_REMOTE</td>
<td>Allows read access to policies imported from remote PAPs</td>
</tr>
<tr>
<td>POLICY_WRITE</td>
<td>Allows write access to locally defined policies</td>
</tr>
<tr>
<td>CONFIGURATION_READ</td>
<td>Allows read access to PAP configuration</td>
</tr>
<tr>
<td>CONFIGURATION_WRITE</td>
<td>Allows write access to PAP configuration</td>
</tr>
<tr>
<td>ALL</td>
<td>All of the above permissions</td>
</tr>
</tbody>
</table>

A set of permission flags can be assigned to an administrator by defining an ACE in the `pap_authorization.ini` configuration file or by using the authorization management commands provided by the `pap-admin` command line interface.

ACEs are expressed as

```plaintext
<principal> : <permission>
```

couples.

The **principal** part of the ACE is either:

- ANYONE, to assign privileges to any authenticated user (i.e., any user that presents a trusted certificate).
- a VOMS FQAN, e.g., `/atlas/Role=VO-Admin`
- a quoted X509 certificate subject, e.g., "'/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Andrea Ceccanti"

The **permission** part of the ACE is either:

- a single PAP permission flag, e.g `CONFIGURATION_READ`
- a | separated list of PAP permission flags, e.g. `POLICY_READ_LOCAL|CONFIGURATION_READ`, to grant a set of permissions.

So, for example, to grant `POLICY_READ_LOCAL` and `POLICY_READ_REMOTE` permissions to a user identified by an X509 certificate with `/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Andrea Ceccanti` subject, one should write:

```
"'/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Andrea Ceccanti" : POLICY_READ_LOCAL|POLICY_READ_REMOTE
```

Note that the subject has been put into quotes! For VOMS FQANs this is not needed (FQAN syntax does not allow whitespaces inside the FQAN), so one could write:

```
/atlas/Role=PAP-Admin : ALL
```

Authorization entries are loaded at PAP service startup time so any `pap_authorization.ini` modifications done “by hand” while the PAP service is running do not take effect until the PAP service is restarted.

To modify the PAP authorization configuration at runtime, use the authorization management commands provided by the `pap-admin` CLI. Changes made to the PAP ACL by these commands are immediately reflected on the `pap_authorization.ini` file.
Configuration File Syntax

In the `pap_authorization.ini` file, ACEs are grouped in two stanzas according to the type of the principal. Currently, two stanzas are supported:

- `[dn]`, that lists ACEs defined for principals identified by an X509 certificate subject.
- `[fqan]`, that lists ACEs defined for principals identified by VOMS fqans.

An example of configuration file is given below:

```
[dn]
"/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Andrea Ceccanti" : ALL
ANYONE : CONFIGURATION_READ|CONFIGURATION_WRITE

[fqan]
/voms-ws/Role=PAP-Admin : ALL
```

Environment file

In the `/etc/sysconfig/argus-pap` file are defined Argus PAP environment variables, described in the table below.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Default value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP_HOME</td>
<td><code>/usr/share/argus/pap</code></td>
<td>Absolute path of PAP installation directory</td>
</tr>
<tr>
<td>PAP_RUN_FILE</td>
<td><code>/var/run/argus-pap.pid</code></td>
<td>Absolute path of PAP service PID</td>
</tr>
<tr>
<td>PAP_JAVA_OPTS</td>
<td>empty</td>
<td>Optional parameters to pass to the JVM when PAP service is started/stopped</td>
</tr>
</tbody>
</table>

4.1.3 Argus: Policy Administration Point (PAP): Operation

Service Operation Commands

Start the PAP service

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td><code>service argus-pap start</code></td>
</tr>
<tr>
<td>EL7</td>
<td><code>systemctl start argus-pap</code></td>
</tr>
</tbody>
</table>

Stop the PAP service

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td><code>service argus-pap stop</code></td>
</tr>
<tr>
<td>EL7</td>
<td><code>systemctl stop argus-pap</code></td>
</tr>
</tbody>
</table>
Service Ports

- Default service port: 8150
- Default shutdown service and status port: 8151

Service Endpoints

/pap/services/ProvisioningService: this endpoint provides the policy provisioning interface

/shutdown: this endpoint instructs the PAP standalone service to shutdown and is reachable only from localhost on the configured shutdown and status port

/status: this endpoint provides current status information on the PAP is reachable only from localhost on the configured shutdown and status port

All the web services implemented by the PAP can be reached at the /pap/services/ context.

Service Logs

The PAP standalone log file (pap-standalone.log) can be found in the $PAP_HOME/logs directory. If the PAP is deployed on top of tomcat, the log file (pap.log) can be found in the $CATALINA_HOME/logs directory.

4.1.4 Argus Policy Administration Point (PAP): Administration

The CLI (Command Line Interface) allows to perform all of the policy management operations as well as to set most of the configuration information of the PAP including authorization settings. All these operations are accessible by means of (sub)commands of the PAP CLI and they are divided in three sections: policy management, pap management and authorization management.

The command to invoke the CLI is pap-admin.

Running the pap-admin client

Type:

pap-admin --help
to get a list of the commands supported by the current version of the PAP command line client.

The general usage is the following:

usage: pap-admin [global-options] <command> [options] [args]

- global-options: are options shared by all commands (all these options are reported by --help).
- command: the command to perform.
- options: command specific options.

Type:

pap-admin <command> --help
to see the available command specific options.

Global options:
• `-h,--help`: help message;
• `-v,--verbose`: set verbose commands output;
• `--host <arg>`: specifies the target PAP hostname (default is localhost). This option defines the PAP endpoint to be contacted as follows: `https://arg:port/pap/services/`;
• `--port <arg>`: specifies the port on which the target PAP is listening (default is 8150);
• `--url <arg>`: specifies the full target PAP endpoint (default: `https://localhost:8150/pap/services/`);
• `--cert <arg>`: specifies non-standard user certificate;
• `--key <arg>`: specifies non-standard user private key;
• `--password <arg>`: specifies the password used to decrypt the user’s private key;
• `--proxy <arg>`: specifies a user proxy to be used for authentication;

By default, the `pap-admin` is configured to contact a PAP daemon on localhost port 8150 (i.e., the standalone PAP daemon). If you want to contact a PAP on another host use the `--host` option, a PAP listening on a different port use the `--port` option. Alternatively the full endpoint can be specified with the `--url` option.

**NOTE:** The Argus PDP caches the policy pulled from the PAP. If you make policy changes to the PAP you will need to restart the PDP in order to force it to refresh its policy. Also, the PEPd caches results from the PDP for a short time (up to 10 minutes, by default) so you may need to restart the PEPd as well.

**Exit status**

Each command returns 0 for success or non-zero in case of error.

**X509 authentication**

A valid X509 certificate or proxy certificate is needed in order to run the `pap-admin` client. The certificate to be used by the command is found as follows:

1. if the user is `root` then the client looks for host certificate at the usual location, i.e. `/etc/grid-security/hostcert.pem` and `/etc/grid-security/hostkey.pem`. These locations can be overridden by setting the `X509_USER_CERT` and `X509_USER_KEY` environment variables.
2. if the user is not `root`, then the client looks for a proxy certificate at the usual location, i.e., `/tmp/x509up_u<uid>`. The default proxy location can be overridden using the `X509_USER_PROXY` environment variable. If no proxy is found, then the client looks for a certificate (and the relative private key) at the usual location, i.e., `$HOME/.globus/usercert.pem` and `$HOME/.globus/userkey.pem`. These locations can be overridden by setting the `X509_USER_CERT` and `X509_USER_KEY` environment variables.

This behaviour can be overridden by specifying the `--cert`, `--key` and `--proxy` command line options.

**Client configuration (since version 1.3.0)**

The `pap-admin.properties` file, found in `/etc/argus/pap` (EMI) or `/opt/argus/pap/conf` (gLite), allows to set the following properties:
This property file is especially useful when administering a PAP installed on a remote machine.

**Policy Management Commands**

This set of commands allows to perform policy management operations. All the commands in this section modifies the *default* PAP. In order to target another local PAP use the option `--pap <alias>`.

**Command: list-policies**

List policies. By default the policies of the *default* PAP are listed unless option `--pap` is specified.

```markdown
usage: pap-admin [global-options] list-policies [options]
```

Command specific options:
- `--pap <alias>`: list policies of PAP “alias” (*default* PAP is assumed if this option is missing);
- `--all`: list policies of all the defined PAPs;
- `--srai,--show-ra-ids`: show resource and action ids;
- `--sai,--show-all-ids`: show all ids (resource, action and rule ids);
- `--show-xacml`: print policies using XACML.

**Command: ban**

Allows to ban an attribute (i.e. SUBJECT, FQAN, CA, etc.).

A *deny* rule is added for the given attribute into the specified resource/action value. If the resource or the action values are not specified then “.*” is assumed.

```markdown
usage: pap-admin [global-options] ban [options] <id> <value>
```

- `id`: id of the attribute. The list of supported id depends on the Argus version:
  - Argus v. 1.0: dn, ca, vo, fqan, pfqan.
  - Argus v. 1.1: subject, subject-issuer, vo, fqan, pfqan.
- `value`: value of the attribute - **note:** If you are using Argus v. 1.0, the DN must be in RFC2253 format, which can be obtained from openssl using the command `openssl x509 -in <cert.pem> -noout -subject -nameopt rfc2253`.

Command specific options:
- `-a,--action <value>`: specify an action value (default is “.*”)
- `-r,--resource <value>`: specify a resource value (default is “.*”)
- `--pap <alias>`: add the policy to the PAP “alias” (*default* PAP is assumed if this option is missing)
• --private: set the policy as private
• --public: set the policy as public

Semantic of the command: the resource and the action where the deny rule is inserted are chosen as follows:
• if the first resource found in the repository matches the given one, then that resource is used, otherwise a new one is created.
• if a matching resource was found, then if its first action matches the given one then this action is used, otherwise a new action is created (i.e. inside the new resource or inside the matched resource).
• otherwise a new resource/action are created and inserted on the top.

Example:
```
pap-admin ban subject "CN=host.test.foo.it, L=FOO, OU=Host, O=ORGANIZATION, C=IT"
```

Command: un-ban

Allows to un-ban an attribute (i.e. SUBJECT, FQAN, CA, etc.), that means removing a deny rule (if it exists in the given resource/action) for the given attribute.

```
usage: pap-admin [global-options] un-ban [options] <id> <value>
```

• id: id of the attribute. The list of supported id depends on the Argus version:
  – Argus v. 1.0: dn, ca, vo, fqan, pfqan.
  – Argus v. 1.1: subject, subject-issuer, vo, fqan, pfqan.
• value: value of the attribute - note: If you are using Argus v. 1.0, the DN must be in RFC2253 format, which can be obtained from openssl using the command openssl x509 -in <cert.pem> -noout -subject -nameopt rfc2253

Command specific options:
• -a,--action <value>: specify an action value (default is ".*")
• -r,--resource <value>: specify a resource value (default is ".*")
• --pap <alias>: remove the ban policy from the PAP alias (default PAP is assumed if this option is missing)

Semantic of the command: the target resource and action to search the deny rule for are chosen as follows:
• the target resource is the first matching resource in the repository;
• inside the target resource the target action is the first matching action;
• if no target resource or action were found than the result is an error message saying “ban policy not found”.

Example:
```
pap-admin un-ban subject "CN=host.test.foo.it, L=FOO, OU=Host, O=ORGANIZATION, C=IT"
```

Command: add-policy

Add a permit/deny policy.

```
usage: pap-admin [global-options] add-policy [options] <permit|deny> <id=value>...
```

4.1. Summary
• permit|deny: effect of the policy.
• id=value: a string in the form “<id>=<value>”, where id is any of the attribute ids that can be specified in the simplified policy language and value the value to be assigned (e.g. fqan=/vo/group).

Required command options: 1 --action-id <action-id> optionally with --rule-id <rule-id>: allows to specify an action-id to insert the policy into. 1 --resource <value> and --action <value>: allows to specify a resource/action value to insert the policy into.

The two groups (1 and 2) of required options are mutually exclusive.

This command allows to add a (permit/deny) rule into an action by specifying an action-id (in this case the action must already exist) or a resource/action value. In the latter case a new resource and/or action are created if they don’t already exist. The command returns an error if there are more than one existing resource and/or action with the same value. By default the rule is inserted at the top of an action unless the --bottom option is given. If the --rule-id is set the rule is inserted before the given rule-id or after if the --after option is present.

Command specific options:
• --pap <alias>: add the policy to the PAP “alias” (default PAP is assumed if this option is missing);
• --action-id <action-id>: specify an action id;
• --rule-id <rule-id>: specify a rule id (requires option --action-id);
• --resource <value>: specify a resource value;
• --action <value>: specify an action value;
• --after: insert the rule after the given rule id;
• --bottom: insert the rule at the bottom of the list of rules of the action.
• --obligation <obligationId>: specify an obligation. (since version 1.2.0)
• --obligation-scope <scope>: Defines in which scope the obligation will be defined. Possible values: action, resource. If not specified, resource is used as default. (since version 1.2.0)

**Command: add-policies-from-file**

Add policies (resources or actions) defined in the given file.


• file: text file containing the policies to add (policies defined with the simplified policy language)
• ResourceId: the resource to insert the policies into.

If resourceId is not specified then file must contain resource elements that will be added, by default, at the bottom (unless option --pivot is specified). Otherwise if resourceId is not specified then file must contain action elements that will be added, by default, at the bottom inside resourceId (unless option --pivot is specified).

Command specific options:
• --pap <alias>: add the policies to the PAP “alias” (default PAP is assumed if this option is missing);
• --pivot <id>: insert before <id>;
• --after: modifies the behavior of the --pivot option in insert after <id>.
**Command: update-policy-from-file**

Update a resource/action with a new resource/action defined in a given file.

```
```

- **id**: id, as listed by the command `pap-admin lp --show-all-ids` command, of the resource or action to be updated;
- **file**: text file containing the new policy definition (using the simplified policy language syntax).

In order to modify an action the `file` must contain only the new action, for example:

```
action ".*" {
  rule deny { subject="/DC=ch/DC=cern/OU=Organic Units/OU=Users/CN=user/CN=111111/CN=user name" }
}
```

Command specific options:
- `--pap <alias>`: update the policies for PAP “alias” (default PAP is assumed if this option is missing);

**Command: remove-policy**

Remove policy by id.

```
usage: pap-admin [global-options] remove-policy [options] id...
```

- **id**: id, as listed by the command `pap-admin lp --show-all-ids` command, of the policy (resource, action or rule) to remove;

Command specific options:
- `--pap <alias>`: remove policies of PAP “alias” (default PAP is assumed if this option is missing);

**Command: remove-all-policies**

Remove all policies of a PAP. Use option `--pap` to specify a PAP different than the default one.

```
usage: pap-admin [global-options] remove-all-policies [options]
```

Command specific options:
- `--pap <alias>`: remove the policies of PAP “alias” (default PAP is assumed if this option is missing);

**Command: move**

Move a resource, action or rule before or after another, respectively, resource, action or rule.

```
usage: pap-admin [global-options] move [options] <id> <pivotId>
```

- **id**: id, as listed by the command `pap-admin lp --show-all-ids` command, of the policy (resource, action or rule) to move;
- **pivotId**: id of the pivot policy (id is moved before pivotId)
If \textit{id} refers to a resource, action or rule then \textit{pivotId} must be, respectively, a resource, action or rule id.

Command specific options:
\begin{itemize}
  \item --\textit{pap} <alias>: move the policy of PAP “alias” \textit{(default} PAP is assumed if this option is missing);  
  \item --\textit{after}: move id after pivotId.  
\end{itemize}

**Command: add-obligation (since version 1.2.0)**

Adds on obligation to an existing resource or action policy.

\textbf{usage:} \texttt{pap-admin [global-options] add-obligation <policyId> <obligationId>}

\begin{itemize}
  \item \textit{policyId}: the id of the policy where the obligation is to be added. In order the get the policyId of existing policies, run the list-policies command with the \texttt{--show-all-ids} option.
  \item \textit{obligationId}: the id of the obligation that will be added.
\end{itemize}

Command specific options:
\begin{itemize}
  \item --\textit{pap} <alias>: add on policies defined in the PAP “alias” \textit{(default} PAP is assumed if this option is missing);  
\end{itemize}

**Command: remove-obligation (since version 1.2.0)**

Removes an obligation from an existing resource or action policy.

\textbf{usage:} \texttt{pap-admin [global-options] remove-obligation <policyId> <obligationId>}

\begin{itemize}
  \item \textit{policyId}: the id of the policy where the obligation is to be removed. In order the get the policyId of existing policies, run the list-policies command with the \texttt{--show-all-ids} option.
  \item \textit{obligationId}: the id of the obligation that will be removed.
\end{itemize}

Command specific options:
\begin{itemize}
  \item --\textit{pap} <alias>: add on policies defined in the PAP “alias” \textit{(default} PAP is assumed if this option is missing);  
\end{itemize}

**PAP Management Commands**

This set of commands allows to perform management operations of the PAPs.

**Command: ping**

Ping a PAP and return version information.

\textbf{usage:} \texttt{pap-admin [global-options] ping}
Command: add-pap

Add a remote or local PAP.


- alias: a friendly (unique) name used to identify the PAP
- endpoint: endpoint of the remote PAP in the form: [<protocol>://]<host>:[<port>/<path>]
- dns: DN of the remote PAP

A just added PAP is disabled by default (its policies are not sent to the PDP), use the command `enable-pap` to enable it.

By default a PAP is considered to be private (use the `--public` option to set the PAP as public). Policies defined in a public PAP can be fetched from other remote PAPs, while this is not allowed when the PAP is set to private.

If `endpoint` and `dn` are present the PAP is considered to be remote (unless option `--local` is specified), otherwise it is local. For the endpoint the only required parameter is the hostname, these are the default values:

- protocol: https
- port: 8150
- service path: pap/services

When a new PAP is added, the PAP service tries immediately to fetch its policies. If the remote PAP is not reachable, the `pap-admin` command prints an error message clarifying that the PAP was successfully added, but the fetching of the policies failed.

If the option `--no-policies` is given, the policies are not fetched at PAP creation time but automatically by the server every polling interval seconds or manually when the a `refresh-cache` command is sent to the server.

Examples of endpoint are:

- test.site.com (hostname);
- test.site.com:9999 (hostname and port);
- test.site.com:9999/service_path (hostname, port, and service path);
- https://test.site.com:9999/service_path (full URL).

Command specific options:

- `-l, --local`: set the PAP as local;
- `--remote`: set the PAP as remote;
- `--private`: set the PAP as private;
- `--public`: set the PAP as public;
- `--no-policies`: do not fetch the policies now.

Example:

```
pap-admin add-pap cnaf_pap test.cnaf.infn.it "/C=IT/O=INFN/OU=Host/L=CNAF/CN=test.cnaf.infn.it"
```
Command: update-pap

Update PAP information.

```
```

The input is the same as for the “add-pap” command, the effect is to update old information with the new one. The alias of a PAP cannot be modified. In the case of a remote PAP the policies are fetched immediately unless option --no-policies is given.

Command: remove-pap

Remove a PAP and delete its policies.

```
usage: pap-admin [global-options] remove-pap <alias>
```

- **alias**: alias of the PAP to remove

Command: list-paps

List all defined PAPs.

```
usage: pap-admin [global-options] list-paps [options]
```

Command specific options:

- **-l**: use a long list format (displays all the information of a PAP).

Command: enable-pap

Set a PAP as enabled (i.e. PDPs will get its policies).

```
usage: pap-admin [global-options] enable-pap <alias>
```

Command: disable-pap

Set a PAP as disabled (i.e. PDPs won’t get its policies).

```
usage: pap-admin [global-options] disable-pap <alias>
```

Command: get-paps-order

Get PAPs ordering.

```
usage: pap-admin [global-options] get-paps-order
```

If no ordering is defined the output message is: No ordering has been defined. If the default PAP is not listed in the ordering (like in the no ordering defined case) by default it is placed for first.
Command: set-paps-order

Define PAPs ordering.

usage: pap-admin [global-options] set-paps-order [alias]...

- alias: a valid PAP alias.

All the aliases must be valid (existing). If no arguments are given then the current ordering (if there’s any defined) is deleted.

Example:

The remote PAP osct contains banning policies and we want that policies to be evaluated for first. This is command to issue:

```
pap-admin set-paps-order osct default
```

If the PAP service contains other PAPs beyond the osct, then their policies are evaluated after the osct and default PAP policies. Since the ordering contains only the osct and the default PAPs it is not guaranteed a special order for the evaluation of the policies of all the other PAPs (except that they are evaluated after these two PAPs).

Command: refresh-cache

Invalidates the local policy cache and retrieves policies from remote PAPs.

usage: pap-admin [global-options] refresh-cache [alias]...

- alias: a valid PAP alias.

The arguments identify the PAPs that will be contacted. If no arguments are given, all the defined remote PAPs are contacted.

Command: get-polling-interval

Get the polling interval in seconds.

usage: pap-admin [global-options] get-polling-interval

Command: set-polling-interval

Invalidates the local policy cache and retrieves policies from remote PAPs.

usage: pap-admin [global-options] set-polling-interval <seconds>

- seconds: polling interval in seconds.

Authorization Management Commands

This set of commands implement Access Control List (ACL) management for PAP administrators.
Command: list-acl

The `list-acl` command provides an easy way of knowing the authorization configuration of a running PAP. Typing:

```
pap-admin list-acl
```

prints out the Access Control Entries (ACEs) comprising the ACL currently defined for the running PAP. Example:

```
~# pap-admin list-acl
/voms-ws/Role=PAP-Admin : POLICY_READ_LOCAL|POLICY_READ_REMOTE|POLICY_WRITE|CONFIGURATION_READ|CONFIGURATION_WRITE
"/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Andrea Ceccanti" : POLICY_READ_LOCAL|POLICY_READ_REMOTE|POLICY_WRITE|CONFIGURATION_READ|CONFIGURATION_WRITE
ANYONE : CONFIGURATION_READ|CONFIGURATION_WRITE
```

Required permissions: `CONFIGURATION_READ`.

Command: add-ace

The `add-ace` command allows to add (or change) an ACE to the PAP ACL. Note that if an ACE entry already exists on the server for the principal specified in the command, the permissions in such ACE are replaced by the ones specified in the command. Usage:

```
pap-admin add-ace <principal> <permissions>
```

where:

- `principal` can be either an X509 DN or a VOMS FQAN. `ANYONE` can be used to assign permissions to any authenticated user.

- `permissions` is a `|` separated list of PAP permissions that will be assigned to principal. The `ALL` shortcut can be used to assign all permission.

Example:

```
pap-admin add-ace '/atlas/Role=VO-Admin' 'ALL'
```

Required permissions: `CONFIGURATION_READ` | `CONFIGURATION_WRITE`

Command: remove-ace

The `remove-ace` command removes an ACE from the PAP ACL. Usage:
pap-admin remove-ace <principal>

where:

- principal can be either an X509 DN or a VOMS FQAN. ANYONE can be used to remove permissions assigned to any authenticated user.

Example:

```
pap-admin remove-ace '/atlas/Role=VO-Admin'
```

Required permissions: CONFIGURATION_READ|CONFIGURATION_WRITE

### 4.1.5 The Simplified Policy Language

As already explained *here*, Argus policies contain collections of rules that state which actions can be performed on which resources by which users. XACML, the language used internally by Argus to define policies, provides great expressiveness and flexibility but it’s very hard to read and author for human beings. For this reason, Argus provides a Simplified Policy Language (SPL) to hide the complexity of XACML while providing much of its flexibility.

As an example, the following policy denies access to all the resources (under Argus control) to the members of the ATLAS VO:

```plaintext
resource ".*" {
    action ".*" {
        rule deny { vo = "atlas" }
    }
}
```

**The SPL syntax**

```plaintext
resource <value> {
    action <value> {
        rule <permit|deny> {
            <attributeId>=<attributeValue>
            ...
        }
        ...
    }
}
```

The SPL defines three stanza types: resource, action and rule. It’s possible to define multiple resource stanzas that can contain multiple action stanzas that can contain multiple rules stanzas.

The resource stanza is used to target a resource (or set of resources, if wildcards are used) under the control of Argus authorization.

The action stanza (always defined in the context of an enclosing resource) is used to target an action (or set of actions, if wildcards are used) that has to be authorized by Argus on the resource identified by the enclosing resource stanza.
The rule stanza defines who is authorized (in case of a permit rule) or not authorized (in case of a deny rule) to perform the action on the resource identified by the enclosing action and resource stanzas.

Identifying actions and resources

Actions and resources are identified by unique identifiers that are assigned to them. This identifiers are usually URIs, but any string that is unique in your deployment may work.

You can also use wildcards in your SPL policies to target group of resources or actions, like in the following example:

```
resource "http://cnaf.infn.it/cream-ce-01" {
    action ".*" {
        rule permit { vo = "cms" }
    }
}
```

This policy authorizes users from the CMS vo to perform any action on the resource http://cnaf.infn.it/cream-ce-01.

Identifying subjects

In Argus policies, the users (or software agents) that need to be authorized to execute an action on a specific resource are identified using a set of attributes, like:

- the subject of the user’s X509 certificate;
- the CA that issued the user’s x509 certificate;
- the VO the user belongs to;
- whether the use has a specific FQAN in its bag of VOMS attributes;
- whether the user has a specific FQAN as his primary FQAN.

The table below specifies the supported attributes for Argus 1.1:

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>subject</td>
<td>The user’s X509 certificate subject in rfc2253 or openssl format</td>
<td>subject = &quot;CN=Andrea Ceccanti, L=CNAF,OU=Personal Certificate, O=INFN,C=IT&quot;</td>
</tr>
<tr>
<td>subject-issuer</td>
<td>The subject (in rfc2254 or openssl format) of the CA that issued the user’s x509 certificate</td>
<td>subject-issuer = &quot;CN=INFN CA, O=INFN,C=IT&quot;</td>
</tr>
<tr>
<td>vo</td>
<td>The name of the VO the user belongs to</td>
<td>vo = &quot;atlas&quot;</td>
</tr>
<tr>
<td>fqan</td>
<td>The fqan present in the user’s bag of VOMS attributes</td>
<td>fqan=&quot;/dteam/Role=VO-Admin&quot;</td>
</tr>
<tr>
<td>pfqan</td>
<td>The user primary fqan</td>
<td>pfqan=&quot;/atlas/Role=pilot&quot;</td>
</tr>
</tbody>
</table>

The contents of the rule stanza

As already pointed out, the rule stanza defines who is authorized to perform a specific action on a specific resource. A subject can be identified using the attributes defined in the previous section.
resource "http://cnaf.infn.it/cream-ce-01" {
    action "submit-pilot-job" {
        rule permit { pfqan="/atlas/Role=pilot" }
    }
}

In the above policy, only subjects that have the /atlas/Role=pilot fqan as their primary fqan are authorized (since the rule is permit rule) to perform the action submit-pilot-job on the resource http://cnaf.infn.it/cream-ce-01. To prevent users from LHCB VO the execution of the same action, one would write the following policy:

resource "http://cnaf.infn.it/cream-ce-01" {
    action "submit-pilot-job" {
        rule deny { vo = "lhcb" }
    }
}

**Multiple attributes inside the rule stanza**

It is possible to define multiple attributes inside a rule stanza. All the attributes defined in the rule stanza need to match with the subject attributes present in the authorization request for the rule to be applied. This can be explained more clearly using an example:

resource "http://cnaf.infn.it/cream-ce-01" {
    action "submit-job" {
        rule permit {
            vo = "cms"
            subject-issuer = "CN=INFN CA,O=INFN,C=IT"
        }
    }
}

The meaning of the above policy is that only members from the VO CMS that have a certificate signed by the CN=INFN CA,O=INFN,C=IT CA will be authorized to perform the action submit-job on resource http://cnaf.infn.it/cream-ce-01. CMS members with certificates signed by the CERN CA, for instance, will not be authorized.

Since all the attributes defined in a rule must be “matched” in the request for the rule to be applied, one can think about multiple attributes inside a rule stanza as conditions that are ANDed to select who will be authorized to perform the action the rule is about.

**How policies are evaluated**

The first applicable policy (and only that one) that matches the authorization request is the one that is applied by Argus. This means that **order matters**. An example will help in understanding this concept.

4.1. Summary
Suppose we want to grant access to our CE to all members of VO CMS but not those that have `/cms/Role=pilot` as their primary FQAN. We would write a policy like this:

```plaintext
resource "http://cnaf.infn.it/cream-ce-01" {
    action ".*" {
        rule deny{ pfqan = "/cms/Role=pilot"}
        rule permit { vo = "cms" }
    }
}
```

Since the deny rule precedes the permit rule in the above policy, we are able to deny access only to CMS users with the pilot role, but grant access to other members of CMS. This is due to the fact that the first deny rule will not match to CMS users that do not have the pilot role, so the following permit rule will be applied. On the contrary, if we reversed the order of the two rules like in the following policy:

```plaintext
resource "http://cnaf.infn.it/cream-ce-01" {
    action ".*" {
        rule permit { vo = "cms" }
        rule deny{ pfqan = "/cms/Role=pilot" }
    }
}
```

the deny rule would be useless, since the permit rule that precedes it would always match any CMS member.

### The obligation stanza

Starting with Argus version 1.1, the SPL supports obligation stanzas. The syntax of the obligation stanza is as follows:

```plaintext
obligation "obligationId" {
    [attributeId = attributeValue]*
}
```

Obligation stanzas can be placed either in the resource or action context and are used to define a set operations that must be performed by the Argus PEP in conjunction with an authorization decision. An obligation stanza can define 0..N attribute definitions, that are passed as parameters to the PEP for the fulfillment of the obligation.

An example of policy with an obligation is the following:

```plaintext
resource "http://cnaf.infn.it/wn"{
    obligation "http://glite.org/xacml/obligation/local-environment-map" {} 
    action "http://glite.org/xacml/action/execute"{
        rule permit { vo = "dteam" }
    }
}
```

The Argus PEP currently supports only the map-to-local-environment obligation.
The map-to-local-environment obligation

The map-to-local-environment obligation, identified by the following id:

http://glite.org/xacml/obligation/local-environment-map

is used within a policy to signify that a mapping to a local Posix account will be produced by the Argus server as a result of a permit policy.

The use of this obligation is mandatory for the policies that authorize the execution and mapping of pilot jobs on the worker node.

Examples

Ban policies

Ban policies are used to deny a subject on all possible resources. For this reason ban policies need to be placed at the top and defined for any action on all the resources.

```
resource ".*" {
    action ".*" {
        rule deny { subject = "CN=Alberto Forti,L=CNAF,OU=Personal Certificate,O=INFN,C=IT" }
        rule deny { fqan = /dteam/test }
    }
}
```

Glexec on the WN policies

Policy that authorize execution and mapping of pilot jobs on the WN need to specify the map-to-local-environment obligation to produce a mapping that gLexec can use to do the user switch. An example of such policy is the following:

```
resource "http://cnaf.infn.it/wn"{
    obligation "http://glite.org/xacml/obligation/local-environment-map" {} 
    action "http://glite.org/xacml/action/execute"{
        rule permit { vo = "dteam" }
        rule permit { pfqan =="/atlas/Role=pilot" }
        rule permit { pfqan =="/ops/Role=pilot" }
    }
}
```

The above policy authorizes the execution of jobs on the WN by:

- people from the dteam VO,
- people that have /atlas/Role=pilot as the primary fqan
- people that have /ops/Role=pilot as the primary fqan

4.1.6 Argus: Policy Administration Point (PAP): Known Issues

There is no known issues.
Argus: Policy Decision Point (PDP)

The Policy Decision Point (PDP) is a policy evaluation engine. The PDP receives authorization requests from Policy Enforcement Points and evaluates these requests against authorization policies retrieved from the PAP.

5.1 Summary

5.1.1 Argus Policy Decision Point (PDP) Installation

To deploy the Argus PDP service, please follow the documentation *Argus Deployment*.

5.1.2 Argus Policy Decision Point (PDP): Configuration

**Configuration Files**

The PDP is configured through the use of the `pdp.ini` file, located in `/etc/argus/pdp` directory.

There is also an `environment file`, located in `/etc/sysconfig/argus-pdp`, that contains environment variables used by the init script that manage the service.

**Configuration File Syntax**

The `pdp.ini` file is a standard INI file with three defined sections. The `SERVICE` section contains properties related the PDP service as a whole and how it listens for incoming requests. The `POLICY` section contains properties for the retrieval of policies from the Policy Administration Point (PAP). The final section, `SECURITY`, contains properties that related to various security aspects of the service, the services private key and certificate, for example.
## Basic Configuration Options

### SERVICE section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>entityID</td>
<td>This is a unique identifier for the PDP. It must be a URI (URL or URN) and</td>
<td>Y</td>
<td>None. Recommended value is a URL corresponding to the logical PDP service</td>
</tr>
<tr>
<td></td>
<td>the same entity ID should be used for all PDP instances that make up a</td>
<td></td>
<td>(e.g. <a href="http://pdp.example.org">http://pdp.example.org</a>).</td>
</tr>
<tr>
<td></td>
<td>single logical PDP. If a URL is used it need not resolve to any specific</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>webpage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>This is the hostname or IP address to which the service will bind.</td>
<td>Y</td>
<td>None.</td>
</tr>
<tr>
<td>port</td>
<td>This is the port to which the service will bind.</td>
<td>N</td>
<td>8152</td>
</tr>
<tr>
<td>admin-Host</td>
<td>The hostname upon which the service will listen for admin commands.</td>
<td>N</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>admin-Port</td>
<td>This is the port upon which the service will listen for admin command.</td>
<td>N</td>
<td>8153</td>
</tr>
<tr>
<td>admin-Password</td>
<td>This is the password required to accompany admin</td>
<td>N</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>commands. If unspecified than no password is required to run admin commands.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### POLICY section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>paps</td>
<td>A space separated list of PAP endpoint URLs. Endpoints will be tried in</td>
<td>Y</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>turn until one returns a successful response. This provides limited failover</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>support. If more intelligent failover is necessary or load balancing is</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>required, a dedicated load-balancer/failover appliance should be used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>retention-Interval</td>
<td>The number of minutes the PDP will retain (cache) a policy retrieved</td>
<td>N</td>
<td>240 (4 hours)</td>
</tr>
<tr>
<td></td>
<td>from the PAP. After this time is passed the PDP will again call out to the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PAP and retrieve the policy.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SECURITY section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>servicePrivateKey</td>
<td>An absolute path to the file containing the unencrypted, PEM-encoded, private key used by this service. All PDPs instances within a single logical PDP should use the same key</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>serviceCertificate</td>
<td>An absolute path to the file containing the unencrypted, PEM-encoded, certificate used by this service. All PDPs instances within a single logical PDP should use the same key</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>trustInfoDir</td>
<td>An absolute path to the directory that contains standard X.509 trust information, such as the IGTF Trust Anchor Distribution</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>enableSSL</td>
<td>Indicates whether the service port should use SSL/TLS or not</td>
<td>No</td>
<td>false</td>
</tr>
<tr>
<td>requireClientCertAuthentication</td>
<td>Indicates whether the client must use a valid client certificate to authenticate to the PDP</td>
<td>No</td>
<td>false</td>
</tr>
</tbody>
</table>

Example pdp.ini files

The following example file contain the bare minimum required for a valid PDP configuration file.

```ini
[SERVER]
entityID = http://argus.example.org/pdp
hostname = argus.example.org

[POLICY]
paps = https://argus.example.org:8150/pap/services/ProvisioningService

[SECURITY]
servicePrivateKey = /etc/grid-security/hostkey.pem
serviceCertificate = /etc/grid-security/hostcert.pem
trustInfoDir = /etc/grid-security/certificates
# HTTPS enabled
enableSSL = true
```

Advanced Configuration Options

The following advanced options are available but are unlikely to ever be used by deployers. They are mostly for performing very fine-grained tuning of request/response handling parameters. Incorrectly configuring these can have a very negative impact on performance so deployers should not change these unless they are very sure they understand what the impact will be.
## SERVICE section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum-requests</td>
<td>The maximum number of requests that will be processed simultaneously. Additional requests will be queued.</td>
<td>N</td>
<td>200</td>
</tr>
<tr>
<td>requestQueueSize</td>
<td>The maximum number of requests that will be queued up when all the processing threads are busy. Incoming requests received when all processing threads are busy and the queue is full will receive an HTTP 503 error.</td>
<td>N</td>
<td>500</td>
</tr>
<tr>
<td>connectionTimeout</td>
<td>This is the length of time, in seconds, the service will wait for the client to send information before it considers the request timed out.</td>
<td>N</td>
<td>30 seconds</td>
</tr>
<tr>
<td>receiveBufferSize</td>
<td>This is the size, in bytes, that will be allocated to the HTTP request buffer.</td>
<td>N</td>
<td>16384 (16kb)</td>
</tr>
<tr>
<td>sendBufferSize</td>
<td>This is the size, in bytes, that will be allocated to the HTTP response buffer.</td>
<td>N</td>
<td>16384 (16kb)</td>
</tr>
</tbody>
</table>

## POLICY section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-SetId</td>
<td>The ID of the policy to fetch from the PAP</td>
<td>None</td>
<td>-1</td>
</tr>
<tr>
<td>connectionTimeout</td>
<td>This is the length of time, in seconds, the PAP client will wait for the PAP to send information before it considers the request timed out</td>
<td>None</td>
<td>30</td>
</tr>
<tr>
<td>receiveBufferSize</td>
<td>This is the size, in bytes, that will be allocated to the PAP client send buffer</td>
<td>No</td>
<td>16384 (16KB)</td>
</tr>
<tr>
<td>sendBufferSize</td>
<td>This is the size, in bytes, that will be allocated to the PAP client request buffer</td>
<td>No</td>
<td>16384 (16KB)</td>
</tr>
</tbody>
</table>

## SECURITY section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustInfoRefresh</td>
<td>The frequency, in minutes, that the trust material specified by trustInfoDir will be checked for updates.</td>
<td>N</td>
<td>60 (1 hour)</td>
</tr>
<tr>
<td>messageValidityPeriod</td>
<td>The number of seconds, from the time a message is issued, until it is considered expired.</td>
<td>N</td>
<td>300s (5 minutes)</td>
</tr>
<tr>
<td>clockSkew</td>
<td>The allowance, in seconds, used when computing validity periods.</td>
<td>N</td>
<td>30s</td>
</tr>
</tbody>
</table>
Environment file

In the `/etc/sysconfig/argus-pdp` file are defined Argus PDP environment variables, described in the table below.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Default value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAVACMD</td>
<td>/usr/bin/java</td>
<td>Absolute path of the JVM executable.</td>
</tr>
<tr>
<td>PDP_JOPTS</td>
<td>-Xmx256M -Djdk.tls.trustNameService=true</td>
<td>Optional parameters to pass to the JVM when PDP is started/stopped.</td>
</tr>
<tr>
<td>PDP_START_JOPTS</td>
<td>empty</td>
<td>Optional parameters to pass to the JVM only when PDP is started/STOPPED; useful to enable JMX or remote debug.</td>
</tr>
<tr>
<td>PDP_HOME</td>
<td>/usr/share/argus/pdp</td>
<td>Absolute path of PDP installation directory.</td>
</tr>
<tr>
<td>PDP_CONF</td>
<td>/etc/argus/pdp/pdp.ini</td>
<td>Absolute path of PDP configuration file.</td>
</tr>
<tr>
<td>PDP_CONFDIR</td>
<td>/etc/argus/pdp</td>
<td>Absolute path of PDP configuration directory.</td>
</tr>
<tr>
<td>PDP_LOGDIR</td>
<td>/var/log/argus/pdp</td>
<td>Absolute path of PDP logs directory.</td>
</tr>
<tr>
<td>PDP_LIBDIR</td>
<td>/var/lib/argus/pdp/lib</td>
<td>Absolute path of PDP libraries.</td>
</tr>
<tr>
<td>PDP_ENDORSEDDIR</td>
<td>/var/lib/argus/pdp/endorsed</td>
<td>Absolute path of PDP endorsed libraries.</td>
</tr>
<tr>
<td>PDP_PROVIDEDDIR</td>
<td>/var/lib/argus/pdp/provided</td>
<td>Absolute path of PDP provided libraries.</td>
</tr>
<tr>
<td>PDP_PID</td>
<td>/var/run/argus-pdp.pid</td>
<td>Absolute path of PDP PID file.</td>
</tr>
</tbody>
</table>

**Attention:**
The option `-Djdk.tls.trustNameService=true` is mandatory in Argus version 1.7 with TLS turned on. This system property enforce the host name check to avoid JDK bug [https://bugs.openjdk.java.net/browse/JDK-8133196](https://bugs.openjdk.java.net/browse/JDK-8133196).

**Attention:**
The Argus version 1.7 provides an environment file with the default values described above. In case of update from the previous version, a new file named `/etc/sysconfig/argus-pdp.rpmnew` will be created. Manually overwrite the file and restart the service.

### 5.1.3 Argus Policy Decision Point (PDP): Operation

#### Service Operation Commands

Start the PDP service

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td><code>service argus-pdp start</code></td>
</tr>
<tr>
<td>EL7</td>
<td><code>systemctl start argus-pdp</code></td>
</tr>
</tbody>
</table>
Stop the PDP service

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>service argus-pdp stop</td>
</tr>
<tr>
<td>EL7</td>
<td>systemctl stop argus-pdp</td>
</tr>
</tbody>
</table>

Restart the PDP service

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>service argus-pdp restart</td>
</tr>
<tr>
<td>EL7</td>
<td>systemctl restart argus-pdp</td>
</tr>
</tbody>
</table>

PDP service status information

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>service argus-pdp status</td>
</tr>
<tr>
<td>EL7</td>
<td>systemctl status argus-pdp</td>
</tr>
</tbody>
</table>

Reload PDP policies Causes the currently cached copy of the policies received from the PAP can be flushed from memory, and retrieved a new from the PAP.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>pdpctl reloadPolicy</td>
</tr>
<tr>
<td>EL7</td>
<td>pdpctl reloadPolicy</td>
</tr>
</tbody>
</table>

Service Information

Service Ports

- Default Service Port: 8152
- Default Admin Port: 8153

The PDP service only requires the standard service port to be open to those PEPd services which will communicate with the PDP. The PDP must also be able to make outbound connections to those PAPs from which remote policies will be retrieved.

Service Endpoint URLs

This service contains the following endpoint URLs:

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://HOSTNAME:8152/authz">https://HOSTNAME:8152/authz</a></td>
<td>This endpoint is the recipient of authorization requests.</td>
</tr>
<tr>
<td><a href="http://127.0.0.1:8153/status">http://127.0.0.1:8153/status</a></td>
<td>This endpoint provides current status information on the PDP. This endpoint is password protected.</td>
</tr>
<tr>
<td><a href="http://127.0.0.1:8153/reloadPolicy">http://127.0.0.1:8153/reloadPolicy</a></td>
<td>This endpoint instructs the PDP to flush, and retrieve anew, its policy from the PAP. This endpoint is password protected.</td>
</tr>
<tr>
<td><a href="http://127.0.0.1:8153/shutdown">http://127.0.0.1:8153/shutdown</a></td>
<td>This endpoint instructs the PDP to shutdown. This endpoint is password protected.</td>
</tr>
</tbody>
</table>
Note: Admin services may be password protected and thus not invokable without this password.

Logging and Logs

This service uses the logback logging library. Java developers are probably familiar with Apache Log4J, logback is written by the developer who initially wrote Log4J and contains a cleaner API and is much more performant. The configuration file for the logging system can be found in $PDP_HOME/conf/logging.xml and changes to this file are picked up every 5 minutes.

Enable Debug Logging

To enable debug logging follow:

1. Locate the line that contains logger name="org.glite.authz" (line 10 in the default logging config)
2. On the following line, change INFO to DEBUG

In some cases it may be helpful to see the policy being evaluated for each request. To do this:

1. Locate the line that contains org.glite.authz.message.policy (line 22 in the default logging config)
2. On the following line, change INFO to DEBUG

In some cases it may be helpful to see the incoming and outgoing messages. To do this:

1. Locate the line that contains org.glite.authz.message.protocol (line 27 in the default logging config)
2. On the following line, change INFO to DEBUG

Note: always change your logging levels back to their original values once you are done debugging a problem. Keeping the system on the debug logging level could fill up your disk partition in a short time.

Service Logs

The service writes three different logs, located in /var/log/argus/pdp (EMI) or $PDP_HOME/logs (gLite):

- **process.log** - This log file contains the normal, human-oriented logging messages that the system generates while in operation. This can be thought of as the debug log (though that’s really only true if configured to log debug messages).
- **access.log** - This file is an Apache-style access log showing information about incoming requests. This log is meant to be machine parsed. Each line contains the following ‘|’ (pipe) delimited fields:
  - request time - time of the request, in the UTC timezone, from the Unix epoch (Jan 1, 1970, 00:00:00 UTC)
  - remote host - the hostname or IP address of the host that contacted the PDP
  - server host - the hostname or IP address on which the server received the request
  - server port - the port on which the server received the request
  - request path - the URL path that was requested
- **audit.log** - This file contains information useful for auditing the system (e.g. results of authorization requests). This log is meant to be machine parsed. Each line contains the following ‘|’ (pipe) delimited fields:
– request time - time of the request, in the UTC timezone, from the Unix epoch (Jan 1, 1970, 00:00:00 UTC)
– requester ID - the entity ID of the PEP that made the request
– request ID - the ID of the incoming authorization request
– policy ID - the ID of the policy set that was evaluated in order to reach the authorization decision
– policy version - the version of the policy that was evaluated in order to reach the authorization decision
– policy decision - the authorization decision that was reached
– response ID - the ID of the authorization response sent back to the PEP

5.1.4 Argus: Policy Decision Point (PDP): Troubleshooting

**PDP Uses “Old” Policies**

The PDP caches policies received from the PAP in order to avoid the cost of fetching and parsing them for every request. In cases where you know, or suspect, the policy used by the PDP is no longer in synch with the policy stored at the PAP you may use the command

```bash
pdpctl reloadPolicy
```

to force the PDP to flush its policy cache and retrieve the latest policy from the PAP.

**Private Key File Access**

Many systems protect their private keys so that only super-user accounts can read them. Starting, and running the PDP, as such an account is strongly discouraged. The recommend approach is to create a special group (e.g. ‘hostkey’) that has read permissions to the key and ensure the user running the PDP service is also in this group. This group should **not** have write permission to the key.

Some people might view this as a loss of security, because, if the service user account were compromised the attacker would be able to read the private key. However, the service holds a copy of key in memory once it starts and this copy can easily be accessed via tools that come with the JRE.
In the Argus authorization framework the Policy Enforcement Point is implemented as a client-server architecture. The PEP Daemon is the server component and there are different lightweight PEP clients available: C client, Java client, and GSI PEP Callout client.

6.1 Summary

6.1.1 Argus PEP Server Installation

Installation

To deploy the Argus PEP Server, please follow the documentation Argus Deployment.

6.1.2 Argus PEP Server: Configuration

Configuration Files

The PEPd is configured through the use of the pepd.ini file, located in /etc/argus/pepd directory.

There is also an environment file, located in /etc/sysconfig/argus-pepd, that contains environment variables used by the init script that manage the service.

Configuration File Syntax

The pepd.ini file is a standard INI file with different defined sections. The SERVICE section contains properties related the PEP Server service as a whole and how it listens for incoming requests. The PDP section that control how callouts to the PDP are made. The final section, SECURITY, contains properties that related to various security aspects of the service, the services private key and certificate, for example.
PIP Configuration

Each Policy Information Point (PIP) is configured in its own INI section, referenced in the `SERVICE` section under the `pips` property.

The configuration properties needed by each PIP is specific to that given PIP. Some will not require any properties beyond the standard set while other will need addition information.

- See the `Policy Information Point` documentation for more information:
  - Request Validator PIP
  - OpenSSL Subject Converter PIP
  - gLite Grid Authorization Profile PIP
  - Common XACML Authorization Profile PIP

Obligation Handler Configuration

Each `Obligation Handler` (OH) is configured in its own INI section, referenced in the `SERVICE` section under the `obligationHandlers` property.

The configuration properties needed by each Obligation Handler is specific to that given OH. Some will not require any properties beyond the standard set while other will need addition information.

See the `Obligation Handler` documentation for more information, in particular the `Gridmap Account Mapping Obligation Handler`.

Basic Configuration Options
**SERVICE section**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>entityID</td>
<td>This is a unique identifier for the PEP. It must be a URI (URL or URN) and the same entity ID should be used for all PEP instances that make up a single logical PEP. If a URL is used it need not resolve to any specific webpage.</td>
<td>Y</td>
<td>None. Recommended value is a URL corresponding to the logical PEP service (e.g. <a href="http://pep.example.org">http://pep.example.org</a>).</td>
</tr>
<tr>
<td>hostname</td>
<td>This is the hostname or IP address to which the service will bind.</td>
<td>Y</td>
<td>None</td>
</tr>
<tr>
<td>port</td>
<td>This is the port to which the service will bind.</td>
<td>N</td>
<td>8154</td>
</tr>
<tr>
<td>adminHost</td>
<td>The hostname upon which the service will listen for admin commands.</td>
<td>N</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>adminPort</td>
<td>This is the port upon which the service will listen for admin commands. This port is only available on the localhost (127.0.0.1).</td>
<td>N</td>
<td>8155</td>
</tr>
<tr>
<td>adminPass</td>
<td>This is the password required to accompany admin commands. If unspecified than no password is required to run admin commands.</td>
<td>N</td>
<td>None</td>
</tr>
<tr>
<td>pips</td>
<td>This is a space separated list of the INI section names that configure policy information points (PIP) that the PEP will invoke upon the arrival of every request. PIPs are executed in the order listed by this property. See the policy information point documentation for more information.</td>
<td>N</td>
<td>None</td>
</tr>
<tr>
<td>obligationHandlers</td>
<td>This is a space separated list of the INI section names that configure obligations handlers that the PEP will use to fulfill obligation requirements sent back by the PDP. See the obligation handler documentation for more information.</td>
<td>N</td>
<td>None</td>
</tr>
</tbody>
</table>

**PDP section**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdps</td>
<td>A space separated list of PDP endpoint URLs. Endpoints will be tried in turn until one returns a successful response. This provides limited failover support. If more intelligent failover is necessary or load balancing is required, a dedicated load-balancer/failover appliance should be used.</td>
<td>Y</td>
<td>None</td>
</tr>
<tr>
<td>maximumCachedResponses</td>
<td>The maximum number of responses from any PDP that will be cached. Setting this value to 0 (zero) will disable caching. The maximum amount of time a single response is cached is controlled by the cachedResponseTTL property described below.</td>
<td>N</td>
<td>500</td>
</tr>
</tbody>
</table>
**SECURITY section**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>servicePrivateKey</td>
<td>An absolute path to the file containing the unencrypted, PEM-encoded, private key used by this service.</td>
<td>Yes, if requests from the PEP client should be done over HTTPS.</td>
<td>None.</td>
</tr>
<tr>
<td>serviceCertificate</td>
<td>An absolute path to the file containing the unencrypted, PEM-encoded, certificate used by this service.</td>
<td>Yes, if requests from the PEP client should be done over HTTPS.</td>
<td>None.</td>
</tr>
<tr>
<td>trustInfoDir</td>
<td>An absolute path to the directory that contains standard X.509 trust information, such as the IGTF Trust Anchor Distribution.</td>
<td>Required when connecting to PDPs over HTTPS.</td>
<td>None.</td>
</tr>
<tr>
<td>enableSSL</td>
<td>Enable HTTPS on the service port (SSL/TLS). The serviceCertificate, servicePrivateKey, and trustInfoDir properties must also be defined in order to use this setting.</td>
<td>N</td>
<td>false</td>
</tr>
<tr>
<td>requireClientCertAuthentication</td>
<td>The client must have a valid X.509 client certificate to authenticate to the PEP Server</td>
<td>N</td>
<td>true</td>
</tr>
</tbody>
</table>

**Example pepd.ini files**

The following example file contain the bare minimum required for a valid PEP configuration file.

```
[SERVICE]
entityId = https://argus.example.org/pep
hostname = argus.example.org

[PDP]
pdps = https://argus.example.org:8152/authz

[SECURITY]
```

The following example file contains the bare minimum required for a valid PEP configuration plus the configuration of a couple PIPs. Note how each element in the list pips list of the SERVER section matches the name section configuring the PIP. Also note that the REQVALIDATOR_PIP takes a few additional configuration parameters.

```
[SERVICE]
entityId = http://argus.example.org/pep
hostname = argus.example.org
pips = REQVALIDATOR_PIP

[PDP]
pdps = https://argus.example.org:8152/authz https://pdp2.example.org:8152/authz

[SECURITY]
servicePrivateKey = /etc/grid-security/hostkey.pem
serviceCertificate = /etc/grid-security/hostcert.pem
trustInfoDir = /etc/grid-security/certificates
enableSSL = true
requireClientCertAuthentication = true
```

(continues on next page)
Advanced Configuration Options

The following advanced options are available but are unlikely to ever be used by deployers. They are mostly for performing very fine-grained tuning of request/response handling parameters. Incorrectly configuring these can have a very negative impact on performance so deployers should not change these unless they are very sure they understand what the impact will be.

SERVICE section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximumRequests</td>
<td>The maximum number of requests that will be processed simultaneously. Additional requests will be queued.</td>
<td>N</td>
<td>200</td>
</tr>
<tr>
<td>requestQueueSize</td>
<td>The maximum number of requests that will be queued up when all the processing threads are busy. Incoming requests received when all processing threads are busy and the queue is full will receive an HTTP 503 error.</td>
<td>N</td>
<td>500</td>
</tr>
<tr>
<td>connectionTimeout</td>
<td>This is the length of time, in seconds, the service will wait for the client to send information before it considers the request timed out.</td>
<td>N</td>
<td>30 seconds</td>
</tr>
<tr>
<td>receiveBufferSize</td>
<td>This is the size, in bytes, that will be allocated to the HTTP request buffer.</td>
<td>N</td>
<td>16384 (16kb)</td>
</tr>
<tr>
<td>sendBufferSize</td>
<td>This is the size, in bytes, that will be allocated to the HTTP response buffer.</td>
<td>N</td>
<td>16384 (16kb)</td>
</tr>
</tbody>
</table>

PDP section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximumRequests</td>
<td>The maximum number of simultaneous requests that will be made to the PDP. Additional requests will wait until a free request slot becomes available</td>
<td>No</td>
<td>200</td>
</tr>
<tr>
<td>cachedResponseTTL</td>
<td>The length of time, in seconds, for which a response will be cached</td>
<td>No</td>
<td>600 (10 minutes)</td>
</tr>
<tr>
<td>connectionTimeout</td>
<td>This is the length of time, in seconds, the PDP client will wait for the PDP to send information before it considers the request timed out</td>
<td>No</td>
<td>30</td>
</tr>
<tr>
<td>receiveBufferSize</td>
<td>This is the size, in bytes, that will be allocated to the PDP client send buffer</td>
<td>None</td>
<td>16384 (16 KB)</td>
</tr>
<tr>
<td>sendBufferSize</td>
<td>This is the size, in bytes, that will be allocated to the PDP client request buffer</td>
<td>None</td>
<td>16384 (16 KB)</td>
</tr>
</tbody>
</table>
SECURITY section

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>trustInfoRefresh</td>
<td>The frequency, in minutes, that the trust material specified by trustInfoDir will be checked for updates.</td>
<td>N</td>
<td>60 (1 hour)</td>
</tr>
</tbody>
</table>

Environment file

In the /etc/sysconfig/argus-pepd file are defined Argus PEPd environment variables, described in the table below.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Default value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAVACMD</td>
<td>/usr/bin/java</td>
<td>Absolute path of the JVM executable.</td>
</tr>
<tr>
<td>PEPD_JOPTS</td>
<td>-Xmx256M -Djdk.tls.trustNameService=true</td>
<td>Optional parameters to pass to the JVM when PEPd is started/stopped</td>
</tr>
<tr>
<td>PEPD_START_JOPTS</td>
<td>empty</td>
<td>Optional parameters to pass to the JVM only when PEPd is started; useful to enable JMX or remote debug</td>
</tr>
<tr>
<td>PEPD_HOME</td>
<td>/usr/share/argus/pepd</td>
<td>Absolute path of PEPd installation directory</td>
</tr>
<tr>
<td>PEPD_CONF</td>
<td>/etc/argus/pepd/pepd.ini</td>
<td>Absolute path of PEPd configuration file.</td>
</tr>
<tr>
<td>PEPD_CONFIGDIR</td>
<td>/etc/argus/pepd/pepd.ini</td>
<td>Absolute path of PEPd configuration directory.</td>
</tr>
<tr>
<td>PEPD_LOGDIR</td>
<td>/var/log/argus/pepd</td>
<td>Absolute path of PEPd logs directory.</td>
</tr>
<tr>
<td>PEPD_LIBDIR</td>
<td>/var/lib/argus/pepd/lib</td>
<td>Absolute path of PEPd libraries.</td>
</tr>
<tr>
<td>PEPD_ENDORSED</td>
<td>/var/lib/argus/pepd/lib/endorsed</td>
<td>Absolute path of PEPd endorsed libraries.</td>
</tr>
<tr>
<td>PEPD_PROVIDED</td>
<td>/var/lib/argus/pepd/lib/provided</td>
<td>Absolute path of PEPd provided libraries.</td>
</tr>
<tr>
<td>PEPD_PID</td>
<td>/var/run/argus-pepd.pid</td>
<td>Absolute path of PEPd PID file.</td>
</tr>
</tbody>
</table>

Attention:
The option -Djdk.tls.trustNameService=true is mandatory in Argus version 1.7 with TLS turned on. This system property enforce the host name check to avoid JDK bug https://bugs.openjdk.java.net/browse/JDK-8133196

Attention:
The Argus version 1.7 provides an environment file with the default values described above. In case of update from the previous version, a new file named /etc/sysconfig/argus-pepd.rpmnew will be created. Manually overwrite the file and restart the service.
6.1.3 Argus PEP Server: Operation

For more Argus details, see the Argus Service Reference Card.

Service Operation Commands

Start the PEP service

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>service argus-pepd start</td>
</tr>
<tr>
<td>EL7</td>
<td>systemctl start argus-pepd</td>
</tr>
</tbody>
</table>

Stop the PEP service

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>service argus-pepd stop</td>
</tr>
<tr>
<td>EL7</td>
<td>systemctl stop argus-pepd</td>
</tr>
</tbody>
</table>

Restart the PEP service

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>service argus-pepd restart</td>
</tr>
<tr>
<td>EL7</td>
<td>systemctl restart argus-pepd</td>
</tr>
</tbody>
</table>

PEP service status information

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>service argus-pepd status</td>
</tr>
<tr>
<td>EL7</td>
<td>systemctl status argus-pepd</td>
</tr>
</tbody>
</table>

Clear PEP service response cache  Causes the currently cached responses from the PDP can be flushed from memory

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>EL6</td>
<td>pepdctl clearResponseCache</td>
</tr>
<tr>
<td>EL7</td>
<td>pepdctl clearResponseCache</td>
</tr>
</tbody>
</table>

Service Information

Service Ports

- Default Service Port: 8154
- Default Admin Port: 8155

The PEP service only requires the standard service port to be open to those PEP clients which will communicate with the PEP. The PEP must also be able to make outbound connections to those PDPs to which is will make policy decision requests.
Service Endpoints

This service contains the following endpoint URLs:

https://argus.example.org:8154/authz  This endpoint is the recipient of authorization requests and is reachable on the standard service host and port.

http://127.0.0.1:8155/status  This endpoint provides current status information on the PEP daemon and is reachable on the standard admin host and port.

http://127.0.0.1:8155/clearResponseCache  This endpoint instructs the PEP daemon to flush its PDP response cache. It is reachable on the standard admin host and port.

http://127.0.0.1:8155/shutdown  This endpoint instructs the PEP daemon to shutdown and is reachable on the standard admin host and port.

Note: Admin services may be password protected and thus not invokable without this password.

Logging and Logs

This service uses the logback logging library. Java developers are probably familiar with Apache Log4J, logback is written by the developer who initially wrote Log4J and contains a cleaner API and is much more performant. The configuration file for the logging system can be found in $PEP_HOME/conf/logging.xml and changes to this file are picked up every 5 minutes.

Enable Debug Logging

To enable debug logging follow:

1. Locate the line that contains logger name="org.glite.authz" (line 10 in the default logging config)
2. On the following line, change INFO to DEBUG

In some cases it may be helpful to see the incoming and outgoing messages. To do this:

1. Locate the line that contains org.glite.authz.message.protocol (line 15 in the default logging config)
2. On the following line, change INFO to DEBUG

Note: Always change your logging levels back to their original values once you are done debugging a problem. Keeping the system on the debug logging level could fill up your disk partition in a short time.

Service Logs

The service writes three different logs, located in $PEP_HOME/logs:

- **process.log** - This log file contains the normal, human-oriented logging messages that the system generates while in operation. This can be thought of as the debug log (though that’s really only true if configured to log debug messages).

- **access.log** - This file is an Apache-style access log showing information about incoming requests. This log is meant to be machine parsed. Each line contains the following ‘|’ (pipe) delimited fields:
– request time - time of the request, in the UTC timezone, from the Unix epoch (Jan 1, 1970, 00:00:00 UTC)
– remote host - the hostname or IP address of the host that contacted the PDP
– server host - the hostname or IP address on which the server received the request
– server port - the port on which the server received the request
– request path - the URL path that was requested

• audit.log - This file contains information useful for auditing the system (e.g. results of authorization requests). This log is meant to be machine parsed. Each line contains the following '|' (pipe) delimited fields:
  – request time - time of the request, in the UTC timezone, from the Unix epoch (Jan 1, 1970, 00:00:00 UTC)
  – request ID - the ID of the authorization request
  – responder ID - the URL of the PDP that responded to the authorization request
  – response ID - the ID of the response message sent back from the PDP
  – policy decision - the authorization decision that was reached

6.1.4 Argus PEP Server: Troubleshooting

PEP Daemon Returns “Stale” Results

The PEPd keeps a short (10 minutes by default) response cache. So identical requests made within a short time period will always provide the same answer. If you’re testing this can be a pain. You can clear the cache using the `pepdctl clearResponseCache` command. You can also turn off the cache through the `maximumCachedResponses` documented in the PEPd configuration. Just be sure to enable it again before you put the system under heavy load.

Note that the PDP also caches the policies it reads, so during testing you may also want to configure the PDP to more quickly pick up policies from the PAP via the `retentionInterval` option.

Testing a policy without submitting a job

When authoring new policies or troubleshooting an existing policies it can be helpful to mock up requests, instead of getting users to perform the request over and over as you diagnose the problem. The PEPd offers a C and Java command line tool. The C tool is useful for specifically testing cases where policies are based on the resource ID, action ID, subject ID, and FQAN attributes. The Java tool allows you to mock up any request.

Here is an example of using the C command line tool to test a job submission. It specifies the PEPd service, resource ID, action ID, user’s DN, and primary FQAN.

```
/opt/glite/bin/pepcli -v -x \
  -p http://vesta.switch.ch:8154/authz \
  -r http://authz-interop.org/xacml/resource/resource-type/wn \
  -a http://authz-interop.org/xacml/action/action-type/execute-now \
  -s "CN=Alessandro Usai,O=SWITCH,C=CH,DC=users,DC=switch,DC=grid,DC=quovadisglobal,DC=com" \
  -f /dech \
```

6.1.5 Argus PEP Server Policy Information Points (PIP)

Policy Information Points (PIPs) are plugins to the authorization service that help populate and/or complete an authorization request. PIPs may rely on information already within the request or they may simply be able to self generate the data that they will add.

6.1. Summary
The following PIPs are currently available:

**Request Validator PIP**

*Warning: This PIP is new in Argus 1.3 (EMI).*

The Request Validator PIP validates the incoming authorization request. It checks that the incoming authorization request contains at least one subject, one resource and one action, and that the attributes within them have at least one value, which is not null or an empty string.

**Configuration**

1. Create a new INI section for your PIP (you may choose any valid INI section name, e.g. REQVALIDATOR_PIP)
2. Into the PIP INI section add the `parserClass` property with the value `org.glite.authz.pep.pip.provider.RequestValidatorPIPIniConfigurationParser`
3. Configure how the authorization request must be validated

**PIP Configuration Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>validateRequestSubjects</td>
<td>Require at least one subject with non-empty attribute values</td>
<td>N</td>
<td>true</td>
</tr>
<tr>
<td>validateRequestResources</td>
<td>Require at least one resource with non-empty attribute values</td>
<td>N</td>
<td>true</td>
</tr>
<tr>
<td>validateRequestAction</td>
<td>Require one action with non-empty attribute values</td>
<td>N</td>
<td>true</td>
</tr>
<tr>
<td>validateRequestEnvironment</td>
<td>Require one environment with non-empty attribute values</td>
<td>N</td>
<td>false</td>
</tr>
</tbody>
</table>

**Example Configuration**

The following example shows a PEP server configuration with the request validator PIP enabled. The PIP validates the incoming authorization request and checks that it contains at least one subject, at least one resource and one action, all with non-empty or null attributes values.

```
[SERVICE]
entityId = https://example.org/pep
hostname = example.org
pips = REQVALIDATOR_PIP

[SECURITY]
trustInfoDir = /etc/grid-security/certificates
```

(continues on next page)
### OpenSSL Subject Converter PIP

**Warning:** This PIP is new in Argus 1.3 (EMI).

The OpenSSL Subject Converter PIP transforms on-the-fly an incoming request subject attribute `subject-id` and/or attribute `subject-issuer` value from the old, unsupported and wrong OpenSSL oneline format (e.g. “/C=CH/O=example.org/CN=John Doe”) into a correct RFC2253 format value (e.g. “CN=John Doe,O=example.org,C=CH”) with the correct datatype.

#### Configuration

1. Create a new INI section for you PIP (you may choose any valid INI section name. e.g. `OPENSSLSUBJECT_PIP`)
2. Into the PIP INI section add the `parserClass` property with the value `org.glite.authz.pep.pip.provider.OpenSSLSubjectPIPIniConfigurationParser`
3. Configure which subject attribute ID and datatype values must be transformed from the OpenSSL format into the RFC2253 format.

#### PIP Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>opensslSubjectAttributeIDs</td>
<td>The space separated list of subject attribute IDs containing an OpenSSL value to convert</td>
<td>No</td>
<td><code>urn:oasis:names:tc:xacml:1.0:subject:subject-id http://glite.org/xacml/attribute/subject-issuer</code></td>
</tr>
<tr>
<td>opensslSubjectAttributeDatatypes</td>
<td>The space separated list of subject attribute datatypes containing an OpenSSL value to convert</td>
<td>No</td>
<td><code>http://www.w3.org/2001/XMLSchema#string</code></td>
</tr>
</tbody>
</table>

#### Example Configuration

The following example shows a PEP server configuration with the OpenSSL Subject Converter PIP enabled, and transforming both the subject attribute IDs `urn:oasis:names:tc:xacml:1.0:subject:subject-id` and `http://glite.org/xacml/attribute/subject-issuer` with the datatype `http://www.w3.org/2001/XMLSchema#string` values from the OpenSSL oneline format into the RFC2253 format.
Grid Authorization Profile PIP

**Warning:** This is the default profile supported starting from Argus 1.2.

This PIP allows the PEP client to send only the end-user certificate or proxy as lone Subject *Key-Info* attribute. It will then parse the certificate, extract all the information from the certificate required by the gLite Grid XACML Authorization Profiles, and populate the request with attributes found in the certificate/proxy.

This PIP implements the XACML Grid Worker Node Authorization Profile (v.1.0) and the XACML Grid Computing Element Authorization Profile (v.1.0) specifications.

**Configuration**

1. Create a new INI section for you PIP (you may choose any valid INI section name. e.g. GLITEXACMLPROFILE_PIP)
2. Into the PIP INI section add the `parserClass` property with the value `org.glite.authz.pep.pip.provider.OpenSSLSubjectPIPIDIniConfigurationParser`
3. To enable VOMS attribute certificate support add the `vomsInfoDir` property with a value corresponding to the absolute path of the VOMS vomsdir, traditionally `/etc/grid-security/vomsdir`.
4. If, in the `SECURITY` section, the `trustInfoDir` property is not already set, add it with a value of the absolute filesystem path of your IGTF trust bundle.
5. Configure which profile IDs are to be accepted.
PIP Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceptedProfileIDs</td>
<td>The space separated list of accepted authorization profile IDs</td>
<td>No</td>
<td>None.</td>
</tr>
<tr>
<td>vomsInfoDir</td>
<td>The absolute path to the VOMS vomsdir directory.</td>
<td>Y</td>
<td>None.</td>
</tr>
<tr>
<td>vomsInfoRefresh</td>
<td>The refresh interval time in minutes of the vomsInfoDir directory.</td>
<td>No</td>
<td>60</td>
</tr>
<tr>
<td>requireCertificate</td>
<td>The request Subject attribute key-info MUST be present in the incoming request.</td>
<td>No</td>
<td>true</td>
</tr>
<tr>
<td>requireProxy</td>
<td>The request Subject attribute key-info MUST be a proxy (PEM encoded proxy chain).</td>
<td>No</td>
<td>false</td>
</tr>
</tbody>
</table>

Note: If the acceptedProfileIDs is not defined, then all profile IDs present in the request environment profile-id attribute are accepted.

Required Request Attributes

This PIP requires that the request environment contains a profile-id attribute with the profile identifier, and that the request subject contains the certificate, and its chain, that were used to authenticate to the service, in the key-info attribute:

- The Profile Identifier
  - type: Environment
  - id: http://glite.org/xacml/attribute/profile-id
  - data type: http://www.w3.org/2001/XMLSchema#anyURI
  - multiple values allowed: no
  - description: The profile ID implemented by the incoming request.

- The Certificate or Proxy Certificate (with chain)
  - type: Subject
  - id: urn:oasis:names:tc:xacml:1.0:subject:key-info
  - data type: http://www.w3.org/2001/XMLSchema#string
  - multiple values allowed: no
  - description: The PEM encoded certificate chain. No certificate order is assumed however all certificates must be version 3 certificates. Zero or one VOMS attribute certificate may also be included.

Populated Effective Request Attributes

The PIP will process the request subject key-info attribute and populate the following attributes:

- The Subject Identifier
  - type: Subject
– **id:** urn:oasis:names:tc:xacml:1.0:subject:subject-id
– **data type:** urn:oasis:names:tc:xacml:1.0:data-type:x500Name
– **multiple values allowed:** no
– **description:** This is the Subject DN as given in the end-entity certificate. It is in RFC2253 format.

• The End-entity Certificate Issuer
  – **type:** Subject
  – **id:** http://glite.org/xacml/attribute/subject-issuer
  – **data type:** urn:oasis:names:tc:xacml:1.0:data-type:x500Name
  – **multiple values allowed:** yes
  – **description:** This is the Subject DN of the root CA and all subordinate CAs that signed within the end-entity certificate chain, included the Subject Identifier DN. It is in RFC2253 format.

If VOMS support is enabled and a VOMS certificate is included within a user's proxy certificate, the following attributes will be populated within the request:

• The VO Name
  – **type:** Subject
  – **id:** http://glite.org/xacml/attribute/virtual-organization
  – **data type:** http://www.w3.org/2001/XMLSchema#string
  – **multiple values allowed:** yes
  – **description:** The names of the VOs to which the user is a member. Currently there is only ever one value.

• The VOMS Primary FQAN
  – **type:** Subject
  – **id:** http://glite.org/xacml/attribute/fqan/primary
  – **data type:** http://glite.org/xacml/datatype/fqan
  – **issuer:** DN of the attribute certificate issuer
  – **multiple values allowed:** no
  – **description:** The primary Fully Qualified Attribute Name (FQAN) for the subject

• The VOMS FQANs
  – **type:** Subject
  – **id:** http://glite.org/xacml/attribute/fqan
  – **data type:** http://glite.org/xacml/datatype/fqan
  – **multiple values allowed:** yes
  – **description:** All the Fully Qualified Attribute Name (FQAN)s for the subject

**Example Configuration**

The following example shows a PEP Server configuration with the Grid authorization profile PIP enabled, and accepting both the [http://glite.org/xacml/profile/grid-ce/1.0](http://glite.org/xacml/profile/grid-ce/1.0) and the [http://glite.org/xacml/profile/grid-wn/1.0](http://glite.org/xacml/profile/grid-wn/1.0) XACML Grid authorization profiles.
Common XACML Authorization Profile PIP

**Warning:** This profile is supported since Argus 1.6 (EMI-3).

This PIP allows the PEP client to send only the end-user certificate or proxy as lone Subject Key-Info attribute. It will then parse the certificate, extract all the information from the certificate required by the Common XACML Authorization Profile, and populate the request with attributes found in the certificate/proxy.

This PIP implements the Common XACML Authorization Profile (1.1.1) specifications.

**Configuration**

1. Create a new INI section for you PIP (you may choose any valid INI section name. e.g. COMMONXACMLPROFILE_PIP)

2. Into the PIP INI section add the `parserClass` property with the value `org.glite.authz.pep.pip.provider.CommonXACMLAuthorizationProfilePIPIniConfigurationParser`

3. To enable VOMS attribute certificate support add the `vomsInfoDir` property with a value corresponding to the absolute path of the VOMS vomsdir, traditionally `/etc/grid-security/vomsdir`.

4. If, in the `SECURITY` section, the `trustInfoDir` property is not already set, add it with a value of the absolute filesystem path of your IGTF trust bundle.

5. Configure which profile IDs are to be accepted, normally `http://dci-sec.org/xacml/profile/common-authz/1.1`
**PIP Configuration Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceptedProfileIDs</td>
<td>The space separated list of accepted authorization profile IDs</td>
<td>No</td>
<td>None.</td>
</tr>
<tr>
<td>vomsInfoDir</td>
<td>The absolute path to the VOMS vomsdir directory</td>
<td>YES</td>
<td>None.</td>
</tr>
<tr>
<td>vomsInfoRefresh</td>
<td>The refresh interval time in minutes of the vomsInfoDir directory.</td>
<td>No</td>
<td>60</td>
</tr>
<tr>
<td>requireCertificate</td>
<td>The request Subject attribute key-info MUST be present in the incoming request.</td>
<td>No</td>
<td>false</td>
</tr>
<tr>
<td>requireProxy</td>
<td>The request Subject attribute key-info MUST to be a proxy (PEM encoded proxy chain).</td>
<td>No</td>
<td>false</td>
</tr>
</tbody>
</table>

**Note:** If the acceptedProfileIDs is not defined, then all profile IDs present in the request environment profile-id attribute are accepted.

**Required Request Attributes**

This PIP requires that the request environment contains a profile-id attribute with the profile identifier, and that the request subject contains the certificate, and its chain, that were used to authenticate to the service, in the key-info attribute:

- **The Profile Identifier Attribute**
  - **type:** Environment
  - **id:** http://dci-sec.org/xacml/attribute/profile-id
  - **data type:** http://www.w3.org/2001/XMLSchema#anyURI
  - **multiple values allowed:** no
  - **description:** The profile ID implemented by the incoming request, typically http://dci-sec.org/xacml/profile/common-authz/1.1

- **The Subject Key-Info (certificate or proxy, with chain) Attribute**
  - **type:** Subject
  - **id:** urn:oasis:names:tc:xacml:1.0:subject:key-info
  - **data type:** http://www.w3.org/2001/XMLSchema#base64Binary
  - **multiple values allowed:** yes
  - **description:** The multiple values are the base64 encoded DER blocks of the certificate/proxy chain.

**Populated Effective Request Attributes**

The PIP will process the request subject key-info attribute and populate the following attributes:

- **The Subject Identifier Attribute**
  - **type:** Subject
• The Subject Issuer Attribute
  
  - **type:** Subject
  - **id:** http://dci-sec.org/xacml/attribute/subject-issuer
  - **data type:** urn:oasis:names:tc:xacml:1.0:data-type:x500Name
  - **multiple values allowed:** yes
  - **description:** X.509 distinguished name of the authority(ies) which issued the end-entity certificate. The values are in RFC2253 format.

• The CA Issuer Subject Attribute
  
  - **type:** Subject
  - **id:** http://glite.org/xacml/attribute/x509-subject-issuer
  - **data type:** urn:oasis:names:tc:xacml:1.0:data-type:x500Name
  - **multiple values allowed:** no
  - **description:** X.509 distinguished name of the authority which issued the end-entity certificate. The values are in RFC2253 format.

If VOMS support is enabled and a VOMS certificate is included within a user’s proxy certificate, the following attributes will be populated within the request:

• The Virtual Organization (VO) Attribute
  
  - **type:** Subject
  - **id:** http://dci-sec.org/xacml/attribute/virtual-organization
  - **data type:** http://www.w3.org/2001/XMLSchema#string
  - **multiple values allowed:** yes
  - **description:** The names of the VOs to which the user is a member. Currently there is only ever one value.

• The Primary Group and Group Attributes
  
  - **type:** Subject
  - **id:** http://dci-sec.org/xacml/attribute/group/primary and http://dci-sec.org/xacml/attribute/group
  - **data type:** http://www.w3.org/2001/XMLSchema#string
  - **multiple values allowed:** no (primary group), yes (groups)
  - **description:** The primary group name, and the list of all group names

• The Primary Role and Role Attributes
  
  - **type:** Subject
  - **id:** http://dci-sec.org/xacml/attribute/role/primary and http://dci-sec.org/xacml/attribute/role
  - **data type:** http://www.w3.org/2001/XMLSchema#string

6.1. Summary
issuer: The group name to which this role belong.

- multiple values allowed: no (primary role), yes (roles)
- description: The primary role, and roles list assigned to the subject.

Example Configuration

The following example shows a PEP Server configuration with the Common XACML authorization profile PIP enabled, and accepting the http://dci-sec.org/xacml/profile/common-authz/1.1 EMI Common XACML Authorization profile.

```
[SERVICE]
entityId = https://argus.example.org/pep
hostname = argus.example.org

pips = COMMONXACMLPROFILE_PIP

[PDP]
pdps = https://argus.example.org:8152/authz

[SECURITY]
trustInfoDir = /etc/grid-security/certificates

[COMMONXACMLPROFILE_PIP]
parserClass = org.glite.authz.pep.pip.provider.
˓→CommonXACMLAuthorizationProfilePIPIniConfigurationParser
vomsInfoDir = /etc/grid-security/vomsdir
acceptedProfileIDs = http://dci-sec.org/xacml/profile/common-authz/1.1
```

Authentication Profile PIP

**Warning:** This PIP has been introduced in Argus 1.7.1

This PIP uses the informations extracted from the certificate by Common XACML Authorization Profile PIP and Grid Authorization Profile PIP, so it must be configured as the last PIP into the PEP server.

This PIP looks in the request subject attributes for the attribute containing subject of the CA that issued the certificate contained in the request, and the attribute containing the VO name linked to the request.

If no attribute is found holding the CA subject, the PIP returns without modifying the request. Otherwise, this PIP checks whether the included certificate subject and VOMS attributes are allowed by local authentication profile policies.

If the policies are NOT met, subject and VOMS attributes are removed from the request. If the policies are met, the `x509-authn-profile` attribute is set, containing the authentication profile resolved for the request.

Configuration

1. Create a new INI section for the PIP, with any valid INI section name (e.g. AUTHN_PROFILE_PIP).
2. In this section add the `parserClass` property with the value `org.glite.authz.pep.pip.provider.authnprofilesip.AuthenticationProfilePIPConfigurationParser`.
3. Add the `authenticationProfilePolicyFile` property with a value corresponding to the absolute path of the authentication profile policies file, traditionally `/etc/grid-security/vo-ca-ap-file`.

4. Add the `trustAnchors.directory` property with a value of the absolute path of the trust anchors directory, where the PIP search the policy info files, typically `/etc/grid-security/certificates`.

5. Add the `trustAnchors.policyFilePattern` property with a value corresponding to a bash globbing expression that matches the policy info files, e.g. `policy-*.info`.

6. Optionally, add the `trustAnchors.refreshIntervalInSecs` property with a value in seconds, that is the refresh time interval used by the PIP to reload the policy files, e.g. 14400.

**Note:** The Argus 1.7.1 packages provide a default authentication profile policy file located in `/etc/argus/pepd/vo-ca-ap-file`. This file grants the access only to certificates issued by CAs in the IGTF `classic`, `mics` and `slcs` profiles.

### PIP Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authenticationProfilePolicyFile</code></td>
<td>Absolute path of authentication profile policy file</td>
<td>Yes</td>
<td><code>/etc/argus/pepd/vo-ca-ap-file</code></td>
</tr>
<tr>
<td><code>trustAnchors.directory</code></td>
<td>Absolute path where policy info files are located</td>
<td>No</td>
<td><code>/etc/grid-security/certificates</code></td>
</tr>
<tr>
<td><code>trustAnchors.policyFilePattern</code></td>
<td>Regular expression that matches the policy files to read</td>
<td>No</td>
<td><code>policy-*.info</code></td>
</tr>
<tr>
<td><code>trustAnchors.refreshIntervalInSecs</code></td>
<td>Time, in seconds, with which the PIP reload the policy files</td>
<td>No</td>
<td>14400</td>
</tr>
</tbody>
</table>

### Populated Effective Request Attributes

This PIP will process the request subject `x509-subject-issuer` attribute and populate the following attribute:

- The X.509 Authentication Profile Attribute
  - `type`: Subject
  - `id`: `http://glite.org/xacml/attribute/x509-authn-profile`
  - `data type`: `http://www.w3.org/2001/XMLSchema#string`
  - `multiple values allowed`: yes
  - `description`: The alias of the policy file that contains the DN of the CA issuer.

### Required Request Attributes

This PIP requires that the request environment contains the attributes extracted from the X.509 certificate/proxy by the other PIPs.

- The X.509 Subject Issuer Attribute
  - `type`: Subject
– **id:** http://glite.org/xacml/attribute/x509-subject-issuer  
– **data type:** urn:oasis:names:tc:xacml:1.0:data-type:x500Name  
– **multiple values allowed:** no  
– **description:** Distinguished Name of the CA issuer.

**Example Configuration**

The following example shows a PEP Server configuration with the Authentication Profile PIP enabled.

```
[SERVICE]
entityId = https://argus.example.org/pep
hostname = argus.example.org

pips = COMMONXACMLPROFILE_PIP AUTHN_PROFILE_PIP

[PDP]
pdps = https://argus.example.org:8152/authz

[AUTHN_PROFILE_PIP]
parserClass = org.glite.authz.pep.pip.provider.authnprofilesip.
  AuthenticationProfilePIPConfigurationParser
authenticationProfilePolicyFile = /etc/argus/pepd/vo-ca-ap-file
trustAnchors.directory = /etc/grid-security/certificates
trustAnchors.policyFilePattern = policy-*.info
trustAnchors.refreshIntervalInSecs = 14400
```

**Other Policy Information Points**

Here are other PIPs that you can configure for testing or debugging purpose:

**Attribute White List PIP**

This PIP can be used to filter out attributes that should not be accepted within a request.

**Configuration**

1. Create a new INI section for you PIP (you may choose any valid INI section name. e.g. WHITELIST_PIP)  
2. In to the PIP INI section add the `parserClass` property with the value `org.glite.authz.pep.pip.
  provider.AttributeWhitelistPIPIniConfigurationParser`  
3. Configure which request attributes are to be accepted
PIP Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceptedActionAttributes</td>
<td>spaced delimited list attribute IDs that may appear in the request action</td>
<td>N</td>
<td>None.</td>
</tr>
<tr>
<td>acceptedEnvironmentAttributes</td>
<td>spaced delimited list attribute IDs that may appear in the request environment</td>
<td>N</td>
<td>None.</td>
</tr>
<tr>
<td>acceptedResourceAttributes</td>
<td>spaced delimited list attribute IDs that may appear in the request resource</td>
<td>N</td>
<td>None.</td>
</tr>
<tr>
<td>acceptedSubjectAttributes</td>
<td>spaced delimited list attribute IDs that may appear in the request subject</td>
<td>N</td>
<td>None.</td>
</tr>
</tbody>
</table>

*Note:* If a property is not given then all attributes within the section (i.e. action, environment, resource, or subject) are accepted.

Example Configuration

The following example shows a PEP Server configuration with the whitelist PIP enabled, accepting only the `key-info` attribute from the request subject, and filtering out all other subject attributes. All the other request attributes (action, resource and environment) are accepted as is.

```
[SERVICE]
entityId = https://example.org/pep
hostname = example.org
pips = WHITELIST_PIP

[PDP]
pdps = http://localhost:8152/authz

[SECURITY]
trustInfoDir = /etc/grid-security/certificates

[WHITELIST_PIP]
parserClass = org.glite.authz.pep.pip.provider.
              AttributeWhitelistPIPIniConfigurationParser
acceptedSubjectAttributes = urn:oasis:names:tc:xacml:1.0:subject:key-info
```

Environment Time PIP

This PIP populates a few time-related attributes within the `environment` portion of the request.

*Tip:* Using this PIP effective disables the response caching in a PEP Server as will make every request different.

Configuration

1. Create a new INI section for you PIP (you may choose any valid INI section name. e.g. `TIME_PIP`)
2. To PIP INI section add the parserClass property with the value `org.glite.authz.pep.pip.provider.EnvironmentTimePIPIIniConfigurationParser`.

3. Add the name of the created PIP INI section to the list of PIPs in the SERVICE section.

**Prerequisite Request Attributes**

None.

**Populate Effective Request Attributes**

This PIP will populate the following attributes within the environment portion of the request.

- The Current Time
  - type: environment
  - data type: http://www.w3.org/2001/XMLSchema#time
  - issuer: any
  - multiple values allowed: no
  - description: The time, in the UTC timezone, the request was issued

- The Current Date
  - type: environment
  - id: urn:oasis:names:tc:xacml:1.0:environment:current-date
  - data type: http://www.w3.org/2001/XMLSchema#date
  - issuer: any
  - multiple values allowed: no
  - description: The date, in the UTC timezone, the request was issued

- The Current Date and Time
  - type: environment
  - id: urn:oasis:names:tc:xacml:1.0:environment:current-dateTime
  - data type: http://www.w3.org/2001/XMLSchema#dateTime
  - issuer: any
  - multiple values allowed: no
  - description: The date and time, in the UTC timezone, the request was issued

**Example Configuration**

The following example shows a PEP Server configuration with the Environment Time PIP enabled:
**Static Attributes PIP**

This PIP can populate the action, environment, resource, and subject of the request with a static set of attributes.

This PIP is very useful for testing as it allows for the creation of any arbitrary request.

**Configuration**

1. Create a new INI section for your PIP (you may choose any valid INI section name)
2. To PIP INI section add the `parserClass` property with the value `org.glite.authz.pep.pip.provider.StaticPIPIniConfigurationParser`
3. Define the property `staticAttributesFile` with a fully qualified path to a file that will hold the definitions for the static attributes
4. If populating action attributes, define the property `actionAttributes` with a space delimited list of the INI sections, defined in the `staticAttributesFile` file, that represent the attributes that should be treated as action attributes.
5. If populating environment attributes, define the property `environmentAttributes` with a space delimited list of the INI sections, defined in the `staticAttributesFile` file, that represent the attributes that should be treated as environment attributes.
6. If populating resource attributes, define the property `resourceAttributes` with a space delimited list of the INI sections, defined in the `staticAttributesFile` file, that represent the attributes that should be treated as resource attributes.
7. If populating subject attributes, define the property `subjectAttributes` with a space delimited list of the INI sections, defined in the `staticAttributesFile` file, that represent the attributes that should be treated as subject attributes.
8. If the defined subject attributes should be added to each subject in the request, define the property `includeSubjectAttributesInAllSubjects` with a value of “true”
9. Optionally define the property `defaultAttributeIssuer` to a value that will be used as the attribute issuer if the attribute definition does not define an issuer.
10. Add the name of the created PIP INI section to the list of PIPs in the `SERVICE` section

To define your static attribute files, repeat the following steps for each static attribute you wish to define:

1. Create a new INI section for you PIP (you may choose any valid INI section name)
2. Define the property `id` with the value of the ID of the attribute
3. Optionally define the property `datatype` with the datatype of the attribute. If no datatype is defined the default data type will be `http://www.w3.org/2001/XMLSchema#string`.

4. Optionally define the property `issuer` with the ID of the issuer for the attribute.

5. Define the property `values` with a delimited string representing the values of the attribute. See next step for the delimiter.

6. Optionally define the property `valueDelimiter` with a delimiter string used to separate values in the previous property. If no delimiter is defined the default delimiter is ',' (comma).

**Prerequisite**

None.

**Populate Attributes**

This PIP will populate those attributes defined in the `staticAttributesFile` file and referenced by either the `actionAttributes`, `environmentAttributes`, `resourceAttributes`, or `subjectAttributes` properties.

**Example Configuration**

The following example shows a PEP Server configuration with the Static Attributes PIP enabled:

```ini
[SERVICE]
entityId = https://example.org/pep
hostname = example.org
pips = STATIC

[PDP]
pdps = http://localhost:8152/authz

[STATIC]
parserClass = org.glite.authz.pep.pip.provider.StaticPIPIIniConfigurationParser
staticAttributesFile = /path/to/some/file.ini
actionAttributes = actionId
resourceAttributes = resourceId
subjectAttributes = subjectId
```

And here is a static attribute definition file, note that this file can include attributes which are not currently used as action, environment, resource, or subject attributes:

```ini
[actionId]
id = urn:oasis:names:tc:xacml:1.0:action:action-id
values = submit

[resourceId]
id = urn:oasis:names:tc:xacml:1.0:resource:resource-id
values = http://example.org/wn

[subjectId]
id = urn:oasis:names:tc:xacml:1.0:subject:subject-id
datatype = urn:oasis:names:tc:xacml:1.0:data-type:x500Name
values = CN=foo
```
6.1.6 Argus PEP Clients

pepcli

pepcli is the main ARGUS PEP client, based on the C API of the PEP client. The pepcli command allows you to submit a XACML request to the PEP daemon and display the XACML response. The command is very useful to check if a XACML policy applies (decision is Permit, Deny, Not Applicable or Indeterminate) for the given XACML request. Or to check if the XACML response correspond to the values you are expecting (uidgid, secondary-gids,...) for the user mapping.

Installation

The pepcli command is by default installed with the argus-authz metapackage, see Argus Deployment. But you can also install it separately on your host for testing purpose. To install it with YUM:

```
yum install argus-pepcli
```

Usage

Usage:
```
pepcli --pepd <URL> --keyinfo <FILE> [options...]
pepcli --pepd <URL> --subjectid <DN> [options...]
```
Submit a XACML Request to the PEPd and show the XACML Response.

Options:
```
-p|--pepd <URL> Argus PEP server endpoint URL.
-k|--keyinfo <FILE> XACML Subject key-info: proxy or X509 file.
-s|--subjectid <DN> XACML Subject identifier: user DN (format RFC2253).
-f|--fqan <FQAN> XACML Subject primary FQAN and FQANs
Add multiple --fqan options for secondary FQANs.
-r|--resourceid <URI> XACML Resource identifier.
-a|--actionid <URI> XACML Action identifier.
-t|--timeout <SEC> Connection timeout in second (default 30s).
-x|--requestcontext Show effective XACML Request context.
-v|--verbose Verbose.
-q|--quiet Turn off output.
-d|--debug Show debug information.
-h|--help This help.
-V|--version Display version and exit.
```
TLS options:
```
--capath <DIR> Directory containing the server PEM encoded CA certificates.
--cacert <FILE> Server PEM encoded CA certificate filename.
--cert <FILE> Client PEM encoded certificate filename.
--key <FILE> Client PEM encoded private key filename.
--keypasswd <PASSWD> Password of the client private key
If the --keypasswd is omitted and the private key is encrypted,
then you will be prompted for the password.
```

The MAN page is also available: man pepcli

6.1. Summary
Return Code

The `pepcli` command return 0 when a valid XACML Response have been received, but neither content of the XACML response, nor the decision value are checked.

On error the `pepcli` command returns the following value:

- 1 on memory allocation error
- 2 invalid option
- 3 certchain file or content (missing certificate block) error
- 4 XACML request error
- 5 PEP-C client library error (see output for more detail)

Examples

Submit a XACML Request to the PEP daemon endpoint URL https://argus.example.org:8154/authz (using SSL/TLS client authentication) for the resource identified by `my_resource_id` for the action `my_action_id`, using the Grid proxy as credentials `/tmp/x509up_u637`:

```bash
Decision: Permit
```

PEP Java Client Command Line

The PEP-J library contains a basic command line utility that is useful for sending test requests to the PEP daemon.

The command line client, `bin/testreq.sh`, takes a single parameter, the path (absolute or relative) path to a client configuration file. This client will create an empty request and then run any configured PIPs in order to populate it. The Static Attribute PIP is very useful for creating custom requests with which to test.

6.1.7 Argus PEP Client Library: C API

Documentation

The Doxygen documentation for the Argus PEP client library describes the C API and have an example.


PEP XACML Object Model

Basic Example

Basically, to use the Argus PEP client API, you will have to the following steps.

First, import the header with

```c
#include "argus/pep.h"
```

Create and initialize the PEP client handle with
PEP * pep = pep_initialize()

Set the PEP Server URL with

pep_setoption(pep, PEP_OPTION_ENDPOINT_URL, "https://pepd.example.org:8154/authz")

If the PEP Server URL is protected by HTTPS with client authentication (the default), you must also configure the client certificate or proxy with

pep_setoption(pep, PEP_OPTION_ENDPOINT_CLIENT_CERT, "/tmp/x509up_u500")

The client private key or proxy key with

pep_setoption(pep, PEP_OPTION_ENDPOINT_CLIENT_KEY, "/tmp/x509up_u500")

And the server CA trust anchors path with

pep_setoption(pep, PEP_OPTION_ENDPOINT_SERVER_CAPATH, "/etc/grid-security/certificates")

Optionally, you can register some Policy Information Points (PIP) and Obligation Handlers (OH) of your own with

pep_addpip(...)

and

pep_addobligationhandler(...)

Create a XACML Request and add the required Subject, Resource, Action and Environment to it with

xacml_request_create()
xacml_request_addsubject(request, subject)

and so on. See the PEP XACML Object Model for the complete API.

Submit the request and get the response:

pep_authorize(pep, &request, &response)

Process the response (if not already done by your obligation handlers). Release the PEP client handle with

pep_destroy(pep)
**Complex Example**

A more detailed PEP client example is available [here](http://argus-authz.github.com/argus-pep-api-c/doc/pep_client_example_8c-example.html).

**Multi-threaded Programming**

The Argus PEP client library is thread-friendly, but you are not allowed to share a PEP handle among multiple threads. Each thread has to create its own PEP handle:

```c
/* Each thread creates its own PEP handle */
PEP * pep = pep_initialize();
```

Within a thread you can reuse the PEP handle (multiple `pep_authorize()` calls).

If your threads are object (OO programming, ...), it is recommended you to create (`pep_initialize`) the PEP handle in the constructor, and release it (`pep_destroy`) in the destructor.

**Processing Authorization Decision**

The PEP client MUST abide by the authorization decision as described in here:

- If the decision is *Permit*, then the PEP client SHALL permit access. If *obligations* accompany the decision, then the PEP client SHALL permit access only if it understands and it can and will enforce those obligations.
- If the decision is *Deny*, then the PEP client SHALL deny access.
- If the decision is *NotApplicable*, meaning that no policy apply, then the PEP client SHALL deny access.
- If the decision is *Indeterminate*, then the PEP client SHALL deny access. The decision status message and status code should be used to produce an error message. Example:

```c
...  
xacml_result_t * result = xacml_response_getresult(response, i);
fprintf(stdout, "response.result[%d].decision=%s\n", i, decision_tostring(xacml_result_getdecision(result)));
fprintf(stdout, "response.result[%d].resourceid=%s\n", i, xacml_result_getresourceid(result));
if (xacml_result_getdecision(result) == XACML_DECISION_INDETERMINATE) {
    xacml_status_t * status = xacml_result_getstatus(result);
    fprintf(stdout, "response.result[%d].status.message=%s\n", i, xacml_status_getmessage(status));
    statuscode = xacml_status_getcode(status);
    fprintf(stdout, "response.result[%d].status.code.value=%s\n", i, xacml_statuscode_getvalue(statuscode));
}
...  
```

**6.1.8 Argus PEP Client: Java Programming Interface**

The Argus PEP Java client library is used to communicate with the Argus PEP daemon. It authorizes request and receives response back from Argus.
Javadoc


PEP XACML Object Model

The PEP client XACML object model implemented in the package org.glite.authz.common.model follow this schema:

```
1. Create a PEP client configuration and initialize it:

PEPClientConfiguration config = new PEPClientConfiguration();
config.addPEPDaemonEndpoint("https://argus.example.org:8154/authz");
// trust and key material for the HTTPS connection with client authentication
config.setTrustMaterial("/etc/grid-security/certificates");
config.setKeyMaterial("/etc/grid-security/hostcert.pem", "/etc/grid-security/hostkey.pem", "keystore_password");

2. Create the PEP client based on the config:

PEPClient pep = new PEPClient(config);
```

At this point you have a multi-threaded PEP client that can be reuse to submit many authorization requests to the PEP server.

3. Create an authorization request for a user proxy certificate, based on a profile:

```
// read the user proxy
PEMFileReader reader = new PEMFileReader();
X509Certificate[] userproxy = reader.readCertificates("/tmp/x509up_u959");

// create the request for a given profile
AuthorizationProfile profile = GridWNAuthorizationProfile.getInstance();
Request request = profile.createRequest(userproxy,
    "http://example.org/wn/cluster1",
    GridWNAuthorizationProfile.ACTION_EXECUTE);
```

4. Authorize the request with the Argus PEP daemon:

Basic Example

This is a very simplified example, omitting all the error handling, on how to create a PEP client, a request, and then authorize the request and process the response.

1. Create a PEP client configuration and initialize it:

```java
PEPClientConfiguration config = new PEPClientConfiguration();
config.addPEPDaemonEndpoint("https://argus.example.org:8154/authz");
// trust and key material for the HTTPS connection with client authentication
config.setTrustMaterial("/etc/grid-security/certificates");
config.setKeyMaterial("/etc/grid-security/hostcert.pem", "/etc/grid-security/hostkey.pem", "keystore_password");
```

2. Create the PEP client based on the config:

```java
PEPClient pep = new PEPClient(config);
```

At this point you have a multi-threaded PEP client that can be reuse to submit many authorization requests to the PEP server.

3. Create an authorization request for a user proxy certificate, based on a profile:

```java
// read the user proxy
PEMFileReader reader = new PEMFileReader();
X509Certificate[] userproxy = reader.readCertificates("/tmp/x509up_u959");

// create the request for a given profile
AuthorizationProfile profile = GridWNAuthorizationProfile.getInstance();
Request request = profile.createRequest(userproxy,
    "http://example.org/wn/cluster1",
    GridWNAuthorizationProfile.ACTION_EXECUTE);
```

4. Authorize the request with the Argus PEP daemon:
Response response = pep.authorize(request);

5. Extract the user mapping information from the response:

```java
// will throw an exception if the authorization response is not *Permit*, or if the
→obligation is not present
Obligation posixMappingObligation = profile.getObligationPosixMapping(response);
String userId = profile.getAttributeAssignmentUserId(posixMappingObligation);
String groupId = profile.getAttributeAssignmentPrimaryGroupId(posixMappingObligation);
List<String> groupIds = profile.
→getAttributeAssignmentGroupIds(posixMappingObligation);
```

**Processing Authorization Decision**

The PEP client MUST abide by the authorization decision as described in here:

- If the decision is Permit, then the PEP client SHALL permit access. If obligations accompany the decision, then the PEP client SHALL permit access **only if it understands and it can and will enforce** those obligations.
- If the decision is Deny, then the PEP client SHALL deny access.
- If the decision is NotApplicable, meaning that no policy apply, then the PEP client SHALL deny access.
- If the decision is Indeterminate, then the PEP client SHALL deny access. The decision status message and status code should be used to produce an error message.

**GUI**

There is also a Java-based GUI available for sending requests to a PEPd. Just download the application to your desktop and start it. Once you’ve downloaded it you can restart it by double-clicking the Argus-PEP-Client.jnlp file.

**Java-based GUI**

![Java-based GUI](image)

**6.1.9 Argus GSI PEP Callout**
Module Description

The Globus Toolkit version 3.2 and later have the ability to customize the authorization and gridmap lookup (currently available in the GridFTP and Gatekeeper servers). The Globus Authorization Callouts framework allows to plug in authorization and mapping modules.

The GSI PEP Callout module implements the functionality to authorize and map the user by calling out to the Argus PEP Server.

Authorization and Mapping

Based on the Grid credentials, typically a proxy certificate, the GSI PEP Callout module will send an authorization request to the Argus PEP Server, and then parse the authorization response decision to authorize the user and the obligations to map him to a local account.

XACML Profile

The GSI PEP Callout module implements the XACML Grid Worker Node Authorization Profile 1.0, and by default uses the identifiers described in the profile.

XACML Request

The GSI PEP Callout module sends a request to the PEP Daemon with the following elements:

- XACML subject with the attribute element:
  - AttributeId: urn:oasis:names:tc:xacml:1.0:subject:key-info
  - Value: The PEM encoded Grid credentials provided by the calling service

- XACML resource with the attribute element:
  - AttributeId: urn:oasis:names:tc:xacml:1.0:resource:resource-id
  - Value: The value of the GSI PEP Callout configuration directive xacml_resourceid.

- XACML action with the attribute element:
  - AttributeId: urn:oasis:names:tc:xacml:1.0:action:action-id
  - Value: The service being requested by the client (e.g. file for GridFTP) or the name of the service passed to the gatekeeper.

- XACML environment with the attribute element:
  - AttributeId: http://glite.org/xacml/attribute/profile-id
  - Value: http://glite.org/xacml/profile/grid-wn/1.0 (Default)

XACML Response

The PEP Daemon sends back a response to the GSI PEP Callout module. The following response elements are parsed to authorize and map the user:

- XACML decision element: Contains the authorization decision Permit, Deny, Indeterminate or NotApplicable
6.1.10 Argus GSI PEP Callout: Installation

6.1.11 Manual Installation

The GSI PEP Callout module requires the following RPM:

```bash
yum install argus-gsi-pep-callout
```

The package includes the shared library implementing the GSI authorization and mapping module.

Configuration

Manual Configuration

To configure the GSI PEP Callout module, you first have to configure the Globus Authorization Callouts framework to use the GSI PEP Callout library to do the authorization and mapping. Then the GSI PEP Callout module must be configured.

Globus Authorization Callouts Configuration

Configuration file and configuration directives for the Globus Authorization Callouts to enable the GSI PEP Callout module.

Configuration File

The Globus Authorization Callouts framework uses the following locations (in order) for the callout configurations file:

- `$GSI_AUTHZ_CONF` (Environment variable)
- `/etc/grid-security/gsi-authz.conf`
- `$GLOBUS_LOCATION/etc/gsi-authz.conf`
- `$HOME/.gsi-authz.conf`

EMI-1 Configuration Directives

Content of the Globus Authorization Callouts configuration file to enable the GSI Argus PEP Callout function `argus_pep_callout` for EMI:

```bash
# Globus authorization and mapping callout to the ARGUS GSI PEP Callout module
# format: globus_mapping <library_path> <function_name>
globus_mapping /usr/lib64/libgsi_pep_callout.so argus_pep_callout
```
For EMI the Argus PEP GSI callout library is installed in the `/usr/lib64` directory.

**GSI PEP Callout Configuration**

Configuration file and configuration directives for the GSI PEP Callout module.

**Configuration File**

The GSI PEP Callout module uses the following locations (in order) for the configurations file:

- `$GSI_PEP_CALLOUT_CONF` (Environment variable)
- `/etc/grid-security/gsi-pep-callout.conf`

**Configuration Directives**

The configuration directives for the GSI PEP Callout are single name value lines. Lines with comments `#` are allowed.
<table>
<thead>
<tr>
<th>Directive</th>
<th>Description</th>
<th>Mandatory?</th>
<th>Default Value</th>
<th>Example</th>
<th>Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>pep_url</td>
<td>The endpoint URL of the PEP daemon.</td>
<td>Yes</td>
<td>pep_url <a href="https://pepd.example.org:8154/authz">https://pepd.example.org:8154/authz</a></td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>xacml_resourceid</td>
<td>XACML request resource-id value. Define this parameter to overwrite the service name passed to the module by the application</td>
<td>Yes</td>
<td>xacml_resourceid x-urn:example.org:resource:ce:gridftp</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>xacml_actionid</td>
<td>XACML request action-id value. Define this parameter to overwrite the service name passed to the module by the application</td>
<td>No</td>
<td>xacml_actionid <a href="http://glite.org/xacml/action/access">http://glite.org/xacml/action/access</a></td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>xacml_profileid</td>
<td>XACML request profile-id value. Define this parameter to overwrite the default profile id</td>
<td>No</td>
<td><a href="http://glite.org/xacml/profile/grid-wm/1.0">http://glite.org/xacml/profile/grid-wm/1.0</a></td>
<td>xacml_profileid <a href="http://glite.org/xacml/profile/grid-ce/1.0">http://glite.org/xacml/profile/grid-ce/1.0</a></td>
<td>1.2</td>
</tr>
<tr>
<td>pep_timeout</td>
<td>Connection timeout in seconds</td>
<td>No</td>
<td>30</td>
<td>pep_timeout 60</td>
<td>1.0</td>
</tr>
<tr>
<td>pep_ssl_validation</td>
<td>Enable SSL validation of the PEP daemon endpoint URL (HTTPS)</td>
<td>No</td>
<td>true</td>
<td>pep_ssl_validation false</td>
<td>1.0</td>
</tr>
<tr>
<td>pep_ssl_server_capath</td>
<td>CA directory path for the HTTPS validation of the PEP daemon endpoint URL</td>
<td>No</td>
<td>/etc/grid-security/certificates</td>
<td>pep_ssl_server_capath /etc/grid-security/certificates</td>
<td>1.0</td>
</tr>
<tr>
<td>pep_ssl_server_cert</td>
<td>Certificate file for the HTTPS validation of the PEP daemon endpoint URL</td>
<td>No</td>
<td>/etc/grid-security/pepdcert.pem</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>pep_ssl_client_cert</td>
<td>Certificate file for the TLS client authentication on the PEP daemon endpoint URL</td>
<td>No</td>
<td>/etc/ssl/mycert.pem</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>pep_ssl_client_key</td>
<td>Client private key file for the TLS client authentication on the PEP daemon endpoint URL</td>
<td>No</td>
<td>/etc/ssl/mykey.pem</td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>pep_ssl_client_keypasswd</td>
<td>Client private key password Only if pep_ssl_client_key is encrypted</td>
<td>Only if pep_ssl_client_key is encrypted</td>
<td>mykeypassword</td>
<td></td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Configuration Example**

Example of a valid configuration file for the GSI PEP Callout module:

```plaintext
#/ GSI PEP Callout configuration example
pep_url https://chaos.switch.ch:8154/authz
xacml_resourceid http://ce.example.org/cream/gridftp
```
YAIM Configuration

The `yaim-core` (>= 4.0.12) the function `config_lcas_lcmaps_gt4` is now able to configure the Argus GSI PEP callout module.

In your `site-info.def` set the following variables:

```plaintext
USE_ARGUS=yes
ARGUS_PEPD_ENDPOINTS="<Argus_URL> ..."
CREAM_PEPC_RESOURCEID=<CreamCE_XACML_resource_id>
```

where `Argus_URL` is the Argus PEP daemon endpoint URL. e.g. `ARGUS_PEPD_ENDPOINTS=https://argus.example.org:8154/authz`

where `CreamCE_XACML_resource_id` is the XACML resource identifier for this cream CE. e.g. `CREAM_PEPC_RESOURCEID=http://glite.org/xacml/resource/cream-ce`

Troubleshooting

Syslog

By default the GSI PEP Callout module logs info and error via syslog.

The syslog facility used is `local5` and the identifier is `gsi_pep_callout`. These log messages are typically in `/var/log/messages`

Enabling Debug Information

You can enable the debugging mode of the GSI PEP Callout module to troubleshoot your problem.

Environment Variables

You can set the following environment variables to enable debug mode:

- `GSI_PEP_CALLOUT_DEBUG_LEVEL` Set the debug level from 0 (none) to 9 (lot of info). Default is 0.
- `GSI_PEP_CALLOUT_DEBUG_FILE` Set the file to log the debugging information. Default is `stderr`.

Example

This example shows how to start the GridFTP server in debug mode. The configuration files `gsi-authz.conf` and `gsi-pep-callout.conf` must be correctly configured as previously described.

```plaintext
export GLOBUS_CALLOUT_DEBUG_LEVEL=5
# set the gsi-authz config to use (default /etc/grid-security/gsi-authz.conf)
export GSI_AUTHZ_CONF=/etc/grid-security/gsi-authz.conf
# set the gsi-pep-callout config to use (default /etc/grid-security/gsi-pep-callout.conf)
export GSI_PEP_CALLOUT_CONF=/etc/grid-security/gsi-pep-callout.conf
export GSI_PEP_CALLOUT_DEBUG_LEVEL=5

globus-gridftp-server -d 255 -p 9999 -debug
```
The GridFTP server is now running and listening on port 9999. Use the `uberftp` client or `globus-url-copy` to connect to the server with your Grid credentials and obtain debugging information from the server:

```
uberftp -P 9999 HOSTNAME
globus-url-copy file:///etc/passwd gsiftp://HOSTNAME:9999/tmp/e33
```

### 6.1.12 Argus PEP Server Obligation Handlers

Obligation handlers are plugins used by the authorization service in order to adjust the environment, under which an action will run, to a state that meets a particular set of obligations. Obligation are things like “write output to directory X” or “perform all work as user 1”.

**Grid Map POSIX Account Mapping Obligation Handler**

**Note:** The Grid Map Account Mapping Obligation Handler only works with the Grid Authorization Profile PIP, or with clients implementing the XACML Grid Worker Node Authorization Profile (v.1.0) or the XACML Grid Computing Element Authorization Profile (v.1.0) specifications.

This obligation handler maps a subject ID, given as a DN, and set of FQANs, for example those provided by the Grid Authorization Profile PIP, in to a POSIX account (login name, primary group name and secondary group names).

This mapping is controlled by two grid map files, one that provides the mapping of the subject to an account indicator (login name or pool account indicator) and one that maps the subject to a set of group names (one primary and any number of secondary).

**Configuration**

1. Create the account and group *mapping files* appropriate for your environment
2. Create a new INI section for your handler (you may choose any valid INI section name)
3. To handler INI section add the `parserClass` property with the value `org.glite.authz.pep.obligation.dfpmap.DFPMObligationHandlerConfigurationParser`
4. Define at least the required (`accountMapFile`, `groupMapFile`, `gridMapDir`) and any optional configuration properties for this handler
OH Configuration Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
<th>Default Value</th>
<th>Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>accountMapFile</td>
<td>The absolute path to the map file used to map a subject to a POSIX login name.</td>
<td>Y</td>
<td>None.</td>
<td>Argus 1.0</td>
</tr>
<tr>
<td>groupMapFile</td>
<td>The absolute path to the map file used to map a subject to a set of POSIX groups.</td>
<td>Y</td>
<td>None.</td>
<td>Argus 1.0</td>
</tr>
<tr>
<td>gridMapDir</td>
<td>The absolute path to the grid map directory.</td>
<td>Y</td>
<td>None.</td>
<td>Argus 1.0</td>
</tr>
<tr>
<td>handledObligationId</td>
<td>The identifier of the obligation handled by the handler. The obligation handler is triggered only if the obligation ID match this value.</td>
<td>N</td>
<td><a href="http://glite.org/xacml/obligation/local-environment-map">http://glite.org/xacml/obligation/local-environment-map</a></td>
<td>Argus 1.5</td>
</tr>
<tr>
<td>preferDNForLoginName</td>
<td>Indicates whether to prefer a DN based mapping for the login name mapping over a primary FQAN login name mapping.</td>
<td>N</td>
<td>true</td>
<td>Argus 1.1</td>
</tr>
<tr>
<td>preferDNForPrimaryGroupName</td>
<td>Indicates whether to prefer a DN based mapping for the primary group name mapping over a primary FQAN group name mapping</td>
<td>N</td>
<td>true</td>
<td>Argus 1.2</td>
</tr>
<tr>
<td>noPrimaryGroupNameIsError</td>
<td>Indicates that if the failure to find a primary group mapping in the group map file cause the obligation handler to fail..</td>
<td>N</td>
<td>false</td>
<td>Argus 1.2</td>
</tr>
<tr>
<td>refreshPeriod</td>
<td>The period, in minutes, between when the map files are checked, and if they have been changed, reread.</td>
<td>N</td>
<td>15</td>
<td>Argus 1.0</td>
</tr>
<tr>
<td>requireSubjectKeyInfo</td>
<td>The obligation handler will only be applied if the request subject contains a key-info attribute (PEM encoded certificate)</td>
<td>N</td>
<td>true</td>
<td>Argus 1.3.0</td>
</tr>
<tr>
<td>useSecondaryGroupNamesForMapping</td>
<td>The obligation handler will create lease file names containing the secondary groups of the user</td>
<td>N</td>
<td>true</td>
<td>Argus 1.3.1</td>
</tr>
</tbody>
</table>

Note: the default preferDNForLoginName property value was false for Argus 1.0 and Argus 1.1. From Argus 1.2 the default is true.

Required Response Obligation Trigger

This obligation handler is triggered if the PDP response contains the obligation http://glite.org/xacml/obligation/local-environment-map, or the value defined by the handledObligationId parameter.

Required Request Attributes

This obligation handler requires the following request attributes in order to correctly map the user. The attributes can be provided by the Grid Authorization Profile PIP, or directly by the clients implementing the XACML Grid
Worker Node Authorization Profile (v.1.0) or the XACML Grid Computing Element Authorization Profile (v.1.0) specifications.

- The Subject Identifier
  - type: Subject
  - id: urn:oasis:names:tc:xacml:1.0:subject:subject-id
  - data type: urn:oasis:names:tc:xacml:1.0:data-type:x500Name
  - multiple values allowed: no
  - description: This is the Subject DN as given in the end-entity certificate. It is in RFC2253 format.
- The VOMS Primary FQAN
  - type: Subject
  - id: http://glite.org/xacml/attribute/fqan/primary
  - data type: http://glite.org/xacml/datatype/fqan
  - issuer: DN of the attribute certificate issuer
  - multiple values allowed: no
  - description: The primary Fully Qualified Attribute Name (FQAN) for the subject
- The VOMS FQANs
  - type: Subject
  - id: http://glite.org/xacml/attribute/fqan
  - data type: http://glite.org/xacml/datatype/fqan
  - multiple values allowed: yes
  - description: All the Fully Qualified Attribute Name (FQAN)s for the subject

Response Obligation Results

This result of this obligation handler is the replacement of the generic http://glite.org/xacml/obligation/local-environment-map with the more specific obligation http://glite.org/xacml/obligation/local-environment-map/posix.

This later obligation carries the account and group names in the following attribute assignments:

- one http://glite.org/attribute/xacml/user-id account login name
- zero or one http://glite.org/attribute/xacml/group-id/primary primary group name
- zero or more http://glite.org/xacml/attribute/group-id secondary group names

Example Configuration

This is an example PEPd configuration file with one gridmap POSIX account mapping obligation handler defined:

```
[SERVICE]
entityId = http://argus.example.org/pep
hostname = argus.example.org
obligationHandlers = ACCOUNT_MAPPING_OH
```

(continues on next page)
Account and Group Mapping

This Obligation Handler uses the following logic to determine the mapping of the subject to a POSIX account.

Preconditions

- The input to this process is the subject DN of the end-entity certificate of the user and optionally a primary FQAN and a list of secondary FQANs.
- When dealing with the account map file (the gridmap file) and the group map file, entries are evaluated in the order listed in the file. Once a match is found processing stops.
- The grid map directory is populated with information for all configured pool accounts on the system. A pool account is considered “configured” if there is a zero-byte file, whose name is the pool account name, in the grid map directory. The grid map directory must also be read/writable by the user running the authorization service.

Mapping Steps

1. If a primary FQAN is given it is checked against the mappings listed in the account map file. If the primary FQAN matches a key in the map file then the associated value provides the account indicator.
2. If no account indicator was determined by means of the primary FQAN the subject DN is checked against the mappings listed in the account map file. If the DN matches a key in the map file then the associated value provides the account indicator. If no match is found processing stops and no map is available.
3. If the account indicator starts with a period (‘.’), its value, without the period, is considered to be a pool account name prefix. If the account indicator does not start with a period it is a POSIX account name. If no account indicator was determined the mapping process fails.
4. If a primary FQAN is given then it is evaluated against entries in a group map file. The first entry that matches determines the primary group name. If no match is found, the mapping process fails.
5. If one or more secondary FQANs are given then each one is matched against the group map file and each match determines a secondary group name. If no matches occur then there are no secondary group names associated with the account.
6. If the account indicator is a POSIX account name, and zero or one primary group and zero or more secondary group names were determined then the mapping is completed. The user is mapped to that account.
7. If the account indicator is a pool account name prefix a lookup in the grid map directory occurs. The file looked for is generated according to the template `encoded_dn{:primary_group_name{:secondary_group_name})*}` with the secondary group names listed in ascending alphabetical order.
8. If the file exists and has a link count of 2 then the hard link is followed to a file whose name is used as the POSIX account name. The last modified time of the two files is updated to the current time. If the link count is not 2 or the POSIX account name does not start with the account name prefix, the mapping process fails.

9. If the file does not exist, a list of files, within the grid map directory, matching the pool account name prefix followed exclusively by one or more numeric digits, is retrieved. An example regular expression representation of this would be prod[0-9]+.

10. This list of files is searched for a file whose link count is 1, this is a candidate pool account file. A hard link to the pool account file, whose name corresponds to the filled in template described above is then created. If no such pool account file is found the mapping process fails.

11. The pool account file link count is rechecked, if it is more than 2 (indicating another request mapped to that same file at the same time) the created link is removed and the mapping process reverts to the previous step.

12. If the link count is 2 the mapping is complete. The user is mapped to the pool account corresponding to the given file.

Note: In the case where no FQANs are available, this obligation handler only returns a login name. No group information is returned.

DN Encoding Rules

1. Leading zeros are removed from attribute types that are encoded as dotted decimal OIDs

2. DirectoryString attribute values of type PrintableString and UTF8String are not output in hexadecimal format

3. DirectoryString attribute values of types other than PrintableString and UTF8String are output in hexadecimal format

4. Leading and trailing white space characters are removed from non-hexadecimal attribute values (unless the value consists entirely of white space characters)

5. Internal substrings of one or more white space characters are converted to a single space in non-hexadecimal attribute values

6. Relative Distinguished Names containing more than one Attribute Value Assertion (AVA) are output in the following order: an alphabetical ordering of AVAs containing standard keywords, followed by a numeric ordering of AVAs containing OID keywords.

7. The only characters in attribute values that are escaped are those which section 2.4 of RFC 2253 states must be escaped (they are escaped using a preceding backslash character)

8. The entire name is converted to upper case using US localization

9. The entire name is converted to lower case using US localization

10. The name is finally normalized using normalization form KD, as described in the Unicode Standard and UAX #15

11. The DN is converted to the non-standard, OpenSSL one line format

12. The string is then URL-encoded

Note:

• A reorder of entries in the group map file that results in a change in the primary group will cause an incoming user to be mapped to a new account as this information is part of the link created in the grid map directory.
• A reordering of entries in the group map file that does not result in a change to the primary group but provides the same secondary groups in a different order does not result in a new mapping for a returning user since the link created in the grid map directory orders the secondary group names in ascending alphabetical order.
7.1 Nagios Probes for Argus (UMD)

7.1.1 Installation

Prerequisites

- Python 2.4 or newer (not Python 3000)
- UMD-3 or later (or EMI-3) repository installed
- Host certificate & IGTF-bundle
- Nagios server

Where to install

- This set of probes needs to be installed on the Nagios server only. On the client side (where the Argus services actually run), no action is required.

Install instructions

There is available a rpm called “nagios-plugins-argus”, (nagios-plugins-argus - v. 1.1.0 (EMI-3). It can be installed as follows:

```
yum install nagios-plugins-argus
```

This installs the plugins into the `/usr/libexec/grid-monitoring/probes/` directory. It is up to the user to bind them into the local Nagios environment.

**NOTE:** If you use iptables you need to open the ports on client side (where the Argus services are installed):

for IPv4 do:
iptables -I INPUT 1 -p tcp --dport 8154 -j ACCEPT
iptables -I INPUT 1 -p tcp --dport 8152 -j ACCEPT
iptables -I INPUT 1 -p tcp --dport 8150 -j ACCEPT
/etc/init.d/iptables save
/etc/init.d/iptables restart

for IPv6 do:

ip6tables -I INPUT 1 -p tcp --dport 8154 -j ACCEPT
ip6tables -I INPUT 1 -p tcp --dport 8152 -j ACCEPT
ip6tables -I INPUT 1 -p tcp --dport 8150 -j ACCEPT
/etc/init.d/ip6tables save
/etc/init.d/ip6tables restart

7.1.2 Overview of probes

There are 9 different probes available, three for each service:

<table>
<thead>
<tr>
<th>Service</th>
<th>Probe-Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP</td>
<td>nagios-plugins-argus.PAP.memory</td>
</tr>
<tr>
<td></td>
<td>nagios-plugins-argus.PAP.policies</td>
</tr>
<tr>
<td></td>
<td>nagios-plugins-argus.PAP.status</td>
</tr>
<tr>
<td>PDP</td>
<td>nagios-plugins-argus.PDP.memory</td>
</tr>
<tr>
<td></td>
<td>nagios-plugins-argus.PDP.status</td>
</tr>
<tr>
<td></td>
<td>nagios-plugins-argus.PDP.traffic</td>
</tr>
<tr>
<td>PEPD</td>
<td>nagios-plugins-argus.PEP.memory</td>
</tr>
<tr>
<td></td>
<td>nagios-plugins-argus.PEP.status</td>
</tr>
<tr>
<td></td>
<td>nagios-plugins-argus.PEP.traffic</td>
</tr>
</tbody>
</table>

PAP probes

nagios-plugins-argus.PAP.status

Checks if the service is available. This is done by a call to https://`hostname`:8150/pap/status, if there is a valid response the service is considered up and running.
## Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--hostname=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>--cert CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td></td>
<td>--key KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td></td>
<td>--capath CAPATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td></td>
<td>--help</td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>--port PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td></td>
<td>--url URL</td>
<td>The status endpoint URL of the service, e.g. <a href="https://hostname:port/status">https://hostname:port/status</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--version</td>
<td>show program’s version number and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>--timeout TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>--verbose</td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>

**nagios-plugins-argus.PAP.memory**

The response of the call executed by the status probe is parsed. The value for the current memory consumption is read out and displayed in the Status information field of the Nagios control panel and written into the Performance Data tab of Nagios. Hence it can be displayed as a graph over time by Nagios add-ons, e.g. pnp.
Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>–host-name=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–warning MEM_WARN</td>
<td>Memory usage warning threshold in MB</td>
<td>224.0</td>
</tr>
<tr>
<td></td>
<td>–critical MEM_CRIT</td>
<td>Memory usage critical threshold in MB</td>
<td>256.0</td>
</tr>
<tr>
<td></td>
<td>–cert CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td></td>
<td>–key KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td></td>
<td>–capath CAPATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td></td>
<td>–help</td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–port PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td></td>
<td>–url URL</td>
<td>The status endpoint URL of the service, e.g. <a href="https://hostname:port/status">https://hostname:port/status</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>–version</td>
<td>show program’s version number and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–timeout TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>–verbose</td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>

`nagios-plugins-argus.PAP.policies`

The response of the call executed by the status probe is parsed. The value for the current number of policies in the monitored PAP is read out and displayed in the Status information field of the Nagios control panel and written into the Performance Data tab of Nagios. Hence it can be displayed as a graph over time by Nagios add-ons, e.g. pnp.
## Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>–hostname=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–cert CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td></td>
<td>–key KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td></td>
<td>–capath CAPATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td></td>
<td>–help</td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–port PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td></td>
<td>–url URL</td>
<td>The status endpoint URL of the service, e.g. <a href="https://hostname:port/status">https://hostname:port/status</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>–version</td>
<td>show program’s version number and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–timeout TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>–verbose</td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>

### PDP probes

**nagios-plugins-argus.PDP.status**

Checks if the service is available. This is done by a call to `https://hostname:8152/status`, if there is a valid response the service is considered up and running.
Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>–hostname=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–cert CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td></td>
<td>–key KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td></td>
<td>–capath CAPATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td></td>
<td>–help</td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–port PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td></td>
<td>–url URL</td>
<td>The status endpoint URL of the service, e.g. <a href="https://hostname:port/status">https://hostname:port/status</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>–version</td>
<td>show program's version number and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–timeout TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>–verbose</td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>

nagios-plugins-argus.PDP.memory

The response of the call executed by the status probe is parsed. The value for the current memory consumption is read out and displayed in the Status information field of the Nagios control panel and written into the Performance Data tab of Nagios. Hence it can be displayed as a graph over time by Nagios add-ons, e.g. pnp.
### Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>--hostname=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td>--warning</td>
<td>MEM_WARN</td>
<td>Memory usage warning threshold in MB</td>
<td>224.0</td>
</tr>
<tr>
<td>--critical</td>
<td>MEM_CRIT</td>
<td>Memory usage critical threshold in MB</td>
<td>256.0</td>
</tr>
<tr>
<td>--cert</td>
<td>CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td>--key</td>
<td>KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td>--capath</td>
<td>CAPATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td>--help</td>
<td></td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td>--port</td>
<td>PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td>--url</td>
<td>URL</td>
<td>The status endpoint URL of the service, e.g. <a href="https://hostname:port/status">https://hostname:port/status</a></td>
<td></td>
</tr>
<tr>
<td>--version</td>
<td></td>
<td>show program’s version number and exit</td>
<td></td>
</tr>
<tr>
<td>--timeout</td>
<td>TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td>--verbose</td>
<td></td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>

**nagios-plugins-argus.PDP.traffic**

The response of the call executed by the status probe is parsed. The value for the current number of requests executed and the number how many of them have been successful is read out and compared to the same numbers of the former test executed. Out of this the requests per second, the completed requests per second and the erroneous requests per second are computed and written into the Performance Data tab of Nagios. Hence it can be displayed as a graph over time by Nagios add-ons, e.g. pnp. Additionally the number of requests since the last test is written into the Status information field of the Nagios control panel.
### Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>–hostname=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–cert CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td></td>
<td>–key KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td></td>
<td>–capath CA-PATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td></td>
<td>–tempdir=TEMP_DIR</td>
<td>Storage path for the needed temporary file</td>
<td>../../../../var/lib/grid-monitoring/nagios-plugins-argus</td>
</tr>
<tr>
<td></td>
<td>–tempfile=TEMP_FILE</td>
<td>Name for the needed temporary file</td>
<td>hostname.nagios-plugins-argus.PDP.traffic.pickle</td>
</tr>
<tr>
<td></td>
<td>–help</td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–port PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td></td>
<td>–url URL</td>
<td>The status endpoint URL of the service, e.g. <a href="https://hostname:port/status">https://hostname:port/status</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>–version</td>
<td>show program’s version number and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–timeout TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>–verbose</td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>

### PEP Server probes

**nagios-plugins-argus.PEP.status**

Checks if the service is available. This is done by a call to `https://hostname:8154/status`, if there is a valid response the service is considered up and running.
## Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>–hostname=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–warning MEM_WARN</td>
<td>Memory usage warning threshold in MB</td>
<td>224.0</td>
</tr>
<tr>
<td></td>
<td>–critical MEM_CRIT</td>
<td>Memory usage critical threshold in MB</td>
<td>256.0</td>
</tr>
<tr>
<td></td>
<td>–cert CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td></td>
<td>–key KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td></td>
<td>–capath CAPATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td></td>
<td>–help</td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–port PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td></td>
<td>–url URL</td>
<td>The status endpoint URL of the service, e.g.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–version</td>
<td>show program’s version number and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–timeout TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>–verbose</td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>

**nagios-plugins-argus.PEP.memory**

The response of the call executed by the status probe is parsed. The value for the current memory consumption is read out and displayed in the Status information field of the Nagios control panel and written into the Performance Data tab of Nagios. Hence it can be displayed as a graph over time by Nagios add-ons, e.g. pnp.
Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>--hostname=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>--warning=MEM_WARN</td>
<td>Memory usage warning threshold in MB</td>
<td>224.0</td>
</tr>
<tr>
<td>YES</td>
<td>--critical=MEM_CRIT</td>
<td>Memory usage critical threshold in MB</td>
<td>256.0</td>
</tr>
<tr>
<td>YES</td>
<td>--cert=CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td>YES</td>
<td>--key=KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td>YES</td>
<td>--capath=CAPATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td>YES</td>
<td>--help</td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>--port=PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td>YES</td>
<td>--url=URL</td>
<td>The status endpoint URL of the service, e.g.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="https://hostname:port/status">https://hostname:port/status</a></td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>--version</td>
<td>show program’s version number and exit</td>
<td></td>
</tr>
<tr>
<td>YES</td>
<td>--timeout=TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td>YES</td>
<td>--verbose</td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>

nagios-plugins-argus.PEP.traffic

The response of the call executed by the status probe is parsed. The value for the current number of requests executed and the number how many of them have been successful is read out and compared to the same numbers of the former test executed. Out of this the requests per second, the completed requests per second and the erroneous requests per second are computed and written into the Performance Data tab of Nagios. Hence it can be displayed as a graph over time by Nagios add-ons, e.g. pnp. Additionally the number of requests since the last test is written into the Status information field of the Nagios control panel.
Options

<table>
<thead>
<tr>
<th>Mandatory</th>
<th>CLI option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES</td>
<td>–hostname=HOSTNAME</td>
<td>The hostname of the service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–cert CERT</td>
<td>The SSL client certificate</td>
<td>/etc/grid-security/hostcert.pem</td>
</tr>
<tr>
<td></td>
<td>–key KEY</td>
<td>The private key (the key must be unencrypted)</td>
<td>/etc/grid-security/hostkey.pem</td>
</tr>
<tr>
<td></td>
<td>–capath CAPATH</td>
<td>The directory where trust anchors are stored on the system</td>
<td>/etc/grid-security/certificates</td>
</tr>
<tr>
<td></td>
<td>–tempdir=TEMP_DIR</td>
<td>Storage path for the needed temporary file</td>
<td>../../../../var/lib/grid-monitoring/nagios-plugins-argus</td>
</tr>
<tr>
<td></td>
<td>–tempfile=TEMP_FILE</td>
<td>Name for the needed temporary file</td>
<td>hostname.nagios-plugins-argus.PDP.traffic.pickle</td>
</tr>
<tr>
<td></td>
<td>–help</td>
<td>show this help message and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–port PORT</td>
<td>The port of the service</td>
<td>8152</td>
</tr>
<tr>
<td></td>
<td>–url URL</td>
<td>The status endpoint URL of the service, e.g.</td>
<td><a href="https://hostname:port/status">https://hostname:port/status</a></td>
</tr>
<tr>
<td></td>
<td>–version</td>
<td>show program’s version number and exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>–timeout TIMEOUT</td>
<td>The TCP timeout for the HTTPS connection in seconds</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>–verbose</td>
<td>verbose mode</td>
<td>False</td>
</tr>
</tbody>
</table>
This section contains a set of documentation allowing to set up a typical Argus installation without going in all the details contained in other sections.

8.1 Argus Quick Start: Site Policy Setup

8.1.1 Policy Basics

A site’s policies are maintained using the command `pap-admin`. Initially the PAP contains an empty policy for the site so no one will be permitted to do anything. The command

```
pap-admin list-policies
```

lists policies, in the *simplified policy language notation*, currently active in the PAP.

The policies you add will be evaluated from most to least recent and the first policy that matches is the result returned by Argus. So, if you added a policy that would deny a user and then added one that would permit the user the result of an authorization request will be permit since the permit policy is most recent. While not covered here, the exhaustive PAP command line interface *reference* provides information for how to re-order policies.

To begin, you will need to create permit policies, for individuals users, VOs, and FQANs, which reflect your site’s access policy. Each of the commands listed require a resource ID and action ID which are deployment and application specific, respectively. These ID were described in the *introduction* to the Argus system. For the purposes of this quick-start we’ll use `http://example.org` as the resource ID and `http://example.org/action` as the action ID. At this point you do not need to worry about what the correct values would be for a production deployment.

*Note:* As you change policies you will need to restart the PDP in order to force it to reread the policy from the PAP. It would do this by default but only after a couple of hours. Restarting forces it do this immediately.
**Permit by User**

Command:

```bash
pap-admin add-policy permit --resource "RESOURCE_ID" --action "ACTION_ID" dn="USER_DN"
```

The provided USER_DN must be in the RFC2253 standard form, not the proprietary format used by OpenSSL by default. To get the standard form of the DN you can use the command:

```bash
openssl x509 -noout -nameopt RFC2253 -subject -in CERT_PATH
```

Here’s an example that permits a user identified by their DN:

```bash
```

**Permit by VO**

Command:

```bash
pap-admin add-policy permit --resource "RESOURCE_ID" --action "ACTION_ID" vo="VO"
```

The name of a VO is the string that appears between, but no including, the first two forward slashes ('/') of an FQAN. Here’s an example that permits a user identified by their VO:

```bash
pap-admin add-policy permit --resource "http://example.org" --action "http://example.org/action" vo="atlas"
```

**Permit by Primary FQAN**

Command:

```bash
pap-admin add-policy permit --resource "RESOURCE_ID" --action "ACTION_ID" pfqan="FQAN"
```

The provided FQAN must be in full canonical (long) form (e.g. /atlas/Role=Production/Capability=NULL or /atlas/Role=NULL/Capability=NULL). You may use Java regular expression in this string.

Here’s an example that permits a user identified by their primary FQAN:

```bash
pap-admin add-policy permit --resource "http://example.org" --action "http://example.org/action" pfqan="/atlas/Role=Production/.*"
```

**Permit by Secondary FQAN**

Command:

```bash
pap-admin add-policy permit --resource "RESOURCE_ID" --action "ACTION_ID" fqan="FQAN"
```

The provided FQAN must be in full canonical (long) form (e.g. /atlas/Role=Production/Capability=NULL or /atlas/Role=NULL/Capability=NULL). You may use Java regular expression in this string.
Here’s an example that permits a user identified by their secondary FQAN:

```
pap-admin add-policy permit --resource "http://example.org" --action "http://example.org/action" pfqan="/atlas/higgs/Role=NULL/Capability=NULL"
```

### Explicit Banning

At times you may wish to deny a specific user, FQAN, or VO. As you may have guessed by looking at the commands above, you can create deny policies by changing the `permit` argument to `deny`.

Here are some examples:

```
pap-admin add-policy deny --resource "http://example.org" --action "http://example.org/action" pfqan="/atlas/higgs/Role=NULL/Capability=NULL"
pap-admin add-policy deny --resource "http://example.org" --action "http://example.org/action" vo="cms"
```

### Removing Policies

The command

```
pap-admin remove-policy POLICY_ID
```

will remove an existing policy from the PAP. The POLICY_ID is the ID for the policy shown by the command

```
pap-admin list-policies --show-all-ids
```

### 8.1.2 Loading and Testing Policies

Now that you have some basic policy commands you should experiment with creating and testing policies.

To test the policies you can use the command `pepcli`. This debugging tool can be used in two different ways. First you can supply it the certificate of a user or you can mock up a request by specifying a subject DN and primary and secondary FQANs. See the `pepcli documentation` for complete list of options or use the examples below.

This command provides the result that the user, represented by the given certificate, would receive:

```
```

The certificate may be an end-entity certificate, a plain proxy certificate, or a proxy certificate with VOMS extensions.

This command allows you to create a request containing a specific user DN, primary FQAN (the first one listed), and secondary FQANs (subsequent ones listed):

```
```

So, for example add a policy to allows people with the primary FQAN of `/atlas/higgs/Role=NULL/Capability=NULL` to be permitted using the following command

```
pap-admin add-policy permit --resource "http://example.org" --action "http://example.org/action" pfqan="/atlas/higgs/Role=NULL/Capability=NULL"
```
Then test the policy using the pepcli command

```
```

The result should be a permit.

### 8.1.3 Cleaning Up

Before you go further be sure to clean out of your test policies from the PAP. You do this by removing select policies as shown above or you may use the command

```
pap-admin remove-all-policies
```

to remove all policies from the PAP. Be sure to restart your PDP as well so that it picks up your new policy set.

**Note:** You are now done with this quick-start guide. At this point you should have a functioning Argus service and be able to add/remove basic policies from your site. It is recommended that you
Example of Authorization Requests and Policies

The following examples of policies and associated requests are meant to illustrate some of the possible policies, requests, and resulting authorization decisions.

Note, the examples below use the PAP’s simplified policy language to express policies. So please review this syntax, before proceeding, if you are not yet familiar with it.

9.1 User Based Authorization

In this example one user is permitted, and one is denied, the ability to submit jobs on the CERN CE resource. Each user is identified by a X.509 subject DN. This example also shows how identity-based access control is simply a degenerate case of attribute-based access control.

9.1.1 Authorization Policy

```plaintext
resource "http://cern.ch/authz/ce1" {
  action "http://cern.ch/authz/actions/ce-submit" {
    rule permit {
      subject="CN=John Doe,OU=Standard Commercial Certificate,O=Acme,L=Zuerich,ST=Zuerich,C=CH"
    }
    rule deny {
      subject="CN=Jane Smith,OU=Standard Commercial Certificate,O=Acme,L=Zuerich,ST=Zuerich,C=CH"
    }
  }
}
```

9.1.2 Requests

A request of:
• resource attributes:
  – any other attributes
• action attributes:
  – any other attributes
• subject attributes:

would result in an authorization decision of permit because the given resource and actions IDs match what was given in the policy and the subject ID DN matches what was given in the permit rule. If the request contained any other resource, action, or subject attribute these would be ignored since the policy does not reference them. If the request had not contained the attributes listed it would have resulted in an authorization decision of not applicable since no policy would have matched the request.

A request of:
• resource attributes:
  – any other attributes
• action attributes:
  – any other attributes
• subject attributes:

would result in an authorization decision of deny since the resource and action IDs match and this time the subject ID matches the requirement for the deny rule.

Note, in the second request, if the subject ID had contained at least the values CN=John Doe, OU=Standard Commercial Certificate, O=Acme, L=Zuerich, ST=Zuerich, C=CH and CN=Jane Smith, OU=Standard Commercial Certificate, O=Acme, L=Zuerich, ST=Zuerich, C=CH the authorization decision would have been permit since the permit rule would have been evaluated first and would have returned the result.

### 9.2 Per-VO Pilot Job Authorization Policy

This example shows a policy that allows pilot jobs from one VO, atlas, and denies pilot jobs from others. It also demonstrates rules that rely on more than one attribute.

---

**Chapter 9. Example of Authorization Requests and Policies**

108
9.2.1 Authorization Policy

```xml
resource "http://cern.ch/authz/ce1" {
  action "http://cern.ch/authz/actions/ce-submit" {
    rule permit {
      vo="atlas"
      pilot-job="true"
    }
    rule deny {
      pilot-job="true"
    }
  }
}
```

9.2.2 Requests

A request of:

- **resource attributes:**
  - id: urn:oasis:names:tc:xacml:1.0:resource:resource-id, **value:** http://cern.ch/authz/ce1
  - any other attributes

- **action attributes:**
  - id: urn:oasis:names:tc:xacml:1.0:action:action-id, **value:** http://cern.ch/authz/actions/ce-submit
  - any other attributes

- **subject attributes:**
  - id: http://authz-interop.org/xacml/subject/vo, **value:** atlas
  - id: http://example.org/authz/attribute/pilot-job, **value:** true

would result in a decision of **permit** since the atlas VO is permitted to submit pilot jobs. A request where the VO was lhcb or cms would result in a decision of **deny** since these VOs are not permitted to submit jobs.

A request of: * resource attributes:

- **id:** urn:oasis:names:tc:xacml:1.0:resource:resource-id, **value:** http://cern.ch/authz/ce1
- any other attributes

- **action attributes:**
  - **id:** urn:oasis:names:tc:xacml:1.0:action:action-id, **value:** http://cern.ch/authz/actions/ce-submit
- any other attributes

- **subject attributes:**
  - **id:** http://authz-interop.org/xacml/subject/vo, **value:** atlas

would result in a decision of **not applicable** since the current policy indicates that only jobs from the VO atlas that are also pilot jobs are permitted. Requests without a pilot-job attribute are not addressed by this policy.
10.1 Definitions

PAP  The Policy Administration Point manages and publishes the authorization policies.
PDP  The Policy Decision Point evaluates the authorization requests.
PEP Server  The Policy Enforcement Point server processes the PEP clients requests and responses.
PEP client  Lightweight PEP client library available for Java and C. Enforces the authorization decision locally.

10.2 Service Reference Card

Functional description:  Render authorization decisions based on XACML policies: “Can user X performs action Y on resource Z ?” or “Is user X banned for any action on any resource ?”

Services running:

- PAP: (Java application) org.glite.authz.pap.server.standalone.PAPServer
- PDP: (Java application) org.glite.authz.pdp.server.PDPDaemon
- PEP Server: (Java application) org.glite.authz.pep.server.PEPDaemon

Init scripts and options:

- PAP: systemctl {start|stop|restart|status} argus-pap or service argus-pap {start|stop|restart|status}
- PDP: systemctl {start|stop|restart|status} argus-pdp or service argus-pdp {start|stop|restart|status}
- PEP Server: systemctl {start|stop|restart|status} argus-pepd or service argus-pepd {start|stop|restart|status}

Configuration files location with example:
• **PAP:**
  - *Config directory:* /etc/argus/pap
  - *Config files:* pap_configuration.ini and pap_authorization.ini

• **PDP:**
  - *Config directory:* /etc/argus/pdp
  - *Config file:* pdp.ini

• **PEP Server:**
  - *Config directory:* /etc/argus/pepd
  - *Config file:* pepd.ini

**Logfile locations (and management) and other useful audit information:**

• **PAP:**
  - *Logging directory:* /var/log/argus/pap
  - *Logging configuration:* /etc/argus/pap/logging/standalone/logback.xml
  - *Example:* PAP logback.xml
  - *Status handler:* https://HOSTNAME:8150/pap/status

• **PDP:**
  - *Logging directory:* /var/log/argus/pdp
  - *Logging configuration:* /etc/argus/pdp/logging.xml
  - *Example:* PDP logging.xml
  - *Status handler:* https://HOSTNAME:8152/status

• **PEP Server:**
  - *Logging directory:* /var/log/argus/pepd
  - *Logging configuration:* /etc/argus/pepd/logging.xml
  - *Example:* PEP logging.xml
  - *Status handler:* https://HOSTNAME:8154/status

**Open ports:**

• **PAP:**
  - *Service port:* *:8150
  - *Admin port:* localhost:8151

• **PDP:**
  - *Service port:* *:8152
  - *Admin port:* localhost:8153

• **PEP Server:**
  - *Service port:* *:8154
  - *Admin port:* localhost:8155
Possible unit test of the service: Nagios probes are available to monitor the services, see *Nagios Probes for Argus (UMD)*.

Where is service state held (and can it be rebuilt): The services (PAP, PDP, PEP Server) are stateless. However:

- **PAP**: The XACML policies are stored locally in the `/usr/share/argus/pap/repository` directory.
- **PEP Server**: The user pool account mapping leases are kept in the `/etc/grid-security/gridmapdir` directory.

Cron jobs: None

Security information

- **Access control mechanism (authentication & authorization):**
  - Authentication: SSL/TLS client authentication on the service ports
  - Authorization: PAP uses access control list

- How to block/ban a user
- Network Usage
- Firewall configuration
- Security recommendations
- Security incompatibilities
- List of externals (packages are NOT maintained by Red Hat)
- Other security relevant comments

Utility scripts:

- `pap-admin` CLI to manage the PAP policies
- `pdpctl {reloadPolicy|version|status}` forces the PDP to reload the policies from the PAP, print version, print status
- `pepdctl {clearResponseCache|version|status}` clears the PEP daemon response cache, print version, print status

Location of reference documentation for users: Not applicable

Location of reference documentation for administrators:

- **General documentation**: Argus Authorization Service
- **PAP admin CLI**: Argus Policy Administration Point (PAP): Administration
- **Simplified Policy Language**: The Simplified Policy Language
Argus Service Deployment for 1.7 version

11.1 Requirements

11.1.1 Platform

The supported platforms are:

- **EL6/x86_64** with the EPEL and UMD3 repositories **enabled**.
- **EL7/x86_64** with the EPEL, CERN WLCG and UMD4 repositories **enabled**.

11.1.2 Host Certificate

The Argus services require a valid host certificate. The key pair is typically installed in `/etc/grid-security/hostcert.pem` and `/etc/grid-security/hostkey.pem`

11.2 Installation with YUM

The Argus Authorization Service is a bundle of 3 services (the PAP, PDP and PEP Server). Packages for the three services can be easily installed on a given machine by installing the `argus-authz` metapackage, as in the following command:

```
yum install argus-authz
```
11.2.1 Install the EGI IGTF Bundle

If not already present on your host, install the EGI IGTF trust anchors. More information available online: https://wiki.egi.eu/wiki/EGI_IGTF_Release

- Install the EGI IGTF trust anchors with YUM

11.2.2 Verify fetch-crl

The Argus metapackage install the fetch-crl cron job; run it once, and verify that the cron job is enabled and started:

```bash
# run it immediately (it can take some time...)
fetch-crl

# enable the periodic fetch-crl cron job
chkconfig fetch-crl-cron on
service fetch-crl-cron start
```

For EL7 system, enable fetch-crl cron job with:

```
systemctl start fetch-crl-cron
systemctl enable fetch-crl-cron
```

11.2.3 Install the Argus Metapackage

The argus-authz metapackage bundles the 3 Argus services: PAP, PDP and PEP Server

Therefore, the argus-authz metapackage is the simplest way to install the Argus Authorization Services (PAP, PDP and PEP Server) on your host.

Use YUM to install the Argus metapackage: `yum install argus-authz`

At this point all 3 Argus services (PAP, PDP and PEP server) are installed on your host. You must now continue with the Argus service configuration with YAIM.

11.3 Update with YUM

Argus and its components are packages in the UMD repositories, and therefore automatically updated if a new version is available and `yum update` is executed. The updating process however is stopping the Argus services (PAP, PEPd and PDP). To get Argus back to work after an update it is recommended to restart the services.

**Warning:** Please make sure that your system does not use the automated yum updating service, since this may lead to a stopped Argus server in case of a unnoticed update.

11.4 Configuration

- Version 1.7: *manual configuration*.
- Older version: *Configuration with YAIM*.
A set of Nagios probes for Argus (EMI-2 and EMI-3) are available to monitor the Argus PAP, PDP and PEP Server:

- Argus Nagios Probes Documentation (EMI): *Nagios Probes for Argus (UMD)*
EMIR Publisher for Argus 1.6 (EMI-3)

You can use EMIR-SERP to publish the Argus resource information to EMIR. EMIR-SERP uses the information already available in the resource BDII and publish it to an EMIR DSR endpoint.

- See the Argus EMIR Configuration to publish the Argus into EMIR: Argus EMIR Publisher Configuration (EMI-3)
In the 1.7 version, there are no known issues. For older versions, see Known Issues for older version.
This guide shows how to configure Argus with a basic setup. Basically configuration consist in:

- set service host name in configuration files;
- set service endpoints
- set certificates path;

### 15.1 Requirements

First, verify that the operating system has Java 1.8 as default JVM:

```bash
$ java -version
openjdk version "1.8.0_77"
```

If the command above shows an older JVM version, change the system configuration with

```bash
alternatives --config java
```

### 15.2 PAP

**/etc/argus/pap/pap-admin.properties**

1. Set **host** variable with the machine host name.

**/etc/argus/pap/pap_configuration.ini**

1. Set **entity_id**.
2. Set **hostname** with server host name.
3. Set **certificate** with the absolute path of the X509 certificate of the server.
4. Set `private_key` with the absolute path of the X509 private key of the server.

`/etc/argus/pap/pap_authorization.ini` Keep default values for basic setup.

`/etc/sysconfig/argus-pap` Keep default values for basic setup.

More details about PAP configuration can be found in *PAP configuration*.

### 15.3 PDP

`/etc/argus/pdp/pdp.ini`

1. Set `entity_id`.
2. Set `hostname` with server host name.
3. Set `paps` with PAP endpoint; one or more PAP endpoints can be specified in a space separated list.
4. Set `serviceCertificate` with the absolute path of the X509 certificate of the server.
5. Set `servicePrivateKey` with the absolute path of the X509 private key of the server.
6. Set `trustInfoDir` with the absolute path of the trusted CAs.

`/etc/sysconfig/argus-pdp` Keep default values.

More details about PDP configuration can be found in *PDP configuration*.

### 15.4 PEP

`/etc/argus/pepd/pepd.ini`

1. Set `entity_id`.
2. Set `hostname` with server host name.
3. Set `pdps` with PDP endpoint; one or more PDP endpoints can be specified in a space separated list.
4. Set `serviceCertificate` with the absolute path of the X509 certificate of the server.
5. Set `servicePrivateKey` with the absolute path of the X509 private key of the server.
6. Set `trustInfoDir` with the absolute path of the trusted CAs.
7. Set `vomsInfoDir` with the absolute path of the VOMS directory.

`/etc/sysconfig/argus-pepd` Keep default values.

More details about PEP configuration can be found in *PEP configuration*.

### 15.5 Grid Mapping

Ensure that following Grid mapping file are present:

`/etc/grid-security/grid-mapfile:` This file contains mapping between Grid users and local pool account

`/etc/grid-security/groupmapfile:` This file contains mapping between Grid users and local Unix groups.

Moreover, ensure there is present the directory:

`/etc/grid-security/gridmapdir:` This directory contains pool accounts and users linked to them.
More information about the syntax can be found in Argus Grip Map File Syntax.

15.6 VOMS configuration

Ensure that following files are present:

/etc/grid-security/voms-grid-mapfile This file contains mapping between Grid users and local pool account, similar to grid-mapfile described above.

Ensure that following directory are present:

/etc/grid-security/vomsdir This directory contains a sub-directory for each supported VOs. In each of this sub-directory there is a .lsc, a file that contains a description of the certificate chain of the certificate used by a VOMS server to sign VOMS attributes.

For example for the some test VO, the directory structure is:

```
vomsdir/
    └── testers.eu-emi.eu
        └── emitestbed07.cnaf.infn.it.lsc
    └── test.vo
        └── vgrid02.cnaf.infn.it.lsc
        └── test.vo.2
            └── vgrid02.cnaf.infn.it.lsc
```

The content for the test.vo.lsc file is:

```
/C=IT/O=INFN/OU=Host/L=CNAF/CN=vgrid02.cnaf.infn.it
/C=IT/O=INFN/CN=INFN Certification Authority
```

More information about VOMS can be found in VOMS client documentation.

15.7 Restart services

Restart Argus services to enable the new configuration.

In EL6-based systems, run this command:

```
for srv in argus-pap argus-pdp argus-pepd; do service $srv restart; done
```

In EL7-based systems, run:

```
systemctl restart argus-pap argus-pdp argus-pepd
```

More details about service management can be found in PAP operations, PDP operations and PEP operation.

15.8 BDII configuration

Install BDII packages:

```
yum install bdii glite-info-provider-service
```

Move into directory /etc/glite/info/service and from the provided templates, create the files:
The provided templates contains a default configuration: for a basic setup, rename the files striping the extension .template.

Into the directory /var/lib/bdii/gip/provider create a shell script, for example named glite-info-glue2-provider-service-argus, with the content:

```bash
#!/bin/sh
#
# Argus services GLUE 2 info provider
#
CONF_DIR=/etc/glite/info/service
/usr/bin/glite-info-glue2-multi \  
   $CONF_DIR/glite-info-glue2-argus-pap.conf,$CONF_DIR/glite-info-glue2-argus-pdp.conf \  
   argus-site $CONF_DIR/glite-info-glue2-service-argus.conf
```

Ensure that this file is owned by the user ldap and that it is readable and executable:

```bash
chown ldap:ldap glite-info-glue2-provider-service-argus
chmod 0755 glite-info-glue2-provider-service-argus
```

Restart the BDII service:

```bash
systemctl restart bdii
```
CHAPTER 16

Configuration with YAIM

Warning: As of UMD 4.0, and in particular on CENTOS 7 YAIM is no longer supported to configure Argus.

The ARGUS_server node type is available to configure the Argus service with YAIM.

16.1 Argus YAIM Configuration Variables

Description of all the available Argus YAIM configuration variables: Argus YAIM Configuration for EMI

16.2 Mandatory YAIM Variables

- ARGUS_HOST Fully qualified host name (FQHN) of the Argus host
- PAP_ADMIN_DN Certificate distinguished name (DN) of the administrator, allowed to use the pap-admin command
- SITE_NAME BDII site name
- USERS_CONF Absolute location of the users configuration file
- GROUPS_CONF Absolute location of the groups configuration file
- VOS List of supported VO names
- VO_<vo-name>_VOMS_CA_DN VOMS CA DN for each VO name listed in VOS
- VO_<vo-name>_VOMSES VOMS definition for each VO name listed in VOS

The USERS_CONF and GROUPS_CONF configuration files MUST be the same on the Argus host as on the client host (CREAM, WMS, gLExec, ...). On successful authorization, the Argus PEP Server is configured to determine the user/group mapping (pool account) for this authorization and send it the client. Therefore, the client must be able to map the resulting user mapping received with the authorization decision.
16.3 Argus site-info.def Configuration

Your site-info.def for Argus must contain at least the following variable:

```
# BDII site name
SITE_NAME=MySiteName

# Argus service hostname
ARGUS_HOST=argus.example.org

# PAP administrator DN allowed to use 'pap-admin' command
PAP_ADMIN_DN="/DC=org/DC=acme/CN=John Doe"

# Users and Groups definition for grid and group mapfile
USERS_CONF=/opt/glite/yaim/examples/users.conf
GROUPS_CONF=/opt/glite/yaim/examples/groups.conf

# Supported VOs
VOS="dteam"

VO_DTEAM_VOMSES="'dteam voms.hellasgrid.gr 15004 /C=GR/O=HellasGrid/OU=hellasgrid.gr/CN=voms.hellasgrid.gr dteam' 'dteam voms2.hellasgrid.gr 15004 /C=GR/O=HellasGrid/OU=hellasgrid.gr/CN=voms2.hellasgrid.gr dteam'"

```

See the documentation of all the supported Argus YAIM configuration variables: Argus YAIM Configuration for EMI.

16.4 Generate Argus Configuration

Run YAIM to generate the Argus configuration for your site:

```
/opt/glite/yaim/bin/yaim -c -s site-info.def -n ARGUS_server
```

At this point, the Argus services (PAP, PDP and PEP Server) must be configured, up and running.
CHAPTER 17

Authorization Service: Grid Map File Syntax

17.1 Description

Grid Map files are used to express a mapping from subject attributes in to a local account.

17.2 File Syntax

Each line of a grid map file is either pure whitespace, a comment, or a mapping.

Comments begin with a number or hash sign (#), may be followed with any character and ends at the end of the line. The following is an example of grid map file which contains only a single comment.

```
# This is a map file with a single comment
```

A mapping line consists of two parts, the first is a key that identifies the subject that will be mapped. This part is always enclosed in double quotes ("). The second part is the comma-separated list of targets to which the subject may be mapped. The first and second parts of the map line are separated by any number of spaces or tabs. The following is an example of a grid map file mapping an FQAN to an account.

```
"/vo/atlas/analysis" .atlas
```

17.3 Subject Keys

The subject key, the first component of a mapping line, may be either an X.509 DN or a Fully Qualified Attribute Name (FQAN).

If an X.509 DN is used it may be either in the non-standard grid form (where each component is separated by a forward slash (/) and the CN comes last), or the standard RFC2253 format (where components are separated by a comma (',') and the CN comes first). The RFC2253 format is preferred. Both formats may be used within a single file and in both case the following escape sequences may be used:
<table>
<thead>
<tr>
<th>Escape Sequence</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\'</code></td>
<td>a single quote</td>
</tr>
<tr>
<td><code>\&quot;</code></td>
<td>a double quote</td>
</tr>
<tr>
<td><code>\\</code></td>
<td>a backwards slash</td>
</tr>
<tr>
<td><code>\/</code></td>
<td>a forward slash</td>
</tr>
<tr>
<td><code>\f</code></td>
<td>a formfeed</td>
</tr>
<tr>
<td><code>\n</code></td>
<td>a new line</td>
</tr>
<tr>
<td><code>\r</code></td>
<td>a carriage return</td>
</tr>
<tr>
<td><code>\t</code></td>
<td>a horizontal tab</td>
</tr>
<tr>
<td><code>\x##</code></td>
<td>the ASCII character corresponding to the given hexadecimal digits</td>
</tr>
<tr>
<td><code>\u####</code></td>
<td>the UTF-8 character corresponding to the given hexadecimal digits</td>
</tr>
</tbody>
</table>

## 17.4 Map Targets

The map target, the second component of a mapping line, is a comma separated list of either an account or group names.

A map target prefixed with a dot . represents a pool account.
CHAPTER 18

Argus YAIM Configuration for EMI

**Warning:** As of UMD 4.0, and in particular on CENTOS 7, YAIM is no longer supported to configure Argus. This page is kept for reference only.

18.1 YAIM Configuration for ARGUS_server

18.1.1 Mandatory General Variables

- **SITE_NAME** BDII site name
- **USERS_CONF**
- **GROUPS_CONF**
- **VOS** List of supported VO names
- **VO_<vo-name>_VOMS_CA_DN** VOMS CA DN for each VO name listed in VOS
- **VO_<vo-name>_VOMSES** VOMS definition for each VO name listed in VOS

More information on these variables available here: https://twiki.cern.ch/twiki/bin/view/LCG/Site-info_configuration_variables

18.1.2 Mandatory Service Specific Variables

They can be found in /opt/glite/yaim/examples/siteinfo/services/glite-argus_server
18.1.3 Default Service Specific Variables

They can be found in /opt/glite/yaim/defaults/glite-argus_server(.pre|.post)
19.1 Timeouts for certificates from CAs that use OCSP

As of late 2013 a few CAs (e.g. the CERN CA) have started using the Online Certificate Status Protocol (OCSP) in addition to the CRL mechanism to advertise which certificates have been revoked. Some security libraries will then by default contact the OCSP responder of the CA in real time when a certificate from such a CA needs to be validated. If that outgoing traffic happens to be blocked, or if the responder is slow or even unreachable, the operation will eventually time out (see GGUS:105666). Depending on the case at hand, such a timeout need not be a fatal error in itself, but will at least slow down operations and may therefore cause timeouts downstream (e.g. for CREAM or gLExec).

19.1.1 Workaround

In EGI and WLCG we do not need OCSP to work at this time, as the CRL mechanism is still deemed sufficient. Therefore it is reasonable to disable OCSP for the time being and version 1.4.1 of the argus-pdp-pep-common rpm does that by default. That version was officially released in Argus v1.6.3 as part of EMI-3 Update 27 (2015-06-10).

19.2 Performance issue with Argus PEP Server (EMI-2, EMI-3, all versions)

After a large number of authorization requests, the PDP responses caching mechanism in the PEP Server becomes unstable and the performance of the service deteriorates. It is recommended to completely disable the PDP responses caching mechanism in the Argus PEP Server.

Additionally, the default memory settings for the Argus PEP Server could be too low for production site. It is recommended to allocate at least 1GB memory.
19.2.1 Workaround

Disabling the caching mechanism

Completely disabling the PDP responses caching mechanism in the PEP Server configuration solves the performance issue. To disable the cache:

1. edit the /etc/argus/pepd/pepd.ini file
2. add the parameter maximumCachedResponses = 0 in the [PDP] section (see example)
3. restart PEP Server: /etc/init.d/argus-pepd restart (or increase the memory settings, then restart)

Example:

```
[PDP]
pdps = https://chaos.switch.ch:8152/authz
# disabling the cache
maximumCachedResponses = 0
```

Increasing the default memory

Allocating 1GB of memory for the Argus PEP Server solves the performance issue. To increase the default memory:

1. edit the /etc/sysconfig/argus-pepd file
2. set the line PEPD_JOPTS="-Xmx1024M"
3. restart PEP Server: /etc/init.d/argus-pepd restart

19.3 Problem the EMI-3 update and Argus PEP Server v.1.6.1

Updating the Argus PEP Server to the last EMI-3 update (argus-pep-server-1.6.1) will not always restart the Argus PEP Server

19.3.1 Workaround

After the update (yum update), restart the Argus PEP Server by hand:

```
root# /sbin/service argus-pepd restart
```

19.4 Problem with Argus 1.6 (EMI-3) and fetch-crl

The Argus metapackage emi-argus have no dependency on the fetch-crl cron job. Installing and starting the Argus services, without having fetch-crl installed, will cause SSL errors when trying to connect to the services.

19.4.1 Workaround

Prior to installing the emi-argus metapackage, install the the fetch-crl package by hand, and run it at least once:

```
root# yum install fetch-crl
root# fetch-crl -v
```
If you have already installed and configured Argus, just install the `fetch-crl` package by hand, run it at least once, and restart the Argus services:

```bash
root# yum install fetch-crl
root# fetch-crl -v
root# service argus-pap restart
root# service argus-pdp restart
root# service argus-pepd restart
```

19.5 Problem with Nagios plugins for Argus and TMP directory permission

The `nagios-plugins-argus` package do not set the correct ownership for the `/var/lib/grid-monitoring/nagios-plugins-argus` temp directory. The plugins will throw errors (Permission denied) because the ownership of the directory is not `nagios`.

19.5.1 Workaround

To fix the temp directory ownership to `nagios`, please do:

```bash
root# yum install nagios-plugins-argus
root# chown -R nagios:nagios /var/lib/grid-monitoring/nagios-plugins-argus
```

19.6 Problem with Argus 1.5 (EMI-2) and CREAM

Under heavy load the Argus PEP Server (v1.5.1) does not always return a user mapping for a permitted operation, causing CREAM to throw an error and abort the job. This typically occurs for 10% of the jobs submitted by CREAM.

19.6.1 Workaround

Disabling the PDP responses caching mechanism in the PEP Server configuration solve this issue. To disable the cache:

1. edit `/etc/argus/pepd/pepd.ini`
2. add the parameter `maximumCachedResponses = 0` in the `[PDP]` section (see example below)
3. restart PEP Server: `/etc/init.d/argus-pepd restart`

Example:

```ini
[PDP]
pdfs = https://chaos.switch.ch:8152/authz
# disabling the cache
maximumCachedResponses = 0
```
19.7 Problem with upgrade from Argus 1.4 (EMI-1) to Argus 1.5 (EMI-2)

When upgrading an previous Argus 1.4 (EMI-1) installation on SL5, you need to re-install Argus 1.5 (EMI-2). This is due to an error in the Argus 1.4 post uninstall script.

19.7.1 Workaround

Simply reinstalling the components with YUM just after the upgrade solves the issue:

```bash
yum upgrade
(argus is upgraded...)
yum reinstall argus-pap argus-pdp argus-pep-server
```
Warning: The pages below have been converted to the new documentation format without any specific review. They are coming from the former Argus and are probably obsolete. They are kept here for reference only.

20.1 Argus EMIR Publisher Configuration (EMI-3)

You can use EMIR-SERP to publish the Argus resource information to the EMIR registry. EMIR-SERP uses the information already available in the resource BDII and publish it to an EMIR DSR endpoint.

20.1.1 Local Resource BDII

Check that the local resource BDII is running and return service information:

```
ldapsearch -x -h localhost -p 2170 -b 'GLUE2GroupID=resource,o=glue' -objectClass=GLUE2Service
```

This query should return 1 entry for the Argus service. If it is not the case, something is fishy in the installation...

20.1.2 Install and Configure EMIR SERP

Install the EMIR SERP package:

```
yum install emir-serp
```

Edit the configuration file `/etc/emi/emir-serp/emir-serp.ini` and set the following:

```
... url = http://emitbdsr1.cern.ch:9126 ...
```

(continues on next page)
And start the EMIR-SERP service:

```
/sbin/service emir-serp start
```

You can verify that the information is correctly published by browsing: http://emitbdsr1.cern.ch:9126/services

## 20.2 Argus Services Fine Tuning

### 20.2.1 Optimizing Argus Memory Usage

The Argus 1.3 services (PAP, PDP and PEP Server) don’t have fine tuned memory limits. For production sites it is therefore recommended to manually set a memory limit for each service.

**NOTICE:** Starting with Argus 1.4, the memory limits are already set, but you can adapt them for your special need.

**Argus PAP Memory**

In the PAP, the memory usage of the PAP depends directly on the number of policies.

- Default memory limit: 512 MB (v.1.4), 256MB (v.1.5)
  - No default memory limit set for version lower than v.1.4
- The default memory limit is typically enough for:
  - ~2'000 policies (resource - action - obligation - rule)
  - ~20'000 rules in one policy (~20'000 DN’s or FQAN’s)

**PAP Memory Setting for Production**

For production sites, which typically have less than 500 policies, we recommend to set the PAP memory limit to 256 MB

- **Recommended** memory limit (assuming less than 500 policies): 256 MB
- The value can be changed by setting the variable `PAP_JAVA_OPTS=-Xmx256m` in the `/etc/sysconfig/argus-pap` configuration file

You have to restart the Argus PAP service to apply the new memory limit settings.

**Argus PDP Memory**

The PDP memory usage depends on the number of policies it has to import from the PAP.

- Default memory limit: 256 MB (v.1.4)
  - No default memory limit set for version lower than v.1.4
- The needed memory is comparable with the memory needed by the PAP
PDP Memory Setting for Production

For production sites, it is highly recommended to set a memory limit, to avoid a growing of the used memory (up to 1 GB) by the PDP.

- **Recommended** memory limit (assuming less than 500 policies in the PAP): 256 MB
- The value can be changed by setting the variable `PDP_JOPTS="-Xmx256M"` in the `/etc/sysconfig/argus-pdp` configuration file

You have to restart the Argus PDP service to apply the new memory limit settings.

Argus PEP Server Memory

The PEP Server memory usage depends on the cache-size.

- Default memory limit: 512MB (v.1.3.1) and 128MB (v.1.4), and 256MB (v.1.5)
  - No default memory limit set for version lower than v.1.3.1
- Default value for the cache size: max. 500 cached PDP responses

The value for the cache size (`maximumCachedResponses`) can be changed following the PEP Server Configuration documentation.

PEP Server Memory Setting for Production

The default memory limit set for the PEP Server v1.3.1 is still rather high. It can safely be lowered without any degradation of performance, and as long as the cache-size is not increased. For PEP Server version lower than v1.3.1, it is highly recommended to set a memory limit, to avoid a growing of the used memory (up to 1 GB).

- **Recommended** memory limit: 256 MB
  - The previous memory limit of 128MB in Argus 1.4.0 was too low for site with a lot of pool accounts.
- The value can be changed by setting the variable `PEPD_JOPTS="-Xmx256M"` in the `/etc/sysconfig/argus-pepd` configuration file

You have to restart the Argus PEP Server service to apply the new memory limit settings.

20.2.2 Production Logging Settings

By default the Argus 1.3 (EMI-1) services don’t have production specific logging configuration, therefore, for production sites it is recommended to manually configure the logging for each service.

**NOTICE:** Starting with Argus 1.4, the services already use these production logging configuration.

For production sites, we have define the following logging policy:

- Log files rotation:
  - daily rotating (at midnight)
  - or when the file size >= 100MB
- Rotated log files are gzipped
- History of log files keep for 90 days

The Argus services uses the Logback Logging Framework to do their logging. The logback framework can be configured to implement the production logging policy.
Argus PAP Logging

The Argus PAP service logging configuration is configured with the `/etc/argus/pap/logging/standalone/logback.xml` file.

**PAP Logging Configuration for Production**

To configure the Argus PAP service for production logging, please download the attached configuration file and store it as `/etc/argus/pap/logging/standalone/logback.xml`.

You have to restart the PAP service to apply the new logging configuration.

Argus PDP Logging

The Argus PDP service logging configuration is configured with the `/etc/argus/pdp/logging.xml` file.

**PDP Logging Configuration for Production**

To configure the Argus PDP service for production logging, please download the attached configuration file and store it as `/etc/argus/pdp/logging.xml`.

The PDP will automatically reload its logging configuration, no need to restart the service.

Argus PEP Server Logging

The Argus PEP Server service logging configuration is configured with the `/etc/argus/pepd/logging.xml` file.

**PEP Server Logging Configuration for Production**

To configure the Argus PEP Server service for production logging, please download the attached configuration file and store it as `/etc/argus/pepd/logging.xml`.

The PEP Server will automatically reload its logging configuration, no need to restart the service.

### 20.3 Argus Development Tools

The tools used by the Argus PT to develop the Argus Authorization Service

#### 20.3.1 Development

- GitHub for the version control of all Argus components ([https://github.com/argus-authz](https://github.com/argus-authz))

#### 20.3.2 Build

- Maven for the compilation of the main Java components ([http://maven.apache.org/](http://maven.apache.org/))
- ANT for the compilation of the PEP Java client library ([http://ant.apache.org/](http://ant.apache.org/))
- Autotools, configure and make for the compilation of the C components
20.3.3 Test

- JUnit for some of the Java components
- Grinder for the internal load and stress testing of the server components (http://grinder.sourceforge.net/)

20.3.4 QA

- GGUS for users support (http://www.ggus.org)
- LCG Savannah for bugs, tasks and patches tracking (https://savannah.cern.ch)
- A code review was done by the PSNC Security Team, but we don’t have enough resource within the Argus PT to do it ourselves
- CERN vNode test bed using the automatic YAIM-gen for product certification

20.3.5 Infrastructure and Repository

- Some virtual machines for internal testing
- CERN YUM repository for deployment
- YAIM for the glite-ARGUS node configuration

20.4 GGUS User Support for Argus

20.4.1 Argus Support Unit FAQ

1801 What is the purpose of the Argus Support?

Provide support for site administrators on the installation, the configuration and the operation of the Argus Authorization Service.

1802 Who is responsible for Argus Support?

Argus product team (PT) members.

1803 How does a ticket arrive at Argus Support?

Currently through the existing argus-support@cern.ch mailing list.

1804 What does the Argus Support manager have to do?

Dispatch support request.
1805 What does the person dealing with Argus Support have to do?

- Try to solve the problem with the user.
- If necessary, submit a bug in savannah.
- If relevant, update our FAQ with problem and solution.

1806 What documentation is available on Argus Support?

Extensive documentation is available at https://twiki.cern.ch/twiki/bin/view/EGEE/AuthorizationFramework

20.5 Authorization Service: Load and Lifetime Testing

It is important to perform load and lifetime tests on any service being put in to production. Load tests are used to determine how the service behaves, and eventually fails, under load while lifetime tests determine how the service behaves over a prolonged period of time with average load.

Note, this testing framework used here was actually developed by the Shibboleth team for testing their software but it allows other test packs to be installed so it can also be used in testing this service.

20.5.1 Testing Framework Basics

Requirements

- Unix OS based machine(s)
- Subversion client (necessary in order to download the framework)
- Java 1.5

Downloading and Installing the Framework

1. Checkout the base testing framework. The resulting grinder-framework directory will be known a GF_HOME throughout the rest of this document.

   - `svn co https://svn.middleware.georgetown.edu/shib-extension/java-loadtest/trunk/grinder-framework grinder-framework`

2. Within _GF_HOME/test checkout the Argus test packs

   - `svn co http://svnweb.cern.ch/guest/glxa/loadtests/pepcli-authz pepcli-authz`
   - `svn co http://svnweb.cern.ch/guest/glxa/loadtests/pepcli-multiauthz pepcli-multiauthz`
   - `svn co http://svnweb.cern.ch/guest/glxa/loadtests/pepj-authz pepj-authz`

Installation is now complete.
Running the Framework

The load testing framework is composed of two parts, an agent and a console. The agent performs the actual work while the console, a GUI application, collects the results from agents and displays some metrics based on those results.

To run the console execute the `GF_HOME/bin/console.sh` command. This will start the console which will listen on port 6372 for agent results. Be sure that this port is accessible to the agents you start.

To run the console execute the `GF_HOME/bin/agent.sh test_name` command. The name of the test is dependent on which test you will run and is given in the documentation for those tests. You can install agents on more than one machine and have them report back to a single client. This is useful if one agent machine is not capable of generating enough load.

Common Configuration Options

Each test package contains a `test.properties` file that contains configuration information for the given test. The later half of these options are Grinder specific properties. In most cases you'll need to change the following properties.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>grinder.consoleHost</td>
<td>The IP address of the machine on which the console is running</td>
</tr>
<tr>
<td>grinder.processes</td>
<td>Number of grinder processes to run. Should be equal to the number of CPU cores on the agent machine.</td>
</tr>
<tr>
<td>grinder.threads</td>
<td>Number of unique clients, per process, that will connect to the service</td>
</tr>
<tr>
<td>grinder.runs</td>
<td>Number of times each client will connect to the service, 0 (zero) means to keep going until the console indicates the test should be stopped. Using a value of 1 (one) is useful for testing that your configuration is correct.</td>
</tr>
</tbody>
</table>

20.5.2 PEPCLI Test

This test uses the C language PEP CLI to issue basic authorization requests. It a good test to run if you are trying get measurements for applications which do not maintain state between requests (e.g. a new client is created for every request).

Test Name: pepcli-authz
## Configuration Options

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>pepcli.bin</td>
<td>The path to the pepcli binary.</td>
<td>Yes</td>
</tr>
<tr>
<td>pepcli.pepds</td>
<td>A space separated list of PEPd endpoints</td>
<td>Yes</td>
</tr>
<tr>
<td>pepcli.certchain</td>
<td>Path, relative to GF_HOME, to the certchain used to identify the subject or the request</td>
<td>Yes</td>
</tr>
<tr>
<td>pepcli.resourceid</td>
<td>The resource ID used within the request</td>
<td>One is required.</td>
</tr>
<tr>
<td>pepcli.resourceid.prefix</td>
<td>Prefix added to the grinder-agent-name to create the resource ID used in the request</td>
<td>^</td>
</tr>
<tr>
<td>pepcli.actionid</td>
<td>The action ID used within the request</td>
<td>One is required.</td>
</tr>
<tr>
<td>pepcli.actionid.prefix</td>
<td>Prefix added to the grinder-agent-run-number to create the resource ID used in the request</td>
<td>^</td>
</tr>
<tr>
<td>pepcli.timeout</td>
<td>The connection timeout in seconds</td>
<td>No, defaults to 30</td>
</tr>
</tbody>
</table>

### 20.5.3 PEPCLI Test

This test uses the C language PEP CLI to issue multiple basic authorization requests. It a good test to run if you are trying get measurements for applications which do not maintain state between requests (e.g. a new client is created for every request).

**Test Name:** pepcli-multiauthz

#### Configuration Options

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>pepcli.bin</td>
<td>The path to the pepcli binary.</td>
<td>Yes</td>
</tr>
<tr>
<td>pepcli.pepds</td>
<td>A space separated list of PEPd endpoints</td>
<td>Yes</td>
</tr>
<tr>
<td>pepcli.timeout</td>
<td>The connection timeout in seconds</td>
<td>No, defaults to 30</td>
</tr>
<tr>
<td>pepcli.tests</td>
<td>A set of test inputs. See below for format.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Test Input Format

The test import format is as follows:

```
[ ['ce1', 'submit', '/home/jsmith/.globus/usercert.pem', 'Permit'],
  ['ce2', 'submit', '/home/jsmith/.globus/usercert.pem', 'Deny'],
  ['ce3', 'submit', '/home/jsmith/.globus/usercert.pem', 'Not Applicable'],
]
```

The property value is contained in matching `[` and `]` brackets. Then each test individual test scenario is contained with matching `[` and `]`. Each testing scenario has four comma-separated values: the resource ID, action ID, and certificate chain used in the request and then the expected outcome. Each test scenario is also comma-separated. The use of the `'` character can be used to indicate that the property value continues on to the next line.
20.5.4 PEP-J Test

This test uses the Java language PEP CLI to issue authorization requests. It is a good test to run if you are trying to get measurements for application which maintain state between requests (e.g. a single client is used for multiple requests).

**Test Name:** pepj-authz

**Configuration Option**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Value</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>authz.client.config</td>
<td>Path to the client configuration file. Relative paths are relative to GF_HOME.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

20.6 Authorization Services Testing Summary

20.6.1 Hardware Description

For the performance and aging tests, we installed:

- EMI-1 Argus 1.3 (PAP, PDP and PEP Server):
  - 1 Xeon CPU 2.33GHz (Dual Core)
  - 5 GB RAM

- PEP client pepcli:
  - 4 hosts running the Grinder framework

Update: Results for the 1.3.1 update using the same Hardware

There is a significant drop in memory consumption coming with the 1.3.1 update for the pepd and the pdp server. Find some load test using those Versions below.

20.6.2 Performance Tests

The performance testing of the Authorization Services was done using the hardware described above. The setup of the test was basically the same as described here, using the following options. Each agent (host running grinder-framework) opens two worker, and each worker opens 5 threads. Therefore a maximum of 40 (4*2*5) simultaneous requests are achieved.

**Test Description (SSL enabled)**

This is the most common case, since the default configuration with YAIM results in a PEPd with SSL enabled

On the Argus Server

The default configuration was used, only the cache-size was lowered to 200 requests

- pepd.ini: maximumCachedResponses = 200

The obligations needed for this test were added to the PAP
The Test-Scripts

To assure that not only cached requests are used by the PEPd, but that the PEPd also sends requests to the PDP, more than 200 different requests need to be defined in the properties file. This can easily be done by changing the resource (e.g. ce1_100, ce1_101, ...)

Results and Metrics

- Test ran for about 16h without interruption
- 1'698'886 authorization requests processed
- 30 requests per second sustained
- 1340 ms average round trip time (pepcli -> PEPd -> PDP -> PEPd -> pepcli)

Memory usage of the PEPd during the load-test:

Memory usage of the PDP during the load-test:
Results and Metrics for the 1.3.1-update

- Test ran for about 63h without interruption
- ~6.9 M authorization requests processed
- 30 requests per second sustained
- 900 ms average round trip time (pepcli -> PEPd (-> PDP -> PEPd) -> pepcli)

Requests per second during the load test for the 1.3.1 update:

Memory usage of the PDP during the load test for the 1.3.1 update:
**20.6.3 Aging Tests**

This test was done analogue to the performance test, but with only one Agent starting one worker starting one thread. This resulted in about 10 requests per second.

**Test Description**

The test was done using the same options as the performance test.

**Results and Metrics**

- Test ran for about 43h without interruption
- 1’486’711 authorization requests processed
- 10 requests per second sustained
- 101 ms average round trip time (pepcli -> PEPd (-> PDP -> PEPd) -> pepcli)

Memory usage of the PDP during the long-test:
Memory usage of the PEPd during the long-test:

20.7 Authorization Services Testing Summary

20.7.1 Hardware Description

For the performance and aging tests, we installed:

- EMI-1 Argus 1.4.0 (PAP, PDP and PEP Server):
  - 1 Xeon CPU 2.33GHz (Dual Core)
  - 5 GB RAM
- PEP client pepcli:
  - 3 hosts running the Grinder framework

20.7.2 Performance Tests

The performance testing of the Authorization Services was done using the hardware described above. The setup of the test was basically the same as described here, using the following options. Each agent (host running grinder-
framework) opens two workers, and each worker opens 2 threads. Therefore a maximum of 12 (3*2*2) simultaneous requests are achieved.

Test Description (SSL enabled)

This is the most common case, since the default configuration with YAIM results in a PEPd with SSL enabled.

On the Argus Server

The default configuration was used The policies needed for this test were added to the PAP

```
pap-admin ap permit pfqan="/dteam" --action "submit" --resource "ce1\._\.*"
pap-admin ap deny pfqan="/dteam" --action "submit" --resource "ce2\._\.*"
```

while the star denotes a number between 1 and 500, so in total the pap was loaded with 1'000 policies each one containing a rule and a obligation.

The Test-Scripts

To assure that not only cached requests are used by the PEPd, but that the PEPd also sends requests to the PDP, more than 200 different sets of Action/Resource/Obligation have been defined in the properties file. This can easily be done by changing the resource (e.g. ce1_100, ce1_101, ...). More than that 100 certificates issued by the ARC instant online CA were randomly combined with those sets, leading to roughly 1’000 different possible requests.

Results and Metrics

- Test ran for about 26.5h without interruption
- 4'078'768 authorization requests processed
- 43 requests per second sustained
- 274 ms average round trip time (pepcli -> PEPd -> PDP -> PEPd) -> pepcli

Memory consumption of the 1.4.0 PDP during a load-test:

![Graph showing Memory Usage over time]

Memory consumption of the 1.4.0 PEPd during a load-test:
20.7.3 Aging Tests

This test was done analogue to the performance test, but with only one Agent starting one worker starting one thread. This resulted in about 9 requests per second.

Test Description

The test was done using the same options as the performance test.

Results and Metrics

- Test ran for about 140h without interruption
- 4'951'677 authorization requests processed
- 9 requests per second sustained
- 97.5 ms average round trip time (pepcli -> PEPd (-> PDP -> PEPd) -> pepcli)

Memory consumption of the 1.4.0 PDP during a aging-test:
Memory consumption of the 1.4.0 PEPd during a aging-test:

Average requests per second during the aging-test:
20.8 Authorization Services Testing Summary

20.8.1 Hardware Description

For the performance and aging tests, we installed:

- EMI-1 Argus 1.4.0 (PAP, PDP and PEP Server):
  - 1 QEMU Virtual CPU 2.66GHz
  - 384 MB RAM
- PEP client pepcli:
  - 3 hosts running the Grinder framework

20.8.2 Performance Tests

The performance testing of the Authorization Services was done using the hardware described above. The setup of the test was basically the same as described here, using the following options. Each agent (host running grinder-framework) opens two worker, and each worker opens 2 threads. Therefore a maximum of 12 (3*2*2) simultaneous requests are achieved.

**Test Description (SSL enabled)**

This is the most common case, since the default configuration with YAIM results in a PEPd with SSL enabled

**On the Argus Server**

The default configuration was used The policies needed for this test were added to the PAP

```bash
pap-admin ap permit pfqane"/dteam" --action "submit" --resource "ce1\_.\*"
pap-admin ap deny pfqane"/dteam" --action "submit" --resource "ce2\_.\*"
```

while the star denotes a number between 1 and 500, so in total the PAP was loaded with 1'000 policies each one containing a rule and a obligation

**The Test-Scripts**

To assure that not only cached requests are used by the PEPd, but that the PEPd also sends requests to the PDP, more than 200 different sets of Action/Resource/Obligation have been defined in the properties file. This can easily be done by changing the resource (e.g. ce1_100, ce1_101, ...). More than that 100 certificates issued by the ARC instant online CA were randomly combined with those sets, leading to roughly 1’000 different possible requests.

**Results and Metrics**

- Test ran for about 42h without interruption
- 4‘362‘423 authorization requests processed
- 28.9 requests per second sustained
- 409 ms average round trip time (pepcli -> PEPd (-> PDP -> PEPd) -> pepcli)

Memory consumption of the 1.4.0 PDP during a load-test:

![Graph showing memory usage over time]

Memory consumption of the 1.4.0 PEPd during a load-test:

![Graph showing memory usage over time]

Average requests per second during the load-test:

![Graph showing request rate over time]
20.8.3 Aging Tests

This test was done analogue to the performance test, but with only one Agent starting one worker starting one thread. This resulted in about 9 requests per second.

Test Description

The test was done using the same options as the performance test.

Results and Metrics

- Test ran for about 190h without interruption
- 7,332,606 authorization requests processed
- 10.7 requests per second sustained
- 89.1 ms average round trip time (pepcli -> PEPd -> PDP -> PEPd) -> pepcli)

Memory consumption of the 1.4.0 PDP during a aging-test:

Memory consumption of the 1.4.0 PEPd during a aging-test:

Average requests per second during the aging-test:
20.9 Argus: Quick Start: Manual Installation

20.9.1 Prerequisites

In order to run the Argus service you will need the following:

- a working Java 5 or better installation. Use `java -version` to determine your Java version.
- a recent version of openssl (>0.9.7) installed on your system
- LCG trusted Certificate Authorities certificates installed. In SL4 and SL5, the `lcg-CA` package provides those certificates.
- a valid, PEM encoded X509 server certificate issued by a trusted CA.

20.9.2 Installation

The Argus service is composed of three components, the PAP, PDP, and PEPd. The following steps provide instructions for installing each component.

**PAP Installation**

1. Download the latest version version of the software. Expand the downloaded archive to the `/opt/argus` directory.

   • This resulting installation directory `/opt/argus/pap` will be referred to, in the documentation, as `PAP_HOME`

1. Export the environment variable `PAP_HOME=/opt/argus/pap` 1

1. Add the `/opt/argus/pap/bin` to your PATH in order to use the PAP `pap-admin` command

**PDP Installation**

1. Download the latest version version of the software. Expand the downloaded archive in to the `/opt/argus` directory.

   • This resulting installation directory `/opt/argus/pdp` will be referred to, in documentation, as `PDP_HOME`
**PEPd Installation**

1. Download the latest version version of the software. 1 Expand the downloaded archive in to the `/opt/argus` directory.
   - The resulting installation directory `/opt/argus/pepd` will be referred to, in documentation, as `PEPD_HOME`

**20.9.3 Starting/Stop the Services**

To start/stop the PAP you can use the command `/opt/argus/pap/bin/pap-standalone start|stop`.
To start/stop the PDP you can use the command `/opt/argus/pdp/bin/pdpctl.sh start|stop`.
To start/stop the PEPd you can use the command `/opt/argus/pepd/bin/pepdctl.sh start|stop`.
You should always start the PAP before the PDP or else the PDP will not be to retrieve its policy from the PAP.

Installation is now complete, proceed to configuring the Argus service.

**20.10 Argus: Quick Start: Manual Configuration**

**TODO**

Configuration is now complete, proceed to setting up your site policies.

**20.11 Quick Start: glite 3.2 Argus Installation**

**20.11.1 Installation and Configuration**

The PAP, PDP, and PEPd are bundled together as the gLite node type `glite-ARGUS`.

**YUM Repository**


**Packages Installation**

To install and initially configure the service do the following: 1 Install the EUGridPMA trust anchors bundle:

1. `yum install lcg-CA`
   1. If not already installed, install the Java VM OpenJDK 1.6:
   1. `yum install java-1.6.0-openjdk`
   1. Install the `glite-ARGUS` metapackage:

     `yum install glite-ARGUS`

1. In your YAIM `site-info.def` configuration set at least the following variables:
   - the `ARGUS_HOST` property to the hostname of the machine on which you are installing
   - the `PAP_ADMIN_DN` property to the subject DN of your user certificate. Allow the use of the `pap-admin` command
   - the `USERS_CONF`, `GROUP_CONF`, and `VOS` property to their appropriate values for your site
   1. Configure the `ARGUS_server` node type with YAIM:

     `yaim -c -s site-info.def -n ARGUS_server`
Example Configuration

Example site-info.def for the ARGUS_server node type:

```plaintext
#
# glite-ARGUS hostname
#
ARGUS_HOST=vesta.switch.ch

# users and groups
USERS_CONF=/opt/glite/yaim/etc/users.conf
GROUPS_CONF=/opt/glite/yaim/etc/groups.conf

# Supported VOs
VOS="dteam"

VO_DTEAM_VOMS_CA_DN='"/DC=ch/DC=cern/CN=CERN Trusted Certification Authority' '/DC=ch/DC=cern/CN=CERN Trusted Certification Authority' "'/DC=ch/DC=cern/CN=CERN Trusted Certification Authority"'

VO_DTEAM_VOMSES="'dteam lcg-voms.cern.ch 15004 /DC=ch/DC=cern/OU=computers/CN=lcg-voms.cern.ch dteam 24' 'dteam voms.cern.ch 15004 /DC=ch/DC=cern/OU=computers/CN=voms.cern.ch dteam 24' 'dteam lxbra2309.cern.ch 15002 /DC=ch/DC=cern/OU=computers/CN=lxbra2309.cern.ch dteam 24'"

# PAP administrator DN
PAP_ADMIN_DN="'/DC=org/DC=acme/CN=John Doe"
```

At this point, you should have a running PAP, PDP, and PEP daemon.

20.11.2 Operation Environment

You should now have Argus installed.

Directories

There are a few directories that you should be aware of:

- `/opt/argus/pap` contains the PAP component of Argus
- `/opt/argus/pdp` contains the PDP component of Argus
- `/opt/argus/pepd` contains the PEPd component of Argus
- `/etc/grid-security/certificates` contains the CAs trusted by Argus
- `/etc/grid-security/grid-mapfile` contains the mappings from DN/FQANs to local user accounts
- `/etc/grid-security/groupmapfile` contains the mappings from FQANs to local groups
- `/etc/grid-security/gridmapdir` contains grid user to local user account mappings
- `/etc/grid-security/vomsdir` contains the VOMS servers trusted by Argus

Note, if you have an existing site and wish to use your existing account mappings you can move your existing mappings over to the Argus host. Simply tar your existing mappings (`tar -cf gridmap.tar /etc/grid-security/gridmapdir`) and then transfer them over the Argus host and untar them (`tar -xf gridmap.tar`).
Endpoint URL

Argus is a network service. Like other network services you should ensure that your network settings only allow anticipated clients communicate with the service.

- Argus 1.1 enables by default client authentication on the service endpoint, therefore the endpoint URL scheme is now HTTPS.
- Client applications must be able to contact the service port 8154
- Example Argus 1.1 endpoint URL (with client authN): https://argus.example.org:8154/authz
- All other ports (8150-8153) should only be accessible within the Argus service host itself.

20.11.3 Starting/Stopping the Services

To start/stop the PAP you can use the command /etc/init.d/pap-standalone start|stop.

To start/stop the PDP you can use the command /etc/init.d/pdp start|stop. You can also force a reload of the policies, retrieved from the PAP, with /etc/init.d/pdp reloadpolicy.

To start/stop the PEPd you can use the command /etc/init.d/pepd start|stop. You can also clear the responses cache with /etc/init.d/pepd clearcache.

You should always start the PAP before the PDP or else the PDP will not be to retrieve its policy from the PAP.

Installation is now complete, proceed to setting up your site policies.

20.11.4 Global Banning Configuration

The following are the required steps to make your Argus server import the global grid banning policies. These policies are maintained by OSCT / EGI CSIRT. The server is located at CERN.

Notice that in following the steps below you will be trusting the global banning server and its policies, so that e.g. users banned by the OSCT / EGI CSIRT will also be rejected at your site as a result.

The pap-admin command is normally installed in /opt/argus/pap/bin

Add the Global Banning PAP server from CERN as a remote PAP:

```
pap-admin add-pap centralbanning argus.cern.ch "/^DC=ch/DC=cern/OU=computers/CN=argus.cern.ch"
```

The CERN PAP is now listed but is by default still disabled.

```
pap-admin enable-pap centralbanning
```

The CERN PAP is now enabled.

```
pap-admin set-paps-order centralbanning default
```

The CERN PAP policies are now parsed before the local policies, so that e.g. a user banned by OSCT is immediately rejected. This step is important as only with this order can black listing work.

```
pap-admin refresh-cache centralbanning
```

The local pap cache, comprising also the CERN policies, is refreshed and the new policies are made available. The policies are then fetched automatically by the server every polling interval seconds or manually when the a refresh-cache command is sent to the server.
CHAPTER 21

Indices and tables

- genindex
- modindex
- search