

AMC Server 6.0

Administration Guide

English Edition | System Release 6.0 | December 2015



AMC Server 6.0

Administration Guide

System Release 6.0

Published December 2015

Copyright Information. The information contained in this user manual may be subject to change without notice and in no way represents a commitment on the part of Arkoon Network Security. The equipment described in this manual is supplied under license and may only be used or copied strictly under the terms of this license. No part of this manual may be translated, reproduced or transmitted for any purpose, in any form or by any means (electronic or mechanical) whatsoever without express written permission from Arkoon Network Security.

Copyright 2006–2015 Arkoon Network Security

The Arkoon Management Center (AMC) is a registered trade mark of Arkoon Network Security.

Contacts.

Arkoon Network Security
1, place Verrazzano
69009 Lyon
France

Tel: +33 (0)4 72 53 01 01
Fax: +33 (0)4 72 53 12 60
Website: <http://www.arkoon.net>

Technical Support Service.

For the latest updates or to contact the Arkoon Technical Support, see the Arkoon Technical Support website: <http://client.arkoon.net>

Table of Contents

Preface	
1. About this Document	7
2. About the AMC	7
3. Audience	7
1. Introduction	
1.1. Requirements	9
1.2. Architecture	10
1.2.1. Single-instance Architecture	10
1.2.2. Multi-instances Architecture	11
2. Installation	
2.1. Installing the Server	13
2.2. Installing MySQL Server	13
2.3. Installing Dependencies for 64-bit Servers	14
2.4. Installing arkoon-amc Package	14
3. Configuring AMC Server with minamcconf	
3.1. Generating the License	15
3.2. Installing the License	16
3.3. Creating an AMC Instance	16
3.3.1. Configuring MySQL Parameters	17
3.3.2. Configuring Certification Authority Parameters	17
3.3.3. Configuring Network Parameters	18
3.4. Creating a Super AMC Instance	18
4. Configuring AMC Server Manually	
4.1. Workflow	19
4.2. Creating an AMC Instance	19
4.3. Creating a Certification Authority (CA)	21
4.4. Installing a Certificate for the Instance	23
4.5. Initializing the Administration Rights	24
4.6. Configuring the Log Centralization	24
4.7. Configuring the System Logs Notification	26
4.8. Configuring the Network Parameters	26
4.9. Configuring a Global Monitoring Instance	27
5. Using AMC Server	
5.1. Starting and Stopping	29
5.2. Connecting Arkoon tools to an AMC Instance	29
5.3. Connecting a Fast360 Appliance to an AMC Instance	29
5.4. Flushing a mySQL Database	30
5.5. Restarting an AMC Service	30
5.6. Managing the Appliances Updates	31
6. Auditing the AMC Server	
6.1. Diagnostic Command	33
6.2. Alerts	34
6.3. Security Level of an AMC Instance	34
7. Maintaining AMC Server	
7.1. Backing up AMC Server Data	35
7.1.1. Backing up All Configuration Files	35



7.1.2. Backing up Certificate Authority only	35
7.1.3. Backing up Role Management Database only	35
7.2. Restoring AMC Server Data	36
7.2.1. Restoring All Configuration Files	36
7.2.2. Restoring Certificate Authority only	36
7.2.3. Restoring Role Management Database only	36
7.3. AMC Server update	36
7.4. Removing arkoon-amc Package	37
7.5. Optimizing MySQL databases	37
8. Terminology	
8.1. Terminology	39
A. Migration cases	
A.1. Migrating from an AMC server to a new AMC or VAMC server	41
A.2. Migrating the master role from the Fast360 appliance to an AMC server	41
A.3. Migrating from a standalone appliance to a slave appliance of a new AMC instance	42
B. Deploying a CRL on all the appliances of an AMC instance	
B.1. With an Arkoon PKI managed by the AMC instance	43
B.2. With an external PKI	43
B.3. Automatic retrieval of the CRL by a new appliance	43
C. Configuration file	
C.1. Configuration file for an instance example	45
C.2. Configuration file to be included: arkoon-config	45
D. Saving regularly the appliances configuration of the AMC instance	
D.1. Saving regularly the appliances configuration of the AMC instance	47

List of Examples

- 7.1. Automatic launch of the database maintenance script at regular intervals with Crontab (every day at 4.00 am) 37
- 7.2. Manual launch of the database maintenance script 37
- 7.3. Manual launch of the database maintenance script with argument 37



Preface

1. About this Document

This document describes the installation, configuration and maintenance of the AMC Platform server software.

2. About the AMC

The AMC (Arkoon Management Center) architecture enables clusters of Fast360 appliances to be managed centrally. Each AMC cluster is made up of several Fast360 appliances connected to an AMC server.

3. Audience

This AMC Administration guide is intended for Linux administrators with Arkoon multi-service security appliances knowledge.



Chapter 1. Introduction

1.1. Requirements

The `arkoon-amc` installation package must meet the following hardware requirements:

- Version 5 or 6 of RedHat Linux ES - 32/64 bits. The latest 6.x version is recommended (<http://www.redhat.com>)
- Version 5 or 6 of CentOS Linux 32/64 bits. The latest 6.x version is recommended (<http://www.centos.org>)
- Intel Xeon Processor 3Ghz (Dual Core)
- 4 Gb RAM
- MySQL database (<http://www.mysql.com>)
- 300 Gb hard disk (SAS hard disk is recommended)

Note

The AMC server mainly uses the `/var` partition for the logs database, configurations and the communication with slaves. Be sure to keep enough space on this partition (about 100 GB).

The information is for the following specific context:

- 1 AMC instance
- 5 to 10 standalone or cluster appliances
- 200 Mb logs per appliance and per day
- 3 days of logs in the database
- 365 days for archiving (legal period for some countries like France)

Note

The MySQL database is used by the AMC server to store logs but it is not an AMC server component. The administration of MySQL databases is not performed by the AMC server and the database administrator remains responsible for it.

Note

The `crond` component must be installed on the AMC server for some features to work. Only the `/etc/cron.d` directory and appropriate files are created when installing the `arkoon-amc` package.

1.2. Architecture

Two types of AMC architecture can be implemented:

- **Single-instance:** an AMC cluster controlling a single instance.
- **Multi-instances:** multiple Fast360 clusters can be controlled on a given AMC server.

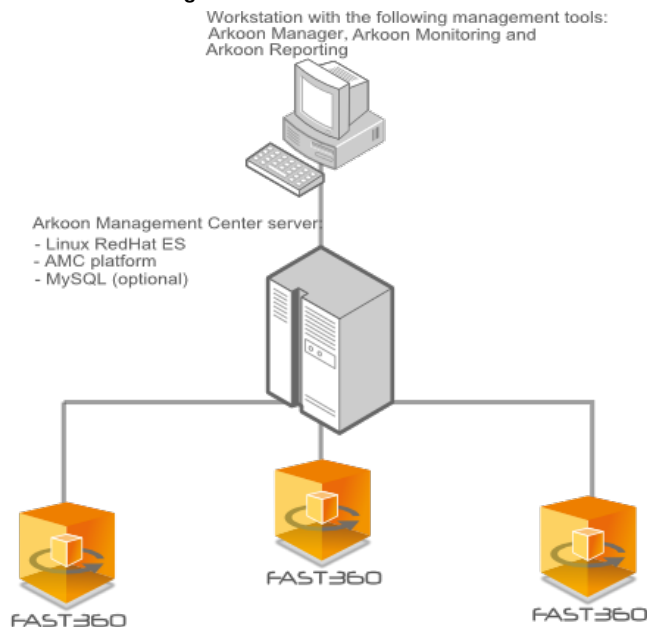
A single AMC instance corresponds to each appliance cluster configured by the administrator. The appliances and the administrator access the AMC server instance using Arkoon tools over secure network connections with the SSL (Secure Socket Layer) V3 protocol on the basis of X.509 certificates from the same Certification Authority.

1.2.1. Single-instance Architecture

Fast360 appliances are connected to the AMC server. You can carry out the following operations from the Management station:

- Connect Arkoon Monitoring to the AMC server to monitor the GOR (Green Orange Red) status and access the logs: Alerts, IP and IDPS Logs, HTTP relays, SMTP relays.
- Connect Arkoon Monitoring to an appliance to monitor a specific parameter.
- Connect Arkoon Monitoring to the instance created on the AMC server to configure the security policy of the cluster (policy common to all appliances in the cluster).

Below is an example of a single-instance architecture with three Fast360 appliances which have a centralised management:

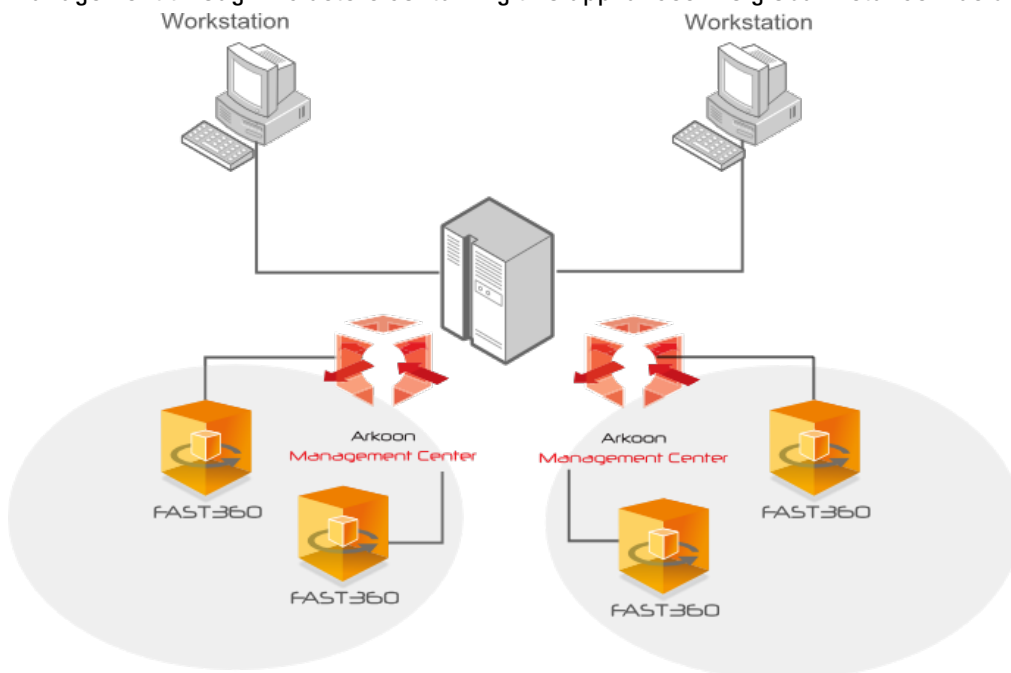


1.2.2. Multi-instances Architecture

A multi-instances architecture allows you to control several clusters, each with its own security policy. In this case, each cluster corresponds to an AMC instance on the AMC server.

- Each AMC instance manages the security policy of its cluster independently of the others.
- Several AMC instances can share a single log database but this is not mandatory. If the AMC instances share a single log database, all the logs are available directly via Arkoon Monitoring.
- You can create AMC instances global management. Instead of monitoring the appliances, they access the GOR status of multiple appliance clusters and centralize the logs in a given database.

Below is an example of a multi-instances architecture with four Fast360 appliances which have a central management through 2 clusters containing two appliances. No global instance was defined.





Chapter 2. Installation

Before you install the AMC server, you must check it meets the technical specifications given in Section 1.1, "Requirements".

To install the AMC server:

1. Install the server, hardware and system.
2. Install the `arkoon-amc` package.
3. Install the AMC license.
4. Optionally, install the MySQL server to enable the appliance log centralization.

2.1. Installing the Server

The server shall have a RedHat ES or CentOS 5.8 ou 6.4 distribution.

To check that the server is installed with the RedHat ES 5.8 distribution for example, enter:

```
[root@amc-server root]# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 5.8
```

Note

Activating SELinux can lead to a malfunctioning of AMC server. To prevent this behaviour, configure SELinux in permissive mode. To do so, modify the `/etc/selinux/config` configuration file and use the `setenforce 0` command.

2.2. Installing MySQL Server

The installation of the MySQL server makes the appliance log centralization feature available on the AMC server. The use of this feature is strongly recommended for the global monitoring of the logs by the appliances.

The MySQL database can be installed on the AMC server or on a remote server.

Install the MySQL server on the AMC server as follows:

Note

The `mysql-server` package is not present on the RedHat ES 5.0 CD-ROM but is available for free from <http://www.redhat.com> or on <https://rhn.redhat.com/>.

1. Install the MySQL server package:

```
yum install mysql-server
```

If you have any issue, you can use the following command to install the package:

```
[root@amc-server root]# rpm -ivh mysql-server-3.23.
58-16.RHEL3.1.i386.rpm
warning: mysql-server-3.23.58-16.RHEL3.1.i386.rpm: V3 DSA
signature: NOKEY, key ID db42a60e
Preparing... #####
[100]
1:mysql-server #####
[100]
```

2. Set the database to start automatically when the server starts:

```
[root@amc-server root]# /sbin/chkconfig --add mysqld
[root@amc-server root]# /sbin/chkconfig mysqld on
```

3. Start the database:

```
[root@amc-server root]# /etc/init.d/mysqld start
Starting MySQL: [ OK ]
```

4. Configure the MySQL server:

1. Leave the MySQL password empty:

```
#/usr/bin/mysqladmin -u root password ""
```

2. Check the connection to MySQL:

```
#!/mysql -u root
```

2.3. Installing Dependencies for 64-bit Servers

For 64-bit servers, you must install the following dependencies. In all cases, after installing the packages below, install:

```
yum install libstdc++.i686
```

Servers under RedHat ES 5/6 or CentOS 5/6

Install the packages below:

```
yum install python-libs.i686 python.i686
```

By default, CentOS configure an "iptables" firewall blocking the access to the AMC server. It is possible to adapt it to suit your needs or to definitely disable it:

```
service iptables save
service iptables stop
chkconfig iptables off
```

2.4. Installing arkoon-amc Package

Install the `arkoon-amc` package:

- for RedHat and CentOS 5 32/64 bits, use the package

```
arkoon-amc-6.0-xxxxxx_xxxx.e15.i386.rpm
```

- for RedHat and CentOS 6 32/64 bits, use the package

```
arkoon-amc-6.0-xxxxxx_xxxx.e16.i386.rpm
```

Enter the command:

```
yum localinstall /tmp/arkoon-amc-6.x-xxxxxx_xxxx.e1x.i386.rpm --nogpgcheck
```

Replace `x` in `e1x` by 5 or 6 according to the RedHat or CentOS version used.

The AMC server does not start after the installation since you have not configured an AMC instance yet.

Chapter 3. Configuring AMC Server with minamcconf

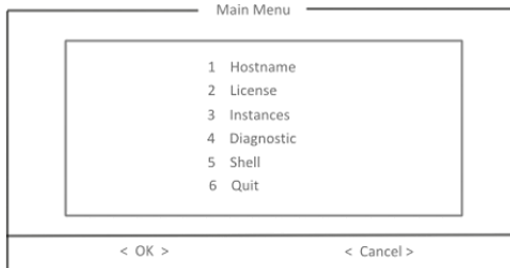
The minamcconf tool helps you to configure the AMC server and also to create and configure the instances.

The minamcconf tool is available on the AMC server via minamcconf.

3.1. Generating the License

The AMC license is based on the main AMC server interface IP address on which the Arkoon appliances shall be connected. For example, if the connections must be made on eth0 (or an alias of eth0), the IP address must be eth0 address IP.

At start-up, the following window is displayed:



1. Select `Hostname` to attribute a name and select `<OK>` to validate.
2. Select `License` and then `Request license`.
3. Enter the license name, the IP addresses (separated with a space) and the license request file name.
4. Validate and connect on `http://license.arkoon.net` with the request file and your license key to register your product and retrieve your license file.

Important

The number of appliances you can connect to all your instances depends on the license you bought.

If there is no license installed, it is possible to manage a maximum of 5 appliances. In this case, the following information is displayed when starting an instance:

```
Warning: amc-license-file (/etc/arkoon-amc/amc-license.akl) not found.
```

If more than 5 instances connect to an AMC instance without a license, the new appliance connection is denied:

- a log is added to the `/var/log/messages` AMC file:

```
akslave[28029]: AMC connection refused due to maxip verification:
Maximum number of arkoons (5) reached
```

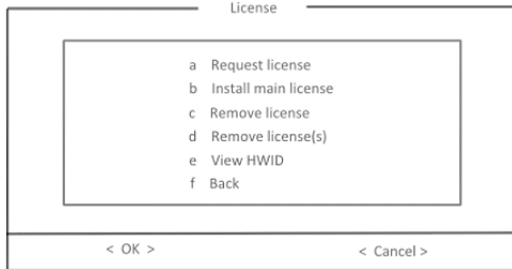
- a log is added to the `/var/log/messages` file of the denied appliance:

```
akslave[10461]: Connecting to 10.2.1.200:1754...
akslave[10461]: Connected with [CN=CERT-INSTANCE-instance_qa,OU=QA,O=Arkoon,L=Lyon,C=FR]
akslave[10461]: SSLCOM_write returns -1 [SSL operation SSL_write failed: Connection reset by peer]
akslave[10461]: SSLCOM_read returns -1 [SSL operation SSL_read failed:
SSL connection closed by peer] akslave[10461]: Master refused our UNKNOWN_CMD command (718756560)
akslave[10461]: ak_slave_start_session failed
```

3.2. Installing the License

To install the license:

1. Copy the license file on the AMC server.
2. Select `Install main license` and validate with `<OK>`.



3. Enter the path to retrieve the license file and validate with `<OK>`.

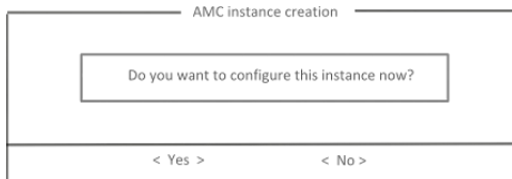
3.3. Creating an AMC Instance

1. Select `Instances` from the main menu and then choose `Create AMC instance`.
2. Enter a name for the instance to create and validate with `<OK>`.

Note

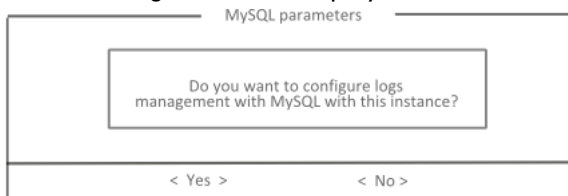
Only the following characters are valid: 0-9, a-z, A-Z, _ and -

The following window is displayed:



3. Validate with `<Yes>`.

The following window is displayed:

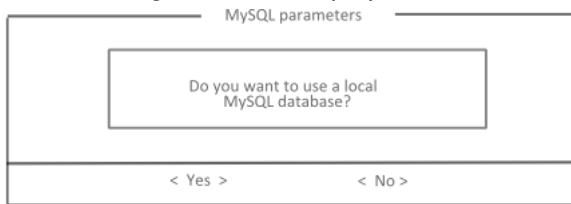


4. Click on `<Yes>` to carry on the procedure described in Section 3.3.1, "Configuring MySQL Parameters".



3.3.1. Configuring MySQL Parameters

The following window is displayed:



- If you validate with <Yes>, the **IP** and **Port** fields are not required.
 - If you validate with <Yes>, you must enter the following fields:
 - IP
 - Port
 - Remote base name
 - User
 - Password (optional)
1. If you use a local database (most common case), you can then enter the MySQL database name to manage logs and alerts, then click on <OK>.
 2. Provide the database user name and click on <OK>.
 3. Click on <OK> to enter a user password and validate with <OK>.

The MySQL database has been correctly created.

3.3.2. Configuring Certification Authority Parameters

Important

By default, Fast360 appliances initialize certification authorities which comply with the French RGS regulatory documentation *Annexe B1 Mécanismes cryptographiques* (http://references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_cryptographiques_v1_20.pdf). According to the documentation, the key size of certification authorities is 4096 bits and the hash algorithm is SHA-256.

However, in the case of a migration from a version 5.x of Fast360, the CA parameters used by an existing instance do not change and the CA remains operational. To have the new parameters, it is necessary to create a new CA for this instance. This operation implies to certificate again appliances, administrators, Arkoon Authentication agent users and nomad VPN users.

To configure the Certification Authority parameters:

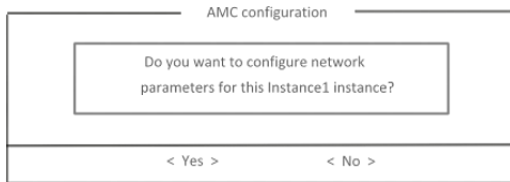
1. Enter the required parameters and validate with <OK> to end the configuration and access the **Certification Authority** creation window.
2. Select <Yes> from the Certification Authority window.
3. Enter a password and validate with <OK>.
4. Enter the required fields and validate with <OK>.

The Certification Authority is created. You must now create the certificate.

5. Select <Yes> to create the certificate, and then enter the required fields.

3.3.3. Configuring Network Parameters

When the AMC creation is finished, the minamcconf tool displays the following window to configure the network parameters for the created instance:



1. Validate with <Yes>.
2. Enter the IP address and validate with <OK>.

The following parameters are required:

- Manager port: 1750
- Monitoring port: 1751
- Master/Slave Signal Port: 1754
- Master/Slave Data Port: 1759

Note

Choose an available port.

3.4. Creating a Super AMC Instance

To create a Super AMC instance, go to the main menu and select `Create Super AMC instance`. The first steps of the procedure are equivalent to the AMC instance procedure (see Section 3.3, “Creating an AMC Instance”).

The last step requires you specify the AMC instance managed by the Super AMC instance.

Note

The manager port is configured but not used.

Important

To access and manage the logs of the instances with Arkoon Monitoring, the Super AMC instance database must be the same as the instances database.

Chapter 4. Configuring AMC Server Manually

This chapter describes how to configure the AMC server manually.

4.1. Workflow

From version 5.0, the AMC server is configured with the `minamcconf` tool. This chapter details how to configure the AMC server without `minamcconf`.

The AMC server configuration is contained in one main configuration file, `/etc/arkoon-amc/config/amc-instances`, and one configuration file per instance, `/etc/arkoon-amc/config/<instance_name>`. Carry out the configuration as follows:

1. Create an AMC instance.
2. Create a Certification Authority (CA) if required.
3. Install the certificate for the instance.

Note

The following steps depend on the features and are optional.

4. Configure the log centralization.
5. Configure the system logs notification.

Note

For a multi-instances architecture, you can configure one global instance to monitor multiple instances from Arkoon Monitoring.

6. Configure the network parameters.
7. Configure a global monitoring instance.

4.2. Creating an AMC Instance

To create an AMC instance:

1. Choose a unique instance identifier.

This identifier is used to refer to the instance in configuration files and audit trails.

Caution

The identifier for an instance is limited to 16 characters and must contain only the characters 0-9, a-z, A-Z, '_' and '-'. E.g. 'amc-main'.

2. Create a configuration file for the instance.

The name of the created file must be the same as the name of the instance. Place it into the `/etc/arkoon-amc/config/` folder. At a minimum, it must include the `/opt/arkoon/etc/arkoon-config` default configuration file and define the `arkoon-amc.instance-name` parameter with the instance name:

```
# Arkoon Management Center (AMC) 'amc-main' configuration
# /etc/arkoon-amc/config/amc-main

include /opt/arkoon/etc/arkoon-config

arkoon-amc.instance-name = "amc-main"
```

Note

The `/opt/arkoon/etc/arkoon-config` default configuration file does not contain a certificate or a database. It is included in the configuration file for each instance and its parameters can be altered. This file is provided as an example in Section C.1, “Configuration file for an instance example”.

Caution

The configuration file contains the passwords protecting the certificate files in clear text. Protect its security by restricting the Unix rights on the file.

3. Add the new AMC instance to the list of configured instances.

The `/etc/arkoon-amc/config/amc-instances` file contains the list of instances configured as a list of instance names separated by spaces as follows:

```
AMC_INSTANCES="amc-main amc-secondary"
```

4. Restart the `arkoon-amc` service.

Once installed and configured, the `arkoon-amc` service starts automatically at machine start-up and stops when the machine is stopped or rebooted. You can force it to start using the following command:

```
[root@amc-server root]# /etc/init.d/arkoon-amc restart
Stopping arkoon-amc server:
Starting arkoon-amc server:
  Starting [amc-main]:
    Checking database: no database configuration
    Starting akserver: amc-main:akserver
    Starting amanaged: no certificate defined
    Starting srvmon: no certificate defined
    Starting akslave: no certificate defined
    Starting akstatsd: no certificate defined
  Creating cron config file: done
```

At this stage of the configuration, the start command shows that no log database has been configured for the instance. Moreover, no certificate has been defined to enable the management and monitoring services to communicate with the appliances and management station.

To restart the `arkoon-amc` service for the ‘amc-main’ instance only, use the following syntax:

```
[root@amc-server root]# /etc/init.d/arkoon-amc restart amc-main
```



4.3. Creating a Certification Authority (CA)

The appliances and the administrator access the AMC server instance using Arkoon tools over secure network connections with the SSL (Secure Socket Layer) V3 protocol on the basis of X.509 certificates from the same Certification Authority.

Each AMC instance depends on a CA, which can be created especially for the instance on the AMC server. Otherwise, the instance can depend on a CA previously defined. In this case, go directly to Section 4.4, “Installing a Certificate for the Instance”.

The Certification Authority on which the AMC instance depends is used to create certificates associated with the following:

- The AMC instance
- A different AMC instance
- An appliance Fast360
- An administrator
- A user

Create the CA on the command line as follows:

```
[root@amc-server root]# /opt/arkoon/bin/arkoon_ca --amc-instance
<INSTANCE-NAME> -initca <CA-PEM-PHRASE> \
<DN-O> <DN-OU> <DN-L> <DN-C> [<DN-CN>]
```

where, in general, DN-O is the name of the organization represented by the CA, DN-OU the department within the organization, DN-L the town and DN-C the country code (FR for example). CA-PEM-PHRASE is the passphrase (password) protecting access to the CA.

Caution

Since the password is provided in a shell command, you may need to use an escape character before characters reserved by the shell (such as *, !, >, &, etc.).

Choose complex passwords and either remember them or keep them in a location with a high level of security (avoid post-it notes or do not save them in a non-protected file).

```
[root@amc-server arkoon]# /opt/arkoon/bin/arkoon_ca --amc-instance amc-main \
-initca<my-secret-password>" "Arkoon Network Security" "AMC - amc-main" \
"Lyon" "FR" "AMC CA [amc-main]"
Arkoon CA [v2]
-----
```

```
Creation of /var/arkoon-amc/amc-main/arkoon-ca...ok
Creation of the other files and directories...ok
Random file initialisation (8192b of /dev/urandom)...ok
Private key generation (1024 bits)...
8192 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Private key generation (1024 bits)...ok
Config file generation...ok
Self signed Certificate creation...
Self signed Certificate creation...ok
Config file generation...ok
New CRL generation...
Using configuration from /tmp/.arkoon-ca.JNsZwW
New CRL generation...ok
New CRL (/var/arkoon-amc/amc-main/arkoon-ca/cr1.pem)...ok
CA Initialization...ok
```

A FIREWALL certificate must then be created for the AMC instance and for each appliance to be connected to the instance. An ADMINRW certificate must be created for the instance administrator.

Note

The appliance certificates must be imported on each appliance to be connected to the instance. Refer to the Fast360 Administration guide for this procedure. The appliances in HA (High Availability) mode will be configured with a unique appliance certificate.

The syntax of the command to create a certificate is:

```
[root@amc-server root]# /opt/arkoon/bin/arkoon_ca --amc-instance
<INSTANCE-NAME> -newcert <CA-PEM-PHRASE> \
  <DN-CN> <DN-M> <DN-O> <DN-OU> <DN-L> <DN-C> <DAYS> <PKCS12-FILE>
<PKCS12-PASSWD> \
  USER|ADMIN|ADMINRW|FIREWALL
```

In addition to the parameters which are similar to the parameters used to initialize the CA, DAYS is the number of days for which the certificate is valid, PKCS12-FILE is the name of the file in which the certificate is to be stored and PKCS12-PASSWD is the password protecting the PKCS#12 file.

Caution

The generation of a certificate in PKCS#12 format requires a secure password be chosen to protect the certificate and that the file be stored in a safe location. The PKCS#12 file generated contains information which is strictly confidential such as the private key used for authenticating and negotiating secure SSL connections. If divulged to a third party, the certificate should be revoked.

```
[root@amc-server arkoon]# /opt/arkoon/bin/arkoon_ca --amc-instance amc-main \
  -newcert<my-secret-password>" "AMC server [amc-main]" "" "Arkoon Network Security" \
  "amc-main" "Lyon" "FR" 3650 /etc/arkoon-amc/certs/cert-amc-main.p12 \
  "<my-p12-secret>" FIREWALL
Arkoon CA [v2]
-----
```

```
Random file initialisation (8192b of /dev/urandom)...ok
Private key generation (1024 bits)...
8192 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
....+++++
.....+++++
e is 65537 (0x10001)
Private key generation (1024 bits)...ok
Config file generation...ok
Request creation...
Request creation...ok
Config file generation...ok
Signing request file...
Using configuration from /tmp/.arkoon-ca.flwC7n
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'FR'
localityName         :PRINTABLE:'Lyon'
organizationName     :PRINTABLE:'Arkoon Network Security'
organizationalUnitName:PRINTABLE:'amc-main'
commonName           :T61STRING:'AMC server [amc-main]'
Certificate is to be certified until Mar  5 10:49:41 2015 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
Signing request file...ok
Config file generation...ok
New CRL generation...
Using configuration from /tmp/.arkoon-ca.aJ8yCw
New CRL generation...ok
New CRL (/var/arkoon-amc/amc-main/arkoon-ca/crl.pem)...ok
Creating PKCS#12 file /etc/arkoon-amc/certs/cert-amc-main.p12...ok
```

Note

Once the certificates have been created for the AMC instance and the administrator, new certificates can be created using the Arkoon Manager graphic management interface.

For the management of certificates and administrator roles, refer to Section 4.5, “Initializing the Administration Rights”.

Note

To change the PEM phrase of your certificate authority:

```
/opt/arkoon/bin/arkoon_ca --amc-instance "instance_name" -passwd <OLD-CA-PEM-PHRASE><NEW-CA-PEM-PHRASE>
```

4.4. Installing a Certificate for the Instance

An AMC instance must have a FIREWALL certificate to establish secure SSL connections with the appliances and the management station. The various services for an instance will not start up without a certificate.

The certificate must have the following characteristics:

- Extension X509v3: Arkoon Firewall Certificate

The X509v3 Arkoon Firewall Certificate extension is fixed when you create the certificate from a Fast360 appliance or the AMC server with FIREWALL usage. If a third-party PKI is used, the following extension must be added to the certificate: `iso.org.dod.internet.private.enterprise.arkoon.sslcom.akCertUsage(1.3.6.1.4.1.8628.2.1)` with value `0x12`.

- PKCS#12 Package

The X509 certificate, the private key and the CA certificate which issued the certificate must be stored in a PKCS#12 package.

Caution

The generation of a certificate in PKCS#12 format requires a secure password to protect the certificate. The file must be stored in a safe location. The PKCS#12 file generated contains information which is strictly confidential such as the private key used for authenticating and negotiating secure SSL connections. If divulged to a third party, the certificate should be revoked.

The PKCS#12 file and the associated CRL (Certificate Revocation List) (if present) are configured as follows in the configuration file for the instance:

```
arkoon-amc.certificate.pkcs12 = /etc/arkoon-amc/certs/cert-amc-main.p12
arkoon-amc.certificate.passwd = "<my-secret-pkcs12-passwd>"
arkoon-amc.certificate.crl = /var/arkoon-amc/<instance_name>/arkoon-ca/crl.pem
```

Caution

Since this file contains the password to the PKCS12 file, its security must be protected and its access restricted, for example by giving it restricted Unix rights such as `600/root/root`.

You must then restart the `arkoon-amc` service for the changes to take effect.

4.5. Initializing the Administration Rights

To remotely manage an instance of the AMC server using the Arkoon tools applications, an administrator needs a certificate signed by the instance's trusted Certificate Authority and administration roles be associated to this certificate.

The Administrator Access Control database of the instance is first initialized from the command line interface by associating the "All Permissions" role with a Management Certificate.

Note

The administrator whose certificate is provided during this procedure will have all the administration permissions and will perform any administration operation on the instance from Arkoon tools. Specifically, this administrator will be authorized to define administration authorizations to new administrators.

1. Copy the certificate of the main administrator in PEM format to the AMC server.
2. Enter the following command:

```
/opt/arkoon/bin/access-control.sh --amc-instance <instance name> -init <certificate path>
```

The certificate has now all permissions when you connect to Arkoon Manager.

The following example is for an instance with its own Certification Authority and the administrator's certificate being 02.pem:

```
---
root@amc-server root# /opt/arkoon/bin/access-control.sh --amc-instance amc-main -init
/var/arkoon-amc/amc-main/arkoon-ca/certs/02.pem
Access control
-----
Access control initialization with /var/arkoon-amc/amc-main/arkoon-ca/certs/02.pem
CN=MainAdministrator,OU=amc-main,O=Arkoon Network Security,L=Lyon,C=FR succeeded
---
```

4.6. Configuring the Log Centralization

This configuration is optional. If you want to activate it, the database server must have been installed previously as described above.

Centralizing the appliance logs for an AMC cluster requires a database is configured for the associated instance. In a multi-instances architecture, multiple instances can share the same database.

The example below shows how to initialize a database `amcdb`, which is accessible to the `amc-server` user (password `amc-password`):

Note

The user is specific to the MySQL database and is not necessarily a system user.


```
[root@amc-server root]# mysql -u root mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 40 to server version: '3.23.58'

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> CREATE DATABASE amcdb;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL ON amcdb.* TO 'amc-server'@localhost IDENTIFIED BY 'amc-password';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql> QUIT
Bye
```

To associate the database with an AMC instance, add the following lines in the configuration file for the instance:

```
arkoon-amc.db.enable = yes
arkoon-amc.db.database = "amcdb"
arkoon-amc.db.user = "amc-server"
arkoon-amc.db.password = "amc-password"
```

For example, to install the database on a remote server at IP address 192.168.1.20 on port 3306, you would add the following lines to the configuration file for the instance:

```
arkoon-amc.db.host = 192.168.1.20
arkoon-amc.db.port = 3306
```

The AMC instance stores the alerts issued in the log database.

A log purge mechanism (similar to the one for Fast360 appliances) is available to control the size of the database. By default, this mechanism is disabled. You can enable it the following way:

```
arkoon-amc.akdbpurge.enable = yes
```

Caution

In a multi-instances architecture, multiple instances can share the same log database. The log purge mechanism must only be activated on one of the AMC instances.

By default, the logs less than 30 days old are kept in the database. This can be changed adding the following line to the instance configuration file:

```
arkoon-amc.akdbpurge.table.pxlogs.db-days = 10
arkoon-amc.akdbpurge.table.smtplogs.db-days = 10
arkoon-amc.akdbpurge.table.alerts.db-days = 40
arkoon-amc.akdbpurge.table.ids_alerts.db-days = 10
arkoon-amc.akdbpurge.table.logs.db-days = 20
```

Besides, the logs backups are kept 20 additional days. To change the archiving duration, modify the following parameters:

- `arkoon-amc.akdbpurge.table.pxlogs.backup-days = 20`
- `arkoon-amc.akdbpurge.table.smtplogs.backup-days = 20`
- `arkoon-amc.akdbpurge.table.alerts.backup-days = 20`
- `arkoon-amc.akdbpurge.table.ids_alerts.backup-days = 20`
- `arkoon-amc.akdbpurge.table.logs.backup-days = 20`

The log purge mechanism is triggered every day at 4 am. This time can be modified as follows:

```
arkoon-amc.akdbpurge.periodicity = 23:30
```

Restart the `arkoon-amc` service for the changes to take effect, and to initialize the database:

```
[root@amc-server root]# /etc/init.d/arkoon-amc restart
```

4.7. Configuring the System Logs Notification

By default, the system logs are not sent back to Arkoon Monitoring by an instance in real time. If you want to send the system logs in real time, you need to create a FIFO (First In, First Out) file and configure syslog and the AMC instance to use it as shown below:

1. Create a FIFO file:

```
[root@amc-server root]# mknod /var/log/arkoon-syslog p
```

2. Change the ownership of the FIFO file (required if the AMC instance does not run as root. In this example, the AMC instance uses the privileges of the "arkoon" user):

```
[root@amc-server root]# chown arkoon:arkoon /var/log/arkoon-syslog
```

3. Configure syslog to use the FIFO file. To do this, the line below must be added to the `/etc/syslog.conf` file :

```
*.* |/var/log/arkoon-syslog
```

4. Configure the instance to use the FIFO file.

```
arkoon-amc.srvmon.syslog-fifo-file = /var/log/arkoon-syslog
```

Afterwards, the `syslog` and `arkoon-amc` services must be restarted for the changes to be taken into account.

5. Restart the `syslog` service:

```
[root@amc-server root]# /etc/init.d/syslog restart
```

6. Restart the `arkoon-amc` service:

```
[root@amc-server root]# /etc/init.d/arkoon-amc restart
```

4.8. Configuring the Network Parameters

By default, AMC instance services listen to all IP server addresses (0.0.0.0) and on the default TCP ports: 1750 (Administration, `amanagerd`), 1751 (Supervision, `srvmon`), 1754 (Fast360 appliances, `akslave`) and 1759 (Arkoon Super Server over SSL, `akserver-over-ssl`).

For multiple AMC instances to co-exist on the same server, this default configuration must be changed so that each instance uses distinct IP addresses or ports.

Configure the IP address to listen to in the AMC instance configuration file, for example:

```
arkoon-amc.bind-ip = 192.168.1.30
```

Configure the TCP ports in the AMC instance configuration file, for example:

```
arkoon-amc.akman_port = 2750
arkoon-amc.akmon_port = 2751
arkoon-amc.akslave_port = 2754
arkoon-amc.akstats_port = 2757
arkoon-amc.akserver_ssl_port = 2759
```

Restart the `arkoon-amc` service for the changes to take effect.



4.9. Configuring a Global Monitoring Instance

A global monitoring instance monitors the status of Fast360 appliances on multiple AMC clusters from a single Arkoon Monitoring connection. A global monitoring instance monitors the Fast360 appliances GOR status on multiple AMC clusters from a single Akoon Monitoring connection.

To configure it, specify the global instance network parameters and the parameters for monitored instances in the configuration file for the global instance:

```
arkoon-amc.bind-ip = 192.168.1.30
arkoon-amc.akmon_port = 3751
arkoon-amc.akstats_port = 3757
arkoon-amc.srvmon.objects-file.0 = /var/arkoon-amc/france/srvmon.conf
arkoon-amc.srvmon.slaves-dir.0 = /var/arkoon-amc/france/slaves
arkoon-amc.srvmon.objects-file.1 = /var/arkoon-amc/usa/srvmon.conf
arkoon-amc.srvmon.slaves-dir.1 = /var/arkoon-amc/usa/slaves
arkoon-amc.srvmon.objects-file.2 = /var/arkoon-amc/japan/srvmon.conf
arkoon-amc.srvmon.slaves-dir.2 = /var/arkoon-amc/japan/slaves
arkoon-amc.srvmon.objects-file.3 = /var/arkoon-amc/germany/srvmon.conf
arkoon-amc.srvmon.slaves-dir.3 = /var/arkoon-amc/germany/slaves
[...]
```

Note

In this example, `france`, `usa`, `japan` and `germany` are the names of monitored instances. The numbering has no functional meaning and is only used to distinguish the instances in this file.

If the instances being monitored are not started by the same user, the user specified for the global monitoring instance must have the right to access the user files for these instances. Refer to the RedHat documentation for instructions on the access rights.

Restart the `arkoon-amc` service for the changes to take effect:

```
[root@amc-server root]# /etc/init.d/arkoon-amc restart
```

Note

For the Super instance to access the instance log, you must configure the same database in the Super instance as in any other instance. All the logs are then stored in the same database.



Chapter 5. Using AMC Server

5.1. Starting and Stopping

Once installed and configured, the `arkoon-amc` service starts automatically at machine start-up and stops when the machine is stopped or rebooted.

For a configuration change to take effect, the `arkoon-amc` service must be restarted using the following command:

```
root@vamac-masslave:~# /etc/init.d/arkoon-amc restart
Stopping arkoon-amc server:
  Stopping [MOOREA-PERF]:
    Stopping aksserver: MOOREA-PERF:aksserver
    Stopping srvmon: MOOREA-PERF:srvmon
  Stopping [MOOREA-SUPER-CA]:
    Stopping aksserver: MOOREA-SUPER-CA:aksserver
    Stopping srvmon: MOOREA-SUPER-CA:srvmon
Starting arkoon-amc server:
Starting [MOOREA-PERF]:
  Checking database [dbperf]: done
  Syncing IDPS profiles and rules in database: done
  Starting aksserver: MOOREA-PERF:aksserver
  Starting srvmon: MOOREA-PERF:srvmon
Creating cron config file: done
```

Note

To restart a single instance (for example 'amc-main') specify its name on the command line:

```
[root@amc-server root]# /etc/init.d/arkoon-amc restart amc-main
```

Note

The start-up of the administration tools' connection services is operated before the database check in order to manage the instance's appliances.

5.2. Connecting Arkoon tools to an AMC Instance

Connecting to an AMC server instance from the Arkoon Manager and Arkoon Monitoring tools requires an administrator certificate (ADMIN or ADMIN/RW) and uses the ports defined in the configuration.

5.3. Connecting a Fast360 Appliance to an AMC Instance

The connection from a Fast360 appliance to an AMC instance is configured on the appliance in `minarkconf` (Configuration / Master/Slave (Config) menu). The appliance must be configured as "slave".

This `minarkconf` option allows you to:

1. Specify the "slave" status for the Fast360 appliance.

To highlight the status required, use the keyboard arrows.

To activate your selection, press the space bar. When the highlighted option is activated, a cross is displayed between the option's square brackets.

- Specify the address of the AMC server in the dialog box which follows (admin from). If the AMC server can be accessed by multiple IP addresses, you can specify all of them by separating them with spaces.

Note

For more details on multi-appliances configuration, refer to the *Multi-Fast360* section in the *Fast360 Administration guide*.

Once connected to the server, the Fast360 appliance appears in the Arkoon Manager.


You need to configure the Fast360 appliance again before installing the configuration (for more information, refer to the *Fast360 Administration guide*).

5.4. Flushing a mySQL Database

Important

The MySQL database is used by the AMC server to store logs but it is not an AMC server component. MySQL databases administration is not performed by the AMC server, and the database administrator remains responsible for it.

The data can be cleared from each database (IP, Alert, SMTP relay, and HTTP relay) via Arkoon

Monitoring by clicking on : the data are cleared but not the database indexes.

In order to clear the data and the database indexes:

- Connect on the AMC server using the console.
- Execute the following commands:
 - Stop AMC service: `/etc/init.d/arkoon-amc stop`
 - Stop mysqld service: `/etc/init.d/mysqld stop`
 - Clear instance tables: `rm -rf /var/lib/mysql/<instanceDBName>/*`

Note

Replace <instanceDBName> by the name of the instance database for which you want to flush the logs.

- Start mysqld service: `/etc/init.d/mysqld start`
- Start AMC service: `/etc/init.d/arkoon-amc start`

The tables are recreated while the service restarts.

5.5. Restarting an AMC Service

To stop, start or restart an AMC service, you can browse to the **Maintenance/Diagnosis** window in Arkoon Monitoring.

You can also use the following command line with the `srvmon/akserver` services:

```
ARKOON_AMC_INSTANCE=<instance_name> /opt/arkoon/init.d/<service> [stop|start|restart]
```



5.6. Managing the Appliances Updates

The AMC server cannot be used as an update server for Fast360 appliances. However, you can launch modules or system updates for the appliances from the **Arkoon Monitoring Update** window.

To do so, you must select the appliances to update from the hierarchical view and then launch the update: the AMC requests the update to the appliances.

It is not possible to follow the update progress and result from the AMC Arkoon Monitoring.

For a system update, you must select the appliances sharing the same distribution.

Note

For a cluster, only the active appliance is updated. You must manually log on the second node to update it.



Chapter 6. Auditing the AMC Server

The `arkoon-amc` package has a diagnostic command which analyzes the status and configuration of the package. The following is checked:

- Package integrity (compared with a reference database contained within the package)
- Server status
- Validity of configured instances
 - Configuration validity
 - Connection with the database
 - Status of daemons

The server and AMC instances can generate alerts concerning their own operation which can be displayed from Arkoon Monitoring (Malfunction of a service, Management connection, Creation/Revocation of a certificate, etc.).

6.1. Diagnostic Command

To carry out a diagnostic from the command line:

```
root@vamc-masslave:~# /opt/arkoon/bin/amc-diag.sh
arkoon-amc package diag
-----
Version: 6.0-1303080137
Distrib: Debian lenny/sid
Package: arkoon_amc_6.0+1303080137

Checking package integrity: done (success)

Checking amc server status: started
Checking amc server license: found (S13.0004C - AMC-SERVER-MOOREA-6-0-1 - Unlimited)

Configured AMC instance(s): MOOREA-SUPER-CA MOOREA-PERF
Running AMC instance(s): MOOREA-PERF MOOREA-SUPER-CA

Instance 'MOOREA-SUPER-CA':
  Checking instance name: done
  Checking configuration: done
  Checking database: database not configured
  Status: running
    akserver          started [21258 21293 21294 21296 21298 21299 21300 21301 21304 21310]
    srvmon            started [21285 21302 21303]

Instance 'MOOREA-PERF':
  Checking instance name: done
  Checking configuration: done
  Checking database: done
  Status: running
    akserver          started [21446 21478 21482 21485 21493 21495 21496 21497 21498 22143 22201]
    srvmon            started [21473 21489 21494 21821]
```



6.2. Alerts

By default, the alerts are sent to the system logs using syslog with the name of the instance:

```
Mar  7 12:45:10 amc-server srvmon[28584]: ALERT - amc-instance:'arkoon'  
type:'Admin Connection' level:'None (Information)' descr:'Monitoring:  
10.10.192.34:58634' admin:'/C=FR/L=Lyon/O=Arkoon Network Security/OU=IP  
- MLA/CN=User Name'
```

If you have defined a database, the alerts issued by the AMC server are also stored in the database belonging to its instance.

6.3. Security Level of an AMC Instance

To know the security level of an AMC instance, enter the following command:

```
> . /opt/arkoon/bin/amc-env.sh
```

Then enter the command:

```
> akutils akcfg tree arkoon-ca.
```

The following results display:

```
algo-hash sha256  
key-numbits 4096  
cr1-days 3650
```

Chapter 7. Maintaining AMC Server

To maintain the AMC server :

- **Back up the AMC server data**
- **Restore the AMC server data**
- **Update the `arkoon-amc` package**
- **Remove the `arkoon-amc` package**

7.1. Backing up AMC Server Data

It is recommended to backup the AMC server data in case of a crash of the server hardware or operating system. The AMC server data is stored in the following directories:

- `/etc/arkoon-amc`
- `/var/arkoon-amc`
- `/var/lib/mysql`

Caution

The database stored in `/var/lib/mysql` may require a large amount of backup storage space.

7.1.1. Backing up All Configuration Files

Use the following command to backup the AMC server and all configured instances:

```
amc-backup
```

7.1.2. Backing up Certificate Authority only

Use the following command to backup the Certificate Authority for an instance:

```
tar czvf /tmp/CA_AMC.tgz /var/arkoon-amc/"instance_name"/arkoon-ca
```

7.1.3. Backing up Role Management Database only

Use the following command to backup the roles database for an instance:

```
cd /var/arkoon-amc/"instance_name"/
```

```
tar czvf /tmp/Access_Control_Database.tgz roleconfig roleconfig_history role_current
```

7.2. Restoring AMC Server Data

In order to restore an AMC server, you have to stop `arkoon-amc` and `mysql` services, and restore the backup up directory content in their original directories. Then, you only have to restart `mysql` and `arkoon-amc` services to have a working AMC server.

7.2.1. Restoring All Configuration Files

Use the following command to restore the server AMC configuration:

```
tar xzvf /tmp/AMC_full_backup.tgz -C /
```

7.2.2. Restoring Certificate Authority only

Use the following command to restore the CA of an instance:

```
tar xzvf /tmp/CA_AMC.tgz -C /
```

7.2.3. Restoring Role Management Database only

Use the following command to restore the roles database of an instance:

```
tar xzvf /tmp/Access_Control_Database.tgz -C /var/arkoon-amc/"instance_name"/
```

7.3. AMC Server update

The AMC Server update procedure can be generated via the Update and Migration Help tool, available from the Customer Area: <http://client.arkoon.net/>.

On page “Update and Migration Help”, select the following criteria to generate the procedure:

- Is your appliance connected to the Internet?: Connected or Disconnected
- What action do you wish to perform?: Update
- Current topology: An AMC server acts as configuration master
- Current architecture: AMC Server. Select the current version of your AMC server
- Target architecture: AMC Server



7.4. Removing arkoon-amc Package

To remove the `arkoon-amc` package, use the following command:

```
[root@amc-server root]# rpm -e arkoon-amc
Stopping arkoon-amc server:
  Stopping [amc-main]:
    Stopping akserver: amc-main:akserver
    Stopping amanaged: amc-main:amanaged
    Stopping srvmon: amc-main:srvmon
    Stopping akslave: amc-main:akslave
    Stopping akstatsd: amc-main:akstatsd
warning: /etc/arkoon-amc/config/amc-instances saved as /etc/arkoon-amc/config/amc-instances.rpmsave
```

The configuration files (`/etc/arkoon-amc`) and directories (`/var/arkoon-amc`) are not deleted when the package is removed. If you want to delete them, do so after the package has been removed:

```
[root@amc-server root]# rm -rf /etc/arkoon-amc /var/arkoon-amc
```

7.5. Optimizing MySQL databases

A script for indexing and optimizing MySQL databases can be launched in order to avoid databases indexes to become too large and to optimize access to logs with Arkoon Monitoring. It also enables to avoid server's hard drives to be saturated because of the size of databases. Regardless of the number of instances you have on your AMC server, the script performs indexation and optimization actions on each instance consecutively.

It is possible to choose one or more instances as a parameter in the command line.

To launch the script, enter `amc-myisamchk-optim-databases`.

Refer to the three examples:

Example 7.1. Automatic launch of the database maintenance script at regular intervals with Crontab (every day at 4.00 am)

```
0 4 * * * /opt/arkoon/bin/amc-myisamchk-optim-databases >/dev/null 2>&1
```

Example 7.2. Manual launch of the database maintenance script

```
/opt/arkoon/bin/amc-myisamchk-optim-databases
```

Example 7.3. Manual launch of the database maintenance script with argument

```
/opt/arkoon/bin/amc-myisamchk-optim-databases « instance name1 »
```

Note

If you have configured an automatic log archiving policy, we recommend you to configure the automatic launch of the database maintenance script a few hours after each archiving.



Chapter 8. Terminology

8.1. Terminology

This section introduces the terminology specific to the AMC architecture which is used throughout the document.

Administrator. Person who works on a Fast360 appliance or AMC server to initialize and configure them, install the security policies to be implemented and carry out monitoring and maintenance. In the documentation, these tasks are assumed to be carried out by a single person – the administrator. In practice, the various management tasks on a Fast360 system may be shared among several administrators.

AMC server. Server management and monitoring platform for Fast360 appliances on which the AMC platform, supplied as the `arkoon-amc` installation package, has been installed and configured. It manages and monitors one or more AMC clusters made up of Fast360 multiservices security appliances.

AMC cluster. Specified group of Fast360 appliances managed and monitored under the control of a given Certification Authority. A single configuration file stored on the AMC server is shared by the appliances in a cluster.

AMC instance. Software service on the AMC server responsible for controlling an AMC group. Each instance is configured and installed independently on the AMC server.

arkoon-amc. Installation package containing the software components required for the operation of the AMC server.

Global AMC instance. AMC instance which consolidates the information from multiple AMC instances. A global AMC instance allows a group of AMC clusters to be monitored.

GOR (Green – Orange – Red) status. Status of a Fast360 appliance. Green status indicates normal operation. Orange status corresponds to a warning (e.g. license about to expire). Red status means a critical problem (e.g. defective service on the appliance).

Management station. Workstation on which the Fast360 monitoring and management tools (Arkoon Manager and Arkoon Monitoring) are installed. These tools interface directly with a Fast360 appliance or an AMC instance to manage AMC clusters.



Appendix A. Migration cases

A.1. Migrating from an AMC server to a new AMC or VAMC server

In case you wish to change the machine of your AMC server or if you wish to switch from a physical server to a virtual server, the migration procedure can be generated via the Update and Migration Help tool, available from the Customer Area: <http://client.arkoon.net/>.

On page “Update and Migration Help”, select the following criteria to generate the procedure:

- Is your appliance connected to the Internet?: Connected or Disconnected
- What action do you wish to perform?: Hardware migration (or migration to AMC Server)
- Current topology: an AMC server acts as configuration master
- Current architecture: AMC Server. Select the current version of your AMC server
- Target architecture: AMC Server or Virtual AMC Server

A.2. Migrating the master role from the Fast360 appliance to an AMC server

The migration procedure of a master/slave architecture to an architecture with an AMC server can be generated via the Update and Migration Help tool, available from the Customer Area: <http://client.arkoon.net/>.

On page “Update and Migration Help”, select the following criteria to generate the procedure:

- Is your appliance connected to the Internet?: Connected or Disconnected
- What action do you wish to perform?: Hardware migration (or migration to AMC Server)
- Current topology: an appliance acts as configuration master
- Current architecture: select the model and current version of your master appliance
- Target architecture: AMC Server



A.3. Migrating from a standalone appliance to a slave appliance of a new AMC instance

The procedure can be generated via the Update and Migration Help tool, available from the Customer Area: <http://client.arkoon.net/>.

On page “Update and Migration Help”, select the following criteria to generate the procedure:

- Is your appliance connected to the Internet?: Connected or Disconnected
- What action do you wish to perform?: Hardware migration (or migration to AMC Server)
- Current topology: Standalone appliance
- Current architecture: select the model and current version of your appliance
- Target architecture: AMC Server

Appendix B. Deploying a CRL on all the appliances of an AMC instance

B.1. With an Arkoon PKI managed by the AMC instance

When you are connected to the AMC instance to manage your certificates (via `minamcconf` or Arkoon Manager), revoking a certificate enables the update of the CRL on the AMC instance and on all the appliances connected to the instance. If an appliance is not connected, the deployment of the CRL is delayed and the CRL will be installed the next time the appliance will connect.

Note

It is always possible to install the CRL via the menu **Advanced administration>Install PEM Certificate Revocation List file...** in Arkoon Manager, on one or several appliances.

B.2. With an external PKI

Use the menu **Advanced administration>Install PEM Certificate Revocation List file...** in Arkoon Manager so that the AMC instance and its appliances take into account the CRL of your external PKI.

B.3. Automatic retrieval of the CRL by a new appliance

When a new appliance connects to the AMC instance for the first time, it tries to retrieve automatically the AMC CRL:

- If the CRL comes from an Arkoon Certification Authority directly managed by the AMC instance, once the configuration of the appliance is finished (via `minarkconf`, **Master/Slave** menu), the appliance directly retrieves the CRL from the instance. There is nothing more to do.
- If the CRL comes from a Certification Authority managed by an external PKI:
 - If the key `arkoon-config : arkoon-amc.certificate.crl-trust-master = yes` is defined on the AMC server (default value), the AMC instance is allowed to send its CRL to the appliance, even if the instance is not a Certification Authority.
 - If the key `arkoon-config : arkoon-amc.certificate.crl-trust-master = no` is defined, the AMC instance does not send its CRL because it is reckoned that it is not a Certification Authority and that it does not have to provide a CRL it cannot manage. As a consequence, you must install manually the CRL on the appliance via the menu **Advanced administration>Install PEM Certificate Revocation List file...** in Arkoon Manager.



Appendix C. Configuration file

C.1. Configuration file for an instance example

This example shows how the configuration file for an instance should be written. The `include` line is mandatory. It includes into the configuration all the default parameters from the `/opt/arkoon/etc/arkoon-config` file shown in the following section. The default parameters may be redefined with new values.

```
# Arkoon Management Center (AMC) 'sample' configuration
include /opt/arkoon/etc/arkoon-config

arkoon-amc.instance-name = sample
arkoon-amc.user = root

arkoon-amc.certificate.pkcs12 = /etc/arkoon-amc/certs/cert_amc.p12
arkoon-amc.certificate.passwd = "my-secret-password"
arkoon-amc.certificate.crl = /var/arkoon-amc/<instance_name>/arkoon-ca/.pem

# enable amc server alerts to be logged inside database
arkoon-amc.db.enable = yes
arkoon-amc.db.database = amcdb
arkoon-amc.db.user = amc-server
arkoon-amc.db.password = "my-db-password"

# if this instance is the first using this database, activate nightly
# database exports and flush
arkoon-amc.akdbpurge.enable = yes
```

C.2. Configuration file to be included: arkoon-config

Using the `include` command to include the `/opt/arkoon/etc/arkoon-config` file in the instance configuration file initializes the default parameters.

You can open the file to see all the default parameters.



Appendix D. Saving regularly the appliances configuration of the AMC instance

D.1. Saving regularly the appliances configuration of the AMC instance

To regularly save the appliances configuration:

1. Launch minamcconf.
2. Select **2. Instances**, then choose the option **d. configure AMC**.
3. Click on **Select Instance**, then select **8. Slaves backup**.
4. Select the frequency and validate with <OK>.
5. Enter the starting time to backup the first slave and click <OK> to validate.

The backups are stored in: `/var/arkoon-amc/<instance_name>/configcard.backup/<FQDN_appliance>/`

Note

An alert per appliance will be generated on the AMC to indicate if the backup is successful or not.

Note

The configuration backup of a slave appliance is kept for a period equivalent to three times the selected backup frequency. It is then overwritten with the new backup. We advise to copy the backups to an external storage support (NAS, SAN, etc.).



