Serveur AMC 6.0

Guide d'administration

Édition Française | Version 6.0 | Décembre 2015

ARKOON
NETWORK SECURITY

Serveur AMC 6.0

Guide d'administration

Version 6.0

Publié en Décembre 2015

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

Support Technique.

Pour les dernières mises à jour ou pour contacter le Support Technique d'Arkoon,
visitez le site web du Support Technique d'Arkoon : http://client.arkoon.net

Table des matières

Liste des exemples

Préface

1. A propos de ce document

Ce document décrit l'installation, la configuration et la maintenance du logiciel AMC (Arkoon Management Center).

2. A propos d'AMC

L'architecture AMC (Arkoon Management Center) permet la gestion centralisée des appliances Fast360. Chaque cluster AMC est composé de plusieurs appliances Fast360 connectées à un serveur AMC.

3. Public concerné

Ce guide est destiné aux administrateurs Linux expérimentés ayant des connaissances sur les appliances de sécurité Arkoon.

Chapitre 1. Introduction

1.1. Prérequis

Le package d'installation `arkoon-amc` nécessite les prérequis matériel suivants :

- Version 5 ou 6 de RedHat Linux ES mode 32/64 bits. La version 6.x la plus récente est recommandée (http://www.redhat.com).
- Version 5 ou 6 de CentOS Linux 32/64 bits. La version 6.x la plus récente est recommandée (http://www.centos.org).
- Processeur Intel Xeon 3GHz (Dual Core).
- 4 Go de RAM.
- Base de données MySQL (http://www.mysql.com).
- Disque dur de 300 Go (disque SAS recommandé).

> **Note**
> Le serveur AMC utilise essentiellement la partition /var pour la base de données des journaux, les configurations et la communication avec les esclaves; veillez donc à réserver une place conséquente sur cette partition (une centaine de gigaoctets environ).

Ces informations correspondent au contexte spécifique suivant :

- 1 instance AMC.
- 5 à 10 appliances standalone ou cluster
- 200 Mo de journaux par appliance et par jour.
- 3 jours de journaux dans la base de données.
- 365 jours d'archivage (période légale pour certains pays, notamment la France).

> **Note**
> La base de données MySQL est utilisée par le serveur AMC pour stocker les journaux mais ce n'est pas un composant du serveur AMC. L'administration et le maintien des bases de données MySQL n'est pas effectuée par le serveur AMC et l'administrateur de la base de données en reste responsable.

> **Note**
> Le composant `crond` doit être installé sur le serveur AMC pour faire fonctionner certaines fonctionnalités. Seul le répertoire `/etc/cron.d` ainsi que les fichiers appropriés sont créés lors de l'installation du package `arkoon-amc`.

1.2. Architecture

Deux types d'architecture AMC peuvent être mises en place :

- Mono-instance : un cluster AMC contrôle une seule instance.
- Multi-instances : plusieurs instances Fast360 peuvent être contrôlés par un serveur AMC donné.

Une instance AMC unique correspond à chaque cluster d'appliance configuré par l'administrateur. Les appliances et l'administrateur accèdent au serveur AMC en utilisant les outils Arkoon via des connexions réseau sécurisées avec le protocole SSL (Secure Socket Layer) V3 sur la base de certificats X.509 de la même autorité de certification.

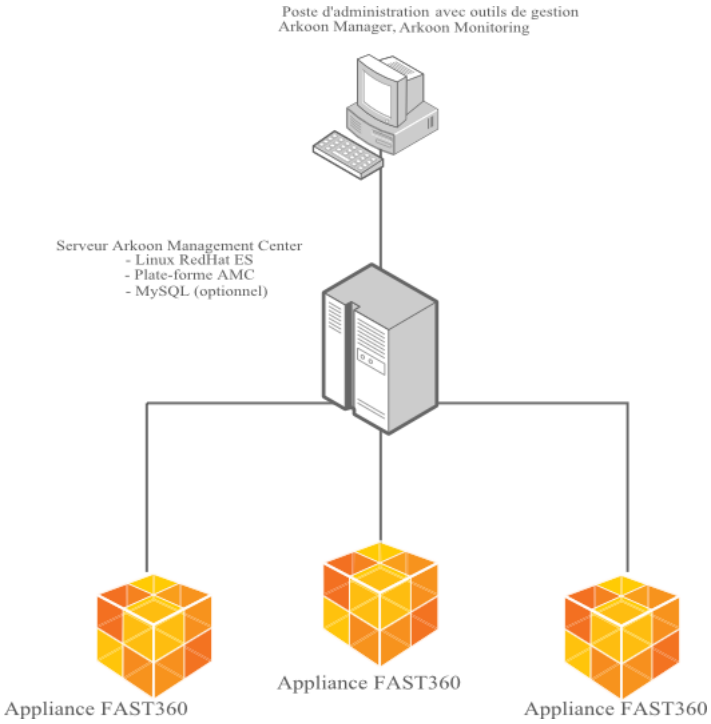
1.2.1. Architecture mono-instance

Les appliances Fast360 sont connectées au serveur AMC.

L'administrateur peut effectuer les opérations suivantes à partir du poste d'administration :

- Connecter Arkoon Monitoring au serveur AMC pour surveiller le statut VOR (Vert Orange Rouge) des appliances et accéder à leurs journaux : alertes, journaux IP et IDPS, relais HTTP et SMTP.
- Connecter Arkoon Monitoring à une appliance pour surveiller un paramètre particulier.
- Connecter Arkoon Manager à l'instance créée sur le serveur AMC pour configurer la politique de sécurité du cluster (politique commune à toutes les appliances Fast360 du cluster).

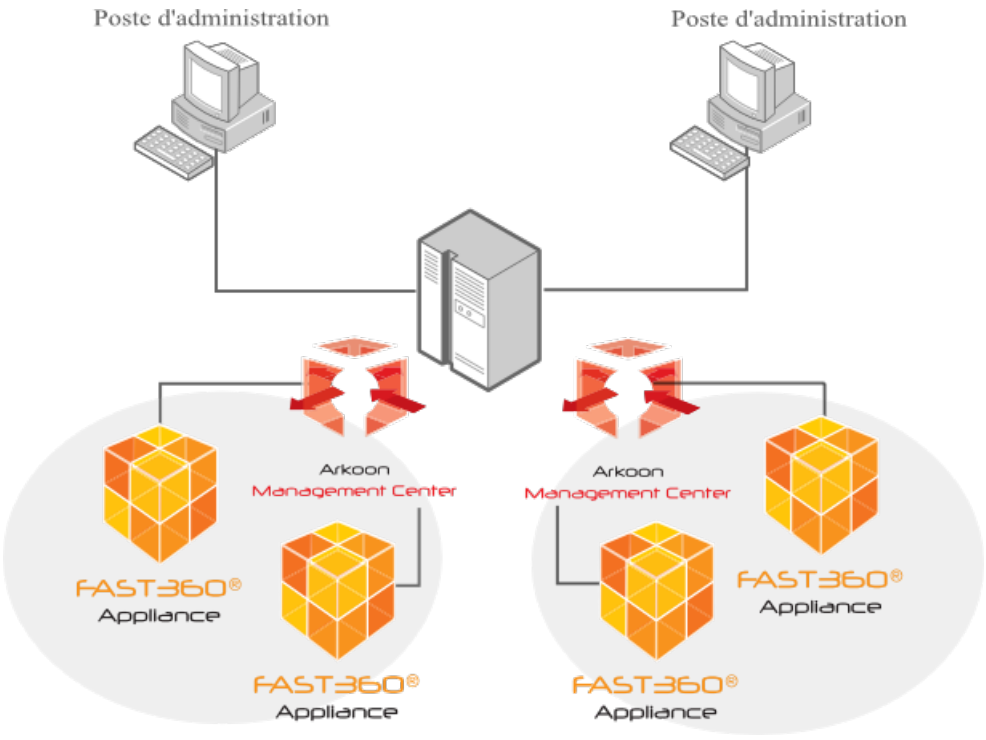
Le graphique suivant présente un exemple d'architecture mono-instance avec trois appliances Fast360 gérées de manière centralisée :



1.2.2. Architecture multi-instances

Une architecture multi-instances permet à l'administrateur de contrôler plusieurs clusters d'appliances, chacun d'entre eux ayant sa propre politique de sécurité. Dans ce cas, chaque cluster correspond à une instance AMC sur le serveur AMC.

- Chaque instance AMC gère la politique de sécurité de son cluster de manière indépendante.
- Plusieurs instances AMC peuvent partager une unique base de données de journaux mais ce n'est pas obligatoire. Si les instances AMC peuvent partager une base de données unique, tous les journaux sont disponibles directement via Arkoon Monitoring.
- L'administrateur peut créer une gestion globale des instances AMC. Au lieu de contrôler les appliances, elles accèdent au statut VOR des clusters multiples et centralisent les journaux dans une base de données précise.



Le graphique ci-dessus présente un exemple d'architecture multi-instances avec quatre appliances Fast360 gérées de manière centralisée via deux clusters contenant deux appliances. Aucune instance globale n'a été définie.

Chapitre 2. Installation

Avant d'installer le serveur AMC, vous devez vérifier les prérequis décrits dans la Section 1.1, « Prérequis ».

Pour installer le serveur AMC :

1. **Installez le serveur, le matériel et le système.**
2. **Installez le package arkoon-amc.**
3. **Installez la licence AMC.**
4. **Installez le serveur MySQL pour permettre la centralisation des journaux de l'appliance (cette dernière étape étant optionnelle).**

2.1. Installation du serveur

Le serveur nécessite RedHat ES ou CentOS 5.8 ou 6.4.

Pour vérifier que le serveur est installé avec RedHat ES 5.8 par exemple, saisissez :

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

Note
L'activation de SELinux peut entraîner un dysfonctionnement du serveur AMC. Pour prévenir ce comportement, configurez SELinux en mode permissif. Pour ce faire, modifiez le fichier de configuration `"/etc/selinux/config"` et utilisez la commande `setenforce 0`.

2.2. Installation du serveur MySQL

L'installation du serveur MySQL permet l'activation de la fonctionnalité de centralisation de journaux de l'appliance sur le serveur AMC. L'utilisation de cette fonctionnalité est fortement recommandée pour la surveillance globale des données de journaux des appliances.

La base de données MySQL peut être installée sur le serveur AMC ou sur un serveur distant.

Pour installer le serveur MySQL sur le serveur AMC :

Note
Le package mysql-server n'est pas présent sur le CD RedHat ES 5.0 mais il est disponible gratuitement depuis le site RedHat (http://www.redhat.com) ou sur le réseau RedHat (https://rhn.redhat.com/).

1. Installez le package du serveur MySQL :

   ```
   yum install mysql-server
   ```

   En cas de problème, installez le package avec la commande suivante :

```
[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. Configurez la base de données pour qu'elle démarre automatiquement au démarrage du serveur :

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

3. Démarrez la base de données :

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

4. Configurez le serveur mySQL :

    1. Laissez le mot de passe mySQL vide :

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

    2. Vérifiez la connexion à mySQL :

    ```
    #mysql -u root
    ```

2.3. Installation de dépendances pour les serveurs 64 bits

Pour les serveurs 64 bits, il est nécessaire d'installer les dépendances suivantes. Dans tous les cas, après l'installation des packages décrits ci-dessous, installez :

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

Serveurs sous RedHat ES 5/6 ou CentOS 5/6

Installez les packages suivants :

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

Par défaut, CentOS configure un firewall "iptables" qui bloque l'accès au serveur AMC. Vous pouvez l'adapter à votre usage ou le désactiver définitivement :

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

2.4. Installation du package arkoon-amc

Installez le package arkoon-amc :

- pour RedHat et CentOS 5 32/64 bits, utilisez le package

  `arkoon-amc-6.0-xxxxxx_xxxx.el5.i386.rpm`
- pour RedHat et CentOS 6 32/64 bits, utilisez le package

  `arkoon-amc-6.0-xxxxxx_xxxx.el6.i386.rpm`

Entrez la commande :

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

Remplacez x dans `elx` par 5 ou 6 selon la version de RedHat ou CentOS utilisée.

Le serveur AMC ne démarre pas après l'installation puisque vous n'avez pas encore configuré d'instance AMC.

Chapitre 3. Configuration du serveur AMC avec Minamcconf

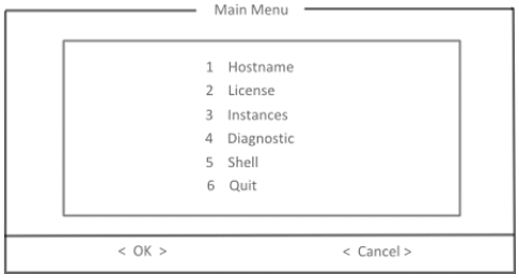
L'outil Minamcconf aide l'administrateur à configurer le serveur AMC mais également à créer et configurer des instances.

L'outil Minamcconf est disponible sur le serveur AMC via `minamcconf`.

3.1. Génération de la licence

La licence AMC est basée sur l'adresse IP principale du serveur AMC sur laquelle les appliances Arkoon sont connectées. Par exemple, si les connexions sont faites sur eth0 (ou un alias de eth0), l'adresse IP doit être celle de eth0.

Au démarrage, la fenêtre suivante s'affiche :



1. Sélectionnez `Hostname` pour attribuer un nom et sélectionnez `<OK>` pour valider.
2. Sélectionnez `License` puis `Request license`.
3. Saisissez le nom de la licence, les adresses IP séparées par un espace et le nom du fichier de requête de licence.
4. Validez et connectez-vous à http://license.arkoon.net avec le fichier de requête et votre clé de licence pour enregistrer votre produit et récupérer votre fichier de licence.

Important

Le nombre d'appliances que vous pouvez connecter à l'ensemble de vos instances dépend de la licence que vous avez achetée.

Si aucune licence n'est installée, il est possible de gérer des instances de cinq appliances au maximum. Dans ce cas, l'information suivante est affichée au démarrage d'une instance :

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

Si plus de cinq appliances se connectent à une instance d'un serveur AMC sans licence, la connexion de la nouvelle appliance est refusée :

- un journal de ce type est ajouté au fichier `/var/log/messages` de l'AMC :

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

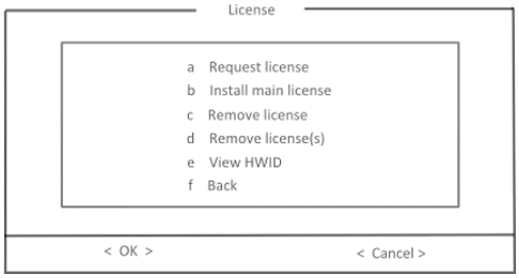
- un journal de ce type est ajouté au fichier `/var/log/messages` de l'appliance refusée :

```
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. Installation de la licence

Pour installer la licence :

1. Copiez le fichier de licence sur le serveur AMC.
2. Sélectionnez `Install main license` puis validez avec `<OK>`.



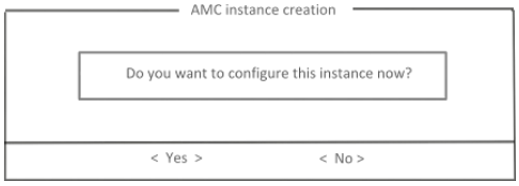
3. Saisissez le chemin pour récupérer le fichier de licence et validez avec `<OK>` .

3.3. Création d'une instance AMC

1. Sélectionnez `Instances` à partir du menu principal puis choisissez `Create AMC instance`.
2. Saisissez un nom pour l'instance à créer et validez avec `<OK>`.

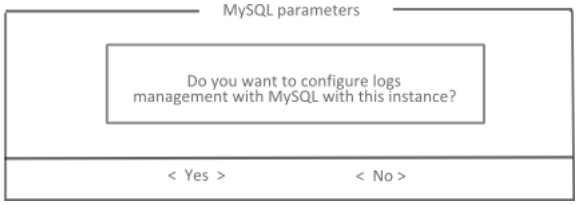
   Note
   Seuls les caractères suivants sont valides :`0-9`, `a-z`, `A-Z`, `_` and `-`

   La fenêtre suivante s'affiche :



3. Validez avec `<Yes>`.

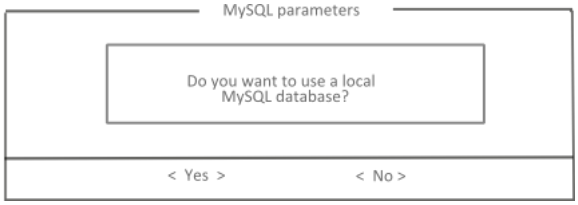
   La fenêtre suivante s'affiche :



4. Cliquez sur `<Yes>` puis poursuivez la procédure décrite à la Section 3.3.1, « Configuration des paramètres MySQL ».

3.3.1. Configuration des paramètres MySQL

La fenêtre suivante s'affiche :



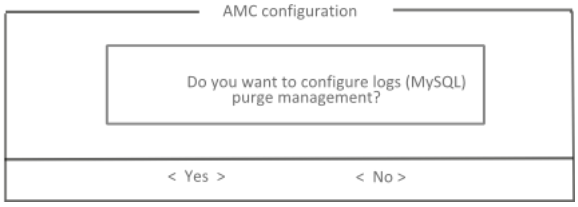
- Si vous validez avec `<Yes>` , les champs **IP** et **Port** ne sont pas nécessaires.
- Si vous validez avec `<No>`, vous devez remplir les champs suivants.
  - IP
  - Port
  - Nom de la base distante
  - Utilisateur
  - Mot de passe (optionnel)

1. Dans le cas où vous utilisez une base locale (cas le plus fréquent), vous devez ensuite entrez le nom de la base de données MySQL pour gérer les journaux et les alertes puis cliquez sur `<OK>`.
2. Fournissez le nom de l'utilisateur de la base de données et cliquez sur`<OK>`.
3. Cliquez sur `<OK>` pour entrez un mot de passe pour l'utilisateur puis validez avec `<OK>`.

   La base de données MySQL a été correctement créée.

3.3.2. Configuration de la purge des journaux

La fenêtre suivante s'affiche :



1. Cliquez sur `<Yes>`.
2. Entrez la périodicité de la purge puis cliquez sur `<OK>`.
3. Entrez le nombre de jours de stockage des données puis cliquez sur `<OK>`.

3.3.3. Configuration des paramètres de l'autorité de certification

Important
Par défaut, les appliances Fast360 initialisent des autorités de certification conformes à la réglementation RGS, *Annexe B1 Mécanismes cryptographiques* (http://references.modernisation.gouv.fr/sites/default/files/RGS_Mecanismes_cryptographiques_v1_20.pdf), c'est-à-dire avec une taille de clé de 4096 bits et l'algorithme de hachage SHA-256.
Cependant, dans le cadre d'une migration depuis une version 5.x de Fast360, les paramètres de CA d'une instance déjà créée ne changent pas et celle-ci reste fonctionnelle. Si vous souhaitez disposer de ces nouveaux paramètres à la suite d'une telle migration, il est nécessaire de recréer une nouvelle CA pour l'instance concernée. Cette opération nécessite alors de re-certifier les appliances, les administrateurs, les utilisateurs de l'agent Arkoon Authentification et les utilisateurs de VPN nomades.

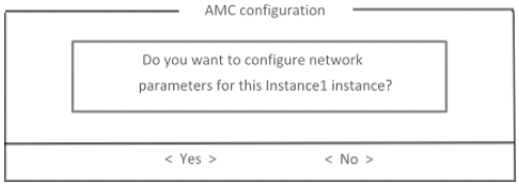
Pour configurer les paramètres de l'autorité de certification :

1. Saisissez les paramètres requis et validez avec `<OK>` pour terminer la configuration et accéder à la fenêtre `Certification Authority`.
2. Sélectionnez `<Yes>` à partir de la fenêtre `Certification Authority` .
3. Saisissez un mot de passe et validez avec `<OK>`.
4. Remplissez les champs requis et validez avec `<OK>`.

   L'autorité de certification est créée. Vous devez maintenant créer le certificat :
5. Sélectionnez `<Yes>` pour créer le certificat puis remplissez les champs requis.

3.3.4. Configuration des paramètres réseau

Lorsque la création est terminée, l'outil Mimamcconf affiche la fenêtre suivante pour configurer les paramètres réseau pour l'instance créée :



1. Validez avec `<Yes>`.
2. Saisissez l'adresse IP et validez avec `<OK>`.

   Les paramètres suivants sont requis :

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

   Note
   Vous devez choisir un port disponible.

3.4. Création d'une Super instance AMC

Une instance globale (ou Super instance) de surveillance surveille le statut des appliances sur des clusters AMC multiples à partir d'une connexion Arkoon Monitoring. Une instance globale de surveillance surveille le statut VOR des appliances Fast360 sur les cluster AMC multiples à partir d'une connexion Arkoon Monitoring.

Pour créer une Super instance AMC, naviguez jusqu'au menu principal et sélectionnez `Create Super AMC instance`. Les premières étapes de la procédure sont équivalentes à celles de la procédure de la création d'instance AMC (voir Section 3.3, « Création d'une instance AMC »).

La dernière étape nécessite que vous spécifiez l'instance AMC gérée par la Super instance AMC.

Note
Le port Arkoon manager est configuré mais pas utilisé.

Important
Pour accéder et gérer les journaux des instances avec Arkoon Monitoring, la base de données de la Super instance AMC doit être la même que la base de données des instances.

Chapitre 4. Configuration manuelle d'un serveur AMC

Ce chapitre explique comment configurer le serveur AMC manuellement.

4.1. Présentation

Le serveur AMC est configuré avec l'outil minamcconf. Ce chapitre décrit comment configurer le serveur AMC sans minamcconf.

La configuration du serveur AMC est contenue dans le fichier principal de configuration `/etc/arkoon-amc/config/amc-instances` et un fichier de configuration par instance `/etc/arkoon-amc/config/<instance_name>`.

Pour configurer AMC :

1. Créez une instance AMC.
2. Créez une autorité de certification (CA), si nécessaire.
3. Installez le certificat pour l'instance.

   Note
   Les étapes suivantes dépendent des fonctionnalités utilisées et sont optionnelles.
4. Configurez la centralisation des journaux.
5. Configurez la notification des journaux système.

   Note
   Pour une architecture multi-instances, vous pouvez configurer une instance globale pour surveiller les instances multiples à partir d'Arkoon Monitoring.
6. Configurez les paramètres réseau.
7. Configurez une instance de surveillance globale.

4.2. Création d'une instance AMC

Pour créer une instance AMC :

1. Choisissez un identifiant d'instance unique.

   Cet identifiant est utilisé pour se référer à l'instance dans les fichiers de configuration et les traces d'audit.

   Attention
   L'identifiant d'une instance est limité à 16 caractères et doit uniquement contenir les caractères 0-9, a-z, A-Z, '_' et '-'. Par exemple “amc-main”.

2. Créez un fichier de configuration pour l'instance.

   Le nom du fichier créé doit être le même que le nom de l'instance.

   Placez-le dans le dossier `/etc/arkoon-amc/config/`. Il doit au moins inclure le fichier de configuration par défaut `/opt/arkoon/etc/arkoon-config` et définir le paramètre `arkoon-amc.instance-name` avec le nom de l'instance :

   ```
   # 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
   Le fichier de configuration par défaut `/opt/arkoon/etc/arkoon-config` ne contient pas de certificat ou de base de données. Il est inclus au fichier de configuration pour chaque instance et ses paramètres peuvent être modifiés. Ce fichier est fourni dans l'annexe.
   Par exemple, un fichier nommé “sample” et contenant la configuration décrite dans ce document est fourni avec le package amc-server. Ce fichier est fourni dans la Section C.1, « Fichier de configuration pour un exemple d'instance ».

   Attention
   Le fichier de configuration contient les mots de passe protégeant les fichiers de certificat en clair. Protégez sa sécurité en restreignant les droits Unix du fichier.

3. Ajoutez la nouvelle instance AMC à la liste des instances configurées.

   Le fichier `/etc/arkoon-amc/config/amc-instances` contient la liste des instances configurées avec les noms des instances séparés par des espaces :

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

4. Redémarrez le service `arkoon-amc`.

   Une fois installé et configuré, le service arkoon-amc est lancé automatiquement au démarrage de la machine et s'interrompt à l'arrêt de la machine ou au redémarrage. Il est possible de forcer le démarrage en utilisant la commande suivante :

```
[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 amanagerd: no certificate defined
    Starting srvmon: no certificate defined
    Starting akslave: no certificate defined
    Starting akstatsd: no certificate defined
  Creating cron config file: done
```

A cette étape de la configuration, la commande de démarrage montre qu'aucune base de données de journaux n'a été configurée pour l'instance. De plus, aucun certificat n'a été défini pour permettre aux services de gestion et de surveillance de communiquer avec les appliances Fast360 et le poste d'administration.

Pour redémarrer le service `arkoon-amc`, uniquement pour l'instance “amc-instance”, utilisez la syntaxe suivante :

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

4.3. Création d'une autorité de certification

Les appliances et l'administrateur accèdent à l'instance du serveur AMC grâce aux outils Arkoon et par des connexions réseau sécurisées avec le protocole SSL (Secure Socket Layer) V3 sur la base de certificats X.509 et à partir de l'autorité de certification.

Chaque instance AMC dépend d'une autorité de certification qui peut-être créée spécifiquement pour l'instance sur le serveur AMC. L'instance peut également dépendre d'une autorité de certification prédéfinie. Si c'est le cas, suivez directement les instructions pour l'installation du certificat d'instance.

L'autorité de certification dont dépend l'instance AMC, est utilisée pour créer les certificats associés avec :

- l'instance AMC.
- une instance AMC différente.
- une Fast360.
- un administrateur.
- un utilisateur.

Créez l'autorité de certification avec la ligne de commande suivante :

```
[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>]
```

où, en général, **DN-O** est le nom de l'entreprise représentée par l'autorité de certification, **DN-OU** est le département au sein de l'entreprise, **DN-L** la ville et **DN-C** le code pays (par exemple FR). **CA-PEM-PHRASE** est la passphrase (mot de passe) protégeant l'accès à l'autorité de certification.

Attention
Le mot de passe étant fourni dans une commande shell, il est possible que vous deviez utiliser un caractère d'échappement avant les caractères réservés par le shell (tel que *, !, >, &, etc.).

Choisissez des mots de passe suffisamment complexes et gardez-les à un emplacement sécurisé (évitez les post-it ou les fichiers non-protégés).

```
[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/crl.pem)...ok
CA Initialization...ok
```

Un certificat FIREWALL doit être créé pour l'instance AMC et pour chaque appliance connectée à l'instance. Un certificat ADMINRW doit être créé pour l'administrateur de l'instance.

Note

Les certificats de l'appliance doivent être importés sur chaque appliance à connecter à l'instance. Reportez-vous au *Guide d'administration* de l'appliance Fast360 pour cette procédure. Les appliances en mode HA (Haute disponibilité) seront configurées avec un certificat unique.

La syntaxe générale de la commande à créer est la suivante :

```
[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
```

En plus des paramètres semblables à ceux utilisés pour initialiser l'autorité de certification, DAYS est le nombre de jours pour lesquels le certificat est valide, PKCS12-FILE est le nom du fichier où est stocké le certificat et PKCS12-PASSWD est le mot de passe protégeant le fichier PKCS#12.

Attention

La génération d'un certificat au format PKCS#12 nécessite un mot de passe sécurisé pour protéger le certificat et pour que le fichier soit stocké dans un lieu sûr. Le fichier PKCS#12 généré contient des informations strictement confidentielles telles que la clé privée utilisée pour l'authentification et la négociation des connexions SSL sécurisées. Le certificat doit être révoqué s'il est divulgué à un tiers.

```
[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.f1wC7n
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

Une fois les certificats créés pour l'instance AMC et l'administrateur, de nouveaux certificats peuvent être créés en utilisant l'outil Arkoon Manager.
Pour la gestion des certificats et des rôles de l'administrateur, reportez-vous à la Section 4.5, « Initialisation des droits d'administration ».

Note

Pour modifier la phrase PEM de votre autorité de certification :

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

4.4. Installation d'un certificat pour l'instance

Une instance AMC doit avoir un certificat FIREWALL pour établir les connexions SSL sécurisées avec les appliances Fast360 et le poste d'administration. Les différents services d'une instance ne démarrent pas sans certificat.

Le certificat doit avoir les caractéristiques suivantes :

- Extension X509v3 : Certificat Firewall Fast360

  L'extension X509v3 est fixée en créant le certificat à partir d'une appliance Fast360 ou du serveur AMC avec FIREWALL. Si une Public Key Infrastructure (PKI) est utilisée, l'extension suivante doit être ajoutée

au certificat : `iso.org.dod.internet.private.enterprise.arkoon.sslcom.akCertUsage (1.3.6.1.4.1.8628.2.1)` avec la valeur 0x12.

- Package PKCS#12

  Le certificat X509, la clé privée et le certificat d'autorité de certification publiant le certificat doivent être stockés dans un package PKCS#12.

  Attention
  La génération d'un certificat au format PKCS#12 nécessite un mot de passe sécurisé pour protéger le certificat. Le fichier doit être stocké dans un endroit sûr. Le fichier PKCS#12 généré contient des informations strictement confidentielles comme par exemple la clef privée utilisée pour l'authentification et la négociation des connections sécurisées SSL. Si divulgué à un tiers, le certificat doit être révoqué.

Le fichier PKCS#12 et le CRL (Certificate Revocation List) associé (si présent) sont configurés de la façon suivante dans le fichier de configuration de l'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
```

Attention
Le fichier contient le mot de passe du fichier PKCS#12. Par conséquent, il doit être protégé et son accès limité, par exemple en attribuant des droits Unix restreints comme `600/root/root`.

Vous devez ensuite redémarrer le service `arkoon-amc` pour que les modifications soient prises en compte.

4.5. Initialisation des droits d'administration

Pour administrer à distance une instance d'un serveur AMC en utilisant les applications Arkoon, l'administrateur a besoin d'un certificat signé par l'Autorité de certification de l'instance et les rôles d'administration doivent être associés à ce certificat.

La base de données de l'instance est d'abord initialisée à partir de l'interface de lignes de commande en associant le rôle **Toutes permissions** au certificat de gestion.

Note
L'administrateur dont le certificat est fourni lors de cette procédure possède toutes les permissions d'administration et peut réaliser toute opération sur un instance à partir des outils Arkoon. Cet administrateur est autorisé à définir les autorisations d'administration aux nouveaux administrateurs.

1. Copiez le certificat de l'administrateur principal au format PEM sur le serveur AMC.
2. Saisissez la commande suivante :

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

   Le certificat a maintenant toutes les permissions lorsque vous vous connectez à Arkoon Manager.

Par exemple, sur une instance avec sa propre autorité de certification et un certificat d'administrateur en 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. Configuration de la centralisation des journaux

Cette configuration est optionnelle. Si vous souhaitez l'activer, le serveur de la base de données doit au préalable avoir été installé de la façon décrite ci-dessous.

La centralisation des journaux pour un cluster AMC nécessite que la base de données de l'instance associée soit configurée. Dans une architecture multi-instances, des instances multiples peuvent partager la même base de données.

L'exemple ci-dessous explique comment initialiser une base de données `amcdb`, accessible à l'utilisateur `amc-server` (mot de passe `amc-password`) :

Note
L'utilisateur est spécifique à la base de données MySQL et il n'est pas nécessairement un utilisateur système.

```
[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
```

Pour associer la base de données à l'instance AMC, ajoutez les lignes suivantes au fichier de configuration de l'instance :

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

Par exemple, pour installer la base de données sur un serveur distant à l'adresse IP `192.168.1.20` sur le port `3306`, ajoutez les lignes suivantes au fichier de configuration de l'instance :

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

L'instance AMC stocke les alertes publiées dans la base de données des journaux.

Un mécanisme de purge (semblable à celui des appliances Fast360) est disponible pour contrôler la taille de la base de données. Par défaut, ce mécanisme est désactivé. Activez-le de la façon suivante :

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

Attention
Dans une architecture multi-instances, les instances multiples peuvent partager la même base de données de journaux. Le mécanisme de purge doit uniquement être activé sur l'une des instances AMC.

Par défaut, les journaux de moins de 30 jours sont conservés dans la base de données. Une modification est possible par l'ajout de la ligne suivante au fichier de configuration de l'instance :

```
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
```

De plus, les journaux sont sauvegardés 20 jours supplémentaires. Pour changer cette durée de conservation, modifiez la valeur des paramètres suivants :

- 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

Le mécanisme de purge est déclenché chaque jour à 4 heures du matin. Cet horaire est modifiable de la façon suivante :

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

Redémarrez le service `arkoon-amc service` pour que les modifications soient prises en compte et pour initialiser la base de données :

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

4.7. Configuration des journaux système

Par défaut, les journaux système ne sont pas renvoyés en temps réel par une instance à Arkoon Monitoring. Si vous souhaitez envoyer les journaux système en temps réel, vous devez créer un fichier FIFO (First In, First Out) puis configurer syslog et l'instance AMC pour l'utiliser :

1. Créez un fichier FIFO :

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

2. Changez l'appartenance du fichier FIFO (nécessaire si l'instance AMC ne fonctionne pas en root). Dans cet exemple, l'instance AMC utilise les privilèges de l'utilisateur “arkoon” :

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

3. Configurez syslog pour utiliser le fichier FIFO.

   Pour cela, ajoutez la ligne ci-dessous au fichier `/etc/syslog.conf`

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

4. Configurez l'instance pour utiliser le fichier FIFO.

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

   Les services syslog et arkoon-amc doivent être redémarrés pour que les modifications soient prises en compte.

5. Redémarrez le service syslog :

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

6. Redémarrez le service arkoon-amc :

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

4.8. Configuration des paramètres réseau

Par défaut, les services d'instance AMC écoutent sur toutes les adresses IP serveur (`0.0.0.0`) et sur les ports TCP par défaut : `1750` (Administration, `amanagerd`), `1751` (Supervision, `srvmon`), `1754` (Appliances Arkoon, `akslave`) et `1759` (Arkoon Super Server sur SSL, `akserver-over-ssl`).

Pour que les instances AMC multiples cohabitent sur le même serveur, cette configuration par défaut doit être modifiée de sorte que chaque instance utilise des ports et des adresses IP distincts.

1. Configurez l'adresse IP pour écouter sur le fichier de configuration de l'AMC.

   Par exemple :

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

2. Configurez les ports TCP dans le fichier de configuration de l'instance AMC. Par exemple :

   ```
   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
   ```

3. Redémarrez le service `arkoon-amc` pour que les modifications soient prises en compte.

4.9. Configuration d'une instance globale de surveillance

Une instance globale de surveillance surveille le statut des appliances Fast360 sur des clusters AMC multiples à partir d'une connexion Arkoon Monitoring. Une instance globale de surveillance surveille le statut VOR des appliances Fast360 sur les cluster AMC multiples à partir d'une connexion Arkoon Monitoring.

Pour la configuration, spécifiez les paramètres réseau de l'instance globale ainsi que les paramètres des instances surveillées dans le fichier de configuration pour l'instance globale :

```
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
Dans cet exemple, `france`, `usa`, `japan` et `germany` sont les noms des instances surveillées. La numérotation utilisée n'a pas de sens fonctionnel et elle uniquement utilisée pour faire la distinction entre les instances.

Si les instances surveillées ne sont pas démarrées par le même utilisateur, l'utilisateur spécifié pour l'instance globale de surveillance doit avoir le droit d'accéder aux fichiers utilisateur de ces instances. Reportez-vous à la documentation RedHat pour les instructions sur le changement des droits d'accès.

Redémarrez le service `arkoon-amc` pour que les modifications soient prises en compte :

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

Note
Pour que la Super instance accède au journal de l'instance, vous devez configurer la même base de données dans la Super instance que pour n'importe quelle autre instance. Tous les journaux sont ensuite stockés dans la même base de données.

4.10. Utilisation des multi-contrôleurs de domaine

Dans le cas où vous souhaitez avoir plusieurs contrôleurs de domaine, il vous suffit de tous les lister dans la liste des serveurs d'authentification, en précisant toujours le contrôleur de domaine principal. Le multi-contrôleurs de domaine est uniquement compatible avec NTLM et Kerberos, mais peut lister plusieurs serveurs d'authentification LDAP dans la liste des serveurs d'authentification.

Chapitre 5. Utilisation du serveur AMC

5.1. Démarrage et arrêt

Une fois installé et configuré, le service `arkoon-amc` démarre automatiquement au démarrage de la machine et s'arrête lorsque la machine est arrêtée ou redémarrée.

Pour qu'une modification de configuration soit prise en compte, le service `arkoon-amc` doit être redémarré en utilisant la commande suivante :

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

Note
Pour redémarrer une instance (par exemple “amc-main”), spécifiez son nom dans la ligne de commande :
`[root@amc-server root]# /etc/init.d/arkoon-amc restart amc-main`

Note
Le démarrage des services de connexion des outils d'administration est réalisé avant la vérification des bases de données. Cela permet d'administrer les appliances de l'instance.

5.2. Connexion des outils Arkoon à une instance AMC

La connexion à une instance de serveur AMC à partir des outils Arkoon Manager et Arkoon Monitoring nécessite un certificat administrateur (ADMIN ou ADMIN/RW) et utilise les ports définis dans la configuration.

5.3. Connexion d'une appliance Fast360 à une instance AMC

La connexion sur une instance à partir d'une appliance Fast360 est configurée dans minarkconf (menu Configuration / Master/Slave (Config)). L'appliance doit être configurée en tant qu' “esclave”.

Cette option minarkconf vous permet de :

1. spécifier le statut d'”esclave” pour l'appliance Fast360.

   Pour souligner le statut requis, utilisez les flèches du clavier.

Pour activer votre sélection, appuyez sur la barre d'espace. Lorsque l'option soulignée est activée, une croix s'affiche entre crochets.

2. spécifier l'adresse du serveur AMC dans la boîte de dialogue qui suit (admin from). Si le serveur AMC est accessible par des adresses IP multiples, vous pouvez toutes les spécifier en les séparant par des espaces.

Note
Pour plus de détails sur la configuration multi-appliances, reportez-vous au *Guide d'administration* de l'appliance Fast360.

Une fois connectée au serveur, l'appliance Fast360 apparaît dans Arkoon Manager.

Vous devez à nouveau configurer l'appliance Fast360 avant d'installer la configuration (reportez-vous au *Guide d'administration* de l'appliance Fast360 pour plus de détails).

5.4. Flush de la base de données mySQL

Important
La base de données MySQL est utilisée par le serveur AMC pour stocker les journaux mais ce n'est pas un composant du serveur AMC. L'administration des bases de données MySQL n'est pas réalisée par le serveur AMC et l'administrateur de la base de données en est responsable.

Les données peuvent être nettoyées de chaque base de données (IP, alerte, relais SMTP et relais HTTP) via Arkoon Monitoring en cliquant sur  . Les données sont nettoyées mais pas les index de la bases de données.

Pour nettoyer les données et les index de la base de données :

- Connectez-vous au serveur AMC en utilisant la console.
- Exécutez les commandes suivantes :
  - Arrêter le service AMC : `/etc/init.d/arkoon-amc stop`
  - Arrêter le service mysqld : `/etc/init.d/mysqld stop`
  - Nettoyer les tables de l'instance : `rm -rf /var/lib/mysql/<instanceDBName>/*`

    Note
    Remplacez <instanceDBName> par le nom de la base de données de l'instance pour laquelle vous souhaitez supprimer les journaux.
  - Démarrer le service mysqld : `/etc/init.d/mysqld start`
  - Démarrer le service AMC : `/etc/init.d/arkoon-amc start`

Les tables sont recréées lors du redémarrage du service.

5.5. Redémarrage d'un service AMC

Pour arrêter, démarrer ou redémarrer un service AMC, vous pouvez naviguer jusqu'à la fenêtre **Maintenance/Diagnostics...** d'Arkoon Monitoring.

Vous pouvez également utiliser la ligne de commande suivante avec les services `srvmon/akserver` :

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

5.6. Gestion des mises à jour des appliances

Le serveur AMC ne peut pas être utilisé comme serveur de mise à jour pour les appliances Fast360. Vous pouvez toutefois lancer les modules ou les mises à jour système pour les appliances à partir de la fenêtre **Arkoon Monitoring Update**.

Pour cela, vous devez sélectionner les appliances à mettre à jour à partir de la vue hiérarchique, puis lancer la mise à jour : l'AMC envoie une requête de mise à jour aux appliances.

Il est impossible de suivre l'évolution et les résultats de la mise à jour à partir d'Arkoon Monitoring.

Pour une mise à jour du système, vous devez sélectionner les appliances partageant la même distribution.

Note
Pour un cluster, seule l'appliance est mise active. Vous devez vous connecter manuellement au deuxième nœud pour le mettre à jour

Chapitre 6. Audit du serveur AMC

Le package `arkoon-amc` possède une commande de diagnostic qui analyse le statut et la configuration du package. Les éléments suivants sont vérifiés :

- **L'intégrité du package (comparé avec une base de données de référence contenue dans le package).**
- **Le statut du serveur.**
- **La validité des instances configurées.**
  - **La validité de la configuration.**
  - **La connexion avec la base de données.**
  - **Le statut des demons.**

Le serveur et les instances AMC peuvent générer des alertes qui concernent leurs propres opérations et qui peuvent être affichées à partir d'Arkoon Monitoring (malfonction d'un service, connexion de la gestion, création/révocation d'un certificat, etc.).

6.1. Commande pour diagnostic

Pour exécuter un diagnostic à partir d'une ligne de commande :

```
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. Alertes

Par défaut, les alertes sont envoyées aux journaux système à l'aide de syslog et avec le nom de l'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'
```

Si vous avez défini une base de données, les alertes publiées par le serveur AMC sont également stockées dans la base de données de l'instance.

6.3. Niveau de sécurité d'une instance AMC

Pour connaître le niveau de sécurité d'une instance AMC, entrez la commande suivante :

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

Puis entrez la commande :

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

Les résultats suivants s'affichent :

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

Chapitre 7. Maintenance du serveur AMC

La maintenance du serveur AMC implique :

- **La sauvegarde des données du serveur AMC.**
- **La restauration des données du serveur AMC.**
- **La mise à jour du package arkoon-amc.**
- **La suppression du package arkoon-amc.**
- **La maintenance des bases de données MySQL**

7.1. Sauvegarde des données du serveur AMC

Il est recommandé de sauvegarder les données du serveur AMC en cas de crash du serveur ou du système d'exploitation. Les données du serveur AMC sont stockées dans les répertoires suivants :

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

Attention
Les données de la base de données stockées dans `/var/lib/mysql` peuvent nécessiter un espace de stockage important.

7.1.1. Sauvegarde des fichiers de configuration

Utilisez la commande suivante pour sauvegarder le serveur AMC et toutes les instances configurées :

```
amc-backup
```

7.1.2. Sauvegarde de l'autorité de certification

Utilisez la commande suivante pour sauvegarder l'autorité de certification d'une instance :

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

7.1.3. Sauvegarde de la base de gestion des rôles

Utilisez la commande suivante pour sauvegarder la base de données des rôles d'une instance :

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

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

7.2. Restauration des données du serveur AMC

Pour restaurer un serveur AMC, vous devez arrêter les services `arkoon-amc` et `mysql`, puis restaurer le contenu du répertoire de sauvegarde dans leurs répertoires d'origine. Redémarrez ensuite les services `mysql` et `arkoon-amc` pour avoir un serveur AMC fonctionnel.

7.2.1. Restauration des fichiers de configuration

Utilisez la commande suivante pour restaurer la configuration du serveur AMC :

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

7.2.2. Restauration de l'Autorité de certification

Utilisez la commande suivante pour restaurer l'autorité de certification d'une instance :

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

7.2.3. Restauration de la base de gestion des rôles

Utilisez la commande suivante pour restaurer la base de données des rôles d'une instance :

```
tar xzvf /tmp/Acces_Control_Database.tgz -C /var/arkoon-amc/"nom_instance"/
```

7.3. Mise à jour du serveur AMC

La procédure de mise à jour du serveur AMC peut être générée grâce à l'outil “Aide à la mise à jour et migration” sur l'espace client : http://client.arkoon.net/.

Sur la page “Aide à la mise à jour et migration”, sélectionnez les critères suivants pour générer la procédure :

- Sélection du mode de connexion : Mode connecté ou Mode déconnecté
- Sélection entre mise à jour ou migration : Mise à jour
- Sélection de la topologie : Un serveur AMC est maître de configuration
- Sélection de l'architecture actuelle : Serveur AMC. Sélectionnez la version actuelle de votre serveur AMC.

- Sélection de l'architecture cible : Serveur AMC

7.4. Suppression du package arkoon-amc

Pour supprimer le package `arkoon-amc` de votre serveur, utilisez la commande suivante avec la ligne de commande suivante :

```
[root@amc-server root]# rpm -e arkoon-amc
Stopping arkoon-amc server:
  Stopping [amc-main]:
    Stopping akserver: amc-main:akserver
    Stopping amanagerd: amc-main:amanagerd
    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
```

Les fichiers de configuration (`/etc/arkoon-amc`) et les répertoires de travail (`/var/arkoon-amc`) ne sont pas supprimés lorsque le package est supprimé. Si vous souhaitez les supprimer, effectuez cette opération une fois que le package a été supprimé :

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

7.5. Optimisation des bases de données MySQL

Afin d'éviter que la taille des index de vos bases de données devienne trop importante et ainsi optimiser l'accès aux journaux via Arkoon Monitoring, il est possible d'appliquer un script d'indexation et d'optimisation des bases de données MySQL. Ce script permet également d'éviter la saturation du ou des disques durs du serveur engendrée par la taille des bases de données. Quel que soit le nombre d'instances présentes sur votre serveur AMC, il permet par défaut de réaliser les actions d'indexation et d'optimisation sur chacune des instances consécutivement.

Il est possible de lancer le script en désignant une ou plusieurs instances en paramètre.

Pour appliquer le script, saisissez la commande suivante : `amc-myisamchk-optim-databases`.

Voici trois exemples d'utilisation du script :

Exemple 7.1. Lancement automatique du script de maintenance de la base de données à intervalles réguliers via Crontab (tous les jours à 4 heures du matin)

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

Exemple 7.2. Lancement manuel du script de maintenance de la base de données

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

Exemple 7.3. Lancement manuel du script de maintenance de la base de données avec argument

```
/opt/arkoon/bin/amc-myisamchk-optim-databases « nom instance1 »
```

Note

Si vous avez mis en place une politique d'archivage automatique des logs des bases de données, nous vous recommandons de paramétrer le lancement automatique du script de maintenance des bases de façon à ce qu'il se lance quelques heures après chaque archivage.

Chapitre 8. Terminologie

8.1. Terminologie

Cette section présente la terminologie spécifique à l'architecture AMC utilisée dans ce document.

Administrateur. Personne travaillant sur une appliance Fast360 ou un serveur AMC pour les initialiser ou les configurer, installer les politiques de sécurité et mener à bien la surveillance et la maintenance. Dans la documentation, il est supposé que ces tâches sont menées par une seule personne : l'administrateur. En pratique, les diverses tâches de gestion d'une appliance Fast360 peuvent être partagées par plusieurs administrateurs.

arkoon-amc. Package d'installation contenant les composants logiciels requis pour l'utilisation du serveur AMC.

Cluster AMC. Groupe d'appliances Fast360 géré et surveillé sous le contrôle d'une autorité de certification donnée. Un fichier de configuration stocké sur le serveur AMC est partagé par les appliances dans un cluster.

Instance AMC. Service logiciel sur le serveur AMC responsable du contrôle d'un groupe AMC. Chaque instance est configurée et installée de façon indépendante sur le serveur AMC.

Instance globale AMC. Instance AMC qui consolide les informations à partir des instances multiples. Une instance globale AMC permet la surveillance d'un groupe de clusters AMC.

Poste d'administration. Poste de travail à partir duquel les outils de gestion et de surveillance (Arkoon Manager, Arkoon Monitoring) sont installés. Ces outils sont l'interface directe avec une appliance Fast360 ou une instance AMC pour la gestion des clusters AMC.

Serveur AMC. Plate-forme de gestion et de surveillance pour les appliances Fast360 sur laquelle la plate-forme AMC a été installée et configurée. Le serveur AMC gère et surveille un ou plusieurs clusters d'appliances Fast360.

Statut VOR (Vert – Orange – Rouge). Statut d'une appliance Fast360. Le statut Vert indique une opération normale. Le statut Orange correspond à un avertissement (par exemple l'expiration d'une licence). Le statut Rouge signifie qu'il y a un problème critique (par exemple un service défectueux sur l'appliance).

Annexe A. Cas de migrations

A.1. Migration d'un serveur AMC vers un nouveau serveur AMC ou VAMC

Dans le cas où vous souhaitez changer de machine pour votre serveur AMC ou si vous souhaitez passer d'un serveur physique à un serveur virtuel, la procédure de migration peut être générée grâce à l'outil “Aide à la mise à jour et migration” sur l'espace client : http://client.arkoon.net/.

Sur la page “Aide à la mise à jour et migration”, sélectionnez les critères suivants pour générer la procédure :

- Sélection du mode de connexion : Mode connecté ou Mode déconnecté
- Sélection entre mise à jour ou migration : Changement de matériel (ou migration vers AMC)
- Sélection de la topologie : Un serveur AMC est maître de configuration
- Sélection de l'architecture actuelle : Serveur AMC. Sélectionnez la version actuelle de votre serveur AMC.
- Sélection de l'architecture cible : Serveur AMC ou Serveur Virtual AMC

A.2. Migration du rôle de maître de configuration d'une appliance vers un serveur AMC

La procédure de migration d'une architecture maître/esclave vers une architecture avec serveur AMC peut être générée grâce à l'outil “Aide à la mise à jour et migration” sur l'espace client : http://client.arkoon.net/.

Sur la page “Aide à la mise à jour et migration”, sélectionnez les critères suivants pour générer la procédure :

- Sélection du mode de connexion : Mode connecté ou Mode déconnecté
- Sélection entre mise à jour ou migration : Changement de matériel (ou migration vers AMC)
- Sélection de la topologie : Une appliance est maître de configuration
- Sélection de l'architecture actuelle : sélectionnez le modèle de votre appliance maître et sa version actuelle.
- Sélection de l'architecture cible : Serveur AMC

A.3. Passage d'une appliance autonome à une appliance esclave d'une nouvelle instance AMC

La procédure peut être générée grâce à l'outil “Aide à la mise à jour et migration” sur l'espace client : http://client.arkoon.net/.

Sur la page “Aide à la mise à jour et migration”, sélectionnez les critères suivants pour générer la procédure :

- Sélection du mode de connexion : Mode connecté ou Mode déconnecté
- Sélection entre mise à jour ou migration : Changement de matériel (ou migration vers AMC)
- Sélection de la topologie : Appliance standalone
- Sélection de l'architecture actuelle : sélectionnez le modèle de votre appliance et sa version actuelle.
- Sélection de l'architecture cible : Serveur AMC

Annexe B. Déploiement d'une CRL sur toutes les appliances d'une instance AMC

B.1. Cas d'une PKI Arkoon gérée par l'instance AMC

Lorsque vous êtes connecté à votre instance AMC pour gérer vos certificats (via minamcconf ou le Manager), la révocation d'un certificat provoque la mise à jour de la CRL sur l'instance AMC et sur toutes les appliances de l'instance. Si une appliance n'est pas connectée, la diffusion de la CRL passe en “reporté” et la CRL sera installée lors de la prochaine connexion de l'appliance.

> **Note**
> Vous pouvez toujours installer la CRL via le menu **Administration avancée** > **Envoyer la liste de révocation des certificats (CRL) ...** d'Arkoon Manager, sur une ou des appliances.

B.2. Cas d'une PKI externe

Pour que la CRL de votre PKI externe soit prise en compte par votre instance AMC et ses appliances, utilisez le menu **Administration avancée** > **Envoyer la liste de révocation des certificats (CRL) ...** d'Arkoon Manager.

B.3. Récupération automatique de la CRL par une nouvelle appliance

Lorsqu'une nouvelle appliance se connecte à votre architecture AMC pour la première fois, elle tente de récupérer automatiquement la CRL que son instance propose :

- Si la CRL provient d'une Autorité de Certification Arkoon gérée directement par l'instance AMC, une fois la configuration de l'appliance (via **minarkconf**, menu **Master/Slave**) terminée, l'appliance va chercher la CRL directement sur l'instance. Vous n'avez n'a rien à faire.
- Si la CRL provient d'une Autorité de Certification gérée par une PKI externe :
  - Si la clé `arkoon-config : arkoon-amc.certificate.crl-trust-master = yes` est définie sur le serveur AMC (valeur par défaut), on autorise l'instance AMC à envoyer sa CRL à son appliance, même si cette instance n'est pas Autorité de Certification.
  - Si la clé `arkoon-config : arkoon-amc.certificate.crl-trust-master = no` est définie, l'instance AMC n'envoie pas sa CRL car il est estimé qu'elle n'est pas Autorité de Certification et qu'elle n'a pas à fournir une CRL qu'elle ne gère pas. Par conséquent, vous devez installer manuellement la CRL sur son appliance via le menu **Administration avancée** > **Envoyer la liste de révocation des certificats (CRL) ...** d'Arkoon Manager.

Annexe C. Fichier de configuration

C.1. Fichier de configuration pour un exemple d'instance

Cet exemple explique comment écrire un fichier de configuration pour une instance. La ligne `include` est obligatoire. Tous les paramètres par défaut sont inclus à la configuration à partir du fichier `/opt/arkoon/etc/arkoon-config` présenté dans la section suivante. Les paramètres par défaut peuvent être redéfinis avec de nouvelles valeurs dans le reste du fichier.

```
# 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. Fichier de configuration à inclure : arkoon-config

Utiliser la commande `include` pour inclure le fichier `/opt/arkoon/etc/arkoon-config` au fichier de configuration de l'instance permet d'initialiser les paramètres par défaut.

Vous pouvez ouvrir le fichier pour voir les paramètres par défaut.

Annexe D. Sauvegarde régulière de la configuration des appliances de l'instance AMC

D.1. Sauvegarde régulière de la configuration des appliances de l'instance AMC

Pour sauvegarder de manière régulière la configuration des appliances :

1. Lancez l'outil **Minamcconf**.
2. Sélectionnez le menu **2. Instances** puis choisissez l'option **d. configure AMC**.
3. Cliquez sur **Select Instance** puis choisissez le menu **8. Slaves backup**.
4. Choisissez ensuite la fréquence de sauvegarde et validez avec `<OK>`.
5. Entrez l'heure de démarrage de la sauvegarde du premier esclave et cliquez sur `<OK>` pour valider la programmation de la sauvegarde.

   Les sauvegardes sont stockées à l'emplacement suivant : `/var/arkoon-amc/<nom_instance>/configcard.backup/<FQDN_appliance>/`

   Note
   Une alerte par appliance sera générée sur l'AMC pour avertir du bon déroulement ou de l'échec d'une (ou de plusieurs) sauvegardes d'appliances.

   Note
   La sauvegarde de la configuration d'une appliance esclave est conservée pour une durée correspondant à trois fois la fréquence de sauvegarde paramétrée. Elle est ensuite écrasée par la prochaine sauvegarde. Il est recommandé de copier les sauvegardes dans un espace de stockage externe (NAS, SAN, etc.).

Annexe D. Sauvegarde régulière de la configuration des appliances de l'instance AMC


Fast360
NETWORK SECURITY


ARKOON
NETWORK SECURITY