

# Documentation d'OCS Inventory NG

Pour une meilleure lecture, la documentation d'OCS Inventory NG documentation a été divisée en 9 pages.

- [Installer le serveur de gestion](#)
- [Installer l'agent sur les ordinateurs clients](#)
- [Résultats des requêtes d'inventaire](#)
- [Administration d'OCS Inventory NG](#)
- [Utiliser la fonctionnalité de découverte IP](#)
- [Déployer des paquets ou exécuter des commandes sur les clients](#)
- [Gérer le paramétrage du serveur](#)
- [Sauvegarder et Restaurer la base de données d'OCS Inventory NG](#)
- [Erreurs fréquentes](#)



# INSTALLER LE SERVEUR DE GESTION

## **Contenu :**

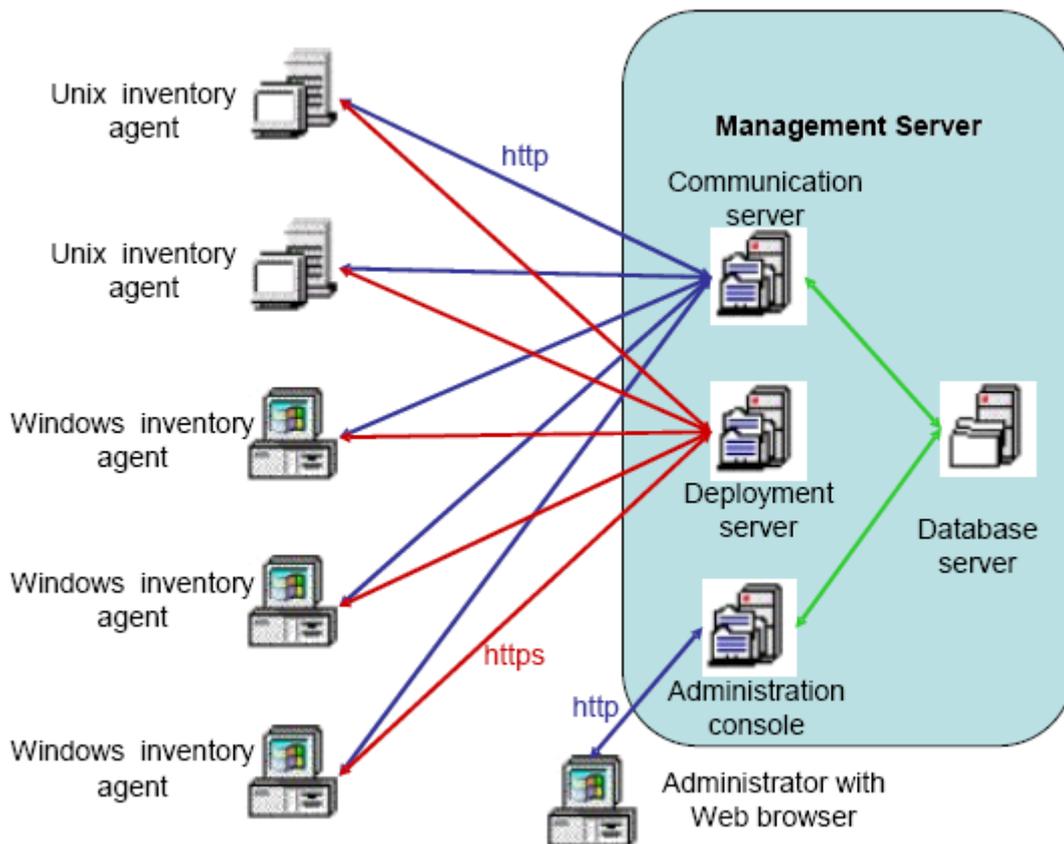
- [1 Installer le serveur de gestion.](#)
  - [1.1 Sur un système d'exploitation Unix](#)
    - [1.1.1 Requis](#)
    - [1.1.2 Installer le serveur de communication requiert les modules PERL.](#)
    - [1.1.3 Installer la console d'administration requiert les modules PHP.](#)
    - [1.1.4 Installer le serveur de gestion](#)
    - [1.1.5 Configurer le serveur de gestion](#)
    - [1.1.6 Mettre-à-jour le serveur de gestion](#)
  - [1.2 Sur un système d'exploitation Windows](#)
    - [1.2.1 Installer le serveur de gestion](#)
    - [1.2.2 Configurer le serveur de gestion](#)
    - [1.2.3 Mettre-à-jour la sécurité des composants de XAMPP](#)
    - [1.2.4 Mettre-à-jour le serveur de gestion](#)

## **Installer le serveur de gestion.**

Le serveur de gestion est composé de 4 éléments :

1. **Le serveur de base de données** qui stocke l'information d'inventaire
2. **Le serveur de communication** qui prend en charge les échanges HTTP entre le serveur de base de données et les agents
3. **La console d'administration** pour que l'administrateur réseau puisse interroger le serveur de base de données depuis un navigateur
4. **Le serveur de déploiement** qui stocke toutes les configurations des paquets à déployer (nécessite HTTPS !)

Ces 4 composants peuvent être installés sur un unique ordinateur ou plusieurs pour un meilleur équilibrage des charges. Au delà de 10000 ordinateurs inventoriés, nous recommandons l'aide d'au moins 2 serveurs physiques, un serveur hébergeant le serveur de base de données + le serveur de communication et un autre hébergeant une sauvegarde de la base de données + le serveur d'administration + le serveur de déploiement.



**Figure 1 : L'architecture du réseau OCS Inventory NG.**

*NOTE : Si vous voulez utiliser plusieurs ordinateurs pour faire de l'équilibrage de charge entre les différents modules du serveur de gestion OCS, nous vous recommandons de l'installer sous Linux. En effet, le serveur d'inventaire OCS pour Windows est un paquet intégré contenant tous les composants (apache, PERL, php, mod\_perl, mysql...).*

**Le serveur de base de données** ne peut, à l'heure actuelle, être que sur MySQL 4.1 (ou supérieur) avec un moteur InnoDB actif.

**Le serveur de communication** est écrit en langage PERL en tant que module Apache. Ainsi, il requiert l'installation de Apache Web Server 1.3.X/2.X. La raison à cela est que le script PERL est compilé au démarrage de Apache, et non à chaque requête pour de meilleures performances (selon la version de votre distribution, des modules PERL supplémentaires pourront être nécessaires à votre serveur de communication)

**Le serveur de déploiement** requiert n'importe quel serveur Web avec SSL activé.

**La console d'administration** est écrite en PHP 4 (ou supérieur) et fonctionne sous server Apache 1.3.X/2.X. La console d'administration nécessite que la compatibilité ZIP et GD soit activée dans PHP pour l'utilisation du déploiement de paquet.

## Sur un système d'exploitation Unix

Vous devez vous assurer d'avoir :

- Le serveur de base de données MySQL fonctionnant et écoutant sur le port par défaut 3306 avec les communications TCP/IP chargées.
- Un serveur web Apache installé et fonctionnant pour le serveur de communication et le serveur d'Administration.
- PHP et Perl installés et utilisables par le serveur web Apache pour la console d'administration.
- Perl et mod\_perl installés et utilisables par le serveur web Apache pour le serveur de communication.

### Requis

- Apache version 1.3.33 ou supérieure ou Apache version 2.0.46 ou supérieure.
  - Mod\_perl version 1.29 ou supérieure.
  - Mod\_php version 4.3.2 ou supérieure.
- PHP version 4.3.2 ou supérieure, avec support ZIP et GD chargé.
- PERL version 5.6 ou supérieure.
  - Module Perl XML::Simple version 2.12 ou supérieure.
  - Module Perl Compress::Zlib version 1.33 ou supérieure.
  - Module Perl DBI version 1.40 ou supérieure.
  - Module Perl DBD::Mysql version 2.9004 ou supérieure.
  - Module Perl Apache::DBI version 0.93 ou supérieure.
  - Module Perl Net::IP version 1.21 ou supérieure.
  - Module Perl SOAP::Lite version 0.66 ou supérieure.
- MySQL version 4.10 ou supérieure avec moteur InnoDB activé.
- Utilitaire Make tel que GNU Make.

N.B. : Le serveur d'installation OCS Inventory NG vérifiera tous ses composants et s'arrêtera s'il en manque un.

### Installer le serveur de communication requiert les modules PERL.

Le serveur de communication requiert le serveur web Apache, le langage de script Perl 5 et quelques modules additionnels pour Perl 5 (cf § [la section intitulée « Requis »](#)). Il agit comme un module d'Apache qui prend la main sur les requêtes HTTP des agents OCS Inventory NG vers le répertoire virtuel /ocsinventory.

### Vous devez avoir les privilèges d'Administrateur pour installer les modules Perl requis.

*Il vaut mieux, pour l'intégrité du système, utiliser les paquets précompilés de votre distribution s'ils sont disponibles.*

**Sur Fedora/RedHat**, vous pouvez utiliser l'outil **Yum** pour installer les modules requis, tels que :

- yum install perl-XML-Simple
- yum install perl-Compress-Zlib
- yum install perl-DBI
- yum install perl-DBD-MySQL
- yum install perl-Apache-DBI
- yum install perl-Net-IP
- yum install perl-SOAP-Lite

**Sur Debian**, vous pouvez utiliser l'outil **apt-get** pour installer les modules requis :

- apt-get install libxml-simple-perl
- apt-get install libcompress-zlib-perl
- apt-get install libdbi-perl
- apt-get install libdbd-mysql-perl
- apt-get install libapache-dbi-perl
- apt-get install libnet-ip-perl
- apt-get install libsoap-lite-perl

```
libxml-simple-perl libcompress-zlib-perl libdbi-perl libdbd-mysql-perl libapache-dbi-perl libnet-ip-perl libsoap-lite-perl
```

Si le paquet précompilé n'est pas disponible pour votre distribution, vous pouvez télécharger les sources du paquet depuis <http://search.cpan.org/> et le construire sur votre système (les compilateurs make et C doivent être disponibles et installés) tel que suivant :

- tar -xvzf package\_name.tar.gz
- cd package\_name
- perl Makefile.PL
- make
- make test
- make install

N.B. : Si vous n'utilisez pas l'interpréteur système PERL, mais un autre tel que l'interpréteur perl XAMPP/LAMPP, vous devez appeler cet interpréteur, non par l'appel système, mais en spécifiant le chemin absolu de votre interpréteur Perl.

Pour l'exemple : `/opt/lampp/bin/perl Makefile.PL`.

### **Installer la console d'administration requiert les modules PHP.**

La console d'Administration requiert le serveur web Apache et le langage de script PHP 4 ainsi que quelques modules additionnels pour PHP (cf § [la section intitulée « Requis »](#)).

**Vous devez avoir les privilèges d'Administrateur pour installer la console d'administration.**

**Vous devez avoir installé le support ZIP pour PHP.**

**Sur Fedora/RedHat**, vous devez utiliser l'outil **Yum** pour installer :

- yum install php-pecl-zip

**Sur Debian**, vous devez utiliser l'outil **apt-get** pour installer :

- apt-get install libphp-pclzip

Toutefois, la meilleure façon de faire cela est d'utiliser le paquet PHP PECL ZIP. Vous devez avoir les bibliothèques de développement PHP (paquet php-devel sous RedHat ou Fedora Core, sous GNU/Linux Debian ou Ubuntu) avant de lancer **phpize**.

Alors, si vous avez installé pear, tapez justement :

- pear install zip

Si vous n'avez pas installé pear, ou que vous n'avez pas de connexion Internet, téléchargez le paquet "zip-1.3.1.tgz" depuis <http://pecl.php.net/package/zip>.

Installez-le (le paquet php devel est requis) :

- tar -xzvf zip-1.3.1.tgz
- cd zip-1.3.1
- phpize
- ./configure
- make
- make install

**Vous avez besoin d'installer le support GD pour PHP.**

**Sur Fedora/RedHat**, vous devez utiliser l'outil **Yum** pour installer :

- yum install php-gd

**Sur Debian**, vous devez utiliser l'outil **apt-get** pour installer :

- apt-get install php-gd

**Installer le serveur de gestion**

**Vous devez avoir les privilèges d'Administrateur pour installer le serveur de gestion.**

N.B. : Soyez sûr que le moteur InnoDB de MySQL est activé sur votre serveur de base de données. Ouvrez le fichier my.cnf et assurez vous qu'il n'y ait pas de ligne "skip-innodb" ou mettez-la en commentaire (avec le symbole #).

Téléchargez "OCSNG\_LINUX\_SERVER\_1.01.tar.gz" depuis le site web d'OCS Inventory NG.

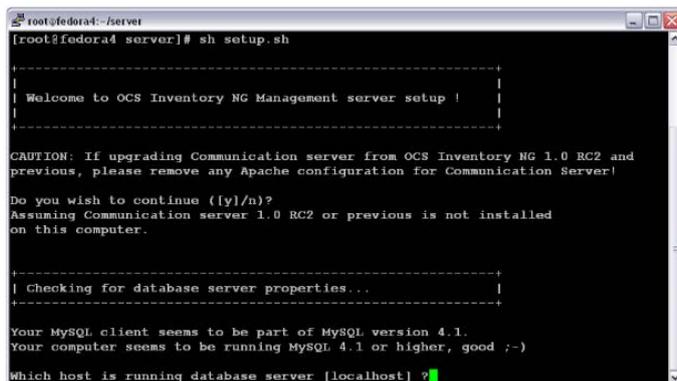
Décompressez-la :

- tar -xzvf OCSNG\_LINUX\_SERVER\_1.01.tar.gz
- cd OCSNG\_LINUX\_SERVER\_1.01

Lancez l'installateur setup.sh. Pendant la phase d'installation, le choix par défaut est présenté entre les symboles [ ]. Par exemple, [y]/n signifie que "y" (yes) est le choix par défaut, et que "n" (no) est un autre choix.

- sh setup.sh

N.B. : L'installateur écrit un fichier log ocs\_server\_setup.log dans le même répertoire. Si vous rencontrez une erreur, veuillez lire ce fichier log pour connaître le message d'erreur.



```
root@fedora4:~/server
[root@fedora4 server]# sh setup.sh

-----
| Welcome to OCS Inventory NG Management server setup !
|-----

CAUTION: If upgrading Communication server from OCS Inventory NG 1.0 RC2 and
previous, please remove any Apache configuration for Communication Server!

Do you wish to continue ([y]/n)?
Assuming Communication server 1.0 RC2 or previous is not installed
on this computer.

-----
| Checking for database server properties...
|-----

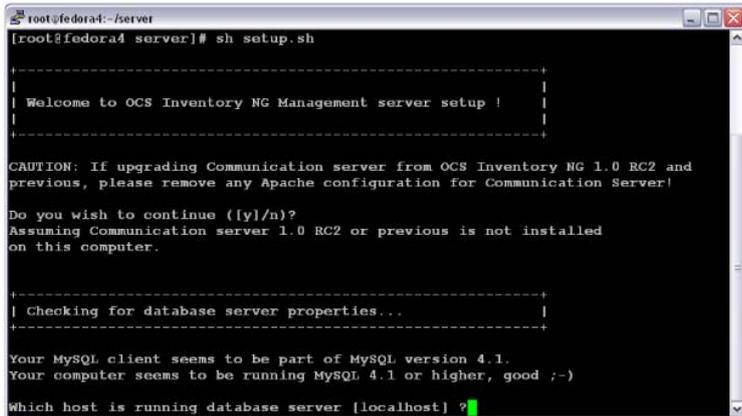
Your MySQL client seems to be part of MySQL version 4.1.
Your computer seems to be running MySQL 4.1 or higher, good ;-)

Which host is running database server [localhost] ?
```

**Attention :**

Si vous faites une mise-à-jour depuis OCS Inventory NG 1.0 RC2 ou inférieure, vous devez en premier supprimer le fichier de configuration d'Apache du serveur de communication.

Tapez sur "y" ou sur la touche "Enter" pour valider, puis entrez l'adresse de l'hôte du serveur MySQL, généralement localhost.



```
root@fedora4:~/server
[root@fedora4 server]# sh setup.sh

-----+
| Welcome to OCS Inventory NG Management server setup ! |
|-----+

CAUTION: If upgrading Communication server from OCS Inventory NG 1.0 RC2 and
previous, please remove any Apache configuration for Communication Server!

Do you wish to continue ([y]/n)?
Assuming Communication server 1.0 RC2 or previous is not installed
on this computer.

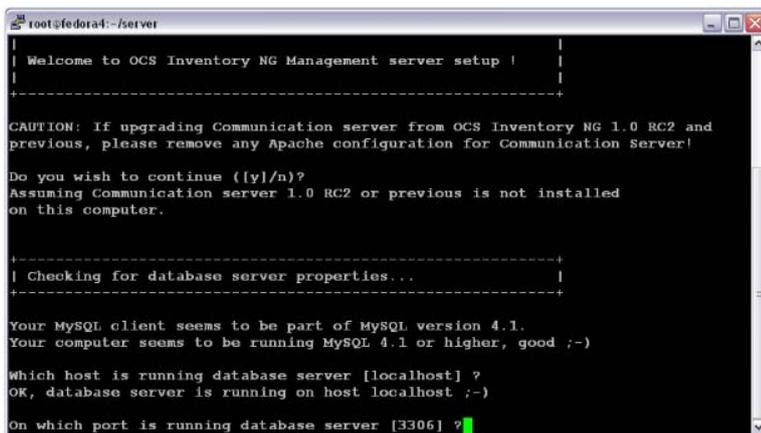
-----+
| Checking for database server properties... |
|-----+

Your MySQL client seems to be part of MySQL version 4.1.
Your computer seems to be running MySQL 4.1 or higher, good ;-)

Which host is running database server [localhost] ?
```

Alors, l'installateur vérifie que la version des fichiers binaires du client MySQL soit la 4.1 ou supérieure. Si elle n'est pas présente, il vous sera demandé de continuer ou d'arrêter l'installateur.

Si tout est OK, entrez le numéro du port de connexion au serveur MySQL, généralement 3306.



```
root@fedora4:~/server

| Welcome to OCS Inventory NG Management server setup ! |
|-----+

CAUTION: If upgrading Communication server from OCS Inventory NG 1.0 RC2 and
previous, please remove any Apache configuration for Communication Server!

Do you wish to continue ([y]/n)?
Assuming Communication server 1.0 RC2 or previous is not installed
on this computer.

-----+
| Checking for database server properties... |
|-----+

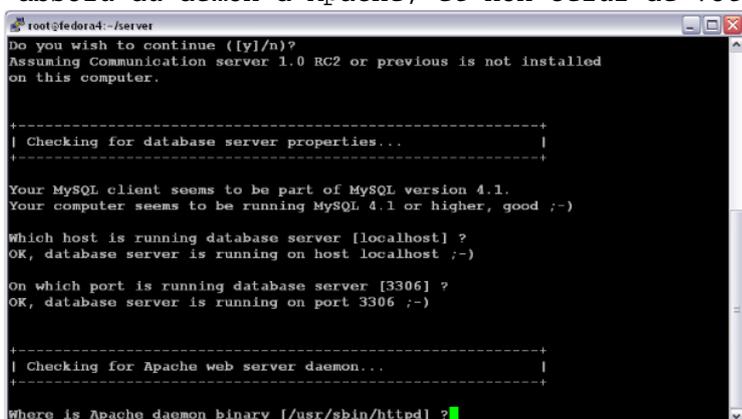
Your MySQL client seems to be part of MySQL version 4.1.
Your computer seems to be running MySQL 4.1 or higher, good ;-)

Which host is running database server [localhost] ?
OK, database server is running on host localhost ;-)

On which port is running database server [3306] ?
```

Entrez ou validez le chemin du démon binaire d'Apache, généralement /usr/sbin/httpd. Il sera utilisé pour trouver les fichiers de configuration d'Apache.

N.B. : Si vous n'utilisez pas le démon système d'Apache, mais un autre tel que celui du serveur Apache XAMPP/LAMPP, vous devez préciser le chemin absolu du démon d'Apache, et non celui de votre système.



```
root@fedora4:~/server

Do you wish to continue ([y]/n)?
Assuming Communication server 1.0 RC2 or previous is not installed
on this computer.

-----+
| Checking for database server properties... |
|-----+

Your MySQL client seems to be part of MySQL version 4.1.
Your computer seems to be running MySQL 4.1 or higher, good ;-)

Which host is running database server [localhost] ?
OK, database server is running on host localhost ;-)

On which port is running database server [3306] ?
OK, database server is running on port 3306 ;-)

-----+
| Checking for Apache web server daemon... |
|-----+

Where is Apache daemon binary [/usr/sbin/httpd] ?
```

Entrez ou validez le chemin du fichier de configuration principal d'Apache, généralement /etc/apache/conf/apache.conf, /etc/httpd/conf/httpd.conf, voire /etc/apache2/conf/httpd.conf.

```
root@fedora4:~/server
Your MySQL client seems to be part of MySQL version 4.1.
Your computer seems to be running MySQL 4.1 or higher, good ;-)

Which host is running database server [localhost] ?
OK, database server is running on host localhost ;-)

On which port is running database server [3306] ?
OK, database server is running on port 3306 ;-)

-----
| Checking for Apache web server daemon... |
-----
Where is Apache daemon binary [/usr/sbin/httpd] ?
OK, Apache daemon /usr/sbin/httpd found ;-)

-----
| Checking for Apache main configuration file... |
-----
Where is Apache main configuration file [/etc/httpd/conf/httpd.conf] ?
```

Entrez ou validez le compte utilisateur servant à faire fonctionner le démon d'Apache, généralement apache ou www.

```
root@fedora4:~/server
OK, database server is running on port 3306 ;-)

-----
| Checking for Apache web server daemon... |
-----
Where is Apache daemon binary [/usr/sbin/httpd] ?
OK, Apache daemon /usr/sbin/httpd found ;-)

-----
| Checking for Apache main configuration file... |
-----
Where is Apache main configuration file [/etc/httpd/conf/httpd.conf] ?
OK, Apache main configuration file /etc/httpd/conf/httpd.conf found ;-)

-----
| Checking for Apache user account... |
-----
Which user account is running Apache web server [apache] ?
```

Entrez ou validez le groupe utilisateur avec lequel fonctionne le démon d'Apache, généralement apache ou www

```
root@fedora4:~/server
OK, Apache daemon /usr/sbin/httpd found ;-)

-----
| Checking for Apache main configuration file... |
-----
Where is Apache main configuration file [/etc/httpd/conf/httpd.conf] ?
OK, Apache main configuration file /etc/httpd/conf/httpd.conf found ;-)

-----
| Checking for Apache user account... |
-----
Which user account is running Apache web server [apache] ?
OK, Apache is running under user account apache ;-)

-----
| Checking for Apache group... |
-----
Which user group is running Apache web server [apache] ?
```

Maintenant, l'installateur vérifie la présence des binaires de l'interpréteur PERL. Entrez ou validez le chemin de l'interpréteur PERL.

N.B. : Si vous n'utilisez pas l'interpréteur perl de votre système, mais un autre tel que l'interpréteur perl XAMPP/LAMPP, vous devez spécifier le chemin absolu de votre interpréteur perl, et non celui du système (/opt/lampp/bin/perl généralement utilisé dans XAMPP/LAMPP).

```
root@labo-av-lin-02:~/server
+-----+
| Checking for Apache user account... |
+-----+
Which user account is running Apache web server [apache] ?
OK, Apache is running under user account apache ;-)
```

```
+-----+
| Checking for Apache group... |
+-----+
Which user group is running Apache web server [apache] ?
OK, Apache is running under users group apache ;-)
```

```
+-----+
| Checking for PERL Interpreter... |
+-----+
Found PERL Intrepreter at </usr/bin/perl> ;-)
```

```
Where is PERL Intrepreter binary [/usr/bin/perl] ?
```

Les informations communes pour l'installation du serveur de communication ou de la console d'administration sont maintenant collectées. L'installateur vous demande si vous voulez installer le serveur de communication sur cet ordinateur. Entrez "y" ou validez, ou "n" pour sauter l'installation du serveur de communication.

```
root@labo-av-lin-02:~/server
+-----+
| Checking for Apache user account... |
+-----+
Which user account is running Apache web server [apache] ?
OK, Apache is running under user account apache ;-)
```

```
+-----+
| Checking for Apache group... |
+-----+
Which user group is running Apache web server [apache] ?
OK, Apache is running under users group apache ;-)
```

```
+-----+
| Checking for PERL Interpreter... |
+-----+
Found PERL Intrepreter at </usr/bin/perl> ;-)
```

```
Where is PERL Intrepreter binary [/usr/bin/perl] ?
OK, using PERL Intrepreter /usr/bin/perl ;-)
```

```
Do you wish to setup Communication server on this computer ((y|n)?
```

L'installateur essaiera alors de trouver l'utilitaire **make**. S'il n'y arrive pas, il s'arrêtera.

Entrez ou validez le chemin d'Apache, incluant le répertoire de configuration. Celui-ci est le répertoire où sont enregistrés les fichiers de configuration spécifiques aux différents modules. Généralement, ce répertoire est /etc/httpd/conf.d ou /etc/apache/conf.d. Si vous n'utilisez pas de répertoire de configuration, mais que vous entrez toutes les informations de configuration dans le fichier principal de configuration d'Apache, entrez "no".

```
root@fedora4:~/server
+-----+
| Checking for PERL Interpreter... |
+-----+
OK, PERL Intrepreter found at </usr/bin/perl> ;-)
```

```
Do you wish to setup Communication server on this computer ((y|n)?
```

```
+-----+
| Checking for Make utility... |
+-----+
OK, Make utility found at </usr/bin/make> ;-)
```

```
+-----+
| Checking for Apache Include configuration directory... |
+-----+
Setup has founnd Apache Include configuration directory in
/etc/httpd/conf.d/.
```

```
If you are not using Include directive, please enter 'no'.
```

```
Where is Apache Include configuration directory [/etc/httpd/conf.d/]
```

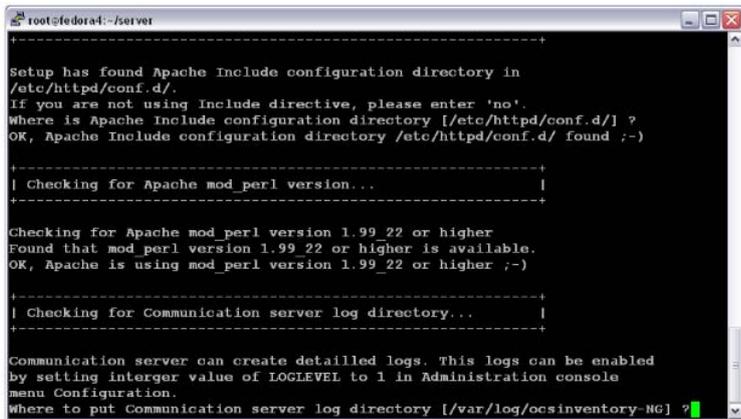
L'installateur va maintenant essayer de déterminer quelle est la version du module Apache "mod\_perl". S'il n'est pas capable de la déterminer, il vous demandera de l'entrer.

Vous pouvez vérifier quelle version du module "mod\_perl" vous utilisez en vérifiant dans la base de données système de votre distribution.

Avec les distributions utilisant RPM (RedHat/Fedora, Mandriva, ...), faites `rpm -q mod_perl`.

Avec les distributions utilisant DPKG (Debian, Ubuntu, ...), faites `dpkg -l libapache*mod-perl*`.

Maintenant, il va vous être demandé d'entrer le répertoire de log où le serveur de communication enregistrera les fichiers logs de débogage/tuning. Validez ou entrez le chemin. S'il n'existe pas, le répertoire sera créé.



```
root@fedora4:~/server
-----+
Setup has found Apache Include configuration directory in
/etc/httpd/conf.d/.
If you are not using Include directive, please enter 'no'.
Where is Apache Include configuration directory [/etc/httpd/conf.d] ?
OK, Apache Include configuration directory /etc/httpd/conf.d/ found ;-)

-----+
| Checking for Apache mod_perl version... |
-----+

Checking for Apache mod_perl version 1.99_22 or higher
Found that mod_perl version 1.99_22 or higher is available.
OK, Apache is using mod_perl version 1.99_22 or higher ;-)

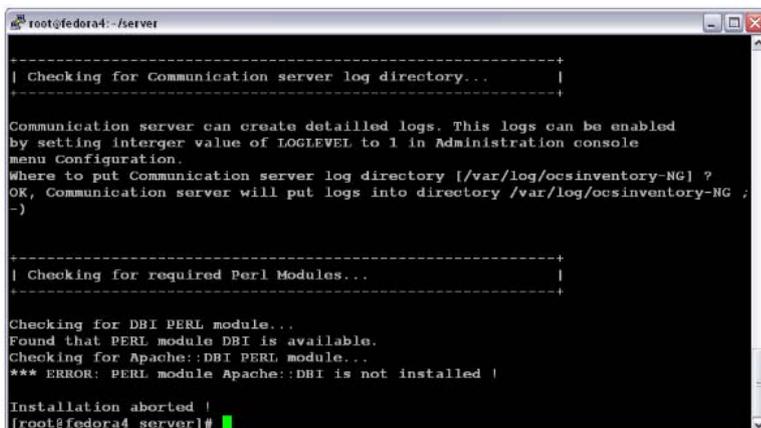
-----+
| Checking for Communication server log directory... |
-----+

Communication server can create detailed logs. This logs can be enabled
by setting interger value of LOGLEVEL to 1 in Administration console
menu Configuration.
Where to put Communication server log directory [/var/log/ocsinventory-NG] ?
```

Maintenant, l'installateur va vérifier la présence des modules PERL requis (cf § [la section intitulée « Requis »](#)):

- XML::Simple version 2.12 ou supérieure
- Compress::Zlib version 1.33 ou supérieure
- DBI version 1.40 ou supérieure
- DBD::MySQL version 2.9004 ou supérieure
- Apache::DBI version 0.93 ou supérieure
- Net::IP version 1.21 ou supérieure
- SOAP::Lite version 0.66 ou supérieure

Si un de ces modules est indisponible, l'installateur s'arrêtera.



```
root@fedora4:~/server
-----+
| Checking for Communication server log directory... |
-----+

Communication server can create detailed logs. This logs can be enabled
by setting interger value of LOGLEVEL to 1 in Administration console
menu Configuration.
Where to put Communication server log directory [/var/log/ocsinventory-NG] ?
OK, Communication server will put logs into directory /var/log/ocsinventory-NG ;
-)

-----+
| Checking for required Perl Modules... |
-----+

Checking for DBI PERL module...
Found that PERL module DBI is available.
Checking for Apache::DBI PERL module...
*** ERROR: PERL module Apache::DBI is not installed !

Installation aborted !
[root@fedora4 server]#
```

Si tout est OK, l'installateur installera le serveur de communication :

- Configurera les modules PERL pour le serveur de communication
- Construera les modules PERL pour le serveur de communication

- Installera les modules PERL pour le serveur de communication dans les répertoires de bibliothèques standard PERL.
- Créera le répertoire des logs du serveur de communication (/var/log/ocsinventory-NG par défaut).
- Configurera la rotation quotidienne des fichiers log pour le serveur de communication (fichier /etc/logrotate.d/ocsinventory-NG par défaut).
- Créera le fichier de configuration pour Apache (ocsinventory.conf). Si vous utilisez le répertoire de configuration d'Apache, ce fichier sera copié dans ledit répertoire. Toutefois, vous pouvez ajouter le contenu de ce fichier à la fin du fichier de configuration d'Apache. **Ne pas ajouter le contenu de ce fichier au fichier de configuration d'Apache, si votre installation d'Apache n'est pas récente. Vous devez copier manuellement le contenu du fichier ocsinventory.conf.local créé par l'installateur dans le fichier de configuration d'Apache, remplaçant ainsi la configuration existante.**

```
#####
# OCS Inventory NG Communication Server Perl Module Setup
# Copyleft 2006 Pascal DANEK
# Web: http://ocsinventory.sourceforge.net
# This code is open source and may be copied and modified as long as the source
# code is always made freely available.
# Please refer to the General Public Licence http://www.gnu.org/ or Licence.txt
#####
# Which version of mod_perl we are using
# For mod_perl <= 1.999_21, replace VERSION_MP by 1
# For mod_perl > 1.999_21, replace VERSION_MP by 2

PerlSetEnv OCS_MODPERL_VERSION VERSION_MP

# Where to write detailed logs

PerlSetEnv OCS_LOGPATH "PATH_TO_LOG_DIRECTORY"

# Database options
# Replace DATABASE_SERVER by hostname or ip of MySQL server, generally localhost
PerlSetEnv OCS_DB_HOST DATABASE_SERVER
# Replace DATABASE_PORT by port where running MySQL server, generally 3306
PerlSetEnv OCS_DB_PORT DATABASE_PORT
# Name of database
PerlSetEnv OCS_DB_NAME ocsweb
PerlSetEnv OCS_DB_LOCAL ocsweb
# User allowed to connect to database
PerlSetEnv OCS_DB_USER ocs
# Password for user
PerlSetVar OCS_DB_PWD ocs

# The options below are overloaded if you are using ocs GUI
# Be careful: you must restart apache to have any effects
PerlSetEnv OCS_OPT_FREQUENCY 0
PerlSetEnv OCS_OPT_PROLOG_FREQ 24
PerlSetEnv OCS_OPT_DEPLOY 1
PerlSetEnv OCS_OPT_TRACE_DELETED 0
PerlSetEnv OCS_OPT_AUTO_DUPLICATE_LVL 7
PerlSetEnv OCS_OPT_LOGLEVEL 0
PerlSetEnv OCS_OPT_INVENTORY_DIFF 1
PerlSetEnv OCS_OPT_INVENTORY_TRANSACTION 1
PerlSetEnv OCS_OPT_PROXY_REVALIDATE_DELAY 3600
PerlSetEnv OCS_OPT_LOCK_REUSE_TIME 3600

# Optional modules
PerlSetEnv OCS_OPT_IPDISCOVER 2
PerlSetEnv OCS_OPT_IPDISCOVER_MAX_ALIVE 7
PerlSetEnv OCS_OPT_IPDISCOVER_LATENCY 100
PerlSetEnv OCS_OPT_REGISTRY 0
PerlSetEnv OCS_OPT_UPDATE 0
PerlSetEnv OCS_OPT_DOWNLOAD 0
```

```

PerlSetEnv OCS_OPT_DOWNLOAD_FRAG_LATENCY 10
PerlSetEnv OCS_OPT_DOWNLOAD_CYCLE_LATENCY 0
PerlSetEnv OCS_OPT_DOWNLOAD_PERIOD_LATENCY 0
PerlSetEnv OCS_OPT_DOWNLOAD_TIMEOUT 30
PerlSetEnv OCS_OPT_WEB_SERVICE_ENABLED 0
PerlSetEnv OCS_OPT_PROLOG_FILTER_ON 1
PerlSetEnv OCS_OPT_INVENTORY_FILTER_ON 1
PerlSetEnv OCS_OPT_INVENTORY_FILTER_FLOOD_IP 1
PerlSetEnv OCS_OPT_INVENTORY_FILTER_FLOOD_IP_CACHE_TIME 60

##### DO NOT MODIFY BELOW ! #####

# External modules
PerlModule Apache::DBI
PerlModule Compress::Zlib
PerlModule XML::Simple

# Ocs
PerlModule Apache::Ocsinventory
PerlModule Apache::Ocsinventory::Server::Constants
PerlModule Apache::Ocsinventory::Server::System
PerlModule Apache::Ocsinventory::Server::Communication
PerlModule Apache::Ocsinventory::Server::Inventory
PerlModule Apache::Ocsinventory::Server::Duplicate

# Options
PerlModule Apache::Ocsinventory::Server::Option::Registry
PerlModule Apache::Ocsinventory::Server::Option::Update
PerlModule Apache::Ocsinventory::Server::Option::Ipdiscover
PerlModule Apache::Ocsinventory::Server::Option::Download

# This module guides you through the module creation
# PerlModule Apache::Ocsinventory::Server::Option::Example
# This module adds some rules to filter some request sent to ocs server in the prolog
# and inventory stages
# PerlModule Apache::Ocsinventory::Server::Option::Filter

# Virtual directory for handling OCS Inventory NG agents communications
# Be carefull, do not create such directory into your web server root document !
#PerlTaintCheck On

<Location /ocsinventory>
    order deny,allow
    allow from all
    Satisfy Any
    SetHandler perl-script
    PerlHandler Apache::Ocsinventory
</Location>
PerlModule Apache::Ocsinventory::SOAP;
<location /ocsinterface>
    SetHandler perl-script
    perlHandler "Apache::Ocsinventory::SOAP"
    order deny,allow
    allow from all
    Satisfy any

</location>

```

L'installation du serveur de communication est maintenant terminée. Il va vous être demandé de démarrer l'installation de la console d'administration. Entrez "y" ou validez pour démarrer l'installation, entrez "n" pour sauter l'installation de la console d'administration.

```
root@fedora4:~/server
Fixing Communication server log directory files permissions.
Configuring logrotate for Communication server.
Writing communication server logrotate to file /etc/logrotate.d/ocsinventory-NG

-----
| OK, Communication server log directory created ;-)|
| Now configuring Apache web server...|
-----
Writing communication server configuration to file /etc/httpd/conf.d/ocsinventory.conf

-----
| OK, Communication server setup successfully finished ;-)|
| Please, review /etc/httpd/conf.d/ocsinventory.conf|
| to ensure all is good. Then restart Apache daemon.|
-----

Do you wish to setup Administration server (web administration console)
on this computer ([y]/n)?
```

L'installateur va vous demander le répertoire racine d'Apache, habituellement /var/www/html ou /var/www-data.

```
root@fedora4:~/server
| OK, Communication server log directory created ;-)|
| Now configuring Apache web server...|
-----
Writing communication server configuration to file /etc/httpd/conf.d/ocsinventory.conf

-----
| OK, Communication server setup successfully finished ;-)|
| Please, review /etc/httpd/conf.d/ocsinventory.conf|
| to ensure all is good. Then restart Apache daemon.|
-----

Do you wish to setup Administration server (web administration console)
on this computer ([y]/n)?

-----
| Checking for Apache root document directory...|
-----

Where is Apache root document directory [] ?/var/www/html
```

Maintenant, l'installateur va vérifier la présence des modules PERL requis (cf § [la section intitulée « Requis »](#)) :

- XML::Simple version 2.12 ou supérieure
- DBI version 1.40 ou supérieure
- DBD::MySQL version 2.9004 ou supérieure
- Net::IP version 1.21 ou supérieure

Si un de ces modules est absent, l'installateur s'arrêtera.

Si tout est OK, l'installateur installera la console d'administration dans le sous-répertoire ocsreports.

- Créera la structure du répertoire /ocsreports.
- Créera la structure du répertoire /download.
- Copiera les fichiers dans le répertoire /ocsreports.
- Fixera les permissions des fichiers et des répertoires afin de permettre au démon Apache de lire et d'écrire les répertoires requis (accès en écriture est requis sur /ocsreports, /ocsreports/ipd et /download, cf § [la section intitulée « Permissions sur les fichiers et répertoires sous Linux »](#)).
- Configurera le script PERL ipdiscover-util.pl pour accéder à la base de données et l'installer.

```
root@fedora4:~/server
Configuring IPDISCOVER-UTIL Perl script.
Installing IPDISCOVER-UTIL Perl script.
Fixing permissions on IPDISCOVER-UTIL Perl script.

-----
| OK, Administration server installation finished ;-) |
| Point your browser to http://server/ocsreports to |
| configure database server and create/update schema. |
-----

Setup has created a log file setup.log. Please, save this file.
If you encounter error while running OCS Inventory NG Management server,
we can ask you to show us his content !

DON'T FORGET TO RESTART APACHE DAEMON !

Enjoy OCS Inventory NG ;-)

[root@fedora4 server]#
```

Maintenant, vous pouvez redémarrer le serveur web Apache pour que les changements prennent effet.

- /etc/init.d/httpd restart ou /etc/init.d/apache restart

```
root@fedora4:~/server
Installing IPDISCOVER-UTIL Perl script.
Fixing permissions on IPDISCOVER-UTIL Perl script.

-----
| OK, Administration server installation finished ;-) |
| Point your browser to http://server/ocsreports to |
| configure database server and create/update schema. |
-----

Setup has created a log file setup.log. Please, save this file.
If you encounter error while running OCS Inventory NG Management server,
we can ask you to show us his content !

DON'T FORGET TO RESTART APACHE DAEMON !

Enjoy OCS Inventory NG ;-)

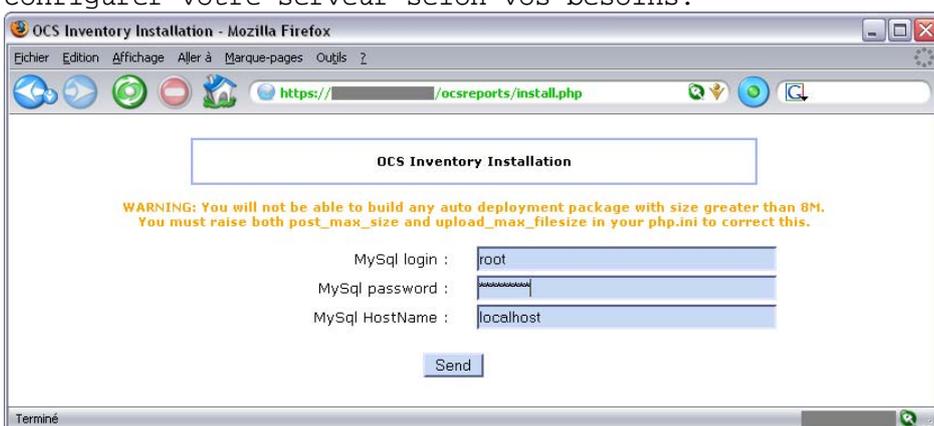
[root@fedora4 server]# /etc/init.d/httpd restart
Arrêt de httpd : [ OK ]
Démarrage de httpd : [ OK ]
[root@fedora4 server]#
```

## Configurer le serveur de gestion

Ouvrez votre navigateur internet favori et pointez sur l'URL [http://your\\_server\\_admin\\_console/ocsreports](http://your_server_admin_console/ocsreports) pour vous connecter à votre serveur d'administration.

Comme la base de données n'est pas encore créée, son processus d'installation OCS Inventory NG va commencer. Toutefois, vous pourrez à nouveau utiliser le processus d'installation en allant sur l'URL [http://your\\_server\\_admin\\_console/ocsreports/install.php](http://your_server_admin_console/ocsreports/install.php) (Ceci doit être utilisé lors d'une mise-à-jour du serveur de gestion OCS Inventory NG).

N.B. : Vous devriez faire attention à la taille maximale des paquets que vous pouvez déployer. S'il-vous-plaît, lisez § [la section intitulée Taille du téléversement pour le déploiement des paquets](#) pour configurer votre serveur selon vos besoins.



Restituez les informations pour se connecter au serveur de base de données MySQL, soit un utilisateur qui a les droits de créer les bases de données, des tables, index, etc ... (habituellement root) :

- Nom de l'utilisateur MySQL
- Mot de passe de l'utilisateur MySQL
- Nom de l'hôte MySQL

N.B. : L'installateur créera la base de données "ocsweb", l'utilisateur MySQL "ocs" avec un mot-de-passe "ocs".

Il donnera aussi à l'utilisateur "ocs" les privilèges "Select | Insert | Update | Delete | Create | Drop | References | Index | Alter | Create temp | Lock" sur la base de données "ocsweb". L'utilisateur sera utilisé par le serveur d'Administration et le serveur de

Communication pour se connecter à la base de données.

Si vous ne voulez pas utiliser l'utilisateur MySQL par défaut "ocs" avec son mot-de-passe "ocs", vous devez mettre-à-jour dans le fichier "dbconfig.inc.php" la variable constante PHP "COMPTE\_BASE", qui est le login de l'utilisateur, et "PSWD\_BASE", qui est le mot-de-passe utilisateur. Ne pas oublier de mettre-à-jour aussi le fichier de configuration du serveur de Communication, spécifiquement son fichier de configuration Apache.

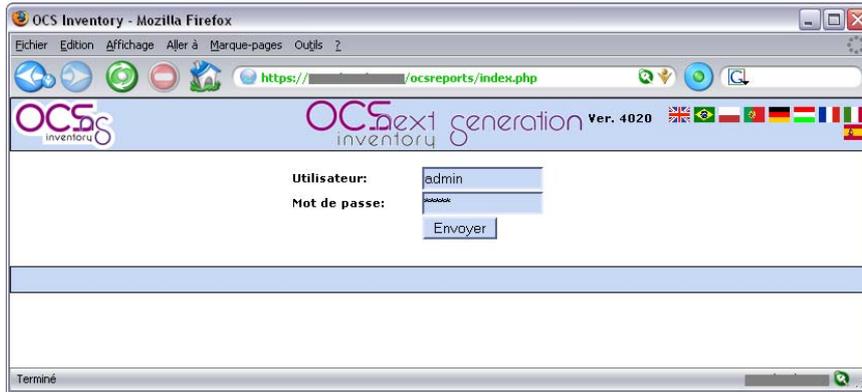
Finalement, vous devriez remplir un texte décrivant le TAG, un caractère affiché au premier lancement de l'agent demandant à l'utilisateur d'entrer la valeur du TAG. C'est une donnée générique qui vous permet de trier les nouveaux ordinateurs (site géographique, "first floor", chambre de John, ...). Si vous ne voulez pas de cette fonctionnalité, laissez à blanc.



La configuration du serveur de Gestion est maintenant terminée !



Faites juste pointer votre navigateur internet à l'URL [http://serveur\\_administration/ocsreports/](http://serveur_administration/ocsreports/) et loguez vous avec l'utilisateur "admin" et son mot-de-passe "admin".



## Mettre-à-jour le serveur de gestion

Quand de nouvelles versions du serveur de communication et de la console d'administration sont effectives, vous pouvez mettre-à-jour votre installation.

N.B. : Assurez vous que le moteur InnoDB de MySQL soit actif sur votre serveur de base de données.

Ouvrez le fichier my.cnf et assurez vous qu'il n'y ait pas de ligne "skip-innodb" ou que cette ligne soit mise en commentaire (par le symbole #).

**Sauvegardez votre base de donnée avant la mise-à-jour !**

**Si vous rencontrez une erreur durant la mise-à-jour, restaurez votre base de données, puis mettez-à-jour votre serveur MySQL vers la version 4.1.20 ou une version supérieure. Ensuite, reprenez la procédure de mise-à-jour.**

Pour mettre-à-jour le serveur de communication et la console d'administration, vous devez suivre les instructions décrites dans § [la section intitulée Installer le serveur de gestion](#). Vous n'avez pas besoin de mettre-à-jour les modules PERL si ce n'est pas requis dans les notes de version.

Alors, faites pointer votre navigateur internet favori à l'URL [http://serveur\\_administration/ocsreports/](http://serveur_administration/ocsreports/), il fera alors fonctionner le processus de mise-à-jour pour s'assurer que le schéma de la base de données et les données par défaut sont mise-à-jour. Le processus de mise-à-jour regardera la configuration du serveur de gestion tel que dans § [la section intitulée Configurer le serveur de gestion](#).

N.B. : Vous devriez faire attention à la taille maximale des paquets que vous pouvez déployer.

SVP, lisez § [la section intitulée Taille du téléversement pour le déploiement des paquets](#)

pour configurer votre serveur selon vos besoins.

Ecrivez dans les champs adéquates le nom de l'administrateur MySQL (habituellement root) et son mot-de-passe, le nom d'hôte du serveur de base de données MySQL, puis cliquez sur le bouton [ Envoyer ].

Finalement, vous pouvez remplir le champ texte décrivant le TAG si vous voulez l'utiliser.

## Sur un système d'exploitation Windows

Vous avez choisi le paquet OCS Inventory NG pour Windows, qui est un paquet intégrant tous les composants nécessaires. En tant que tel, les 3 composants du serveur de gestion (serveur de base de données, serveur de communication, et serveur web d'administration) sont installés sur le même ordinateur.

Le serveur OCS Inventory NG 1.0 pour Windows est basé sur ApacheFriends XAMPP version 1.5.5 (<http://www.apachefriends.org/fr/index.html>) qui installera les composants suivant sur votre ordinateur :

- Apache 2.2.3
- MySQL 5.0.27
- PHP 5.2.20 + PHP 4.4.4 + PEAR
- PHP-Switch win32 1.0
- XAMPP Control Version 2.33 de [www.nat32.com](http://www.nat32.com)
- XAMPP Security 1.0
- SQLite 2.8.15
- OpenSSL 0.8.9d
- phpMyAdmin 2.9.1.1
- ADOdb 4.93
- Mercury Mail Transport System pour Win32 et Netware Systems v4.01b
- FileZilla FTP Serveur 0.9.20
- Webalizer 2.01-10
- Zend Optimizer 3.0.2
- eAccelerator 0.9.5 RC1 pour PHP 5.1.6 (mise-en-commentaire dans php.ini)
- Perl 5.8.8
- mod\_perl 2.0.2

N.B. : Même si tous les composants sont installés, vous devriez être capable de choisir les composants que vous voulez démarrer automatiquement.

### Installer le serveur de gestion

**Vous devez avoir les privilèges d'Administrateur pour installer le serveur OCS Inventory NG sous Windows NT4, Windows 2000, Windows XP ou Windows 2003.**

Téléchargez "OCSNG\_WIN32\_SERVER\_1.01.zip" depuis le site web d'OCS Inventory NG, décompressez-le et lancez "OcsWin32ServerSetup.exe".

Si les composants XAMPP (le serveur et les modules Perl) ne sont toujours pas installés, l'installateur vous demandera de les installer. Dans le cas contraire, l'installateur installera automatiquement le serveur OCS Inventory NG dans les répertoires de XAMPP.

Cliquez sur le bouton [ Suivant ] et acceptez la licence.

Choisissez le répertoire d'installation, par défaut "C:\Program Files\OCS Inventory NG". Vous avez besoin de 400 Mo d'espace disque dur libre si les composants XAMPP sont installés, autrement seul 10 Mo seront nécessaires.

N.B. : Durant la mise-à-jour, assurez-vous que l'installateur détecte bien le répertoire incluant le répertoire de XAMPP.

Lisez § [la section intitulée Mettre-à-jour le serveur de gestion.](#)

En suivant, vous pouvez choisir le nom de groupe du programme dans le menu de démarrage, où les icônes d'OCS Inventory NG seront créées, puis cliquez sur le bouton [ Install ] pour démarrer l'installation.

S'il a été choisi d'installer XAMPP, l'installeur lancera en premier l'installation de XAMPP 1.5.5 en mode silencieux. Ceci créera un répertoire "xampp" dans le répertoire d'installation, et un groupe de programme "Apache Friends" dans le menu de démarrage.

Il vous sera demandé de démarrer le Panneau de Contrôle XAMPP. SVP, répondez "Non".

Alors, sera lancé l'installation des modules PERL de XAMPP en mode silencieux.

Enfin, l'installeur installera les fichiers d'OCS Inventory NG, configurera les serveurs Apache et MySQL de XAMPP pour le serveur d'OCS Inventory NG et démarrera automatiquement les serveurs MySQL et Apache.

À la fin du processus, l'installeur lancera votre navigateur internet par défaut pour démarrer la configuration du serveur d'OCS Inventory NG (lire § [la section intitulée Configurer le serveur de gestion](#)).

L'installation est maintenant terminée, et vous pouvez cliquer sur le bouton [ Fermer ].

N.B. : L'installation d'OCS Inventory NG pour Windows a installé les composants de XAMPP dans le sous-répertoire "xampp" du répertoire d'installation choisi. Le répertoire racine des documents du serveur web Apache est localisé dans "htdocs" dans le sous-répertoire de XAMPP. C'est là que les fichiers de la console d'Administration "ocsreports" sont installés.

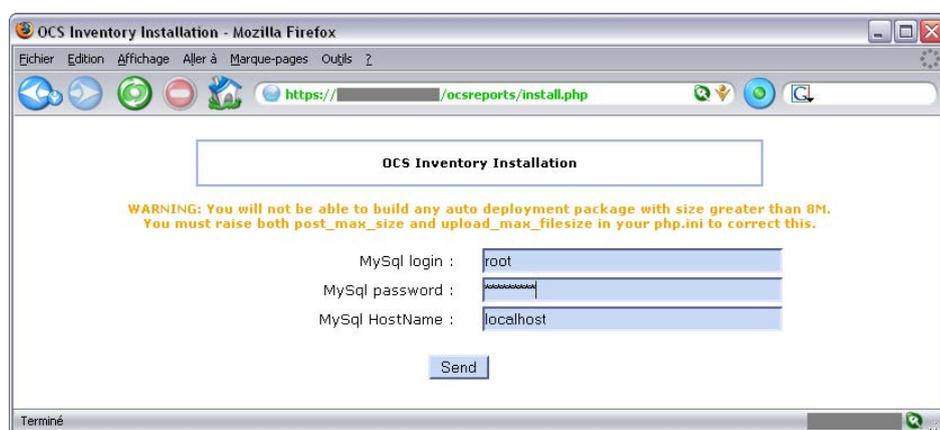
Les fichiers du serveur de Communication sont maintenant localisés dans le répertoire des bibliothèques standards de PERL.  
Les logs d'Apache (access.log, error.log et phperror.log) et le log du serveur de Communication sont localisés dans le sous-répertoire "Apache\Logs".

## Configurer le serveur de gestion

Ouvrez votre navigateur web favori sur le serveur et pointez vers l'URL "<https://localhost/ocsreports>" pour vous connecter au serveur d'Administration.

Vous devrez restituer les informations pour vous connecter au serveur de base de données MySQL avec un utilisateur qui a les droits de créer une base de données, les tables, les index, etc :

- le nom de l'utilisateur MySQL, "root" par défaut,
- le mot-de-passe de l'utilisateur MySQL (le mot-de-passe est vide par défaut)
- le nom de l'hôte MySQL, "localhost"



N.B. : L'installeur créera la base de données "ocsweb", l'utilisateur MySQL "ocs" avec un mot-de-passe "ocs".

Il donnera aussi à l'utilisateur "ocs" les privilèges "Select | Insert | Update | Delete | Create | Drop | References | Index | Alter |

Create temp | Lock" sur la base de données "ocsweb". L'utilisateur sera utilisé par le serveur d'Administration et le serveur de Communication pour se connecter à la base de données.

Si vous ne voulez pas utiliser l'utilisateur MySQL par défaut "ocs" avec son mot-de-passe "ocs", vous devez mettre-à-jour dans le fichier "dbconfig.inc.php" la variable constante PHP "COMPTE\_BASE", qui est le login de l'utilisateur, et "PSWD\_BASE", qui est le mot-de-passe utilisateur. Ne pas oublier de mettre-à-jour aussi le fichier de configuration du serveur de Communication, spécifiquement son fichier de configuration Apache.

Finalement, vous devriez remplir un texte décrivant le TAG, un caractère affiché au premier lancement de l'agent demandant à l'utilisateur d'entrer la valeur du TAG. C'est une donnée générique qui vous permet de trier les nouveaux ordinateurs (site géographique, "first floor", chambre de john, ...). Si vous ne voulez pas de cette fonctionnalité, laissez à blanc.



La configuration du serveur de Gestion est maintenant terminée !



Faites juste pointer votre navigateur internet à l'URL [http://serveur\\_administration/ocsreports/](http://serveur_administration/ocsreports/) et loguez vous avec l'utilisateur "admin" et son mot-de-passe "admin".



## Mettre-à-jour la sécurité des composants de XAMPP

Par défaut, XAMPP est installé sans aucune sécurité. Le compte administrateur MySQL n'a pas de mot-de-passe, l'interface web de configuration XAMPP est accessible par tout le monde sans aucune authentification.

Vous devez modifier cela.

Ouvrez votre navigateur internet favori sur le serveur et pointez-le à cette URL

"<http://localhost/xampp/splash.php>" pour vous connecter à l'interface graphique de configuration de XAMPP.

Cliquez sur la langue du menu de configuration principal de XAMPP à laquelle vous souhaitez accéder. Alors, cliquez sur "Sécurité" dans le menu de gauche. Comme vous pouvez le remarquer, tout est marqué comme "non sécurisé" ou "inconnu" pour les composants non démarrés.

Vous pouvez changer cela en cliquant sur le lien <http://localhost/security/xamppsecurity.php> (en bas de page).

En premier, vous devez remplir les champs du mot-de-passe de l'administrateur MySQL et sélectionnez la méthode d'authentification pour phpMyAdmin.

N.B. : Vous pouvez changer cela à chaque fois que vous visitez la page web de sécurité du serveur XAMPP.

Validez vos changements en cliquant sur le bouton [ Changer le mot de passe ].

Vous pouvez alors protéger l'accès au menu de configuration XAMPP en remplissant les champs utilisateur et mot-de-passe dans la section Protection du Répertoire de XAMPP (.htaccess). Ainsi, l'utilisateur et le mot-de-passe seront demandés lors de la connexion au menu de configuration XAMPP au moyen du navigateur web.

Validez vos changements en cliquant sur le bouton [ Sécuriser XAMPP ].

**Ne chargez pas le safe mode PHP**, que si vous rencontrez des erreurs sur la console d'Administration.

Finalement, vous devez redémarrer les services d'Apache et de MySQL pour que les changements prennent effet.

Ouvrez le Panneau de Contrôle de XAMPP depuis la barre système ou le menu de démarrage "OCS Inventory NG", cliquez sur le bouton [ Stop ] d'Apache puis sur le bouton [ Start ] et faites de même pour MySQL.

Vous pouvez maintenant cliquer à nouveau sur "Sécurité" dans le menu de gauche pour voir que tous les services démarrés sont maintenant sécurisés.

## Mettre-à-jour le serveur de gestion

Pour mettre-à-jour le serveur de communication et la console d'administration, vous devez suivre les instructions décrites dans § [la section intitulée Installer le serveur de gestion](#). Assurez-vous juste que l'installateur détecte correctement l'ancien répertoire d'installation.

Vous n'avez pas besoin de mettre-à-jour les composants de XAMPP, et l'installateur, par défaut, ne sélectionnera pas l'installation des composants de XAMPP. **Si vous voulez le faire et mettre-à-jour les composants de XAMPP, sauvegardez vos bases de données et vos sites web.** Voir § [la section intitulée Sauvegarder et Restaurer la base de donnée d'OCS Inventory NG](#).

À la fin du processus, l'installateur lancera votre navigateur internet par défaut et lancera le processus de mise-à-jour pour s'assurer que le schéma de votre base de données et les données par défaut soient mises-à-jour. Le processus de mise-à-jour regardera la configuration du serveur de gestion tel que dans § [la section intitulée Configurer le serveur de gestion](#).

N.B. : Vous devriez faire attention à la taille maximale des paquets que vous pouvez déployer.

SVP, lisez § [la section intitulée Taille du téléversement pour le déploiement des paquets](#) pour configurer votre serveur selon vos besoins.

Ecrivez dans les champs adéquates le nom de l'administrateur MySQL (habituellement root) et son mot-de-passe, le nom d'hôte du serveur de base de données MySQL, puis cliquez sur le bouton [ Envoyer ].

Finalement, vous pouvez remplir le champ texte décrivant le TAG si vous voulez l'utiliser.

# INSTALLER L'AGENT SUR LES PC CLIENTS

## Contenu :

- [1 Installer l'agent sur les ordinateurs clients](#)
  - [1.1 Sur un système d'exploitation Windows](#)
    - [1.1.1 Quelle version de l'Agent Windows dois-je utiliser ?](#)
      - [1.1.1.1 Comment travaille l'Agent Windows ?](#)
      - [1.1.1.2 Comment le Service Windows travaille ?](#)
      - [1.1.1.3 Dois-je utiliser l'Agent de Service ou l'Agent solo](#)
    - [1.1.2 Installer manuellement la version de l'Agent de Service](#)
    - [1.1.3 Installer manuellement l'Agent Solo \(sans le service\)](#)
    - [1.1.4 Déployer l'Agent en utilisant le lanceur OcsLogon.exe au moyen de script de login ou de GPO Active Directory](#)
      - [1.1.4.1 Déploiement de l'Agent au moyen de GPO Active Directory](#)
      - [1.1.4.2 Déploiement de l'Agent au moyen de script d'ouverture de session](#)
    - [1.1.5 L'Agent et ses arguments de ligne de commande](#)
  - [1.2 Sur un système d'exploitation Unix](#)
    - [1.2.1 Requis](#)
      - [1.2.1.1 Pré-requis pour Linux](#)
    - [1.2.2 Installer l'Agent interactivement](#)
      - [1.2.2.1 Sur Linux](#)
    - [1.2.3 Déployer l'Agent au moyen de script d'installation sans interaction utilisateur](#)
      - [1.2.3.1 Sur Linux](#)
    - [1.2.4 L'Agent et ses arguments de ligne de commande](#)

## Installer l'agent sur les ordinateurs clients

Il y a deux manières d'inventorier un ordinateur client utilisant l'agent d'OCS Inventory NG :

- Si l'ordinateur client ne peut se connecter au serveur OCS Inventory NG, l'inventaire est fait localement et enregistré dans un fichier XML compressé avec l'extension de fichier ".ocs". L'utilisateur peut alors envoyer ce fichier au moyen d'un courriel, d'un disque USB ou de toute autre manière indiquée par l'Administrateur, ce qui lui permettra de l'importer dans la base de données au moyen du serveur d'Administration.
- Si l'ordinateur client peut se connecter en utilisant le protocole HTTP au serveur de Communication à-travers le réseau, l'agent demandera au serveur de Communication les paramètres pour l'inventaire et enverra le résultat de l'inventaire directement au serveur de Communication.

## Sur un système d'exploitation Windows

**L'Agent pour Windows d'OCS Inventory NG est capable de travailler en tant que service**, démarré automatiquement au démarrage de l'ordinateur. **Toutefois, nous fournissons aussi un agent solo ne fonctionnant pas en tant que service**, qui peut être lancé au moyen de script de login, de règle GPO Active Directory, de planificateur de tâche ou d'un raccourci dans le menu de démarrage.

N.B. : Nous recommandons que vous utilisiez l'Agent de service, spécifiquement si vous planifiez d'utiliser la fonctionnalité de déploiement de paquet.

Téléchargez et dézippez OCSNG\_WIN32\_AGENT\_1.01.zip. Ce paquet contient 3 fichiers :

- **OcsAgentSetup.exe**, l'agent installeur de service Windows inclu. Nous recommandons d'utiliser ce paquet.
- **OcsAgent.exe**, qui installera l'agent solo sur un ordinateur non connecté à un réseau qui permettra de faire fonctionner l'inventaire manuellement avec l'argument de ligne de commande /LOCAL (ou si vous ne voulez pas utiliser l'agent de service).
- **OcsLogon**, lanceur de l'agent OCS Inventory NG à utiliser quand vous déployez l'agent au moyen de script de login ou de règle GPO Active Directory sur le domaine. Si l'agent est toujours installé, il fera juste fonctionner l'agent. Dans le cas contraire, il téléchargera le binaire de l'agent depuis le serveur de Communication, l'installera et le lancera.

## Quelle version de l'Agent Windows dois-je utiliser ?

En premier, nous allons expliquer comment l'Agent et le Service fonctionnent.

### *Comment travaille l'Agent Windows ?*

Quand l'Agent OCS Inventory NG "OCSInventory.exe" est lancé, il contacte le serveur de Communication en utilisant le protocole HTTP pour lui demander ce qu'il doit faire. Le Serveur peut lui répondre "nothing" (pas le moment pour un inventaire ou aucun paquet à déployer), alors l'agent s'arrête.

Quand l'agent est lancé, il génère seulement l'inventaire et l'envoi.

Autrement, le Serveur peut répondre à l'Agent :

- **Envoie un inventaire** : l'agent reçoit toutes les propriétés de l'ordinateur et les envoie au serveur en utilisant le protocole HTTP. Le Serveur demande cela si seulement la date du dernier inventaire dans la base de données est plus vieille que l'option de configuration générale "FREQUENCY", spécifiée en jours. (Voir [la section intitulée Gérer les options générales d'OCS Inventory NG](#)).
- **Découvre le réseau** : l'agent reçoit toutes les propriétés de l'ordinateur, scanne son segment de réseau pour découvrir les matériels actifs écoutant le réseau, et envoie ces informations au serveur en utilisant le protocole HTTP. Le Serveur demande cela si seulement il a été choisi de faire fonctionner l'option "IPDISCOVERY" (voir § [la section intitulée Utiliser la fonctionnalité de découverte IP](#)).
- **Déploie un paquet** : l'agent contacte le serveur de déploiement en utilisant le protocole HTTPS pour avoir le fichier d'information, télécharger les fragments de paquets depuis le dépôt, le paquet reconstruit et le lance.

N.B. : L'Agent OCS Inventory NG n'écoute pas le réseau. Cela est toujours initié par le serveur de communication.

Ainsi, vous n'avez pas à ouvrir de port dans votre pare-feu personnel. Mais vous pouvez permettre le fichier "OCSInventory.exe" de l'agent d'OCS Inventory NG à contacter le Serveur de Communication ou le Serveur de Déploiement en utilisant HTTP ou HTTPS.

Chaque fois que l'inventaire est fait, l'Agent écrit un fichier de configuration "OCSInventory.dat" dans son propre répertoire où il y met les options de configuration téléchargées depuis le serveur de communication.

Quand il est lancé pour la première fois, l'Agent OCS Inventory NG demandera à l'utilisateur la valeur du TAG (si la fonctionnalité est activée). Un texte d'aide est affiché dans la boîte de dialogue à l'identique de celui que vous avez entré lors de la [configuration du serveur de gestion](#). L'utilisateur peut entrer la même valeur, ou laisser à blanc (vous pourrez mettre-à-jour cette valeur au moyen du serveur d'Administration).

Alors (ou au contraire, si la fonctionnalité TAG n'est pas active), il fera l'inventaire et enverra les résultats de l'inventaire au serveur de Communication par le biais de HTTP.

### ***Comment le Service Windows travaille ?***

N.B. : Vous devez avoir les privilèges d'Administrateur pour installer l'Agent d'OCS Inventory NG en tant que service, ou vous devez utiliser le Packager d'OCS Inventory NG pour créer un installateur qui soit capable de fonctionner même si vous n'avez pas les droits d'Administrateur.

Référez-vous à [la section intitulée Téléverser l'Agent pour le déploiement au moyen du lanceur "OcsLogon.exe"](#) ou la documentation du Packager OCS Inventory NG.

L'Agent OCS Inventory NG "OCSInventory.exe" est lancé par le service "OcsService.exe" chaque heure PROLOG\_HOUR définie. Il garde trace du compte-à-rebours en secondes dans le fichier "service.ini" (valeur TTO\_WAIT) ainsi que le temps de fonctionnement EFFECTIVE.

Le nombre d'heures d'attente est aléatoire à chaque moment d'installation et à chaque moment PROLOG\_FREQ défini dans la console d'Administration.

Il fait en sorte que tous les agents n'aient pas à contacter en même temps le serveur de Communication. Le réarrangement aléatoire est définie entre 0 et la valeur PROLOG\_FREQ.

Vous pouvez ajuster ces paramètres en considérant la charge du serveur.

Quand l'agent de service est lancé, il est appelé en utilisant les arguments de lignes de commande spécifiés dans la valeur "Miscellaneous" dans le fichier "service.ini".

```
[OCS_SERVICE]
NoProxy=1
Server=my_server_ocs.domain.tld
Pnum=80
Miscellaneous=/DEBUG /NP /SERVER:my_server_ocs.domain.tld /pnum:80
PROLOG_FREQ=10
OLD_PROLOG_FREQ=10
TTO_WAIT=1505
```

Comme vous pouvez le voir, le Service est seulement un lanceur qui fera fonctionner l'Agent régulièrement, même s'il n'y a aucun log sur l'ordinateur.

### ***Dois-je utiliser l'Agent de Service ou l'Agent solo***

#### **Vous voulez avoir les ordinateurs inventoriés, même si vous n'avez aucun log ?**

Utilisez l'Agent de Service.

**Vous voulez utiliser la fonctionnalité de déploiement de paquets ?** Utilisez l'Agent de Service. En tant que tel, le paquet sera téléchargé en tâche de fond, l'utilisateur connecté pouvant continuer à travailler.

**Vous ne voulez pas du service d'installation, ou que quelques écritures apparaissent dans la base de registre ?** Utilisez l'Agent solo. Toutefois, le déploiement de paquets peut prendre plus de temps quand l'utilisateur est connecté.

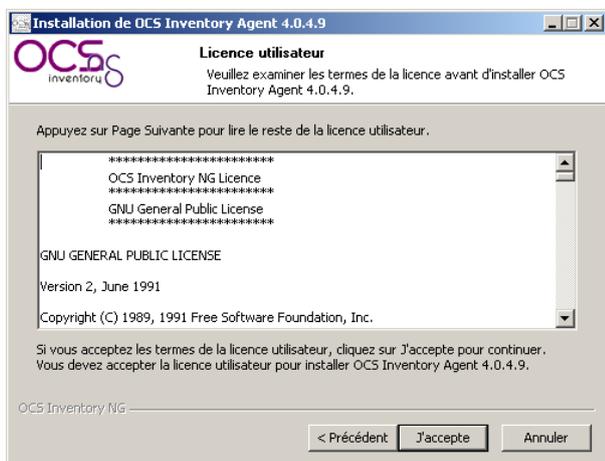
En d'autres mots, nous recommandons l'agent de service.

## Installer manuellement la version de l'Agent de Service

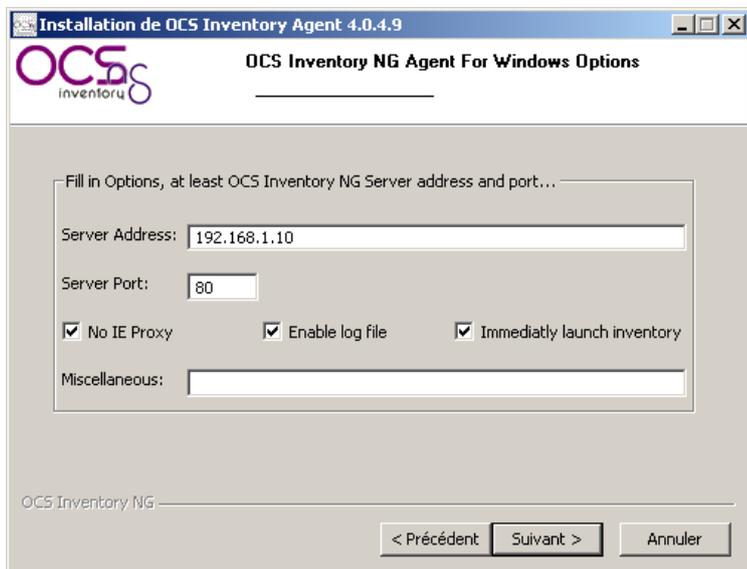
Faites fonctionner "OcsAgentSetup.exe" sur l'ordinateur client et cliquez sur le bouton [ Suivant > ].



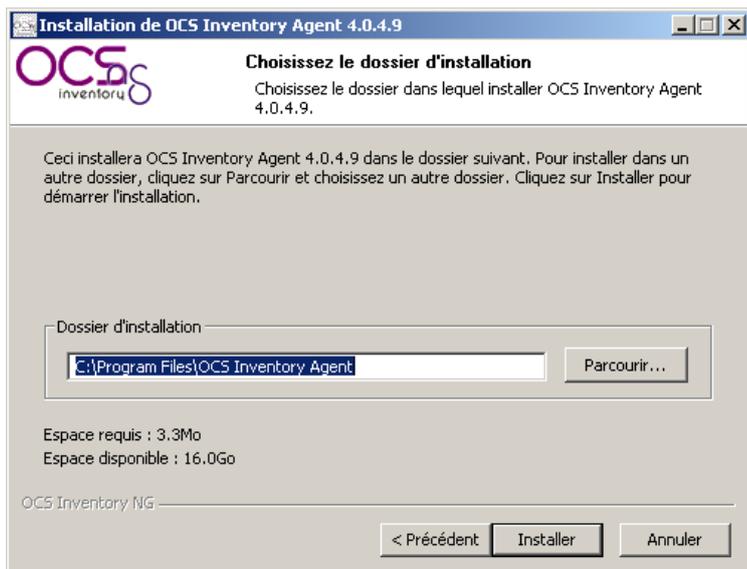
Validez la licence en cliquant sur le bouton [ J'accepte ].



Remplissez les champs de l'adresse et du port du serveur de Communication OCS Inventory NG. Si vous ne voulez pas utiliser les paramètres du proxy de Microsoft Internet Explorer (par exemple, parce que votre proxy requiert l'authentification), cliquez sur l'option "No Proxy". Le champ "Miscellaneous" permet de passer à l'agent des arguments en ligne de commande. (cf § [la section intitulée L'Agent et ses arguments de ligne de commande](#)). Alors, cliquez sur le bouton [ Suivant > ].



Choisissez le répertoire de destination, par défaut "C:\Program Files\OCS Inventory Agent\", et cliquez sur le bouton [ Installer ].



Cliquez sur le bouton [ Fermer ] pour enregistrer l'Agent de Service OCS Inventory NG dans le système.



L'Agent est maintenant installé en tant que service automatiquement démarré au démarrage du système sous le compte LocalSystem.

Ceci est la méthode d'installation interactive. Toutefois, le processus requiert que vous le lanciez sur tous les ordinateurs. Heureusement, l'installation peut se faire grâce aux scripts.

N.B. : L'installateur de l'Agent de Service supporte en ligne de commande tous les arguments de l'agent définis dans [la section intitulée L'Agent et ses arguments de ligne de commande](#).

L'installateur de l'Agent de Service "OcsAgentSetup.exe" peut être appelé avec quelques paramètres de ligne de commande :

- /S pour faire fonctionner l'installation en mode silencieux, sans aucune interaction utilisateur
- /UPGRADE pour mettre-à-jour une installation existante de l'Agent de Service.
- /NOSPLASH pour désactiver l'écran d'accueil,
- /NoOcs\_ContactLnk pour désactiver le raccourcis Ocs-Contact dans le menu Démarrer,

- /D= pour spécifier un chemin d'installation, (doit être le **dernier** paramètre sans ["] Ex: /D=E:\my install folder)
- et tous les arguments de ligne de commande de l'Agent, spécifiquement /SERVER pour spécifier l'adresse du serveur de Communication quand est utilisée l'installation en mode silencieux. (voir [la section intitulée L'Agent et ses arguments de ligne de commande](#)).

## Installer manuellement l'Agent Solo (sans le service)

Cette manière est très pratique sur un ordinateur non connecté à un réseau.

L'installateur peut fonctionner avec les droits d'un utilisateur normal, ou mieux avec ceux de l'administrateur système.

Vous avez juste à faire fonctionner l'exécutable ainsi "OcsAgent.exe /LOCAL" pour lancer l'installateur de l'Agent OCS Inventory NG. L'installateur essaiera d'installer les fichiers de l'agent OCS Inventory NG dans le répertoire "C:\ocs-ng" ou, si vous n'avez pas les permissions nécessaires pour créer un répertoire à la racine du système, dans un répertoire "ocs-ng" créé dans le répertoire temporaire lié à votre connexion. Alors, il lancera l'agent OCS Inventory NG.

L'Agent demandera à l'utilisateur sous quel répertoire il devra sauvegarder les résultats de l'inventaire.

Lors de son premier lancement, l'agent OCS Inventory NG demandera la valeur du TAG. L'utilisateur pourra entrer la valeur ou laisser à blanc (vous pourrez modifier cette valeur au moyen du serveur d'administration).

Quand l'inventaire sera terminé, l'agent affichera un message à l'utilisateur l'informant où est enregistré le fichier de résultat d'inventaire et son nom.

L'utilisateur a juste à envoyer le fichier à l'administrateur. L'administrateur pourra alors importer les résultats d'inventaire dans la base de données au moyen du serveur d'administration.

Si vous voulez un autre inventaire, vous n'aurez qu'à faire fonctionner "**Ocsinventory.exe /LOCAL**" depuis le répertoire d'installation de l'agent d'OCS Inventory NG.

N.B. : L'installateur de l'Agent Solo supporte en ligne de commande tous les arguments d'Agent définis dans [la section intitulée L'Agent et ses arguments de ligne de commande](#).

## Déployer l'Agent en utilisant le lanceur OcsLogon.exe au moyen de script de login ou de GPO Active Directory

Le lanceur "OcsLogon.exe" est un petit outil capable de fonctionner dans un script d'ouverture de session ou dans une règle GPO d'Active Directory. Son but est de lancer l'agent OCS Inventory NG sur chaque ordinateur, et si l'Agent n'est pas installé de l'installer.

Le lanceur "OcsLogon.exe" essaiera par défaut de se connecter au Serveur de Communication en utilisant le nom DNS suivant "ocsinventory-ng", tout comme quand vous ouvrez votre navigateur internet favori et que vous entriez l'URL <http://ocsinventory-ng/ocsinventory>.

Pour utiliser une adresse URL différente si vous n'avez pas ajouté ce nom DNS, il faut juste renommer "OcsLogon.exe" par le nom DNS ou l'adresse IP de votre Serveur de Communication (par exemple, "ocsinventory-ng.domain.tld.exe" si vous avez créé pour votre serveur un enregistrement DNS "ocsinventory-ng.domain.tld" ou "192.168.1.2.exe" si votre serveur a pour adresse IP "192.168.1.2"). Le

lanceur essayera de se connecter au nom DNS ou à l'adresse IP que vous avez nommé.  
(<http://ocsinventory-ng.domain.tld/ocsinventory> ou <http://192.168.1.2/ocsinventory>).

N.B. : Utilisez toujours la dernière version d'OcsLogon.exe.  
Vous pouvez obtenir celui-ci avec le dernier paquet OCSNG\_WIN32\_AGENT\_xx.zip

Le lanceur vérifiera une première fois si l'agent OCS Inventory NG est installé, et si il ne l'est pas, il contactera le Serveur de Communication en HTTP pour télécharger les derniers binaires de l'agent et l'installera localement sur l'ordinateur :

- **L'Agent Solo dans le répertoire "C:\ocs-ng"** par défaut ou, si l'utilisateur connecté n'a pas les permissions de créer un répertoire à la racine du système, dans un répertoire "ocs-ng" dans le répertoire temporaire de l'utilisateur. Si l'Agent Solo est installé, le lanceur le fera fonctionner.
- **L'Agent de Service dans le répertoire "C:\Program Files\OCS Inventory Agent"** par défaut.

N.B. : Pour déployer l'Agent Solo avec le lanceur, **vous avez besoin de téléverser le fichier "ocsagent.exe" de l'Agent Solo** avec la Console d'Administration.

Pour déployer l'Agent de Service avec le lanceur, **vous avez besoin de téléverser le fichier "ocspackage.exe" de l'Agent de Service** avec la Console d'Administration.

Référez-vous à § [la section intitulée Téléverser l'Agent pour le déploiement au moyen du lanceur "OcsLogon.exe"](#).

**Pour choisir entre l'Agent Solo ou de Service, il y a juste à spécifier l'argument "/INSTALL" si vous voulez utiliser le Service ou non. Si vous ajoutez l'argument de ligne de commande "/INSTALL", le lanceur utilisera l'Agent de Service. Autrement, il utilisera l'Agent Solo.**

Si vous voulez mettre-à-jour l'Agent, vous devez spécifier dans le lanceur la version de la nouvelle version avec l'argument "/DEPLOY:XXXX" où XXXX est la version de l'agent, 4301 pour la version 1.01.

### ***Déploiement de l'Agent au moyen de GPO Active Directory***

N.B. : Nous recommandons d'utiliser l'Agent de Service si vous planifiez d'utiliser la fonctionnalité de déploiement de paquets.

**Pour déployer l'Agent Solo** avec le lanceur, **vous avez besoin de téléverser le fichier "ocsagent.exe"** avec la Console d'Administration.

**Pour déployer l'Agent de Service** avec le lanceur, **vous avez besoin de téléverser le fichier "ocspackage.exe"** avec la Console d'Administration **et d'utiliser l'argument de ligne de commande /INSTALL** avec le lanceur.

Référez-vous à § [la section intitulée Téléverser l'Agent pour le déploiement au moyen du lanceur "OcsLogon.exe"](#).

Ouvrir la console "Utilisateurs et ordinateurs Active Directory".

Faites un clic-droit sur votre nom de domaine Active Directory ou Unité Organisationnelle et sélectionnez "Propriété".

Dans l'onglet "Stratégie de Groupe", créez une nouvelle stratégie, ou éditez une existante.

Vous utiliserez l'une ou l'autre des stratégies, de l'Ordinateur ou de l'Utilisateur. La configuration de la stratégie ordinateur sera lancé au démarrage de l'ordinateur, celle de l'utilisateur lors de sa connexion.

N.B. : Dans notre exemple, vous utiliserez Configuration Ordinateur > Script > Démarrage. L'adresse du Serveur de Communication est 192.168.1.2, parce que nous avons choisi d'installer la version de l'Agent de Service. Si vous avez choisi d'utiliser l'Agent Solo, il sera préférable d'utiliser Configuration Utilisateur > Script > Démarrage, pour permettre à l'agent de fonctionner à chaque fois que l'utilisateur sera connecté.

Ouvrir l'arbre "Configuration Ordinateur" dans le panneau gauche, puis allez à "Paramètres Windows" et "Scripts (démarrage/arrêt)". Alors, double-cliquez sur "Démarrage" dans le panneau droit.

Cliquez sur le bouton "Voir les fichiers" pour afficher les fichiers et scripts exécutables, utilisables par les scripts de démarrage de l'ordinateur.

Copiez le lanceur "OcsLogon.exe" ou renommez-le (dans notre exemple "192.168.1.2.exe") dans le répertoire pour permettre au script de démarrage de l'utiliser.

En suivant, fermez le répertoire "Startup" et cliquez sur le bouton [ Ajouter ], cliquez sur le bouton [ Parcourir ] pour sélectionner le lanceur "OcsLogon.exe" ou celui que vous avez renommé (dans notre exemple "192.168.1.2.exe") et restituez les paramètres du lanceur dans le champ "Paramètres de script" (dans notre exemple, "/S" pour installation silencieuse, "/DEBUG" pour permettre la création de fichier log, "/NP" pour désactiver l'usage des paramètres de proxy d'Internet Explorer, "/INSTALL" pour déployer l'Agent de Service, "/DEPLOY:4029" pour forcer le déploiement de la version 4029, "/SERVER:192.168.1.2" pour utiliser l'adresse IP 192.168.1.2 du Serveur de Communication).

Validez toutes les fenêtres pour activer la règle GPO.

Quand l'ordinateur démarrera (ou quand l'utilisateur se connectera si vous avez utilisé les règles utilisateurs), le lanceur installera et/ou lancera l'agent OCS Inventory NG.

N.B. : Le lanceur OcsLogon.exe peut rencontrer des problèmes pour accéder au Serveur de Communication si vous avez configuré un proxy avec authentification dans les paramètres d'Internet Explorer. Vous pouvez forcer le lanceur à ne pas utiliser les paramètres de proxy avec l'argument de ligne de commande "/NP". Vous pouvez aussi spécifier un port différent pour communiquer avec le Serveur de Communication avec l'argument de ligne de commande "/PNUM:XX" où XX est le numéro de port à utiliser.

Lire § [la section intitulée L'Agent et ses arguments de ligne de commande](#).

### ***Déploiement de l'Agent au moyen de script d'ouverture de session***

N.B. : Nous recommandons d'utiliser l'Agent de Service si vous planifiez d'utiliser la fonctionnalité de déploiement de paquets.

**Pour déployer l'Agent Solo** avec le lanceur, **vous avez besoin de téléverser le fichier "ocsagent.exe"** avec la Console d'Administration.

**Pour déployer l'Agent de Service** avec le lanceur, **vous avez besoin de téléverser le fichier "ocspackage.exe"** avec la Console d'Administration **et d'utiliser l'argument de ligne de commande /INSTALL** avec le lanceur.

Référez-vous à § [la section intitulée Téléverser l'Agent pour le déploiement au moyen du lanceur "OcsLogon.exe"](#).

Copiez le fichier "OcsLogon.exe" (ou celui que vous avez renommé) vers le répertoire partagé sur le réseau. Celui-ci doit être lisible par tout utilisateur. Alors, ajoutez un appel à "OcsLogon.exe" (ou celui que vous avez renommé) dans votre script de Login utilisateur.

Voici un exemple de script d'ouverture de session :

```
@echo off
echo Running system inventory, please wait...
REM Call to OCS Inventory NG agent for deployment
REM Using shared folder MY_SHARE on server MY_SERVER
REM Connect to Communication server at address 192.168.1.2
REM Enable debug log with /DEBUG to create OcsLogon.log and computer_name.log
REM Force setup agent version 4030 if agent not up to date
REM Deploy service version of agent using /INSTALL
"\\MY_SERVER\MY_SHARE\192.168.1.2.exe" /DEBUG /NP /INSTALL /DEPLOY:4030
echo Done. Thanks a lot.
```

N.B. : Pour être conforme avec Windows 9X, vous devez enfermer le nom du chemin vers le lanceur entre double-quotes, autrement Windows 9X ne serait pas capable de l'utiliser, mais restituerait un nom tel que "192~1.exe", le lanceur ne serait pas capable de trouver correctement l'adresse IP ou le nom DNS.

Mettez ce script - nommé "ocs.bat" par exemple - sur votre Contrôleur de Domaine dans le répertoire "%WINDIR%\SYSVOL\Domain\Scripts", où "%WINDIR%" est généralement "C:\WINNT" ou "C:\Windows".

Ensuite, vous devez lier le script d'ouverture de session à chaque utilisateur enregistré dans votre domaine Active Directory. Vous devez utiliser pour cela l'outil "Utilisateurs et ordinateurs Active Directory".

Pour chaque utilisateur, ouvrez ses propriétés et dans l'onglet "Profil", ajoutez le nom du script d'ouverture de session dans le champ "Script d'ouverture de session".

Quand l'utilisateur se connectera, le lanceur installera et/ou lancera OCS Inventory NG.

N.B. : Le lanceur OcsLogon.exe peut rencontrer des problèmes pour accéder au Serveur de Communication si vous avez configuré un proxy avec authentification dans les paramètres d'Internet Explorer. Vous pouvez forcer le lanceur à ne pas utiliser les paramètres de proxy avec l'argument de ligne de commande "/NP". Vous pouvez aussi spécifier un port différent pour communiquer avec le Serveur de Communication avec l'argument de ligne de commande "/PNUM:XX" où XX est le numéro de port à utiliser.

Lire § [la section intitulée L'Agent et ses arguments de ligne de commande.](#)

## L'Agent et ses arguments de ligne de commande

Les versions 4.0.1.0 et supérieures de l'agent OCS Inventory NG inclut quelques arguments de ligne de commande pour permettre de détecter des erreurs.

Une fois que l'agent est installé, vous pouvez le lancer manuellement pour diagnostiquer les problèmes. Utilisez en ligne de commande "C:\ocs-ng\OCSInventory.exe [options]" (pour l'agent solo) ou "C:\Program Files\OCS Inventory Agent\OCSInventory.exe [options]" (pour l'agent de service) où [options] doivent être les arguments de ligne de commandes suivants :

L'Agent et ses arguments de ligne de commande	
Arguments	Énoncé
<b>/server:[server name]</b>	Demande à l'agent de se connecter au serveur ayant tel nom « [nom serveur] »
<b>/np</b>	Désactive l'usage du proxy défini dans les paramètres d'Internet Explorer.
<b>/pnum:XX</b>	Spécifie un port IP pour communiquer avec le serveur de communication. Par exemple, vous pouvez forcer l'usage du port 8080 avec l'argument /pnum:8080.
<b>/local</b>	Faire fonctionner l'agent en mode inventaire local. Ainsi, l'agent n'essayera pas de communiquer avec le serveur de communication. Un fichier « {hostname}.ocs », en XML compressé contenant les résultats de l'inventaire, sera créé dans le répertoire de l'agent.
<b>/file</b>	Identique à /local, mais interagit avec le serveur de communication.
<b>/xml</b>	L'agent créera un fichier XML non compressé « {hostname}.xml », contenant les résultats de l'inventaire dans son répertoire.
<b>/notag</b>	Le client ne demande pas à l'utilisateur la valeur TAG.
<b>/tag:« valeur »</b>	Spécifie la valeur TAG.
<b>/hkcu</b>	Force agent to search for installed software also under HKEY_CURRENT_USER registry hive.
<b>/debug</b>	Crée un fichier log « {hostname}.log » dans le répertoire de l'agent.
<b>/force</b>	Force l'agent à toujours envoyer les résultats de l'inventaire, indépendamment du paramètre FREQUENCY.
<b>/uid</b>	Force l'agent à générer un nouveau deviceid.
<b>/dmi</b>	Si le numéro de série de l'ordinateur ne peut être reçu avec WMI, cela force l'agent à utiliser les tables DMI pendant que fonctionne l'outil « BiosInfo.exe ». Autrement, l'agent essaiera en premier les fonctions BIOS et ensuite les tables DMI.
<b>/biosfunc</b>	Si le numéro de série de l'ordinateur ne peut être reçu avec WMI, cela force l'agent à utiliser les fonctions BIOS pendant que fonctionne l'outil « BiosInfo.exe ». Autrement, l'agent essaiera en premier les fonctions BIOS et ensuite les tables DMI.
<b>/conf:[filename]</b>	Demande à l'agent d'utiliser le fichier « [filename] » comme fichier de configuration. Autrement, il utilisera par défaut le fichier « Ocsinventory.dat ».
<b>/test</b>	L'agent testera seulement la connexion HTTP au serveur de communication et écrira un fichier « ok.ok » si tout est bon. Peut-être utilisé seulement avec les arguments /DEBUG, /NP et /PNUM (désactivé avec tous les autres).
<b>/ipdisc:[network number]</b>	Force l'agent à faire fonctionner la fonctionnalité IPDISCOVERY sur le réseau nommé « [network number] » si le serveur demande un inventaire. Il peut être utilisé en conjonction avec /FORCE pour s'assurer de son fonctionnement. Ne peut être utilisé avec /LOCAL.
<b>/fastip</b>	L'agent scanne seulement 5 IPs s'il est élu comme hôte IPDISCOVER (à utiliser seulement en débogage ou en test, pas en production).

Quand vous utilisez le lanceur "OcsLogon.exe" pour déployer ou faire fonctionner l'agent, vous pouvez utiliser les arguments de lignes de commandes suivants :

N.B. : Vous pouvez aussi ajouter tous les arguments supportés par l'agent OCS Inventory NG.

Le lanceur et ses arguments de ligne de commande	
Arguments	Énoncé
<b>/DEPLOY:XXXX</b>	Force le déploiement d'une version XXXX spécifique de l'agent. Utilisez "/DEPLOY:4030" pour mettre-à-jour l'agent à la version 4.0.3.0
<b>/INSTALL</b>	Demande au lanceur d'installer l'Agent de Service, au lieu de l'Agent Solo.
<b>/URL:[download_url]</b>	Demande au lanceur de télécharger l'Agent Solo "ocsagent.exe" ou l'Agent de Service "ocspackage.exe" depuis "[download_url]" (sans le nom de fichier). Utilisable pour le déploiement de l'Agent dans de multiples domaines Active Directory, mais utilisant un seul serveur de Communication.
<b>/NP</b>	Désactive l'usage du proxy défini dans les paramètres d'Internet Explorer.
<b>/PNUM:X</b>	Spécifie un numéro de port pour communiquer avec le serveur de communication. Par défaut, le port HTTP 80 est utilisé. Vous pouvez forcer l'usage du port 8080 par exemple avec l'argument "/PNUM:8080".
<b>/LOCAL</b>	Faire fonctionner l'agent en mode inventaire local. Ainsi, l'agent n'essaiera pas de se connecter au serveur de communication. Un fichier "{hostname}.ocs" contenant les résultats de l'inventaire, en XML compressé, sera créé dans le répertoire de l'agent.
<b>/NOTAG</b>	Le client ne demande pas à l'utilisateur la valeur TAG.
<b>/TAG:"valeur"</b>	Spécifie la valeur TAG en ligne de commande.
<b>/DEBUG</b>	Crée un fichier log "{hostname}.log" dans le répertoire de l'agent.
<b>/FOLDER:[PATH]</b>	Demande au lanceur d'installer l'agent dans le répertoire d'installation nommé "[PATH]". DOIT ÊTRE LE DERNIER ARGUMENT !

## Sur un système d'exploitation Unix

L'Agent \*nix peut seulement être installé localement. Vous ne pouvez pas déployer l'agent au moyen du réseau comme cela est possible pour l'agent Windows. Toutefois, vous pouvez choisir durant l'installation d'activer la mise-à-jour automatique de l'agent si vous choisissez la méthode d'inventaire par protocole HTTP.

N.B. : Vous devez avoir les privilèges d'Administrateur pour installer le serveur d'administration.

## Requis

### Pré-requis pour Linux

L'agent OCS Inventory pour Linux requiert :

- dmidecode version 2.2 ou supérieure
- PERL 5.6 ou supérieur
  - Module PERL XML::Simple version 2.12 ou supérieure
  - Module PERL Compress::Zlib version 1.33 ou supérieure
  - Module PERL Net::IP version 1.21 ou supérieure
  - Module PERL LWP::UserAgent version 5.800 ou supérieure
  - Module PERL Digest::MD5 version 2.33 ou supérieure
  - Module PERL Net::SSLeay version 1.25 ou supérieure
- Utilitaire Make
- Compilateur C/C++ tel que GNU GCC

N.B. : Il vaut mieux utiliser pour l'intégrité de votre système les paquets précompilés de votre distribution si ceux-ci sont disponibles.

**Sur Fedora/RedHat**, vous devez utiliser l'outil "yum" pour installer les modules requis suivants :

```
* yum install perl-XML-Simple
* yum install perl-Compress-Zlib
* yum install perl-Net-IP
* yum install perl-LWP
* yum install perl-Digest-MD5
* yum install perl-Net-SSLeay
```

**Sur Debian**, vous devez utiliser l'outil "apt-get" pour installer les modules suivants :

```
* apt-get install libxml-simple-perl
* apt-get install libcompress-zlib-perl
* apt-get install libnet-ip-perl
* apt-get install libwww-perl
* apt-get install libdigest-md5-perl
* apt-get install libnet-ssleay-perl
```

**Le nouveau script d'installation "setup.sh" est capable d'installer ses dépendances si elles ne sont pas disponibles. Toutefois, il ne mettra jamais à jour un module déjà installé. Si un des modules est à une version inférieure à celle requise, vous devez vous-même le mettre-à-jour.**

N.B. : L'installateur n'installera pas les dépendances requises aux composants. Par exemple, Net::SSLeay requiert qu'OpenSSL soit installé. S'il n'est pas installé, l'installation de Net::SSLeay échouera ainsi que celle de l'agent OCS Inventory NG.

**Ainsi, le script installer produit un fichier log "setup.log". Si vous rencontrez une erreur durant l'installation de l'agent OCS Inventory NG, svp référez-vous à ce fichier pour avoir le message d'erreur détaillé.**

## Installer l'Agent interactivement

### *Sur Linux*

Téléchargez "OCSNG\_LINUX\_AGENT\_1.01.tar.gz" depuis le site web d'OCS Inventory NG.

Décompressez-le :

- tar -xzf OCSNG\_LINUX\_AGENT\_1.01.tar.gz

Faites fonctionner l'installateur "setup.sh". Durant la phase d'installation, les choix par défaut sont présentés entre crochets [ ]. Par exemple, "[y]/n" signifie que "y" - yes/oui - est le choix par défaut et que "n" - no/non- est l'autre choix possible.

- cd OCSNG\_LINUX\_AGENT\_1.01
- sh setup.sh

N.B. : L'installateur écrit un fichier log "ocs\_agent\_setup.log" dans le même répertoire.

Si vous rencontrez une erreur, svp référez-vous à ce fichier log pour obtenir le message d'erreur détaillé.

Vous avez alors le choix entre deux méthodes pour générer l'inventaire :

1. http : l'ordinateur est connecté au réseau et il est capable d'atteindre le Serveur de Communication par le biais du protocole HTTP.
2. local : l'ordinateur n'est pas connecté au réseau, l'inventaire sera généré dans un fichier qui sera envoyé manuellement à l'opérateur OCS Inventory NG.

Entrez "http" ou validez si votre ordinateur peut atteindre le serveur de communication, ou "local" pour activer le mode local.

Entrez l'adresse du serveur de communication.

Entrez le port du serveur de communication OCS Inventory NG, ou validez si le serveur de communication fonctionne sur le port HTTP 80 standard.

Entrez une valeur TAG.

L'installateur vérifiera le binaire de l'interpréteur PERL, le compilateur C/C++ et l'utilitaire Make. Si un de ces composants manque, l'installateur s'arrêtera.

L'installateur vérifiera :

- le binaire dmidecode,
- le module PERL Compress::Zlib
- le module PERL XML::Simple
- le module PERL Net::IP
- le module PERL LWP::UserAgent
- le module PERL Digest::MD5
- le module PERL Net::SSLeay

S'ils ne sont pas trouvés, il demandera si vous voulez l'installer. Entrez "y" ou validez si vous voulez installer les modules requis. Si vous entrez "n", l'installateur s'arrêtera là.

Si tout est OK, ou vous avez choisi d'installer les dépendances, l'installateur fera alors les opérations suivantes :

- Décompresse, configure, construit, et installe dmicode si besoin est,
- Décompresse, configure, construit, et installe Compress::Zlib si besoin est,
- Décompresse, configure, construit, et installe XML::Simple si besoin est,
- Décompresse, configure, construit, et installe Net::IP si besoin est,
- Décompresse, configure, construit, et installe LWP (libwww-perl) si besoin est,
- Décompresse, configure, construit, et installe Digest::MD5 si besoin est,
- Décompresse, configure, construit, et installe Net::SSLeay si besoin est,
- Compile le binaire IPDISCOVER,
- Configure le module PERL de l'agent OCS Inventory NG,
- Construit le module PERL de l'agent OCS Inventory NG,
- Installe le module PERL de l'agent OCS Inventory NG dans le répertoire standard des bibliothèques PERL,
- Créé un lien symbolique "/usr/sbin/ocsinv" pour faire fonctionner l'agent OCS Inventory NG manuellement,
- Créé le répertoire des logs de l'agent OCS Inventory NG (/var/log/ocsinventory-NG par défaut),
- Configure la rotation quotidienne des logs de l'agent OCS Inventory NG (fichier /etc/logrotate.d/ocsinventory-client par défaut),
- Créé le fichier de configuration "ocsinv.conf" de l'agent OCS Inventory NG dans le répertoire "/etc/ocsinventory-client",
- Créé le fichier d'information administratif "ocsinv.adm" de l'agent OCS Inventory NG dans le répertoire "/etc/ocsinventory-client" pour enregistrer les valeurs TAG et autres valeurs administratives,
- Créé une tâche cron pour lancer l'agent OCS Inventory NG chaque jour (par défaut, le fichier /etc/cron.d/ocsinventory-client),
- Lance l'agent OCS Inventory NG pour s'assurer que tous les paramètres sont OK.

Ce qui suit est un simple fichier de configuration de l'agent OCS Inventory NG :

```
<CONF>
<DEVICEID>computer.domain.tld-2006-02-27-13-59-47</DEVICEID>
<DMIVERSION>2.2</DMIVERSION>
<IPDISCOVER_VERSION>3</IPDISCOVER_VERSION>
<OCSFSERVER>my_ocs_com_server.domain.tld:80</OCSFSERVER>
</CONF>
```

## Déployer l'Agent au moyen de script d'installation sans interaction utilisateur

### Sur Linux

Téléchargez "OCSNG\_LINUX\_AGENT\_1.01.tar.gz" depuis le site web d'OCS Inventory NG.

Décompressez-le :

- `tar -xzvf OCSNG_LINUX_AGENT_1.01.tar.gz`

Lancez l'installateur "setup.sh" avec les arguments de ligne de commande suivants :

- `cd OCSNG_LINUX_AGENT_1.01`
- `sh setup.sh <SETUP DEPENDANCES> <ADRESSE SERVEUR> [<PORT SERVEUR> <VALEUR TAG>]`

où les valeurs des arguments sont :

- `<SETUP DEPENDANCES>` doit être "1" si vous voulez activer automatiquement l'installation des dépendances oubliées, "0" pour désactiver (l'installateur s'arrêtera si une dépendance est manquante).
- `<ADRESSE SERVEUR>` doit être l'adresse IP ou le nom DNS du serveur de communication. Si vous planifiez d'installer l'agent en mode local sur un ordinateur non connecté à un réseau, vous devez paramétrer la valeur sur "local".
- `<PORT SERVEUR>` doit être le port du serveur de communication d'OCS Inventory NG si vous n'utilisez pas le port HTTP 80 standard.
- `<VALEUR TAG>` doit être la valeur TAG, entre quotes.

Les arguments de ligne de commandes `<SETUP DEPENDANCES>` et `<ADRESSE SERVEUR>` sont requis. Les autres paramètres sont optionnels, mais si vous paramétrez la valeur TAG, vous devez aussi spécifier le paramètre optionnel prévu `<PORT SERVEUR>`.

Exemples :

- **`sh setup.sh 1 ocsng.domain.tld`** installera l'agent, les dépendances manquantes si nécessaire, et se connectera au serveur de communication OCS Inventory NG "ocsng.domain.tld".
- **`sh setup.sg 0 ocsng.domain.tld 8080`** installera l'agent, sans les dépendances manquantes, et se connectera au serveur de communication OCS Inventory NG "ocsng.domain.tld" sur le port 8080.
- **`sh setup.sh 192.168.1.2 8080 "ma valeur TAG"`** installera l'agent, sans les dépendances manquantes, et se connectera au serveur de communication OCS Inventory NG ayant l'adresse IP "192.168.1.2 sur le port 8080, et paramétrera la valeur TAG avec "ma valeur TAG".

N.B. : L'installateur écrira un fichier log "ocs\_agent\_setup.log" dans le même répertoire.

Si vous rencontrez une erreur, svp référez-vous à ce fichier pour avoir le message d'erreur détaillé.

## L'Agent et ses arguments de ligne de commande

Si vous rencontrez des erreurs, l'agent produit un fichier log dans le répertoire `"/var/log/ocsinventory-client"`.

Toutefois, l'agent supporte aussi quelques arguments de ligne de commande. Vous pouvez les utiliser quand vous lancez manuellement l'agent en utilisant la commande `"ocsinv"` :

L'agent et ses arguments de ligne de commande	
Arguments	Énoncé
<b>-local</b>	Fait fonctionner l'agent en mode local, sans aucune connexion au serveur de communication. Il vous sera demandé un répertoire de destination où l'agent déposera les résultats de l'inventaire dans un fichier XML compressé ayant l'extension ".ocs".
<b>-xml</b>	L'agent créera un fichier XML non compressé ayant l'extension ".ocs", contenant les résultats de l'inventaire. Il vous sera demandé un répertoire de destination où l'agent déposera le fichier. Si vous ne l'utilisez pas en conjonction avec l'argument "-local", l'agent essaiera de se connecter au serveur de communication.
<b>-nosoft</b>	Ne pas rechercher les logiciels installés.
<b>-tag="ma valeur tag"</b>	Dit à l'agent de paramétrer la valeur TAG à "ma valeur tag".
<b>-force</b>	Force l'agent à toujours envoyer les résultats de l'inventaire, indépendamment du paramètre FREQUENCY.
<b>-info</b>	Montre une sortie détaillée du fonctionnement de l'agent.
<b>-debug</b>	Force l'agent à produire plus de détails dans le fichier log, montrant les échanges XML avec le serveur de communication.



# RESULTATS DES REQUETES D'INVENTAIRE

## Contenu

### [1 Résultats des requêtes d'inventaire](#)

- [1.1 Tous les ordinateurs](#)
- [1.2 TAG / Répartition du nombre de PC](#)
- [1.3 Recherche selon plusieurs critères](#)

## Résultats des requêtes d'inventaire

Pointez votre navigateur internet à l'URL "[http://serveur\\_administration/ocsreports/](http://serveur_administration/ocsreports/)" et connectez-vous dans la console d'Administration. (par défaut, l'identifiant est "admin" et le mot-de-passe aussi).

Vous devez utiliser le menu de gauche pour lancer les requêtes prédéfinies.



pour voir tous les ordinateurs



pour voir les ordinateurs par répartition de TAG



pour rechercher les ordinateurs selon plusieurs critères

Pour toutes ces recherches, vous pouvez personnaliser la vue en ajoutant ou supprimant des colonnes, en changeant le nombre de lignes par page à afficher. Toutes ces personnalisations seront sauveées par l'utilisateur, entre chaque connexion. Cela signifie que lorsque vous reviendrez sur la console d'administration d'OCS Inventory NG, vos paramètres seront restaurés tels qu'ils étaient lors de votre dernière connexion.

N.B. : Les ordinateurs marqués d'une bulle rouge au commencement de leur ligne sont des ordinateurs ayant des paramètres spécifiques personnalisés. Ils doivent avoir une fréquence d'inventaire spécifique, un statut ipdiscover ou un déploiement de paquets affecté.

## Tous les ordinateurs

Cette requête vous permet d'afficher tous les ordinateurs inventoriés. Les ordinateurs marqués avec un ballon rouge au commencement de leur ligne sont ceux qui ont des options spécifiques personnalisées.

Juste, cliquez sur le nom d'un des ordinateurs pour ouvrir ses propriétés dans une nouvelle fenêtre du navigateur internet.

- Bannière du haut : Affiche les informations générales pour le matériel en cours.
- Section de liens : Cliquez juste sur le lien approprié pour afficher l'information correspondante.
- Section du bas : Utilisez "Tout afficher" pour afficher toutes les sections. Pour imprimer l'information couramment affichée, utilisez "Imprimez cette page".
- Section spéciale Données Administratives : Utilisez cette section pour afficher les informations administratives du matériel. Cette page s'adapte selon vos paramètres de l'onglet "admininfo". Utilisez le bouton [ Mettre à jour ] pour changer ces valeurs.

- Section spéciale Personnalisation : Utilisez cette section pour personnaliser les options de configuration pour chaque ordinateur individuel. Vous pouvez ainsi sélectionner les paquets à déployer sur un ordinateur en particulier.

## **TAG / Répartition du nombre de PC**

Cette requête vous permet d'afficher tous les ordinateurs groupés par information du compte TAG. Cliquez sur le nombre de machines pour obtenir les matériels correspondants.

Par exemple, si vous choisissez de paramétrer votre information TAG reflétant vos différents sites géographiques, ceci affichera le nombre d'ordinateurs pour chaque site différent.

## **Recherche selon plusieurs critères**

Cette requête vous permet de rechercher les ordinateurs selon de spécifiques critères.

Vous pouvez ajouter de nouveaux paramètres en sélectionnant dans la liste déroulante.

Les paramètres de recherche par défaut sont :

- Fabricant du BIOS,
- Version (du) BIOS,
- Nom (de la) machine,
- IpDiscover (personnalisé),
- Télédéploiement,
- Description,
- Domaine,
- Espace libre (de disque dur),
- Fréquence (d'inventaire),
- Passerelle,
- Adresse IP,
- IpDiscover (statut),
- Dernier inventaire,
- Adresse MAC,
- Fabricant (système),
- Mémoire,
- Modèle (système),
- Écran : description,
- Écran : fabricant,
- Écran : numéro de série,
- Numéro Réseau,
- Système (d'exploitation),
- Vitesse CPU,
- Clé de registre,
- Logiciel,
- Tag,
- Utilisateur connecté,
- Type d'agent (montre la version de l'agent OCs Inventory NG),
- Toutes les informations administratives que vous avez définies.

Pour chaque paramètre, vous pouvez utiliser un des opérateurs de comparaison suivants, dépendants du paramètre que vous avez sélectionné :

- ÉGAL
- DIFFÉRENT
- PLUS PETIT
- PLUS GRAND
- ENTRE
- HORS DE

N.B. : Ne pas oublier de paramétrer les paramètres dans chaque recherche !

N.B. : Vous pouvez rechercher différents logiciels dans une même requête. Cela signifie que vous pouvez rechercher les ordinateurs ayant tel logiciel 1, tel logiciel 2, ...  
Hormis le champ logiciel, tous les autres champs peuvent être seulement spécifiés une seule fois à chaque requête.



# ADMINISTRATION D'OCS INVENTORY

## Contenu

- [1 Administration d'OCS Inventory NG](#)
  - [1.1 Gérer les utilisateurs du serveur d'administration OCS Inventory NG](#)
  - [1.2 Gérer les options générales d'OCS Inventory NG](#)
  - [1.3 Téléverser l'Agent pour le déploiement au moyen du lanceur "OcsLogon.exe"](#)
  - [1.4 Utiliser les fonctionnalités de requêtes sur le Registre](#)
  - [1.5 Gérer les ordinateurs dupliqués](#)
  - [1.6 Éditer les informations administratives](#)
  - [1.7 Éditer le label](#)
  - [1.8 Importer l'inventaire pour des ordinateurs non connectés au réseau](#)
    - [1.8.1 Avec le serveur d'Administration au moyen du navigateur internet](#)
    - [1.8.2 Avec le serveur de Communication au moyen d'un script Perl](#)
  - [1.9 Utiliser le dictionnaire de logiciels pour l'intégration GLPI](#)

## Administration d'OCS Inventory NG

Pointer votre navigateur internet sur l'URL "[http://serveur\\_administration/ocsreports/](http://serveur_administration/ocsreports/)" et connectez-vous à la console d'Administration (par défaut, l'identifiant est "admin" et le mot-de-passe est identique).

**Vous pouvez changer le mot-de-passe administrateur par défaut, ou mieux, ajouter un nouveau et supprimer celui par défaut.**

N.B. : Toutes ces fonctionnalités sont seulement disponibles pour les administrateurs OCS Inventory NG.

## Gérer les utilisateurs du serveur d'administration OCS Inventory NG

Cliquez sur le menu "Users" de la barre d'outils pour afficher tous les utilisateurs configurés du serveur d'administration OCS Inventory NG.

Vous pouvez ajouter de nouveaux utilisateurs en entrant leur nom, leur mot-de-passe (l'utilisateur pourra le changer quand il sera connecté), et sélectionner leur type. Vous pouvez choisir entre :

- Administrateur : l'utilisateur qui a la capacité de configurer tous les paramètres du produit.
- Utilisateur : l'utilisateur peut seulement faire une requête à la base de données et voir les résultats de l'inventaire. Il a juste accès au menu en haut à gauche pour faire fonctionner les requêtes génériques.

Pour effacer un utilisateur, cliquez juste sur la croix rouge en fin de ligne correspondante.

## Gérer les options générales d'OCS Inventory NG

Cliquez sur le menu "Configuration" de la barre d'outil pour afficher les options générales.

Ceci est un mémento de chaque option :

Options générales de configuration	
Options	Énoncé
<b>AUTO_DUPLICATE_LVL</b>	Choisissez quelle valeur vous voulez activer pour détecter les ordinateurs en double (renommé, réinstallé, ...). Si vous vérifiez de multiples valeurs, le serveur essaiera de détecter les doublons en comparant ces valeurs.
<b>DEPLOY</b>	Active ou non le déploiement automatique d'une nouvelle version de l'agent.
<b>DOWNLOAD</b>	Active ou non la fonctionnalité de déploiement de paquets. Positionnez à Off arrêtera cette fonctionnalité sur le serveur ET pour les agents. Avec DOWNLOAD sur Off, les agents qui ont contacté le serveur OCS arrêteront leur téléchargement courant SANS nettoyer les paquets.
<b>DOWNLOAD_CYCLE_LATENCY</b>	Temps en secondes à attendre entre chaque cycle de téléchargement. (cf § <a href="#">la section intitulée Comment cela fonctionne-t-il ?</a> )
<b>DOWNLOAD_FRAG_LATENCY</b>	Temps en secondes à attendre entre chaque téléchargement de fragments. (cf § <a href="#">la section intitulée Comment cela fonctionne-t-il ?</a> )
<b>DOWNLOAD_PERIOD_LATENCY</b>	Temps en secondes à attendre entre chaque période de téléchargement. (cf § <a href="#">la section intitulée Comment cela fonctionne-t-il ?</a> )
<b>DOWNLOAD_PERIOD_LENGTH</b>	Nombre de cycles par période (cf § <a href="#">la section intitulée Comment cela fonctionne-t-il ?</a> )
<b>DOWNLOAD_TIMEOUT</b>	Validité en jours du paquet d'un agent. Si la période en nombre de jours utilisée pour télécharger un paquet est au-delà de la valeur DOWNLOAD_TIMEOUT, le paquet sera "nettoyé" et une erreur ERR_TIMEOUT sera envoyée au serveur OCS.
<b>FREQUENCY</b>	Spécifie la fréquence d'inventaire en nombre de jours.
<b>INVENTORY_DIFF</b>	Activer ou non l'inventaire différentiel. Avec l'inventaire différentiel, seuls les changements seront enregistrés par le serveur, et non pas un inventaire complet.
<b>INVENTORY_TRANSACTION</b>	Activer ou non la transaction sur le serveur. Avec la transaction, un inventaire est seulement enregistré si toutes les données ont correctement été produites.
<b>IPDISCOVER</b>	Spécifie le numéro de l'agent qui demande à faire fonctionner la fonctionnalité de découverte IP pour chaque passerelle (sous-réseau). Si vous laissez la valeur 2 par défaut, cela signifie que le serveur de communication demandera aux 2 ordinateurs les plus actifs de chaque sous-réseau de faire fonctionner la fonctionnalité de découverte IP. Si vous le paramétrez à 0, la fonctionnalité sera désactivée.
<b>IPDISCOVER_LATENCY</b>	Temps en secondes entre chaque scan de chaque adresse IP. (cf § <a href="#">la section intitulée Comment cela fonctionne-t-il ?</a> ).
<b>IPDISCOVER_MAX_ALIVE</b>	Nombre maximal de jours entre deux inventaires pour une découverte d'IP activée sur l'ordinateur qui a pris en charge la fonctionnalité de découverte d'IP. Un ordinateur ayant activé la découverte d'IP perdra son statut s'il n'a pas été vu par le serveur de communication durant la période de nombre de jours définie dans ce paramètre. Un autre ordinateur dans le même sous-réseau sera alors désigné.
<b>LOCAL_PORT</b>	Port du serveur de communication.
<b>LOCAL_SERVER</b>	Adresse IP ou nom DNS du serveur de communication.
<b>LOGLEVEL</b>	Active ou non les logs détaillés pour le serveur de communication. Si cela est activé, le serveur écrira les logs dans le fichier "ocsinventory-NG.log" dans le répertoire "/var/log/ocsinventory-NG" pour Linux et dans "...\\xampp\\apache\\logs" pour Windows.
<b>PROLOG_FREQ</b>	Nombre d'heures entre deux lancements de l'agent (utilisé par le service). Toutefois, l'agent prendra contact (pas nécessairement pour envoyer un inventaire si l'inventaire n'est pas plus vieux que le nombre de jours spécifiés dans FREQUENCY) avec le serveur OCS selon le nombre d'heures définies dans PROLOG_FREQ.
<b>REGISTRY</b>	Active ou non la fonction de requête sur le registre (seulement pour l'agent Windows).
<b>TRACE_DELETED</b>	Active ou non le suivi des ordinateurs effacés ou renommés pour l'intégration avec GLPI. Activer seulement cette fonctionnalité si vous utilisez l'intégration avec le logiciel de gestion GLPI.
<b>UPDATE</b>	Non utilisé, toujours paramétré sur Off.

Cliquez sur le bouton [ Mettre à jour ] pour paramétrer tous les changements.

## Téléverser l'Agent pour le déploiement au moyen du lanceur "OcsLogon.exe"

**Cette fonctionnalité travaille seulement avec les ordinateurs connectés au réseau capable de communiquer avec le serveur de communication.**

OCS Inventory NG est capable d'installer automatiquement l'agent sur les ordinateurs quand le lanceur "OcsLogon.exe" est utilisé au moyen de script d'ouverture de session ou de règle GPO. Les fichiers de l'agent seront téléchargés depuis le serveur de communication.

Vous avez juste à téléverser le paquet de l'agent dans la console d'administration et à activer la fonctionnalité de déploiement en paramétrant l'option générale "DEPLOY" sur ON (cf [la section intitulée Gérer les options générales d'OCS Inventory NG](#)).

Le fichier téléversé doit être un de celui-là :

- le fichier "ocsagent.exe" pour l'agent Windows, à déployer sans le service Windows,
- le fichier "ocspackage.exe", créé en utilisant le packager OCS Inventory NG, pour déployer la version de l'agent de service Windows, même si l'utilisateur connecté n'a pas les droits d'administrateur.

Pour créer le fichier "ocspackage.exe", faites juste fonctionner le packager OCS Inventory NG et remplissez les informations suivantes :

- Le chemin du fichier "OcsAgentSetup.exe", l'installateur de l'Agent de Service OCS Inventory NG, inclu dans le paquet OCSNG\_WIN32\_AGENT\_XX.zip.
- Le chemin du fichier de certificat à utiliser, pour vérifier le certificat du serveur quand est utilisée la fonctionnalité de déploiement de paquets.
- Optionnellement, un fichier à inclure dans l'installateur.
- Les arguments de ligne de commande à faire fonctionner avec l'installateur "OcsAgentSetup", au minimum "/S" pour le mode silencieux et "/SERVER:adresse\_serveur\_ocs" pour spécifier "adresse\_serveur\_ocs" en tant qu'adresse du serveur de communication.
- Le nom utilisateur (**compte@domaine** pour un compte Active Directory et **domaine\compte** pour un compte NT) et mot-de-passe du compte Administrateur sur les ordinateurs clients. "OcsAgentSetup.exe" fonctionnera sur ce compte sur les ordinateurs clients, pour permettre d'installer le service même si l'utilisateur connecté n'a pas les privilèges d'Administrateur.

N.B. : Référez-vous à la [documentation du packager d'OCS Inventory NG](#) pour avoir plus d'informations sur comment utiliser le Packager.

"OcsAgentSetup.exe" supporte les paramètres de ligne de commandes suivants (et tous les paramètres de l'agent définis dans [la section intitulée L'Agent et ses arguments de ligne de commande](#)) :

- /S utilise le mode silencieux pour l'installation,
- /SERVER:ADRESSE\_IP utilise l'adresse IP du serveur de communication,
- /PNUM:XX utilise le port XX en lieu-et-place du port HTTP 80 par défaut,
- /NP ne pas utiliser les paramètres du proxy d'Internet Explorer,
- /DEBUG produit un fichier de log à l'exécution de l'agent OCS Inventory NG. Ce mode est automatiquement utilisé sous Windows pour lancer l'agent en tant que service comme entrée dans la base de registre en tant que clé "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices".

Ceci créera le fichier "ocspackage.exe" à téléverser dans la console d'Administration.

Cliquez sur le menu "Client" de la barre d'outil, puis sur le bouton [ Parcourir ] pour sélectionner le fichier de l'agent puis sur le bouton [ Envoyer ].

N.B. : Si vous rencontrez des erreurs pendant le téléversement de l'agent, référez-vous aux erreurs communes dans § [la section intitulée Requête PHP content-length](#).

## Utiliser les fonctionnalités de requêtes sur le Registre

L'Agent OCS Inventory NG pour Windows est capable d'interroger la base de registre des ordinateurs inventoriés pour obtenir la valeur d'une clé ou de toutes les clés des registres intitulés HKEY\_CLASSES\_ROOT, HKEY\_CURRENT\_USER, HKEY\_LOCAL\_MACHINE, HKEY\_USERS, HKEY\_CURRENT\_CONFIG (et HKEY\_DYN\_DATA pour les ordinateurs fonctionnant sur Windows 9x).

Vous devez activer cette fonctionnalité dans la configuration générale, option "REGISTRY".

Vous pouvez alors définir votre requête de registre en cliquant sur le menu "Registre" dans la barre d'outil.

Cliquez sur le bouton [ Ajouter ] pour ajouter une nouvelle requête. Entrez un nom pour cette requête, par exemple MS Office XP si vous voulez obtenir le numéro d'enregistrement MS Office XP, sélectionnez le registre désiré (dans l'exemple HKEY\_LOCAL\_MACHINE), entrez la clé de registre (SOFTWARE\Microsoft\Office\10.0\Registration\{9011040C-6000-11D3-8CFE-0050048383C9}) et le nom de la valeur de la requête (ProductID) puis validez. Mettez le symbole '\*' dans le champ "Nom de la clé à lire" pour obtenir toutes les valeurs de la clé (Ceci est utilisable pour obtenir toutes les valeurs de la clé "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" afin de savoir quels processus sont démarrés automatiquement, par exemple).

Après cela, chaque fois que le client Windows se connecte ; il recevra et enregistrera toutes les valeurs correspondantes à cette clé.

## Gérer les ordinateurs dupliqués

OCS Inventory NG est capable de détecter un ordinateur renommé, réinstallé, ...

Généralement, il se débrouillera tout seul. Mais quelques fois, il est impossible au serveur de savoir que deux ordinateurs sont identiques ou non, par exemple quand il n'y a pas d'adaptateur réseau (pas d'adresse MAC) ou quand le numéro de série n'est pas proprement paramétré par le constructeur (Si vous changez le nom d'un ordinateur, l'application ne sera pas capable de le reconnaître s'il n'y a pas de numéro de série ou d'adresse MAC, elle dupliquera l'ordinateur).

Cette page est accessible en cliquant sur le menu "Doubles" dans la barre d'outils pour résoudre ce genre de problèmes.

Vous pouvez choisir le genre de comparaison que vous désirez dans la liste déroulante en haut à droite :

- Résumé redondance : montre le nombre d'ordinateurs redondants détectés selon chacune des méthodes de comparaison
- "Hostname + Serial number", "Hostname + Mac address", "Mac address + Serial number" : Ce sont des méthodes de comparaison avec deux critères, les plus fiables. Elle retourne tous les ordinateurs qui ont ses deux critères en commun.
- "Hostname seul", "Serial seul", "Mac address seul" : Ce sont des méthodes de comparaison à un seul critère ; elle montre seulement tous les ordinateurs qui partagent ce même paramètre.

Pour chaque ordinateur visible, cela permet de vérifier que ces ordinateurs sont redondants ou non.

Après cela, vous avez juste à sélectionner (checkbox) les ordinateurs qui sont semblables, et à cliquer sur le bouton [ Fusion des ordinateurs redondants ] : toutes les données des ordinateurs vérifiés seront fusionnés.

Les données administratives de l'ancien ordinateur sont gardées dans le matériel fusionné.

N.B. : Quand ces filtres sont appliqués, certaines valeurs sont mises de côtés (Par exemple : 'NNNNNNNN' ou 'xxxxxxxx' pour le numéro de série).

## Éditer les informations administratives

OCS Inventory NG vous permet d'enregistrer les informations personnalisées pour chaque ordinateur inventorié. Par exemple, vous pouvez ajouter une information administrative qui spécifie le propriétaire de l'ordinateur, ou la localisation de l'ordinateur.

Cette information administrative est enregistrée à la fois sur le serveur et sur le client pour éviter toute perte de données.

Pour l'exemple, si la base de données est perdue, tous les clients "reviendront" avec leur information administrative.

[[Image:]] Vous pouvez définir les informations administratives que vous voulez pour chaque ordinateur en cliquant sur le menu "Admininfo" dans la barre d'outils.

Vous pouvez ajouter de nouvelles définitions d'information administrative en entrant leur nom (les espaces ou les caractères spéciaux ne sont pas permis) et en sélectionnant leur type. Vous pouvez choisir entre :

- Texte
- Entier
- Réel
- Date

Pour effacer une définition d'information administrative, cliquez tout simplement sur la croix rouge à la fin de la ligne correspondante.

Pour l'exemple, nous pourrions ajouter une information administrative correspondant à la date d'achat de l'ordinateur.

Vous pouvez maintenant parcourir tous les ordinateurs pour paramétrer leur date d'achat.

## Éditer le label

Si l'option "DEPLOY" est activée, les clients peuvent obtenir le fichier "label". Il est utilisé pour remplir la fenêtre popup vue au premier démarrage du client.

Cette fenêtre popup demande la valeur "TAG" qui est utilisée pour la classe des ordinateurs (cela peut être, par exemple, un code d'unité, le nom de la section administrative de la société, un numéro de rue, etc ...).

[[Image:]] Ce fichier "label" est généré durant l'installation du serveur, et peut être édité en cliquant sur le menu "Modifier le label" dans la barre d'outils.

Si vous soumettez un label vide, le fichier label sera effacé, et aucune fenêtre ne sera plus affichée sur l'ordinateur client.

## Importer l'inventaire pour des ordinateurs non connectés au réseau

### Avec le serveur d'Administration au moyen du navigateur internet

Pour les ordinateurs non connectés à un réseau, vous pouvez importer les résultats de l'inventaire depuis un fichier créé sur l'ordinateur par l'agent fonctionnant en mode local (voir [Nous avons choisi le paquet OCS Inventory NG Serveur pour Windows en tant que paquet contenant tous les composants requis. Tels quels, les 3 composants du Serveur de Gestion \(serveur de base de données, serveur web de communication, et serveur web d'administration\) sont installés sur le même ordinateur.](#))

Nous supposons que vous êtes capable de sauvegarder ce fichier sur votre disque dur depuis votre client mail, ou par tout autre moyen.

N.B. : Si le Serveur de Communication ne fonctionne pas sur le port standard HTTP 80, ou sur le même ordinateur que la Console d'Administration vous devez mettre-à-jour les options générales. (Voir § [la section intitulée Gérer les options générales d'OCS Inventory NG](#))

Cliquez sur le menu "Import local", parcourez votre disque dur pour sélectionner le fichier ".ocs" créé par l'agent, et cliquez sur le bouton [ Envoyer ].

### Avec le serveur de Communication au moyen d'un script Perl

Le serveur de communication fournit la possibilité d'importer l'inventaire depuis un fichier créé sur l'ordinateur. Ce fichier a l'extension ".ocs".

Nous supposons que l'administrateur peut avoir ce fichier de n'importe où, par sa boîte mail, une clé usb, ou par tout autre moyen.

Allez dans le répertoire où vous avez installé le serveur de communication, "/usr/local/ocsinventory-NG" dans notre cas, et faites fonctionner le script "Ocsinventory\_local.pl" en précisant le chemin du fichier, qui contient les résultats de l'inventaire, comme argument.

N.B. : Avec le serveur OCS Inventory pour Windows, le script d'import "local\_import.bat" est localisé dans le répertoire "REPERTOIRE\_INSTALL\binutils", où "REPERTOIRE\_INSTALL" est le répertoire d'installation choisi durant l'installation du serveur.

Ceci importera les résultats d'inventaire dans la base de données.

```
[root@l16753101aao ocsinventory-NG]# Ocsinventory_local.pl ST32491DL-2005-06-23-10-04-02.ocs
OK for ST32491DL-2005-06-23-10-04-02.ocs
-----
Successfully inventoried : 1
Errors : 0
:-)
```

Si vous avez de multiples fichiers à importer, vous pouvez les mettre dans un répertoire et lancer le script "Ocsinventory\_local.pl" sans arguments, mais dans le répertoire où résident les fichiers à importer.

```
[root@l16753101aao home]# Ocsinventory_local.pl
OK for ST32491DL-2005-06-23-10-04-02.ocs
-----
Successfully inventoried : 1
Errors : 0
:-)
```

## Utiliser le dictionnaire de logiciels pour l'intégration GLPI

Le dictionnaire de logiciels est utilisé pour mettre en catégorie les logiciels détectés. Cette fonctionnalité est très intéressante quand vous utilisez OCS Inventory NG en combiné avec GLPI. Tel quel, vous pouvez grouper les logiciels dans une catégorie et GLPI les importera avec leur nom de catégorie.

Par exemple, vous avez beaucoup de versions de Microsoft Office (97, 2000, XP, 2003, ...), mais vous ne voulez pas faire attention à leur version. Vous voulez juste gérer le nombre total de MS Office. Vous pouvez créer une catégorie "Microsoft Office" et insérer dans cette catégorie toutes les versions de Microsoft Office. Dans GLPI, vous verrez seulement "Microsoft Office". Le dictionnaire de logiciels agit comme un utilitaire de renommage ou de groupe pour GLPI.

Cliquez sur le menu "Dictionnaire" dans la barre d'outils.

Il y a 3 catégories par défaut :

- **NOUVEAU** : inclut tous les nouveaux logiciels ou ceux qui n'ont pas de catégorie.
- **IGNORÉ** : vous pouvez mettre dans cette catégorie tous les logiciels que vous ne voulez pas importer dans GLPI.
- **INCHANGÉ** : vous pouvez mettre dans cette catégorie tous les logiciels que vous ne voulez pas "renommer" dans GLPI. Ces logiciels seront importés tels quels.

Vous pouvez rechercher les logiciels avec une partie de leur nom en remplissant le champ d'entrée et en cliquant sur le bouton [ Chercher logiciel PARTOUT ].

Si vous gérez plusieurs catégories, vous pouvez rechercher une catégorie par une partie de son nom en remplissant le champ d'entrée et en cliquant sur le bouton [ Chercher catégorie ].

Cliquez sur le nom d'une des catégories pour afficher les logiciels inclus.

Vous pouvez sélectionner les logiciels pour les changer dans une nouvelle catégorie (vous devez remplir le nom de la nouvelle catégorie) ou vers une catégorie existante (sélectionnez-la dans la liste déroulante).

Si vous cliquez sur "Move all", tous les logiciels, même ceux qui ne sont pas affichés, seront changés vers la catégorie désirée, pas seulement ceux qui sont sélectionnés.

Vous pouvez sélectionner tous les logiciels affichés en cliquant sur "La page" et les dé-sélectionner en cliquant sur "Rien".



# UTILISER LA FONCTION DECOUVERTE IP

## Contenu

- [1 Utiliser la fonctionnalité de découverte IP](#)
  - [1.1 Introduction](#)
  - [1.2 Comment cela fonctionne-t-il ?](#)
    - [1.2.1 Recevoir l'information](#)
    - [1.2.2 Mécanisme d'élection](#)
    - [1.2.3 Comment l'agent travaille ?](#)
    - [1.2.4 Personnalisation du Serveur](#)
  - [1.3 Travailler avec les résultats](#)
    - [1.3.1 Gérer les noms de vos réseaux](#)
    - [1.3.2 Voir la liste des réseaux](#)
    - [1.3.3 Voir les hôtes répertoriés du réseau](#)
    - [1.3.4 Voir les matériels réseau non-inventoriés](#)
    - [1.3.5 Voir les hôtes fonctionnant avec IPDISCOVER](#)
    - [1.3.6 Voir les hôtes identifiés ou connus](#)
    - [1.3.7 Gérer les types de matériel connus](#)
    - [1.3.8 Enregistrer les hôtes connus](#)
    - [1.3.9 Scanner une adresse IP](#)

## Utiliser la fonctionnalité de découverte IP

La fonctionnalité de découverte IP permet à OCS Inventory NG de découvrir tous les matériels connectés au réseau.

Pour cela, le Serveur de Communication demande à un nombre d'ordinateurs les plus "actifs" faisant fonctionner l'agent OCS Inventory NG de scanner les adresses MAC dans leur sous-réseau respectif. **Ils ne scanneront pas l'ensemble du réseau complet, mais seulement leur propre réseau local défini par le couple adresse IP/masque de sous-réseau.**

## Introduction

Le logiciel d'inventaire est très utile pour l'administrateur. Il permet de "mettre en lumière" le stock d'ordinateurs. Aujourd'hui, avec l'usage de TCP/IP, nous pouvons dire que la mise-en-lumière est faite en même temps pour tous les réseaux de l'entreprise, spécialement si, comme pour OCS Inventory NG, ils travaillent nativement dans un réseau défini.

Mais, qu'en est-il à-propos des matériels qui n'envoient pas l'inventaire, pour différentes raisons tel qu'un oubli, un manque de coopération des utilisateurs ? Qu'en est-il à-propos des matériels "vivants" qui ne peuvent faire fonctionner l'agent (imprimantes, concentrateurs, routeurs, points d'accès Wifi, ...) ? Qu'en est-il à propos des ordinateurs qui ne sont pas connectés au réseau qui attirent l'évidence par leur discrétion ?

IPDISCOVER essaye de répondre à cette problématique. Même s'il peut fonctionner indépendamment, il fonctionne parfaitement avec la structure d'OCS. Comme son travail est basé sur la communication entre le système d'exploitation de tous les hôtes et le serveur central, il est très facile au serveur d'ordonner à son "subordonné" de créer quelques petites tâches, tel qu'obtenir des clés de registre, faire un inventaire ou recevoir tous les matériels interrogés sur son segment IP.

## Comment cela fonctionne-t-il ?

### Recevoir l'information

Le système OCS Inventory NG est basé sur un dialogue entre les agents installés sur les ordinateurs et le module Apache sur le serveur OCS NG. L'échange est fait en XML compressé et permet de configurer les tâches des agents.

Quand un ordinateur envoie les résultats de l'inventaire, le serveur essaye de déterminer s'il a besoin que d'autres ordinateurs (le nombre peut être configuré) scanne l'hôte dans son sous-réseau. L'adresse IP de la passerelle est utilisée pour cartographier le réseau de l'entreprise.

Si cela est nécessaire, le serveur estime l'hôte de qualité et décide d'activer ou non l'hôte en tant qu'ordinateur chargé de la découverte d'IP. Dans ce cas, l'ordinateur enverra systématiquement un inventaire, indépendamment du paramètre de configuration générale "FREQUENCY".

### Mécanisme d'élection

Une fois que le serveur a déterminé celui dont il a besoin pour la passerelle choisie, il évalue les critères suivants :

- OS : le système d'exploitation doit être Windows XP, Windows 2000 (toutes versions) ou Linux.
- QUALITÉ : ce paramètre signifie le moyenne de connexion de l'hôte au serveur en jours. Il est évalué dynamiquement par le serveur de communication seulement quand il y a plus que le nombre d'hôtes inventoriés par la passerelle (défini par l'option "IPDISCOVER"). Si l'ordinateur courant qui envoie les résultats de l'inventaire est de meilleure qualité que l'ordinateur chargé de la découverte d'IP par la passerelle, l'ordinateur courant remplacera celui-ci. L'option "IPDISCOVER" doit être supérieure à zéro pour activer cette fonctionnalité !
- FIDELITÉ : nombre total de connexion au serveur par l'ordinateur. Ce nombre doit au moins être de 3, pour allouer le paramètre de QUALITÉ pour être reconnu comme données représentatives.
- NETMASK (MASQUE-DE-RÉSEAU) : masque de sous-réseau. Il doit décrire un réseau de classe B, au maximum (les 2 premiers bytes à 255 => 255.255.X.X).
- LASTDATE (DERNIÈRE DATE) : quand le serveur de communication définit un ordinateur en tant que QUALITÉ, s'il trouve un hôte qui n'a pas envoyé de résultats d'inventaire depuis un nombre de jour défini par l'option "IPDISCOVER\_MAX\_ALIVE", il remplacera cet hôte par un nouveau.

N.B. : Vous pouvez personnaliser les paramètres ipdiscover de l'agent pour chaque ordinateur depuis la console d'administration.

Vous pouvez totalement désactiver ipdiscover ou forcer ipdiscover sur un réseau spécifique. Ces options sont disponibles depuis la page de propriétés de l'ordinateur, sous la section "Personnalisation". Toutefois, le mécanisme d'élection est la meilleure façon de faire la découverte du réseau. Utilisez la personnalisation ipdiscover avec précaution.

### Comment l'agent travaille ?

Une fois que l'agent a reçu l'ordre de procéder à la découverte de son sous-réseau, il identifie en premier l'interface réseau à utiliser. Il essaye alors de résoudre au moyen d'ARP toutes les adresses IP questionnées sur son segment (le délai entre 2 hôtes peut être défini en utilisant l'option "IPDISCOVER\_LATENCE", voir § [la section intitulée Gérer les options générales d'OCS Inventory NG](#)). Tous les matériels répondant à cette question ont sauvegardé en XML les résultats de l'inventaire et les ont envoyés au serveur.

## Personnalisation du Serveur

Quand est faite une nouvelle installation d'OCS Inventory NG, il est facile de comprendre que cela prend un certain temps pour être prêt à activer la fonctionnalité ipdiscover. Un certain temps est requis pour trouver toutes les passerelles et choisir les ordinateurs pour la découverte d'IP. En tant que tel un ordinateur peut être choisi s'il fournit RÉELLEMENT un inventaire, il faut d'abord configurer au commencement l'option "FREQUENCY" à zéro, ce qui génère toujours un inventaire. Vous pouvez modifier cette valeur plus tard, quand l'infrastructure sera prête.

Analyser les erreurs (au moyen d'ipdiscover-util.pl utilisé directement ou depuis l'interface web) vous permettra de détecter les problèmes potentiels. Plus la valeur de la QUALITÉ est minime, plus votre information ipdiscover sera mis-à-jour.

Le système fonctionnera mieux dans un domaine, avec authentification quotidienne et inventaire. Des tests ont été faits avec une configuration de 20 000 hôtes et de 250 sous-réseaux générant une actualisation QUOTIDIENNE de 15 000 adresses IP.

Pour finir, la valeur paramétrée pour IPDISCOVER demandera au serveur combien d'ordinateurs sont choisis comme passerelle pour faire fonctionner cette tâche (si vous paramétrez cette valeur à zéro, la fonctionnalité sera désactivée).

## Travailler avec les résultats

[[Image:]] Vous pouvez voir quels ordinateurs fonctionnent le scan de découverte d'IP en cliquant sur le menu "Sécurité" dans la barre d'outils (menu "IpDisc" dans quelques langues).

## Gérer les noms de vos réseaux

**Vous pouvez gérer vos sous-réseaux par un nom et un unique ID, pour voir les résultats facilement.**

Cliquez sur le menu "Configuration" puis sur le sous-menu "Noms Sous-Réseau" pour gérer vos sous-réseaux.

Entrez le nom du sous-réseau (exemple DMZ), ID, adresse IP et masque de réseau puis cliquez sur le bouton [ Envoyer ] pour valider.

Pour supprimer une définition de sous-réseau, cliquez juste sur la croix rouge à la fin de la ligne correspondante.

## Voir la liste des réseaux

Vous pouvez voir la liste des sous-réseaux configurés dans votre réseau en sélectionnant le menu "Information Réseau".

Pour chaque réseau, vous serez capable de voir combien d'hôtes sont inventoriés, non inventoriés, d'hôtes ayant activés la fonctionnalité d'IPDISCOVER et d'hôtes identifiés (connus comme enregistrés manuellement dans la base de données) qui sont connectés au réseau.

Cliquez sur le nombre de la colonne désirée pour voir chaque type de matériel.

## Voir les hôtes répertoriés du réseau

Vous pouvez voir la liste des hôtes inventoriés (les ordinateurs avec l'agent OCS Inventory NG installé) de votre réseau en cliquant sur le nombre dans la colonne "Inventorié" dans la liste du réseau.

## Voir les matériels réseau non-inventoriés

Vous pouvez voir la liste des matériels réseaux actifs détectés par IPDISCOVER sur votre réseau en cliquant sur le nombre dans la colonne "Non Inventorié" (les ordinateurs n'ayant pas l'agent OCS Inventory NG installés) dans la liste de réseau.

S'il y a ici, dans la liste, des matériels que vous connaissez comme légitime, vous pouvez alors les enregistrer ainsi ils ne seront plus affichés la prochaine fois. Pour cela, cliquez juste sur l'icône en fin de ligne correspondante. Avant, vous devez enregistrer le "Type Matériel" pour identifier facilement les hôtes connus. (Voir § [la section intitulée Enregistrer les hôtes connus](#)).

Vous pouvez de plus analyser ce réseau en cliquant le bouton [ Analyser ]. Le script perl IPDISCOVER-UTIL sera utilisé pour déterminer, pour chaque matériel réseau, son nom NetBios ou nom DNS et le type de système d'exploitation.

N.B. : Cette fonctionnalité utilise le script perl IPDISCOVER-UTIL disponible seulement sur serveur Linux qui requiert les composants suivants :

```
* nmap (testé sur 3.75)
* nmblookup (partie de la suite Samba, testé sur 3.0.7/3.0.10)
* module Perl Net::IP
* module Perl DBI
* module Perl DBD::mysql
* module Perl XML::Simple
```

Les types suivants sont utilisés :

- **Windows** : les hôtes qui semblent faire fonctionner une des versions du système d'exploitation de Microsoft Windows.
- **Linux** : les hôtes qui semblent faire fonctionner un système d'exploitation Linux.
- **Network** : le système d'exploitation ne peut être déterminé, il peut donc être un matériel réseau tel qu'un routeur, un concentrateur intelligent, une imprimante, ou un hôte fonctionnant avec Sun Solaris ou IBM AIX ... Peut-être que l'hôte fait fonctionner un logiciel pare-feu ?
- **Phantom** : un hôte qui ne répond pas à temps. Peut-être est-il éteint ou que c'est un pare-feu matériel ?

Si un matériel réseau est légitime, vous pouvez l'enregistrer en cliquant sur l'icône "Enregistrer" à la fin de la ligne correspondante. Vous serez capable d'entrer une brève description et de sélectionner le matériel réseau durant l'enregistrement (voir § [la section intitulée Enregistrer les hôtes connus](#)).

## Voir les hôtes fonctionnant avec IPDISCOVER

Vous pouvez voir la liste des hôtes faisant fonctionner IPDISCOVERY (les ordinateurs avec l'agent OCS Inventory NG installés, et l'agent est choisi par le serveur pour faire la découverte de son sous-réseau) sur votre réseau en cliquant sur le numéro dans la colonne "IpDiscover" dans la liste du réseau.

## Voir les hôtes identifiés ou connus

Vous pouvez voir la liste des hôtes connus toujours identifiés par quelqu'un sur votre réseau en cliquant sur le numéro dans la colonne "Identifié" dans la liste du réseau.

## Gérer les types de matériel connus

Vous pouvez enregistrer les matériels (tels que routeurs, concentrateurs, imprimantes réseaux, ordinateurs sur lesquels il n'y a pas l'agent d'inventaire ...) que vous connaissez comme légitimes. En tant que tels, ils ne seront pas affichés dans la liste des matériels non inventoriés, pour vous permettre de vous concentrer sur les matériels suspects.

Vous devez en premier définir quelques types de matériel pour les identifier facilement.

Cliquez sur le menu "Config" pour gérer les types de matériel.

Vous pouvez ajouter de nouveau type de matériel en entrant le "Nom Type" que vous voulez et en cliquant sur le bouton [ Envoyer ].

Vous pouvez supprimer tout type de matériel en cliquant sur la croix rouge à la fin de la ligne correspondante.

## Enregistrer les hôtes connus

Vous pouvez ajouter de nouveaux matériels en parcourant la liste des matériels non inventoriés et en cliquant sur l'icône à la fin de la ligne correspondante. Cela vous amènera sur la page pour ajouter ou supprimer les matériels réseaux et le champ "MAC" sera automatiquement rempli.

Pour supprimer un matériel réseau, cliquez juste sur la croix rouge à la fin de la ligne correspondante.

## Scanner une adresse IP

Vous pouvez faire une requête pour scanner une adresse IP spécifique afin d'obtenir l'information à-propos d'un hôte. Allez sur le menu "Sécurité" et cliquez sur le menu "Requête IP" et ensuite entrez l'adresse IP, le masque de réseau et cliquez sur le bouton [ Envoyer ].

N.B. : Cette fonctionnalité utilise le script perl IPDISCOVER-UTIL seulement sur serveur Linux qui requiert les composants suivants :

```
* nmap (testé sur 3.75)
* nmblookup (partie de la suite Samba, testé sur 3.0.7/3.0.10)
* module Perl Net::IP
* module Perl DBI
* module Perl DBD::mysql
* module Perl XML::Simple
```

Le script perl IPDISCOVER-UTIL utilise les utilitaires NMAP et NMBLOOKUP pour obtenir l'information à-propos de l'hôte (nom DNS, nom NetBios, ...) et aussi pour voir si l'hôte est inventorié et/ou découvert.



# TELEDEPLOYER DES PAQUETS

## Contenu

- [1 Déployer des paquets ou exécuter des commandes sur les clients](#)
  - [1.1 Comment cela fonctionne-t-il ?](#)
  - [1.2 Requis](#)
  - [1.3 Créer les paquets](#)
    - [1.3.1 Déployer les paquets au moyen de la commande "Lancer"](#)
    - [1.3.2 Déployer les paquets au moyen de la commande "Exécuter"](#)
    - [1.3.3 Commander au moyen de la commande "Exécuter"](#)
    - [1.3.4 Paquets enregistrés au moyen de la commande "Stocker"](#)
  - [1.4 Activer les paquets](#)
  - [1.5 Affecter les paquets aux ordinateurs](#)
  - [1.6 Désactiver les paquets](#)
  - [1.7 Déploiement des statistiques et validation des succès](#)
  - [1.8 Utiliser les certificats SSL dans le déploiement des paquets](#)
    - [1.8.1 Utiliser vos propres certificats](#)
      - [1.8.1.1 Avec un serveur OCS Inventory NG sous Linux](#)
      - [1.8.1.2 Avec le serveur OCS Inventory NG pour Windows](#)
    - [1.8.2 Utiliser PKI avec une Autorité de Certification](#)
      - [1.8.2.1 Avec un serveur OCS Inventory NG pour Linux](#)
      - [1.8.2.2 Avec un serveur OCS Inventory NG pour Windows](#)
  - [1.9 Exemple : Déployer de nouvelle version de l'Agent de Service Windows](#)

## Déployer des paquets ou exécuter des commandes sur les clients

OCS Inventory NG inclut la fonctionnalité de déploiement de paquet sur les ordinateurs clients. Depuis le serveur central de gestion, vous pouvez téléverser les paquets qui seront téléchargés au moyen d'HTTP/HTTPS et lancés par l'agent sur l'ordinateur client.

N.B. : Cette fonctionnalité a été testé seulement avec l'Agent de Service OCS Inventory NG pour Windows.

Comme l'installation du logiciel requiert les privilèges d'Administrateur, l'agent lancé au moyen d'un script d'ouverture de session ou par raccourci dans le menu de démarrage sous le compte de l'utilisateur qui ne peut être capable de lancer l'installation du logiciel.

Ainsi, le téléchargement en arrière plan du paquet peut prendre beaucoup de temps, et peut bloquer le script d'ouverture de session. Nous ne recommandons pas l'utilisation de la fonctionnalité de déploiement de paquet en utilisant un script d'ouverture de session d'inventaire.

## Comment cela fonctionne-t-il ?

### Un paquet a 4 composants principaux :

- une priorité
- une action
- optionnellement un fichier ZIP ou TAR.GZ incluant les fichiers ou répertoires que vous désirez
- et optionnellement une commande à lancer

Il y a 11 niveaux de priorité, niveau 0 à 10. Le niveau 0 est la plus haute priorité et le niveau 10 la plus basse. Un paquet ayant une priorité de niveau 0 sera déployé avant un paquet de niveau 1. Un paquet ayant une priorité de niveau 1 sera déployé avant un paquet de niveau 2 ...

L'action est associée avec le fichier à déployer ou la commande à lancer'. Ce triplet peut être un des suivants :

- **Action de lancement** : pour déployer un fichier ZIP ou TAR.GZ et lancer avec ou sans paramètre un fichier exécutable **incluant** un fichier ZIP ou TAR.GZ.  
Le fichier ZIP ou TAR.GZ sera décompressé dans un répertoire temporaire, et la commande associée (le nom du fichier exécutable sans le chemin !) sera lancée dans le répertoire temporaire.  
**Cette action permettra la réception du code de résultat de la commande lancée.**
- **Action d'exécution** : pour déployer un fichier ZIP ou TAR.GZ (optionnellement), et lancer avec ou sans paramètre un fichier exécutable **incluant ou non** un fichier ZIP ou TAR.GZ.  
Si l'exécutable n'est pas inclut dans le fichier ZIP ou TAR.GZ, il doit être une partie de logiciel toujours installé dans l'ordinateur client. Typiquement, cela peut être une commande Windows standard tel qu'un appel de l'installateur Windows, commande RPM, DPKG ou TAR.GZ sur Linux.  
Le fichier ZIP ou TAR.GZ sera décompressé dans un répertoire temporaire, et la commande associée (le nom du fichier exécutable avec le chemin ou les paramètres si besoin) sera lancée dans le répertoire temporaire.  
**Cette action ne permettra pas la réception du code de résultat de la commande lancée.**  
Toutefois, cette action vous permettra de faire fonctionner la commande sur chaque ordinateur client, sans déployer aucun fichier. Par exemple, vous pouvez l'utiliser pour faire fonctionner une commande spécifique de configuration du système d'exploitation.
- *Action d'enregistrement* : pour déployer un fichier ZIP ou TAR.GZ et enregistrer seulement son contenu dans un enregistrement de son ordinateur client.  
**Ceci n'est pas une commande associée avec une action, seulement un chemin à spécifier où enregistrer les fichiers extraits.**

N.B. : Tous les paquets que vous voulez déployer doivent être compressés en ZIP pour l'agent Windows et en TAR.GZ pour les ordinateurs Linux.

Si vous voulez construire votre propre installateur, vous pouvez regarder vers l'Installateur Système NullSoft (<http://nsis.sourceforge.net/>) ou l'Installateur Inno (<http://www.jrsoftware.org/>).

Ces outils sont des installateurs GPL pour Windows capables de créer un fichier installateur auto-extractible.

Par exemple, cette fonctionnalité vous permet de créer un paquet ZIP incluant l'exécutable Media Player Classic, un sous-répertoire incluant quelques fichiers MP3 et une playlist pour le Media Player Classic référençant ces MP3 dans le sous-répertoire. La commande associée appellera le Media Player Classic avec l'argument de lignes de commande pour lancer la playlist. Une fois les paquets téléchargés sur les clients Windows, les utilisateurs auront le Media Player Classic lancé et jouant les MP3 depuis la playlist. Merveilleux, n'est-ce pas ? ;-)

**Vous créez au moyen de la console d'administration votre paquet à déployer.** Il est automatiquement décrit par :

- Une référence dans la base de données, utilisée par le serveur de communication pour demander à l'agent de télécharger le paquet.
- Un fichier d'information, nommé "info". C'est un fichier XML décrivant le paquet et l'action de l'agent à lancer.
- 0 ou plusieurs fragments de fichier de données. Le fichier que vous téléversez (si cela est) sera découpé en plusieurs petites parties pour permettre à l'agent de le télécharger partie par partie, et alors de reprendre facilement un téléchargement échoué. Si le téléchargement de fragment échoue, seul ce fragment sera téléchargé une autre fois, et non pas tout le paquet. Il vous sera possible de choisir la taille des fragments en relation avec les capacités de votre réseau.

N.B. : Tout comme vous aurez téléversé votre paquet au moyen de la console d'administration, vous pourrez configurer

PHP et Apache pour permettre le téléversement de gros fichiers.

Voir § [la section intitulée Taille du téléversement pour le déploiement des paquets](#) pour savoir comment le configurer.

**Une fois le paquet construit, vous devez l'activer.** Cela indique où est localisé le serveur Web SSL (cf déploiement des serveurs) où l'agent sera capable de télécharger le fichier d'information et les fragments de fichiers.

**Finalement, vous devez sélectionner sur quel ordinateur vous déploierez le paquet.**

Maintenant, l'agent sera capable de déployer le paquet.

Quand l'agent envoie un inventaire au serveur de communication, le serveur de communication dit à l'agent s'il a un ou plusieurs paquets à déployer, avec le niveau de priorité pour chaque paquet, et où il peut trouver les fichiers d'information.

L'agent démarre alors une période de téléchargement. Une période est composée de cycles, définie par l'option de configuration "DOWNLOAD\_PERIOD\_LENGTH". Par défaut, une période contient une dizaine de cycles.

À chaque cycle, il calcule "le nombre de cycle modulo la priorité des paquets". Si cela est égale à 0, il télécharge les fichiers de fragments de paquets. Après chaque fragment, il attend une période "DOWNLOAD\_FRAG\_LATENCY" (option de configuration paramétrée à 10 par défaut) avant de télécharger le prochain fragment.

Quand tous les fragments du paquet sont téléchargés, il lance la commande de paquet et attend selon l'option "DOWNLOAD\_CYCLE\_LATENCY" (option de configuration paramétrée à 60 par défaut) avant de commencer un nouveau cycle et d'incrémenter le nombre de cycle.

Quand tous les cycles de la période ont été exécutés, il attend selon l'option "DOWNLOAD\_PERIOD\_LATENCY" (option de configuration paramétrée à 0 par défaut).

Si tous les paquets ont été téléchargés et installés avec succès, il s'arrête. Si cela n'est pas le cas, il commence une nouvelle période de cycles.

ATTENTION : Un niveau de priorité à 0 est un niveau spécial. Tous les paquets avec une priorité à 0 sont téléchargés avant tous les autres paquets avec la plus grande priorité au commencement de chaque cycle. Si le téléchargement échoue, l'agent essaiera de télécharger les paquets à priorité 0 échoués, sans vérifier les autres paquets.

Cela peut complètement stopper le déploiement. UTILISER LE NIVEAU DE PRIORITÉ À 0 AVEC PRÉCAUTION !

Vous pouvez utiliser ces paramètres pour personnaliser l'usage de la bande passante de votre réseau. En réduisant les options de latence, vous pouvez réduire le temps de téléchargement des fragments et réduire l'usage de votre réseau.

En réduisant l'option de la longueur de période, vous pouvez mettre en sursis de nouveaux téléchargements de paquets échoués, mais aussi, en réduisant la longueur de la période sur une valeur plus basse que 10, vous pouvez stopper le téléchargement de paquets avec un niveau de priorité plus haute que cette valeur.

## **Requis**

**Le serveur de déploiement enregistrant les fichiers d'information doit avoir SSL d'activé**, car le téléchargement des fichiers d'information de déploiement est très critique. Ce fichier d'information contient la description du paquet et la commande à lancer. Ainsi, si quelqu'un peut usurper votre serveur de déploiement, il peut lancer n'importe quelle commande sur votre ordinateur. C'est pourquoi le serveur de déploiement doit utiliser SSL pour permettre aux agents de s'authentifier au serveur et de s'assurer que c'est le véritable serveur de déploiement.

**L'agent doit avoir un certificat pour valider l'authentification au serveur de déploiement.** Ce certificat doit être enregistré dans un fichier "cacert.pem" dans le répertoire de l'agent OCS Inventory NG sous Windows et dans le répertoire "/etc/ocsinventory-client" sous Linux.

Sous Windows, vous pouvez utiliser le Packager OCS Inventory NG (voir § [la section intitulée Téléverser l'Agent pour le déploiement au moyen du lanceur "OcsLogon.exe"](#)) pour créer un installateur de l'agent qui inclut le certificat, ou vous pouvez utiliser le script d'ouverture de session suivant pour copier le fichier du certificat dans le répertoire de l'agent (assurez-vous que l'agent soit installé dans le répertoire "C:\Program Files\OCS Inventory Agent" et que le fichier de certificat est disponible dans la partage "MON\_PARTAGE" sur le serveur "MON\_SERVEUR").

```
@echo off
REM Check if CA file exists
if exist "C:\Program Files\OCS Inventory Agent\cacert.pem" goto CA_END
REM CA file does not exists, install it
Copy \\MON_SERVEUR\MON_PARTAGE\cacert.pem "C:\Program Files\OCS Inventory
Agent\cacert.pem"
:CA_END
```

**Si vous avez une infrastructure à clé publique**, vous devez créer un certificat de serveur valide pour votre serveur de déploiement et copier votre fichier de certificat d'autorité dans le fichier "cacert.pem".

**Si vous n'avez pas une infrastructure à clé publique**, vous pouvez utiliser votre propre certificat signé pour votre serveur de déploiement, et copier le certificat du serveur dans le fichier "cacert.pem".

Référez-vous à § [la section intitulée Utiliser les certificats SSL dans le déploiement des paquets](#), pour plus d'informations.

## **Créer les paquets**

En tout premier, vous devez créer les paquets.

Pointez votre souris sur le menu "Télédéploiement", et sélectionnez "Création".

Entrez un nom pour votre paquet.

Sélectionnez le système d'exploitation pour votre paquet. Vous pouvez choisir entre Windows et Linux.

Sélectionnez le protocole de téléchargement pour ce paquet. Pour l'instant, seul le protocole HTTP est disponible.

Sélectionnez la priorité du paquet. Vous pouvez choisir un niveau de priorité allant de 0 à 10. Les paquets ayant un niveau de priorité bas seront téléchargés avant ceux ayant un niveau de priorité plus grand, sauf si le téléchargement échoue. (cf § [la section intitulée Déploiement des statistiques et validation des succès](#)).

Vous pouvez aussi choisir d'avertir l'utilisateur que quelque chose est entrain de fonctionner sur l'ordinateur. Paramétrez la liste défilante "Prévenir utilisateur" sur "OUI", remplissez le champ "Texte" par le nom de l'utilisateur, combien de temps sera affiché le texte avant que l'installation du paquet s'auto-valide (paramétrez à 0 pour attendre indéfiniment), si l'utilisateur peut annuler le déploiement ou le retarder jusqu'au prochain inventaire.

Vous pouvez aussi spécifier si le déploiement du paquet a besoin de l'interaction utilisateur en paramétrant la liste déroulante "La fin de l'installation nécessite une intervention utilisateur :" sur "OUI", pour par exemple, si l'installateur a besoin que l'utilisateur remplisse des informations avant de terminer.

Enfin, vous pouvez sélectionner une action dans la liste déroulante "Action". Ci-dessous est décrit comment vous pouvez utiliser tout cela.

## Déployer les paquets au moyen de la commande "Lancer"

Le paquet que vous désirez déployer a un ou plusieurs fichiers, avec au minimum un fichier exécutable pour lancer l'installation du paquet. Comprimez ces fichiers en utilisant un outil ZIP si le paquet est à destination d'ordinateurs sous Windows, ou en utilisant tar et gzip si le paquet est à destination d'ordinateurs sous Linux.

Choisissez l'action "Lancer" puis cliquez sur le bouton [ Parcourir ] pour sélectionner votre fichier ZIP ou TAR.GZ.

Dans le champ "Nom du fichier :", remplissez simplement le nom du fichier sans son chemin, mais avec, en option, des arguments. Cette commande sera lancée sur l'ordinateur client une fois que le paquet sera téléchargé et décompressé dans un répertoire temporaire.

Dans notre exemple, nous déployons une nouvelle version de l'agent OCS Inventory Agent pour Windows, en utilisant l'installation silencieuse, en spécifiant l'adresse du serveur de Communication "mon\_serveur\_communication\_ocs", en désactivant l'usage des paramètres du proxy d'Internet Explorer et en utilisant le mode de débogage. Ainsi, le fichier ZIP inclut le fichier "OcsAgentSetup.exe" et contient les informations du champ nommé "Nom de fichier" :

- `OcsAgentSetup.exe /S /SERVER:mon_serveur_communication_ocs /NP /DEBUG`

Cliquez sur le bouton [ Envoyer ] pour téléverser le paquet dans la console d'Administration.

Maintenant, vous devez spécifier la taille de chaque fragment du paquet pour permettre à l'agent de télécharger le paquet par petits morceaux. Ceci permet le téléchargement par résumé. Si le téléchargement d'un fragment échoue, seul ce fragment sera téléchargé une autre fois, et non l'ensemble du paquet. Ainsi choisir la taille des fragments permet d'activer cette fonctionnalité réseau.

La console d'administration découpera alors le paquet en fragments et les enregistrera avec le nom du paquet daté dans le répertoire "download" à la racine du répertoire du serveur web Apache. Il créera aussi

dans le même répertoire le fichier d'information nommé "info" relatif au paquet, dans un fichier XML décrivant le paquet et l'action de l'agent à lancer.

## Déployer les paquets au moyen de la commande "Exécuter"

Le paquet que vous désirez déployer a un ou plusieurs fichiers, avec au minimum un fichier exécutable pour lancer l'installation du paquet. Comprimez ces fichiers en utilisant un outil ZIP si le paquet est à destination d'ordinateurs sous Windows, ou en utilisant tar et gzip si le paquet est à destination d'ordinateurs sous Linux.

Choisissez l'action "Exécuter" puis cliquez sur le bouton [ Parcourir ] pour sélectionner votre fichier ZIP ou TAR.GZ.

Dans le champ "Commande", remplissez le nom du chemin du fichier de l'exécutable à lancer avec ces arguments (le nom complet du chemin n'est pas requis tant que l'application exécutable est listé dans le système, ou est inclu dans le paquet). Cette commande sera lancé sur l'ordinateur client une fois que le paquet sera téléchargé.

N.B. : Les variables d'environnement sont ajoutables dans la "Commande". Il est permis d'utiliser des variables telles que %SystemDrive%, %SystemRoot%, %windir%, %ProgramFiles%, %CommonProgramFiles%, etc...

Dans notre exemple, nous déployons le logiciel en utilisant l'installation silencieuse de Windows Installer. Ainsi, le fichier ZIP inclue le fichier "software.msi" et le champ de "Commande" :

- `msiexec.exe /i software.msi /quiet`

Cliquez sur le bouton [ Envoyer ] pour téléverser le paquet dans la console d'Administration.

Maintenant, vous devez spécifier la taille de chaque fragment du paquet pour permettre à l'agent de télécharger le paquet par petits morceaux. Ceci permet le téléchargement par résumé. Si le téléchargement d'un fragment échoue, seul ce fragment sera téléchargé une autre fois, et non l'ensemble du paquet. Ainsi choisir la taille des fragments permet d'activer cette fonctionnalité réseau.

La console d'administration découpera alors le paquet en fragments et les enregistrera avec le nom du paquet daté dans le répertoire "download" à la racine du répertoire du serveur web Apache. Il créera aussi dans le même répertoire le fichier d'information nommé "info" relatif au paquet, dans un fichier XML décrivant le paquet et l'action de l'agent à lancer.

## Commander au moyen de la commande "Exécuter"

Le paquet que vous voulez déployer est seulement une commande à lancer.

Choisissez l'action "Exécuter" et laissez le champ "Fichier" vide.

Dans le champ "Commande", remplissez le nom de la commande avec, en option, ces arguments. Cette commande sera lancée sur l'ordinateur client une fois que le paquet sera téléchargé.

N.B. : Les variables d'environnement sont ajoutables dans la "Commande". Il est permis d'utiliser des variables telles que %SystemDrive%, %SystemRoot%, %windir%, %ProgramFiles%, %CommonProgramFiles%, etc...

Dans notre exemple, nous déployons une commande pour spécifier l'adresse du proxy à utiliser pour les systèmes d'exploitation sous Windows. Ainsi le champ "Commande" contiendra :

- `Proxycfg.exe /p 192.168.1.1`

Cliquez sur le bouton [ Envoyer ] pour téléverser le paquet dans la console d'administration.

Comme vous n'avez pas sélectionné de fichier à téléverser, la page pour configurer la taille des fragments ne sera pas affichée. La console d'administration créera seulement, dans un répertoire nommé comme le paquet daté dans le répertoire "download" à la racine du serveur web Apache, le fichier d'information du paquet nommé "info", un fichier XML décrivant le paquet et l'action de l'agent à lancer.

## **Paquets enregistrés au moyen de la commande "Stocker"**

Le paquet que vous désirez déployer a un ou plusieurs fichiers, pour être enregistré dans un répertoire spécifique sur les ordinateurs clients. Comprimez ces fichiers en utilisant un outil ZIP si le paquet est à destination d'ordinateurs sous Windows, ou en utilisant tar et gzip si le paquet est à destination d'ordinateurs sous Linux.

Choisissez l'action "Stocker" et cliquez sur le bouton [ Parcourir ] pour sélectionner votre fichier ZIP ou TAR.GZ.

Dans le champ "Chemin", remplissez le nom du chemin où l'agent extraira les fichiers une fois que le paquet sera téléchargé.

N.B. : Les variables d'environnement sont ajoutables dans la "Commande". Il est permis d'utiliser des variables telles que %SystemDrive%, %SystemRoot%, %windir%, %ProgramFiles%, %CommonProgramFiles%, etc... Ainsi, si le répertoire requis n'existe pas, il sera récursivement créé.

Dans notre exemple, nous déployons un fichier à enregistrer dans le répertoire "C:\MyFolder".

Cliquez sur le bouton [ Envoyer ] pour téléverser le paquet dans la console d'administration.

Maintenant, vous devez spécifier la taille de chaque fragment du paquet pour permettre à l'agent de télécharger le paquet par petits morceaux. Ceci permet le téléchargement par résumé. Si le téléchargement d'un fragment échoue, seul ce fragment sera téléchargé une autre fois, et non l'ensemble du paquet. Ainsi choisir la taille des fragments permet d'activer cette fonctionnalité réseau.

La console d'administration découpera alors le paquet en fragments et les enregistrera avec le nom du paquet daté dans le répertoire "download" à la racine du répertoire du serveur web Apache. Il créera aussi dans le même répertoire le fichier d'information nommé "info" relatif au paquet, dans un fichier XML décrivant le paquet et l'action de l'agent à lancer.

## **Activer les paquets**

Une fois que le paquet a été créé, vous devez spécifier où l'agent peut le télécharger.

L'agent en premier téléchargera le fichier d'information. Comme ce fichier est d'une importance très critique, ce téléchargement doit être fait en utilisant HTTPS afin de s'assurer que l'agent s'authentifie auprès du serveur de déploiement. Puis, le téléchargement des fragments de paquet décrits dans le fichier d'information sera fait en utilisant le standard HTTP.

N.B. : Si vous ne voulez pas utiliser le serveur d'administration comme serveur de déploiement, vous devez copier en premier le répertoire "download/paquet\_daté" depuis la racine du serveur web Apache de votre serveur d'administration vers un autre serveur.

Vous devriez utiliser un utilitaire de synchronisation tel que rsync (<http://samba.anu.edu.au/rsync>) pour automatiser cette tâche, autrement il vous faudra le faire manuellement.

Vous devriez choisir aussi le fichier d'information hôte sur le serveur web différent de celui qui a les fichiers de fragments.

Par exemple, si vous avez de multiples sites géographiques avec un seul serveur de communication central, vous devriez avoir les fichiers d'information hôte sur le serveur de communication, et les fichiers de fragments sur chacun des serveurs web sur chaque site.

Pour cela, vous avez besoin d'activer un paquet par site, et pour chaque paquet, le fichier d'information sera hébergé sur le serveur de communication et les fragments de fichiers sur les serveurs web par site. Ceci diminuera dramatiquement la bande passante entre vos réseaux.

Pointez votre souris sur le menu "Téléploiement" et sélectionnez "Activation". Vous verrez ici tous les paquets construits, et aussi TOUS les paquets activés.

**Vous pouvez cliquer sur la croix rouge pour supprimer un paquet construit.** Ceci supprimera toute référence au paquet dans la base de données et effacera aussi les fichiers d'informations et de fragments dans le répertoire de téléchargement de la console d'administration. Ainsi, les paquets supprimés seront indisponibles à l'activation, tous les paquets activés utilisant ce paquet seront supprimés, et aussi les non affectés à des ordinateurs.

**Cliquez sur le bouton [ Activer ] de la ligne correspondante au paquet que vous voulez activer.**

Dans le champ "Url HTTPS", entrez l'URL HTTPS du fichier d'information de paquet.

Dans le champ "Url HTTP", entrez l'URL HTTP des fichiers de fragments de paquet.

N.B. : Ne pas entrer 'localhost' comme URL ! Souvenez-vous que ces URLs sont fournis par les agents.

Si votre serveur de déploiement HTTP ou HTTPS fonctionne sur des ports non standards, vous devez spécifier le port

en utilisant la notation standard "adresse\_serveur:port\_serveur/repertoire".

Par exemple, votre serveur de déploiement fonctionne sur le port HTTP 8080 et sur le port HTTPS 4343

sur le serveur 192.168.1.1, les paquets sont localisés dans le répertoire /download.

Vous devez remplir ainsi :

https url: 192.168.1.1:4343/download

http url: 192.168.1.1:8080/download

Dans notre cas, nous avons choisi d'utiliser le serveur d'administration comme serveur de déploiement pour les deux fichiers d'information et fichiers de fragments de paquet.

Ainsi, nous avons rempli dans les deux champs quelque chose comme "ocs-admin-srv.domain.tld/download".

Cliquez sur le bouton [ Envoyer ]. La console d'administration s'assurera alors que les deux fichiers d'information et de fragments de paquets sont disponibles aux adresses URLs spécifiées.

**La colonne "Non notifié"** vous montre le nombre d'ordinateurs qui n'ont pas été notifiés qu'ils ont un paquet à télécharger.

**La colonne "Succès"** vous montre le nombre d'ordinateurs qui ont déployé avec succès le paquet correspondant.

**La colonne "Erreurs"** vous montre le nombre d'ordinateurs qui ont rencontré une erreur dans le déploiement du paquet correspondant.

**L'icône "Stat"** vous permet de voir le pourcentage d'ordinateurs qui sont en attente de notification, ceux qui ont été notifiés (le serveur leur demande de déployer le paquet) et ceux qui ont fini le déploiement avec un code de résultat (SUCCESS ou ERROR).

## ***Affecter les paquets aux ordinateurs***

Vous pouvez affecter les paquets à l'ordinateur, un par un, en affichant les propriétés de l'ordinateur, en cliquant sur l'icône "Personnalisation" et en ajoutant le paquet. Toutefois, ce n'est vraiment pas la meilleure façon si vous voulez affecter des paquets à plusieurs ordinateurs.

La meilleure façon est d'utiliser la "recherche multicritères" pour rechercher les ordinateurs que vous désirez, et d'affecter les paquets à tous ces ordinateurs en une seule fois.

Dans l'exemple suivant, nous affectons les paquets que nous avons créés à tous les ordinateurs MS Windows XP.

En premier, nous recherchons les ordinateurs MS Windows XP.

La recherche nous retourne 59 ordinateurs sur 4 pages.

Cliquez juste sur le lien "Déployer" pour déployer sur tous les ordinateurs retournés par la recherche, et pas seulement ceux qui sont visibles.

Cliquez sur l'icône "Affecter" sur la ligne du paquet pour affecter ce paquet à tous les ordinateurs.

Les agents sur les ordinateurs seront notifiés au prochain contact avec le serveur de communication qu'ils ont tel paquet à déployer. Ainsi, tant que l'agent ne contacte pas le serveur de communication, l'ordinateur apparaîtra dans la console d'administration avec le statut "EN ATTENTE DE NOTIFICATION". Une fois que l'agent aura contacté le serveur de communication, le statut deviendra "NOTIFIÉ".

## ***Désactiver les paquets***

[[Image:]] Pointez votre souris sur le menu "Téléploiement" et sélectionnez "Activés". Vous verrez ici tous les paquets disponibles pour le déploiement sur les ordinateurs.

**L'icône en forme de croix rouge désaffectera le paquet pour tous les ordinateurs, et désactivera le paquet.** Ainsi le paquet est toujours référencé dans la base de donnée, les fichiers d'information et de fragments sont encore disponibles dans le répertoire de téléchargement du serveur d'administration. Toutefois, ils ont le même statut tout comme si vous veniez juste de les construire et en attente d'être activés.

## ***Déploiement des statistiques et validation des succès***

Comme les paquets ont été activés puis désactivés, les statistiques de déploiement sont visibles depuis le menu "Activation".

Vous pouvez voir les statistiques de déploiement en cliquant sur l'icône "Stats" pour chaque paquet.

Dès que vous avez affecté le paquet à au moins un ordinateur, vous avez une statistique graphique montrant le statut de notification de déploiement.

Le statut peut être un des suivants :

Tableau des différents codes de statut de notification	
Code de statut	Énoncé
WAITING NOTIFICATION EN ATTENTE DE NOTIFICATION	Le serveur attend la communication avec l'agent pour notifier celui-ci qu'il a quelque chose à télécharger.
NOTIFIED NOTIFIÉ	L'agent a été notifié qu'il a quelque chose à télécharger. Maintenant est en attente du code de résultat.
SUCCESS [code] SUCCÈS	L'agent a téléchargé avec succès le paquet et à lancer la commande d'extraction ou d'enregistrement des données.
ERR_ALREADY_SETUP	Le paquet a été précédemment installé avec succès sur l'ordinateur.
ERR_BAD_ID	L'agent est incapable de télécharger le paquet parce qu'il ne peut trouver l'ID(entifiant) du paquet sur le serveur de déploiement.
ERR_BAD_DIGEST	Le téléchargement des données a une mauvaise signature, ainsi l'agent n'exécute pas la commande associée.
ERR_DOWNLOAD_PACK	L'agent a été incapable de décompresser le fichier ZIP ou TAR.GZ téléchargé.
ERR_BUILD	L'agent a été incapable de reconstruire les fragments de paquets.
ERR_EXECUTE	L'agent a été incapable d'exécuter la commande associée.
ERR_CLEAN	L'agent a été incapable de nettoyer (supprimer ?) le paquet téléchargé.
ERR_TIMEOUT	L'agent a été incapable de télécharger le paquet durant le nombre de jours permis.
ERR_ABORTED	L'utilisateur a arrêté la commande d'exécution du paquet. (Vous aviez choisi de lui notifier, et de lui permettre l'arrêt).
ERR_EXECUTE_PACK	Non utilisée.

**"Valider Succès"** effacera les statistiques des ordinateurs qui ont déployé avec succès les paquets.

**"Désaffecter les non notifiés"** désaffectera les paquets pour les ordinateurs qui n'ont pas été contactés par le serveur depuis que vous avez affecté les paquets aux ordinateurs. Le paquet ne sera pas supprimé, seulement les ordinateurs qui n'ont pas maintenant reçu cet ordre de déployer le paquet auront l'ordre d'abandonner.

**"Tout valider"** effacera toutes les statistiques, et désaffectera le paquet pour les ordinateurs non notifiés. Ceci est identique à "Valider Succès" + "Désaffecter les non notifiés".

N.B. : Vous DEVEZ valider le statut de déploiement une fois que le déploiement est terminé pour nettoyer la base de donnée du statut de déploiement sur les ordinateurs. Autrement, la base de données grossira et diminuera en puissance !

Vous pouvez cliquer sur le numéro de ligne de chaque statut pour afficher les ordinateurs qui ont un statut de déploiement.

### **Utiliser les certificats SSL dans le déploiement des paquets**

L'infrastructure de déploiement de paquet est beaucoup trop puissante, ainsi elle requiert l'accès SSL pour s'authentifier au serveur avant d'essayer à télécharger quelque chose depuis celui-ci. Nous avons ainsi besoin de certificats SSL à utiliser avec votre serveur de déploiement.

La définition de certificat est lisible sur [http://fr.wikipedia.org/wiki/Certificat\\_%C3%A9lectronique](http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique) :

Un **certificat électronique** est une carte d'identité numérique dont l'objet est d'identifier une entité physique ou non-physique. Le certificat numérique ou électronique est un lien entre l'entité physique et

l'entité numérique (Virtuel). L'autorité de certification fait foi de tiers de confiance et atteste du lien entre l'identité physique et l'entité numérique. (...).

(voir aussi [http://fr.wikipedia.org/wiki/Public\\_Key\\_Infrastructure](http://fr.wikipedia.org/wiki/Public_Key_Infrastructure))

Vous pouvez utiliser un rapide, manière facile mais limitée, **certificat auto-signé** ou un outil plus sécurisé et fiable, **une clé PKI avec Autorité de Certification**.

Le serveur web Apache est fourni avec les bibliothèques de cryptage OpenSSL, qui permet de créer et gérer les certificats.

## Utiliser vos propres certificats

N.B. : Veuillez faire attention à la période de validité des certificats, comme le serveur web signe lui-même les certificats à installer sur chaque ordinateur qui fait fonctionner l'agent. Quand le certificat expire, vous devrez générer et déployer de nouveaux certificats sur chaque ordinateur !

## Avec un serveur OCS Inventory NG sous Linux

Habituellement, les paquets Apache et mod\_ssl s'installent avec des exemples de scripts pour générer les certificats, et spécifiquement des certificats de tests.

Toutefois, nous vous fournissons ci-dessous un exemple de script utilisant OpenSSL pour générer soi-même un certificat à utiliser avec Apache, que vous nommerez 'apache\_generate\_cert.sh' :

```
<script>
#!/bin/sh
#
# En premier, generer le certificat requis
#
# Generer une clé RSA de 1024 bits, enregistrer la cle privée dans un
# fichier PEM de mot-de-passe non protege server.key, en utilisant
# le fichier de configuration par default d'openssl
#
echo
echo Generation de la cle privée du serveur Apache...
echo
openssl genrsa -out server.key 1024
#
# Maintenant, signez le certificat du serveur Apache avec
# la cle du serveur Apache
#
# Signez avec le certificat PEM server.crt,
# en utilisant le fichier PEM server.key pour cle privée du server,
# en utilisant le fichier de configuration par default d'openssl.
#
# Le certificat produit sera valide durant 1825 jours (soit 5 ans).
#
echo
echo Generation des certificats auto-signes du serveur Apache ...
echo
openssl req -outform PEM -new -key server.key -x509 -days 1825 -out server.crt
</script>
```

Ce script génère une clé privée RSA dans le fichier "server.key" et un certificat X.509 auto-signé dans le fichier "server.crt".

**En premier**, lancez ce script en utilisant cette commande :

- `sh apache_generate_cert.sh`

Celui-ci générera la clé privée, et vous demandera les propriétés du certificat :

- le code pays, habituellement requis
- le nom de la province ou de l'état, habituellement requis
- le nom de la ville, habituellement requis
- le nom de votre organisation, habituellement requis
- le nom de votre section d'organisation, habituellement requis
- le nom commun (le nom DNS ou l'adresse ip de votre serveur), requis
- une adresse email, habituellement optionnelle

Dans notre exemple, nous avons généré un certificat auto-signé pour le serveur ayant le nom "ocs.domain.tld".

**Maintenant**, vous devez copier le fichier du certificat du serveur "server.crt" et le fichier de la clé privée "server.key" dans les répertoires appropriés du serveur Apache et mettre-à-jour les fichiers de configuration d'Apache/mod\_ssl pour utiliser ces fichiers.

**Voici un exemple minimaliste de configuration d'Apache/mod\_ssl** pour utiliser SSL sous CentOS/Fedora/RedHat Linux. (Le certificat du serveur est enregistré dans le répertoire "/etc/httpd/conf/ssl.crt" et la clé du serveur est enregistrée dans le répertoire "/etc/httpd/conf/ssl.key").

N.B. : Généralement, la configuration Apache/mod\_ssl est fournie par votre système. Aussi, vous ne devez pas utiliser la configuration ci-dessous si votre système a toujours un fichier de configuration pour mod\_ssl.

```
#
# This is the Apache server configuration file providing SSL support.
# It contains the configuration directives to instruct the server how to
# serve pages over an https connection. For detailing information about these
# directives see <URL:http://httpd.apache.org/docs-2.0/mod/mod_ssl.html>
#
# For the moment, see <URL:http://www.modssl.org/docs/> for this info.
# The documents are still being prepared from material donated by the
# modssl project.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
LoadModule ssl_module modules/mod_ssl.so
# Until documentation is completed, please check http://www.modssl.org/
# for additional config examples and module documentation. Directives
# and features of mod_ssl are largely unchanged from the mod_ssl project
# for Apache 1.3.
#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
# To allow connections to IPv6 addresses add "Listen [::]:443"
#
Listen 0.0.0.0:443
#
# Some MIME-types for downloading Certificates and CRLs
#
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl
# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is a internal
# terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog builtin
##
## SSL Virtual Host Context
##
```

```

<VirtualHost _default_:443>
# Use separate log files:
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. A test
# certificate can be generated with `make certificate' under
# built time. Keep in mind that if you've both a RSA and a DSA
# certificate you can configure both in parallel (to also allow
# the use of DSA ciphers, etc.)
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
# SSL Engine Options:
# StdEnvVars:
# This exports the standard SSL/TLS related `SSL_*' environment variables.
# Per default this exportation is switched off for performance reasons,
# because the extraction step is an expensive operation and is usually
# useless for serving static content. So one usually enables the
# exportation for CGI and SSI requests only.
SSLOptions +StdEnvVars
# SSL Protocol Adjustments:
# The safe and default but still SSL/TLS standard compliant shutdown
# approach is that mod_ssl sends the close notify alert but doesn't wait for
# the close notify alert from client. When you need a different shutdown
# approach you can use one of the following variables:
# o ssl-unclean-shutdown:
# This forces an unclean shutdown when the connection is closed, i.e. no
# SSL close notify alert is send or allowed to received. This violates
# the SSL/TLS standard but is needed for some brain-dead browsers. Use
# this when you receive I/O errors because of the standard approach where
# mod_ssl sends the close notify alert.
# o ssl-accurate-shutdown:
# This forces an accurate shutdown when the connection is closed, i.e. a
# SSL close notify alert is send and mod_ssl waits for the close notify
# alert of the client. This is 100% SSL/TLS standard compliant, but in
# practice often causes hanging connections with brain-dead browsers. Use
# this only for browsers where you know that their SSL implementation
# works correctly.
# Notice: Most problems of broken clients are also related to the HTTP
# keep-alive facility, so you usually additionally want to disable
# keep-alive for those clients, too. Use variable "nokeepalive" for this.
# Similarly, one has to force some clients to use HTTP/1.0 to workaroud
# their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
# "force-response-1.0" for this.
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
# Per-Server Logging:
# The home of a custom SSL log file. Use this when you want a
# compact non-error SSL logfile on a virtual host basis.
CustomLog logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>

```

Une fois que vous avez configuré votre serveur web Apache, n'oubliez pas de redémarrer le démon Apache pour que les changements prennent effets.

**En dernier**, vous devez installer le fichier du certificat du serveur "server.crt" sur chaque ordinateur client dans le répertoire d'installation de l'agent OCS Inventory NG, sous le nom de "cacert.pem".

## Avec le serveur OCS Inventory NG pour Windows

La solution XAMPP Apache est fournie avec un script "makecert.bat" pour générer les certificats auto-signés. Ce script est localisé sous le répertoire "CHEMIN\_INSTALL\xampp\apache" (où CHEMIN\_INSTALL est le répertoire d'installation du serveur OCS Inventory NG).

```
@echo off
set OPENSSSL_CONF=./bin/openssl.cnf
if not exist .\conf\ssl.crt mkdir .\conf\ssl.crt
if not exist .\conf\ssl.key mkdir .\conf\ssl.key
bin\openssl req -new -out server.csr
bin\openssl rsa -in privkey.pem -out server.key
bin\openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 365
set OPENSSSL_CONF=
del .rnd
del privkey.pem
del server.csr
move /y server.crt .\conf\ssl.crt
move /y server.key .\conf\ssl.key
echo.
echo -----
echo Das Zertifikat wurde erstellt.
echo The certificate was provided.
echo.
Pause
```

Le script génère un certificat auto-signé utilisable 365 jours. Si vous voulez augmenter la validité du certificat, vous devez modifier la directive "-days 365" pour spécifier en nombre de jours la nouvelle période de validité (1825 jours, soit 5 ans doit être une bonne valeur ;- ) ... )

Faites fonctionner deux fois le script "makecert.bat". Ceci générera une clé privée RSA et vous demandera un mot-de-passe (au moins 4 caractères).

Tapez-le mot-de-passe et confirmez-le.

En suivant, vous devrez remplir certaines propriétés :

- le code pays, habituellement requis
- le nom de la province ou de l'état, habituellement requis
- le nom de la ville, habituellement requis
- le nom de votre organisation, habituellement requis
- le nom de votre section d'organisation, habituellement requis
- le nom commun (le nom DNS ou l'adresse ip de votre serveur), requis
- une adresse email, habituellement optionnelle

Finalement, il vous sera demandé le mot-de-passe de la clé privée :

Maintenant, le certificat auto-signé est créé et installé. Redémarrez justement les services d'Apache2 pour que les changements prennent effets.

## Utiliser PKI avec une Autorité de Certification

Nous supposons que vous utilisez un serveur PKI interne ou commercial tel que Verisign.

Toutefois, si vous n'en avez pas un en interne, et que vous ne souhaitez pas payer vos certificats, vous pouvez utiliser les services fournis par cacert.org (<http://cacert.org>), un fournisseur de services PKI, mondial et gratuit.

Utiliser les services du CAcert requiert que vous enregistriez votre email et votre nom de domaine DNS, avant d'être capable de demander le certificat serveur. Lire les manuels sur cacert.org.

Vous pouvez regarder l'excellent article de Pablo Iranzo Gómez (<http://alufis35.uv.es/OCS-Inventory-Package-Deployment.html>) pour de plus amples instructions à-propos de l'usage de certificat du cacert dans OCS Inventory NG.

## Avec un serveur OCS Inventory NG pour Linux

Habituellement, les paquets Apache et mod\_ssl sont fournis avec des exemples de scripts pour générer les certificats requis à soumettre à un fournisseur PKI.

Toutefois, nous vous fournissons ci-dessous un exemple de script utilisant OpenSSL pour générer un certificat requis à utiliser avec Apache.

### Exemple de script apache\_request\_cert.sh

```
<script>
#!/bin/sh
#
# Generate server certificate request
#
# Generate 1024 bits RSA key, store private key in a
# no password protected PEM file server.key, store certificate
# request in a PEM file server.csr, using system default
# configuration file
#
# The produced key will be valid for 1825 days (5 years)
#
echo
echo Generating server private key and certificate request...
echo
openssl req -newkey rsa:1024 -outform PEM -out server.csr -keyout server.key -keyform
PEM -days 1825 -nodes
</script>
```

Ce script génère une clé privée RSA dans le fichier "server.key" et un certificat requis dans le fichier "server.csr".

**En premier**, lancez le script par cette commande :

- `sh apache_request_cert.sh`

Cela générera la clé privée et vous demandera des informations pour le certificat requis :

- Code pays, habituellement requis
- Nom de la province ou de l'Etat, habituellement requis
- Nom de la ville, habituellement requis
- Nom de votre organisation ou société, habituellement requis
- Nom de votre section, habituellement optionnel
- Nom commun (nom DNS ou adresse IP de votre serveur), requis

- Une adresse courriel, requis pour recevoir le certificat généré par l'Autorité de Certification.
- Un mot-de-passe en option
- Un nom de société en option

Dans notre exemple, nous générons un certificat requis pour notre serveur de nom "ocs.domain.tld".

**Ensuite**, vous devez transmettre notre certificat requis "server.csr" à votre Autorité de Certification PKI.

**Une fois le certificat serveur de l'Autorité de Certification reçu**, vous avez juste à copier le fichier "server.crt", le certificat serveur, et la clé privée du serveur "server.key" dans leur répertoire approprié, et de mettre-à-jour les fichiers de configuration d'Apache et mod\_ssl pour utiliser ces fichiers.

Vous devez aussi recevoir le Certificat Racine de l'Autorité de Certification dans un fichier "ca\_root.crt" à spécifier dans la configuration d'Apache.

**Voici un exemple minimaliste de configuration Apache et mod\_ssl** pour utiliser SSL avec Linux CentOS/Fedora/Red Hat. (Le certificat serveur est enregistré dans le répertoire "/etc/httpd/conf/ssl.crt" et la clé du serveur sous "/etc/httpd/conf/ssl.key").

N.B. : Généralement, Apache pour Windows est fourni avec un fichier de configuration Apache et mod\_ssl prédéfini.

Ainsi, n'utilisez pas la configuration suivante si votre système a déjà un fichier de configuration pour mod\_ssl !

#### **Exemple de fichier de configuration Apache/mod\_ssl**

```
<script>
#
# This is the Apache server configuration file providing SSL support.
# It contains the configuration directives to instruct the server how to
# serve pages over an https connection. For detailing information about these
# directives see <URL:http://httpd.apache.org/docs-2.0/mod/mod_ssl.html>
#
# For the moment, see <URL:http://www.modssl.org/docs/> for this info.
# The documents are still being prepared from material donated by the
# modssl project.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
LoadModule ssl_module modules/mod_ssl.so
# Until documentation is completed, please check http://www.modssl.org/
# for additional config examples and module documentation. Directives
# and features of mod_ssl are largely unchanged from the mod_ssl project
# for Apache 1.3.
#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
# To allow connections to IPv6 addresses add "Listen [::]:443"
#
Listen 0.0.0.0:443
#
# Some MIME-types for downloading Certificates and CRLs
#
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl
# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is a internal
# terminal dialog) has to provide the pass phrase on stdout.
```

```

SSLPassPhraseDialog builtin
##
## SSL Virtual Host Context
##
<VirtualHost _default_:443>
# Use separate log files:
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. A test
# certificate can be generated with `make certificate' under
# built time. Keep in mind that if you've both a RSA and a DSA
# certificate you can configure both in parallel (to also allow
# the use of DSA ciphers, etc.)
SSLCertificateFile /etc/httpd/conf/ssl.crt/server.crt
# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.key
# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
# Note: Inside SSLCACertificatePath you need hash symlinks
#       to point to the certificate files. Use the provided
#       Makefile to update the hash symlinks after changes.
#SSLCACertificatePath /etc/httpd/conf/ssl.crt
SSLCACertificateFile /usr/share/ssl/certs/ca_root.crt
# SSL Engine Options:
# StdEnvVars:
# This exports the standard SSL/TLS related `SSL_*' environment variables.
# Per default this exportation is switched off for performance reasons,
# because the extraction step is an expensive operation and is usually
# useless for serving static content. So one usually enables the
# exportation for CGI and SSI requests only.
SSLOptions +StdEnvVars
# SSL Protocol Adjustments:
# The safe and default but still SSL/TLS standard compliant shutdown
# approach is that mod_ssl sends the close notify alert but doesn't wait for
# the close notify alert from client. When you need a different shutdown
# approach you can use one of the following variables:
# o ssl-unclean-shutdown:
# This forces an unclean shutdown when the connection is closed, i.e. no
# SSL close notify alert is send or allowed to received. This violates
# the SSL/TLS standard but is needed for some brain-dead browsers. Use
# this when you receive I/O errors because of the standard approach where
# mod_ssl sends the close notify alert.
# o ssl-accurate-shutdown:
# This forces an accurate shutdown when the connection is closed, i.e. a
# SSL close notify alert is send and mod_ssl waits for the close notify
# alert of the client. This is 100% SSL/TLS standard compliant, but in
# practice often causes hanging connections with brain-dead browsers. Use
# this only for browsers where you know that their SSL implementation
# works correctly.
# Notice: Most problems of broken clients are also related to the HTTP
# keep-alive facility, so you usually additionally want to disable

```

```

# keep-alive for those clients, too. Use variable "nokeepalive" for this.
# Similarly, one has to force some clients to use HTTP/1.0 to workaroud
# their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
# "force-response-1.0" for this.
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
# Per-Server Logging:
# The home of a custom SSL log file. Use this when you want a
# compact non-error SSL logfile on a virtual host basis.
CustomLog logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
</script>

```

Une fois votre serveur web Apache configuré, n'oubliez pas de redémarrer le service Apache pour que les modifications prennent effet.

**Dernièrement**, vous devez installer le fichier certificat racine de l'Autorité de Certification "ca\_root.crt" sur chaque ordinateur client dans le répertoire d'installation de l'agent OCS Inventory NG, sous le nom "cacert.pem".

## Avec un serveur OCS Inventory NG pour Windows

Nous fournissons ci-dessous un exemple de script utilisant OpenSSL pour générer le certificat requis à utiliser dans XAMPP Apache.

### Exemple de script apache\_request\_cert.sh

```

<script>
@echo off
REM
REM Generate server certificate request
REM
REM Generate 1024 bits RSA key, store private key in a
REM no password protected PEM file server.key, store certificate
REM request in a PEM file server.csr, using system default
REM configuration file
REM
REM The produced key will be valid for 1825 days (5 years)
REM
echo.
echo Generating server private key and certificate request...
echo.
set OPENSSL_CONF=./bin/openssl.cnf
bin\openssl req -newkey rsa:1024 -outform PEM -out server.csr -keyout server.key -
keyform PEM -days 1825 -nodes
</script>

```

Ce script génère une clé privée RSA dans le fichier "server.key" et un certificat requis dans le fichier "server.csr".

**Premièrement**, copiez ce script dans le répertoire "INSTALL\_PATH\xampp\apache" (où INSTALL\_PATH est le répertoire d'installation d'OCS Inventory NG) puis lancez-le.

Cela générera la clé privée et vous demandera certaines informations pour le certificat requis :

- Code du pays, habituellement requis
- Nom de la province ou de l'état, habituellement requis
- Ville, habituellement requis
- Nom de l'organisation ou société, habituellement requis
- Nom de l'unité dans la société, habituellement optionnel

- Nom commun (ceci est le nom DNS ou l'adresse IP), requis
- Une adresse de courriel, requis pour recevoir le certificat généré par l'Autorité de Certification
- Un mot-de-passe en option
- Le nom de la société en option

Dans notre exemple, nous avons généré le certificat requis pour notre serveur "ocs.domain.tld".

**Ensuite**, vous devez transmettre votre certificat requis "server.csr" à votre Autorité de Certification PKI.

**Une fois votre certificat serveur de l'Autorité de Certification reçu**, vous avez juste à copier le fichier "server.crt" de certificat serveur dans le répertoire "INSTALL\_PATH\xampp\apache\conf\ssl.crt" et le fichier de la clé privée du serveur "server.key" dans le répertoire "INSTALL\_PATH\xampp\apache\conf\ssl.key".

Vous devriez aussi recevoir le certificat racine de l'Autorité de Certification dans le fichier "ca\_root.crt" pour le spécifier dans la configuration Apache. Enregistrez ce fichier dans le répertoire "INSTALL\_PATH\xampp\apache\conf\ssl.crt" et nommez-le "ca-bundle.crt".

**Mettez-à-jour la configuration Apache et mod\_ssl** en éditant le fichier "INSTALL\_PATH\xampp\apache\conf\extra\httpd-ssl.conf" en décommentant la ligne 132 (supprimez le caractère '#' en début de ligne) comme suit :

#### Exemple de fichier de configuration Apache/mod\_ssl

```
# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
# Note: Inside SSLCertificatePath you need hash symlinks
#       to point to the certificate files. Use the provided
#       Makefile to update the hash symlinks after changes.
#SSLCertificatePath conf/ssl.crt
SSLCertificateFile conf/ssl.crt/ca-bundle.crt
```

Une fois votre serveur web Apache configuré, n'oubliez pas de redémarrer les services d'Apache2 pour que les changements prennent effets.

**Pour finir**, vous devez installer le fichier de certificat racine de l'Autorité de Certification "ca\_root.crt" sur chaque ordinateur client dans le répertoire d'installation de l'agent OCS Inventory NG, sous le nom "cacert.pem".

### **Exemple : Déployer de nouvelle version de l'Agent de Service Windows**

Créez une archive ZIP "OcsAgentSetup.zip" incluant le fichier "OcsAgentSetup.exe".

En suivant, connectez-vous à la console d'Administration et allez au menu "Téléploiement" > "Création".

- **Renseignez le nom du paquet**, par exemple "OCS Agent Service 4031",
- **Sélectionnez le système d'exploitation cible** "Windows",
- **Sélectionnez le protocole** "HTTP",
- **Sélectionnez la priorité** "5",
- **Parcourez le système de fichier pour sélectionner l'archive Zip**,
- **Sélectionnez l'action** "Lancer",
- **et renseignez le nom du fichier** avec les paramètres de ligne de commande d'installation de l'agent de service, par exemple "OcsAgentSetup.exe /S /NOSPLASH /UPGRADE /NP /DEBUG /SERVER:my\_ocs\_server.domain.tld" (/S pour lancer l'installateur en mode silencieux,

/NOSPLASH pour désactiver l'écran d'accueil de l'installateur, /UPGRADE pour indiquer que vous mettez-à-jour l'agent de service déjà installé, /NP pour désactiver l'usage des paramètres du proxy d'Internet Explorer, /DEBUG pour permettre la création des fichiers logs, /SERVER pour indiquer à l'agent de se connecter au serveur "my\_ocs\_server.domain.tld").

N.B. : Ne pas oublier le paramètre /UPGRADE pour permettre de mettre-à-jour un agent de service OCS Inventory NG déjà existant.

Puis, validez en cliquant sur le bouton [ Envoyer ].

En suivant, choisissez la taille des fragments de fichiers, par exemple 500 Kb, et cliquez sur le bouton [ Envoyer ].

Maintenant, le déploiement de paquet est créé. Vous pouvez l'activer.

Allez au menu "Téléploiement" > "Activation".

Cliquez sur le lien "Activer" sur la ligne correspondante.

- Renseignez l'url HTTPS où le fichier de métadonnées INFO peut être téléchargé par les agents utilisant HTTPS,
- Renseignez l'url HTTP où les fragments de fichier peuvent être téléchargés par l'agent utilisant HTTP.

Et, cliquez sur le bouton [ Envoyer ].

Maintenant, le paquet est prêt à être affecté aux ordinateurs.

Allez au menu "Recherche multicritères", recherchez les ordinateurs ayant le système d'exploitation "WINDOWS (tous)" puis cliquez sur le bouton [ Recherche ].

Maintenant, cliquez sur le lien "Télédéployer" dans la ligne "Traitement par lots".

Pour finir, cliquez sur le lien "Affecter" sur la ligne correspondante au paquet que vous désirez affecter.

# PARAMETRAGE DU SERVEUR

## *Gérer le paramétrage du serveur*

Le Serveur de Gestion d'OCS Inventory NG a besoin de paramétrage pour supporter la charge d'un grand nombre d'ordinateurs inventoriés. Les performances sont juste limitées par la configuration matérielle (spécifiquement la capacité en RAM, le processeur n'étant pas très sollicité) de l'ordinateur hébergeant les 3 composants principaux :

- le serveur de base de données MySQL,
- le serveur de Communication,
- le serveur d'Administration,
- le serveur de Déploiement.

Par exemple, notre serveur de production gère plus de 70 000 clients. Pour cela, nous avons 3 serveurs fonctionnant sous Debian GNU/Linux "Sarge", un pour le serveur de base de donnée et le serveur de communication, un autre pour la console d'Administration et la réplication du serveur de base de données (nous avons choisi de répliquer la base de données sur le serveur d'Administration pour permettre à la console d'administration les requêtes SQL utilisant le CPU et les connections à la base de données MySQL utilisées par le serveur de Communication) et le dernier pour le serveur de déploiement. La configuration matérielle pour les serveurs est la suivante :

- 1 Intel Pentium Xeon 2,8 Ghz,
- 3 Go RAM.

À cause de la disponibilité de la RAM, nous avons choisi de limiter le nombre de connections HTTP simultanées aux serveurs de communication et d'administration à 400.

**Vous devez garder à l'œil les journaux du serveur web Apache du serveur de communication pour détecter tout problème. Aussi, vérifiez le journal du serveur de communication dans le répertoire "/var/log/ocsinventory-NG".**

Si vous voulez augmenter le nombre de connexions simultanées, vous devez modifier la directive "MaxClients" dans le fichier de configuration d'Apache, habituellement "/etc/httpd/conf/httpd.conf".

**Référez-vous au manuel de paramétrage d'Apache sur le site web d'Apache (<http://httpd.apache.org/>) pour plus d'informations.**

Ensuite, le serveur de base de données MySQL est limité par défaut à 100 connexions simultanées. Ainsi, si le serveur de communication a à gérer plus que les 100 requêtes simultanées pour l'inventaire, il ne sera pas capable de répondre à toutes. Vous devez modifier la variable MySQL "max\_connections" pour le service mysql.

Ceci fait partie des exemples de recommandations trouvées sur le site web de MySQL, à utiliser avec un serveur ayant différentes capacités de mémoire physique.

Paramètres	800 Mo	1,7 Go	2,4 Go
Table_cache	64M	64M	64M
Key_buffer	128M	256M	256M
Sort_buffer_size	2M	2M	2M
Read_buffer_size	2M	2M	2M
Read_rnd_buffer_size	4M	4M	4M
Myisam_sort_buffer_size	64M	64M	64M
Query_cache_size	128M	128M	128M
InnoDB_buffer_pool_size	384M	1024M	1700M
InnoDB_additional_mem_pool_size	20M	20M	20M
InnoDB_log_buffer_size	8M	8M	8M

Référez-vous au manuel de paramétrage MySQL sur le site web MySQL (<http://dev.mysql.com/tech-resources/articles/>) pour plus d'informations.

# SAUVEGARDE RESTAURATION B.D.D.

## *Sauvegarder et Restaurer la base de données d'OCS Inventory NG*

Vous pouvez utiliser des outils tels que phpMyAdmin ou MySQL Administrateur pour sauvegarder ou restaurer les bases de données MySQL.

Toutefois, le serveur MySQL fournit en standard des outils utilisables en ligne de commande.

### **Sauvegarder la base de données d'OCS Inventory NG**

L'outil "mysqldump" vous permet de verser tout le contenu de la base de données dans un simple fichier. Cet outil est disponible dans le répertoire "INSTALL\_PATH\xampp\mysql\bin" où INSTALL\_PATH est le répertoire d'installation que vous avez choisi pour le serveur OCS Inventory NG pour Windows, et peut généralement être appelé directement sous Linux.

Faites fonctionner tout simplement la commande suivante pour sauvegarder la base de donnée d'OCS Inventory NG :

- `Mysqldump --add-drop-table --complete-insert --extended-insert --quote-names --host=localhost -user="root" --password="root password" ocsweb > mysqldump_ocsweb.sql`

Ceci sauvera le contenu de la base de donnée OCS Inventory NG nommée "ocsweb" dans le fichier "mysqldump\_ocsweb.sql".

### **Restaurer la base de données d'OCS Inventory NG**

L'outil "mysql" vous permet de lancer des requêtes SQL sur la base de données. Cet outil est disponible dans le répertoire "INSTALL\_PATH\xampp\mysql\bin" où INSTALL\_PATH est le répertoire d'installation que vous avez choisi pour le serveur OCS Inventory NG pour Windows, et peut généralement être appelé directement sous Linux.

Faites juste fonctionner l'interpréteur MySQL en ligne de commande pour importer le fichier précédemment créé correspondant à la base de donnée "ocsweb".

- `Mysql -u root -p ocsweb`
- Source "chemin vers le fichier"
- `exit`

N.B. : Il vous sera demandé le mot-de-passe administrateur. Si vous n'avez pas paramétré le mot-de-passe administrateur, vous pouvez simplement utiliser l'argument '-p'.

# ERREURS FREQUENTES

## Contenu

- [1 Erreurs fréquentes](#)
  - [1.1 Problèmes d'exécution de l'agent](#)
    - [1.1.1 Le lanceur OcsLogon.exe sous Windows ne télécharge pas l'agent](#)
    - [1.1.2 L'agent Windows n'envoie pas l'inventaire au serveur](#)
    - [1.1.3 L'agent Linux n'envoie pas l'inventaire au serveur](#)
    - [1.1.4 Erreurs HTTP de l'agent](#)
  - [1.2 Erreurs dans la console d'Administration](#)
    - [1.2.1 Erreur MySQL Max allowed packet](#)
    - [1.2.2 Le client MySQL ne supporte pas le protocole d'authentification](#)
    - [1.2.3 Requête PHP content-length](#)
    - [1.2.4 Taille du téléversement pour le déploiement des paquets](#)
      - [1.2.4.1 upload\\_max\\_size et post\\_max\\_size](#)
      - [1.2.4.2 memory\\_limit](#)
      - [1.2.4.3 max\\_execution\\_time et max\\_input\\_time](#)
      - [1.2.4.4 Commentaires additionnels](#)
  - [1.3 Erreurs du serveur de Communication](#)
    - [1.3.1 Je vois "Unknown directive PerlRequire..." dans les fichiers log d'Apache](#)
    - [1.3.2 Je vois "Can't locate \[Perl module name\], cannot resolve handler Ocsinventory.pm..." dans les fichiers log d'Apache](#)
    - [1.3.3 Je vois "Cannot open log file: ..." dans les fichiers log d'Apache. Le serveur de Communication ne peut pas écrire ses fichiers log](#)
  - [1.4 Permissions des fichiers et répertoires sous Linux](#)
  - [1.5 Obtenir l'aide dans les forums](#)

## Erreurs fréquentes

### Problèmes d'exécution de l'agent

#### Le lanceur OcsLogon.exe sous Windows ne télécharge pas l'agent

**Quand je lance l'agent OcsLogon.exe, les fichiers d'installation de l'agent ne sont pas téléchargés.**

Le lanceur "OcsLogon.exe" doit être renommé avec l'adresse IP du serveur de communication ou son nom DNS (ex: 192.168.1.12.exe ou ocs\_com.domain.tld.exe). Si cela est déjà fait, vous avez peut-être configuré l'usage du proxy dans Internet Explorer et OCS l'utilise dans sa configuration. Essayez de désactiver l'usage du proxy en lançant OcsLogon avec l'argument de commande '/NP'. Dans tous les cas, lancez OcsLogon with l'argument "/DEBUG" puis lisez les fichiers journaux "C:\ocs-ng\ocslogon.log" et "C:\ocs-ng\computer\_name.log".

Ce qui suit est un exemple typique de contenu du fichier OcsLogon.bat faisant part d'un problème de lancement :

```
OCS server port number : Default (80)
Install folder : C:\Ocs-ng
OCSserver is set to: a.b.c.d
Internal Ocslogon version: 4.0.1.4
Testing: C:\ocs-ng\BIOSINFO.EXE
Ocs Inventory NG () was not previously installed.
Start deploying OCS
http://a.b.c.d/ocsinventory/deploy/ocsagent.exe : HTTP/1.1 500 Internal
Server Error
http://a.b.c.d/ocsinventory/deploy/label : HTTP/1.1 500 Internal Server
Error
End Deploying
Testing ocsagent.exe version:0000
Proxy use.
Launching : C:\ocs-ng\OCSInventory.exe /debug /server:a.b.c.d
Cmdline option is :\\server_share\a.b.c.d.exe /debug
```

Tel que vous le lisez, le lanceur utilise les paramètres de proxy d'IE, ce qui est la raison de l'erreur "HTTP/1.1 500 Internal Server Error" quand est téléchargé le fichier "ocsagent.exe". Cela signifie que le lanceur n'est pas capable de télécharger le fichier d'installation de l'agent. Ainsi, essayez de désactiver l'usage du proxy en ajoutant "/NP" lors du lancement de l'agent, et ensuite lisez les chapitres intitulés § [Erreurs HTTP de l'agent](#) et ensuite § [Erreurs du serveur de communication](#).

N.B. : L'erreur "label" n'est pas blocante. Cela signifie que vous n'utilisez pas le TAG.

## L'agent Windows n'envoie pas l'inventaire au serveur

**J'ai installé le serveur OCS Inventory NG tel que dit le manuel, mais quand je lance l'agent, rien n'apparaît dans la console d'administration.**

Sur les ordinateurs clients Windows, lancez "INSTALL\_FOLDER\ocsinventory.exe /server:communication\_server\_ip /debug". Un fichier journal "computer\_name.log" est créé dans le répertoire "C:\ocs-ng", qui vous aidera à trouver le problème. Généralement, vous verrez quelque chose comme "...is not a well configured ocs server" et une erreur HTTP (voir le chapitre § [Erreurs HTTP de l'agent](#)).

Ce qui suit est le contenu typique du fichier "computer\_name.log" d'un agent en erreur :

```
OCS INVENTORY ver. 4014 Starting session for Device <COMPUTER_NAME>
on Friday, February 24, 2006 15:34:27...
Command line parameters: </np /debug /server:a.b.c.d>
WMI Connect: Trying to connect to WMI namespace root\cimv2 on device
<Localhost>...OK.
Registry Connect: Trying to connect to HKEY_LOCAL_MACHINE on device
<Localhost>...OK.
SetupAPI Connect: Trying to connect to SetupAPI on device
<Localhost>...OK.
CHECKINGS: No ocsinventory.dat file found !
IpHlpAPI GetNetworkAdapters...
IpHlpAPI GetNetworkAdapters: Calling GetIfTable to determine network
adapter properties...OK
IpHlpAPI GetNetworkAdapters: Calling GetAdapterInfo to determine IP
Infos...OK
IpHlpAPI GetNetworkAdapters: OK (1 objects).
DID_CHECK: Mac changed new:<00:40:63:D8:BC:61> old:<>, hname changed
new:<COMPUTER_NAME> old:<>
Generating Unique ID for device <COMPUTER_NAME>...OK (COMPUTER_NAME-2006-
02-24-15-34-27)
```

```

CHECKINGS:          write          <COMPUTER_NAME-2006-02-24-15-34-27>          and
<00:40:63:D8:BC:61>
in ocsinventory.dat
HTTP SERVER: Connection WITHOUT proxy
HTTP SERVER: Creating CInternetSession to get inventory parameters...OK.
HTTP SERVER: Connecting to server a.b.c.d 80...OK.
HTTP SERVER: Sending prolog query...
HTTP SERVER: The server <a.b.c.d> is not a well configured OCS server
HTTP ERROR:
<...>
<h1>Server error!</h1>
<p>The server encountered an internal error and was unable to complete
your request.
Either the server is overloaded or there was an error in a CGI script.
</p>
<p>If you think this is a server error,          please contact the <a
href="mailto:admin@localhost">webmaster</a>.
</p>
<h2>Error 500</h2>
<address>
<a href="/">a.b.c.d</a><br />
<span>24.02.2006 15:40:10<br />
Apache/2.2.0          (Win32)          DAV/2          mod_ssl/2.2.0          OpenSSL/0.9.8a
mod_autoindex_color PHP/5.1.1 mod_perl/2.0.2 Perl/v5.8.7
</span>
</address>
HTTP SERVER: Closing HTTP connection
WMI Disconnect: Disconnected from WMI namespace.
SetupAPI Disconnect: Disconnected from SetupAPI.
Execution duration: 00:00:00.

```

Tel que vous pouvez le lire, l'agent n'utilise pas les paramètres du proxy d'IE ("HTTP SERVER: Connection WITHOUT proxy"), et il y a l'erreur "HTTP SERVER: The server is not a well configured OCS server" suivi de "Error 500". Veuillez lire les chapitres intitulés § [Erreurs HTTP de l'agent](#) et ensuite § [Erreurs du serveur de communication](#).

## L'agent Linux n'envoie pas l'inventaire au serveur

**J'ai installé le serveur OCS Inventory NG tel que dit dans le manuel, mais quand je lance l'agent Linux, rien n'apparaît dans la console d'Administration.**

Sur les ordinateurs clients Linux, vous pouvez utiliser "ocsinv -debug" ou "ocsinv -info" pour obtenir un suivi.

Généralement, vous verrez quelque chose comme "...is not a well configured ocs server" et une erreur HTTP. Veuillez lire les chapitres intitulés § [Erreurs HTTP de l'agent](#) et ensuite § [Erreurs du serveur de communication](#).

## Erreurs HTTP de l'agent

**Je vois dans les journaux de l'agent des erreurs HTTP. Qu'est-ce que cela signifie ?**

- **500:** le serveur rencontre un problème interne. Regardez les fichiers journaux d'Apache, spécialement le fichier "error.log", généralement localisé sous "/var/log/httpd".
- **404:** l'url "/ocsinventory" ne peut être trouvé sur le serveur. Vous avez fait une erreur dans la configuration d'Apache. Avez-vous inclu le contenu de configuration Apache dans le fichier de configuration d'Apache ? Avez-vous mis-à-jour ce contenu selon vos besoins ?
- **301:** Cette erreur signifie que vous avez toujours un répertoire nommé "/ocsinventory" dans votre serveur Apache, et que ce nom est en conflit avec la directive <location> du fichier de configuration apache. Vous devez changer le nom du répertoire "/ocsinventory".

Dans tous les cas, vous devriez lire les journaux du serveur de communication et vérifier le chapitre intitulé § [Erreurs du serveur de communication](#).

## Erreurs dans la console d'Administration

### Erreur MySQL Max\_allowed\_packet

Si vous rencontrez un message d'erreur avec l'erreur MySQL "max\_allowed\_packet", vous devez modifier la configuration de MySQL en augmentant la taille maximale de paquet acceptée par MySQL. Nous recommandons de paramétrer cette valeur à 4 Mo.

Ouvrez le fichier "my.cnf" (habituellement disponible dans le répertoire "/etc" sous Linux, et dans "C:\OCSinventoryNG\xampp\mysql\bin" sous Windows) et ajoutez la ligne "max\_allowed\_packet=4M" dans les sections "[mysqld]", "[mysql.server]" ou "[safe\_mysqld]".

#### Exemple de fichier de configuration MySQL my.cnf

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
max_allowed_packet=4M

[mysql.server]
user=mysql
basedir=/var/lib
max_allowed_packet=4M

[safe_mysqld]
err-log=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
max_allowed_packet=4M
```

Alors, redémarrez le serveur MySQL :

- /etc/rc.d/init.d/mysql restart

## Le client MySQL ne supporte pas le protocole d'authentification

Si vous rencontrez un message d'erreur avec une erreur MySQL "Client does not support authentication protocol requested by server; consider upgrading MySQL client", vous devez activer le support de l'ancienne méthode d'enregistrement pour les mots-de-passe dans votre configuration de MySQL.

Il y a deux façons de faire cela :

1. Ajoutez la directive "old-password" dans le fichier "my.cnf"

#### Exemple de fichier de configuration MySQL my.cnf

```
# The MySQL server
[mysqld]
old-passwords
port          = 3306
socket        = mysql
```

1. Ajoutez l'argument "--old-password" en ligne de commande lors du lancement du serveur MySQL.

Puis, redémarrez le serveur MySQL :

- `/etc/rc.d/init.d/mysql restart`

Maintenant, vous devez mettre-à-jour le mot-de-passe 'root' par les arguments de commandes suivants :

- Connectez-vous à la base de données MySQL en tant que root pour mettre-à-jour son mot-de-passe : `“mysql -u root -p mysql”`
- Ensuite, faites la modification suivante : `“update user set password=OLD_PASSWORD('root_password') where user='root';”`
- Une fois fait, sortez de l'interpréteur de commande MySQL par la commande 'exit'.

### Exemple de modification du mot-de-passe root

```
[root@linux root]# mysql -u root -p mysql
Enter password:
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 19 to server version: 4.1.7-standard

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

mysql> update user set password=OLD_PASSWORD('admin123') where user='root';
Query OK, 1 row affected (0.00 sec)
Rows matched: 1 Changed: 1 Warnings: 0

mysql> exit
Bye
[root@linux root]#
```

## Requête PHP content-length

Si vous lisez dans le fichier journal d'erreur d'Apache un message tel que le suivant :

```
[Mon Sep 05 18:30:03 2005] [error] [client XXX.XXX.XXX.XXX] Requested content-length
of 831148 is larger than the configured limit of 524288, referer:
http://administration_server/ocsreports/?multi=8
```

Cela est dû à la directive Apache “LimitRequestBody” qui est utilisée pour limiter la taille des requêtes HTTP.

Pour fixer cela, ouvrez le fichier de configuration Apache "httpd.conf", habituellement dans le répertoire "/etc/httpd/conf" (dans certaines distributions, la configuration d'Apache pour PHP peut résider ailleurs, tel que dans un répertoire “/etc/httpd/conf.d”).

Cherchez la directive "LimitRequestBody" et assurez-vous que la taille soit au moins de 4 Mo (4194304) et non par défaut de 512 Ko (524288).

### Exemple de configuration Apache pour PHP

```
#
# PHP is an HTML-embedded scripting language which attempts to make it
# easy for developers to write dynamically generated webpages.
#
LoadModule php4_module modules/libphp4.so
#
# Cause the PHP interpreter handle files with a .php extension.
#
<Files *.php>
    SetOutputFilter PHP
```

```
SetInputFilter PHP
LimitRequestBody 4194304
</Files>
```

Modifiez cette valeur si besoin et redémarrez le service Apache.

- `/etc/rc.d/init.d/httpd restart`

## Taille du téléversement pour le déploiement des paquets

Tous les paramètres de configuration pour votre installation sont contenus dans le fichier "php.ini" ou les fichiers de configuration d'Apache. Quelques fois ces paramètres peuvent être outre-passés par des directives dans les fichiers .htaccess ou lorsque des scripts les comportent eux-mêmes. Toutefois vous ne pouvez outre-passer ces paramètres qui affectent le téléversement de fichiers avec des directives .htaccess. Vous devriez juste les concentrer dans le fichier ini.

Vous pouvez appeler la fonction `phpinfo()` pour trouver la location de votre fichier "php.ini", et les valeurs courantes pour les paramètres définis que nous aurions besoin de modifier :

- `file_uploads`
- `upload_max_filesize`
- `max_input_time`
- `memory_limit`
- `max_execution_time`
- `post_max_size`

La première fois, il est clairement évident que cela est inactif, que le téléversement est désactivé, ainsi vous ne serez pas capable de téléverser des logiciels pour le déploiement. Nous verrons les autres paramètres de configuration en détail, ci-dessous.

N'oubliez pas de redémarrer le serveur web Apache pour que les changements prennent effets.

***upload\_max\_size et post\_max\_size***

***memory\_limit***

***max\_execution\_time et max\_input\_time***

***Commentaires additionnels***