CARMI TERTIAIRE
Centre Académique de Ressources et Maintenance Informatique Tertiaire
Lycée Emmanuel Mounier
6 avenue Marcelin Berthelot – 38029 GRENOBLE CEDEX 2
✆ 04 76 86 58 15 carmit@ac-grenoble.fr
site collaboratif : http://carmit.ac-grenoble.fr

INSTALLATION D'UN SERVEUR OVIDENTIA EN DMZ

Le serveur Ovidentia doit être déployé installé sur une machine Windows 2003 Server située dans la DMZ gérée par un SLIS 4.
L'objectif du paramétrage présenté dans la suite de cette documentation consiste à autoriser les accès indispensables vers et depuis ce serveur Ovidentia.
Cette documentation ne prend pas en charge un serveur Cegid en DMZ.

Principaux paramétrages:
1. Accès au serveur Ovidentia en DMZ :

➢ depuis internet, à l'aide

- du protocole https,
- d'une connexion ODBC,

➢ depuis le réseau local, à l'aide :

- d'une connexion Bureau à distance,
- du protocole https,
- d'une connexion ODBC.

Le protocole https est utilisé sur le réseau local pour des raisons de sécurité. *En effet, les paramètres de connexion à Ovidentia (nom et mot de passe) proviennent d'Active Directory (synchronisation) et doivent être chiffrés car ils sont identiques à ceux utilisés pour l'ouverture de session Windows.*

2. Accès du serveur Ovidentia vers le réseau local et internet :

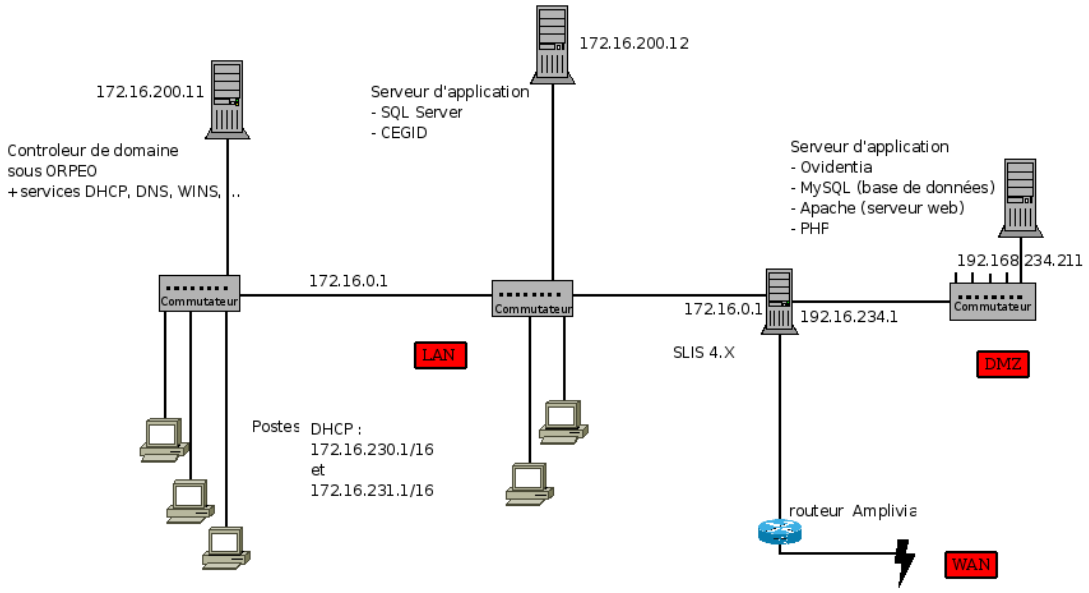
➢ autorisation d'accès à l'annuaire AD d'ORPÉO.

➢ autorisation d'accès au partage Windows sur le serveur NAS.

➢ autorisation d'accès aux serveurs de courrier suivant les protocoles POP ou IMAP.

1. Déplacement du serveur Ovidentia

La machine hébergeant le serveur Ovidentia doit être branchée à un commutateur situé en DMZ (derrière la 3ème carte réseau du SLIS 4).



Architecture matérielle d'un réseau tertiaire

Pour un serveur OVIDENTIA existant situé sur le réseau local tertiaire, il est conseillé de modifier le paramétrage de la carte réseau avant son déplacement :

➢ ouvrir une session sur le serveur Ovidentia en administrateur,

➢ Panneau de configuration, Réseau, Configuration, TCP/IP, Propriétés,

- Adresse IP : 192.168.234.211,
- Passerelle : 192.168.234.1,
- Serveur DNS préféré : 192.168.234.1.

➢ Panneau de configuration, Options Internet, Connexions, Paramètres réseau,

- cocher "Utiliser un serveur proxy pour votre réseau local",
- Adresse : 192.168.234.1,
- Port : 3128,
- cocher "Ne pas utiliser de serveur proxy pour les adresses locales".

2. Installation du serveur Ovidentia

2.1. Cas d'un serveur existant

La procédure d'installation suivante a pour objectif la modification du paramétrage du serveur Ovidentia pour permettre l'accès au serveur Ovidentia déplacé dans la DMZ.

L'installation s'effectue à partir du fichier Ovidentia_DMZ.exe à télécharger sur le site du CARMI Tertiaire
http://carmit.ac-grenoble.fr/index.php?tg=fileman&id=72&gr=Y&path=CtOvidentia%2FCtOvidTelecharg&idf=2564&file=Ovidentia_DMZ.exe&sAction=getFile

➢ Ouvrir une session sur le serveur Ovidentia en Administrateur[1].

➢ Télécharger le fichier Ovidentia_DMZ.exe.

➢ Exécuter le fichier autodécompressible.

➢ Exécuter le fichier C:_Ovidentia\dmz.bat.

➢ Saisir les différentes informations requises par le script :

- disque des données,
- identifiant et mot de passe de l'administrateur de la base de données MySQL de l'application Ovidentia,
- nom du SLIS,
- adresse IP (192.168.234.1) et port (3128) du serveur proxy (SLIS) à l'intérieur de la DMZ,
- adresse IP (192.168.234.6) et port (25) du serveur de courrier sortant SMTP (LCS) à l'intérieur de la DMZ,
- adresse du compte de messagerie du coordonnateur tertiaire (compte l3 ou s3).

Le script sauvegardera les fichiers de configuration httpd.conf, php.ini ainsi et config.php. Il importera le nouveau modèle des fichiers de configuration httpd.conf et php.ini qu'il adaptera à la configuration du site. Il modifiera également le fichier config.php (modification du paramètre $babUrl pour tenir compte de la nouvelle adresse du serveur Ovidentia). Le serveur Apache2.2 sera arrêté puis relancé avec les nouveaux paramètres de configuration.

L'accès au serveur Ovidentia ne s'effectuera plus que suivant le protocole https : la nouvelle adresse à utiliser est affichée : elle est à communiquer à l'ensemble des utilisateurs d'Ovidentia.

2.2. Cas d'un serveur nouveau

L'installation s'effectue à partir de la version 7.3.1 à télécharger sur le site du CARMI Tertiaire
http://carmit.ac-grenoble.fr/index.php?tg=articles&topics=227

➢ Ouvrir une session sur le serveur Ovidentia en administrateur,

➢ télécharger sur le site http://carmit.ac-grenoble.fr la dernière version d'Ovidentia,

➢ exécuter le fichier téléchargé et accepter la décompression de l'archive à la racine du disque C:,

➢ menu Démarrer, Exécuter, saisir la commande "C:_Ovidentia\OTCterInstall.bat",

➢ accepter l'installation d'un serveur A-M-P (réponse : O),

➢ saisir la lettre correspondant au choix du disque des données et valider,
si le disque des données est le disque système, un message de mise en garde apparaît. Confirmer par le choix précédemment effectué et valider,

➢ valider les différents messages,

➢ choisir 1 pour la copie des raccourcis de l'administrateur des serveurs Apache 2.2 et MySQL,

➢ saisir les différentes informations requises par le script :

- nom du SLIS,
- adresse IP (192.168.234.1) et port (3128) du serveur proxy (SLIS) à l'intérieur de la DMZ,
- adresse IP (192.168.234.6) et port (25) du serveur de courrier sortant SMTP (LCS) à l'intérieur de la DMZ,
- adresse du compte de messagerie du coordonnateur tertiaire (compte l3 ou s3),
- nom de l'établissement.

➢ la procédure d'installation se termine.

Pour plus d'informations, se reporter à la procédure d'installation décrite sur le site du CARMI Tertiaire :

http://carmit.ac-grenoble.fr/index.php?tg=fileman&sAction=getFile&inl=1&id=72&gr=Y&path=CtOvidentia%2FCtOvidTelecharg&file=OTCterOO.exe&idf=2256

[1] Ne pas arrêter les services Apache2.2 et MySQL.

3. Paramétrage du SLIS

Chaque paragraphe inclut un item "Vérification du fonctionnement" afin de bien comprendre l'objectif de chaque paramétrage.

Il est nécessaire de paramétrer le SLIS pour autoriser certaines communications avec le serveur Ovidentia en DMZ.
Se connecter à l'interface d'administration de SLIS4 via un navigateur depuis une machine quelconque (réseau local, internet) à partir de l'URL : https://172.16.0.1:1098.

3.1. Configuration du "proxy reverse"

Le serveur Ovidentia sera désormais considéré comme un sous domaine virtuel du SLIS.
Pour cela, il est nécessaire au préalable de déclarer une entrée dans le DNS.
➢ Menu Réseau, DNS, Entrées DNS, Ajouter une entrée

- Adresse IP : saisir l'adresse du SLIS à l'intérieur du réseau local "172.16.0.1"
- Nom : saisir "ovidentia"
- Commentaire : saisir "Serveur Ovidentia"
- Zone à laquelle ajouter l'enregistrement DNS : cocher "<nom du SLIS>"
- Valider

Le proxy reverse peut ensuite être mis en place.
➢ Menu Réseau, Proxy inverse, Ajouter une redirection

- Description : Serveur Ovidentia
- Source des requêtes : sélectionner "Toutes les sources"
- Requêtes sortantes : cocher "Utiliser la redirection par hôte virtuel"
- Nom de l'hôte virtuel : saisir "ovidentia"
- Cible de la redirection (Url distante) : saisir "http://192.168.234.211/"
- Options SSL (Comportement SSL) : sélectionner "Forcer l'utilisation du protocole http sécurisé"
- Valider

Vérification du fonctionnement
➢ À partir d'une machine située à l'intérieur ou à l'extérieur du réseau local, saisir l'adresse : https://ovidentia.<nom du SLIS>
La page d'accueil publique du site s'affiche (ne pas chercher à ce niveau de s'authentifier sur le site).

3.2. Paramétrage du pare-feu

3.2.1. Déclaration du serveur Ovidentia en DMZ

➢ Menu Sécurité, Pare-feu, Pare-feu.

➢ Administration de la DMZ, cliquer sur "vue d'ensemble".

➢ Déclarer une nouvelle machine sur la DMZ.

➢ Saisir "Serveur OVIDENTIA" et son adresse IP "192.168.234.211"
la machine se trouve dans la liste des hôtes.

a) Autorisation d'utilisation du bureau à distance depuis le réseau local

Le local technique est parfois exigu et l'accès direct au serveur Ovidentia est parfois difficile. L'utilisation du bureau à distance est donc nécessaire pour réaliser la maintenance du serveur (mise à jour, gestion des sauvegardes…).

Mise en place de la règle du pare-feu
➢ Menu Sécurité, pare-feu, pare-feu,

➢ Administration de la DMZ, cliquer sur "vue d'ensemble",

➢ pour la machine "Serveur OVIDENTIA", cliquer sur l'icône modifier,

➢ **Services proposés par l'hôte, créer une règle :**

- donner une description courte : "RL bureau distant",
- autoriser la source depuis le réseau local : 0.0.0.0/0,
- choisir le(s) port(s) source(s) Le(s) port(s) source(s) : all,
- choisir le protocole : tcp,
- choisir le port d'écoute : Le port d'écoute : 3389,
- Adresse et port 'natté' : Voulez-vous 'natter' l'adresse et le port depuis le SLIS ? cocher "Yes",
- Saisir le port d'écoute pour le slis : 3390, Valider.

***Lorsque le SLIS reçoit une requête** à destination de cette adresse (IP ou nom du SLIS) associée à ce port (3390), il transmet le flux vers l'adresse du serveur Ovidentia dont le port d'écoute est 3389.*

Autorisation du bureau à distance sur le serveur Ovidentia
➢ clic droit Propriétés sur Poste de travail,

➢ onglet Utilisation à distance, cocher "Autoriser les utilisateurs à se connecter à distance à cet ordinateur", Ok (le compte Administrateur local de la machine est automatiquement autorisé).

Vérification du fonctionnement
➢ À partir d'une machine du réseau local, lancer une connexion bureau à distance.

➢ Saisir : 172.16.0.1:3390 ou <nom du SLIS>:3390,
Nom d'utilisateur : "administrateur", saisir le mot de passe.

b) Autorisation d'une connexion ODBC depuis le réseau local

Cette règle permet d'accéder depuis le réseau local à des bases de données via le serveur MySql.
Mise en place de la règle du pare-feu
➢ Menu Sécurité, Pare-feu, Pare-feu,

➢ Administration de la DMZ, cliquer sur "vue d'ensemble",

➢ pour la machine "Serveur OVIDENTIA", cliquer sur l'icône "modifier",

➢ **Services proposés par l'hôte, créer une règle :**

- donner une description courte : "RL ODBC",
- autoriser la source depuis le réseau local : 0.0.0.0/0,
- choisir le(s) port(s) source(s) Le(s) port(s) source(s) : all,
- choisir le protocole : tcp,
- choisir le port d'écoute : Le port d'écoute : 3306,
- Adresse et port 'natté' : Voulez-vous 'natter' l'adresse et le port depuis le SLIS ? cocher "Non", Valider.

***Lorsque le SLIS reçoit une requête** à destination de cette adresse (IP du serveur Ovidentia), il transmet le flux vers l'adresse du serveur Ovidentia dont le port d'écoute est 3306.*

Vérification du fonctionnement
À partir d'une machine du réseau local, configurer une connexion ODBC,
Pour cela, il est nécessaire de disposer d'un accès à une base de données sur le serveur MySql avec un compte valide (testé sous PhpMyAdmin).
Pour un exemple, voir le document "FormVirtual2010UsagesPedago.doc".
Remarque : pour le champ "Serveur", renseigner l'adresse du serveur Ovidentia (192.168.234.211)[2].

c) Autorisation d'une connexion ODBC depuis internet

Cette règle permet d'accéder depuis internet à des bases de données via le serveur MySql.
Mise en place de la règle du pare-feu
➢ Menu Sécurité, Pare-feu, Pare-feu,

[2] Il est possible également de natter et d'indiquer ici l'adresse ou le nom du SLIS.

➢ Administration de la DMZ, cliquer sur "vue d'ensemble",

➢ pour la machine "Serveur OVIDENTIA", cliquer sur l'icône "modifier",

➢ **Services proposés par l'hôte, créer une règle :**

- donner une description courte : "Web - ODBC",
- autoriser la source depuis internet : 0.0.0.0/0,
- choisir le(s) port(s) source(s) Le(s) port(s) source(s) : all,
- choisir le protocole : tcp,
- choisir le port d'écoute : Le port d'écoute : 3306,
- Adresse et port 'natté' : Voulez-vous 'natter' l'adresse et le port depuis le SLIS ? cocher "Yes",
- Saisir le port d'écoute pour le slis : 3306, Valider.

Lorsque le SLIS reçoit une requête** à destination de cette adresse (IP ou nom du SLIS) associée à ce port (3306), il transmet le flux vers l'adresse du serveur Ovidentia dont le port d'écoute est également 3306.**

Vérification du fonctionnement

➢ à partir d'une machine extérieure au lycée, configurer une connexion odbc,
Pour le champ "Serveur", renseigner l'adresse ou le nom du SLIS.

3.2.2. Accès du serveur Ovidentia vers le réseau local ou internet

a) Autorisation d'accès à l'annuaire AD d'ORPÉO

Mise en place de la règle du pare-feu

➢ Menu Sécurité, Pare-feu, Pare-feu,

➢ Administration de la DMZ, cliquer sur "vue d'ensemble",

➢ pour la machine "Serveur OVIDENTIA", cliquer sur l'icône modifier,

➢ **Droits d'accès sortants de l'hôte, créer une règle :**

- donner une description courte : "Accès AD ORPÉO",
- choisir le schéma : Consulter un annuaire ldap(s),
- autoriser l'accès sortant : vers le réseau local : 172.16.200.11,
- cible : accepter, Valider.

Vérification du fonctionnement

Afin d'accéder à l'annuaire Active Directory d'ORPÉO, il est nécessaire d'ajouter le serveur ORPÉO comme DNS secondaire dans le SLIS (cf. paragraphe suivant).

b) Autorisation d'accès aux serveurs de messagerie

Cette règle est nécessaire si la messagerie Ovidentia est utilisée.

Mise en place de la règle du pare-feu

➢ Menu Sécurité, Pare-feu, Pare-feu,

➢ Administration de la DMZ, cliquer sur "vue d'ensemble",

➢ pour la machine "Serveur OVIDENTIA", cliquer sur l'icône modifier,

➢ **Droits d'accès sortants de l'hôte, créer une règle :**

- donner une description courte : "Accès Serveurs de messagerie",
- choisir le schéma : Consultation par un client de messagerie pop(s) imap(s)
- autoriser l'accès sortant : vers internet : 0.0.0.0/0,
- cible : accepter, Valider.

c) Autorisation d'accès au partage du serveur NAS

Cette règle est nécessaire pour mettre en œuvre la planification de la sauvegarde d'Ovidentia sur un serveur NAS

Mise en place de la règle du pare-feu

- Menu Sécurité, Pare-feu, Pare-feu,
- Administration de la DMZ, cliquer sur "Vue d'ensemble",
- pour la machine "Serveur OVIDENTIA", cliquer sur l'icône modifier,
- **Droits d'accès sortants de l'hôte, créer une règle :**
- donner une description courte : "Accès à Partage serveur NAS",
- créer le schéma suivant :
  en face de "Choisissez un schéma", cliquer sur "Créer", puis compléter la nouvelle fenêtre comme indiqué ci-dessous, et terminer par "Valider".

- choisir ce schéma : "Partage Windows netbios",
- autoriser l'accès sortant : vers le réseau local : 172.16.200.15 (adresse du serveur NAS),
- cible : Toujours accepter, Valider.

Vérification du fonctionnement

- ouvrir une session en administrateur sur le serveur Ovidentia en DMZ et lancer une fenêtre DOS,
  saisir la commande suivante, qui doit créer le lecteur T sous le compte local OrpeoSauv avec son mot de passe:
  net use T: \\172.16.200.15\Partage /USER:<NomDuNas>\OrpeoSauv <MotDePasse>
- supprimer ensuite le lecteur T par la commande :
  net use T: /d

3.3. Ajout du serveur ORPÉO comme zone DNS secondaire

- Menu Réseau, DNS, Zones secondaires,
- Nom de la zone : orpeo.local,
- Serveur maître de la zone : 172.16.200.11,
- cliquer sur "Ajouter".

Configuration du serveur DNS sur le serveur ORPÉO

L'adresse IP du SLIS doit être incluse dans le transfert de zone du serveur DNS :

- Démarrer, Programmes, Outils d'administration, DNS,
- développer Zones de recherche directes, orpeo.local,
- sélectionner orpeo.local, clic droit, Propriétés,
- onglet Transfert de zone, cocher :

- "Autoriser les transferts de zone",
- "Uniquement vers les serveurs suivants",

➢ saisir l'adresse IP du SLIS, 172.16.0.1, Ajouter, Ok.

La vérification du fonctionnement est réalisée au § 4.

4. Paramétrage de la synchronisation entre l'application Ovidentia et l'Active Directory d'ORPÉO

➢ À partir d'une machine du réseau local, lancer un navigateur,

➢ saisir l'adresse : https://ovidentia**.**<Nom du SLIS> (ne pas oublier le point après ovidentia)

➢ se connecter en EtabAdmin,

➢ menu Synchronisation AD, Paramétrage, Mise en place de la synchronisation, et saisir les informations suivantes :

- Nom de l'établissement : correspond au nom d'UO de l'établissement dans l'Active Directory sur le serveur ORPÉO,
- Nom de l'hôte : correspond au nom NETBIOS du serveur ORPÉO (par ex. 1AA11111),
- Nom du domaine DNS : orpeo,
- Suffixe DNS : local,
- Port : 389,
- Nom de l'administrateur : ldapreader,
- Mot de passe associé : ******** (P@ssw0rd),
- Méthode d'authentification, choisir "Active Directory d'ORPÉO",
- Cliquer sur le bouton "Valider".

Vérification du fonctionnement

➢ Le message suivant doit apparaître : "Inscription réussie du paramétrage de la synchronisation".