OPTENET DCAgent 2.01

Manuel d'utilisateur

SOMMAIRE

1. INTRODUCTION

Pour fournir un service de filtrage aux utilisateurs et aux groupes, OPTENET Server doit identifier les utilisateurs de votre réseau. OPTENET Server peut identifier les utilisateurs des manières suivantes:

1- De manière transparente.
2- Grâce à votre produit partenaire d'intégration (OPTENET Server recueille les 'informations utilisateur' de votre produit partenaire d'intégration).
3- Manuellement (Les utilisateurs doivent s'identifier manuellement).

Ce manuel vous indiquera comment configurer OPTENET Server et OPTENET DCAgent pour travailler avec la première méthode ci-dessus. Ses points principaux sont:

1- Les utilisateurs ne devront pas se connecter via un navigateur.
2- Vous pouvez paramétrer les profils de filtrage et les groupes d'utilisateurs de votre Domaine Windows.

Les étapes pour travailler avec une 'identification transparente' sont:

1- Installation de OPTENET DCAgent.
2- Configuration de OPTENET DCAgent.
3- Configuration de OPTENET Server.

Ce manuel décrit la première et la deuxième étape ci-dessus. Les références aux instructions de configuration de OPTENET Server sont incluses dans le 'Manuel d'utilisateur de OPTENET Server'.

2. INSTALLATION

Pour installer OPTENET DCAgent, exécutez le fichier Optenet-DCAgent-2.00.XX.exe.

Pendant le processus d'installation, vous pouvez sélectionner le répertoire d'installation, le nom d'utilisateur et le mot de passe qui seront utilisés par le service OPTENET DCAgent. Ce nom d'utilisateur est celui utilisé pour interroger les domaines Windows. L'utilisateur doit être configuré au format .\UTILISATEUR ou DOMAINE\UTILISATEUR et doit être disponible sur chacun des domaines consultés par OPTENET DCAgent. En l'absence de nom d'utilisateur et de mot de passe, OPTENET DCAgent s'exécutera suivant les paramètres du compte système par défaut.

Si l'installateur introduit un nom d'utilisateur non disponible dans le domaine ou sur la machine où OPTENET DCAgent est installé, le service sera créé pour l'utilisateur par défaut (utilisateur système) et un message sera envoyé à ce dernier pour l'en informer. Il pourra à tout moment définir un nom d'utilisateur et un mot de passe à partir des propriétés du service OPTENET DCAgent.

Il n'est PAS nécessaire d'installer OPTENET DCAgent dans votre Contrôleur de Domaine Windows. Vous pouvez l'installer sur n'importe quel Serveur Windows du réseau.

OPTENET DCAgent est installé comme un service Windows qui démarrera automatiquement au redémarrage du serveur.

OPTENET DCAgent remplit trois tâches principales:
1- Répertorie les utilisateurs et les groupes appartenant à des domaines différents.
2- Fournit les groupes d'un utilisateur déterminé.
4- Obtient l'adresse IP de l'ordinateur d'un utilisateur concret.

Afin de pouvoir faire ces tâches, DCAgent interroge les contrôleurs (Primaire ou Sauvegarde).

OPTENET Server communique régulièrement avec les DCAgents qui sont configurés et demande ces informations. Ainsi, il sera capable d'identifier les utilisateurs ayant accès à Internet. Cette communication est réalisée en établissant une connexion à un port du Contrôleur de Domaine. Par défaut, ce port est 10240 même s'il peut être modifié grâce à la clé suivante dans le registre Windows.

HKEY_LOCAL_MACHINE
\SOFTWARE
\OPTENET
\OPTENET DCAgent
\2.0
\AgentPort

Si la valeur du Registre est modifiée, le service OPTENET DCAgent devra être redémarré pour que ces modifications prennent effet.

Sous certaines configurations d'Active Directory, il peut arriver que l'application ne soit pas correctement lancée au démarrage du système dans le contrôleur de domaine OPTENET DCAgent. Cette situation peut être résolue en modifiant la clé suivante dans le registre de Windows :

HKEY_LOCAL_MACHINE
\SOFTWARE
\OPTENET
\OPTENET DCAgent
\SleepOnBoot

Cette clé définit le nombre de secondes pendant lequel OPTENET DCAgent doit attendre au moment du démarrage. Par défaut, cette valeur est fixée sur ‘0’ mais il est possible d’introduire une valeur plus élevée pour que tous les services du système soient chargés avant l’ouverture d’OPTENET DCAgent, ce qui permet d’éviter des problèmes d’initialisation.

Si vous modifiez cette clé de registre, vous devez redémarrer le service OPTENET DCAgent pour que vos changements prennent effet.

3. ÉTABLISSEMENT DES PERMISSIONS

OPTENET DCAgent utilise les informations du contrôleur de domaine en lecture seule ; il ne les modifie en aucun cas.

Ainsi, si le contrôleur de domaine autorise l'accès anonyme aux données, OPTENET DCAgent peut fonctionner sous n'importe quel compte. Si seuls les utilisateurs authentifiés peuvent accéder aux informations, OPTENET DCAgent doit alors s'exécuter sous un compte d'utilisateur valide dans le contrôleur.

OPTENET vous recommande d'octroyer des privilèges d'administrateur à l'utilisateur créé pour OPTENET DCAgent. Cela est nécessaire au bon fonctionnement d'OPTENET Server et d'OPTENET DCAgent sous certaines configurations en domaines et en réseau.

Si vous installez OPTENET DCAgent sous Windows 2000 ou Windows 2003, l'utilisateur OPTENET DCAgent devra sans doute pouvoir accéder au registre.

Si vous souhaitez restreindre plus ou moins les privilèges d'OPTENET DCAgent, vous devez savoir qu'OPTENET DCAgent utilise les appels NetSessionEnum et NetUserGetGroups de l'API réseau de Windows. Le bon fonctionnement de l'appel NetSessionEnum dépend de la politique de sécurité définie au niveau du contrôleur de domaine. Pour de plus amples informations, veuillez vous reporter à http://msdn.microsoft.com/library/default.asp?url=/library/enus/netmgmt/netmgmt/netusergetgroups.asp. Le bon fonctionnement de l'appel NetUserGetGroups dépend de la politique de sécurité définie au niveau du contrôleur de domaine et de la version de ce contrôleur. Pour de plus amples informations, veuillez vous reporter à http://msdn.microsoft.com/library/default.asp?url=/library/en-us/stgmgmt/fs/netsessionenum.asp.

DCAgent peut également être installé et exécuté sous certaines configurations de Windows XP mais cela n'est pas recommandé. Le cas échéant, vous devez savoir que, si vous installez OPTENET DCAgent sous Windows XP, vous devez octroyer à l'utilisateur OPTENET DCAgent l'autorisation d'accéder à la clé de registre suivante :
HKEY_LOCAL_MACHINE\SOFTWARE\OPTENET

Pour de plus amples informations, reportez-vous aux annexes « Conditions requises par les contrôleurs de domaine Active Directory » et « Conditions requises par les serveurs et les postes de travail ».

4. LE PROCESSUS D'IDENTIFICATION DE L'UTILISATEUR

1- Détection de domaines : Au démarrage, DCAgent identifie les domaines disponibles, les contrôleurs de domaine et les contrôleurs de sauvegarde automatiquement (toutes les 24 heures par défaut). Vous pouvez paramétrer les domaines disponibles sur votre réseau manuellement et désactiver cette option. Vous pouvez également éditer l'intervalle de découverte des domaines. C'est le mode de fonctionnement par défaut (mode « all »). Toutefois, OPTENET DCAgent peut détecter uniquement les domaines considérés fiables par le domaine local * (mode « trusted ») au lieu de détecter tous les domaines du réseau (voir chapitre « Fichiers de configuration » du présent manuel).
2- Informations des utilisateurs authentifiés : DCAgent demande à chaque contrôleur de domaine primaire disponible (ou de sauvegarde s'il y a lieu) des sessions d'authentification d'utilisateur (nom d'utilisateur, nom de l'ordinateur) toutes les 20 secondes. Cet intervalle est configurable (voir ultérieurement « 4. Fichiers de configuration » dans ce manuel).
3- Nom d'utilisateur-Adresse IP : Pour chaque session d'authentification, DCAgent transforme le nom de l'ordinateur en adresse IP et enregistre cette paire dans la mémoire locale. DCAgent inscrit ces informations dans le fichier mapping.dat toutes les 10 minutes par défaut (voir '4. Fichiers de configuration' plus loin dans ce manuel pour modifier cet intervalle).
4- Envoi utilisateur: DCAgent envoie 'nom d'utilisateur-adresse IP-groupes' à OPTENET pour que ce dernier puisse identifier les demandes Internet de chaque utilisateur.
5- Envoi tous les utilisateurs: OPTENET Server doit afficher tous les utilisateurs des domaines disponibles pour que vous puissiez paramétrer les profils de filtrage via Internet. DCAgent interroge les contrôleurs et envoie ces informations à OPTENET Server.
6- Envoi tous les groupes: OPTENET Server doit afficher tous les groupes des domaines disponibles pour que vous puissiez paramétrer les profils de filtrage via Internet. DCAgent interroge les contrôleurs et envoie ces informations à OPTENET Server.
7- Envoi groupes d'utilisateurs: OPTENET Server doit connaître les groupes d'un utilisateur déterminé pour appliquer les profils de filtrage. DCAgent qui interroge les contrôleurs et envoie ces informations à OPTENET Server. Ces données sont également régulièrement inscrites dans le fichier mapping_groups.dat.

Lors de la première étape, pour que la détection automatique des domaines fonctionne correctement, le trafic NetBIOS doit être activé au niveau des routeurs et des pare-feux reliant les différents sous-réseaux ou domaines.

Les trois premières étapes sont réalisées à chaque intervalle de temps lorsque DCAgent est en marche. La première peut être désactivée. Les 4è et 7è étapes sont réalisées à chaque fois que DCAgent reçoit une demande de la part de OPTENET Server. Les 5e et 6e étapes sont réalisées à chaque fois que la définition des règles de filtrage est donnée à la touche Actualiser, aux utilisateurs ou aux groupes.

* Ce mode fonctionne uniquement sous Windows NT.

5. OBTENTION DES INFORMATIONS CONCERNANT LES DOMAINES WINDOWS

OPTENET DCAgent est capable d'obtenir les informations des contrôleurs de domaines Windows (Windows NT, Windows 2000, Windows 2003). C'est la raison pour laquelle le contrôleur de domaine peut fonctionner avec Active Directory. Dans ce cas, les informations obtenues par OPTENET DCAgent proviennent d'Active Directory à proprement parler.

OPTENET DCAgent détecte les sessions d'authentification lancées lors de son exécution. Si un utilisateur lance une session d'authentification avant le démarrage d'OPTENET DCAgent, celle-ci ne sera pas détectée. Il est recommandé de tenir compte de cette contrainte lors de l'établissement des règles de filtrage d'OPTENET Server.

Pour qu'OPTENET DCAgent obtienne correctement toutes les informations nécessaires des domaines Windows et qu'aucun problème d'autorisation ne survienne, vous devez choisir l'une des configurations suivantes :

1- Configurez les contrôleurs de domaine de telle sorte que les utilisateurs anonymes puissent effectuer des requêtes sur les utilisateurs, les groupes et les sessions. Dans ce cas, OPTENET DCAgent peut s'exécuter sous le compte système par défaut.

2- Créez vos propres comptes OPTENET DCAgent :

- Vous devez créer le même compte et le même mot de passe* dans chaque domaine.
- Activez l'option : 'Le mot de passe n'expire jamais'.
- Configurez ce compte comme compte du service OPTENET DCAgent.

Pour des raisons de sécurité, OPTENET recommande la deuxième solution.

Lorsque OPTENET DCAgent s'exécute sous un compte ne disposant pas de droits suffisants pour interroger les contrôleurs de domaine, l'un des messages suivants peut s'afficher dans l'observateur d'événements de Windows :

"CDomainController::GetUsers *DOMAIN**CONTROLLER* NetQueryDisplayInformation ERROR_ACCESS_DENIED while trying to get users"

"CDomainController::GetGroups *DOMAIN**CONTROLLER* NetQueryDisplayInformation ERROR_ACCESS_DENIED while trying to get groups"

"CDomainController::GetUserGroup *DOMAIN**CONTROLLER* NetUserGetGroups ERROR_ACCESS_DENIED while trying to get groups for *USER*"

Pour terminer, n'oubliez pas que si le DNS dans lequel l'utilisateur ouvre sa session d'authentification n'est pas correctement configuré, cet utilisateur apparaîtra comme 'utilisateur anonyme' dans le contrôleur de domaine Windows. C'est pour cette raison que les journaux d'OPTENET Server n'affichent que l'adresse IP et non le nom de l'utilisateur. Dans ce cas de figure, ni OPTENET DCAgent ni OPTENET Server n'affichent d'erreurs.
* Aucune autorisation particulière n'est exigée, ce qui signifie qu'il n'est pas nécessaire de disposer d'un compte d'administrateur.

6. FICHIERS DE CONFIGURATION

Si vous éditez l'un de ces fichiers, vous devez redémarrer le service DCAgent pour que les modifications prennent effet.

6.1. mapping.dat

Ce fichier contient une liste des 'noms d'utilisateur, adresses IP et dates' (format UTC, 1-1-1970). Ce fichier est initialement vide. Le champ heure indique la dernière fois que la saisie 'nom d'utilisateur-adresse ip' a été vérifiée. Vous pouvez éditer ce fichier.

Format du fichier :

Nom d'utilisateur+ 4bytes indiquant l'adresse IP + 4bytes indiquant l'heure

Le format du nom d'utilisateur est 'domaine\\nom d'utilisateur'. Le champ IP est sauvegardé sous forme de position non signée et l'heure est sauvegardée en secondes (Unix).

Le nom d'utilisateur doit être citée et Unicode.

6.2. Mapping_groups.dat

Ce fichier contient une liste des 'utilisateurs, groupes et heures' (format UTC, 1-1-1970). Il existe une liste de groupes pour chaque utilisateur. Ce fichier est initialement vide. Le champ heure indique la dernière fois que la saisie 'groupes-utilisateur' a été vérifiée. Vous pouvez éditer ce fichier.

Format du fichier:

GROUPS+
Groupe+index
USERS+
Nom d'utilisateur+ttl[+groupe index 1]…

6.3. config.conf

Ce fichier contient les paramètres de configuration de DCAgent. Lorsque DCAgent lit une valeur de paramètrage incorrecte au démarrage, les valeurs par défaut seront chargées.

DOMInterval: Intervalle auquel la détection auto de domaine se déclenche. Lorsque ce paramètre est désactivé, les domaines de dcenums.txt seront chargés.
MAPInterval: Intervalle auquel les saisies 'nom d'utilisateur, adresse IP, heure' sont sauvegardées sur le disque. (mapping.dat)
DCQInterval: Intervalle auquel DCAgent interroge les contrôleurs de domaine.
DOLIgnore: Permet à DCAgent d'ignorer les sessions d'authentification de la part de n'importe quel nom d'utilisateur comprenant le signe du dollar ($).
IPCLifetime: Période avant qu'une saisie non vérifiée (nom du poste de travail, adresse IP) soit supprimée.
MAPLifetime: Période avant qu'une saisie non vérifiée (nom d'utilisateur, adresse IP, heure) soit supprimée.
DOMMode : Méthode de détection des domaines. Il existe deux valeurs possibles :

« all » OPTENET DCAgent détecte tous les domaines du réseau autorisant le trafic NetBIOS.
« trusted » : Tous les domaines considérés fiables par le domaine où OPTENET DCAgent a été installé, indépendamment des autorisations concernant le trafic NetBIOS. Ce mode fonctionne uniquement sous Windows NT.

REQThreads : Nombre de fils OPTENET DCAgent répondant aux demandes d'OPTENET Server et consultant les domaines.
RESThreads : Nombre de fils OPTENET DCAgent obtenant l'adresse IP des utilisateurs par le biais du nom d'utilisateur détecté lors de chaque session d'authentification.

Le paramètre MAPLifeTime est désactivé dans cette version d'OPTENET (pas d'expiration).

Le paramètre REQThreads doit toujours avoir une valeur supérieure au nombre de contrôleurs de domaine consultés. Par ailleurs, dans les environnements possédant un grand nombre d'utilisateurs, il est recommandé d'augmenter la valeur de REQThreads et de RESThreads.

	Type	Valeur par défaut	Min	Max	Désactivée
DOMInterval	Int	86400 (24 hr)	3600sec	----	0
MAPInterval	Int	600 (10 min)	30sec	3600sec	-----
DCQInterval	Int	10 sec	5sec	90sec	-----
DOLIgnore	indicateur	1	----	----	0
IPCLifetime	Int	86400 (24 hr)	3600sec	----	0
MAPLifetime	Int	0	1800sec	----	0 *
DOMMode	string	"all"	---	----	----
REQThreads	Int	10	10	----	----
RESThreads	int	10	10	----	----

* Lorsque les saisies désactivées ne seront jamais supprimées. Autres paramètres ; Aucune mise en antémémoire lorsque désactivée.

6.4. dcenums.txt

Ce fichier contient tous les domaines disponibles et leurs contrôleurs. Ce fichier est initialement vide.

Format du fichier :

```
domainE "domainName"
        {
         dc "domainControllerName"
         {
          monitor TRUE
         }
         dc "domainControllerName"
         {
          monitor FALSE
         }
        }
```

L'indicateur du moniteur permet à DCAgent d'interroger le contrôleur. Vous pouvez éditer ce fichier de manière à pouvoir paramétrer les contrôleurs de domaine interrogés par un DCAgent. Ceci est très utile lorsque votre réseau dispose de plusieurs contrôleurs.

Si DOMInterval est activé, DCAgent interroge l'ensemble des contrôleurs trouvés lors de la recherche auto. DCAgent interroge l'ensemble des contrôleurs de ce fichier grâce à l'indicateur du moniteur réglé sur ‘TRUE', lorsque DOMInterval est désactivé.

6.5. ignore.txt

Ce fichier contient une liste d’utilisateurs ([nom d'utilisateur]) ignorés par DCAgent. Cela peut s’avérer particulièrement utile pour détecter les utilisateurs non réels comme les utilisateurs créés par le système d’exploitation ou par une application.

Lorsque OPTENET DCAgent détecte automatiquement un utilisateur de ignore.txt, il l’écarte et ne le résout pas, ne le cache pas et ne l’envoie pas à OPTENET Server.
Ces noms peuvent englober un ‘nom d’ordinateur‘ ([nom d'utilisateur][nom d’ordinateur]). Ainsi, OPTENET DCAgent ignore l’utilisateur seulement dans le cas où il se sera authentifié à partir de la machine spécifiée.

La valeur par défaut pour ce fichier est:
[LocalService]
[NetworkService]

Ces derniers sont des noms d'utilisateur internes de Windows XP.

Pour insérer des observations, commencez la ligne par le caractère '#'. (par exemple, # ceci est une observation).

[Nom d'utilisateur]
[Nom d'utilisateur] [Nom de poste de travail]
....

En cas d'absence de nom de poste de travail, le nom d'utilisateur sera ignoré pour l'ensemble des domaines.

7. ANNEXES

7.1. Conditions requises par les contrôleurs de domaine Active Directory

Sur un contrôleur de domaine avec Active Directory, l'accès en lecture aux informations sera autorisé ou refusé en fonction des ACL définies (les listes de contrôle d'accès sont spécifiées dans le répertoire).

Par défaut, les ACL autorisent la lecture des données à tous les utilisateurs authentifiés et aux membres du groupe « Accès compatible avec les versions antérieures de Windows 2000 » (« Pre-Windows 2000 compatible access »).

L'accès anonyme à la lecture des données implique que l'utilisateur 'anonyme' (Anonymous) soit explicitement ajouté au groupe « Accès compatible avec les versions antérieures de Windows 2000 ».

> **Windows 2000 :** Autorise l'accès anonyme par défaut. Si les utilisateurs 'anonymes' et 'tous' sont supprimés du groupe « Accès compatible avec les versions antérieures de Windows 2000 », seuls les utilisateurs authentifiés pourront accéder aux données.
>
> **Windows NT :** Par défaut, l'accès anonyme permet la lecture des données.

7.2. Conditions requises par les serveurs et les postes de travail

Par défaut, tous les utilisateurs authentifiés peuvent lire les données.

> **Windows Server 2003 et Windows XP :** L'accès anonyme aux données n'est possible que si les paramètres de configuration de la politique 'EveryoneIncludesAnonymous' autorisent les accès anonymes.
>
> **Windows 2000 :** L'accès anonyme aux données n'est possible que si les paramètres de configuration de la politique 'RestrictAnonymous' autorisent les accès anonymes. Il est possible de restreindre l'accès anonyme en introduisant '1' dans la clé de registre suivante :
> **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\ RestrictAnonymous**