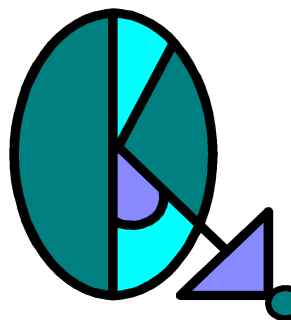


NetAdmin

Document Technique Version 5.0



GENERALITES

Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis dans le cadre de l'évolution du produit. Le logiciel décrit dans ce document est cédé dans le cadre d'un accord de licence et ne peut être utilisé ou copié que selon les stipulations de ce contrat. A moins d'être spécifiquement autorisée aux termes de l'accord, la reproduction du logiciel sur quelque support que ce soit est illégale. Toute copie ou transmission de ce manuel sous quelque forme, à quelque fin ou par quelque procédé électronique ou mécanique que ce soit, photocopie et enregistrement compris, sans le consentement écrit exprès de OïkiaLog est interdite par la loi.

Calyx SSO, Calyx Crypto et NetAdmin sont des marques déposées de la société **OÏKIALOG**.

Protect est une marque déposée de la société **ICZ Group**.

DOS/Windows, Outlook et outlook Express sont des marques déposées de MICROSOFT Corporation.

VPN1 est une marque déposée de CHECKPOINT Corporation

Lotus Notes est une marque déposée de IBM Corporation.

SAP est une marque déposée de SAP GMBH.

© Copyright 1997-2008 OÏKIALOG , tous droits réservés.

SOMMAIRE

1	PRESENTATION DE NETADMIN	5
1.1	INTRODUCTION	5
1.2	DESCRIPTION DU SYSTEME.....	5
1.2.1	<i>Le serveur NetAdmin</i>	<i>5</i>
1.2.2	<i>L'agent NetAdmin</i>	<i>5</i>
1.2.3	<i>Principes de communication.....</i>	<i>5</i>
1.3	FONCTIONNALITES	6
1.4	CONFIGURATION REQUISE	7
1.4.1	<i>Configuration requise console / serveur</i>	<i>7</i>
1.4.2	<i>Configuration requise agent.....</i>	<i>7</i>
1.5	BASE DE DONNEES	7
1.5.1	<i>Microsoft Data Engine (MSDE).....</i>	<i>7</i>
1.5.2	<i>Microsoft SQL Server 2000.....</i>	<i>7</i>
1.5.3	<i>Oracle 8.1.7 ou 9.2</i>	<i>8</i>
2	CONSOLE NETADMIN.....	8
2.1	GENERALITES.....	8
2.1.1	<i>Identification par badge.....</i>	<i>8</i>
2.2	ORGANISATION GENERALE DE LA CONSOLE	8
2.2.1	<i>Arborescence de la console.....</i>	<i>8</i>
2.2.2	<i>Panneau de paramétrage détaillé.....</i>	<i>9</i>
2.2.3	<i>Caractéristiques système des stations</i>	<i>9</i>
2.3	SCRIPT DE L'AGENT NETADMIN	9
2.4	GESTION DES UTILISATEURS.....	10
2.4.1	<i>Importation depuis une base Sam</i>	<i>10</i>
2.4.2	<i>Importation synchronisée depuis un annuaire LDAP</i>	<i>10</i>
2.4.3	<i>Configuration des badges utilisateurs.....</i>	<i>10</i>
2.4.4	<i>Gestion de la photo utilisateur</i>	<i>10</i>
2.4.5	<i>Affectation des badges aux utilisateurs</i>	<i>10</i>
2.5	DELEGATION DES FONCTIONS D'ADMINISTRATION	12
2.5.1	<i>Délégation des opérations d'administration.....</i>	<i>12</i>
2.5.2	<i>Droits d'accès aux objets à administrer.....</i>	<i>12</i>
2.6	JOURNALISATION DES OPERATIONS D'ADMINISTRATION	13
2.7	ANALYSE DE LOGS	14
3	SERVEUR NETADMIN	16
3.1	GENERALITES.....	16
3.2	LISTE D'ADRESSES AUTORISEES OU INTERDITES	16
3.3	TRAITEMENT DES LOGS	16
4	AGENT NETADMIN	16
4.1	GENERALITES.....	16
4.2	DEPLOIEMENT DE L'AGENT NETADMIN	16
4.3	AFFECTATION AUTOMATIQUE DES NOUVELLES STATIONS.....	17
4.4	GESTION DES CONNEXIONS RESEAU FURTIVES	17
5	DEPLOIEMENT LOGICIEL	17
5.1	GENERALITES.....	17
5.2	APPLICATIONS DES STRATEGIES	17
5.3	GESTION DES VARIABLES D'ENVIRONNEMENT	18
6	GESTION DES UTILISATEURS.....	18
6.1	GESTION DYNAMIQUE DES UTILISATEURS	18
6.2	DATE DE VALIDITE ET DESACTIVATION DE BADGE	18
6.3	SAUVEGARDE DU CONTENU DES BADGES	18
6.4	GESTION CENTRALISEE DES INFORMATIONS CONFIDENTIELLES.....	19

7	GESTION DES CLES DE CHIFFREMENT	20
8	GESTION DES APPLICATIONS	20
9	OUTILS ET UTILITAIRES	20
9.1	SAUVEGARDE ET RESTAURATION DE LA BASE	20
9.2	GESTION ET ANALYSE DES LOGS DISPONIBLE DANS LA CONSOLE	20
9.3	MECANISME D'ALERTE	21

1 PRESENTATION DE NETADMIN

1.1 Introduction

NetAdmin est un logiciel permettant de réaliser de manière centralisée le déploiement et le paramétrage d'applications. Il permet notamment de déployer et de paramétrer l'ensemble des produits de la Calyx Suite. NetAdmin se compose de 3 éléments distincts :

- Une console d'administration : ce logiciel permet à l'administrateur de mettre en place sa politique de déploiement et de paramétrage depuis le poste où cette console est installée. Celle-ci est installée par défaut sur le serveur mais peut-être installée sur un autre poste du parc.
- Un serveur : il a pour tâche de stocker les programmes d'installation des produits à déployer mais aussi de stocker les informations de paramétrage définies par l'administrateur à l'attention des postes du parc et les rapports et logs générés par les stations et consultés par l'administrateur.
- Un agent : installé sur chaque poste à administrer, il est en charge de la communication avec le serveur NetAdmin et de l'application des stratégies d'installation et de paramétrage définies par l'administrateur pour ce poste.

Le mécanisme de communication agent - serveur développé pour NetAdmin vous permet de vous affranchir des contraintes de droits liés au domaine et ainsi de gérer un parc de machines multi- domaines à travers le même serveur NetAdmin.

La possibilité d'installer la console d'administration de manière séparée du serveur NetAdmin vous donne l'opportunité de partager la gestion du parc entre différents administrateurs.

Une fois le serveur et une console installée, vous avez la possibilité de paramétrer l'installation de l'agent et des différents produits de la Calyx Suite mais aussi d'en définir les stratégies.

Après installation de l'agent, la console d'administration permet de visualiser les différents produits de la Calyx Suite déjà installés sur les postes, de les mettre à jour et de leur appliquer les stratégies définies par l'administrateur à travers la console d'administration.

1.2 Description du système

1.2.1 Le serveur NetAdmin

Le serveur se compose de 2 éléments : un serveur Web et une base de données. Ces deux éléments peuvent être installés sur un serveur unique ou répartis sur deux serveurs.

- Base de données : la base données est utilisée pour le stockage des stratégies définies par l'administrateur, des informations système et de configuration remontées par les agents, les logs et rapports. Cette base de données peut être au choix une base de données SQL Server 2000 (non fournie dans le produit NetAdmin), une base MSDE 2.0(fournie en standard dans NetAdmin) ou un serveur Oracle 8.1.7 ou 9.2 (non fournie dans le produit NetAdmin).
- Serveur Web : le serveur Web est un serveur propriétaire dont la tâche est de réaliser l'interface entre les agents et la base de données. Lorsque les agents contactent le serveur, celui-ci retranscrit les requêtes reçues pour les transmettre à la base de données puis renvoie les informations obtenues de la base de données vers ceux-ci.

1.2.2 L'agent NetAdmin

L'agent est un service exécuté sous le compte système qui permet d'exécuter les opérations définies par l'administrateur via la console d'administration. Il est en charge de l'installation, de la mise à jour et de la désinstallation des produits de la Calyx Suite, mais aussi de leur paramétrage et de la collecte d'informations concernant le poste et les logiciels Calyx installés sur celui-ci.

1.2.3 Principes de communication

2 méthodes de communication sont définies dans NetAdmin :

- Communication Agent – Serveur NetAdmin : la communication entre les agents et le serveur se fait de manière périodique en http. Les agents se réveillent périodiquement et contactent le serveur sur un port défini lors de l'installation de NetAdmin.
Toutefois, il peut être nécessaire dans certaines situations de réveiller l'agent sans attendre la fin de son délai de reconnexion : pour cela chacun des agents est en écoute sur un port défini lors de l'installation du serveur NetAdmin. La console d'administration utilise ce port pour contacter l'agent et ordonner le réveil de celui-ci.
L'ensemble des connexions Agent – Serveur est chiffré. Les clés de chiffrement sont générés lors

de l'initiation de chaque connexion et échangées de manière sécurisée à travers un mécanisme de chiffrement asymétrique utilisant l'algorithme RSA (longueur de clé 1024 bits).

- Communication Console – Serveur NetAdmin : la communication entre une console d'administration et le serveur NetAdmin se fait par l'intermédiaire d'un lien ODBC.

1.3 Fonctionnalités

- **Mécanisme de communication client - serveur http et base de données SQL** : le principe d'utilisation d'une ressource partagée comme cœur du mécanisme est abandonné au bénéfice d'une communication http et d'un stockage des informations dans une base de données SQL.
- **Dissociation agent / console** : la console d'administration et l'agent sont maintenant totalement dissociés. La console est une application à part entière et son installation est faite par l'administrateur sur les postes qu'ils souhaitent utiliser pour le paramétrage.
- **Agent et format du programme d'installation** : L'agent NetAdmin fonctionne dorénavant en tant que service et utilise le compte System, simplifiant ainsi son installation et sa maintenance. Le programme d'installation se présente sous la forme d'un fichier exécutable unique permettant ainsi son déplacement et son stockage sur d'autres ressources. De plus il est possible de générer des programmes d'installation contenant un compte d'administration NT permettant ainsi à un utilisateur sans pouvoir de réaliser l'installation.
- **Gestion des produits préalablement installés** : lors de son installation, l'agent est capable de détecter une Calyx Suite pré installée sur le poste et de prendre en charge son paramétrage. (Fonctionnalité disponible à partir de la version 5.4 de la Calyx Suite).
- **Paramétrage et héritage des paramètres** : l'héritage du paramétrage des produits ne se fait plus de manière globale. Il est maintenant possible de ne pas conserver l'héritage de droits uniquement pour un logiciel ou une partie d'un logiciel, l'ensemble des autres paramètres restants hérités.
- **Gestion des utilisateurs Calyx** : il est maintenant possible d'affecter jusqu'à 5 badges à un utilisateur. Ces badges peuvent être de type différent ou non. Chacun d'eux dispose d'une date de validité et peut être activé ou désactivé par l'administrateur.
- **Synchronisation LDAP** : la gestion des utilisateurs Calyx est possible via une synchronisation avec un annuaire LDAP. Si un utilisateur est créé par importation à partir d'un annuaire LDAP, alors sa disparition de l'annuaire sera signalée dans la console d'administration. Ce mécanisme de synchronisation peut être appliqué soit aux utilisateurs présents dans l'annuaire mais également à la structure arborescente de groupes de celui-ci.
- **Téléchargement dynamique de profils** : cette fonctionnalité permet de télécharger un profil depuis un annuaire LDAP lors de l'ouverture de session avec un badge. Cette fonctionnalité permet de ne pas surcharger un poste de profils quand celui-ci doit être accessible à toute personne détentrice d'un badge autorisé.
- **Sauvegarde du contenu des badges** : Calyx Suite utilise par défaut les badges afin d'assurer le stockage sécurisé des informations confidentielles. NetAdmin permet en option de réaliser une sauvegarde synchronisée de ces informations sur le serveur. Lors du renouvellement d'un badge, cette fonctionnalité permet de fournir à l'utilisateur un badge contenant les mêmes informations que le précédent même si celui-ci a été perdu.
- **Gestion centralisée des informations de connexion** : Calyx Suite utilise par défaut les badges afin d'assurer le stockage sécurisé des informations confidentielles. NetAdmin permet en option de gérer ce stockage sécurisé au niveau du serveur. Cette fonctionnalité permet notamment l'utilisation de type de badge où le stockage d'informations est impossible (biométrie, carte à puce CPS, etc...).
- **Reporting et analyse de log** : Les agents NetAdmin collectent et centralisent les rapports et logs générés sur les postes de travail. Ces données ont deux types d'origine distincte :
 - les rapports et logs générés par les agents NetAdmin et qui fournissent des informations concernant l'état de configuration des postes et les incidents rencontrés.
 - Les journaux générés par les logiciels Calyx Suite. Ces données fournissent des informations concernant l'utilisation réalisée par les utilisateurs des produits Calyx.

La console NetAdmin fournit des outils permettant d'analyser de manière synthétique et / ou de manière détaillée (station par station) les différents rapports et logs. Elle fournit notamment une liste de rapports synthétiques permettant d'avoir une vision globale du fonctionnement des solutions Calyx Suite.

Mécanisme d'alertes : un mécanisme d'alertes permet d'émettre des messages à destination des administrateurs en cas d'actions contraires à la politique de sécurité mise en place. Ce mécanisme d'alertes permet notamment :

- De signaler toute désinstallation de produit Calyx réalisé via « Ajout / Suppression de Programmes » sur les stations.
- D'envoyer le message en SMTP (mail)
- D'envoyer le message en SNMP.
- De recevoir les messages SNMP sur une trap interne à la console NetAdmin.

1.4 Configuration requise

Le serveur NetAdmin s'installe de préférence sur un serveur membre d'un domaine Windows NT ou 2000. L'utilisation d'un serveur de fichiers est recommandée car l'installation sur un contrôleur de domaine risque d'avoir un impact négatif sur les performances du logiciel NetAdmin et sur le contrôleur en lui-même.

1.4.1 Configuration requise console / serveur

La console d'administration et le serveur NetAdmin requièrent les ressources suivantes :

- Un processeur Intel Pentium fonctionnant au minimum à 500 Mhz.
- Un espace disque disponible minimum de 200 Mo sachant que la taille de la base de données évolue sur le nombre de postes et d'utilisateurs à administrer.
- 256 Mo à 512 Mo de RAM suivant la taille de la base.
- Une carte réseau prenant en charge le protocole TCP/IP ainsi qu'une adresse IP fixe.
- Windows NT4 Service Pack 6 minimum ou Windows 2000 Service Pack 2. Toutefois des systèmes d'exploitation serveur sont recommandés.

De plus vous devez décider préalablement à l'installation du serveur NetAdmin sur quel environnement de base de données vous souhaitez utiliser :

- Microsoft Desktop Engine 2.0 (MSDE).
- Microsoft SQL Server SQL Server 2000.
- Oracle 8.1.7 ou 9.2

1.4.2 Configuration requise agent

L'agent NetAdmin nécessite au minimum les ressources suivantes :

- 1 Mo d'espace disque sur le poste client.
- Un espace disque supplémentaire pour l'installation des logiciels à déployer. Pour plus d'informations, reportez vous au manuel de chacun des produits déployables via NetAdmin.
- 32 Mo de RAM.
- L'agent peut-être installé sur l'un des systèmes d'exploitation suivants : Windows 95, Windows 98, Windows NT4 Service Pack 3 ou ultérieur, Windows 2000 Service Pack 1 ou ultérieur, Windows XP.
- Internet Explorer version 4 ou ultérieure.
- A partir de Windows XP Service Pack 2, il est nécessaire de configurer le firewall XP afin qu'il autorise les flux liés à l'agent NetAdmin.

1.5 Base de données

La base de données nécessaire au fonctionnement de NetAdmin peut être au choix Microsoft Data Engine 2.0 (MSDE), Microsoft SQL Server 2000, Oracle 8.1.7 ou Oracle 9.2. Toutefois, il vous est possible de débiter votre installation avec MSDE puis de migrer vers Microsoft SQL Server en installant celui-ci sur le serveur où se trouve installé MSDE.

1.5.1 Microsoft Data Engine (MSDE)

Microsoft Data Engine (MSDE) est fourni avec le logiciel NetAdmin.

- Il permet l'utilisation d'une base de données jusqu'à une taille maximale de 2 Go.
- Il offre cinq connexions simultanées à la base ce qui limite à 5 le nombre de consoles pouvant se connecter en même temps sur cette base.

1.5.2 Microsoft SQL Server 2000

Microsoft SQL Server n'est pas inclus dans le logiciel NetAdmin. Vous devez donc l'acquérir de manière séparée.

- Il permet une capacité de stockage illimitée.
- Le nombre de connexions simultanées à la base est illimité.

- De nombreux outils d'administration de la base sont fournis en standard.
- La base de données NetAdmin peut être ajoutée à un système de base de données (SGBD) existant.

1.5.3 Oracle 8.1.7 ou 9.2

La licence pour le serveur Oracle n'est pas incluse dans le logiciel NetAdmin. Vous devez donc l'acquérir de manière séparée.

- L'utilisation d'Oracle permet une capacité de stockage illimitée.
- Le nombre de connexions simultanées à la base est illimité.
- De nombreux outils d'administration de la base sont fournis en standard.
- La base de données NetAdmin peut être ajoutée à un système de base de données (SGBD) existant.

2 CONSOLE NETADMIN

2.1 Généralités

La console NetAdmin est l'interface unique permettant la configuration à distance des agents et du serveur NetAdmin. Cette console assure de plus le paramétrage et le déploiement des produits Calyx sur l'ensemble du parc en s'appuyant sur une gestion par stations ou groupes de stations.

La console d'administration se connecte directement à la base SQL à travers les liens ODBC définis lors de l'installation de NetAdmin. Cette console d'administration peut être installée sur une machine différente de celles qui hébergent la base de données ou le serveur.

la console NetAdmin requiert la saisie d'un compte d'administration du domaine. Ce compte sera utilisé dans la console au niveau de toutes les fonctionnalités nécessitant un compte d'administration.

2.1.1 Identification par badge

Si l'administrateur a limité l'ouverture de la console NetAdmin à l'utilisation d'un badge administrateur de la console, deux cas sont possibles :

- authentification biométrique (empreinte digitale).
- authentification par badge USB ou carte à puce.

Toutefois l'administrateur a toujours la possibilité de s'authentifier à l'aide du mot de passe.

2.2 Organisation générale de la console

La console NetAdmin est structurée en 3 parties principales :

- Une barre d'outils et de menus permettant d'accéder à un certain nombre d'outils et de paramétrages généraux du serveur, de la base de données et de la console
- Une arborescence sur la gauche de la console.
- La partie droite de la console présente en détails les paramétrages, configuration ou rapports définissant l'élément sélectionné de l'arborescence. Suivant cet élément, cette partie droite peut être elle-même divisée en 2 panneaux.

L'apparence générale de la console évolue pour permettre de refléter l'état et/ou la configuration de l'élément sélectionné dans l'arborescence de gauche.

2.2.1 Arborescence de la console

L'arborescence de la console correspond à la vue de gauche de la console. Cette arborescence est composée de six nœuds principaux :

- Le nœud **Tous les Groupes** : il contient la liste des stations administrées par le serveur NetAdmin. Ces stations sont classées dans une sous arborescence de groupes permettant de simplifier la gestion des différentes configurations possibles. Par défaut chaque groupe et chaque station héritent ses configurations du groupe parent..

- Le nœud **Utilisateurs** permet la gestion des utilisateurs Calyx. Cette gestion peut être réalisée par groupe d'utilisateurs afin de faciliter la gestion des restrictions. Un utilisateur se trouvant dans cette sous arborescence peut se voir affecter de 1 à 5 badges (badge USB, carte à puce, empreinte digitale) ainsi qu'une liste de clés de chiffrement.
- Le nœud **Domaine** permet un accès au voisinage réseau et à une visualisation des machines visibles sur le réseau dans chacun des domaines. L'intérêt du nœud **Domaine** est de pouvoir intégrer des noms de machines visibles dans sa sous arborescence dans la sous arborescence **Tous les Groupes** par Glisser / Déposer.
- Le nœud **Requête Sam** permet de réaliser des importations d'utilisateurs à partir des noms d'utilisateurs présents dans une base SAM locale ou distante. Dans la sous arborescence du nœud requête SAM apparaît la liste des requêteurs vers les différentes bases SAM. A partir de chacun des requêteurs, il est possible d'importer les utilisateurs présents par glisser / déposer.
- Le nœud **Requête LDAP** permet de réaliser des importations d'utilisateurs à partir de ceux présents dans un annuaire s'interfaçant grâce au protocole Ldap. Dans la sous arborescence du nœud requête Ldap apparaît la liste des requêteurs Ldap vers les différents annuaires. Un mécanisme de synchronisation Ldap permet à l'administrateur d'importer automatiquement tous les utilisateurs apparaissant dans les annuaires définis mais aussi de supprimer dans la sous arborescence Utilisateurs ceux qui ont été supprimés des annuaires.
- Le nœud **Clés de chiffrement** : la sous arborescence de ce nœud contient la liste des clés de chiffrement stockées dans la base de données et administrables par NetAdmin. A partir de ce nœud, il est possible d'affecter des clés de chiffrement à un utilisateur ou un groupe d'utilisateur par Glisser / Déposer de celles-ci sur les utilisateurs ou groupe d'utilisateurs du nœud Utilisateurs.
- Le nœud **Configuration Application** : la sous-arborescence de ce nœud contient la liste des paramètres d'applications dont l'authentification est gérée par Calyx SSO. A partir de ce nœud, il est possible d'importer des fichiers de paramétrage Calyx SSO, de réaliser l'apprentissage de fenêtres d'authentification et de pages Web, de gérer les stratégies de mot de passe et d'affecter ces paramètres à des stations ou des groupes de stations.

2.2.2 Panneau de paramétrage détaillé

Le panneau de paramétrage détaillé forme la partie droite de la console et a pour but de présenter les détails de configuration correspondant à l'objet sélectionné dans l'arborescence. Pour cette raison, les données présentées dans ce panneau seront différentes suivant la sous arborescence dans laquelle se trouve cet objet. Dans certains cas, la partie droite de la console peut être inutilisée (comme c'est le cas pour les clés de chiffrement).

2.2.3 Caractéristiques système des stations

Des informations système concernant les stations sont remontées par l'agent NetAdmin vers le serveur dès lors que son installation est réalisée. Ces informations sont remises à jour à chaque réveil de l'agent.

Les informations systèmes récoltées sont les suivantes :

- Port d'écoute de l'agent NetAdmin.
- Mémoire physique disponible.
- Nombre et type de processeurs.
- Liste des partitions existantes sur le poste ainsi que leurs tailles totales et disponibles.
- Liste des services classés entre services arrêtés et en cours d'exécution.
- Liste des périphériques classés entre périphériques arrêtés et en cours d'exécution.
- Version d'Internet Explorer installé sur le poste client.

2.3 Script de l'agent NetAdmin

Au démarrage de l'agent NetAdmin, il est possible d'exécuter sur les postes clients un script. Ce script est un batch qui peut contenir toutes les commandes utilisables dans ce type de fichiers.

2.4 Gestion des utilisateurs

Le nœud **Utilisateur** est la racine de l'arborescence permettant la gestion centralisée des utilisateurs Calyx depuis la console NetAdmin. Cette arborescence peut contenir 2 types d'objets : des groupes et des utilisateurs. Un groupe contient des utilisateurs qui se voient affecter les restrictions appliquées au groupe. Le nom d'un utilisateur ou d'un groupe est unique dans l'ensemble de l'arborescence **Utilisateur**.

2.4.1 Importation depuis une base Sam

Les bases SAM contiennent les informations des comptes utilisateurs définis au niveau d'un serveur ou d'une station de travail de type Windows NT4, Windows 2000 ou Windows XP. La console d'administration de NetAdmin vous permet de définir des utilisateurs Calyx en utilisant ces informations..

2.4.2 Importation synchronisée depuis un annuaire LDAP

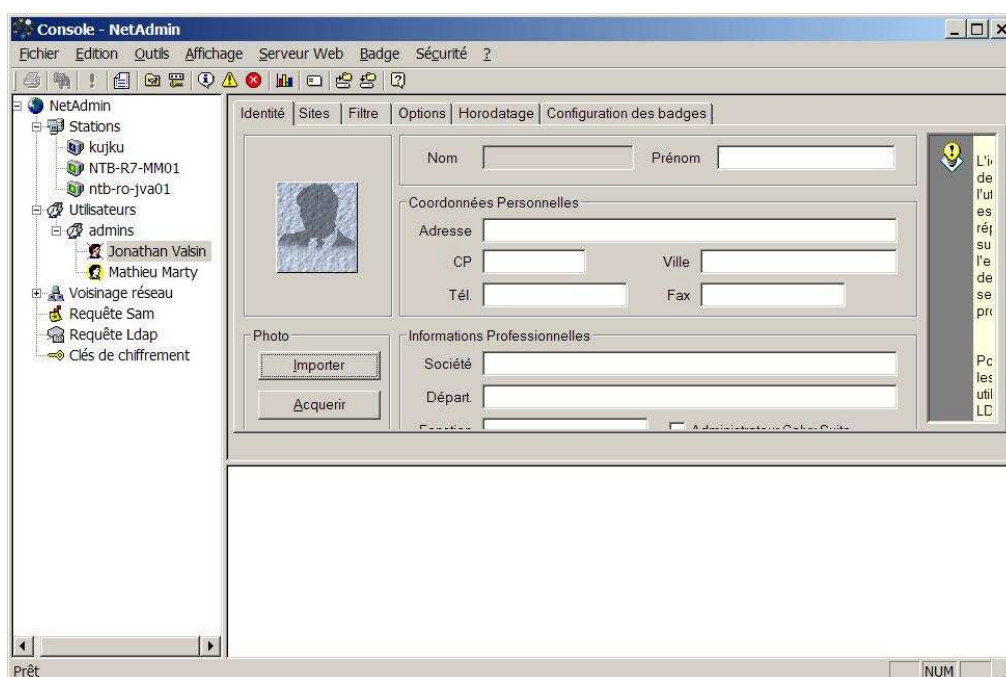
Les serveurs d'annuaire LDAP contiennent des données sur les membres d'une société. Si votre société a mis en place un tel serveur, vous pouvez importer ces données pour créer de nouveaux utilisateurs Calyx. Ce mécanisme de synchronisation peut être appliqué soit aux utilisateurs présents dans l'annuaire mais également à la structure arborescente de groupes de celui-ci.

2.4.3 Configuration des badges utilisateurs

La console d'administration NetAdmin permet de définir pour chaque utilisateur Calyx jusqu'à 5 badges ou empreintes. Ceux-ci peuvent être soit du même type ou de type différents.

2.4.4 Gestion de la photo utilisateur

L'onglet Identité des utilisateurs gère à partir de la version 4.6 le stockage et l'affichage de la photo de l'utilisateur. Par défaut, une image par défaut est proposée.



Le bouton « Importer » permet d'importer une photo stockée dans un fichier aux formats jpeg, bmp ou gif. Le bouton « Acquérir » fournit une interface permettant de réaliser l'acquisition de la photo suivant plusieurs sources (appareil photo numérique, caméra numérique, webcam, etc.).

Une table complémentaire de la base de données présente certaines données utilisateurs (nom, prénom, photo, numéro de série des badges) sous un format exploitable par un outil de personnalisation graphique de badges. Ces données peuvent ainsi être imprimées sur la carte de l'utilisateur.

2.4.5 Affectation des badges aux utilisateurs

L'affectation des badges aux utilisateurs est réalisé dans la console d'administration NetAdmin. Toutefois, le badge n'étant pas toujours à la disposition de l'administrateur (notamment dans le cadre d'un renouvellement lors d'une perte ou d'un oubli de badge), des outils disponibles sur les postes de travail

permettent de réaliser l'affectation d'un badge à un utilisateur. Ces outils sont disponibles aussi bien session fermée que session ouverte.

2.5 Délégation des fonctions d'administration

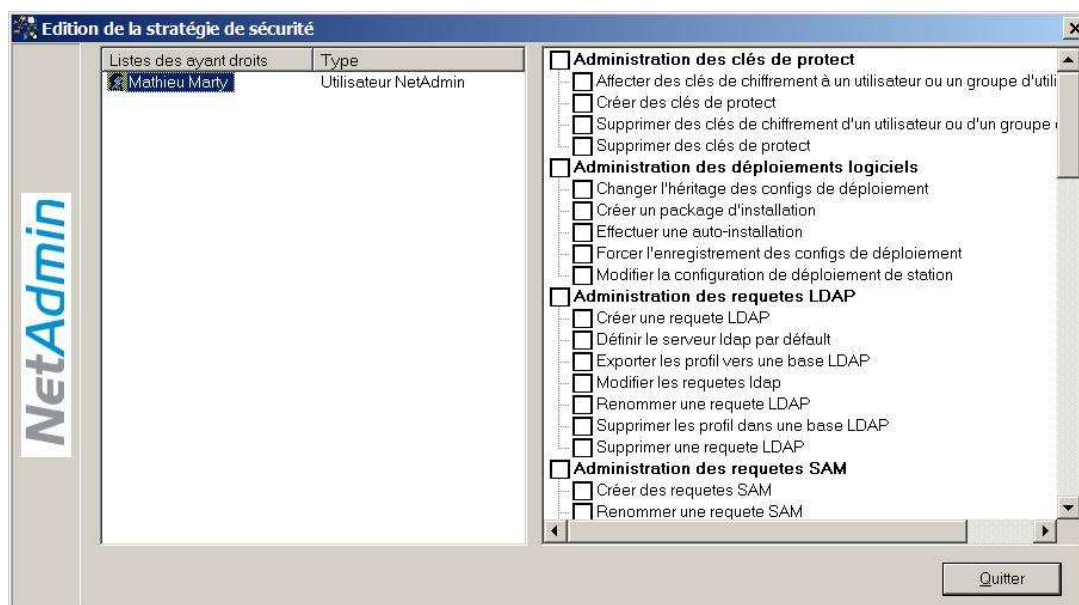
Les fonctions d'administration peuvent être découpées afin de limiter les droits des différents administrateurs. Ces restrictions portent sur les opérations que chaque administrateur peut réaliser ainsi que sur les objets (utilisateurs, groupes d'utilisateurs, stations, groupes de stations, etc.) sur lesquels l'administrateur pourra lire ou modifier les configurations.

Deux types d'accédants à la console NetAdmin sont désormais définissables : les administrateurs de la console et les utilisateurs de la console. Les administrateurs de la console NetAdmin ont tous les droits, les utilisateurs ont des droits restreints. Le paramétrage de ces 2 types d'accédants est réalisé de la même manière. Sélectionnez un utilisateur Calyx dans la console NetAdmin. Dans le menu contextuel (bouton droit), sélectionnez soit « Administrateur NetAdmin » soit « Utilisateur NetAdmin ».

2.5.1 Délégation des opérations d'administration

L'administrateur définit pour chacun des utilisateurs NetAdmin les différentes opérations d'administration qu'il sera autorisé à réaliser (exemple : création d'un utilisateur, affectation d'un badge à un utilisateur, ajout d'une station, etc.).

Ce paramétrage est réalisé dans la console NetAdmin à travers le panneau de configuration suivant :



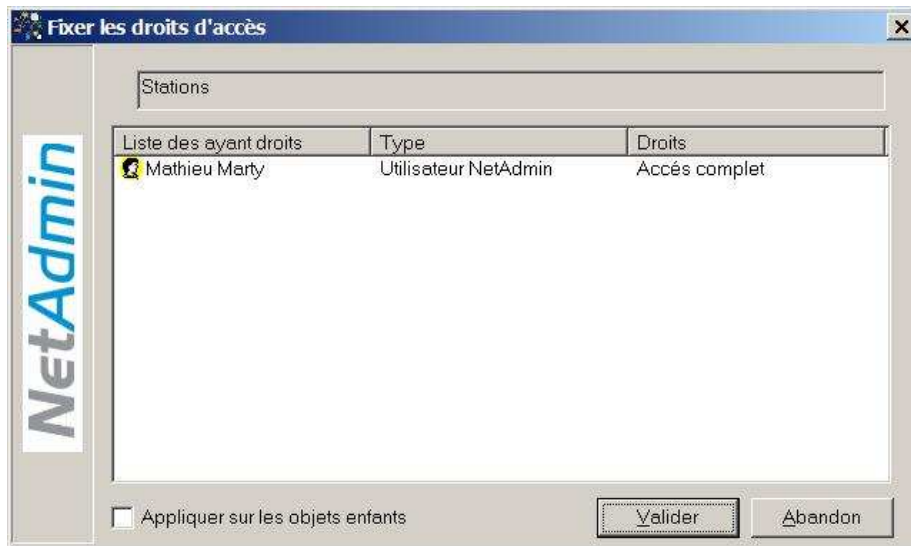
2.5.2 Droits d'accès aux objets à administrer

La console NetAdmin permet de configurer une multitude d'objets de types différents : des stations, des groupes de stations, des utilisateurs, des groupes d'utilisateurs, des clés de chiffrement, des badges, etc.

Chacun de ses objets dispose de propriétés de sécurité. Ces propriétés de sécurité définissent la liste des utilisateurs NetAdmin ainsi que leurs droits d'accès sur l'objet concerné. Par défaut, un objet appartenant à un groupe hérite des propriétés de sécurité de son groupe.

Pour chaque objet de la console NetAdmin, l'administrateur NetAdmin fixe les sécurités qui lui sont associés. 3 droits différents peuvent être affectés à chaque utilisateur NetAdmin :

- Accès complet
- Lecture seule
- Aucun accès



2.6 Journalisation des opérations d'administration

La console NetAdmin journalise l'ensemble des opérations d'administration réalisées par les administrateurs NetAdmin et les utilisateurs NetAdmin. Dans le cadre d'une délégation importante des droits d'administration, la console NetAdmin permet aux administrateurs centraux de l'entreprise d'avoir une visibilité sur les opérations réalisées par les utilisateurs NetAdmin.

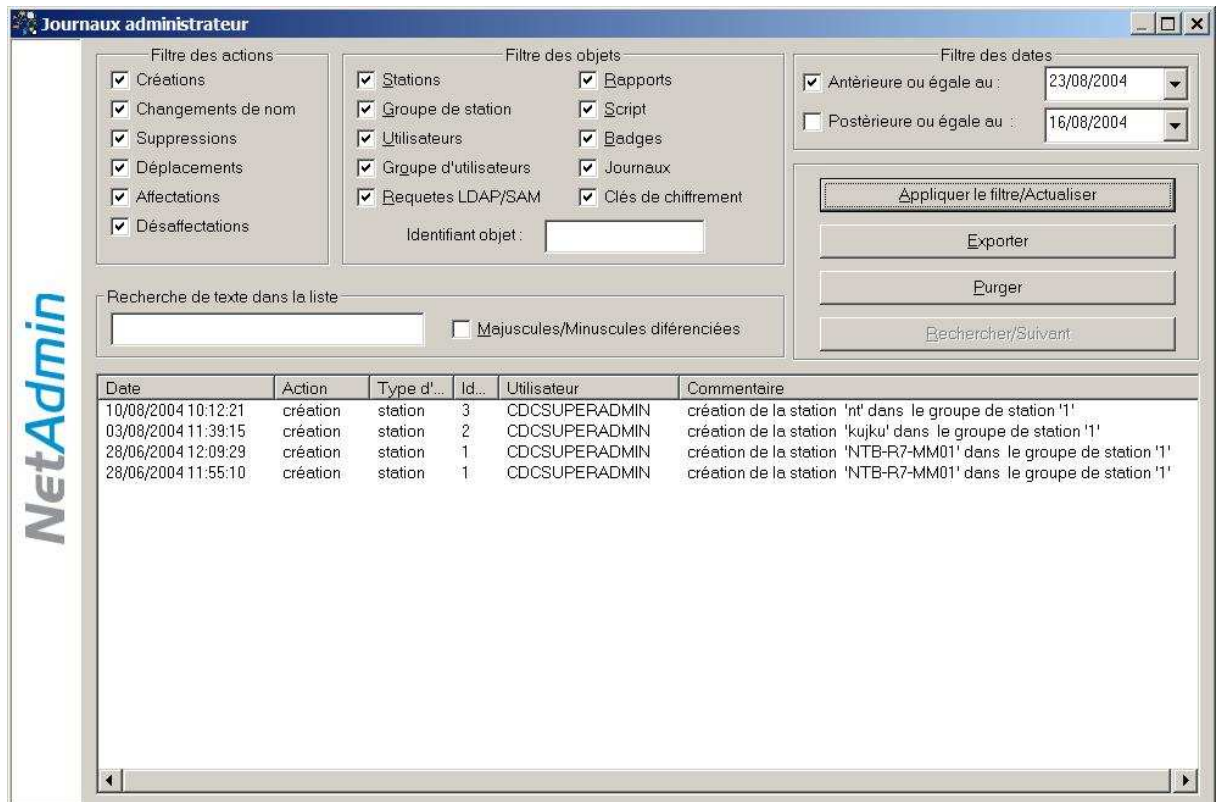
L'ensemble des actions suivantes est journalisée :

- Création d'un objet
- Changement de nom d'un objet
- Suppression d'un objet
- Déplacement d'un objet
- Affectation d'un objet
- Désaffectation d'un objet

Sachant que les objets existants dans la console NetAdmin sont :

- Les stations et les groupes de stations
- Les utilisateurs et les groupes d'utilisateurs
- Les requêtes SAM et LDAP
- Les rapports et journaux
- Les scripts
- Les badges
- Les clés de chiffrement

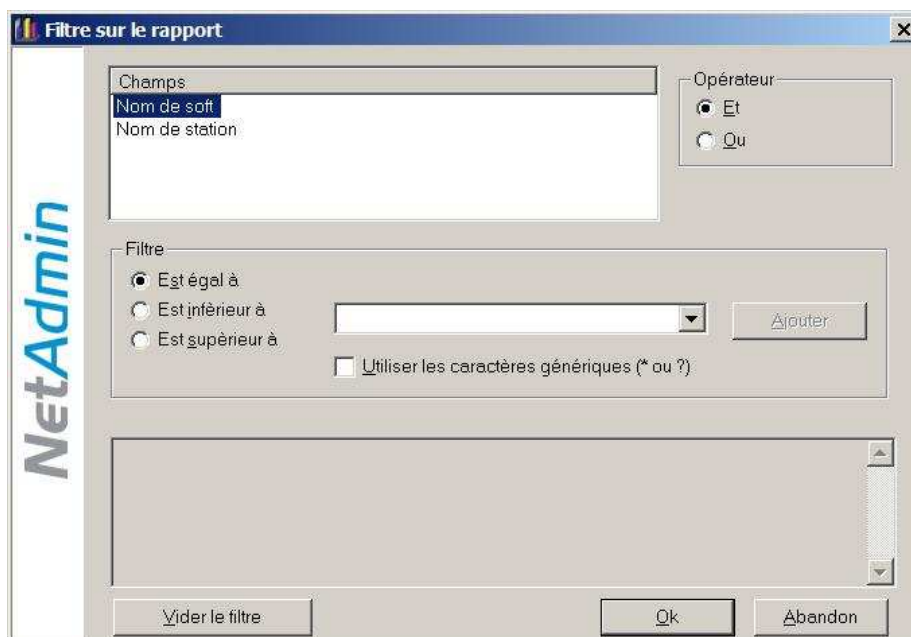
Chaque enregistrement est complétée de la date et du nom de l'administrateur ou de l'utilisateur NetAdmin ayant réalisé l'action.



L'interface de visualisation de ces logs propose des systèmes de filtre permettant de limiter la liste des logs affichés suivant des contraintes de recherche définies par l'administrateur.

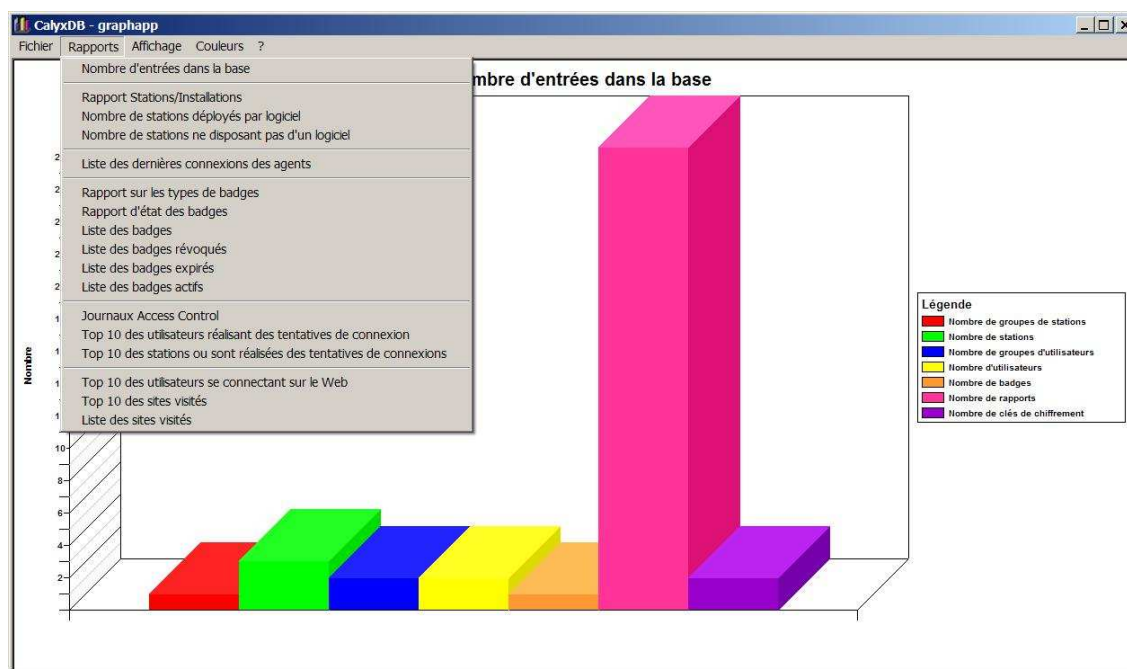
2.7 Analyse de logs

La console NetAdmin dispose d'un outil d'analyse de log présentant une liste de requêtes prédéfinies. Chaque requête est personnalisable par l'utilisateur lors de la génération du rapport. Cette personnalisation permet à l'utilisateur de mettre en place des filtres sur les requêtes exécutées. Elle permet par exemple de réaliser un rapport concernant une partie précise des postes de travail administrés.



Le résultat de la requête est alors présenté sous la forme d'un rapport graphique. Le format d'affichage de ce rapport graphique est défini par l'utilisateur et peut être modifié à tout moment. Les choix d'affichage possibles sont les suivants :

- Camembert
- Camembert 3D
- Histogramme
- Histogramme 3D
- Liste détaillées des éléments renvoyés par la requête.



La liste des rapports disponibles sont les suivants :

- **Nombre d'entrées dans la base** : présente le nombre d'objets différents gérés par la console NetAdmin.
- **Rapport Stations / Installation** : présente le nombre de postes existants ainsi que le nombre de postes disposant de chacun des produits Calyx.
- **Nombre de stations déployées par logiciel** : présente par logiciel Calyx le nombre de postes où ce logiciel est installé.
- **Nombre de stations ne disposant pas d'un logiciel** : présente par logiciel Calyx le nombre de postes ne disposant de ce logiciel.
- **Liste des dernières connexions des agents** : liste détaillée des stations et de leur dernière date de connexion au serveur NetAdmin.
- **Rapport sur les types de badges** : présente pour chaque type, le nombre de badges administrés dans la console.
- **Rapport d'état des badges** : présente le nombre de badges révoqués, actifs ou expirés.
- **Liste des badges** : présente une liste détaillée des badges administrés par la console NetAdmin.
- **Liste des badges révoqués** : présente une liste détaillée des badges révoqués.
- **Liste des badges expirés** : présente une liste détaillée des badges expirés.
- **Liste des badges actifs** : présente une liste détaillée des badges actifs.
- **Journaux Access Control** : présente une liste détaillée des tentatives de connexion de tout ou partie des utilisateurs sur tout ou partie des postes de travail.
- **Top 10 des utilisateurs réalisant des tentatives de connexion** : présente la liste des 10 utilisateurs réalisant des tentatives de connexion ainsi que le nombre de tentatives de chacun d'eux.
- **Top 10 des stations où sont réalisées des tentatives de connexion** : présente la liste des 10 stations où est réalisé le plus grand nombre de tentatives de connexion.
- **Top 10 des utilisateurs se connectant sur le Web** : présente la liste des 10 utilisateurs se connectant le plus sur Internet.
- **Top 10 des sites visités** : présente la liste des 10 sites Web les plus visités.
- **Liste des sites visités** : présente la liste détaillée des différents sites visités.

3 SERVEUR NETADMIN

3.1 Généralités

Le serveur NetAdmin est un serveur Web propriétaire dont la tâche est d'assurer la communication entre les agents NetAdmin installés sur les postes clients et la base de données SQL. Le serveur et la console NetAdmin sont donc les seuls processus autorisés à accéder à la base de données limitant ainsi la diffusion des droits d'accès à cette même base.

3.2 Liste d'adresses autorisées ou interdites

Il est possible de configurer une liste d'adresses IP dont les connexions seront soit refusées soit acceptées par le serveur NetAdmin. Cette liste est établie en spécifiant soit des adresses IP soit des plages d'adresses IP. Pour chaque entrée (adresse ou plage d'adresses), l'administrateur définit si elle correspond à des adresses autorisées ou interdites.

3.3 Traitement des logs

Le serveur NetAdmin réalise de manière permanente 2 types d'actions sur les journaux et rapports remontés par les agents NetAdmin.

- Les journaux Calyx Suite reçus par le serveur NetAdmin (journaux de contrôle d'accès et de contrôle d'accès à Internet) sont découpés et stockés dans la base de données dans des tables spécifiques à chaque type de logs. Le format simple de stockage des journaux des produits Calyx Suite dans la base NetAdmin permet à l'administrateur d'exploiter ces informations à travers un outil externe d'analyse et de corrélation de logs.
- Le serveur NetAdmin limite les volumes de logs et de rapports stockés dans la base de données en supprimant les logs les plus anciens. Cette suppression automatique est paramétrée depuis la console NetAdmin. L'administrateur NetAdmin définit par type de données, le nombre de jours de logs ou de rapports à conserver.

4 AGENT NETADMIN

4.1 Généralités

L'agent NetAdmin est un service s'exécutant sur chacun des postes clients et dont la charge est d'assurer la gestion des produits Calyx installés sur le poste. L'agent réalise les installations, les mises à jour et les désinstallations de produits, les paramétrages de ceux-ci et applique localement les stratégies affectées aux utilisateurs Calyx.

Toutes ces opérations sont réalisées par l'agent suite aux ordres reçus par l'intermédiaire du serveur NetAdmin. Au démarrage du poste client puis de manière périodique, l'agent NetAdmin contacte le serveur NetAdmin. L'agent remonte vers le serveur l'état de sa configuration (notamment la liste des produits Calyx installés en local) puis reçoit de lui des opérations à effectuer.

Il est de plus possible depuis la console NetAdmin de réveiller un ou plusieurs agents afin d'interrompre l'attente. Dès son démarrage, l'agent NetAdmin est en écoute sur un port sur lequel il reçoit l'ordre de réveil. La valeur de ce port est définie par station ou groupe de stations dans la console d'administration. Le port défini par défaut est le port 1024. A la réception de ce message, l'agent contacte le serveur NetAdmin immédiatement.

4.2 Déploiement de l'agent NetAdmin

L'agent NetAdmin peut être déployé sur les postes de travail de 3 manières différentes :

- En utilisant les fonctions d'auto-installation de la console NetAdmin : cette solution permet à l'administrateur de déployer sur les postes de travail à distance en utilisant uniquement la console NetAdmin. Cette solution a l'avantage d'être la plus simple et de ne demander aucune action complémentaire à l'utilisation de la console NetAdmin. L'installation de l'agent NetAdmin est totalement transparente pour l'utilisateur. Néanmoins elle ne peut être utilisée que sur des stations Windows NT4, 2000 ou XP et nécessite que les stations soient connectées au réseau à l'instant où l'administrateur l'utilise.

- Installation manuelle de l'agent NetAdmin : cette solution est la plus contraignante car elle nécessite une intervention directe sur les postes de travail.
- Réalisation d'un package personnalisé : ce package personnalisé, réalisé dans la console NetAdmin permet de définir un setup contenant le programme d'installation de l'agent NetAdmin, les paramètres d'installation et le compte disposant des droits nécessaires à cette installation. L'avantage de cette solution est qu'elle permet d'intégrer l'installation de l'agent NetAdmin aux scripts existants des utilisateurs. Ainsi il permet à l'administrateur d'installer automatiquement l'agent NetAdmin sur toute nouvelle machine ajoutée au réseau.

4.3 Affectation automatique des nouvelles stations

En cas d'utilisation d'un package personnalisé pour l'installation de l'agent NetAdmin sur les postes de travail, la station apparaissant dans la console NetAdmin est immédiatement affecté au groupe de stations à partir duquel le package a été réalisé.

Exemple d'utilisation :

Si l'entreprise dispose de plusieurs sites distants, l'administrateur définit dans la console NetAdmin un groupe de stations par site et un package personnalisé pour chacun des sites. Toute station où l'agent est installée apparaît alors automatiquement dans la console NetAdmin dans le groupe correspondant à son site.

4.4 Gestion des connexions réseau furtives

L'agent NetAdmin détecte les ouvertures de connexions réseau. A chaque détection, l'agent NetAdmin interrompt son attente périodique et contacte le serveur NetAdmin dans un délai aléatoire maximum de 3 minutes.

Cette fonctionnalité permet de s'assurer d'une connexion régulière de l'agent NetAdmin avec son serveur y compris dans le cas d'un poste nomade qui se connecte uniquement par liaison RTC ou VPN.

5 DEPLOIEMENT LOGICIEL

5.1 Généralités

Après installation du serveur et déploiement de l'agent, il est possible pour l'administrateur de mettre en place une politique de déploiement des produits Calyx sur un ou plusieurs postes du parc.

5.2 Applications des stratégies

Après installation du serveur NetAdmin et de sa console et après déploiement de l'agent NetAdmin et des produits Calyx sur les postes clients, il est possible de déployer à distance les stratégies de configuration de ces logiciels.

- A partir de la console d'administration NetAdmin, les stratégies logicielles sont définies et stockées dans la base de données du serveur NetAdmin.
- Lorsque l'agent se connecte au serveur NetAdmin, il indique à celui-ci la liste des applications Calyx installées et administrables à travers le logiciel NetAdmin.
- Le serveur NetAdmin fournit à l'agent les stratégies à appliquer pour chacune des applications Calyx présentes sur le poste client et administrables par NetAdmin.
- Le serveur NetAdmin transmet à l'agent la liste des applications Calyx à installer, à mettre à jour ou à désinstaller.
- L'agent NetAdmin réalise les opérations d'installation, de mise à jour et de désinstallation spécifiées par le serveur.

En cas d'erreurs lors de l'application des stratégies et durant les opérations d'installation, de mise à jour ou de désinstallation, un rapport est renvoyé par l'agent en direction du serveur NetAdmin. Ces rapports sont accessibles à travers la console NetAdmin.

Lors du réveil de l'agent NetAdmin, les stratégies logicielles sont appliquées. Si la connexion Agent – Serveur est réussie, les nouvelles stratégies logicielles sont appliquées. Si la connexion échoue, les dernières stratégies logicielles reçues par l'agent sont réappliquées.

5.3 Gestion des variables d'environnement

Toutes les configurations nécessitant la définition d'un chemin d'accès vers un fichier ou un répertoire sur un poste client se font à travers un assistant qui permet de définir au mieux le format d'écriture de ce chemin. Cet assistant propose notamment à l'administrateur l'ensemble des combinaisons possibles de variables d'environnement qui permettent de définir ce chemin d'accès.

6 GESTION DES UTILISATEURS

Cette gestion peut être réalisée par groupe d'utilisateurs afin de faciliter la gestion des restrictions. Un utilisateur se trouvant dans cette sous arborescence peut se voir affecter de 1 à 5 badges (badge USB, carte à puce, empreinte digitale) ainsi qu'une liste de clés de chiffrement.

6.1 Gestion dynamique des utilisateurs

Cette méthode de gestion des utilisateurs Calyx s'appuie sur l'utilisation d'un annuaire LDAP auquel on ajoute un objet dans le schéma. Elle ne s'applique qu'aux utilisateurs Calyx définis à partir de cet annuaire et uniquement sur les stations dont le paramétrage autorise la gestion dynamique des utilisateurs Calyx.

Lors de l'ouverture de session, l'agent NetAdmin se connecte à l'annuaire et télécharge sur le poste client les informations d'identification de l'ensemble des badges et empreintes digitales de l'utilisateur (si ces informations sont présentes dans l'annuaire).

L'agent NetAdmin signale dans la base de données à travers le serveur Web le fait que cet utilisateur est maintenant déployé sur cette station. Dans la console NetAdmin, l'utilisateur apparaît déployé comme si cela avait été fait manuellement.

Si l'utilisateur ou un de ses badges est supprimé de la base des utilisateurs Calyx du serveur NetAdmin, alors la modification est propagée jusqu'aux stations où l'utilisateur s'est déjà connecté.

6.2 Date de validité et désactivation de badge

La console NetAdmin vous permet de définir des dates de validité pour les badges de vos différents utilisateurs. Avant et après cette période de validité, le badge de l'utilisateur est désactivé. Celui-ci ne pourra donc pas utiliser ce badge pour accéder à un des postes client.

Cette fonction de désactivation peut être utilisée manuellement afin de bloquer de manière temporaire l'utilisation d'un badge.

6.3 Sauvegarde du contenu des badges

Dans leur fonctionnement traditionnel, Calyx Suite et NetAdmin utilise les badges comme des supports de stockage sécurisés des informations confidentielles (informations de connexion système, informations d'authentification applicatives et Web, clés de chiffrement, etc...).

NetAdmin propose au choix de l'administrateur de réaliser une sauvegarde synchronisée du contenu des badges utilisateurs. Activable par station ou groupe de stations, cette fonctionnalité permet à chaque modification des données contenues dans le badge de réaliser une sauvegarde de celles-ci dans le serveur NetAdmin.

Les intérêts principaux de ce second mode sont les suivants :

- En cas de perte ou de remplacement de badge, pouvoir restaurer les données sauvegardées, dans le badge nouvellement affecté à l'utilisateur.
- Conserver un mode de fonctionnement où toutes les données confidentielles sont stockées sur un support externe sécurisé (clé USB ou cartes à puce) et ne sont jamais présentes directement sur le poste client.

Principe de fonctionnement :

- Un utilisateur souhaite se connecter sur un poste client sur lequel il est autorisé à accéder. Il insère son badge ou saisit son empreinte.
- Dans le cas d'un système biométrique, il saisit son nom d'utilisateur.
- Il saisit son code PIN.
- Calyx SSO utilise classiquement les données stockées dans le badge.
- En cas de modification d'une des données par l'utilisateur, l'agent transmet les modifications au serveur NetAdmin. Si la communication réseau est interrompue, il conserve la modification pour la transmettre plus tard.
- En cas de remplacement du badge, l'administrateur affecte le nouveau badge à l'utilisateur dans la console NetAdmin puis y sélectionne le numéro de série ajouté. Dans le menu contextuel (bouton droit), il utilise l'option « Restauration d'un badge ».

6.4 Gestion centralisée des informations confidentielles

Dans leur fonctionnement traditionnel, Calyx Suite et NetAdmin utilise les badges comme des supports de stockage sécurisés des informations confidentielles (informations de connexion système, informations d'authentification applicatives et Web, clés de chiffrement, etc...).

NetAdmin propose au choix de l'administrateur un second mode de fonctionnement qui consiste à stocker l'ensemble de ces informations confidentielles dans le serveur NetAdmin et de les transmettre temporairement sur le poste de travail après authentification de l'utilisateur à l'aide de son badge.

Les intérêts principaux de ce second mode sont les suivants :

- Support de types de badges sur lesquels il est impossible d'enregistrer de l'information (Exemple : cartes de transport public ASK, Carte Professionnel Santé, etc...)
- Adaptation plus rapide à des badges propriétaires utilisées par de nouveaux clients.
- Capacité de réaffecter les données confidentielles vers un nouveau badge en cas de perte ou de vol.
- Pas de diffusion d'informations confidentielles en cas de perte ou de vol de badges. En effet aucune information n'y est stockée.
- Plus grande souplesse d'utilisation et plus grande mobilité des utilisateurs utilisant des dispositifs biométriques. Lorsque ceux-ci changent leur mot de passe, cette modification est répercuté non pas localement mais dans la base de données NetAdmin en central.

Principe de fonctionnement :

- Un utilisateur souhaite se connecter sur un poste client sur lequel il est autorisé à accéder. Il insère son badge ou saisit son empreinte.
- Dans le cas d'un système biométrique, il saisit son nom d'utilisateur.
- Il saisit son code PIN.
- L'agent transmet au serveur NetAdmin une demande d'authentification de l'utilisateur.
- En cas d'acceptation, le serveur NetAdmin transmet le package d'informations confidentielles à l'agent qui le stockent chiffré localement.
- En cas de modification d'une des données par l'utilisateur, l'agent transmet les modifications au serveur NetAdmin. Si la communication réseau est interrompue, il conserve la modification pour la transmettre plus tard.
- Un cache local contenant les informations confidentielles des X derniers utilisateurs peut être conservé sur les postes clients afin de permettre un fonctionnement en mode dégradé (pas de connexion réseau entre le poste client et le serveur).

7 GESTION DES CLES DE CHIFFREMENT

La console NetAdmin permet de gérer de manière centralisée les clés de chiffrement de Calyx Crypto. La génération des clés de chiffrement dans les badges se réalise à travers la SetBox de Calyx Crypto. Cette application est installée sur l'ensemble des machines où se trouve Calyx Crypto.

A travers la console NetAdmin, il est possible de lire les clés présentes dans le badge inséré et de les stocker de manière sécurisée dans la base de données NetAdmin.

La console NetAdmin permet d'affecter de manière centralisée des clés de chiffrement aux utilisateurs Calyx et de les déployer dans leur badge et à distance.

8 GESTION DES APPLICATIONS

La console NetAdmin permet de gérer de manière centralisée les paramètres Calyx SSO liés à la prise en charge de l'authentification applicative et web.

L'ensemble de ces paramètres se décomposent en :

- La reconnaissance des fenêtres d'authentification, de changement de mots de passe et de mots de passe invalide pour les applications modales.
- La reconnaissance des formulaires d'authentification, de changement de mots de passe et de mots de passe invalide pour les applications web.
- La définition et l'affectation aux applications des stratégies de mots de passe.

Ces paramètres peuvent être réalisées soit à l'aide des outils Calyx SSO puis importées dans la console NetAdmin ou directement dans celle-ci. Afin de simplifier l'administration des applications, les interfaces de paramétrage Calyx SSO et celles présentes dans la console NetAdmin sont identiques.

9 OUTILS ET UTILITAIRES

9.1 Sauvegarde et restauration de la base

La console NetAdmin propose en standard un outil de sauvegarde de la base de données. Cet outil permet de réaliser des sauvegardes ponctuelles de l'ensemble des configurations des stations et des utilisateurs.

Cet outil de sauvegarde et de restauration est particulièrement intéressant dans le cas de l'utilisation d'une base de données MSDE car celle-ci est fournie sans outil d'administration.

De plus une sauvegarde d'une base NetAdmin / MSDE peut être restaurée dans une base de données SQL Server.

Toutefois la sauvegarde d'une base MSDE à travers la console NetAdmin nécessite que la console NetAdmin et la base MSDE soient installées sur la même machine.

9.2 Gestion et analyse des logs disponible dans la console

NetAdmin collecte les logs générés par les logiciels Calyx sur les postes clients et les agrègent dans la base de données NetAdmin. Depuis la console NetAdmin, l'administrateur peut ainsi consulter l'ensemble de ces informations. Les logs disponibles sont les suivants :

- Journaux d'accès aux postes de travail : l'administrateur visualise les connexions réalisées sur les machines par les utilisateurs.
- Journaux d'accès à Internet ; l'administrateur visualise les connexions Internet réalisées par les utilisateurs.
- Journaux d'accès à la console d'administration : permet de tracer les accès réalisés au niveau de la console d'administration.
- Journaux de sauvegarde : ces journaux permettent de loguer chaque opération de sauvegarde de la base de données réalisée à travers une des consoles d'administration NetAdmin.

Il est possible de limiter la visualisation des logs suivant une plage de dates et non plus seulement date par date.

Un mécanisme automatique permet de NetAdmin de réaliser une suppression automatisée des logs et rapports les plus anciens. Ce mécanisme se paramètre en fixant la durée pendant laquelle logs et rapports doivent être conservés.

9.3 Mécanisme d'alertes

Un mécanisme d'alertes permet d'émettre des messages à destination des administrateurs en cas d'actions contraires à la politique de sécurité mise en place. Ces alertes sont diffusables sous 2 formes différentes :

- D'envoyer le message en SMTP (mail) en définissant l'adresse du serveur de messagerie et les adresses de l'expéditeur affiché et du destinataire. De plus, il est possible de définir si le message est envoyé en format texte brute ou en format html.
- D'envoyer le message en SNMP en stipulant l'adresse du serveur.

Ce paramétrage du mode d'envoi est configurable par station ou par groupe de stations. Il est ainsi possible de faire varier la destination des alertes en fonction des populations de postes administrés.

Les alertes disponibles permettent :

- De signaler toute désinstallation de produit Calyx réalisé via « Ajout / Suppression de Programmes » sur les stations.
- De renvoyer l'ensemble des messages apparaissant dans la fenêtre de trace de l'agent. Cette fonctionnalité permet à l'administrateur d'analyser un incident de fonctionnement de l'agent NetAdmin sans avoir à se déplacer jusqu'au poste de travail incriminé.

La console NetAdmin dispose de sa propre trap SNMP permettant de visualiser directement les alertes envoyées. Elle est particulièrement intéressante dans le cas de l'analyse de fonctionnement de l'agent NetAdmin comme décrit plus haut.