

## Qu'est-ce que le serveur de connectivité ?

Il s'agit d'un composant de NetSupport Manager qui fournit une méthode stable et sécurisée pour connecter les Clients et les Contrôleurs via Internet en utilisant le http, ainsi qu'un contrôle à distance basé sur le web sans avoir besoin de modifier la configuration existante de pare-feux.

Le serveur de connectivité sert de passerelle entre le Contrôleur NetSupport et le Client NetSupport, et il n'y a aucune communication directe entre le Client et le Contrôleur lorsque vous utilisez un serveur de connectivité.

Un utilisateur de Contrôleur NetSupport peut alors se connecter à la passerelle en utilisant le protocole HTTP et parcourir les Clients, puis se connecter à eux quel que soit leur nombre.

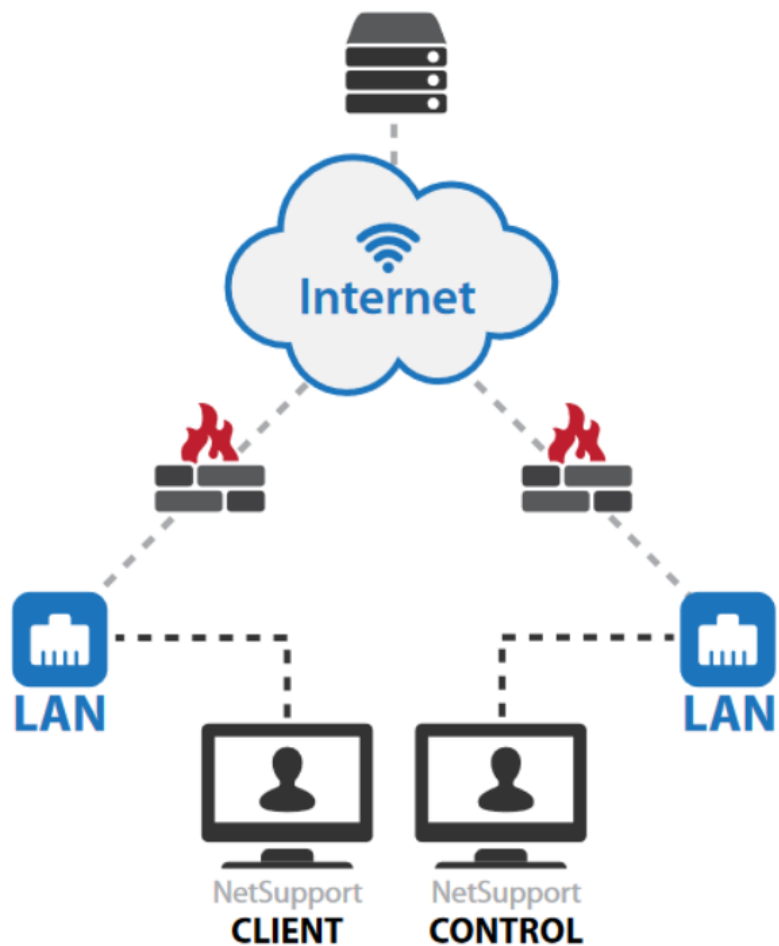
Comme il n'y a pas de connexion directe entre le Client et le Contrôleur NetSupport, le protocole utilisé est HTTP, ce qui signifie que chaque machine peut se trouver derrière un firewall configuré pour utiliser un NAT (*Network Address Translation*) sans devoir modifier la configuration du firewall.

Pour que le serveur de connectivité puisse connecter un Client et un Contrôleur, ces derniers doivent pouvoir se connecter au serveur de connectivité en utilisant le protocole HTTP sur le port configuré du serveur de connectivité (le port par défaut est 443).

Le serveur de connectivité peut être situé dans différents emplacements du réseau comme indiqué dans les scénarios suivants.

Cela permet la redondance du serveur de connectivité. Lorsque le serveur de connectivité primaire n'est pas disponible, les Clients passent automatiquement au serveur de connectivité secondaire.

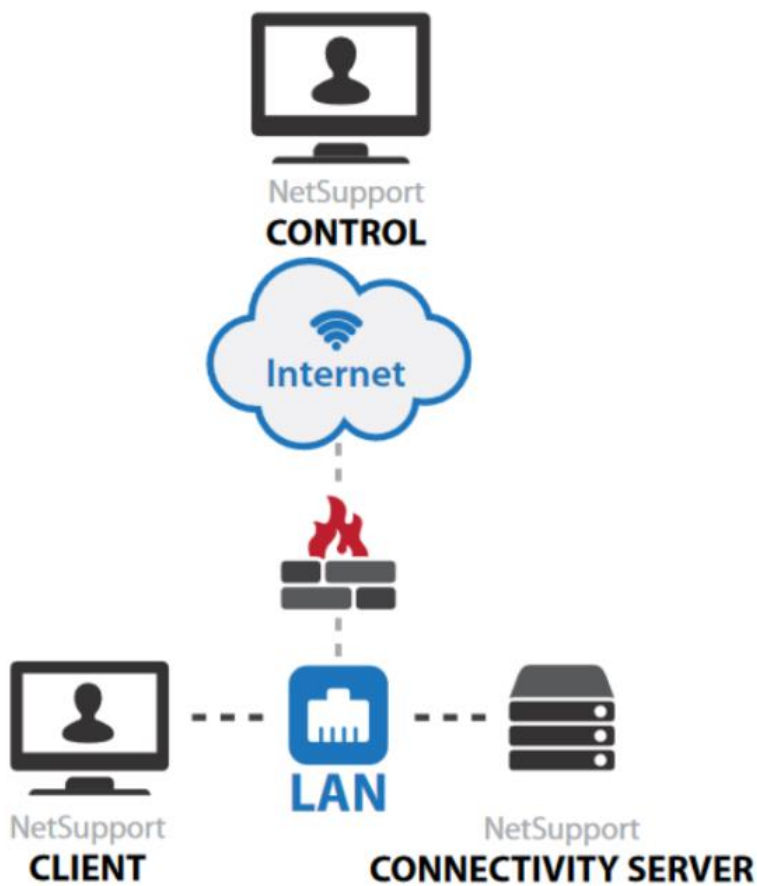
Une fois que le serveur de connectivité primaire est disponible, les Clients retournent au serveur de connectivité primaire, et le serveur de connectivité secondaire passe à nouveau en mode veille. Ce processus ne perturbe pas les sessions de contrôle à distance actives en cours.



### Scénario 1

**Dans ce scénario, le serveur de connectivité NetSupport est installé sur l'Internet public.**

Dans cet exemple, aucun changement de configuration n'aurait normalement dû être apporté à l'un ou l'autre des pare-feux. Cependant, la machine qui exécute le serveur de connectivité NetSupport est librement disponible sur Internet et pourrait être ouverte à une attaque.



### Scénario 2

Dans ce scénario, le pare-feu du site où se trouve le Contrôleur NetSupport doit être configuré pour autoriser les connexions HTTP entrantes vers le serveur de connectivité (sur le numéro de port configuré).

Cela reviendrait à installer un serveur web sur le réseau du Client et à le rendre disponible sur Internet.

Cet exemple pourrait être utilisé pour fournir un accès à distance aux utilisateurs travaillant à domicile.

### Scénario 3

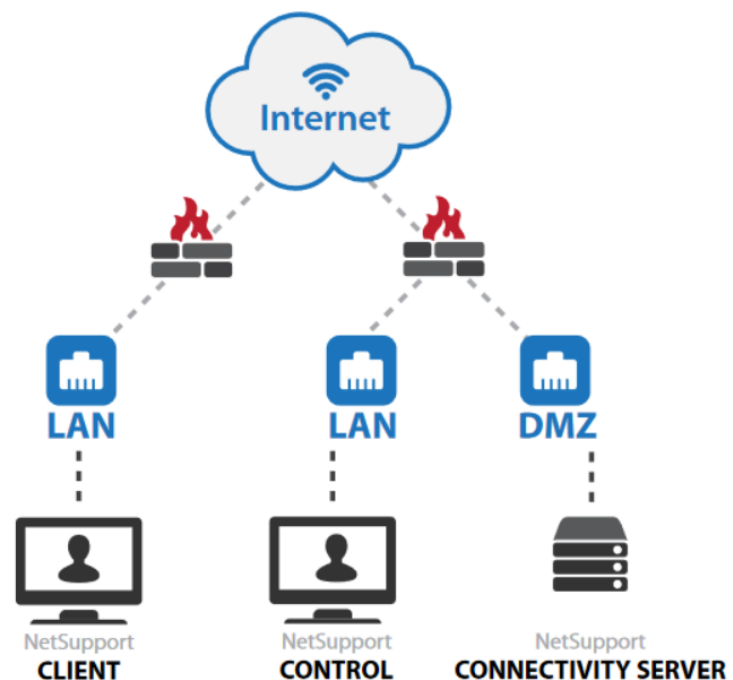
#### Serveur de connectivité sur un serveur DMZ

Dans ce scénario, le pare-feu du site où se trouve le Contrôleur NetSupport doit être configuré pour autoriser les connexions HTTP entrantes vers le serveur de connectivité (sur le numéro de port configuré).

Cela reviendrait à installer un serveur web sur la DMZ et à le rendre disponible sur le site web de l'internaute.

L'avantage de cet emplacement pour le serveur de connectivité est que la machine exécutant le serveur de connectivité est maintenant protégée contre les attaques externes par un pare-feu.

Cependant cette configuration nécessite quelques modifications de configuration du pare-feu sur le site du Contrôleur.



## Scénario 4

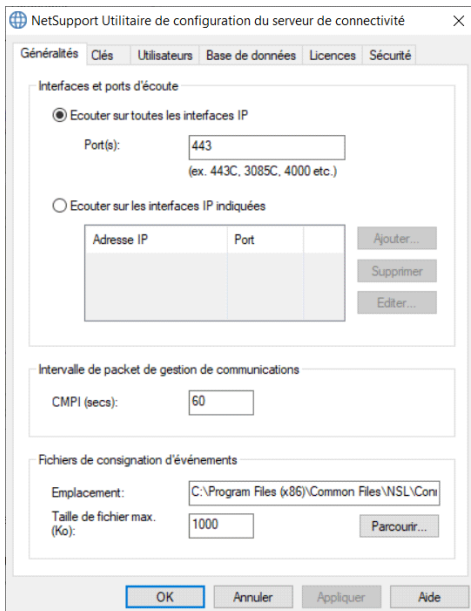
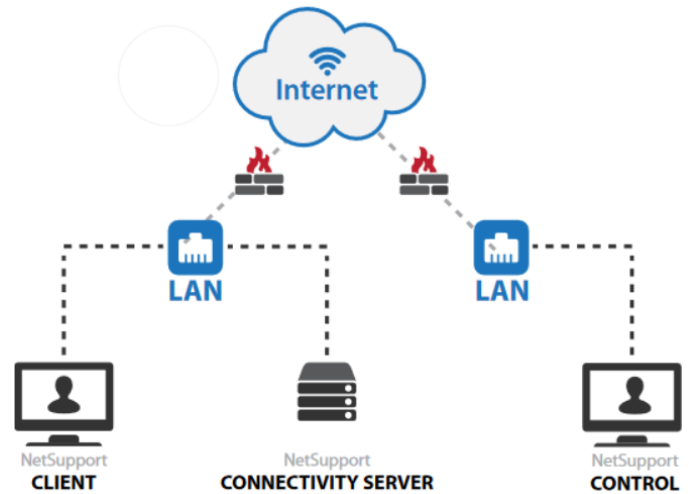
### Serveur de connectivité sur le réseau Client

Dans ce scénario, le pare-feu du site où se trouve le Client NetSupport doit être configuré pour autoriser les connexions HTTP entrantes vers le serveur de connectivité (sur le numéro de port configuré).

Cela reviendrait à installer un serveur web sur le réseau du Client NetSupport et à le rendre disponible pour les utilisateurs sur Internet.

L'avantage de cet emplacement pour le serveur de connectivité est que la machine exécutant le serveur de connectivité est maintenant protégée contre les attaques externes par un pare-feu.

Mais cette configuration nécessite quelques modifications de configuration du pare-feu sur le site client.



### Installation du serveur de connectivité

Le serveur de connectivité nécessite un système d'exploitation basé sur NT (XP, Vista, 2003, 2008, 2008 R2, Windows 7, Windows 8 et Server 2012), car il est installé comme service.

Pour installer le serveur de connectivité, exécutez le package d'installation NetSupport standard. Lorsque vous êtes invité à choisir un type d'installation, choisissez "Personnalisé".

L'écran suivant affichera alors une liste des composants NetSupport. A la fin de l'installation, l'utilitaire de configuration du serveur de connectivité s'affiche.

## Général

Vous pouvez ici définir le numéro de port sur lequel le serveur de connectivité acceptera les connexions entrantes.

Lorsque vous installez le serveur de connectivité sur une machine sur laquelle IIS (*Internet Information Services*) est déjà installé, le numéro de port doit être changé de 443 à 3085 (également enregistré dans NetSupport) ou à un autre numéro de port. Le port par défaut du protocole HTTP sur Internet est le port 80, et vous pouvez configurer le serveur de connectivité pour accepter les connexions sûres.

Cependant certains FAI (Fournisseurs d'Accès à Internet) utilisent des serveurs cache ou proxy qui mettent en cache le trafic HTTP sur le port 80.

Si votre FAI utilise un serveur cache ou proxy, les connexions du serveur de connectivité échoueront.

Le serveur de connectivité peut être configuré pour écouter sur des interfaces IP spécifiées, ou sur toutes les interfaces IP de la machine.

CMPI (secs) : Lorsqu'il est configuré pour les connexions au serveur de connectivité, le poste Client confirme sa disponibilité en interrogeant périodiquement le serveur de connectivité. Par défaut, un paquet réseau est envoyé toutes les 60 secondes, mais vous pouvez le modifier si nécessaire et spécifier l'emplacement et la taille maximale du fichier journal du serveur de connectivité.

Les fonctions de journalisation du serveur de connectivité sont expliquées en détail plus loin dans ce document.

## Clés

Vous pouvez ajouter une clé de passerelle à partir de l'onglet "Clés". Les clés de passerelle sont utilisées pour authentifier les Clients et les Contrôleurs NetSupport, garantissant ainsi que les utilisateurs non autorisés ne peuvent pas se connecter et utiliser le serveur de connectivité.

Vous devez définir au moins une clé de passerelle avant de pouvoir appliquer la configuration, car le serveur de connectivité n'acceptera aucune connexion s'il n'y en a pas au moins de configurée.

## Opérateurs

L'onglet "Opérateurs" vous permet de restreindre l'accès au contrôle à distance à une liste d'utilisateurs spécifiés. Sur le Contrôleur, un utilisateur devra saisir un nom d'utilisateur et un mot de passe afin de pouvoir utiliser le serveur de connectivité et se connecter aux Clients.

## Licences

L'onglet "Licences" affiche toutes les licences NetSupport qui ont été appliquées au serveur de connectivité. Le champ "Statut" indique si la licence a été activée. Si la licence n'a pas été activée, le bouton "Activer" peut être utilisé pour lancer le processus d'activation.

Ce processus d'activation s'effectue soit automatiquement sur Internet, soit manuellement en contactant l'équipe d'assistance technique NetSupport ou le revendeur local qui peut fournir un code d'activation.

## Sécurité

Dans l'onglet "Sécurité", l'option "Activer le cryptage des communications vers les ordinateurs distants" est disponible. Lorsque cette option est activée, toutes les communications dans le processus de connexion via le serveur de connectivité sont chiffrées.

NB : Les ordinateurs distants (Contrôleurs et Clients) doivent exécuter NetSupport Manager version 11.00.0005 ou ultérieure pour pouvoir utiliser l'option de chiffrement.

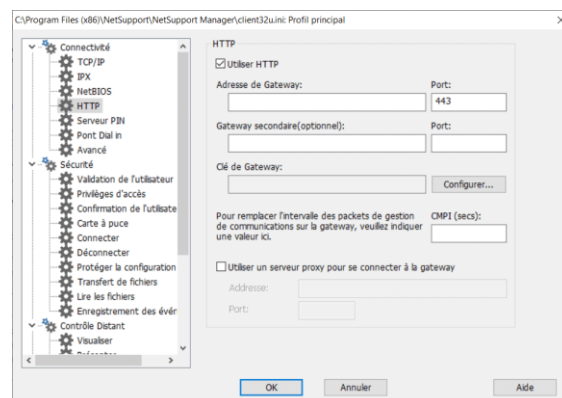
Il y a une option supplémentaire "Bloquer tous les ordinateurs distants qui n'utilisent pas les communications cryptées". L'activation de cette option empêchera les versions antérieures du Client NetSupport Manager qui ne prennent pas en charge le niveau de chiffrement amélioré de se connecter au serveur de connectivité.

## Configuration des Clients pour l'utilisation du serveur de connectivité

Pour configurer un Client afin d'utiliser le protocole HTTP, vous devez exécuter NetSupport Manager Configurateur.

- Cliquez sur "Avancé" puis double-cliquez sur le profil de votre choix.
- Dans "Connectivité", cliquez sur "HTTP" puis cochez l'option "Utiliser HTTP".
- Entrez le numéro de port pour lequel le serveur de connectivité que vous allez utiliser est configuré, la valeur par défaut étant 443.
- Entrez l'adresse IP du serveur de connectivité principal
- Entrez l'adresse IP et le numéro de port du serveur de connectivité secondaire (facultatif)
- Appuyez sur le bouton "Configurer" pour saisir la clé de passerelle, qui doit être identique à l'une des clés de passerelle ajoutées dans le serveur de connectivité.

- Entrez les détails du serveur proxy si le Client en utilise un pour se connecter à Internet. Une fois les détails de configuration requis entrés, cliquez sur "OK" pour enregistrer la configuration et redémarrer le Client NetSupport. La configuration complète d'un Client NetSupport est stockée dans le fichier de configuration client32.ini. Ce fichier peut être facilement copié ou déployé (à l'aide de l'outil NetSupport Manager Déployer) sur d'autres machines Clients. Pour plus de détails sur le déploiement de NetSupport Manager, consultez le manuel de l'utilisateur de NetSupport Manager.



## Configuration du Contrôleur pour utiliser le serveur de connectivité

Avant de pouvoir vous connecter à un Client NetSupport à l'aide du serveur de connectivité, vous devez modifier la configuration d'un Contrôleur. Pour cela, suivez les étapes suivantes :

- Exécutez le Contrôleur de NetSupport Manager.
- Dans le volet de gauche, sélectionnez le groupe "Gateway Internet".
- Double-cliquez sur l'icône "Ajouter un Gateway".
- Dans la première fenêtre, entrez le nom et la description, puis cliquez sur "Suivant" ; vous pouvez entrer ici tous les détails que vous souhaitez décrivant le serveur de connectivité.
- Entrez l'adresse IP du serveur de connectivité et le numéro de port pour lequel il est configuré (par défaut 443).
- Si nécessaire, cochez la case "Utiliser le serveur proxy" et entrez l'adresse IP et le numéro de port du serveur proxy, puis cliquez sur "Suivant".
- Cliquez sur le bouton "Configurer" et entrez la clé de passerelle.
- NB : Si le serveur de connectivité est configuré avec plusieurs clés de passerelle, lorsque vous recherchez des clients sur une passerelle, vous ne verrez que les clients qui utilisent la même clé de passerelle que celle entrée.
- Si des opérateurs ont été configurés sur le serveur de connectivité, cliquez sur "Configurer" et entrez le nom d'utilisateur et le mot de passe correspondants. Il est possible de configurer plusieurs serveurs de connectivité dans un Contrôleur avec la même adresse IP mais avec des clés de passerelle différentes. Une fois que vous avez configuré une passerelle dans un Contrôleur, l'option "Parcourir" peut être utilisée pour afficher la liste des machines Clients actuellement connectées au serveur de connectivité.

## Sécurisation du serveur de connectivité

Le serveur de connectivité prend en charge plusieurs clés de passerelle.

Chaque clé de passerelle doit comporter au moins 8 caractères.

Les clés de passerelle peuvent être ajoutées dynamiquement au serveur de connectivité, sans perturber les connexions aux clients en cours.

Le serveur de connectivité n'acceptera pas les connexions d'un Contrôleur ou d'un Client NetSupport à moins qu'une clé de passerelle correspondante n'ait également été configurée sur le serveur de connectivité.

Les clients ne peuvent être configurés qu'avec une seule clé de passerelle, alors qu'un Contrôleur peut prendre en charge plusieurs serveurs de connectivité, chacun avec une clé de passerelle différente. Toutes les données de la clé de passerelle sont envoyées chiffrées entre le Client, le Contrôleur et le serveur de connectivité. Une fois connecté au serveur de connectivité, toutes les sécurités du Client et du Contrôleur telles que la validation de l'utilisateur, les clés de sécurité, etc. fonctionnent normalement.

Un Contrôleur ne peut afficher et se connecter qu'aux Clients utilisant une même clé de passerelle que lui.

## Matrice de connexion des clés de passerelle

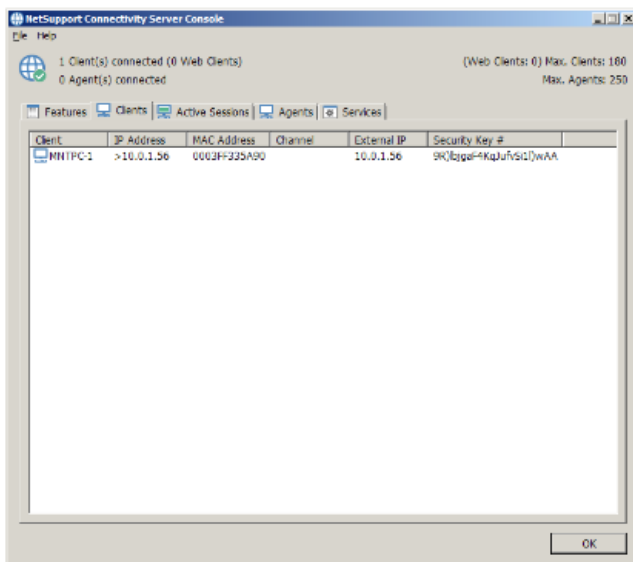
Clé du Contrôleur	Clés du Gateway	Clé du Client	Résultat
Test1	Test2	Test1	Aucune connexion du Client ou du Contrôleur
Test2	Test1, Test2	Test1	Le Client se connecte au serveur de connectivité, mais le Contrôleur ne peut pas se connecter à ce Client ou voir le Client dans un navigateur.
Test1	Test1	Test1	Le Client se connecte, le Contrôleur peut se connecter au Client et voir le Client dans une fenêtre de navigation.
Test2	Test1	Test2	Aucune connexion du Client ou du Contrôleur
Test2	Test1, Test2, Test3		Le Client se connecte, le Contrôleur peut se connecter au Client et le voir dans une fenêtre de navigation.

### Enregistrement et surveillance du serveur de connectivité

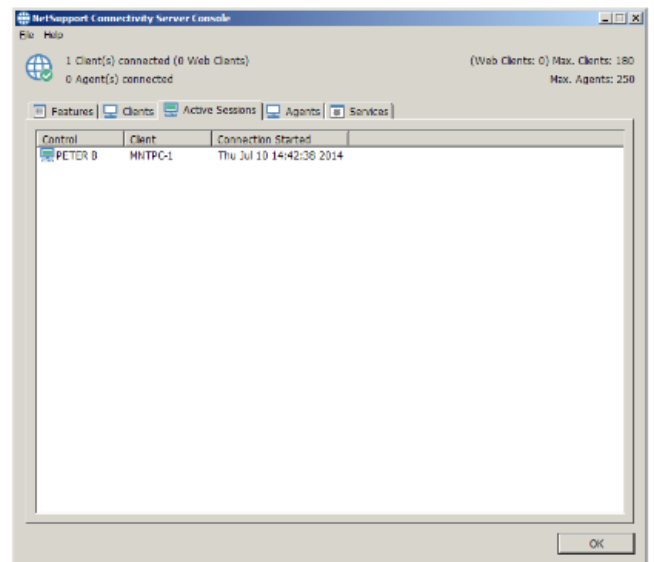
Le serveur de connectivité fonctionne en tant que service "Gateway32" et s'affiche sous forme d'icône dans la barre d'état système. Un clic droit sur l'icône permet d'afficher un menu contextuel avec les options "Ouvrir", "Configurer le serveur de connectivité" ou "A propos".

Sélectionner "Ouvrir" affichera la fenêtre "Console de serveur de connectivité" comme ci-dessous.

L'onglet "Clients" affiche la liste de tous les Clients NetSupport actuellement connectés au serveur de connectivité.



L'onglet "Sessions actives" affiche la liste des connexions en cours entre un Contrôleur et un Client, avec la date et l'heure à laquelle la connexion a commencé.



Le serveur de connectivité crée un fichier journal qui enregistre son activité. Le nom du fichier journal est GWxxxxx.log, et il est stocké à l'emplacement spécifié dans la fenêtre de configuration du serveur de connectivité.

**Exemple de logs :**

29-Jan-14, 16:11:20, NetSupport V12.00, running on Windows NT 6.0 Service Pack 1 (build 6001), platform 2

29-Jan-14, 16:11:20, Connectivity Server started, Max. Licensed connections: 5, Listening port: 443

29-Jan-14, 16:15:32, Connectivity Server stopped

Ce qui suit est une liste d'événements qui sont écrits dans le fichier journal du serveur de connectivité :

**<product\_name> <product\_version>, running on <operating\_system> <operating\_system\_version> <operating\_system\_service\_pack> (build <build\_number>), platform <platform\_number>**

Cet événement est enregistré lors du premier démarrage du serveur de connectivité. Un exemple typique serait le suivant : NetSupport V12.00, fonctionnant sous Windows NT 6.0 Service Pack 1 (build 6001), plate-forme 2

**Gateway started. Mac licensed connections: <max\_connections>**

Cet événement est enregistré lors du premier démarrage du serveur de connectivité.

**Failed to start Gateway**

Cet événement est enregistré lorsque le serveur de connectivité ne démarre pas.

**Gateway stopped**

Cet événement est enregistré lorsque le serveur de connectivité est arrêté.

**Listening on port <port\_number>**

Cet événement est enregistré lorsque le serveur de connectivité commence à écouter sur le port spécifié. Cela se produit au démarrage et lorsqu'une modification du port du serveur de connectivité est appliquée dans le configurateur du serveur de connectivité.

**Failed to bind to listening port <port\_number>**

Cet événement est enregistré lorsque le serveur de connectivité ne parvient pas à attribuer le port spécifié pour écouter les connexions entrantes. Le port est probablement utilisé par une autre application.

**Reloading configuration**

Cet événement est enregistré par le serveur de connectivité lorsque l'administrateur a utilisé le configurateur du serveur de connectivité pour appliquer des modifications de configuration.

**Listen port has changed. All current connections and sessions will be terminated.**

Cet événement est enregistré par le serveur de connectivité lorsque l'administrateur modifie le port d'écoute dans le configurateur du serveur de connectivité, puis applique la modification pendant l'exécution de la passerelle.

**Reloading Gateway Keys**

Cet événement est enregistré par le serveur de connectivité lorsque l'administrateur a utilisé le configurateur de passerelle pour appliquer des modifications de configuration, lesquelles ont pu inclure des ajouts ou des suppressions à la liste des clés de passerelle.

**Client <Clientname> connected**

Cet événement est enregistré lorsqu'un client se connecte au serveur de connectivité.

**Client <Clientname> Disconnected**

Cet événement est enregistré lorsqu'un client se déconnecte du serveur de connectivité.

**Control <controlname> connected to Client <Clientname>**

Cet événement est enregistré lorsqu'un Contrôleur se connecte à un Client.

**Control <controlname> disconnected from Client <Clientname>**

Cet événement est enregistré lorsqu'un Contrôleur se déconnecte d'un Client.

**Licence exceed. Rejecting connection from Client <Clientname> (<real\_ip\_address>, <public\_ip\_address>)**

Cet événement est enregistré lorsqu'un client se connectant au serveur de connectivité dépasse le nombre de clients sous licence.

**Security check failed for Client <Clientname> (<real\_ip\_address>). Terminating connection from <public\_ip\_address>**

Cet événement est enregistré lorsqu'une nouvelle connexion Client ne fournit pas de clé de passerelle valide.

**Security check failed for Control browse. Terminating connection from <public\_ip\_address>**

Cet événement est enregistré lorsqu'un Contrôleur ne parvient pas à fournir une clé de passerelle valide lors d'une requête de navigation à des Clients.

**Security check failed for Control <controlname>. Rejecting connection request to Client <Clientname> from <public\_ip\_address>**

Cet événement est enregistré lorsqu'un Contrôleur ne parvient pas à fournir une clé de passerelle valide lors d'une demande de connexion à un Client.

**Client/Control security check failed for Control <controlname>. Rejecting connection request to Client <Clientname> from <public\_ip\_address>**

Cet événement est enregistré lorsque la clé de passerelle fournie par le Contrôleur lors d'une demande de connexion à un Client ne correspond pas à la clé de passerelle fournie par le Client.