NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

STORMSHIELD NETWORK SSO AGENT - INSTALLATION ET DÉPLOIEMENT

Produits concernés : SNS3.x,SNS4.x

Date : 9 décembre 2019

Référence : sns-fr-sso_agent_note technique-v4

Table des matières

Avant de commencer

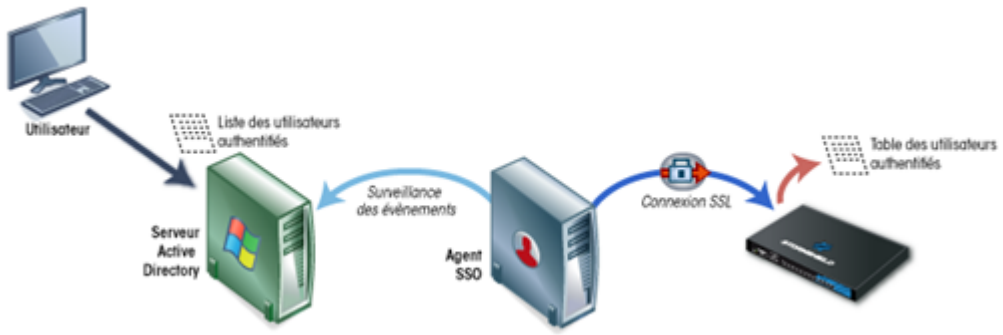
SN SSO Agent est un service Windows permettant aux Firewalls Stormshield Network de bénéficier de l'authentification sur l'annuaire Windows Active Directory de manière transparente.

A l'ouverture d'une session, c'est-à-dire lorsqu'un utilisateur se connecte au domaine Microsoft Active Directory, celui-ci est automatiquement authentifié sur le Firewall.

Principe

La méthode SSO (*Single Sign-On* ou *Authentification Unique*) permet à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs services.

A l'ouverture d'une session, un utilisateur est identifié sur le domaine Windows par le contrôleur de domaine Active Directory. L'Agent SSO collecte ces informations en se connectant à distance sur l'observateur d'événements du contrôleur de domaine. L'Agent SSO relaie ensuite ces informations au Firewall par une connexion SSL, qui met à jour sa table des utilisateurs authentifiés.



Annuaires Active Directory multiples

Lorsqu'un firewall gère l'authentification sur plusieurs domaines (forêt contenant plusieurs domaines liés par une relation d'approbation ou domaines Active Directory indépendants), il est impératif de dédier un Agent SSO à chaque domaine d'authentification.

Installation

Les installations nécessaires pour utiliser un Agent SSO sont les suivantes :

- Un domaine Windows Active Directory,
- SN SSO Agent,
- Un Firewall Stormshield Network.

Le service Stormshield Network SSO Agent peut être installé sur une machine Windows (client ou serveur) appartenant au domaine Active Directory ou sur un contrôleur de domaine (serveur hébergeant l'annuaire Active Directory). Cependant nous vous suggérons d'installer l'Agent SSO sur une machine dédiée plutôt que sur le serveur hébergeant l'Active Directory.

Pendant l'installation sur un poste de travail (client), il vous sera demandé de renseigner les informations d'un **Compte utilisateur** répertorié sur l'annuaire qui sera associé à l'Agent SSO .

NOTE

Avant de procéder à l'installation, ce compte doit au préalable être **enregistré sur l'annuaire** et avoir **certains droits** (voir la section suivante).

Les plate-formes Windows compatibles sont les suivantes :

- Installation sur un **serveur** : Windows Server 2008 ou 2008 R2, Windows Server 2011, Windows Server 2012 et Windows Server 2016,
- Installation sur un **poste client** : Windows 7, Windows 7 SP1, Windows 8 et Windows 8.1.

L'Agent SSO est un service 32 bits, compatible avec les versions Windows 64bits.

NOTE

Si vous avez au préalable installé Netasq SSO Agent, il est impératif de désinstaller ce service avant de procéder à l'installation de Stormshield Network SSO Agent.

Limite du service

Après avoir verrouillé une première session sans la fermer, une seconde session ouverte remplace la précédente. En cas de reconnexion sur la première session, celle-ci restera identifiée avec les privilèges de la seconde session.

En conséquence, il est conseillé de fermer toute session et non de la verrouiller en cas de changement d'utilisateur sur une même machine.

Compte utilisateur Active Directory

L'annuaire Active Directory doit autoriser un compte permettant à SN SSO Agent d'avoir **accès à l'observateur d'événements** de l'annuaire et avoir le droit d'**ouvrir une session en tant que service**. Le paramétrage de ce compte doit précéder l'installation de l'Agent SSO.

Pour cela vous pouvez soit créer un « compte privilégié » dédié à l'agent SSO, soit donner les droits à un utilisateur existant. Il est cependant déconseillé d'utiliser le compte Administrateur du domaine AD afin d'éviter de potentiels problèmes de sécurités.

NOTE

Si plusieurs contrôleurs AD régissent le domaine, il est impératif que le compte utilisé par l'Agent SSO soit un compte dédié appartenant au domaine, car les droits décrits ci-après doivent s'appliquer sur tous les contrôleurs, afin de relayer l'ensemble des événements survenus sur le domaine (les traces générées rapportent l'accès refusé à la lecture des événements).

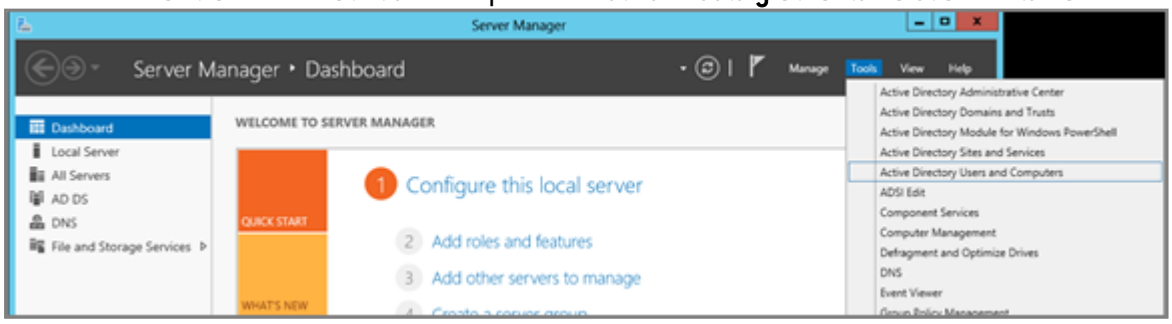
Si vous souhaitez utiliser la méthode de détection des déconnexions par Base de registre (cf. section Détection des déconnexions), ce compte doit appartenir au groupe **Administrateur du serveur Active Directory** ou être défini en tant qu'**administrateur local sur les machines supervisées**. D'autre part, cette méthode requiert la configuration de la zone inverse du domaine sur le serveur DNS afin de détecter les changements d'adresse IP (en cas de renouvellement d'adresse DHCP, par exemple). Pour plus d'informations, consultez la section **Cas spécifiques**, Changement d'adresse IP.

Paramétrer le compte utilisateur

Le paramétrage du compte utilisateur Active Directory pour l'agent SSO nécessite les 3 étapes suivantes :

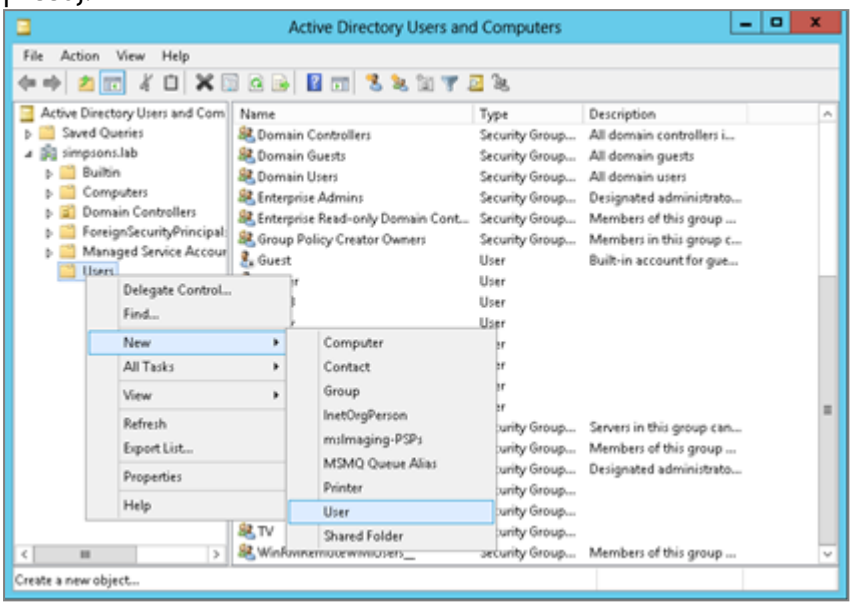
Créer le compte

Connectez-vous sur votre serveur Active Directory Windows. Depuis le **Tableau de Bord**, sélectionnez **Outils d'Administration** et cliquez sur **Active Directory Utilisateurs et Ordinateurs**.



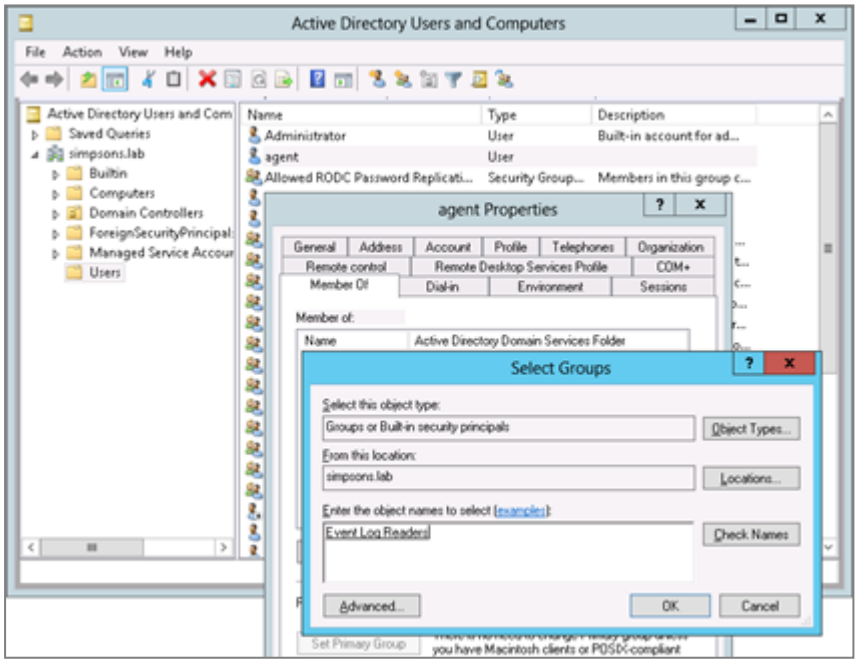
Pour créer un nouvel utilisateur, faites un clic droit sur le dossier **Utilisateur** et choisissez **Nouveau**, puis **Utilisateur**. Renseignez les champs relatifs au compte (noms, identifiant et mot de

passe).



Attribuer le droit "Lecture sur l'observateur d'événements" au compte

Ce compte doit appartenir au groupe ayant les **droits de lecture sur l'observateur d'événements** de l'annuaire. Pour cela, ouvrez le dossier **Utilisateurs :**



1. Faites un double clic sur le **compte choisi** dans la liste,
2. Cliquez sur le signet *Membre de*,
3. Cliquez sur **Ajouter**,
4. Cliquez sur **Avancées**,
5. Cliquez sur **Trouver Maintenant**,
6. Faites un double clic sur **Lecture sur l'observateur des événements**,

7. Cliquez sur **OK**,
8. Cliquez sur **Appliquer**.

Attribuer le droit "Ouvrir une session en tant que service" au compte

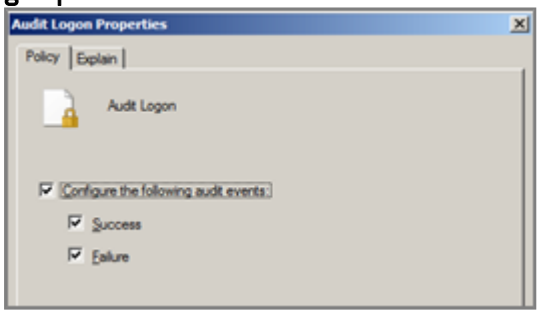
1. Dans le panneau de configuration, cliquez sur **Politique locale de sécurité**,
2. Dans les **Stratégies locales**, choisissez le dossier **Attribution des droits d'utilisateur**,
3. Double cliquez sur **Ouvrir une session en tant que service** et ajoutez le compte dédié.

Enregistrer les ouvertures de session dans l'observateur d'événements

Afin de générer les traces d'ouvertures de sessions (correspondant à l'ID 4624 dans l'observateur d'événements) sur lesquelles se base l'agent SSO pour détecter une nouvelle authentification, vérifiez que la stratégie d'audit des événements de connexion est bien activée.

Sous Windows Server 2008 : Menu **Démarrer** > **Outils d'administration** > **Stratégie de sécurité locale** > **Configuration avancée de la stratégie d'audit** > **Stratégie d'audit système – Objet Stratégie de groupe local** > **Ouvrir/fermer la session** > **Auditer l'ouverture de session**.

Sous Windows Server 2012 : **Gestionnaire de serveur** > **Outils** > **Stratégie de sécurité locale** > **Configuration avancée de la stratégie d'audit** > **Stratégie d'audit système – Objet Stratégie de groupe local** > **Ouvrir/fermer la session** > **Auditer l'ouverture de session**.



Les 3 cases de l'onglet *Paramètre de stratégie de sécurité* doivent être cochées.

Installation de Stormshield Network SSO Agent

Vous pouvez installer SN SSO Agent sur une machine appartenant au domaine Windows ou sur votre serveur Active Directory. L'assistant d'installation permet de configurer les paramètres de l'Agent SSO sur la machine.

Assistant d'installation

1. Récupérez le programme d'installation de SN SSO Agent dans votre espace privé Mystormshield (menu **Téléchargements** > **Stormshield Network Security** > **SSO Agent**).
2. Exécutez ce programme sur la machine choisie. Si vous n'êtes pas connecté en tant qu'administrateur, faites un clic droit sur l'icône de l'Agent SSO et cliquez sur **Exécuter en tant qu'administrateur**.
   L'assistant d'installation de SN SSO Agent se lance.

Type de machine

Précisez le compte choisi pour ce service et si vous souhaitez installer l'Agent SSO sur un contrôleur de domaine (serveur hébergeant l'annuaire AD) ou sur une machine appartenant au domaine Active Directory.

- Vous êtes actuellement sur le serveur hébergeant l'annuaire Active Directory et souhaitez utiliser le **compte système local**.
- Vous souhaitez utiliser un **compte dédié** sur le serveur hébergeant l'annuaire Active Directory ou sur une machine du domaine.

Compte utilisateur associé à l'Agent SSO

Entrez les informations du **compte dédié** sur le contrôleur de domaine, défini dans la section précédente (Compte utilisateur Active Directory) :

1. Entrez le nom de ce compte au format **Domaine\Utilisateur** ou **Utilisateur@Domaine** (Exemple : masociété\ssoagent).
2. Entrez le mot de passe, puis confirmez-le.

Sélection de la Clé de chiffrement SSL

La **clé pré-partagée** permet de chiffrer les communications entre l'Agent SSO et le Firewall Stormshield Network. Cette clé (mot de passe) doit également être indiquée au Firewall. En conséquence, conservez-là pour la saisir lors de la configuration de la méthode d'authentification sur le Firewall (voir la section suivante).

Si ce n'est pas la première installation, l'Agent SSO détecte la clé pré-partagée existante. Dans le cas d'une réinstallation suite à une modification à la machine, une mise à jour de l'Agent SSO ou autre, il est suggéré de conserver la clé pré-partagée.

NOTE

Dans le cadre d'une mise à jour de l'Agent SSO, il est conseillé de ne pas désinstaller la version précédente du service. En effet, cela nécessite de redémarrer la machine, ce qui

peut ne pas être aisé sur un serveur. La mise à jour de l'Agent SSO ne requiert pas de désinstallation au préalable.

Confirmation des Paramètres

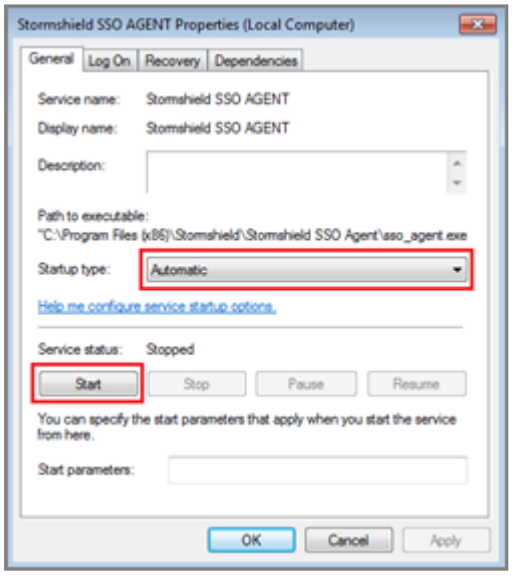
Pour modifier les paramètres que vous avez configurés, cliquez sur **Précédent**.

L'installation est complétée avec succès, cliquez sur **Terminer**.

Démarrer le service

Démarrez le service **Stormshield Network SSO Agent** dans les services Windows :

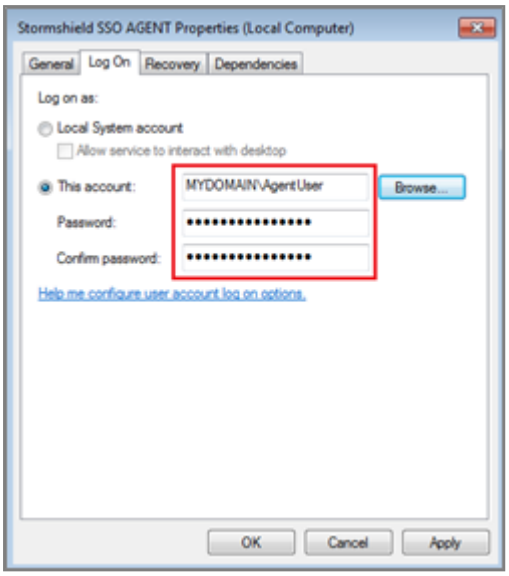
1. Entrez **Services** dans la case de recherche.
2. Appuyez sur la touche **Entrée** du clavier.
3. Double cliquez sur le service **Stormshield Network SSO AGENT**.
4. Dans l'onglet **Général**, vérifiez que le service est configuré en mode **Automatique** lors du démarrage de Windows.
5. Dans la partie **État du service**, cliquez sur le bouton **Démarrer**.
6.



Agent SSO installé sur une machine du domaine

Dans le cas où l'Agent SSO est installé sur une machine différente du contrôleur de domaine, l'identifiant et le mot de passe du **Compte utilisateur Active Directory** doivent être renseignés dans l'onglet **Log On**.

Pour rappel, ce compte doit avoir les droits de lecture sur l'observateur d'événements et d'ouvrir une session en tant que service (cf. section **Compte utilisateur Active Directory**).


Stormshield SSO AGENT Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
MYDOMAIN\AgentUser
Browse...
Password:
Confirm password:
Help me configure user account log on options.
OK
Cancel
Apply

Configuration du Firewall Stormshield Network

Pour configurer l'Agent SSO, connectez-vous sur le Firewall via un navigateur web, à l'adresse : https://*adresseIP_du_firewall*/admin.

Objets

Vous devez créer les **Objets réseaux** correspondant aux machines hébergeant les **Agents SSO** et aux **contrôleurs de domaine Active Directory**, si vous en avez plusieurs.

Pour créer ces objets, cliquez sur le module **Configuration** > **Objets** > **Objets réseaux**.

Cliquez ensuite sur **Ajouter**. Sélectionnez le type **Machine** et entrez le nom de l'Agent SSO ou du contrôleur de domaine. Précisez si cette machine est configurée en résolution DNS **dynamique** (DHCP changeant l'adresse IP à chaque connexion) ou **statique** (adresse IP fixe). L'adresse MAC de la machine n'est pas requise.

Configuration des annuaires

Il est nécessaire de configurer les annuaires Active Directory (module **Configuration** > **Utilisateur** > **Configuration des annuaires**) correspondant aux différents Agents SSO (5 maximum) précisés dans les méthodes d'authentification gérées par le firewall. Cela permet également d'avoir accès à la recherche d'utilisateurs et de groupes, notamment dans les règles d'authentification et de construire une politique de sécurité basée sur ces groupes et utilisateurs. D'autre part, la Méthode *Agent SSO* propose une option avancée définissant un Délai de mises à jour des groupes d'utilisateurs.

Authentification

Pour configurer la méthode d'authentification Agent SSO, allez dans le module **Configuration** > **Utilisateurs** > **Authentification**.

Onglet "Méthodes disponibles"

1. Cliquez sur **Ajouter une méthode**.
2. Sélectionnez **Agent SSO** dans le menu déroulant.

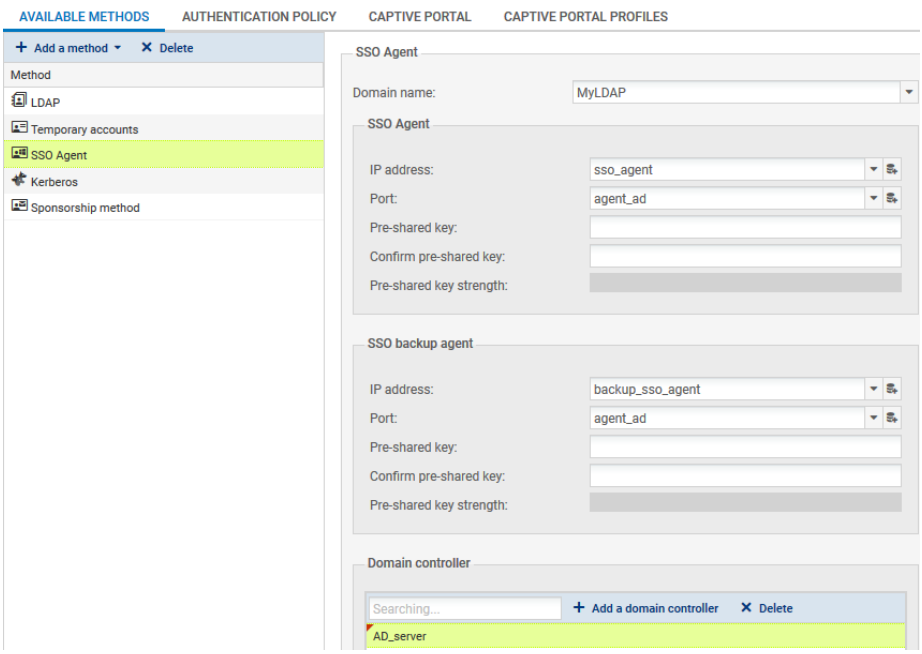
Agent SSO

Renseignez les informations de l'Agent SSO principal :

1. **Nom de domaine** : sélectionnez dans la liste déroulante le domaine Active Directory associé à l'agent SSO.
2. **Adresse IP** : sélectionnez dans le menu déroulant l'**objet réseau** correspondant à la machine où est installée l'Agent SSO.
3. **Port** : par défaut, le port "agent_ad" est sélectionné, correspondant au port 1301. Le protocole utilisé est TCP.

4. **Clé pré-partagée** (mot de passe) : renseignez la clé définie lors de l'installation de l'Agent SSO (voir la section Sélection de la Clé de chiffrement SSL).
   Cette clé est utilisée pour le chiffrement en SSL des échanges entre l'Agent SSO et le Firewall.
   La force de la clé pré-partagée indique le niveau de sécurité de ce mot de passe. Il est fortement conseillé d'utiliser des majuscules et des caractères spéciaux.

Vous pouvez également préciser ces informations pour un agent de secours (optionnel).



Contrôleur de Domaine

Vous devez ajouter tous les contrôleurs qui régissent le domaine. Ceux-ci doivent au préalable être enregistrés dans la base Objet du Firewall.

> **RAPPEL**
>
> Si plusieurs contrôleurs AD régissent le domaine, il est impératif que le compte utilisé par l'Agent SSO soit un compte dédié appartenant au domaine ayant les droits décrits dans la section Compte utilisateur Active Directory. Ces droits s'appliquent sur tous les contrôleurs, afin de relayer l'ensemble des événements survenus sur le domaine.

Configuration Avancée

1. **Durée maximum d'authentification** : définissez la durée maximum de session d'un utilisateur authentifié. Passé ce délai, le Firewall supprime l'utilisateur associé à cette adresse IP de sa table d'utilisateurs authentifiés, déconnectant l'utilisateur du Firewall.
   Ce seuil est à définir en secondes ou minutes et par défaut, est fixé à 36000 sec. (soit 10h).

2. **Délai de mises à jour des groupes d'utilisateurs** : pour chaque annuaire AD configuré sur le Firewall (**Configuration des annuaires**), le Firewall consulte les éventuelles modifications apportées aux **groupes de l'annuaire LDAP**. Le Firewall met à jour sa configuration de l'annuaire, puis renvoie ces informations à l'Agent SSO.
Cette durée définie en secondes, minutes ou heures, est fixée par défaut, à 3600 sec. (1 h).

3. **Détection des déconnexions** : activer la méthode de déconnexion permet de supprimer les utilisateurs authentifiés lors d'une déconnexion de la machine ou d'une fermeture de session. Ce test des machines connectées au Firewall s'effectue soit par méthode PING, soit par Base de Registre.
Sans l'activation de cette méthode, l'utilisateur ne sera désauthentifié qu'après la durée d'authentification fixée, même en cas de fermeture de la session.

> **NOTE**
>
> Il faut que les machines du domaine autorisent les réponses au test de PING (paramètres du *Pare-feu Windows* des machines).
>
> D'autre part, si l'agent SSO passe au travers d'un Firewall pour accéder aux machines du domaine, il faut établir les règles autorisant l'Agent SSO à tester les stations dans la politique de filtrage du Firewall.

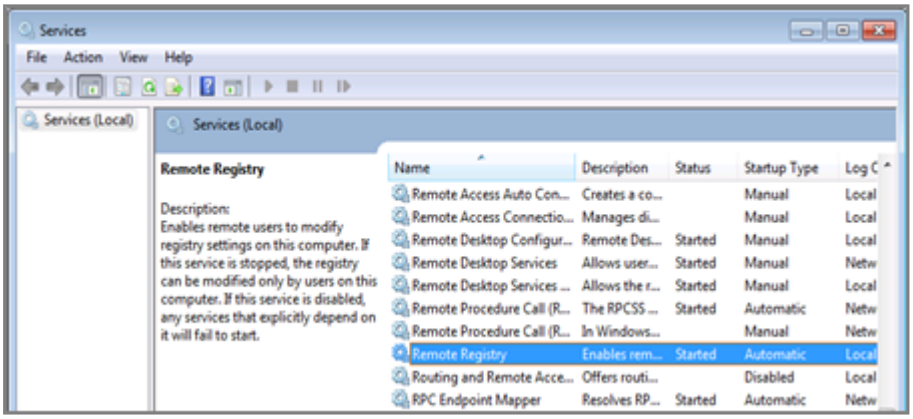
4. **Méthode de détection** :
   - **Méthode PING :** l'agent SSO teste l'accessibilité de toutes les machines authentifiées sur le Firewall toutes les 60 secondes par défaut. Dans le cas d'une réponse *host unreachable* ou d'absence de réponse d'une adresse IP après un délai défini ci-après, l'Agent SSO envoie une demande de déconnexion au Firewall. Ce dernier supprime alors l'utilisateur associé à l'adresse IP de sa table d'utilisateurs authentifiés, déconnectant ainsi l'utilisateur du Firewall.

- **Méthode Base de registre :** cette méthode permet par exemple de détecter une session fermée sur une machine toujours allumée. La **Base de registre (BDR)** est une base de données utilisée par le système d'exploitation Windows pour stocker les informations de configuration du système et des logiciels installés.
  Dans le cas d'une réponse positive au test (PING), l'Agent SSO se connecte à distance sur la machine et vérifie dans la Base de Registre la liste des utilisateurs ayant une session ouverte sur la machine. Cela permet de mettre à jour sa table des utilisateurs authentifiés.

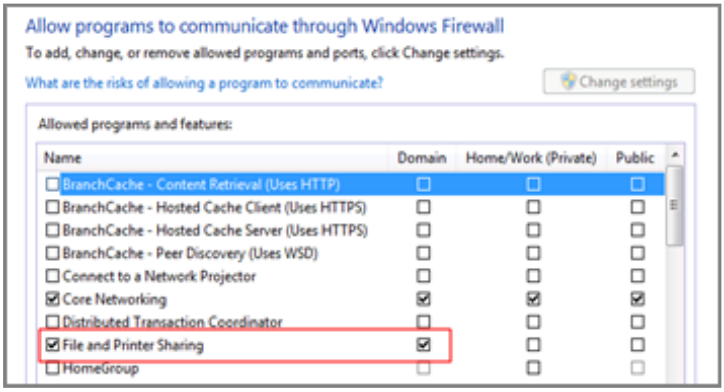
NOTE

Pour cette méthode, le compte associé à l'Agent SSO doit avoir **les droits d'administration sur toutes les machines authentifiées sur le Firewall**; ce compte doit appartenir au groupe **Administrateur du serveur Active Directory** ou être défini en tant qu'**administrateur local sur les machines supervisées** (voir la section Compte utilisateur Active Directory).

D'autre part, le service **Registre à distance** doit être activé sur ces machines. Pour cela, rendez-vous dans les **Services** de Windows, sélectionnez le service **Registre à distance** puis cliquez sur **Démarrer**. Il faut également passer le statut de ce service de l'état **Manuel** à **Automatique**.



Enfin, les ports 139 et 445 (Ports Windows) & l'ICMP doivent être ouverts. Suivez par exemple, le chemin **Panneau de configuration** > **Système et sécurité** > **Système** > **Pare-feu Windows** et cliquez sur **Autoriser un programme via le pare-feu Windows**, puis cochez le **Partage de fichiers et d'imprimante**.



RAPPEL

D'autre part, cette méthode requiert la configuration de la zone inverse du domaine sur le serveur DNS afin de détecter les changements d'adresse IP (en cas de renouvellement

d'adresse DHCP, par exemple). Pour plus d'informations, consultez la section **Cas spécifiques**, Changement d'adresse IP.

5. **Considérer comme déconnecté après** : si une machine ne répond pas au test d'accessibilité (PING) après ce délai, elle est considérée comme déconnectée. Le Firewall supprime alors l'utilisateur associé à la machine de sa table d'utilisateurs authentifiés. Cette durée est déterminée en secondes, minutes ou heures et est fixée par défaut à 5 minutes.

Comptes d'Administration ignorés

Dans la configuration d'usine du Firewall, il existe une liste d'utilisateurs dont l'authentification est ignorée. Cette liste comporte les identifiants usuels dédiés à l'administrateur (*Administrator* et *Administrateur* par défaut).

Ce mécanisme a été mis en place car le lancement d'un service ou d'une application (fonction *Exécuter en tant qu'administrateur*, par exemple) est vu par le contrôleur de domaine comme une authentification. L'agent SSO restreignant à une authentification par adresse IP, ce type d'authentification peut potentiellement remplacer l'authentification de l'utilisateur ayant ouvert une session Windows. Cette liste préétablie de « Comptes Administrateur ignorés » permet à l'agent SSO de ne pas prendre en compte leur authentification.

Cette liste de comptes d'administration est modifiable depuis le menu **Configuration avancée** de la méthode d'authentification Agent SSO.

Pour établir cette liste, consultez également la section **Cas spécifiques**, paragraphe Autres comptes du domaine.

Onglet "Politique d'Authentification"

Il est nécessaire de définir les règles autorisant le trafic dédié à la méthode de l'**Agent SSO :**

1. Cliquez sur le bouton **Nouvelle règle**.
2. Sélectionnez **Règle standard** pour lancer l'assistant de création.
3. Onglet **Utilisateur**, dans le champ *Utilisateur ou groupe* : sélectionnez l'utilisateur ou le groupe concerné ou laissez la valeur par défaut Any_user@*domaine_sélectionné*.
4. Onglet **Source** : cliquez sur **Ajouter un objet** afin de cibler l'origine (source) du trafic concernée par la règle. Cela peut être l'objet correspondant aux réseaux internes (exemple : *network_internals*).

   IMPORTANT

   La méthode d'authentification Stormshield Network SSO Agent se base sur les évènements d'authentification collectés par les contrôleurs de domaine Windows. Ceux-ci n'indiquant pas l'origine du trafic, la politique d'authentification ne peut être spécifiée avec des interfaces.
5. Onglet **Méthodes d'authentification** : cliquez sur **Autoriser une méthode** et sélectionnez dans la liste déroulante, les méthodes d'authentification à appliquer au trafic concerné par la règle. La **Méthode par défaut** sélectionnée correspond à la méthode choisie dans l'onglet *Méthode disponible*.
   Les méthodes d'authentification **sont évaluées dans l'ordre de la liste** et du haut vers le bas. La méthode *Agent SSO* étant transparente, elle est par définition, toujours appliquée en priorité.
6. Cliquez sur **OK** puis sur **Appliquer**.

NOTE

La méthode Agent SSO ne supporte pas les objets multi-utilisateur (plusieurs utilisateurs authentifiés sur une même adresse IP). Or, un objet de ce type peut être contenu dans un réseau, une plage ou un groupe défini comme source d'une règle faisant appel à la méthode Agent SSO.

Pour éviter d'avoir des traces de rejet de l'agent SSO pour les utilisateurs sur une adresse déclarée comme multi-utilisateur, il est conseillé d'ajouter deux règles dédiées à ce type d'objet, précédant celles utilisant la méthode Agent SSO :

- La première règle précise la méthode employée par l'objet multi-utilisateur,
- La suivante a l'action d'"interdire" toute autre méthode d'authentification.

Paramètres avancés de l'Agent SSO sur la machine

En cas de dysfonctionnement, il peut être utile de vérifier l'état et les propriétés de Stormshield SSO Agent.

Traces (logs)

Les traces enregistrent les communications entre l'Agent SSO et les Firewalls Stormshield Network. Les informations de connexions des utilisateurs de l'Active Directory sont collectées lorsque l'Agent SSO envoie ces informations au Firewall.

Chemin d'accès

L'Agent SSO installe les logs sur la machine hôte dans le répertoire suivant :

C:\Program Files (x86) \Stormshield\ Stormshield SSO Agent\log

Double-cliquez sur le fichier **stormshieldssoagent.log** pour visualiser son contenu.

Contenu

Le fichier de traces **stormshieldssoagent.log** contient les informations suivantes :

- la date et l'heure de la connexion,
- le nom de l'utilisateur connecté,
- l'adresse IP de la machine,
- le SID (l'identifiant sécuritaire de l'utilisateur connecté).

La taille maximale d'un fichier est de 1Mb. Le dossier peut contenir un maximum de 100Mb, soit 100 fichiers de traces. Quand le dossier atteint la taille maximum, le fichier de traces le plus ancien est supprimé.

Service Stormshield SSO Agent

Vérifiez dans les services Microsoft Windows que le service **Stormshield SSO Agent** est démarré.

Vérifier l'état du service Stormshield SSO Agent

Sur un hôte Microsoft Windows Server

1. Ouvrez le menu **Outils administratifs.**
2. Faites un double clic sur l'icône **Services** pour afficher la liste des services.
3. Vérifiez que le service Stormshield SSO Agent est en état "En cours d'exécution" et que le type de démarrage est "Automatique".

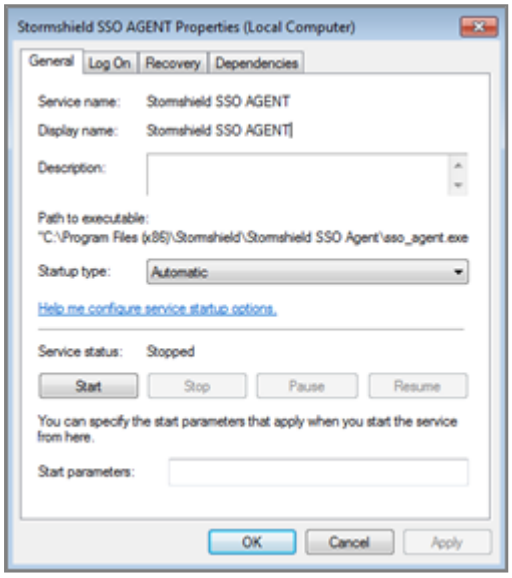
Sur un poste client Microsoft Windows

Pour les postes clients, l'utilisateur doit avoir les **Droits administrateur** sur la machine pour modifier les **Services**.

1. Tapez "services" dans la case de recherche.
2. Cliquez sur l'icône **Services** proposée.
   La liste des services s'affiche.
3. Vérifiez que le service Stormshield SSO Agent est en état "En cours d'exécution" et que le type de démarrage est "Automatique".

Visualiser les propriétés du service Stormshield SSO Agent

Double cliquez sur le service **Stormshield SSO Agent** pour afficher la fenêtre des propriétés du service :



- Onglet **Général** : vérifiez que le service est configuré en mode **Automatique** lors du démarrage de Windows. Si l'état du service est en statut **Arrêté**, cliquez sur le bouton **Démarrer**.
- Onglet **Connexion** : pour empêcher l'arrêt du service sans autorisation, vous pouvez y associer le compte utilisateur du service. Exemple : Domaine\utilisateur & mot de passe sur le domaine.
- Onglet **Récupération** : cela permet de configurer le service de l'Agent SSO s'il est arrêté; par défaut, aucune modification n'est nécessaire.
- Onglet **Dépendances** : le service SN SSO Agent ne dépend d'aucun autre service; par défaut, aucune modification n'est nécessaire.

Configuration du Pare-feu Windows

En cas d'échec du paramétrage du Pare-feu pendant l'installation, vérifiez l'ouverture du port 1301 (port par défaut) dans sa configuration.

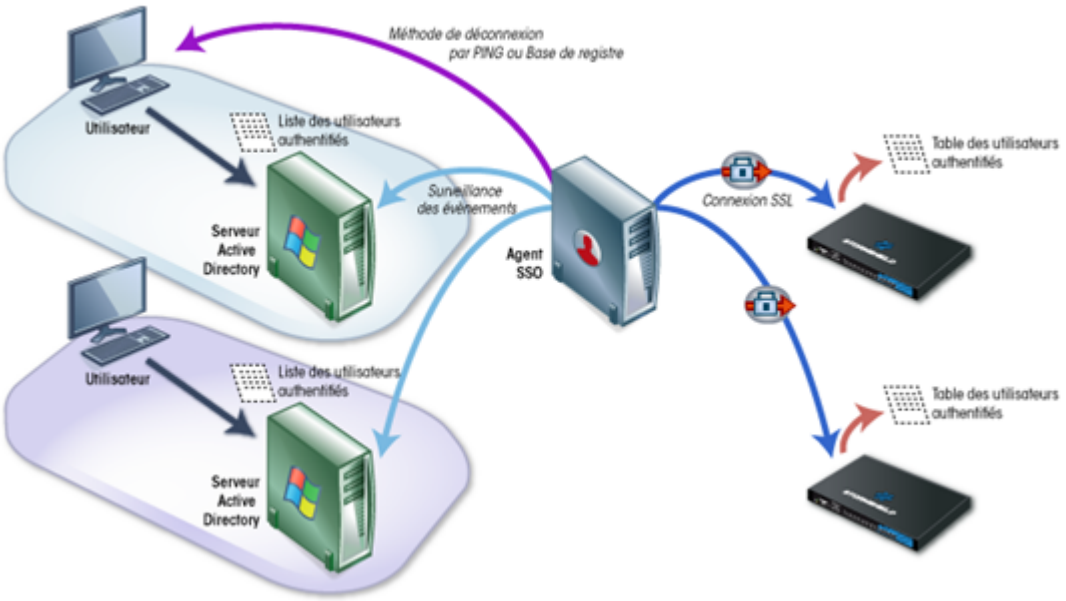
Cas spécifiques

Cette section aborde le cas de configurations autres que celle mettant en œuvre un firewall unique dans un seul domaine Active Directory.

Firewalls multiples

Plusieurs Firewalls gérant le même domaine peuvent se connecter au même Agent SSO.

Domaines multiples (annuaires différents)



Un Firewall peut gérer jusqu'à 5 domaines différents. Dans le cas d'annuaires multiples, un Agent SSO est requis par domaine.

Approbation de domaine

L'approbation de domaine permet d'établir des domaines dits "de confiance".

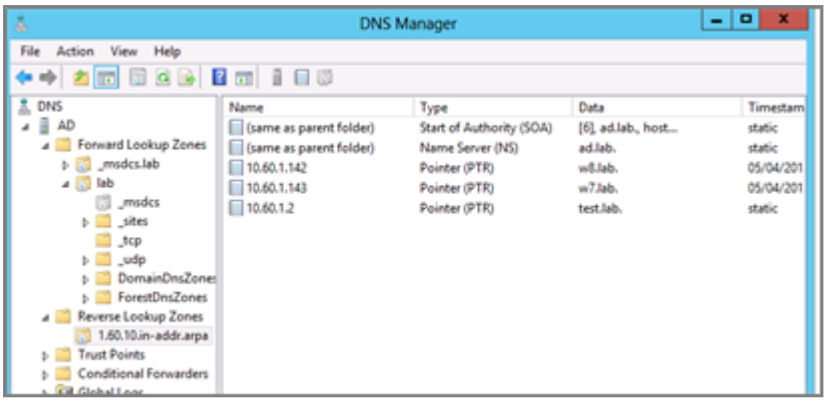
Sur une forêt Active directory intégrant des sous domaines (par exemple company.int et son sous domaine lab.company.int), les relations d'approbation permettent d'utiliser les identifiants d'un domaine pour accéder aux ressources d'un autre domaine.

Comme dans le cas des annuaires multiples, il est nécessaire de dédier un Agent SSO par domaine (ou sous-domaine) faisant partie de la relation d'approbation.

Changement d'adresse IP

Périodiquement l'agent effectue une requête DNS (PTR) pour vérifier que les machines n'ont pas changé d'IP. En cas de nouvelle adresse IP, l'information est envoyée au Firewall.

Pour cela, dans les paramètres de votre serveur DNS, il faut ajouter une **Zone de recherche inversée** ou **Reverse lookup zone** (clic droit sur le dossier) pour les machines du domaine.


DNS Manager
File Action View Help
DNS
AD
Forward Lookup Zones
_msdcs.lab
lab
_msdcs
_sites
_tcp
_udp
DomainDnsZones
ForestDnsZones
Reverse Lookup Zones
1.60.10.in-addr.arpa
Trust Points
Conditional Forwarders
Name
Type
Data
Timestam
(same as parent folder)
Start of Authority (SOA)
[6], ad.lab., host...
static
(same as parent folder)
Name Server (NS)
ad.lab.
static
10.60.1.142
Pointer (PTR)
w8.lab.
05/04/201
10.60.1.143
Pointer (PTR)
w7.lab.
05/04/201
10.60.1.2
Pointer (PTR)
test.lab.
static

Vérification du service SN SSO Agent

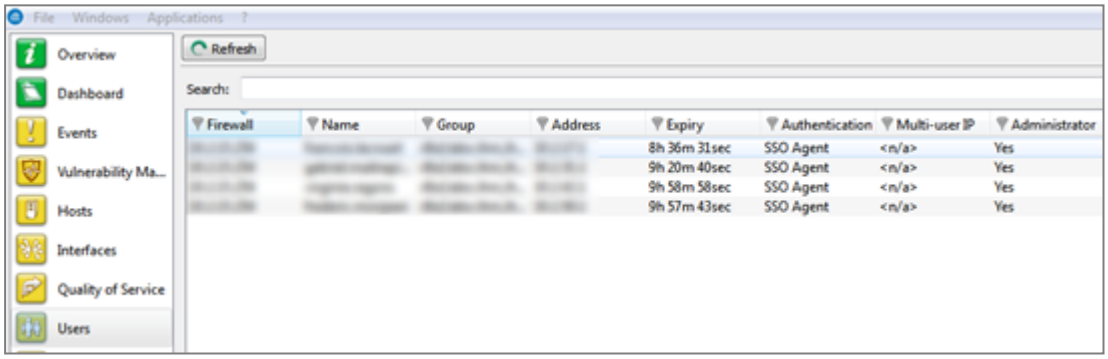
Pour vous assurer que l'Agent SSO est correctement installé et configuré, vous pouvez vérifier l'état du service à l'aide du logiciel **Stormshield Network Real-Time Monitor** ou via les **Événements Systèmes** (*System Logs*) de la machine hébergeant l'Agent SSO.

Téléchargez **SN Real-Time Monitor** depuis votre espace privé (Mystormshield) ou à l'adresse: http://gui.stormshield.eu/last-version

Stormshield Network Real-Time Monitor

Lancez SN Real-Time Monitor et connectez-vous à votre Firewall via le logiciel. Allez dans le module **Utilisateurs**.

Les informations de connexions via l'Agent SSO sont affichées par utilisateur.



Traces - Agent SSO

Sur la machine où est installé l'Agent SSO, consultez les fichiers de traces dans le dossier : **C:\Program Files (x86)\Stormshield\ Stormshield SSO AGENT\log**

Vérifiez que le fichier de trace **stormshieldssoagent.log** contient les informations suivantes :

- La connexion au Firewall.
- Les règles d'authentification appliquées aux utilisateurs.
- Les ouvertures de session des utilisateurs authentifiés envoyées au Firewall.
- Les déconnexions des machines associées aux utilisateurs.

L'image ci-dessous affiche l'information de connexion au Firewall dans le fichier de trace.

Si la connexion de l'Agent SSO au Firewall échoue, un message d'erreur est retourné.

Ce fichier, qui permet le débogage du service, est nécessaire lors d'une Assistance technique.

Problèmes fréquemment rencontrés

Les points suivants répertorient les problèmes fréquemment rencontrés. La vérification de ces éléments peut aider à la résolution d'un éventuel dysfonctionnement.

Symptôme :

L'agent SSO ne peut pas se connecter au Firewall

Solutions :

- Vérifiez la **clé de chiffrement SSL** dite **clé pré-partagée** (mot de passe),
- Vérifiez que le **port 1301** n'est pas bloqué par un Firewall ou sur la machine hébergeant l'Agent SSO,
- Vérifiez les traces dans le journal "System" (fichier */log/l_system*) du Firewall via les outils d'Administration Stormshield Network (voir Vérification du service SN SSO Agent).

Symptôme :

L'agent SSO ne peut pas se connecter au contrôleur de domaine

Solutions :

- Vérifiez que le compte associé à l'Agent SSO a les **droits de lecture sur l'observateur d'événements** de l'Active Directory,
- Vérifiez que les **ports 139 et 445** ne sont pas bloqués par un Firewall ou sur la machine hébergeant l'Agent SSO.

Symptôme :

Aucune authentification sur le Firewall

Solution :

S'il n'y a pas d'utilisateurs authentifiés sur le Firewall selon Stormshield Network Real-Time Monitor ou le fichier de traces, il est conseillé de tester la méthode d'authentification par une règle d'authentification avec la valeur *Tous* comme **Utilisateur** et la valeur *Any* comme **Source**.

Symptôme :

Les machines ne répondent pas au PING (utilisateurs désauthentifiés du Firewall).

Solution :

Si l'Agent SSO ne réussit pas à tester une machine par PING, le Firewall supprime automatiquement l'identifiant de sa table d'utilisateurs authentifiés. Cela est visible dans les traces de l'Agent SSO (voir Vérification du service SN SSO Agent):

- Vérifiez l'autorisation du protocole ICMP sur les machines du domaine (configuration du *Pare-feu Windows*).

Symptôme :

Connexion à la Base de registre impossible.

Solutions :

Si l'Agent SSO ne réussit pas à accéder à une machine, cela est visible dans les traces de l'Agent SSO (voir Vérification du service SN SSO Agent):

- Vérifiez l'**autorisation du protocole ICMP** et l'ouverture des **ports 139 et 445** sur les machines du domaine (configuration du *Pare-feu Windows*).
- Vérifiez également que la Base de registre distante est démarrée dans les services Windows et que le compte utilisé par l'Agent SSO a le droit d'administration sur ces machines.

Symptôme :

Changement d'adresse IP non détecté.

Solutions :

Les changements d'adresse IP sont détectés par des requêtes DNS:

- Vérifiez que les serveurs DNS sont bien configurés pour les machines du domaine.

Si les machines sont configurées en DHCP, le serveur DHCP doit effectuer la mise à jour des entrées des serveurs DNS:

- Vérifiez que la Zone de recherche inversée (Reverse lookup zone) a été bien crée (voir le cas spécifique Changement d'adresse IP).

documentation@stormshield.eu