NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN SSO AGENT POUR WINDOWS - INSTALLATION ET DÉPLOIEMENT

Produits concernés : SNS 4.x, SSO Agent 3.0 pour Windows

Dernière mise à jour du document : 23 octobre 2024

Référence : sns-fr-sso_agent_note technique-v4

Table des matières

Avant de commencer

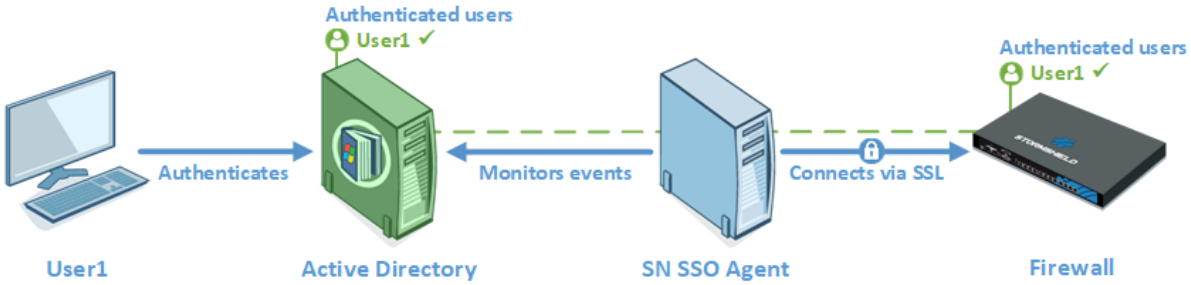
SN SSO Agent pour Windows permet aux firewalls SN de bénéficier de l'authentification sur l'annuaire Active Directory de manière transparente.

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



Annuaires Active Directory multiples

Depuis la version 3 des firewall SN, il est possible de gérer jusqu'à 5 SN SSO Agent et donc 5 domaines Active Directory sur un firewall.

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 SN SSO Agent à chaque domaine d'authentification.

Prérequis

Les prérequis nécessaires pour utiliser SN SSO Agent sont les suivants :

- Un contrôleur de domaine sous Windows Server 2016, 2019 ou 2022,
- Un compte utilisateur répertorié sur l'annuaire Active Directory qui sera associé au SN SSO Agent considéré. Ce compte doit disposer de certains droits et est demandé pendant l'installation sur un poste de travail (client). Pour plus d'informations, reportez-vous à la section Paramétrer un accès sur l'Active Directory.
- Un firewall SNS et SN SSO Agent Windows dans une version compatible. Cette information est disponible dans le guide du cycle de vie Stormshield Network Security & Tools.

NOTE

SN SSO Agent pour Windows peut être installé sur :

- Une machine Windows (client ou serveur) appartenant au domaine Active Directory,
- Un contrôleur de domaine, c'est-à-dire le serveur hébergeant l'annuaire Active Directory.

Cependant, nous vous suggérons d'installer SN SSO Agent sur une machine dédiée plutôt que sur le contrôleur de domaine.

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.

Paramétrer un accès sur l'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 SN SSO Agent.

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

NOTE
Si plusieurs contrôleurs de domaine régissent le même domaine, il est impératif que le compte utilisé par SN SSO Agent soit un compte dédié appartenant au domaine. Les droits décrits ci-après doivent s'appliquer sur tous les contrôleurs de domaine 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, 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, par exemple en cas de renouvellement d'adresse DHCP. Consultez la section Changement d'adresse IP des **Cas spécifiques** pour plus d'informations.

Installation de l'agent SSO sur un poste de travail membre du domaine

Pour faire fonctionner l'agent SSO sur un poste membre du domaine AD, il est nécessaire d'activer 3 règles dans le Pare-feu de ce poste :

- Gestion à distance des journaux des événements (NP-Entrée),
- Gestion à distance des journaux des événements (RPC),
- Gestion à distance des journaux des événements (RPC-EMAP),

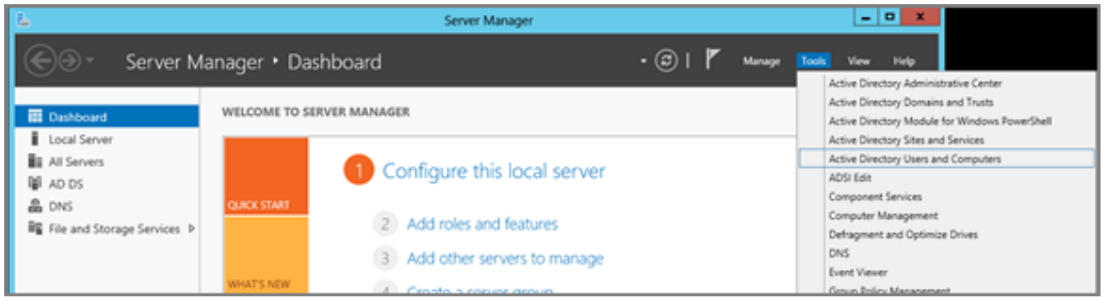
Cette manipulation est décrite dans la partie Installer SN SSO Agent.

Paramétrer le compte utilisateur

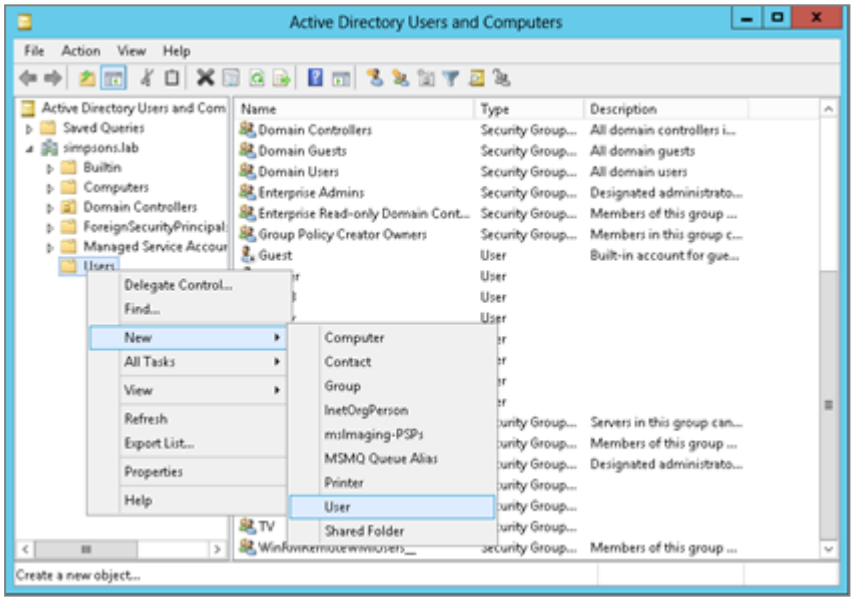
Le paramétrage du compte utilisateur Active Directory pour SN SSO Agent nécessite les 3 étapes suivantes :

Créer un compte

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



3. 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).

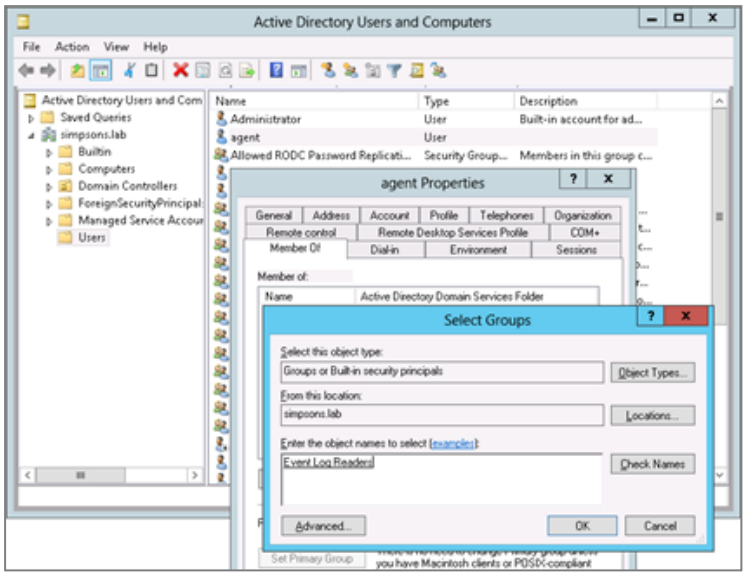


Attribuer le droit "Lecture sur l'observateur d'événements" au compte

Ce compte doit appartenir au groupe ayant les **droits de lecture sur l'observateur d'événements** de l'annuaire Active Directory.

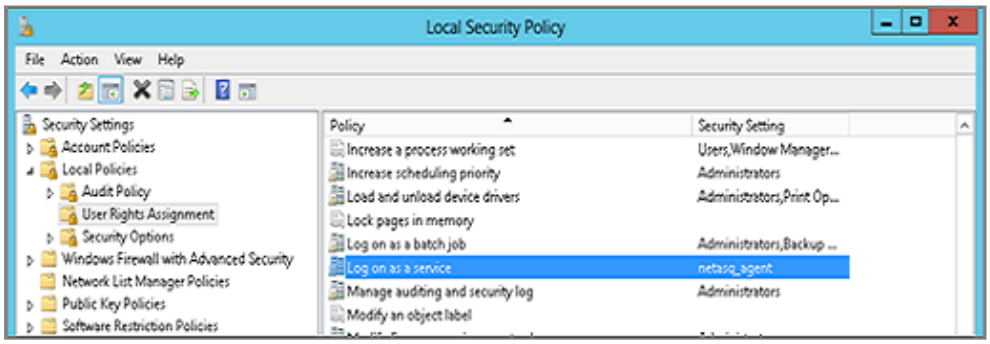
1. Ouvrez le dossier **Utilisateurs** et faites un double clic sur le **compte choisi** dans la liste,
2. Cliquez sur le signet *Membre de*,
3. Cliquez sur **Ajouter**,
4. Cliquez sur **Avancées**,

5. Dans le champ de recherche, indiquez "Lecteurs des journaux",
   Le groupe est ajouté à la liste *Membre de*.



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 le SN SSO Agent pour détecter une nouvelle authentification, vérifiez que la stratégie d'audit des événements de connexion est bien activée.

1. Rendez-vous dans le menu suivant : **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**.
2. Cochez les 3 cases de l'onglet **Stratégie**.

Installer SN SSO Agent

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

NOTE
Dans un environnement Microsoft Active Directory, SN SSO Agent version 3.x peut être déployé de façon automatique par le biais d'une stratégie de groupe (GPO : Global Policy Object). L'installation peut ainsi être réalisée de manière silencieuse (invisible pour l'utilisateur), avec les droits d'administration nécessaires, et ce à l'occasion du passage d'un client nomade sur le réseau de l'entreprise.

Si vous installez l'agent SSO sur un poste de travail membre du domaine

1. Lancez le programme **Windows Defender avec fonction fonctions avancées de sécurité**,
2. Cliquez sur le menu de gauche **Règles de trafic entrant** : la liste des règles s'affiche,
3. A l'aide la touche [Ctrl] et de la souris, sélectionnez les 3 règles suivantes :
   - Gestion à distance des journaux des événements (NP-Entrée),
   - Gestion à distance des journaux des événements (RPC),
   - Gestion à distance des journaux des événements (RPC-EMAP),
4. Dans le panneau **Actions** situé sur la droite de l'écran, cliquez sur **Activer la règle,**
5. Quittez le programme **Windows Defender avec fonction fonctions avancées de sécurité**.

Ouvrir l'assistant d'installation

1. Récupérez le programme d'installation de SN SSO Agent pour Windows dans votre espace personnel MyStormshield, dans le 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 du SN SSO Agent et cliquez sur **Exécuter en tant qu'administrateur**. L'assistant d'installation se lance.

Type de machine

Précisez le compte choisi pour ce service et si vous souhaitez installer SN SSO Agent sur un contrôleur de domaine ou sur une machine appartenant au domaine Active Directory.

- Vous êtes sur le contrôleur de domaine et souhaitez utiliser le compte système local.
- Vous souhaitez renseigner un compte dédié au service.

Compte utilisateur associé à SN SSO Agent

Entrez les informations du **compte dédié** sur le contrôleur de domaine, défini dans la section précédente Paramétrer un accès sur l'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 SN SSO Agent et le firewall SN. 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.

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

> **NOTE**
> Si SN SSO Agent est installé sur la machine dans une version antérieure à la version 1.4, il est impératif de le désinstaller avant d'installer la nouvelle version. Un redémarrage de la machine est indispensable pour finaliser la désinstallation. Prévoyez de réaliser cette manipulation au moment le plus opportun pour votre activité.

Confirmation des paramètres

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

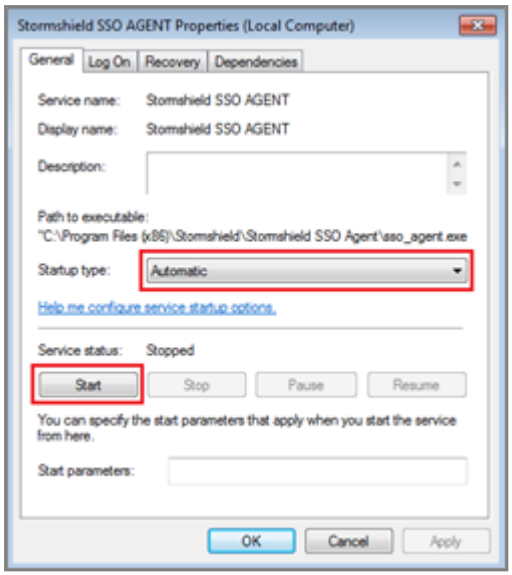
L'installation est complétée avec succès, cliquez sur **Terminer**.

Démarrer le service Windows

Une fois SN SSO Agent installé, démarrez le service **Stormshield SSO Agent** dans les services Windows :

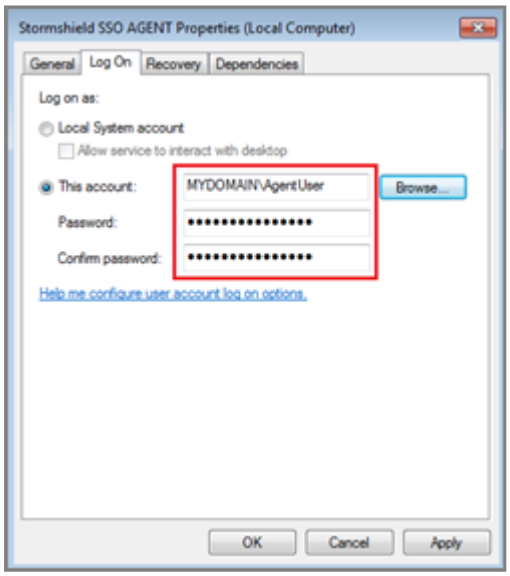
1. Entrez **Services** dans la case de recherche.
2. Appuyez sur la touche **Entrée** du clavier.
3. Double cliquez sur le service **Stormshield SSO AGENT**.
4. Dans l'onglet **Général**, vérifiez que le service est configuré en mode **Automatique** lors du démarrage de Windows.

5. Dans la partie **État du service**, cliquez sur le bouton **Démarrer**.



Si SN SSO Agent 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. Pour plus d'informations, reportez-vous à la section Paramétrer un accès sur l'Active Directory.



Configurer le firewall SN

Pour configurer SN SSO Agent sur votre firewall SN, connectez-vous à l'interface web d'administration du firewall à l'adresse : https://*adresseIP_du_firewall*/admin.

Créer les objets réseau

Vous devez créer les **Objets réseau** correspondant aux machines hébergeant les **SN SSO Agent** et aux **contrôleurs de domaine**, si vous en avez plusieurs.

1. Rendez-vous dans le module **Configuration** > **Objets** > **Objets réseau**.
2. Cliquez sur **Ajouter**.
3. Dans l'assistant, assurez-vous d'être positionné sur l'onglet **Machine**.
4. Entrez le nom du SN SSO Agent ou du contrôleur de domaine dans le champ **Nom de l'objet**.
5. Renseignez l'adresse IPv4 de la machine. Pour sa résolution DNS, nous recommandons une utilisation **statique** (adresse IP fixe). Il est cependant possible, selon votre configuration, d'utiliser une résolution dynamique (DHCP changeant l'adresse IP à chaque connexion).
6. L'adresse MAC de la machine n'est pas requise. Renseignez-la seulement si cela est nécessaire à votre configuration.

Configurer les annuaires Active Directory

Il est nécessaire de configurer les annuaires Active Directory correspondants aux différents SN SSO Agent (5 maximum) précisés dans les méthodes d'authentification gérées par le firewall. Cette configuration permet 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.

La configuration des annuaires Active Directory se réalise dans le module **Configuration** > **Utilisateur** > **Configuration des annuaires**.

Configurer la méthode et la politique d'authentification

Configurer la méthode d'authentification

1. Rendez-vous dans le module **Configuration** > **Utilisateurs** > **Authentification**, onglet *Méthodes disponibles*.
2. Cliquez sur **Ajouter une méthode** ou **Activer une méthode** (selon la version installée sur le firewall SNS).
3. Sélectionnez **Agent SSO** dans le menu déroulant.
4. Dans la partie de droite, pour le champ **Nom de domaine**, sélectionnez dans la liste déroulante le domaine Active Directory associé au SN SSO Agent.
5. Poursuivez ensuite la configuration zone par zone selon les éléments ci-dessous.

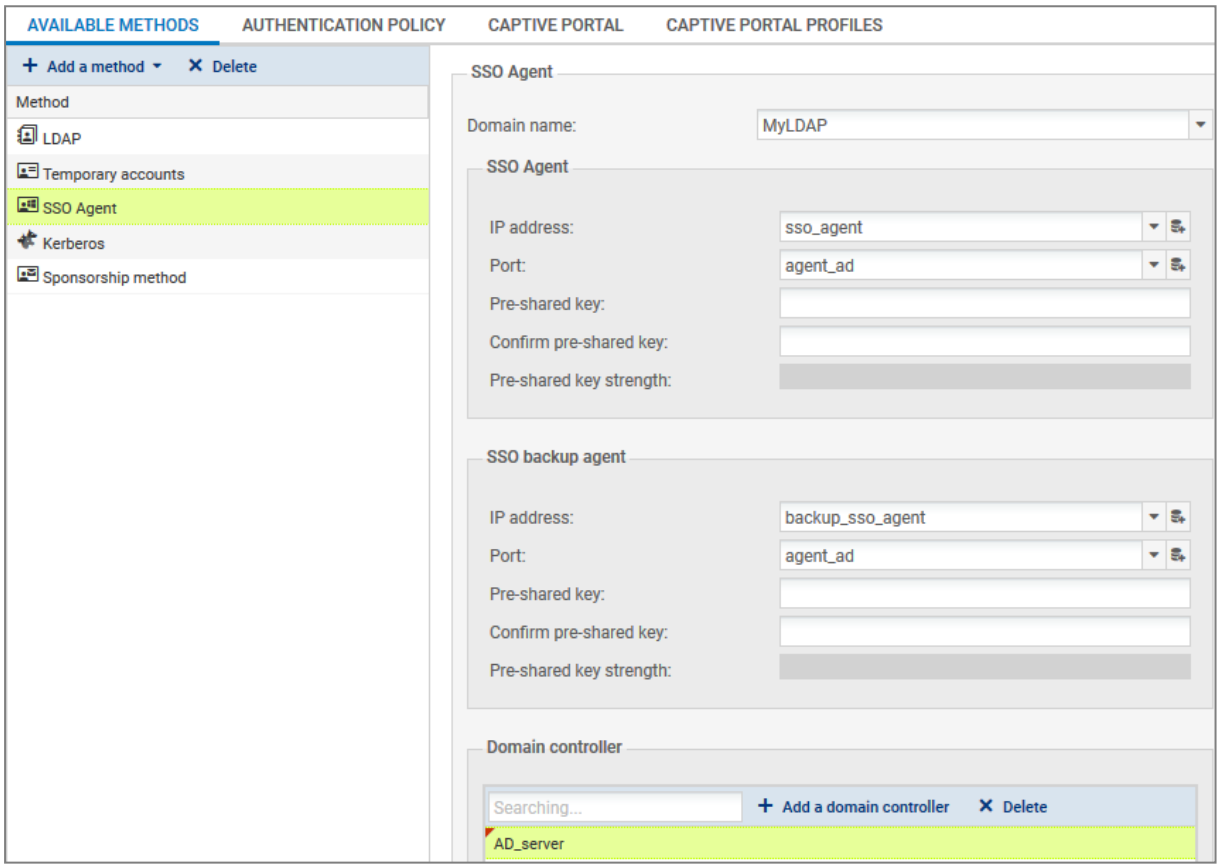
Zone "Agent SSO"

Renseignez les informations du SN SSO Agent principal :

- **Adresse IP** : sélectionnez dans le menu déroulant l'**objet réseau** correspondant à la machine où est installée le SN SSO Agent.

- **Port** : par défaut, le port "agent_ad" est sélectionné, correspondant au port 1301. Le protocole utilisé est TCP.
- **Clé pré-partagée** (mot de passe) : renseignez la clé définie lors de l'installation de SN SSO Agent.
  Cette clé est utilisée pour le chiffrement en SSL des échanges entre SN SSO Agent 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 SN SSO Agent de secours (optionnel).



Zone "Contrôleur de domaine"

Vous devez ajouter tous les contrôleurs qui régissent le domaine. Ceux-ci doivent au préalable être enregistrés dans la base **Objets réseau** du firewall.

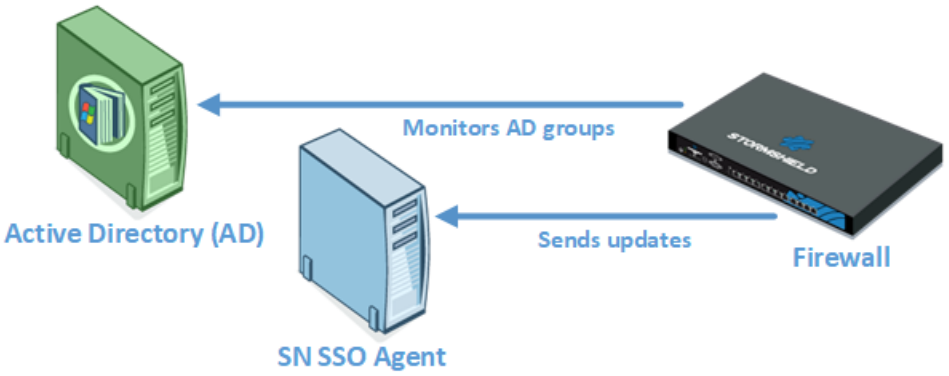
Si plusieurs contrôleurs de domaine régissent le domaine, il est impératif que le compte utilisé par le SN SSO Agent soit un compte dédié appartenant au domaine ayant les droits décrits dans la section Paramétrer un accès sur l'Active Directory. Ces droits s'appliquent sur tous les contrôleurs de domaine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

Zone "Configuration avancée"

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 minutes ou heures et est par défaut fixé à 10 heures.

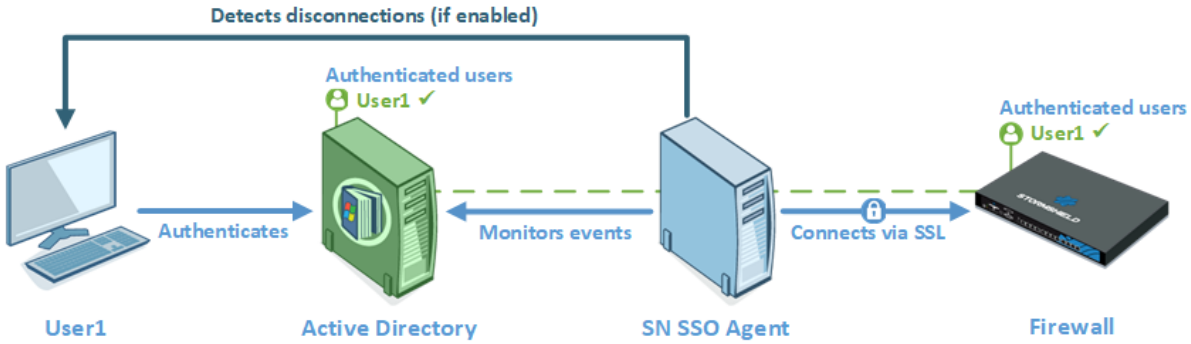
Délai de mises à jour des groupes d'utilisateurs : pour chaque annuaire Active Directory configuré sur le firewall (**Configuration des annuaires**), le firewall consulte les éventuelles modifications apportées aux **groupes de l'annuaire LDAP**. Il met à jour sa configuration de

l'annuaire, puis renvoie ces informations au SN SSO Agent.
Ce seuil est à définir en minutes ou heures et est par défaut fixé à 1 heure.



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. 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.

Ce test des machines connectées au firewall s'effectue soit par méthode **PING**, soit par **Base de registre**.



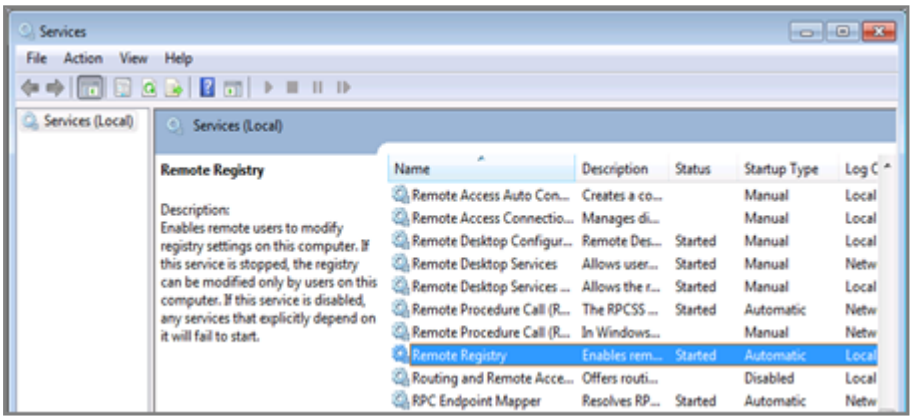
- **PING** : SN SSO Agent teste l'accessibilité de toutes les machines authentifiées sur le firewall toutes les 60 secondes par défaut.
  Dans le cas d'une réponse "*host unreachable*" ou d'absence de réponse d'une adresse IP après un délai défini ci-après, le SN SSO Agent envoie une demande de déconnexion 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

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

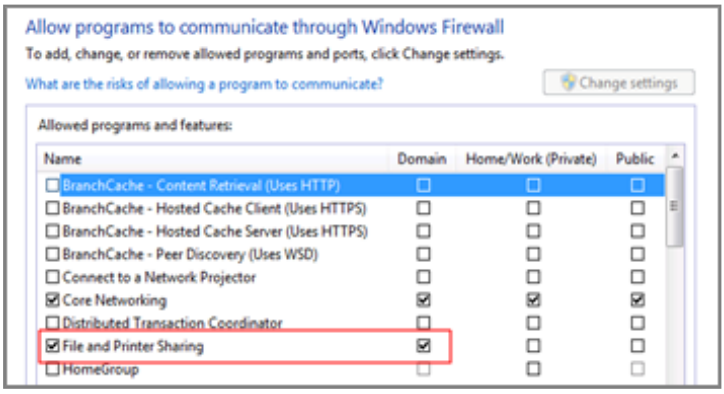
- **Base de registre** : cette méthode permet par exemple de détecter une session fermée sur une machine toujours allumée. Dans le cas d'une réponse positive au test (PING), le SN SSO Agent se connecte à distance sur la machine et vérifie dans la **Base de registre** la liste des utilisateurs ayant une session ouverte sur la machine. Cela permet de mettre à jour sa table des utilisateurs authentifiés.

  Pour mettre en oeuvre la méthode par **Base de registre**, les conditions suivantes doivent être respectées :

  - Le compte associé au SN SSO Agent doit avoir **les droits d'administration sur toutes les machines authentifiées sur le firewall** et doit appartenir au groupe **Administrateur du serveur Active Directory** ou être défini en tant qu'**administrateur local sur les machines supervisées** (voir la section Paramétrer un accès sur l'Active Directory).
  - 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**.



  - 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**.



  - 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). Consultez la section Changement d'adresse IP des **Cas spécifiques** pour plus d'informations.

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 ou minutes 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. Le SN SSO Agent 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 au SN SSO Agent de ne pas prendre en compte leur authentification. Modifiez-la si nécessaire.

Configurer la politique d'authentification

Pour autoriser le trafic dédié à la méthode d'authentification **Agent SSO** configurée, vous devez définir des règles dans la **Politique d'authentification**.

Ajouter une nouvelle règle standard

1. Rendez-vous dans le module **Configuration** > **Utilisateurs** > **Authentification**, onglet *Politique d'authentification*.
2. Cliquez sur **Nouvelle règle**.
3. Sélectionnez **Règle standard** pour lancer l'assistant de création.
4. 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*.
5. Onglet **Source** : cliquez sur **Ajouter un objet** afin de cibler l'origine (source) du trafic concerné par la règle. Cela peut être l'objet correspondant aux réseaux internes (exemple : *network_internals*).

   La méthode d'authentification **Agent SSO** se base sur les événements d'authentification collectés par les contrôleurs de domaine. Ceux-ci n'indiquant pas l'origine du trafic, la politique d'authentification ne peut être spécifiée avec des interfaces.
6. Onglet **Méthodes d'authentification** : cliquez sur **Activer une méthode** et sélectionnez dans la liste déroulante, les méthodes d'authentification à appliquer au trafic concerné par la règle.
   Elles 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.
   La **Méthode par défaut** peut être modifiée en dessous du tableau des règles de la politique d'authentification.
7. Cliquez sur **OK** puis sur **Appliquer**.

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 du SN SSO Agent 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.

Vérifier le fonctionnement de SN SSO Agent

Pour vérifier que le SN SSO Agent est correctement installé et configuré, vous pouvez :

- Consulter les logs sur la machine hôte,
- Consulter les logs sur l'interface d'administration du firewall,
- Vérifier l'état du service Stormshield SSO Agent,
- Vérifier la configuration du Pare-feu Windows.

Consulter les logs sur la machine hôte

Les logs enregistrent les communications entre le SN SSO Agent et les firewalls SN. Les informations de connexion des utilisateurs de l'Active Directory sont collectées lorsque le SN SSO Agent envoie ces informations au firewall.

SN SSO Agent crée des fichiers de logs sur la machine hôte dans le répertoire suivant :

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

> **NOTE**
> La taille maximale d'un fichier est de 1Mo. Le dossier peut contenir un maximum de 100Mo, soit 100 fichiers de logs. Quand le dossier atteint la taille maximum, le fichier de logs le plus ancien est supprimé.
> Ce fichier, qui permet le débogage du service, est nécessaire lors d'une assistance technique auprès de notre Technical Assistance Center.

Double-cliquez sur un fichier de logs pour l'ouvrir, par exemple **stormshieldssoagent.log**. Il peut contenir les informations suivantes :

- La connexion de SN SSO Agent au firewall. Si elle échoue, un message d'erreur est retourné.
- Les règles de la politique d'authentification appliquées aux utilisateurs.
- Les ouvertures de session des utilisateurs. Ces logs contiennent :
  - La date et l'heure de la session,
  - Le nom de l'utilisateur concerné,
  - L'adresse IP de la machine utilisée.
- Les déconnexions des machines associées aux utilisateurs.

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

Consulter les logs sur le firewall

Sur le firewall où est configuré le SN SSO Agent, vous pouvez consulter les logs des utilisateurs qui s'authentifient.

1. Connectez-vous à l'interface d'administration du firewall.
2. Rendez-vous dans le module **Monitoring** > **Logs - Journaux d'audit** > **Utilisateurs**.
3. Dans la fenêtre, affichez les données selon la période de temps souhaitée.

Vérifier le service Stormshield SSO Agent

Vérifiez l'état et les propriétés du service **Stormshield SSO Agent** dans les services Microsoft Windows.

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

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". L'utilisateur doit avoir les **Droits administrateur** sur la machine pour modifier les **Services**.

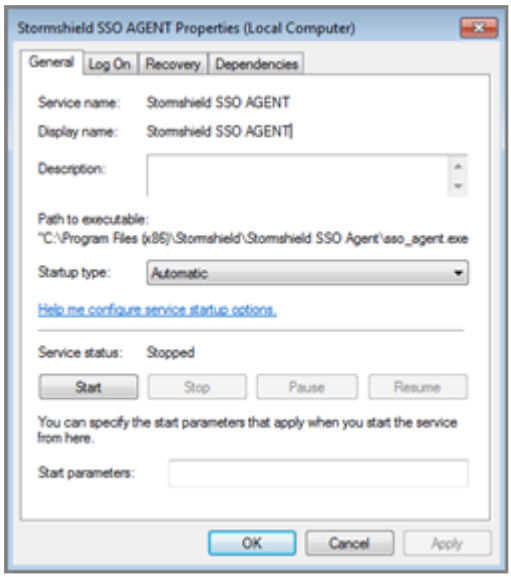
Vérifier les propriétés du service Stormshield SSO Agent

Double cliquez sur le service **Stormshield SSO Agent** pour afficher les propriétés du service.

Selon les informations ci-dessous et ce que vous constatez, modifiez les propriétés du service si nécessaire.

- 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 et mot de passe sur le domaine.
- Onglet **Récupération** : cela permet de configurer le service de SN SSO Agent s'il est arrêté. Par défaut, aucune modification n'est nécessaire.

- Onglet **Dépendances** : le service **Stormshield SSO Agent** ne dépend d'aucun autre service. Par défaut, aucune modification n'est nécessaire



Vérifier la 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

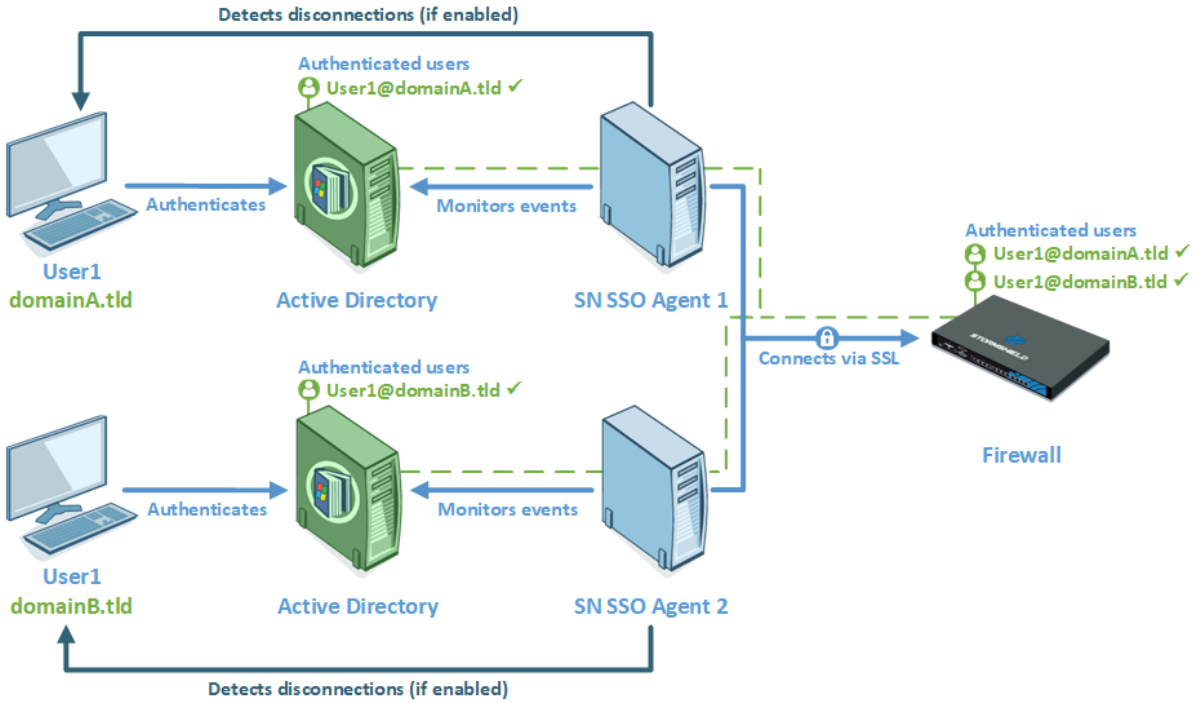
Cette section aborde des cas différents que celui mettant en œuvre un firewall unique dans un seul domaine Active Directory.

Firewalls multiples

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

Domaines multiples (annuaires différents)

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



Approbation de domaine

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

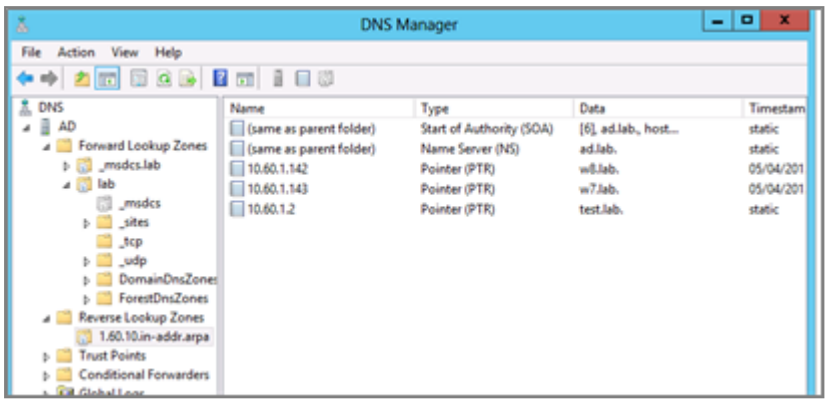
Sur une forêt Active Directory intégrant des sous domaines (par exemple *company.int* et son sous domaine *lab.company.int*), les relations d'approbation permettent d'utiliser les identifiants d'un domaine pour accéder aux ressources d'un autre domaine.

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

Changement d'adresse IP

Périodiquement le SN SSO 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.



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 :

SN SSO Agent 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 le SN SSO Agent,
- Vérifiez les logs depuis l'interface d'administration du firewall dans le module **Monitoring** > **Logs - Journaux d'audit** > **Utilisateurs** . Pour plus d'informations, reportez-vous à la section Consulter les logs sur le firewall.

Symptôme :

SN SSO Agent ne peut pas se connecter au contrôleur de domaine.

Solutions :

- Vérifiez que le compte associé au SN SSO Agent 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 le SN SSO Agent.

Symptôme :

Aucune authentification sur le firewall.

Solution :

S'il n'y a pas d'utilisateurs authentifiés sur le firewall selon les logs, 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 le SN SSO Agent 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 SN SSO Agent. Pour plus d'informations, reportez-vous à la section Consulter les logs sur la machine hôte.

- 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 le SN SSO Agent ne réussit pas à accéder à une machine, cela est visible dans les traces de SN SSO Agent. Pour plus d'informations, reportez-vous à la section Consulter les logs sur la machine hôte.

- 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 le SN SSO Agent 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 créée. Pour plus d'informations, reportez-vous à la section Changement d'adresse IP des **Cas spécifiques**.

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions relatives à l'Agent SSO sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu