NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN TS AGENT - INSTALLATION ET DÉPLOIEMENT

Produits concernés : SNS 4.7 et versions supérieures, SN TS Agent 1.0.2 et versions supérieures

Dernière mise à jour du document : 30 octobre 2023

Référence : sns-fr-SN_TS_Agent_installation_et_deploiement_note_technique

Table des matières

Historique des modifications

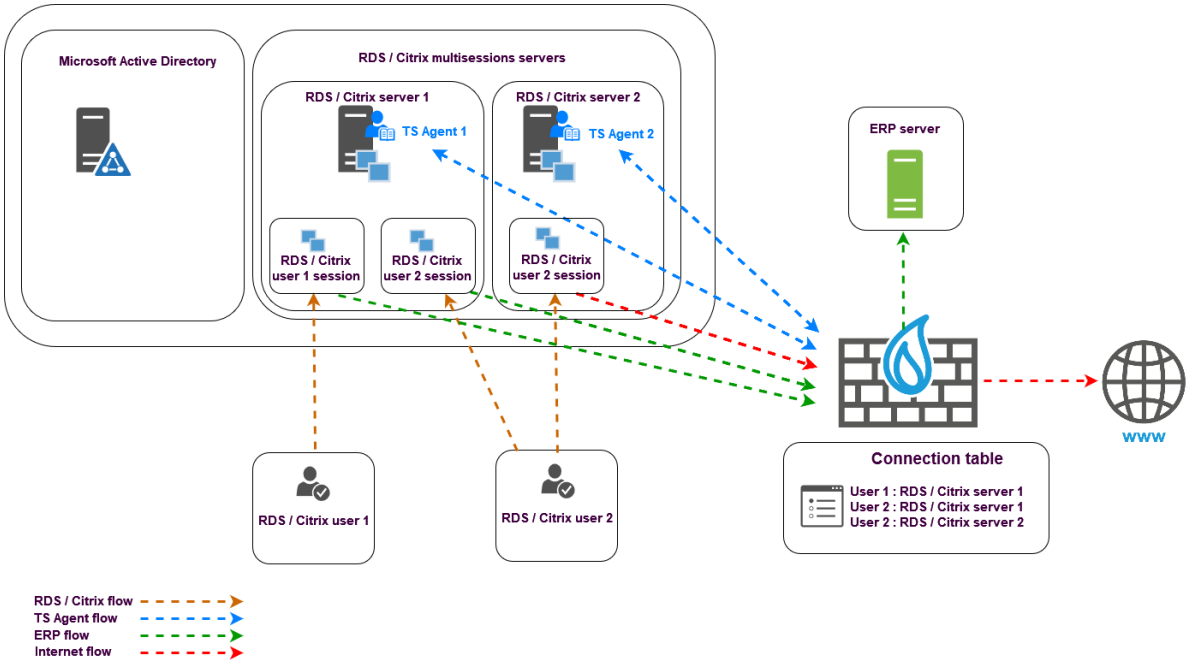
Date	Description
30 octobre 2023	Nouveau document

Avant de commencer

La méthode d'authentification transparente SN TS Agent est destinée à réaliser de l'authentification multi-utilisateurs dans des infrastructures de postes de travail virtuels (VDI : *Virtual Desktop Infrastructure*).

Cette méthode repose sur des échanges entre un service dédié présent sur le firewall SNS (service TSD) et des agents (TS Agents) déployés sur des serveurs Citrix Virtual Apps and Desktops ou Microsoft Remote Desktop Services (RDS).

Chaque utilisateur se présentant avec l'adresse IP du serveur est identifié par le firewall grâce à une plage de ports réseau source (ports réseau supérieurs à 1024) dédiée que lui attribue SN TS Agent.



NOTE

Dans la suite de ce document :

- Les serveurs Citrix Virtual Apps and Desktops seront nommés "serveurs Citrix",
- Les serveurs Microsoft Remote Desktop Services seront nommés "serveurs RDS",
- SN TS Agent pourra également être nommé "Agent TS" en référence à sa dénomination dans l'interface Web d'administration SNS.

Cliquez sur les liens ci-dessous pour plus d'informations sur :

- Microsoft (Remote Desktop Services),
- Citrix Virtual Apps and Desktops.

Compatibilité et limitations

Compatibilité

Stormshield Network Firewall

4.7 et versions supérieures

Systèmes d'exploitation

Windows Server 2016, 2019 et 2022

Composants serveur

Citrix Virtual Apps and Desktop 7 LTSR (2203) Microsoft Remote Desktop Services (RDS)

Spécifications

Nombre maximal d'Agents TS pour un firewall SNS :	100
Nombre maximal d'utilisateurs par Agent TS :	20 à 50 (valeurs recommandées par les éditeurs Citrix et Microsoft pour un serveur multi-sessions).
Nombre maximal de plages de ports par utilisateur :	20 (par défaut : 2)
Nombre de ports par plage :	50 à 1000 (par défaut : 200)

Limitations et précisions sur les cas d'utilisation

- L'authentification transparente de l'Agent TS ne fonctionne pas si de la translation de ports (PAT) ou d'adresses (NAT) est réalisée entre l'Agent TS et le firewall SNS,
- Il n'est pas possible de déconnecter un utilisateur authentifié via l'Agent TS depuis le menu contextuel de la supervision des utilisateurs.
  Une déconnexion forcée d'un utilisateur ne peut être réalisée qu'à l'aide de la commande *sfctl -a* depuis la console du firewall et nécessite un redémarrage du service TSD sur le firewall pour que l'utilisateur concerné puisse à nouveau s'authentifier.

Configurer la méthode d'authentification Agents TS sur le firewall

Placez-vous dans le module **Configuration** > **Utilisateurs** > **Authentification** > onglet **Méthodes disponibles**.

La méthode Agents TS est directement affichée dans la liste des méthodes d'authentification activées (partie gauche de l'écran).

Créer les Agents TS

Dans la grille **Liste des Agents TS** située à droite de l'écran :

1. Cliquez sur **Ajouter**.
2. Pour l'état (interrupteur ON / OFF), il est conseillé de laisser l'Agent TS inactif (OFF) afin de ne pas générer d'alarmes et de logs inutiles.
   Il sera activé une fois l'Agent déployé sur le serveur RDS / Citrix.
3. Dans le champ **Nom de l'Agent TS**, indiquez le nom souhaité pour cet agent (exemple : *RDS-1-TS-AGENT*).
4. Dans le champ **Serveur TS**, sélectionnez ou créez directement l'objet correspondant au serveur RDS / Citrix sur lequel sera installé l'Agent TS (exemple : *RDS-1-SERVER*).
5. Dans le champ **Port**, sélectionnez ou créez directement l'objet correspondant au port de dialogue entre le firewall et l'Agent TS.
   L'objet *agent_ts* (TCP/1303) est proposé par défaut.

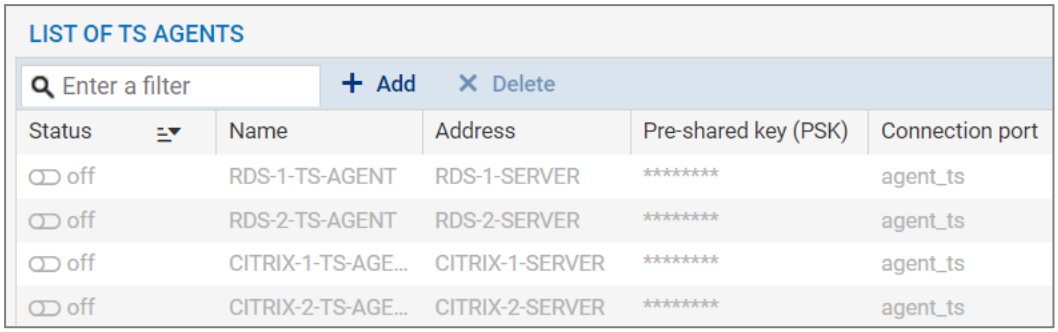
   > **NOTE**
   > Si vous sélectionnez un autre port que celui proposé par défaut, ce port devra également être modifié sur l'Agent TS correspondant (voir la section Identifier / modifier les paramètres de fonctionnement de SN TS Agent).

6. Saisissez et confirmez la **clé pré-partagée** utilisée pour les échanges entre le firewall et l'Agent TS.
   Cette clé pré-partagée doit respecter l'entropie minimale définie sur le firewall (module **Configuration** > onglet **Configuration générale** > cadre **Politique des mots de passe**).

   > **NOTE**
   > Cette clé peut être modifiée par la suite.
   > Vous devrez également modifier la clé pré-partagée sur l'Agent TS concerné, par le biais de la clé de registre Windows du serveur sur lequel est installé cet Agent TS (voir la section Identifier / modifier les paramètres de fonctionnement de SN TS Agent).

7. Validez en cliquant sur **Appliquer**.
   L'Agent TS est ajouté dans la grille **Liste des Agents TS**.

Recommencez les étapes 1 à 7 pour chaque Agent TS à créer sur le firewall (maximum 100 Agents TS par firewall).



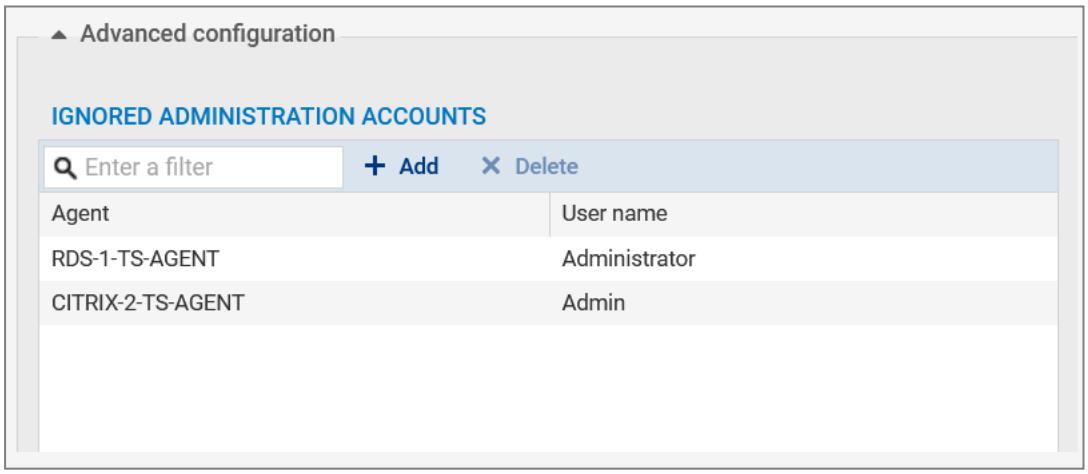
Exclure les comptes d'administration (optionnel)

Il est possible, pour chaque Agent TS configuré, d'exclure des comptes d'administration du mécanisme d'authentification Agent TS.

Dans ce cas, les flux initiés par les comptes administrateurs sélectionnés, bien qu'ils puissent correspondre à des règles de filtrage autorisant la méthode Agent TS, sont bloqués par le firewall.

Pour ajouter un compte s'administration ignoré :

1. Dépliez le cadre **Configuration avancée**,
2. Dans la grille **Comptes d'administration ignorés**, cliquez sur **Ajouter**,
3. Sélectionnez un Agent TS précédemment configuré,
4. Saisissez le nom du compte d'administration à ignorer.



Ajouter la méthode d'authentification Agents TS à la politique d'authentification

NOTE
Il est nécessaire d'avoir préalablement défini sur le firewall l'annuaire LDAP externe Microsoft Active Directory auquel appartiennent les utilisateurs devant être authentifiés par l'Agent TS.

Plus d'informations sur la configuration des annuaires sur un firewall SNS.

Placez-vous dans le module **Configuration** > **Utilisateurs** > **Authentification** > onglet **Politique d'authentification** puis :

1. Cliquez sur **Nouvelle règle** et sélectionnez **Règle standard**.
2. Dans le menu **Utilisateurs** : sélectionnez un utilisateur ou un groupe d'utilisateurs autorisés à utiliser la méthode Agents TS.
3. Dans le menu **Sources** : ajoutez les interfaces réseau sur lesquelles sont connectés les serveurs RDS / Citrix ou des objets / groupes représentant les réseaux ou les serveurs RDS / Citrix (exemple : *RDS1-SERVER*).
4. Dans le menu **Méthodes d'authentification** : ajoutez la méthode Agents TS.

IMPORTANT
Il n'est pas possible de combiner la méthode Agents TS avec une autre méthode d'authentification dans une même règle d'authentification.

5. Validez cette nouvelle règle d'authentification en cliquant sur **OK**.
   La règle est ajoutée à la politique d'authentification mais n'est pas activée par défaut.
6. Dans la grille des règles d'authentification, double-cliquez sur l'état de cette règle pour l'activer.

Status	Source	Methods (assess by order)	One-time password
Enabled	RDS-USERS@documentation.org RDS-2-SERVER RDS-1-SERVER	1 TS agent	N/A
Enabled	CITRIX-USERS@documentation.org CITRIX-2-SERVER CITRIX-1-SERVER	1 TS agent	N/A
Enabled	Any user@documentation.org in	1 LDAP	☐

Les règles sont examinées dans l'ordre de leur numérotation lors d'une authentification. Veillez donc à les organiser à l'aide des boutons **Monter** et **Descendre** selon vos besoins.

Installer ou mettre à jour SN TS Agent

Télécharger SN TS Agent (package *msi*)

1. Connectez-vous à votre espace personnel MyStormshield.
2. Rendez-vous dans **Téléchargements > Téléchargements**.
3. Dans les catégories, sélectionnez **Stormshield Network Security > TS Agent**.
4. Cliquez sur le programme d'installation de TS Agent (fichier *msi*). Le téléchargement se lance automatiquement.
5. Vous pouvez vérifier l'intégrité des binaires récupérés grâce à l'une des commandes suivantes :
   - Système d'exploitation Linux : *sha256sum <filename>*
   - Système d'exploitation Windows : *CertUtil -hashfile <filename> SHA256*

   Comparez ensuite le résultat obtenu avec l'empreinte (hash) indiquée sur MyStormshield. Pour la visualiser, cliquez sur **Afficher** dans la colonne **SHA256** du fichier concerné.

Installer ou mettre à jour manuellement SN TS Agent sur un serveur RDS ou un serveur Citrix

Installer manuellement SN TS Agent

> **NOTE**
> Il est nécessaire de redémarrer le serveur après l'installation de SN TS Agent afin de prendre en compte le nouveau pilote installé. Ce redémarrage vous sera proposé en fin d'installation de l'agent.

Pour installer SN TS Agent sur un serveur RDS ou un serveur Citrix :

1. Ouvrez une session administrateur sur le serveur sur lequel vous souhaitez installer SN TS Agent.
2. Déposez sur ce serveur le fichier *msi* d'installation de SN TS Agent précédemment téléchargé.
3. Double cliquez sur ce fichier *msi* pour lancer l'installation.
4. Cliquez sur **Exécuter** puis sur **Suivant**.
5. Suivez les étapes du programme d'installation :

- Dans la fenêtre **Type de compte**, sélectionnez le compte utilisé pour exécuter ce service (**Compte système local** ou **Compte dédié au service**).
- Dans la fenêtre **Clé de chiffrement,** saisissez et confirmez la clé pré-partagée définie sur le firewall pour cette instance de TS Agent (voir la section Créer les Agents TS de la partie Paramétrer la méthode d'authentification Agents TS sur le firewall).

> **NOTE**
> S'il s'agit d'une réinstallation, vous pouvez cocher la case **Utiliser la configuration existante** pour conserver la clé pré-partagée et les valeurs éventuellement personnalisées des paramètres de la version de SN TS Agent précédemment installée sur le serveur.

- Dans la fenêtre **Prêt à installer Stormshield TS Agent**, cochez la case **Redémarrer maintenant** si vous souhaitez redémarrer le serveur à l'issue de l'installation de SN TS Agent.

IMPORTANT
Si vous n'avez pas demandé le redémarrage immédiat du serveur, pensez à le programmer afin de pouvoir utiliser SN TS Agent.

Mettre à jour manuellement SN TS Agent

NOTE
Il est nécessaire de redémarrer le serveur après la mise à jour de SN TS Agent afin de prendre en compte le nouveau pilote installé. Ce redémarrage vous sera proposé en fin d'installation de l'agent.

Pour mettre à jour SN TS Agent sur un serveur RDS ou un serveur Citrix :

1. Ouvrez une session administrateur sur le serveur sur lequel vous souhaitez mettre à jour SN TS Agent.
2. Déposez sur ce serveur le fichier *msi* d'installation de la nouvelle version de SN TS Agent.
3. Double cliquez sur ce fichier *msi* pour lancer la mise à jour.
4. Cliquez sur **Suivant**.
5. Suivez les étapes du programme d'installation :

- Dans la fenêtre **Type de compte**, sélectionnez le compte utilisé pour exécuter ce service (**Compte système local** ou **Compte dédié au service**).
- Dans la fenêtre **Clé de chiffrement,** cochez la case Utiliser la configuration existante pour conserver la clé pré-partagée et les valeurs éventuellement personnalisées des paramètres de la version de SN TS Agent déjà installée sur le serveur.
- Dans la fenêtre **Prêt à installer Stormshield TS Agent**, cochez la case **Redémarrer maintenant** si vous souhaitez redémarrer le serveur à l'issue de l'installation de SN TS Agent.

IMPORTANT
Si vous n'avez pas demandé le redémarrage immédiat du serveur, pensez à le programmer afin de pouvoir utiliser SN TS Agent.

Installer SN TS Agent sur un serveur RDS ou un serveur Citrix via une GPO Microsoft

Installer SN TS Agent via une GPO Microsoft

NOTE
Dans un environnement Microsoft Active Directory, SN TS Agent peut être déployé de façon automatique par le biais d'une stratégie de groupe (GPO : Global Policy Object).

Copiez le programme d'installation de SN TS Agent (fichier *msi*) dans un répertoire partagé accessible au contrôleur de domaine Microsoft Active Directory ainsi qu'aux serveurs RDS / Citrix.

Créer le package *mst* contenant les arguments indispensables au déploiement de SN TS Agent via GPO

Lors du déploiement de SN TS Agent, deux actions sont nécessaires :

- Préciser la clé pré-partagée (PSK) nécessaire à la communication entre SN TS Agent et le firewall SNS,
- Redémarrer le serveur en fin d'installation de SN TS Agent.

Ceci ne peut être réalisé qu'au travers d'un package *mst*, dans lequel seront précisées les deux propriétés pour réaliser ces actions :

- PKEY_VALUE, précisant la clé pré-partagée,
- REBOOT, positionné sur "Force".

> **NOTE**
> Pour définir le package *mst*, il st nécessaire d'utiliser un outil tiers. La procédure décrite ci-dessous utilise l'outil Microsoft *Orca* disponible dans les composants du kit de développement logiciel (SDK) Microsoft Windows Installer.

Depuis une machine disposant de l'outil Microsoft *Orca* (poste administrateur, contrôleur Microsoft Active Directory...) et accédant au répertoire partagé contenant le programme d'installation de SN TS Agent (fichier *msi*) :

1. Faites un clic droit sur le package *msi* de SN TS Agent et choisissez **Edit with Orca**.
2. Cliquez sur **Transform** > **New transform** et sélectionnez le package *msi* de l'Agent TS.
3. Sélectionnez la table **Property**.
4. Faites un clic droit et choisissez **Add Row**.
5. Pour le champ **Property**, tapez *PKEY_VALUE*.
6. Pour le champ **Value** de la propriété *PKEY_VALUE*, indiquez la valeur de la clé pré-partagée.
7. Validez en cliquant sur **OK**.
8. Répétez les étapes 4 à 7 avec les valeurs suivantes :
   - **Property** : *REBOOT*,
   - **Value** : *Force*.
9. Cliquez sur **Transform** > **Generate Transform**.
10. Choisissez un nom pour le package mst (exemple : SN_TS_AGENT.mst) et enregistrez-le dans le même répertoire que le package *msi* d'installation de SN TS Agent.
11. Fermez l'éditeur *Orca* en cliquant sur **File** > **Exit**.

Créer la GPO de déploiement des packages *msi* et *mst* de SN TS Agent

Sur le sur le contrôleur de domaine Microsoft Active Directory destiné à créer la GPO :

1. Lancez le gestionnaire de serveur.
2. Dans la barre supérieure de menu, cliquez sur **Outils** puis sur **Gestion des stratégies de groupe**.
3. Dans la liste de gauche, faites un clic droit sur le nom du domaine Microsoft Active Directory et sélectionnez **Créer un objet GPO dans ce domaine, et le lier ici...**
4. Nommez la GPO et validez en cliquant sur **OK** (exemple : *SN TS Agent*).
5. Dans la liste de gauche, faites un clic droit sur le nom de la GPO que vous venez de créer et sélectionnez **Modifier**.
   La fenêtre d'édition de la GPO s'ouvre.

6. Dans le menu de gauche de la GPO, dépliez le menu **Configuration ordinateur** > **Stratégies** > **Paramètres du logiciel**.
7. Faites un clic droit sur **Installation de logiciel** et sélectionnez **Nouveau** > **Package**. Sélectionnez le package *msi* d'installation de SN TS Agent.
8. Choisissez le mode **Avancé** et cliquez sur **OK**.
   La fenêtre d'édition de la GPO s'ouvre.
9. Vous pouvez renommer cette instance d'installation si vous le souhaitez (*Stormshield TS Agent 1.0.0* par exemple).
10. Dans l'onglet **Modifications**, cliquez sur **Ajouter...** , sélectionnez le package *mst* précédemment créé (*SN_TS_AGENT.mst* dans l'exemple) et cliquez sur Ouvrir.
    Le package *mst* sélectionné est désormais associé à la GPO d'installation de SN TS Agent.
11. Validez en cliquant sur **OK**.

Ce package d'installation de TS Agent est désormais prêt à être déployé sur les machines du domaine Microsoft Active Directory.

La GPO s'appliquera au prochain redémarrage des machines concernées (serveurs RDS / Citrix).

Mettre à jour à jour SN TS Agent via une GPO Microsoft

Sur le contrôleur de domaine Microsoft Active Directory :

1. Lancez le gestionnaire de serveur.
2. Dans la barre supérieure de menu, cliquez sur **Outils** puis sur **Gestion des stratégies de groupe**.
3. Dans la liste de gauche, faites un clic droit sur le nom de la GPO concernée et sélectionnez **Modifier**.
   La fenêtre d'édition de la GPO s'ouvre.
4. Dans le menu de gauche de la GPO, dépliez le menu **Configuration ordinateur** > **Stratégies** > **Paramètres du logiciel**.
5. Faites un clic droit sur **Installation de logiciel** et sélectionnez **Nouveau** > **Package**. Sélectionnez le nouveau package *msi* d'installation de SN TS Agent.
6. Choisissez le mode **Avancé** et cliquez sur **OK**.
   La fenêtre d'édition de la GPO s'ouvre.
7. Vous pouvez renommer cette instance d'installation si vous le souhaitez (*Stormshield TS Agent 1.0.2* par exemple).
8. Dans l'onglet **Modifications**, cliquez sur **Ajouter...** , sélectionnez le package *mst* précédemment créé (*SN_TS_AGENT.mst* dans l'exemple) et cliquez sur Ouvrir.
   Le package *mst* sélectionné est désormais associé à la GPO d'installation de la mise à jour de SN TS Agent.
9. Dans l'onglet **Mises à niveau**, l'instance d'installation du précédent package Stormshield TS Agent (nommée Stormshield TS Agent 1.0.0 dans l'exemple) est affichée avec la mention **Mettre à niveau**. Sélectionnez-la et cliquez sur **Supprimer**. Il est en effet nécessaire de modifier cette propriété pour une mise à jour correcte de SN TS Agent.
10. Cliquez sur **Ajouter...**, sélectionnez le package de mise à jour puis cochez l'option **Désinstaller le package existant, puis installer le package de mise à niveau**.
11. Cliquez sur **OK** pour valider.
    Dans l'onglet **Mises à niveau**, l'instance d'installation Stormshield TS Agent 1.0.0 est désormais associée à l'action **Remplacer**.
12. Cliquez sur **OK** pour valider.

Ce package de mise à jour de TS Agent est désormais prêt à être déployé sur les machines du domaine Microsoft Active Directory.

La GPO s'appliquera au prochain redémarrage des machines concernées (serveurs RDS / Citrix).

Identifier / modifier les paramètres de fonctionnement de SN TS Agent

La version 1.0 de SN TS Agent ne dispose pas d'une interface de configuration : les paramètres de fonctionnement de SN TS Agent sont consultables dans la base de registre du serveur sur lequel il est installé.

Pour les consulter / modifier ces paramètres :

1. Ouvrez une session administrateur sur le serveur sur lequel est installé SN TS Agent.
2. Ouvrez la base de registre du serveur.
3. Positionnez-vous dans : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StormshieldRdsDrv\Parameters.

Les paramètres du pilote de l'Agent TS sont les suivants :

Paramètre	Description
ExhaustedPortAction	Action effectuée par l'Agent TS lorsque plus aucun port n'est disponible pour une nouvelle connexion. Les valeurs possibles sont : • **Pass** : la connexion est autorisée et se voit affecter un port issu de la plage [EphemeralPortMin-EphemeralPortMax]. • **Block** : la connexion est bloquée. • Valeur par défaut : **block**.
PortsPerRange	Nombre de ports inclus dans chaque plage de ports affectée à un utilisateur : • Minimum : 50, • Maximum : 1000, • Valeur par défaut : 200.
RangePerUser	Nombre de plages de ports affectées à un utilisateur : • Minimum : 1, • Maximum : 20, • Valeur par défaut : 2.
ReservedSystemPorts	Ports compris dans l'intervalle [TotalPortsRangeLow-TotalPortsRangeHigh] devant être réservés au fonctionnement du système. Ils ne pourront pas être affectés à un utilisateur. Il s'agit de chaînes sous la forme «aaaa-bbbb ». Plusieurs chaînes peuvent être définies. **EXEMPLE** • 1025-1025 : pour exclure le port 1025, • 1025-1358 : pour exclure la plage de ports [1025-1358].

TcpTimedWaitDelay	Délai (en secondes) entre la fermeture d'une connexion et le moment où le port associé est de nouveau disponible : • Minimum : 30, • Maximum : 300, • Valeur par défaut : 240.
TotalPortsRangeLow	Borne inférieure de la plage de ports attribuée à un utilisateur. • Minimum : 1024, • Valeur par défaut : 1024.
TotalPortsRangeHigh	Borne supérieure de la plage de ports attribuée à un utilisateur. • Maximum : 49151, • Valeur par défaut : 49151.
MaximumNumberRequests	Nombre de requêtes pouvant être traitées en simultanément dans le pilote. Cette valeur est à ajuster en fonction de la capacité mémoire du serveur. • Minimum : 1, • Maximum : 65535, • Valeur par défaut : 512. **NOTE** La valeur 0 désactive cette limitation du nombre de requêtes simultanées. Il est fortement recommandé de ne pas désactiver cette limitation : ceci pourrait entraîner une surconsommation de la mémoire du serveur RDS / Citrix.

4. Positionnez-vous dans : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\stormshield-rds-service\Parameters.

Les paramètres du service Agent TS sont les suivants :

Paramètre	Description
PSK	Clé pré-partagée pour les échanges avec le firewall SNS. Cette clé est renseignée lors de l'installation de SN TS Agent. **NOTE** Cette clé de registre doit être modifiée si la clé pré-partagée est changée sur le firewall SNS.
EphemeralPortMin	Borne inférieure de la plage de ports additionnels attribuables à un utilisateur lorsque le paramètre **ExhaustedPortAction** est positionné sur **pass** : • Minimum : 49152, • Maximum : 65535, • Valeur par défaut : 49152.

EphemeralPortMax	Borne supérieure de la plage de ports additionnels attribuables à un utilisateur lorsque le paramètre **ExhaustedPortAction** est positionné sur **pass** : • Minimum : 49152, • Maximum : 65535, • Valeur par défaut : 65535.
LogLevel	Niveau de verbosité des logs pour les communications entre l'agent et le firewall. Ces logs sont consultables dans l'observateur d'événements du serveur sur lequel l'agent est installé : • Minimum : 1 (erreurs uniquement), • Maximum : 3 (erreurs, informations et debug). • Valeur par défaut : 2 (erreurs et informations).
ServerPort	Port de communication avec le firewall SNS. Ce port est TCP/1303 par défaut : il correspond à l'objet réseau prédéfini *agent_ts* sur le firewall SNS. **NOTE** Cette clé de registre doit être modifiée si le port de connexion déclaré sur le firewall SNS est différent de l'objet *agent_ts* (TCP/1303).
SNS Timeout	Temps d'attente (en secondes) avant que le firewall ne soit considéré par l'Agent TS comme injoignable. Une fois ce délai atteint, l'Agent TS coupe la communication avec le firewall. Il conserve alors toutes les informations concernant les utilisateurs authentifiés et les transmet au firewall lorsque celui-ci parvient à rétablir la connexion avec l'Agent TS. Les valeurs possibles sont : • Minimum : 0, • Maximum : 60, • Valeur par défaut : 2.

NOTE
Toute modification d'une ou plusieurs de ces clés de registre nécessite le redémarrage du serveur pour être prise en compte.

Activer les Agent TS et configurer la politique de filtrage

Activer les Agents TS

Sur le firewall, placez-vous dans le module
Configuration > **Utilisateurs** > **Authentification** > onglet **Méthodes disponibles** :

1. Dans la grille **Liste des Agents TS** située à droite de l'écran, et pour chacun des Agents TS que vous souhaitez activer, double-cliquez sur son état pour le faire passer de *off* à *on*.
2. Cliquez sur **Appliquer** pour prendre en compte cette modification de configuration.

Créer les règles de filtrage

Vous devez créer les règles permettant aux utilisateurs authentifiés par la méthode Agent TS d'accéder aux différentes ressources autorisées. Il peut s'agir de groupes d'utilisateurs ou d'utilisateur uniques.

Il est également important de prévoir des règles "d'exception" permettant aux serveurs RDS / Citrix d'accéder aux ressources de mises à jour de sécurité (Microsoft Windows Update et Antivirus par exemple) sans nécessité d'une authentification préalable.

Un ensemble de règles répondant à ces critères pourrait ressembler à ceci :

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Access to security update resources for RDS and Citrix servers without authentication (contains 1 rules, from 1 to 1)							
	on	pass	RDS-1-SERVER RDS-2-SERVER CITRIX-1-SERVER CITRIX-2-SERVER	Any Web services and IP reputations Microsoft public IPs windowsupdate Microsoft Azure	http https		IPS
Access to production server for groups of users authentified by TS Agent (contains 2 rules, from 2 to 3)							
	on	pass	RDS-USERS	ERP-SERVER	http https		IPS
	on	pass	CITRIX-USERS	ERP-SERVER	http https		IPS
Access to production server for unique user authentified by TS Agent (contains 1 rules, from 4 to 4)							
	on	pass	john.doe	ERP-SERVER	http https		IPS
Access to Internet for unique user authentified by TS Agent (contains 2 rules, from 5 to 6)							
	on	pass	john.doe	Internet	https		IPS

Pour créer une règle d'exception concernant la mise à jour des serveurs

Dans le module **Configuration** > **Politique de sécurité** > **Filtrage et NAT** :

1. Sélectionnez la politique de sécurité à modifier.
2. Placez-vous sur la règle au-dessous de laquelle vous souhaitez créer une nouvelle règle. Vous pourrez déplacer cette règle par la suite à l'aide des flèches ⬆ ⬇ présentes dans la barre d'action.
3. Cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
4. Double-cliquez dans la colonne **Action** de cette nouvelle règle. La fenêtre d'édition de la règle s'ouvre.
5. Cliquez sur le menu de gauche **Général**.
6. Dans le champ **État** : sélectionnez la valeur *On*. Vous pouvez ajouter un commentaire si vous le souhaitez.

7. Cliquez sur le menu de gauche **Action**.
8. Dans l'onglet **Général**, pour le champ **Action**, choisissez *passer*.
9. Cliquez sur le menu de gauche **Source**.
10. Dans l'onglet **Général**, pour le champ **Machines sources**, sélectionnez les serveurs ou les groupes de serveurs autorisés à accéder aux services de mises à jour de sécurité (serveurs *RDS-1-SERVER*, *RDS-2-SERVER*, *CITRIX-1-SERVER* et *CITRIX-2-SERVER* dans cet exemple).
11. Cliquez sur le menu de gauche **Destination**.
12. Dans l'onglet **Général**, pour le champ **Services Web et réputations IP**, sélectionnez les objets *Microsoft public IPs*, *Windows update* et *Microsoft Azure*.
13. Cliquez sur le menu de gauche **Port / Protocole**.
14. Dans le champ **Port destination**, sélectionnez les objets *http* et *https*.
15. Validez la création de la règle de filtrage en cliquant sur **OK**.

Pour créer une règle destinée à un groupe d'utilisateurs ou un utilisateur unique authentifiés par la méthode Agent TS

Dans le module **Configuration** > **Politique de sécurité** > **Filtrage et NAT** :

1. Sélectionnez la politique de sécurité à modifier.
2. Placez-vous sur la règle au-dessous de laquelle vous souhaitez créer une nouvelle règle. Vous pourrez déplacer cette règle par la suite à l'aide des flèches ⬆ ⬇ présentes dans la barre d'action.
3. Cliquez sur **Nouvelle règle** et sélectionnez **Règle simple**.
4. Double-cliquez dans la colonne **Action** de cette nouvelle règle.
La fenêtre d'édition de la règle s'ouvre.
5. Cliquez sur le menu de gauche **Général**.
6. Dans le champ **État** : sélectionnez la valeur *On*.
Vous pouvez ajouter un commentaire si vous le souhaitez.
7. Cliquez sur le menu de gauche **Action**.
8. Dans l'onglet **Général**, pour le champ **Action**, choisissez *passer*.
9. Cliquez sur le menu de gauche **Source**.
10. Dans l'onglet **Général**, pour le champ **Utilisateur**, sélectionnez l'utilisateur ou le groupe d'utilisateurs authentifiés par la méthode Agent TS utilisateur (groupe d'utilisateurs *RDS-USERS@documentation.org* ou CITRIX-USERS@documentation.org ou utilisateur unique john.doe@documentation.org dans cet exemple).

> **NOTE**
> Un seul utilisateur ou un seul groupe d'utilisateurs peut être sélectionné dans une règle de ce type.
> Vous devrez donc créer autant de règles que de groupes d'utilisateurs ou d'utilisateurs uniques authentifiés par la méthode Agent TS et autorisés à accéder à des ressources identiques.

11. Cliquez sur le menu de gauche **Destination**.
12. Dans l'onglet **Général**, pour le champ **Machines destinations**, sélectionnez les machines à rendre accessibles aux utilisateurs authentifiés par la méthode Agent TS (machine *ERP-SERVER* dans cet exemple).
13. Cliquez sur le menu de gauche **Port / Protocole**.

14. Dans le champ **Port destination**, sélectionnez les objets correspondant aux ports à autoriser (objets *http* et *https* dans cet exemple).
15. Validez la création de la règle de filtrage en cliquant sur **OK**.

Répétez cette procédure pour créer les autres règles de filtrage destinées aux utilisateurs authentifiés par la méthode Agent TS.

Lorsqu'un firewall est positionné entre les utilisateurs à authentifier via l'Agent TS et les serveurs RDS / CITRIX

Dans ce cas, il est nécessaire de créer sur ce firewall une règle autorisant les réseaux des utilisateurs concernés à joindre :

- Les serveurs RDS sur le port TCP/3389 (objet *microsoft-ts* sur un firewall SNS),
- Les serveurs Citrix sur le port 1494 correspondant au protocole Citrix ICA (objet *citrix* sur un firewall SNS).

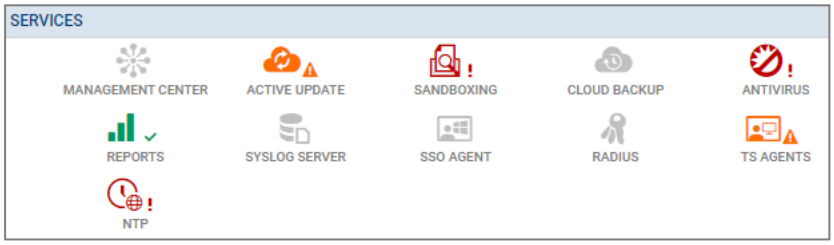
Superviser l'authentification et les Agents TS sur le firewall

Différents types d'événement peuvent être consultés depuis l'interface Web d'administration du firewall.

Superviser l'état des agents

Tableau de bord de supervision

L'état des agents peut être consulté via l'onglet **Monitoring** > **Tableau de bord** > widget **Services** :



Selon l'état des Agents TS, l'icône change de couleur et s'accompagne d'un symbole :

- Icône grise sans symbole : tous les Agents TS configurés sur le firewall sont inactifs.
- Icône verte et symbole ✓ : la communication avec tous les Agents TS configurés et actifs est optimale.
- Icône orange et symbole ⚠ : la communication avec au moins un des Agents TS configurés et actifs présente un problème. En survolant l'icône, une info-bulle vous indique la raison de cet état.
- Icône rouge et symbole ! : la communication avec tous les Agents TS est rompue. En survolant l'icône, une info-bulle vous indique la raison de cet état.

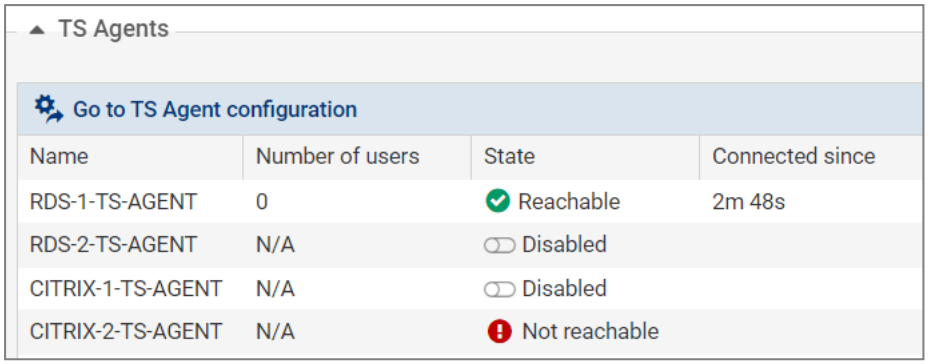
Un double clic sur l'icône Agents TS vous conduit au widget Agents TS du module Supervision Système.

Supervision système

Le détail de l'état de chaque Agent TS peut également être consulté via l'onglet **Monitoring** > module **Supervision système** > widget **Agents TS**.

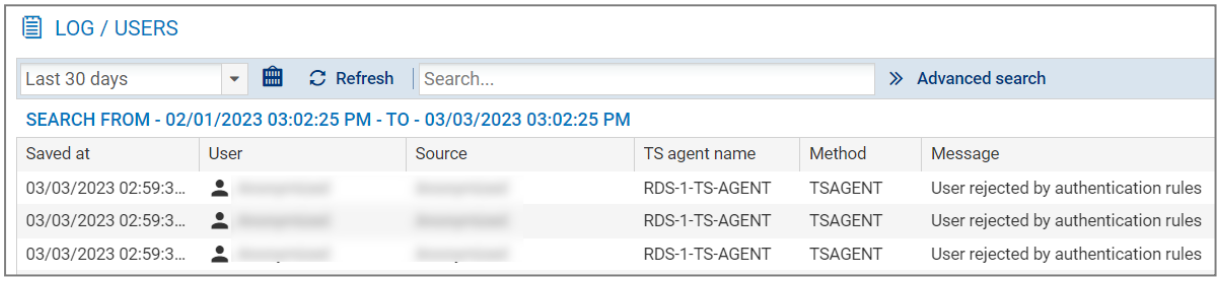
Cette grille présente les informations suivantes pour chaque Agent TS configuré sur le firewall, incluant les agents non activés :

- Le nom de l'Agent TS,
- Le nombre d'utilisateurs connectés par le biais de cet Agent TS,
- L'état de l'Agent TS (**Joignable**, **Non joignable** ou **Désactivé**),
- Le temps écoulé depuis la connexion entre le firewall et l'Agent TS.



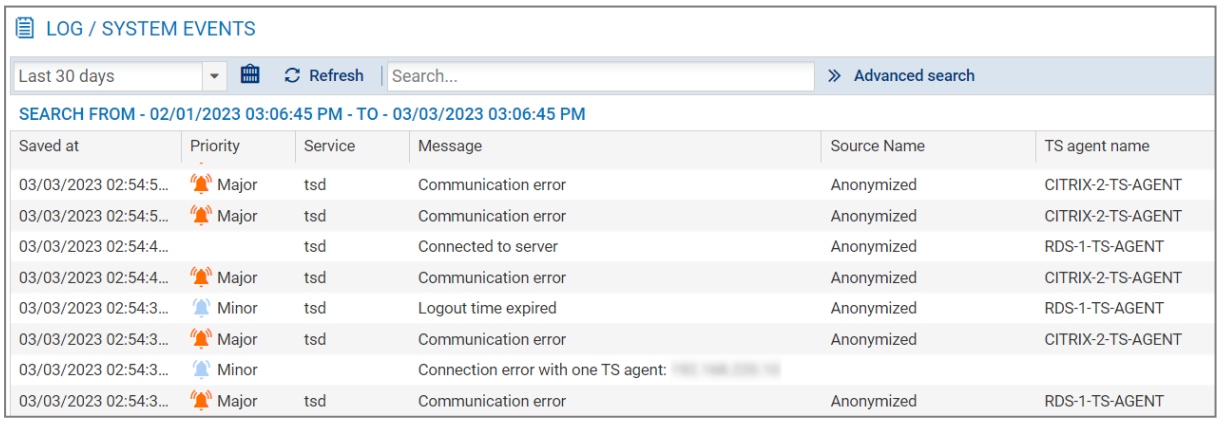
Consulter les logs d'authentification

Consultez les authentifications réussies ou les échecs d'authentification dans l'onglet **Monitoring** > module **Logs - Journaux d'audit** > **Utilisateurs** :



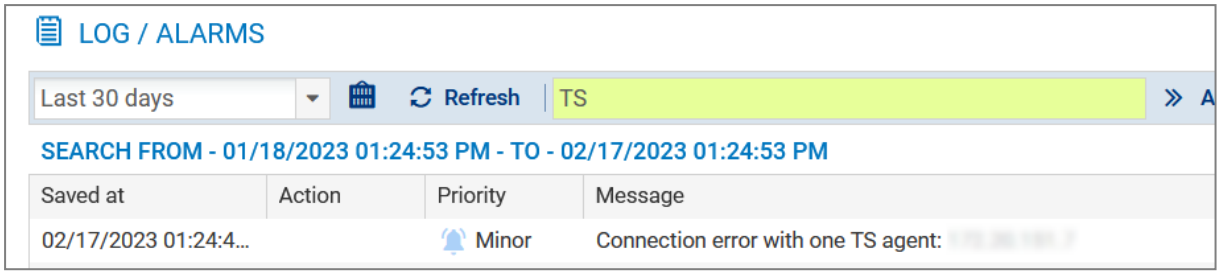
Consulter les logs système

Consultez les événements concernant la communication entre le firewall (service TSD) et les agents TS dans l'onglet **Monitoring** > module **Logs - Journaux d'audit** > **Événements système** :



Consulter les alarmes

Consultez les événements concernant la communication entre le firewall et les agents TS dans l'onglet **Monitoring** > module **Logs - Journaux d'audit** > **Alarmes** :


LOG / ALARMS
Last 30 days
Refresh
TS
SEARCH FROM - 01/18/2023 01:24:53 PM - TO - 02/17/2023 01:24:53 PM
Saved at
Action
Priority
Message
02/17/2023 01:24:4...
Minor
Connection error with one TS agent:

Superviser l'Agent TS sur le serveur

Modifier le niveau de logs de l'Agent TS sur le serveur RDS / Citrix

Si nécessaire, sur le serveur sur lequel est déployé l'Agent TS :

1. Ouvrez la base de registre du serveur.
2. Positionnez-vous dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\stormshield-rds-service\Parameters.
3. Modifiez la valeur de la clé **LogLevel** et validez en cliquant sur **OK**.
4. Redémarrez le serveur (recommandé) ou, à l'unique condition qu'aucun utilisateur ne soit connecté sur le serveur, redémarrez le service *stormshield-rds-service* depuis le **Gestionnaire de Serveur Microsoft**.

Consulter les logs de l'Agent TS sur le serveur RDS / Citrix

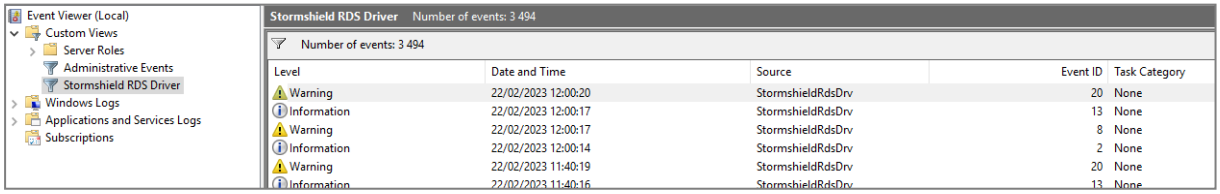
Sur le serveur sur lequel est déployé l'Agent TS :

1. Ouvrez l'**Observateur d'événements**.
2. Dans le menu **Journaux des applications et services**, sélectionnez **Stormshield RDS Service**. La liste des événements survenus pour le service Stormshield RDS Service est affichée.

Consulter les logs du pilote de l'agent RDS

Sur le serveur sur lequel est déployé l'Agent TS :

1. Ouvrez l'**Observateur d'événements**.
2. Faites un clic droit sur **Affichages personnalisés** et sélectionnez **Créez une vue personnalisée**.
3. Cochez **Par source**.
4. Dans la liste **Source d'événements**, sélectionnez **StormshieldRdsDrv** et cliquez sur **OK**.
5. Donnez un nom à votre filtre (exemple : *Stormshield RDS Driver*) et cliquez sur **OK**. Cette nouvelle vue est ajoutée à la liste des **Affichages personnalisés**.

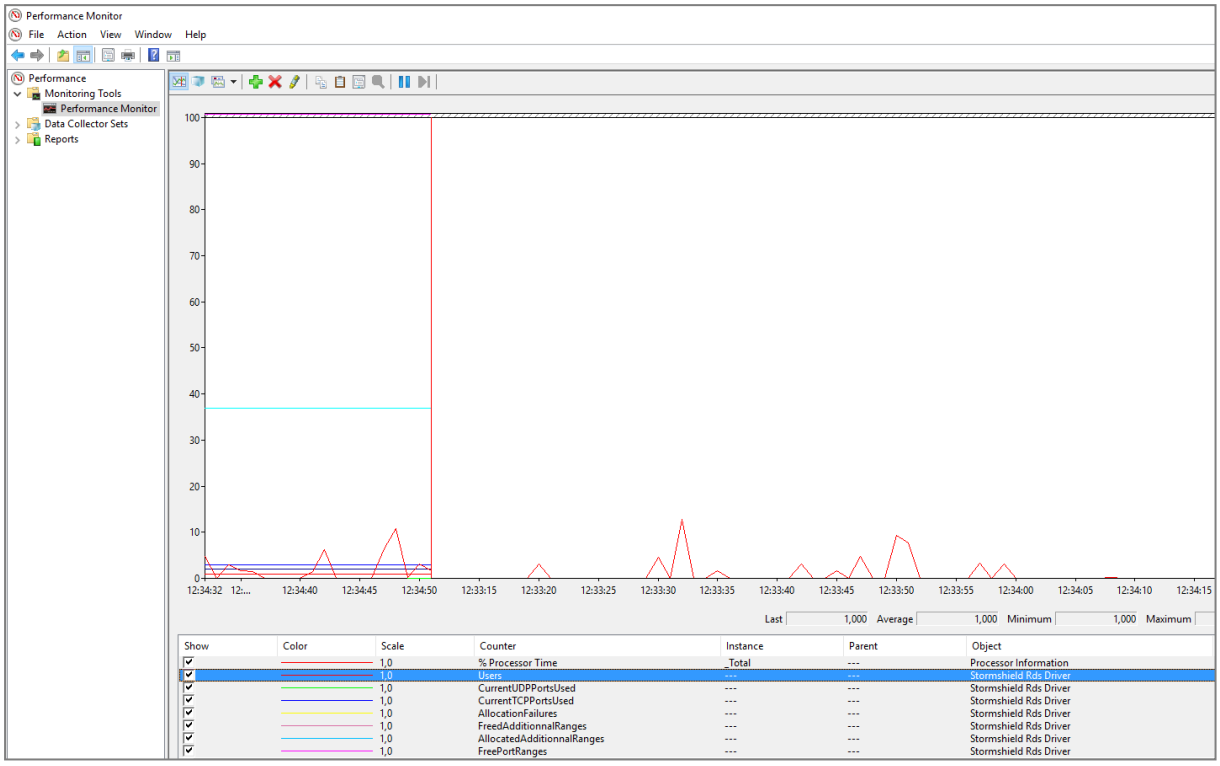


Visualiser les performances du pilote de l'Agent TS dans l'Analyseur de performances Windows

Sur le serveur sur lequel est déployé l'Agent TS :

1. Ouvrez l'**Analyseur de performances**.
2. Cliquez sur **Outils d'Analyse** > **Analyseur de performances**.
3. Cliquez sur la croix verte de la fenêtre de droite.

4. Dans la liste des **Compteurs disponibles**, sélectionnez **Stormshield Rds Driver**.
5. Cliquez sur le bouton **Ajouter** et validez en cliquant sur **OK**.



Diagnostiquer et résoudre les problèmes les plus fréquents

Identifier les ports affectés à un utilisateur

Depuis l'interface Web d'administration

Dans le module **Monitoring** > **Supervision** > **Utilisateurs**, le survol à la souris d'une ligne correspondant à un utilisateur connecté via la méthode Agent TS affiche une info-bulle avec les ports attribués à cet utilisateur.

Depuis la console du firewall

La commande `sfctl -s user -H name=<username> -v` permet de lister les ports affectés par l'Agent TS à un utilisateur donné.

EXEMPLE

```
VMSNSX01B2085A9&gt;sfctl -s user -H name=john.doe -v
User (ASQ):
username            domain              addr                      ports       timeout cookhash    authmethod  flags
john.doe            documentation.org   fe80::dd80:7fa:4148:c2ae  1424-1623   85870   0           TSAGENT     (0x0000)
Memberof: TS-USERS
john.doe            documentation.org   TS-SERVER-1               1424-1623   85870   0           TSAGENT     (0x0000)
Memberof: TS-USERS
```

Le serveur Microsoft Active Directory transmet à l'Agent TS le nom NETBIOS du domaine et non le FQDN

Le serveur Microsoft Active Directory peut parfois transmettre à l'Agent TS le nom NETBIOS du domaine plutôt que le FQDN (exemple : MYDOMAIN au lieu de mydomain.org).

Pour que le firewall puisse faire le lien avec l'annuaire Active Directory de référence, il est possible de créer une correspondance entre le nom NETBIOS et le FQDN du domaine à l'aide de la suite de commandes CLI / Serverd :

```
CONFIG AUTH NETBIOS FQDN ADD NETBIOS=<netbiosname> FQDN=<fqdn>
CONFIG AUTH ACTIVATE.
```

EXEMPLE

```
CONFIG AUTH NETBIOS FQDN ADD NETBIOS=documentation
FQDN=documentation.org
CONFIG AUTH ACTIVATE
```

NOTE

5 correspondances NETBIOS / FQDN peuvent être déclarées sur un même firewall.

Plus d'informations sur la commande **CONFIG AUTH NETBIOS FQDN**.

Pour aller plus loin

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

documentation@stormshield.eu