NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

INSTALLATION ET DÉPLOIEMENT DE L'AGENT TS

Produits concernés : SNS 4.7 et versions supérieures, TS Agent 1.0

Dernière mise à jour du document : 18 mars 2025

Référence : sns-fr-SN_TS_Agent_installation_et_deploiement_note_technique

Table des matières

Historique des modifications

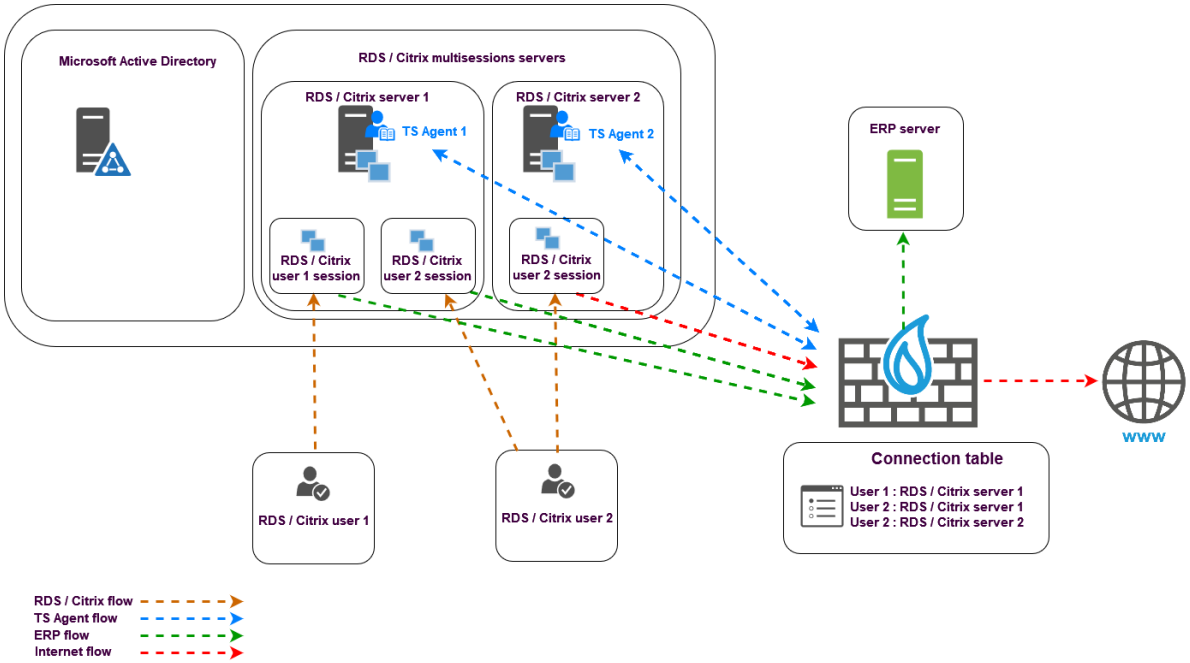
Date	Description
18 mars 2025	• Ajout de trois limitations et précisions sur les cas d'utilisation dans la section "Spécifications et limitations" • Ajout de précisions concernant le choix du port et de la clé pré-partagée dans la section "Configurer la méthode d'authentification Agents TS sur le firewall > Créer les Agents TS" • Les contenus liés à l'installation et à la mise à jour de l'Agent TS disposent à présent de leur propre section distincte dans le document • Ajout de la procédure de mise à jour de l'Agent TS depuis une version 1.0.3 ou inférieure dans la section "Mettre à jour l'Agent TS" • Modification des procédures d'installation et de mise à jour manuelle de l'Agent TS concernant le redémarrage du serveur et la configuration des ports réservés au fonctionnement du système dans la section "Installer ou mettre à jour l'Agent TS" • Ajout du paramètre **ReservedPortAction** et modification de la description des paramètres **ExhaustedPortAction**, **PortsPerRange**, **RangePerUser**, **ReservedSystemPorts**, **TcpTimedWaitDelay**, **TotalPortsRangeLow**, **TotalPortsRangeHigh**, **EphemeralPortMin** et **EphemeralPortMax** dans la section "Identifier / modifier les paramètres de fonctionnement de l'Agent TS" • Le contenu lié à la supervision des utilisateurs connectés par le biais des Agents TS dispose à présent de sa propre section distincte dans le document • Modification de la procédure de consultation des logs du pilote de l'Agent TS dans la section "Superviser l'Agent TS sur le serveur RDS / Citrix" • Ajout du cas du redémarrage du serveur RDS / Citrix alors que des utilisateurs sont connectés dans la section "Résoudre les problèmes" • Ajout de l'annexe "Utiliser le script de configuration des ports réservés au fonctionnement du système"
30 octobre 2023	• Nouveau document

Avant de commencer

La méthode d'authentification transparente "Agents TS" 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 (Agents TS) 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 dédiée que lui attribue l'Agent TS.



NOTE

Dans ce document :

- Les serveurs Citrix Virtual Apps and Desktops sont nommés "serveurs Citrix",
- Les serveurs Microsoft Remote Desktop Services sont nommés "serveurs RDS",
- SN TS Agent est nommé "Agent TS".

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

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

Spécifications et limitations

Compatibilité

Pour plus d'informations, reportez-vous à la section TS Agent du guide *Cycle de vie produits Network Security & Tools*.

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 (2 par défaut)
Nombre de ports par plage	50 à 1000 (200 par défaut)

Limitations et précisions sur les cas d'utilisation

Translation de ports (PAT) ou d'adresses (NAT)

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.

Réception d'un nom de domaine au format NETBIOS

Dans le cas où l'Agent TS reçoit un nom de domaine au format NETBIOS, vous devez définir une correspondance entre ce nom et le nom de domaine Active Directory au format FQDN. Pour plus d'informations, reportez-vous à la section Résoudre les problèmes.

Paramètres de fonctionnement de l'Agent TS

Les paramètres de fonctionnement de l'Agent TS (port d'écoute, plage de ports, clé pré-partagée, etc.) sont consultables dans la base de registre du serveur sur lequel il est installé. Pour plus d'informations, reportez-vous à la section Identifier / modifier les paramètres de fonctionnement de l'Agent TS.

Déconnexion d'un utilisateur authentifié via l'Agent TS

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 peut être réalisée uniquement 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.

Caractères interdits dans l'identifiant d'un utilisateur de l'annuaire LDAP

```
" <tab> & ~ | = * < > ! ( ) \ $ % ? ' ` <space>
```

IMPORTANT
Dans le cas d'un annuaire externe de type Microsoft Active Directory, l'identifiant utilisateur **doit à la fois** respecter les critères énoncés ci-dessus **et** les critères imposés par Microsoft.

Configurer la méthode d'authentification Agents TS sur le firewall SNS

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

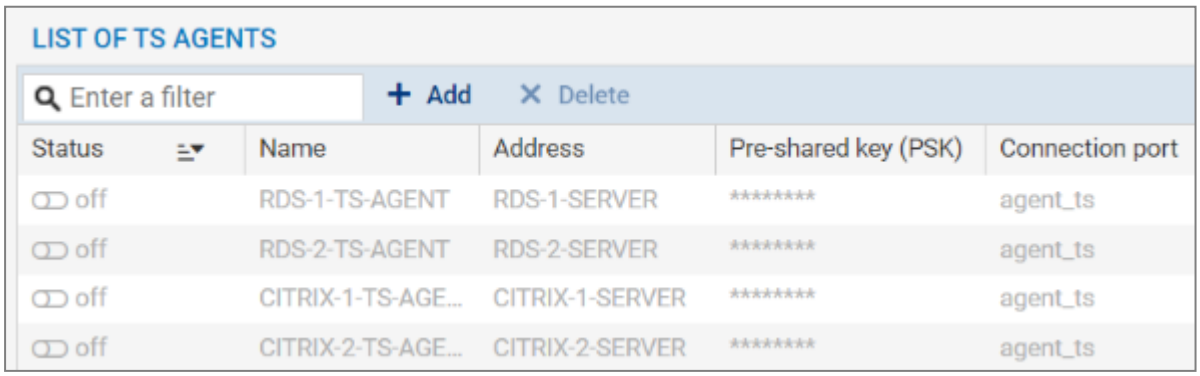
La méthode Agents TS est directement affichée dans la liste des méthodes d'authentification activées à gauche de l'écran. Cliquez sur la méthode Agents TS pour afficher ses informations.

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**, l'objet *agent_ts* (TCP/1303) est proposé par défaut. Ce même port est également renseigné dans la configuration par défaut de l'Agent TS.
   Vous pouvez sélectionner ou créer un autre objet correspondant au port de dialogue entre le firewall et l'Agent TS. Vous devrez alors modifier le paramètre **ServerPort** de l'Agent TS correspondant pour y renseigner le nouveau port sélectionné (voir la section Identifier / modifier les paramètres de fonctionnement de l'Agent TS).
6. Saisissez et confirmez la **clé pré-partagée** utilisée pour les échanges entre le firewall et l'Agent TS. Elle doit respecter l'entropie minimale définie sur le firewall (module **Configuration** > onglet **Configuration générale** > cadre **Politique des mots de passe**). Cette clé peut être modifiée par la suite.
   Vous devrez également renseigner cette clé dans les paramètres de l'Agent TS concerné :
   - Soit lors de son installation (voir la section Installer ou mettre à jour l'Agent TS),
   - Soit après en modifiant le paramètre **PSK** (voir la section Identifier / modifier les paramètres de fonctionnement de l'Agent TS).
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).



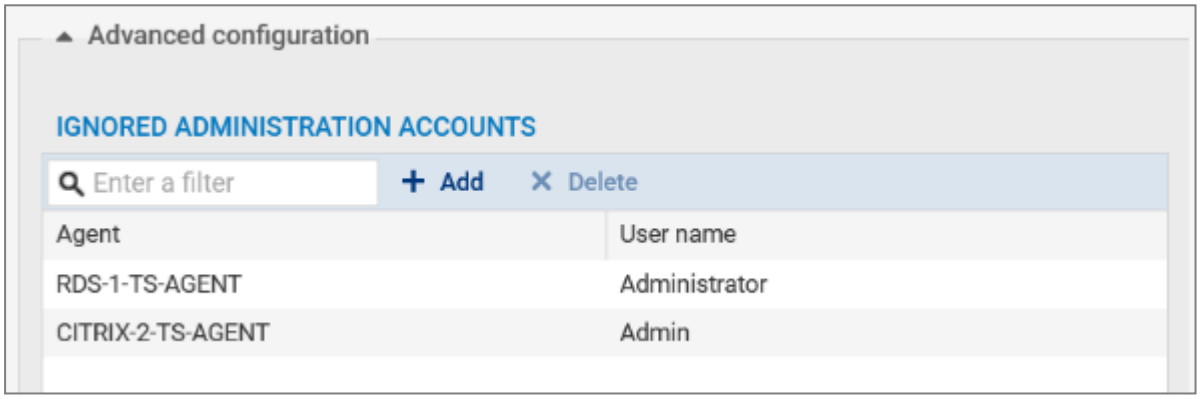
Exclure les comptes d'administration (optionnel)

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 d'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 autorisé 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 : *RDS-1-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 l'Agent TS

Cette section explique comment installer ou mettre à jour l'Agent TS, que ce soit manuellement ou via une GPO Microsoft.

Télécharger le programme d'installation de l'Agent TS (package *MSI*)

Débutez par télécharger le programme d'installation de l'Agent TS (package *MSI*).

1. Connectez-vous à votre espace 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 l'Agent TS

Cette section explique comment installer l'Agent TS manuellement ou via une GPO Microsoft.

Installer l'Agent TS manuellement

1. Ouvrez une session administrateur sur le serveur sur lequel installer l'Agent TS.
2. Déposez le fichier *.msi* d'installation précédemment téléchargé.
3. Double-cliquez sur ce fichier pour lancer l'installation.
4. Cliquez sur **Exécuter** puis sur **Suivant**.
5. Sur le 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**).
6. 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).

   > **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 personnalisées des paramètres de la version de l'Agent TS précédemment installée sur le serveur.

7. Dans la fenêtre **Prêt à installer Stormshield TS Agent**, cliquez sur **Installer**.
8. Vous devez redémarrer le serveur pour finaliser l'installation de l'Agent TS. Si vous ne le redémarrez pas immédiatement, pensez à le programmer afin de pouvoir utiliser l'Agent TS.

> **NOTE**
> Avant de redémarrer le serveur, vous pouvez exécuter un script qui analyse les ports

susceptibles d'entrer en conflit avec l'Agent TS et qui les ajoute à ses paramètres afin de les réserver au fonctionnement du système. Ainsi, ces ports ne pourront pas être attribués à un utilisateur. Vous pouvez utiliser ce script ultérieurement, mais un nouveau redémarrage du serveur sera nécessaire. Pour plus d'informations, reportez-vous à la section Annexe : utiliser le script de configuration des ports réservés au fonctionnement du système.

Installer l'Agent TS via une GPO Microsoft

Dans un environnement Microsoft Active Directory, l'Agent TS peut être déployé de façon automatique par le biais d'une stratégie de groupe (GPO : *Group Policy Objects*). Ce déploiement s'effectue en deux étapes.

Créer un package *MST* contenant les arguments indispensables au déploiement de l'Agent TS

Vous devez au préalable créer un package MST pour intégrer les arguments suivants indispensables au déploiement de l'Agent TS :

- *PKEY_VALUE* précisant la clé pré-partagée (PSK) nécessaire à la communication entre l'Agent TS et le firewall,
- *REBOOT* positionné sur *Force* permettant de redémarrer le serveur en fin d'installation.

Pour cela, vous devez utiliser un outil tiers pour créer le package *MST*. La procédure décrite ci-dessous utilise l'outil Microsoft *Orca* disponible dans les composants du kit de développement logiciel (SDK) Microsoft Windows Installer.

1. Copiez le programme d'installation de l'Agent TS (fichier *.msi*) précédemment téléchargé dans un répertoire partagé accessible au contrôleur de domaine Microsoft Active Directory ainsi qu'aux serveurs RDS / Citrix.
2. Depuis une machine disposant de l'outil Microsoft *Orca* (poste administrateur, contrôleur Microsoft Active Directory...) et accédant au répertoire partagé, faites un clic droit sur le package *MSI* de l'Agent TS et choisissez **Edit with Orca**.
3. Cliquez sur **Transform** > **New transform** et sélectionnez le package *MSI* de l'Agent TS.
4. Sélectionnez la table **Property**.
5. Pour préciser la clé pré-partagée nécessaire à la communication entre l'Agent TS et le firewall SNS :
    1. Faites un clic droit et choisissez **Add Row**.
    2. Dans le champ **Property**, indiquez *PKEY_VALUE*.
    3. Dans le champ **Value**, indiquez la valeur de la clé pré-partagée.
    4. Cliquez sur **OK**.
6. Pour redémarrer le serveur en fin d'installation de l'Agent TS :
    1. Faites un clic droit et choisissez **Add Row**.
    2. Dans le champ **Property**, indiquez *REBOOT*.
    3. Dans le champ **Value**, indiquez *Force*.
    4. Cliquez sur **OK**.
7. Cliquez sur **Transform** > **Generate Transform**.
8. Choisissez un nom pour le package *MST* et enregistrez-le dans le même répertoire que le package *MSI* d'installation de l'Agent TS.
9. Fermez l'éditeur *Orca* en cliquant sur **File** > **Exit**.

Créer la GPO de déploiement des packages *MSI* et *MST* de l'Agent TS

Une fois le package *MST* créé, vous pouvez créer la GPO de déploiement des packages *MSI* et *MST* de l'Agent TS.

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 : *Agent TS*).
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 l'Agent TS.
8. Choisissez le mode **Avancé** et cliquez sur **OK**.
   La fenêtre d'édition de la GPO s'ouvre.
9. Renommez cette instance d'installation si vous le souhaitez en y ajoutant par exemple le numéro de version de l'Agent TS.
10. Dans l'onglet **Modifications**, cliquez sur **Ajouter...** , sélectionnez le package *MST* précédemment créé et cliquez sur **Ouvrir**. Le package *MST* sélectionné est désormais associé à la GPO d'installation de l'Agent TS.
11. Validez en cliquant sur **OK**.

Ce package d'installation de l'Agent TS 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 l'Agent TS

Cette section explique comment mettre à jour l'Agent TS manuellement ou via une GPO Microsoft.

Mettre à jour l'Agent TS depuis une version 1.0.3 ou inférieure

Avant de mettre à jour l'Agent TS en version 1.0.5 ou supérieure, vous devez désinstaller intégralement la version 1.0.3 ou inférieure grâce à un script fourni par Stormshield.

IMPORTANT
Même si vous avez utilisé le programme de désinstallation de l'Agent TS en version 1.0.3 ou inférieure, vous devez suivre cette procédure pour désinstaller intégralement la version.

1. Dans votre espace MyStormshield, rendez-vous dans **Téléchargements > Téléchargements**.
2. Dans les catégories, sélectionnez **Stormshield Network Security > TS Agent**.
3. Cliquez sur le script de désinstallation (fichier *.ps1*) pour le télécharger.

4. Copiez le script sur chaque serveur RDS ou Citrix où un Agent TS est installé.
5. Exécutez le script en tant qu'administrateur.
6. Lors de l'exécution du script, des erreurs peuvent s'afficher si des fichiers de la précédente installation sont déjà supprimés.

Mettre à jour l'Agent TS manuellement

1. Ouvrez une session administrateur sur le serveur sur lequel mettre à jour l'Agent TS.
2. Déposez le fichier *.msi* d'installation de la nouvelle version précédemment téléchargé.
3. Double-cliquez sur ce fichier pour lancer la mise à jour.
4. Cliquez sur **Suivant**.
5. Sur le 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**).
6. 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 l'Agent TS déjà installée sur le serveur.
7. Dans la fenêtre **Prêt à installer Stormshield TS Agent**, cliquez sur **Installer**.
8. Vous devez redémarrer le serveur pour finaliser l'installation de la nouvelle version de l'Agent TS. Si vous ne redémarrez pas immédiatement le serveur, pensez à le programmer afin de prendre en compte le nouveau pilote installé.

> **NOTE**
> Avant de redémarrer le serveur, vous pouvez exécuter un script qui analyse les ports susceptibles d'entrer en conflit avec l'Agent TS et qui les ajoute à ses paramètres afin de les réserver au fonctionnement du système. Ainsi, ces ports ne pourront pas être attribués à un utilisateur. Vous pouvez utiliser ce script ultérieurement, mais un nouveau redémarrage du serveur sera nécessaire. Pour plus d'informations, reportez-vous à la section Annexe : utiliser le script de configuration des ports réservés au fonctionnement du système.

Mettre à jour l'Agent TS via une GPO Microsoft

Dans un environnement Microsoft Active Directory, la mise à jour de l'Agent TS peut être déployée de façon automatique par le biais d'une stratégie de groupe (GPO : *Group Policy Objects*). Ce déploiement s'effectue en deux étapes.

Créer un package *MST* contenant les arguments indispensables au déploiement de la nouvelle version de l'Agent TS

Vous devez au préalable créer un package MST pour intégrer les arguments suivants indispensables au déploiement de la nouvelle version de l'Agent TS :

- *PKEY_VALUE* précisant la clé pré-partagée (PSK) nécessaire à la communication entre l'Agent TS et le firewall,
- *REBOOT* positionné sur *Force* permettant de redémarrer le serveur en fin d'installation.

Pour cela, vous devez utiliser un outil tiers pour créer le package *MST*. La procédure décrite ci-dessous utilise l'outil Microsoft *Orca* disponible dans les composants du kit de développement logiciel (SDK) Microsoft Windows Installer.

1. Copiez le programme d'installation de l'Agent TS (fichier *.msi*) dans un répertoire partagé accessible au contrôleur de domaine Microsoft Active Directory ainsi qu'aux serveurs RDS / Citrix.
2. Depuis une machine disposant de l'outil Microsoft *Orca* (poste administrateur, contrôleur Microsoft Active Directory...) et accédant au répertoire partagé, faites un clic droit sur le package *MSI* de l'Agent TS et choisissez **Edit with Orca**.
3. Cliquez sur **Transform** > **New transform** et sélectionnez le package *MSI* de l'Agent TS.
4. Sélectionnez la table **Property**.
5. Pour préciser la clé pré-partagée nécessaire à la communication entre l'Agent TS et le firewall SNS :
   1. Faites un clic droit et choisissez **Add Row**.
   2. Dans le champ **Property**, indiquez *PKEY_VALUE*.
   3. Dans le champ **Value**, indiquez la valeur de la clé pré-partagée.
   4. Cliquez sur **OK**.
6. Pour redémarrer le serveur en fin d'installation de l'Agent TS :
   1. Faites un clic droit et choisissez **Add Row**.
   2. Dans le champ **Property**, indiquez *REBOOT*.
   3. Dans le champ **Value**, indiquez *Force*.
   4. Cliquez sur **OK**.
7. Cliquez sur **Transform** > **Generate Transform**.
8. Choisissez un nom pour le package *MST* et enregistrez-le dans le même répertoire que le package *MSI* d'installation de l'Agent TS.
9. Fermez l'éditeur *Orca* en cliquant sur **File** > **Exit**.

Modifier la GPO de déploiement des packages *MSI* et *MST* de l'Agent TS

Une fois le package *MST* créé, vous pouvez modifier la GPO de déploiement des packages *MSI* et *MST* de l'Agent TS.

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 l'Agent TS.
6. Choisissez le mode **Avancé** et cliquez sur **OK**.
   La fenêtre d'édition de la GPO s'ouvre.
7. Renommez cette instance d'installation si vous le souhaitez en y ajoutant par exemple le numéro de version de l'Agent TS.
8. Dans l'onglet **Modifications**, cliquez sur **Ajouter...** , sélectionnez le package *MST* précédemment créé et cliquez sur **Ouvrir**. Le package *MST* sélectionné est désormais associé à la GPO d'installation de la mise à jour de l'Agent TS.

9. Dans l'onglet **Mises à niveau**, l'instance d'installation du précédent package de l'Agent TS 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 l'Agent TS.
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. Validez en cliquant sur **OK**.
    Dans l'onglet **Mises à niveau**, l'instance d'installation du précédent package de l'Agent TS est désormais associée à l'action **Remplacer**.
12. Validez en cliquant sur **OK**.

Ce package de mise à jour de l'Agent TS 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 l'Agent TS

L'Agent TS ne dispose pas d'une interface graphique de configuration : ses paramètres de fonctionnement sont consultables dans la base de registre du serveur sur lequel il est installé.

Pour consulter / modifier les paramètres de l'Agent TS :

1. Ouvrez une session administrateur sur le serveur sur lequel est installé l'Agent TS.
2. Ouvrez la base de registre du serveur (*regedit*).

Vous retrouvez dans la base de registre les paramètres du pilote de l'Agent TS et les paramètres du service de l'Agent TS. L'emplacement de ces paramètres est différent.

Paramètres du pilote de l'Agent TS

IMPORTANT
Toute modification des clés de registre du pilote de l'Agent TS nécessite le redémarrage du serveur pour être prise en compte.

Emplacement dans la base de registre :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StormshieldRdsDrv\Parameters

Paramètre	Description / Valeurs possibles
ExhaustedPortAction	Action effectuée par l'Agent TS lorsqu'un utilisateur n'a plus de port disponible dans ses plages de ports pour une nouvelle connexion. • **pass** (par défaut) : la connexion est autorisée par l'Agent TS et un port issu de la plage [**EphemeralPortMin-EphemeralPortMax**] est attribué à l'utilisateur. Ces connexions sont anonymes pour le firewall. Sa politique de filtrage doit laisser passer les connexions réseau anonymes dont les ports sources sont supérieurs ou égaux à la valeur du paramètre **EphemeralPortMin**. Dans le cas contraire, ces connexions seront bloquées par le firewall. • **block** : la connexion est bloquée par l'Agent TS.
ReservedPortAction	Action effectuée par l'Agent TS lorsqu'une application tente d'utiliser un port de la plage de ports réservée aux utilisateurs [**TotalPortsRangeLow-TotalPortsRangeHigh**]. • **block** (par défaut) : la connexion est bloquée par l'Agent TS, sauf si l'utilisateur concerné dispose de ce port dans ses plages de ports attribuées. Dans le cas d'un blocage, un événement est généré dans l'**Observateur d'événements** Windows : `Process [...] has been blocked because it tried to use a port [...] which is reserved by the driver.` • **pass** : la connexion est autorisée par l'Agent TS. Modifier ce paramètre en "*pass*" est considéré comme une configuration avancée, car cela peut entraîner des problèmes d'attribution des ports sur la machine.

Paramètre	Description / Valeurs possibles
PortsPerRange	Nombre de ports inclus dans chaque plage de ports attribuée à chaque utilisateur (200 par défaut). • Minimum : 50, • Maximum : 1000. Si la valeur par défaut est inadaptée, par exemple si certaines applications nécessitent un grand nombre de ports pour fonctionner, vous pouvez la modifier. Ceci permet d'éviter que les utilisateurs se retrouvent à court de ports disponibles, mais réduit le nombre maximal d'utilisateurs sur l'Agent TS.
RangePerUser	Nombre de plages de ports attribuées à un utilisateur (2 par défaut). • Minimum : 1, • Maximum : 20. Si la valeur par défaut est inadaptée, par exemple si certaines applications nécessitent un grand nombre de ports pour fonctionner, vous pouvez la modifier. Ceci permet d'éviter que les utilisateurs se retrouvent à court de ports disponibles, mais réduit le nombre maximal d'utilisateurs sur l'Agent TS.
ReservedSystemPorts	Liste des ports compris dans l'intervalle [**TotalPortsRangeLow-TotalPortsRangeHigh**] devant être réservés au fonctionnement du système. Ces ports ne pourront pas être attribués à un utilisateur. Vous pouvez définir plusieurs chaînes en respectant le format "[aaaaa-bbbbb]". Par exemple : • Pour réserver le port 20025 : [20025-20025] • Pour réserver la plage de ports [20025-20358] : [20025-20358] Par défaut, les ports suivants sont réservés : [1303-1303] [3389-3389] [5353-5353] [5355-5355] Vous pouvez exécuter un script qui analyse les ports susceptibles d'entrer en conflit avec l'Agent TS et qui les ajoute à ce paramètre. Pour plus d'informations, reportez-vous à la section Annexe : utiliser le script de configuration des ports réservés au fonctionnement du système. **NOTE** Lorsqu'un port est ajouté à cette liste, c'est toute la plage de ports (paramètre **PortsPerRange**) qui contient ce port qui est réservée.
TcpTimedWaitDelay	Délai en secondes entre la fermeture d'une connexion et le moment où le port associé est de nouveau disponible (120 par défaut). • Minimum : 30, • Maximum : 300. La valeur doit correspondre à celle utilisée par le serveur Windows sous la clé de registre **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** (120 par défaut). Assurez-vous d'utiliser la même valeur pour les deux paramètres.

Paramètre	Description / Valeurs possibles
TotalPortsRangeLow	Borne inférieure de la plage de ports réservée aux utilisateurs (20000 par défaut). • Minimum : 1024. Si vous abaissez cette valeur, assurez-vous que les ports de la nouvelle plage ne sont pas utilisés par d'autres applications. Vous pouvez réserver des ports au fonctionnement du système avec le paramètre **ReservedSystemPorts**.
TotalPortsRangeHigh	Borne supérieure de la plage de ports réservée aux utilisateurs (49151 par défaut). • Maximum : 65535. Si vous augmentez cette valeur, assurez-vous qu'aucune plage de ports dynamiques de Windows ne chevauche la nouvelle plage de ports réservée aux utilisateurs. Utilisez la commande suivante pour le vérifier : `netsh int <ipv4|ipv6> show dynamicport <tcp|udp>` **NOTE** Le pilote de l'Agent TS ne gère qu'une seule plage de ports.
MaximumNumberRequests	Nombre de requêtes pouvant être traitées simultanément par le pilote (512 par défaut). Ajustez cette valeur selon la capacité mémoire du serveur. • Minimum : 1, • Maximum : 65535. La valeur 0 désactive la 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.

Paramètres du service Agent TS

IMPORTANT
Toute modification des clés de registre du service de l'Agent TS nécessite le redémarrage du service "*Stormshield-rds-service*" pour être prise en compte.

Emplacement dans la base de registre :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\stormshield-rds-service\Parameters

Paramètre	Description
PSK	Clé pré-partagée pour les échanges avec le firewall. Cette clé est renseignée lors de l'installation de l'Agent TS. **NOTE** Modifiez cette valeur si la clé pré-partagée est changée sur le firewall.

Paramètre	Description
EphemeralPortMin	Borne inférieure de la plage de ports additionnels attribuables aux utilisateurs (49152 par défaut). Elle est utilisée lorsqu'un utilisateur n'a plus de port disponible dans ses plages de ports (paramètre **ExhaustedPortAction** positionné sur "*pass*"). • Minimum : 1, • Maximum : 65535. Si vous modifiez cette valeur, assurez-vous que la plage de ports [**EphemeralPortMin-EphemeralPortMax**] englobe la totalité des plages de ports dynamiques de Windows. Utilisez la commande suivante pour le vérifier : `netsh int <ipv4|ipv6> show dynamicport <tcp|udp>` **NOTE** Le service de l'Agent TS n'envoie qu'une seule plage de ports au pilote.
EphemeralPortMax	Borne supérieure de la plage de ports additionnels attribuables aux utilisateurs (65535 par défaut). Elle est utilisée lorsqu'un utilisateur n'a plus de port disponible dans ses plages de ports (paramètre **ExhaustedPortAction** positionné sur "*pass*"). • Minimum : 1, • Maximum : 65535. Si vous modifiez cette valeur, assurez-vous que la plage de ports [**EphemeralPortMin-EphemeralPortMax**] englobe la totalité des plages de ports dynamiques de Windows. Utilisez la commande suivante pour le vérifier : `netsh int <ipv4|ipv6> show dynamicport <tcp|udp>` **NOTE** Le service de l'Agent TS n'envoie qu'une seule plage de ports au pilote.
LogLevel	Niveau des logs (*verbose*) pour les communications entre l'Agent TS et le firewall. Ces logs sont consultables dans l'**Observateur d'événements** Windows du serveur sur lequel l'Agent TS est installé. • Niveau 1 : erreurs uniquement, • Niveau 2 : erreurs et informations (par défaut), • Niveau 3 : erreurs, informations et debug.
ServerPort	Port de communication avec le firewall (par défaut TCP/1303). Le port par défaut correspond à l'objet réseau prédéfini *agent_ts* sur le firewall. **NOTE** Modifiez cette valeur si le port de connexion déclaré sur le firewall 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 (2 par défaut). 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. • Minimum : 0, • Maximum : 60.

Activer les Agents TS et configurer la politique de filtrage

Cette section explique comment activer les Agents TS et configurer la politique de filtrage sur le firewall SNS.

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'utilisateurs 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

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**.

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.

Règle 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 :

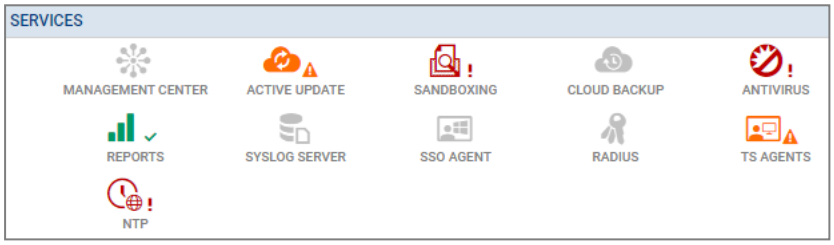
- Les serveurs RDS sur le port TCP/3389 (objet *microsoft-ts* sur un firewall SNS),
- Les serveurs Citrix sur le port 1494 correspondant au protocole Citrix ICA (objet *citrix* sur un firewall SNS).

Superviser l'état des communications entre les Agents TS et le firewall SNS

Différents types d'événements peuvent être consultés depuis l'interface Web d'administration du firewall pour superviser l'état des communications entre les Agents TS et le firewall SNS.

Depuis le module Tableau de bord

L'état des Agents TS peut être consulté via l'onglet **Monitoring** > module **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.

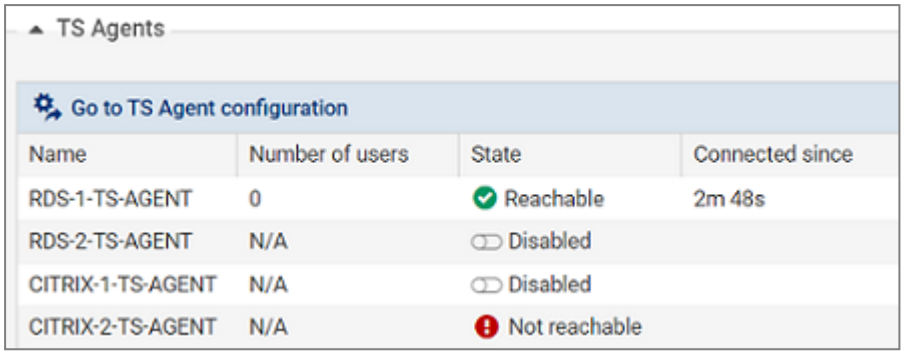
Un double-clic sur l'icône Agents TS vous conduit au widget **Agents TS** du module **Supervision Système**.

Depuis le module 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 :

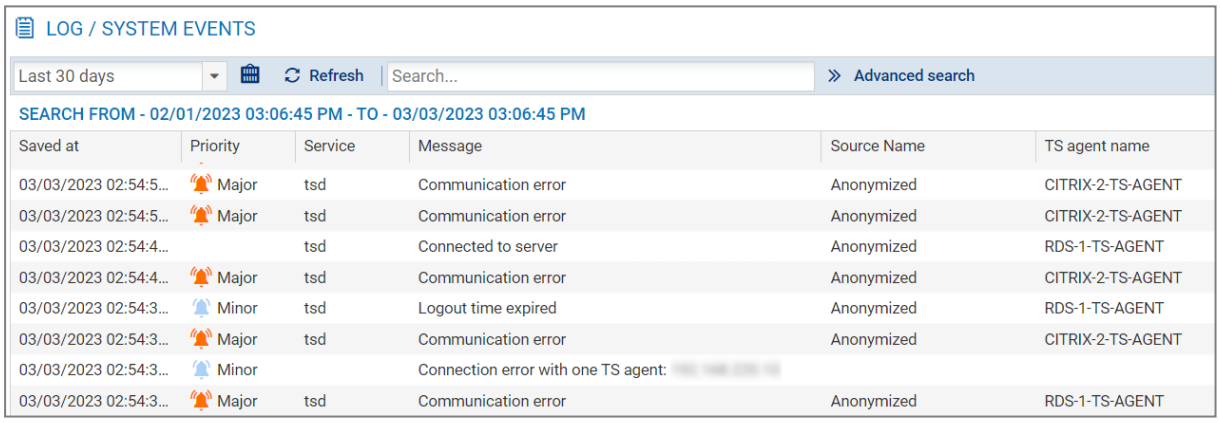
- Le nom de l'Agent TS,
- Le nombre d'utilisateurs connectés par le biais de cet Agent TS,
- L'état de l'Agent TS (**Joignable**, **Non joignable** ou **Désactivé**),
- Le temps écoulé depuis la connexion entre le firewall et l'Agent TS.



Depuis le module Logs - Journaux d'audit

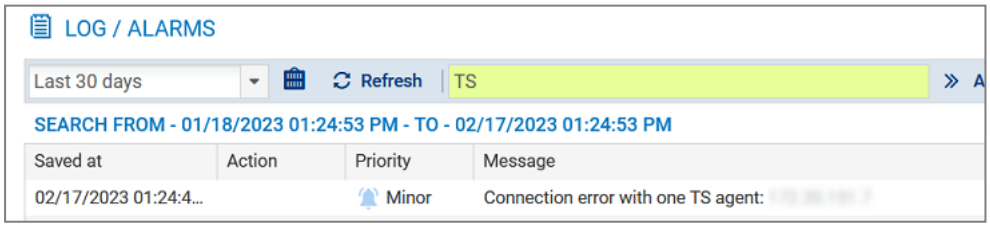
Événements système

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** :



Alarmes

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



Superviser l'Agent TS sur le serveur RDS / Citrix

Cette section explique comment superviser un Agent TS (performances, logs) installé sur un serveur RDS / Citrix.

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

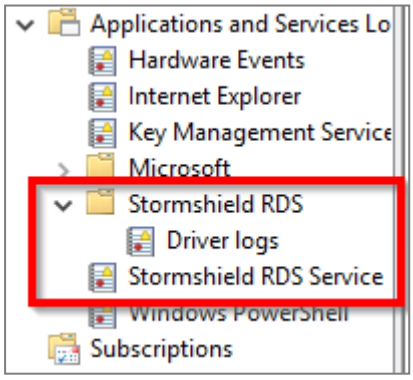
Si nécessaire, sur le serveur sur lequel est déployé l'Agent TS :

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 du pilote et du service de l'Agent TS

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

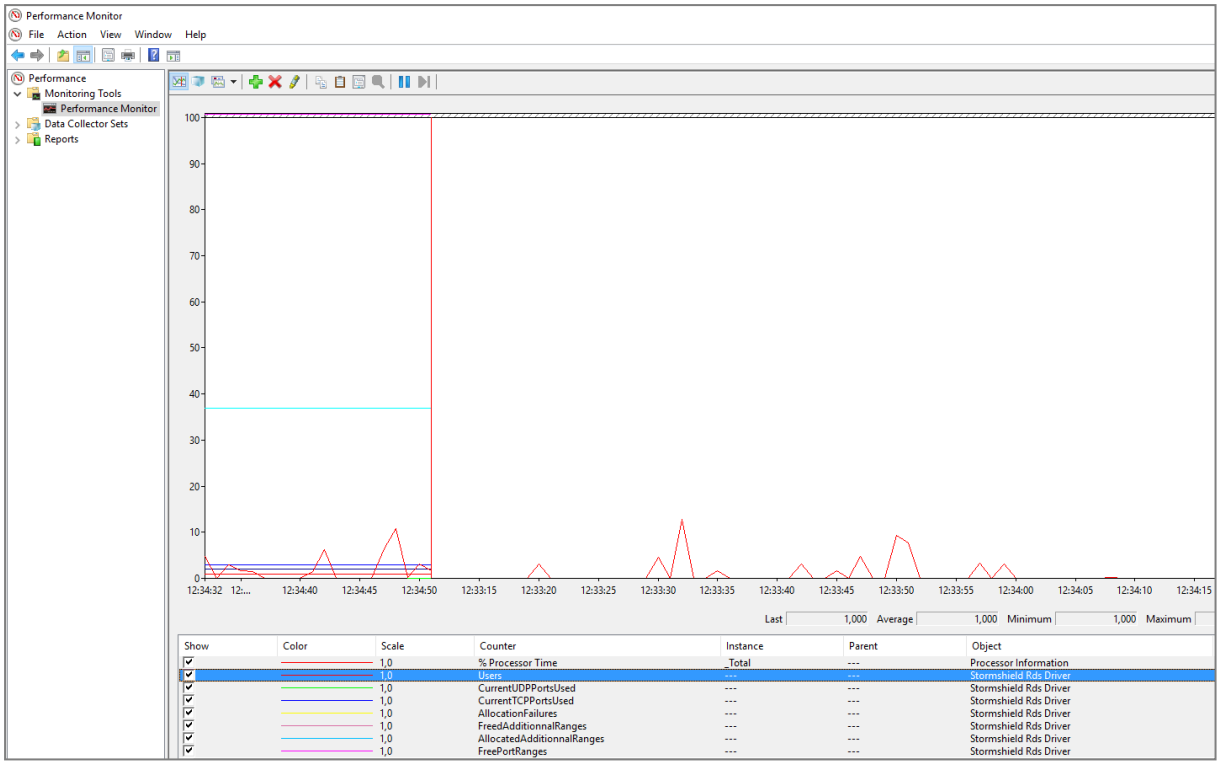
1. Ouvrez l'**Observateur d'événements**.
2. Dans le menu **Journaux des applications et services**, sélectionnez :
   - **Stormshield RDS Service** pour afficher la liste des événements survenus pour le service Stormshield RDS Service,
   - **Stormshield RDS** > **Driver logs** pour afficher la liste des événements survenus pour le pilote de l'Agent TS.



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**.

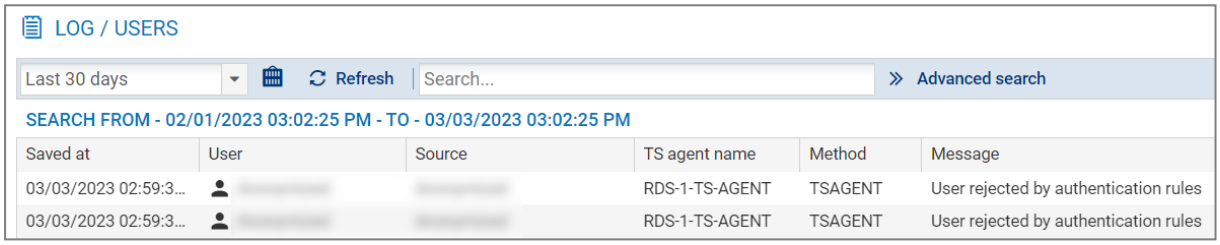

Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
Reports
100
90
80
70
60
50
40
30
20
10
0
12:34:32 12:...
12:34:40
12:34:45
12:34:50
12:33:15
12:33:20
12:33:25
12:33:30
12:33:35
12:33:40
12:33:45
12:33:50
12:33:55
12:34:00
12:34:05
12:34:10
12:34:15
Last 1,000 Average 1,000 Minimum 1,000 Maximum
Show Color Scale Counter Instance Parent Object
1,0 % Processor Time _Total --- Processor Information
1,0 Users --- --- Stormshield Rds Driver
1,0 CurrentUDPPortsUsed --- --- Stormshield Rds Driver
1,0 CurrentTCPPortsUsed --- --- Stormshield Rds Driver
1,0 AllocationFailures --- --- Stormshield Rds Driver
1,0 FreedAdditionnalRanges --- --- Stormshield Rds Driver
1,0 AllocatedAdditionnalRanges --- --- Stormshield Rds Driver
1,0 FreePortRanges --- --- Stormshield Rds Driver

Superviser les utilisateurs connectés par le biais des Agents TS

Cette section explique comment superviser les utilisateurs connectés par le biais des Agents TS (logs d'authentification, ports attribués aux utilisateurs).

Consulter les logs d'authentification

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



Identifier les ports attribués 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 attribués par l'Agent TS à un utilisateur donné.

```
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    21424-21623   85870   0           TSAGENT     (0x0000)
Memberof: TS-USERS
john.doe            documentation.org   TS-SERVER-1                 21424-21623   85870   0           TSAGENT     (0x0000)
Memberof: TS-USERS
```

Résoudre les problèmes

Cette section liste certains problèmes fréquemment rencontrés lors de l'utilisation de l'Agent TS. Si celui que vous rencontrez ne se trouve pas dans cette section, nous vous recommandons de consulter la Base de connaissances Stormshield.

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

- *Situation* : 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.tld).
- Solution : Pour que le firewall puisse faire le lien avec l'annuaire Active Directory de référence, vous devez créer une correspondance entre le nom NETBIOS et le FQDN du domaine.
  5 correspondances NETBIOS / FQDN peuvent être déclarées sur un même firewall 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=STORMSHIELD FQDN=stormshield.eu
CONFIG AUTH ACTIVATE
```

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

Des utilisateurs ne peuvent pas se reconnecter après un redémarrage du serveur RDS / Citrix

- *Situation* : Redémarrer le serveur RDS / Citrix alors que des utilisateurs sont connectés via la méthode TS Agent peut empêcher ces utilisateurs de se reconnecter ensuite.
- Solution : Redémarrez de nouveau le serveur RDS / Citrix pour résoudre le problème.

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).

Annexe : utiliser le script de configuration des ports réservés au fonctionnement du système

Cette annexe explique comment utiliser le script de configuration des ports réservés au fonctionnement du système (**AddRangeReservedSystemPorts.ps1**).

Vous pouvez utiliser ce script :

- Juste après l'installation de l'Agent TS, idéalement avant de redémarrer le serveur,
- Plus tard pour ajuster les paramètres de l'Agent TS, par exemple en cas d'installation de nouvelles applications ou de problèmes de connexion.

Principe de fonctionnement du script

Ce script, fourni par Stormshield, analyse les ports susceptibles d'entrer en conflit avec l'Agent TS et les ajoute au paramètre **ReservedSystemPorts** de l'Agent TS pour les réserver au fonctionnement du système. Ainsi, ces ports ne pourront pas être attribués à un utilisateur.

Le script analyse les ports de plusieurs manières :

- En analysant l'état du réseau de la machine (comme un *netstat* amélioré),
- En analysant les événements de l'Agent TS dans l'**Observateur d'événements** afin d'y repérer d'éventuels conflits de port (ID de l'événement 32781). Cette analyse s'effectue par défaut sur un mois (le nombre de jours exact varie d'un mois à un autre).

Prérequis pour utiliser le script

- Pouvoir exécuter Windows PowerShell en tant qu'administrateur.
- Pouvoir lancer des scripts locaux sur la machine.
  Vous pouvez modifier cette politique d'exécution avec les commandes :

```
Set-ExecutionPolicy unrestricted
Set-ExecutionPolicy remotesigned
```

Télécharger le script

1. Dans votre espace MyStormshield, rendez-vous dans **Téléchargements > Téléchargements**.
2. Dans les catégories, sélectionnez **Stormshield Network Security > TS Agent**.
3. Cliquez sur le script **AddRangeReservedSystemPorts.ps1** pour le télécharger.
4. Copiez le script sur chaque serveur RDS ou Citrix où un Agent TS est installé.

Utiliser le script

1. Dans Windows PowerShell, exécutez la commande :

```
.\AddRangeReservedSystemPorts.ps1
```

2. Prenez connaissance du résultat du script :
   - Les ports affichés sont susceptibles d'entrer en conflit avec l'Agent TS,
   - Les ports *Pre-configured* sont issus de la configuration par défaut de l'Agent TS.

3. Indiquez avec "**yes**" ou "**no**" si vous souhaitez que le script modifie le paramètre **ReservedSystemPorts** de l'Agent TS dans la base de registre en y ajoutant les ports trouvés.
4. Indiquez avec "**yes**" ou "**no**" si vous souhaitez redémarrer immédiatement le serveur. Les nouveaux ports réservés au fonctionnement du système ne seront pris en compte qu'après le redémarrage du serveur. Si vous ne redémarrez pas immédiatement le serveur, pensez à le programmer afin de prendre en compte les modifications.

Options possibles

Vous pouvez utiliser le script avec des options :

```
.\AddRangeReservedSystemPorts.ps1 -Options
```

Option	Description
-PauseAtExit	Force le script à attendre que l'utilisateur appuie sur une touche du clavier avant de se terminer, et cela dans tous les cas. Cette option est utile pour voir le résultat du script lorsqu'il est appelé par un autre script ou un programme.
-Force	Modifie le paramètre **ReservedSystemPorts** de l'Agent TS dans la base de registre sans demander de confirmation.
-HistoryDepth <days>	Détermine une période d'analyse en jours des événements de l'Agent TS dans l'**Observateur d'événements**. Par défaut, l'analyse s'effectue sur un mois (le nombre de jours exact varie d'un mois à un autre). Cette option n'est pas compatible avec l'option **-FullLog**.
-FullLog	Analyse l'historique complet disponible des événements de l'Agent TS dans l'**Observateur d'événements**. Cette option n'est pas compatible avec l'option **-HistoryDepth**.
-AutoRestart	Redémarre automatiquement le serveur sans demander de confirmation, à condition que le script se soit exécuté correctement. Cette option est utile pour prendre en compte immédiatement les nouveaux ports réservés au fonctionnement du système. Cette option n'est pas compatible avec l'option **-NoRestart** .
-NoRestart	Détermine que le serveur ne doit pas être redémarré, ce qui évite l'affichage de la demande de confirmation de redémarrage lors de l'exécution du script. Cette option n'est pas compatible avec l'option **-AutoRestart**.
-Verbose	Affiche des messages supplémentaires lors de l'exécution du script. Cette option est utile lors d'une assistance technique, par exemple avec le support Stormshield.
-DryRun	Affiche uniquement le résultat de l'analyse du script. Aucune action n'est initiée avec cette option. Cette option est souvent utilisée avec l'option **-Verbose**. Cette option est utile pour exécuter le script sans être administrateur.

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2025. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.