Guide sur les agents des services de terminaux (TS) Cisco, version 1.4

Cisco Secure Firewall Management Center
Updated NaN,

Table des matières

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Chapitre

1 Nouveautés de ce guide

Sujets :

- Quoi de neuf dans ce livre

Nouveautés du guide de l’agent TS.

Quoi de neuf dans ce livre

Changements dans cette version du guide de l'agent TS.

Changements dans ce guide :

- Téléchargez le logiciel TS Agent 1.4.2 : Installer ou mettre à niveau l'agent TS à la page 18
- Liste des problèmes résolus dans cette version : problèmes résolus à la page 14.

Chapitre

2 Introduction à l’agent de services de terminaux (TS)

Sujets :

Les rubriques liées à l’agent TS.

À propos de l'agent Cisco Terminal Services (TS)

Renseignements généraux sur l'agent TS.

L'agent Cisco Terminal Services (TS) permet au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)ou au On-Prem Management Center d'identifier de manière unique le trafic utilisateur surveillé par un serveur de terminaux Microsoft Windows. Sans l'agent TS, les systèmes reconnaissent tout le trafic provenant d'un serveur de terminaux Microsoft Windows comme une seule séance de l'utilisateur provenant d'une adresse IP.

L'agent TS peut être utilisé avec tous les éléments suivants :

- Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est disponible avec le Contrôle de Security Cloud.
- Le On-Prem Management Center est disponible avec Contrôle de Security Cloud.
- Un centre de gestion autonome ou un système à haute disponibilité qui n'est pas associé à Contrôle de Security Cloud.

Pour simplifier, dans ce guide, sauf indication contraire, *On-Prem Management Center* peut désigner soit un Management Center associé à Contrôle de Security Cloud, soit un système autonome qui n'est pas associé à Contrôle de Security Cloud.

Remarque

Pour éviter les problèmes potentiels et pour vous assurer que vous utilisez le logiciel le plus récent, Cisco vous recommande d'utiliser la dernière version publiée de l'Agent TS. Pour trouver la dernière version, accédez au site d'assistance Cisco.

Lorsqu'il est installé et configuré sur votre serveur de terminaux Microsoft Windows, l'agent TS attribue une plage de ports aux séances de l'utilisateur individuelles et les ports de cette plage aux connexions TCP et UDP dans la séance de l'utilisateur. Les systèmes utilisent des ports uniques pour identifier les connexions TCP et UDP individuelles par les utilisateurs sur le réseau. Les plages de ports sont attribuées selon le principe du moins récemment utilisé, ce qui signifie qu'après la fin d'une session utilisateur, la même plage de ports n'est pas immédiatement réutilisée pour les nouvelles sessions utilisateur.

Remarque

Les messages ICMP sont transmis sans mappage de port.

Le trafic généré par un service exécuté dans le contexte système de l'ordinateur n'est pas suivi par l'agent TS. En particulier, l'agent TS n'identifie pas le trafic Server Message Block (SMB), car le trafic SMB est exécuté dans le contexte système.

L'agent TS prend en charge jusqu'à 199 séances de l'utilisateur simultanées par hôte TS Agent. Si un seul utilisateur exécute plusieurs séances de l'utilisateur simultanées, l'agent TS attribue une plage de ports unique à chaque séance de l'utilisateur individuelle. Lorsqu'un utilisateur met fin à une session, l'agent TS peut utiliser cette plage de ports pour une autre séance de l'utilisateur.

Chaque Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou On-Prem Management Center prend en charge jusqu'à 50 agents TS qui s'y connectent simultanément.

Il y a trois composants principaux de l'agent TS installés sur votre serveur :

- Interface : application permettant de configurer l'agent TS et de surveiller les séances de l'utilisateur en cours.
- Service : programme qui surveille les connexions et les déconnexions des utilisateurs.
- Pilote – programme qui effectue la traduction de port

L'agent TS peut être utilisé pour éléments suivants :

- Les données de l'agent TS sur le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou le On-Prem Management Center peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur. Pour plus de renseignements sur l'utilisation des données de l'agent TS dans le système Firepower, consultez le *Guide de configuration des périphériques de Secure Firepower Management Center*.

> **Remarque**
>
> Pour utiliser l'agent TS à des fins de sensibilisation et de contrôle des utilisateurs, vous devez le configurer pour qu'il envoie des données *uniquement* au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou au On-Prem Firewall Management Center. Pour en savoir plus, consultez Configurer l'agent TS à la page 20.

Exigences en matière d'environnement de serveur et de système

Exigences en matière de serveur et de logiciel avant d'installer l'agent TS.

Vous devez satisfaire aux exigences suivantes pour installer et exécuter l'Agent TS sur votre système.

> **Remarque**
>
> Pour éviter les problèmes potentiels et pour vous assurer que vous utilisez le logiciel le plus récent, Cisco vous recommande d'utiliser la dernière version publiée de l'Agent TS. Pour trouver la dernière version, accédez au site d'assistance Cisco.

Exigences en termes de serveur

Installez l'Agent TS sur l'une des versions de serveur de terminaux Microsoft Windows de 64 bits suivantes :

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows Server 2022
- Microsoft Windows Server 2025

L'Agent TS nécessite les éléments suivants et les installe s'ils ne sont pas présents :

- Microsoft .NET Framework 4.6.2
- Microsoft Visual C++ Update 4

Remarque

L'installation de l'Agent TS nécessite 653 Ko d'espace libre sur votre serveur.

Remarque

Si le serveur de l'agent TS utilise un logiciel antivirus qui agit comme un proxy pour le trafic web, le trafic utilisateur est généralement attribué à l'utilisateur System et On-Prem Management Center ou Management Center voit ces utilisateurs comme inconnus. Pour éviter le problème, désactivez la fonction de mandataire pour le trafic Web.

L'agent TS est compatible avec l'une des solutions de services de terminaux suivantes installées sur votre serveur :

- Provisionnement Citrix
- Citrix XenDesktop
- Citrix XenApp
- Hyperviseur de projet Xen
- Hyperviseur VMware vSphere/VMware ESXi 7.0
- Services de terminaux Windows/Services de bureau à distance Windows (RDS)

Cette version de l'agent TS prend en charge l'utilisation d'une seule interface réseau (NIC) pour la traduction de ports et les communications entre le serveur et le système. Si deux interfaces réseau valides (NIC) ou plus sont présentes sur votre serveur, l'agent TS effectue la traduction de ports uniquement sur l'adresse que vous spécifiez lors de la configuration. Une carte réseau valide doit avoir une adresse IPv4 ou IPv6 unique, ou une de chaque type; une carte réseau valide ne peut pas avoir plusieurs adresses du même type.

Remarque

Si les annonces de routeur sont activées sur des appareils connectés à votre serveur, les appareils peuvent attribuer plusieurs adresses IPv6 aux NIC sur votre serveur et invalider les NIC pour une utilisation avec l'Agent TS.

Exigences du système Firepower

Cette version de l'agent TS prend en charge la connexion à des Firepower Management Center autonomes ou en haute disponibilité exécutant les versions 6.4 ou ultérieures du système Firepower.

Dépanner les problèmes en utilisant l'agent TS

Dépannage des problèmes que vous pourriez rencontrer lors de l'utilisation de l'agent TS.

Échec du test de connexion au On-Prem Firewall Management Center

Si vous êtes connecté au serveur de l'agent TS en tant qu'utilisateur local (et non en tant qu'utilisateur de domaine), le test de connexion de l'agent TS avec On-Prem Firewall Management Center échoue. Cela se produit parce que, par défaut, l'agent TS n'autorise pas les processus système à communiquer sur le réseau.

Pour contourner le problème, effectuez l'une des opérations suivantes :

- Cochez **Unknown Traffic Communication** (Communication du trafic inconnu) sur la page de l'onglet **Configure** (Configurer) pour autoriser le trafic, comme indiqué dans Champs de configuration de l'agent TS à la page 21.
- Connectez-vous à l'ordinateur de l'agent TS en tant qu'utilisateur de domaine plutôt qu'en tant qu'utilisateur local.

L'Agent TS signale les utilisateurs comme inconnus et règles non correspondantes

Si des agents de services de terminaux d'autres fournisseurs s'exécutent sur le même serveur que l'agent de services de terminaux Cisco (TS), les numéros de port pour les connexions utilisateur peuvent ne pas être dans la plage de ports utilisateur attribuée. Par conséquent, les utilisateurs peuvent être identifiés comme Unknown (Inconnus) et, par conséquent, les règles d'identité ne correspondent pas pour les utilisateurs.

Pour résoudre ce problème, désactivez ou désinstallez les autres agents des services de terminaux s'exécutant sur le même serveur que l'Agent TS de Cisco.

L'agent TS demande un redémarrage lors de la mise à niveau.

Parfois, même si l'adresse IP de la machine ne change pas, l'agent TS signale un changement d'adresse IP après la mise à niveau et vous invite à redémarrer le serveur. Cela se produit parce que l'agent TS détecte une différence entre l'adresse IP et la valeur de la clé de registre suivante :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TSAgent\{IPv4 | IPv6}
```

Si la valeur de la clé est différente de l'adresse IP de l'adaptateur principal configuré, l'agent TS signale le changement et vous demande d'enregistrer la configuration puis de redémarrer l'ordinateur.

Cela peut se produire, par exemple, si l'ordinateur a été recréé ou restauré à partir d'une sauvegarde et que DHCP attribue une nouvelle adresse IP.

Vous pouvez ignorer l'erreur, mais vous devez quand même redémarrer l'ordinateur après la mise à niveau.

Les clients Citrix Provisioning ne démarrent pas

Vous devez configurer l'agent TS pour qu'il ignore le(s) port(s) UDP que vous avez configuré(s) pour le serveur Citrix Provisioning.

La valeur que vous précisez dans le champ **Reserve Port(s)** (Réserver le(s) port(s)) de l'agent TS doit correspondre à l'un des **numéros de port du premier et du dernier UDP** de Citrix Provisioning.

> ⚠ **ATTENTION**
>
> Si vous ne précisez pas le bon port, les clients ne pourront pas démarrer.

Exceptions lors de l'enregistrement de l'adresse IP de l'agent TS

Dans de rares cas, des exceptions s'affichent lorsque vous tentez d'enregistrer la configuration de l'agent TS avec une adresse IP non valide. Une adresse IP non valide peut être de l'une des options suivantes :

- La même adresse IP qu'un autre appareil sur le réseau.
- Modification de l'adresse IP statique dans Windows lorsque l'application de l'agent TS est ouverte.

Les exceptions comprennent les éléments suivants :

- `System.argumentsException : un élément avec la même clé a déjà été ajouté.`
- `System.NullReferenceException : référence d'objet non définie sur une instance d'objet.`

Solution de contournement : définissez l'adresse IP du serveur de l'agent TS sur une adresse IP valide, enregistrez la configuration et redémarrez le serveur.

problèmes résolus

Liste des problèmes résolus dans cette version.

Problèmes résolus

Numéro d'identification de la mise en garde	Description
CSCwc41073	Des erreurs de protocole lors de la communication avec le Firewall Management Center amènent l'agent TS à réessayer la connexion au lieu d'échouer.
CSCwp38698	Fuite de mémoire résolue.
CSCwo79230	Problème de résolution de nom DNS résolu lors de l'utilisation de l'agent TS.

Historique de l'agent TS

Historique de ce document.

Fonctionnalités	Version
Prend en charge On-Prem Firewall Management Center et Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) disponible avec le Contrôle de Security Cloud, ainsi qu'un Management Center autonome.	1.4

Fonctionnalités	Version
• Ajout de la prise en charge du provisionnement Citrix • La valeur que vous précisez dans le champ **Reserve Port(s)** (Réserver le(s) port(s)) de l'agent TS doit correspondre à l'un des **numéros de port du premier et du dernier UDP** de Citrix Provisioning. **⚠ ATTENTION** Si vous ne précisez pas le bon port, les clients ne pourront pas démarrer.	1.3
• Détecte un changement d'adresse IP sur le serveur, vous invite à enregistrer la configuration et à redémarrer. Voir la section Champs de configuration de l'agent TS à la page 21. • Vous permet d'effectuer une mise à niveau vers cette version sans désinstaller la version précédente. Consultez Installer ou mettre à niveau l'agent TS à la page 18. • Renommer le champ de configuration **Exclude Port(s)** (Exclure port[s]) en **Reserve Port(s)** (Réserver port[s]). Consultez Champs de configuration de l'agent TS à la page 21. • Prise en charge des ports éphémères. Consultez Champs de configuration de l'agent TS à la page 21. • La page de l'onglet **Monitor** (Surveiller) vous avertit lorsque plus de 50 % des ports TCP ou UDP ont été utilisés pour une session particulière. Consultez Afficher les renseignements sur l'Agent TS à la page 32. • Les plages de ports de session utilisateur attribuées selon la base du moins récemment utilisées. Consultez À propos de l'agent Cisco Terminal Services (TS) à la page 10. • Vous permet d'exporter des informations de dépannage vers un fichier XML. Consultez Afficher les renseignements sur l'Agent TS à la page 32. • Vous permet de refluer les séances de l'utilisateur vers le centre de gestion. Consultez Afficher les renseignements sur l'Agent TS à la page 32. • Tentative de fin de toutes les séances de l'utilisateur lorsque l'agent TS est désinstallé. Consultez Désinstallation de l'agent TS à la page 37.	1.2

Fonctionnalités	Version
• Le nombre maximal de sessions d'utilisateur par défaut a été modifié de 200 à 30. • La plage de ports est passée de 200 ou plus à 5 000 ou plus Ces modifications sont toutes abordées dans Champs de configuration de l'agent TS à la page 21.	1.1
Agent TS Fonctionnalité introduite. L'agent TS permet aux administrateurs de suivre l'activité des utilisateurs en utilisant le mappage de port. L'agent TS, lorsqu'il est installé sur un serveur de terminaux, affecte une plage de ports aux séances de l' utilisateur individuelles et les ports de cette plage aux connexions TCP et UDP dans la séance de l'utilisateur. Les systèmes utilisent des ports uniques pour identifier les connexions TCP et UDP individuelles par les utilisateurs sur le réseau.	1.0

Chapitre

3 Installer et configurer l’Agent TS

Sujets :

Rubriques liées à l’installation, à la mise à niveau et à la configuration de l’agent TS.

Installer ou mettre à niveau l'agent TS

Apprenez à télécharger, à exécuter et à configurer l'agent TS pour obtenir des performances optimisées et une compatibilité avec les environnements pris en charge.

- Confirmez que l'agent TS est pris en charge dans votre environnement, comme décrit dans Exigences en matière d'environnement de serveur et de système à la page 11.
- Mettez fin à toutes les sessions utilisateur en cours, comme décrit dans Mettre fin à une session d'utilisateur en cours à la page 36.

Installer ou mettre à niveau le logiciel de l'agent TS.

1. Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.
2. Téléchargez le paquet de l'agent TS à partir du site d'assistance : TSAgent-1.4.2.exe.

> **Remarque**
>
> Téléchargez la mise à jour directement à partir du site. Si vous transférez le fichier par courriel, il pourrait être corrompu.

3. Faites un clic droit sur `TSAgent-1.4.2.exe` et choisissez **Run as Administrator** (Exécuter en tant qu'administrateur).
4. Cliquez sur **Installer** et suivez les invites pour installer ou mettre à niveau l'agent TS.

- Confirmez que l'agent TS fonctionne comme indiqué dans Visualisation de l'état du composant de service de l'agent TS à la page 36.
- Démarrez l'agent TS comme indiqué dans Démarrage et arrêt des processus de l'agent TS à la page 36.
- Configurez l'agent TS comme indiqué dans Configurer l'agent TS à la page 20.

  Si vous effectuez une mise à niveau à partir d'une version antérieure de l'agent TS et que vous utilisez Citrix Provisioning, vous devez entrer `6910` dans le champ **Reserve Port(s) (Réserver le(s) port(s))** après avoir effectué la mise à niveau.

> **Remarque**
>
> Si le programme d'installation de l'agent TS signale que le cadre .NET a échoué, exécutez la mise à jour de Windows et réessayez d'installer l'agent TS.

Lancer l'interface de configuration de l'agent TS

Démarrez l'agent TS et utilisez-le pour surveiller le trafic du serveur de terminaux.

S'il existe un raccourci de l'agent TS sur votre bureau, double-cliquez sur ce raccourci. Sinon, utilisez la procédure suivante pour lancer l'interface de configuration de l'agent TS.:

1. Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.
2. Ouvrez `C:\Program Files (x86)\Cisco\Terminal Services Agent`.

3. Affichez les fichiers de programme pour l'agent TS.

> **Remarque**
>
> Les fichiers de programme sont en affichage seulement. Ne supprimez pas, ne déplacez pas et ne modifiez pas ces fichiers.

4. Double-cliquez sur le fichier `TSAgentApp` pour lancer l'agent TS.

Configurer un serveur proxy

Requis uniquement si votre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas communiquer avec la machine sur laquelle l'agent TS est installé.

Si votre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas communiquer avec la machine sur laquelle l'agent TS est installé, vous devez utiliser un proxy avec le protocole HTTPS activé.

La façon dont vous le faites dépend de vous. Par exemple, vous pouvez avoir un mandataire commercial et utiliser un mandataire du système Windows avec HTTPS activé pour communiquer avec lui.

> **Remarque**
>
> Cette tâche n'est pas nécessaire pour utiliser un Centre de gestion de pare-feu local avec l'agent TS ou si vous n'utilisez pas Contrôle de Security Cloud du tout.

Configurer un proxy d'application

Configurez un proxy pour l'agent TS sur Windows Server en modifiant le fichier machine.config. Apprenez comment mettre à jour les paramètres du proxy pour activer la connectivité réseau de l'agent TS, comme requis par votre environnement.

Vous devez déjà avoir configuré un serveur proxy; cela dépasse la portée de cette documentation.

Cette tâche propose une option pour configurer un proxy sur le serveur Windows sur lequel l'agent TS est en cours d'exécution. Cisco ne garantit pas que cette procédure fonctionnera dans votre situation. Pour plus d'informations, consultez votre fournisseur de proxy ainsi que la documentation de Windows.

1. Connectez-vous en tant qu'administrateur à votre serveur Windows.
2. En tant qu'administrateur, ouvrez le fichier suivant dans un éditeur de texte :

```
\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config
```

3. Collez les éléments suivants dans `machine.config` dans le `<system.net>` section. Remplacez l'adresse IP et le port d'exemple par l'adresse IP et le port de votre serveur proxy.

```
<! -- Configuration for TS Agent -->
<system.net>
    <defaultProxy>
        <proxy autoDetect="false" bypassonlocal="false"
proxyaddress="http://192.0.2.197:3128" usesystemdefault="false" />
    </defaultProxy>
</system.net>
```

```
<! -- Configuration for TS Agent -->
```

4. Enregistrez vos modifications dans `machine.config` et quittez l'éditeur de texte.
5. Redémarrez le serveur pour que les modifications prennent effet.

Consultez Obtenir un jeton API à la page 20.

Obtenir un jeton API

Comment générer un jeton API dans Security Cloud Control pour l'authentification de l'agent TS lors de l'utilisation de Cloud-Delivered Firewall Management Center.

Cette tâche explique comment obtenir le jeton API, qui est utilisé par l'agent TS pour s'authentifier auprès du Contrôle de Security Cloud.

Rôle requis :

- Super administrateur
- Admin
- Déploiement uniquement (ou mieux) avec API uniquement activée

> **Remarque**
>
> Cette tâche s'applique uniquement à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).
>
> Si vous utilisez On-Premesis Firewall Management Center, consultez Création du rôle VDI REST à la page 29 à la place.

1. Connectez-vous à Contrôle de Security Cloud en tant qu'utilisateur avec l'un des rôles suivants :
   - Super Admin : pour créer un utilisateur d'agent TS facultatif ou pour obtenir le jeton API pour vous-même.
   - Admin ou Déployer uniquement avec l'API uniquement activée : pour obtenir un jeton API pour vous-même.
2. (Facultatif pour l'utilisateur Super Admin uniquement.) Créez un utilisateur pour l'agent TS avec le rôle Déployer uniquement ou un rôle supérieur et vérifiez **API uniquement**.
3. Dans le coin supérieur droit, cliquez sur votre nom de connexion, puis sur **Paramètres**.
4. Sur la ligne Paramètres généraux, cliquez sur **Générer un jeton API**.
5. Copiez le jeton dans le presse-papier; vous pouvez cliquer sur  pour le faire.

Configurez l'agent TS comme indiqué dans Configurer l'agent TS à la page 20.

Configurer l'agent TS

Configurez l'agent TS pour qu'il se connecte à Cloud-Delivered Firewall Management Center ou On-Prem Firewall Management Center, synchronisez l'heure du serveur et testez la connexion à l'API REST afin de prendre en charge la surveillance sécurisée des utilisateurs et une intégration transparente.

- Si vous vous connectez au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou au On-Prem Firewall Management Center, configurez et activez un ou plusieurs domaines Active Directory ciblant

les utilisateurs que votre serveur surveille, comme décrit dans le *Guide de configuration des appareils du système de gestion de Cisco Secure Firewall*.

- Si vous vous connectez au On-Prem Firewall Management Center, configurez un compte d'utilisateur disposant de privilèges REST VDI.

  Vous devez créer le rôle REST VDI dans le centre de gestion Cisco Firepower Management Center, comme indiqué dans Création du rôle VDI REST à la page 29.

- Si vous êtes déjà connecté au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou au On-Prem Firewall Management Center et que vous mettez à jour la configuration de votre agent TS pour vous connecter à un autre Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou On-Prem Firewall Management Center, vous devez mettre fin à toutes les sessions utilisateur en cours avant d'enregistrer la nouvelle configuration. Pour en savoir plus, consultez Mettre fin à une session d'utilisateur en cours à la page 36 .

- Synchronisez l'heure de votre serveur d'agent TS avec celle du Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)ou du On-Prem Firewall Management Center.

- Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)uniquement, obtenez un jeton API comme indiqué dans Obtenir un jeton API à la page 20

- Passez en revue et comprenez les champs de configuration, comme décrit dans Champs de configuration de l'agent TS à la page 21.

Utilisez l'interface de l'agent TS pour configurer l'agent TS. Vous devez enregistrer vos modifications et redémarrer le serveur pour que vos modifications prennent effet.

1. Sur le serveur où vous avez installé l'agent TS, démarrez celui-ci comme décrit dans Lancer l'interface de configuration de l'agent TS à la page 18.
2. Cliquez sur l'onglet **Configure** (Configurer).
3. Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) uniquement : cliquez sur l'onglet **Cloud** au bas de la page.
4. Centre de gestion de pare-feu local uniquement : cliquez sur l'onglet **On-Prem** au bas de la page.
5. Consultez Champs de configuration de l'agent TS à la page 21.
6. Après avoir configuré l'Agent TS, cliquez sur **Test** pour tester la connexion API REST entre l'Agent TS et le système.

   Si vous avez configuré un On-Prem Firewall Management Center principal et un On-Prem Firewall Management Center secondaire, le test de connexion au serveur secondaire échoue. Il s'agit du comportement attendu. L'agent TS communique en permanence avec On-Prem Firewall Management Center actif. Si le serveur principal bascule et devient On-Prem Firewall Management Center inactif, l'agent TS communique avec le serveur secondaire, qui est désormais On-Prem Firewall Management Center actif.

7. Cliquez sur **Save** (Enregistrer) et confirmez que vous souhaitez redémarrer le serveur.

Champs de configuration de l'agent TS

Les champs suivants sont utilisés pour configurer les paramètres sur un agent TS.

Paramètres généraux

Tableau 1 : Champs des paramètres généraux

Champ	Description	Exemple
Nombre maximal de sessions par utilisateur	Le nombre maximal de séances de l'utilisateur que vous souhaitez que l'agent TS surveille. Un seul utilisateur peut exécuter plusieurs sessions d'utilisateur à la fois. Cette version de l'agent TS prend en charge 29 séances de l'utilisateur par défaut, jusqu'à un maximum de 199 séances de l'utilisateur.	`29` (la valeur maximale prise en charge dans cette version de l'agent TS)

Champ	Description	Exemple
Carte réseau du serveur	L'agent TS prend en charge l'utilisation d'un contrôleur d'interface réseau (NIC) unique pour la traduction de ports et les communications entre systèmes de serveurs. Si deux interfaces réseau valides (NIC) ou plus sont présentes sur votre serveur, l'agent TS effectue la traduction de ports uniquement sur l'adresse que vous spécifiez lors de la configuration. L'agent TS remplit automatiquement ce champ avec l'adresse IPv4 et/ou l'adresse IPv6 de chaque NIC sur le serveur sur lequel l'agent TS est installé. Une carte réseau valide doit avoir une adresse IPv4 ou IPv6 unique, ou une de chaque type; une carte réseau valide ne peut pas avoir plusieurs adresses du même type. **Remarque** Si l'adresse IP du serveur change, vous êtes invité à enregistrer la configuration et à redémarrer le serveur pour que la modification entre en vigueur. **Remarque** Vous devez désactiver les messages d'annonce du routeur sur tous les appareils connectés à votre serveur. Si les annonces de routeur sont activées, les appareils peuvent attribuer plusieurs adresses IPv6 aux NIC sur votre serveur et invalider les NIC pour une utilisation avec l'agent TS.	`Ethernet 2 (192.0.2.1)` (une carte d'interface réseau sur votre serveur)
Ports du système		**Start** (Début) défini sur `10000` et **Range** (Plage) défini sur `5000`

Champ	Description	Exemple
	La plage de ports que vous utilisez pour les processus système. L'agent TS ignore cette activité. Configurez un port **Start** (Début) pour indiquer où vous souhaitez commencer la plage. Configurez une valeur **Range** (Plage) pour indiquer le nombre de ports que vous souhaitez désigner pour chaque processus système individuel. Cisco recommande une valeur **Range** (Plage) de de 5000 ou plus. Si vous remarquez que l'Agent TS manque fréquemment de ports pour les processus système, augmentez la valeur **de la plage**. **Remarque** Si un processus système nécessite un port qui ne correspond pas à vos **System ports** (Ports système) désignés, ajoutez le port au champ **Exclude port(s)** (Exclure port[s]). Si vous n'identifiez pas un port utilisé par les processus système dans la plage **System Ports** (Ports système) ou si vous ne l'excluez pas, les processus système peuvent échouer. L'agent TS renseigne automatiquement la valeur de **fin** à l'aide de la formule suivante : : `( [Start value] + [Range value] ) - 1` Si vos entrées font que la valeur **End** (Fin) dépasse la valeur **Start** (Début) de **User Ports** (Ports utilsiateurs), vous devez ajuster vos valeurs **Start** (Début) et **Range** (Plage).	

Champ	Description	Exemple
Ports utilisateur	La plage de ports que vous souhaitez désigner pour les utilisateurs. Configurez un port **Start** (Début) pour indiquer où vous souhaitez commencer la plage. Configurez une valeur **Range** (Plage) pour indiquer le nombre de ports que vous souhaitez désigner pour les connexions TCP ou UDP dans chaque session utilisateur individuelle. **Remarque** Le trafic ICMP est transmis sans mappage de port. Cisco recommande une valeur **Range** (Plage) de de 1000 ou plus. Si vous constatez que l'agent TS manque fréquemment de ports pour le trafic utilisateur, augmentez la valeur de la **plage**. **Remarque** Lorsque le nombre de ports utilisés dépasse la valeur de **Range** (Plage), le trafic utilisateur est bloqué. L'agent TS renseigne automatiquement la valeur de **fin** à l'aide de la formule suivante : : `[Start value] + ( [Range value] * [Max User Sessions value] ) - 1` Si vos entrées font que la valeur **End** (Fin) dépasse 65535, vous devez ajuster vos valeurs **Start** (Début) et **Range** (Plage).	**Start** (Début) défini sur `15000` et **Range** (plage) défini sur `1000`
Ports éphémères	Saisissez une plage de ports éphémères (également appelés *ports dynamiques*) à surveiller par l'agent TS.	**Start** (Début) défini sur `49152` et **Range** (Plage) défini sur `16384`

Champ	Description	Exemple
Communication avec le trafic inconnu	Cochez **Autoriser** pour permettre à l'agent TS d'autoriser le trafic sur les ports système ; toutefois, l'agent TS ne suit pas l'utilisation des ports. Les ports système sont utilisés par le compte de système local ou d'autres comptes d'utilisateurs locaux. (Un compte utilisateur local existe uniquement sur le serveur de l'agent TS ; il ne possède aucun compte Active Directory correspondant.) Vous pouvez choisir cette option pour autoriser les types de trafic suivants : • Autorisez le trafic exécuté par le compte de système local (comme Server Message Block (SMB)) au lieu de le bloquer. Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou le On-Prem Firewall Management Center identifie ce trafic comme provenant de l'utilisateur Unknown, car l'utilisateur n'existe pas dans Active Directory. L'activation de cette option vous permet également de tester avec succès la connexion au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou au On-Prem Firewall Management Center si vous vous connectez au serveur de l'agent TS à l'aide d'un compte système local. • Lorsqu'une session d'utilisateur ou de système épuise tous les ports disponibles de sa plage, l'agent TS autorise le trafic sur les ports éphémères. Cette option active le trafic ; le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou le On-Prem Firewall Management Center identifie le trafic comme provenant de l'utilisateur Unknown. Cela est particulièrement utile lorsque les ports système sont nécessaires pour maintenir le système en bon état, par exemple pour les mises à jour de contrôleur de domaine, les authentifications, les requêtes d'interface de gestion de fenêtres (WMI), etc. Décocher la case pour bloquer le trafic sur les ports du système.	S.O.

Champ	Description	Exemple
(Exclure port(s)) Reserve Port(s) (Réserver le(s) port(s))	Le ou les ports que vous souhaitez que l'agent TS ignore. Saisissez les ports que vous souhaitez exclure sous forme de liste séparée par des virgules. L'agent TS renseigne automatiquement les champs **Reserve Port(s) (Réserver le(s) port(s))** avec des valeurs de ports par défaut pour Citrix MA Client (2598), Citrix Provisioning (6910) et Windows Terminal Server (3389). Si vous n'excluez pas les ports appropriés, les applications nécessitant ces ports peuvent échouer. Si vous utilisez Citrix Provisioning et effectuez une mise à niveau à partir d'une version antérieure de TS Agent, vous devez saisir `6910` dans ce champ. La valeur que vous précisez dans le champ **Reserve Port(s)** (Réserver le(s) port(s)) de l'agent TS doit correspondre à l'un des **numéros de port du premier et du dernier UDP** de Citrix Provisioning. **ATTENTION** Si vous ne précisez pas le bon port, les clients ne pourront pas démarrer. **Remarque** Si un processus sur votre serveur utilise un port qui ne se trouve pas dans votre plage **System Ports** (Ports système) ou écoute sur celui-ci, vous devez exclure manuellement ce port à l'aide du champ (Exclure port[s]) **Reserve Port(s)** (Réserver port[s]). **Remarque** Si une application cliente est installée sur votre serveur et que l'application est configurée pour se lier à un connecteur à l'aide d'un numéro de port précis, vous devez utiliser le champ (Exclure port[s]) **Reserve Port(s)** (Réserver port[s]) pour exclure ce port de la traduction.	Généralement, l'un des éléments suivants : - `2598,3389` (les ports du client Citrix MA et du serveur de terminaux Windows) - `2598,3389, 6910` (les ports du client Citrix MA, du serveur de terminaux Windows et de Citrix Provisioning)

Paramètres de On-Prem Firewall Management Center

Vous pouvez configurer un appareil de système principal de connexion et, éventuellement, des appareils de système de

secours (basculement) :

- Si votre appareil de système est autonome, laissez la deuxième ligne de champs de connexion de l'API FMC/REST vide.
- Si votre appareil de système est déployé avec un appareil de secours (basculement), utilisez la première ligne pour configurer une connexion à l'appareil principal et la deuxième ligne pour configurer une connexion à l'appareil de secours (basculement).

Exemple de page à onglet **On-Prem** :

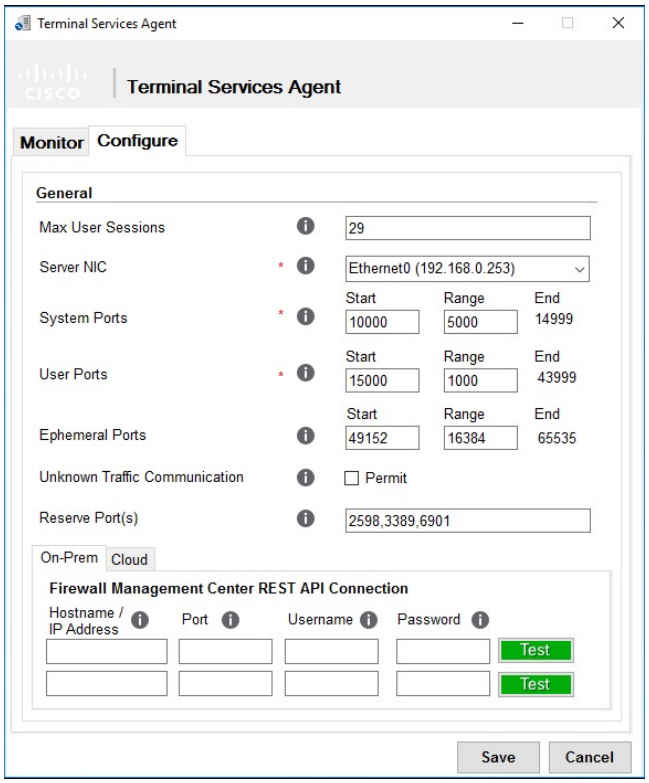

Tableau 2 : On-Prem Firewall Management Center

Champ	Description	Exemple
Nom d'hôte/adresse IP	Le nom d'hôte ou l'adresse IP de l'instance principale du ou du On-Prem Firewall Management Center.	`192.0.2.1`
Port	Le port que le ou le On-Prem Firewall Management Center utilise pour les communications de l'API REST. L'agent TS remplit automatiquement ce champ avec `443`, le port de l'API REST du ou du On-Prem Firewall Management Center.	`443`
Nom d'utilisateur et mot de passe	Le nom d'utilisateur et le mot de passe du ou du On-Prem Firewall Management Center pour un utilisateur disposant de privilèges REST VDI sur le ou le On-Prem Firewall Management Center. Pour plus d'informations sur la configuration de cet utilisateur, consultez Création du rôle VDI REST à la page 29.	S.O.

Création du rôle VDI REST

Créez le rôle d'utilisateur VDI REST dans Secure Firewall Management Center pour connecter l'agent TS. Attribuez ce rôle à l'utilisateur approprié afin de configurer correctement l'agent TS dans On-Prem Firewall Management Center.

Pour connecter l'agent TS à On-Prem Secure Firewall Management Center, l'utilisateur doit disposer du rôle VDI REST. Le VDI REST n'est pas défini par défaut. Vous devez créer le rôle et l'attribuer à tout utilisateur utilisé dans la configuration de l'Agent TS.

Pour en savoir plus sur les utilisateurs et les rôles, consultez *Guide de configuration des appareils du système de gestion de Cisco Secure Firewall*.

> **Remarque**
>
> Cette tâche s'applique uniquement à Centre de gestion de pare-feu local.
>
> Si vous utilisez Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), consultez Obtenir un jeton API à la page 20 à la place.

1. Connectez-vous au centre de gestion sécurisé en tant qu'utilisateur disposant des autorisations pour créer des rôles.
2. Cliquez sur **Administration** > **Users (Utilisateurs)System** > **Users** (Système > Utilisateurs).
3. Cliquez sur l'onglet **Rôles d'utilisateur**.
4. Dans la page de l'onglet User Roles (Rôles d'utilisateur), cliquez sur **Create User Role** (Créer le rôle d'utilisateur).
5. Dans le champ Name (nom), saisissez `REST VDI`.

   Le nom du rôle n'est pas sensible à la casse.
6. Dans la section enu-Based Permissions (Autorisations basées sur le menu), cochez **REST VDI** et assurez-vous que la case **Modify REST VDI** (Modifier REST VDI) est également cochée.
7. Cliquez sur **Save** (enregistrer).
8. Attribuez le rôle à l'utilisateur utilisé dans la configuration de l'agent TS.

Chapitre

4 Visualisation des données de l’agent TS

Sujets :

Sujets liés à l’utilisation de l’agent TS.

Afficher les renseignements sur l'Agent TS

Comment afficher les sessions utilisateur actuelles, les affectations de port et les détails des sessions dans l'agent TS, surveiller l'activité des sessions et exporter les données de dépannage pour la gestion des utilisateurs et les diagnostics.

Utilisez la procédure suivante pour afficher les sessions utilisateur actuelles sur le réseau et les plages de ports attribuées à chaque session. Les données sont en lecture seule.

1. Sur le serveur où vous avez installé l'Agent TS, démarrez l'interface de l'Agent TS comme décrit dans Lancer l'interface de configuration de l'agent TS à la page 18.
2. Cliquez sur l'onglet **Monitor** (Surveiller). Les colonnes suivantes s'affichent :
   - **ID du serveur REST**: nom d'hôte ou adresse IP du serveur Firepower Management Center qui rapporte les informations. Ces renseignements sont utiles si vous avez une configuration à haute disponibilité.
   - **Source IP** (IP source) : affiche la valeur de l'adresse IP de l'utilisateur au format IPv4 ou IPv6. Lorsque les adresses IPv4 et IPv6 sont configurées et qu'une nouvelle session vient d'être créée, les adresses IPv4 et IPv6 s'affichent sur des lignes distinctes.
   - **Status** (État) : affiche l'état de l'attribution de ports à l'utilisateur. Pour en savoir plus, consultez Afficher l'état de la connexion à la page 33.
   - **Session ID** (ID de session) : numéro qui identifie la session de l'utilisateur. Un utilisateur peut avoir plusieurs sessions à la fois.
   - **Username** (Nom d'utilisateur) : nom d'utilisateur associé à la session.
   - **Domain** (Domaine) : domaine Active Directory auquel l'utilisateur est connecté.
   - **Port Range** : plage de ports attribuée à l'utilisateur. (Une valeur de `0` indique un problème d'attribution de ports; pour en savoir plus, consultez Afficher l'état de la connexion à la page 33).
   - **TCP Ports Usage** (Utilisation des ports TCP) et **UDP Ports Usage** (Utilisation des ports UDP): affiche le pourcentage de ports alloués par utilisateur. Lorsque le pourcentage dépasse 50 %, l'arrière-plan du champ est jaune. Lorsque le pourcentage dépasse 80 %, l'arrière-plan du champ est rouge.
   - **Login Date** (Date de connexion) : date à laquelle l'utilisateur est connecté.
3. Le tableau suivant montre les actions que vous pouvez effectuer :

Article	Description
Cliquez sur un en-tête de colonne.	Triez les données du tableau en fonction de cette colonne.
	Saisissez une partie du nom d'utilisateur ou un nom d'utilisateur complet dans le champ de recherche **Filter by Username** (Filtrer par nom d'utilisateur).
	Cliquez sur cette page pour actualiser les sessions affichées sur cette page d'onglet.
	Exportez les informations de résolution de problèmes suivantes concernant l'agent TS en tant que fichiers texte : • Fichier XML contenant les données de configuration de l'agent TS • Sortie de la commande **netstat -a -n -o** • Liste des tâches de Windows • Liste des pilotes en cours d'exécution
	Cochez la case à côté d'une ou de plusieurs sessions afin de retransmettre ces sessions vers le Cloud-Delivered Firewall Management Center (centre de gestion de

Article	Description
	pare-feu en nuage) ou le On-Prem Firewall Management Center. Vous pouvez l'utiliser en cas de défaillance du service utilisateur sur le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou le On-Prem Firewall Management Center. Par exemple, supposons qu'un utilisateur se connecte au serveur de l'agent TS après la défaillance du service utilisateur sur le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou le On-Prem Firewall Management Center. Vous pouvez utiliser cette option pour renvoyer la session utilisateur après la restauration du service utilisateur. Cela devrait entraîner l'affichage du mot **Success** (Réussite) pour cet utilisateur dans la colonne Status (État).

Afficher l'état de la connexion

Affichez les utilisateurs et les plages de ports vus par l'agent TS.

Lorsque les utilisateurs se sont connectés aux services de terminaux où l'agent TS est installé, une nouvelle session système est créée, une plage de ports est attribuée à cette session et les résultats sont envoyés au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou au On-Prem Firewall Management Center pour être propagés aux périphériques gérés.

La page de l'onglet Monitor (Surveiller) vous permet de confirmer que la plage de ports a bien été envoyée au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou au On-Prem Firewall Management Center . Voici quelques-unes des raisons pour lesquelles le processus a peut-être échoué :

- Problèmes de connectivité réseau
- Identifiants VDI non valides
- Expiration du jeton
- Nom de domaine configuré pour le mauvais domaine

1. Sur le serveur où vous avez installé l'Agent TS, démarrez l'interface de l'Agent TS comme décrit dans Lancer l'interface de configuration de l'agent TS à la page 18.
2. Cliquez sur l'onglet **Monitor** (Surveiller).
3. La colonne Status (État) comporte l'une des valeurs suivantes :
   - **Pending** (En attente) : l'action est en attente, mais pas encore terminée.
   - **Failed** (Échec) : l'action a échoué. Cliquez sur le mot **Failed** (Échec) pour afficher un message d'erreur. Si l'erreur indique un échec de communication avec le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou le On-Prem Firewall Management Center, essayez de retransmettre le trafic de cette session comme indiqué dans Afficher les renseignements sur l'Agent TS à la page 32.
   - **Success** (Réussite) : l'action a bien été exécutée.

Afficher les données sur l'utilisateur de l'agent TS, les sessions utilisateur et les connexions TCP/UDP sur le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou le On-Prem Secure Firewall Management Center

Afficher les données sur l'activité de l'utilisateur sur l'agent TS.

Utilisez la procédure suivante pour afficher les données signalées par l'Agent TS. Pour plus d'informations sur les tableaux utilisateur, consultez le *Guide d'administration de Cisco Secure Firewall Management Center*.

1. Connectez-vous au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou au On-Prem Firewall Management Center. Assurez-vous qu'il s'agit de l'instance où vous avez configuré les domaines ciblant les utilisateurs que votre serveur surveille.
2. Pour afficher les utilisateurs dans le tableau Users (Utilisateurs) :

   Dans votre On-Prem Firewall Management Center , cliquez sur **Events & Logs (Événements et journaux)** > **Users (Utilisateurs)** > **User Details (Détails de l'utilisateur)**.

   Dans le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cliquez sur **Integrations (Intégrations)** > **Users (Utilisateurs)** > **User Details (Détails de l'utilisateur)**.

   Si votre session d'agent TS est active, Firewall Management Center affiche les valeurs des colonnes **Current IP** (Adresse IP actuelle), **End Port** (Port de fin) et **Start Port** (Port de début).

3. Pour afficher les sessions utilisateur dans le tableau d'activité des utilisateurs :

   Dans votre On-Prem Firewall Management Center , cliquez sur **Events & Logs (Événements et journaux)** > **Users (Utilisateurs)** > **User Activity (Activité de l'utilisateur)**.

   Dans le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cliquez sur **Integrations (Intégrations)** > **Users (Utilisateurs)** > **User Activity (Activité de l'utilisateur)**.

   Si l'agent TS signale une session utilisateur, vous voyez des valeurs dans les colonnes **Current IP** (Adresse IP actuelle), **End Port** (Port de fin) et **Start Port** (Port de début).

4. Pour afficher les connexions TCP/UDP dans le tableau des événements de connexion :

   Dans votre On-Prem Firewall Management Center , cliquez sur **Events & Logs (Événements et journaux)** > **+ Show more (Afficher plus)** > **Connection (Connexion)** > **Events (Événements)**.

   Dans le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cliquez sur **Events & Logs (Événements et journaux)** > **Analysis (Analyse)** > **Unified Events (Événements unifiés)**.

   Le champ **Initiator/Responder IP** (Adresse IP de l'initiateur/du répondeur) affiche l'adresse IP signalée par l'agent TS pour la connexion. Le champ **Source Port/ICMP Type** (Port source/type ICMP) affiche le port attribué à la connexion par l'agent TS.

Chapitre

5 Gestion de l’agent TS

Sujets :

Sujets liés à la gestion de l’agent TS.

Mettre fin à une session d'utilisateur en cours

Comment mettre fin à une session utilisateur à l'aide de l'agent TS.

Utilisez la procédure suivante pour déconnecter un utilisateur du réseau et mettre fin à la session.

1. Connectez-vous à votre serveur d'agent TS en tant qu'utilisateur avec des privilèges d'administrateur.
2. Ouvrez **Start** > **> [All Programs]** > **Task Manager** (Démarrer > [Tous les programmes], Gestionnaire de tâches).
3. Développez la fenêtre en cliquant sur **More Details** (Plus de détails).
4. Cliquez sur l'onglet **Users** (Utilisateurs).
5. (Facultatif) Pour informer un utilisateur que vous mettez fin à sa session, effectuez un clic droit sur la session utilisateur et choisissez **Send message** (Envoyer un message).
6. Faites un clic droit sur la session utilisateur et choisissez **Sign off** (Se déconnecter).
7. Cliquez sur **Sign out user** (Déconnecter l'utilisateur) pour confirmer l'action.

Visualisation de l'état du composant de service de l'agent TS

Comment confirmer que le service de l'agent TS est en cours d'exécution.

Utilisez la procédure suivante pour confirmer que le composant de service de l'agent TS est en cours d'exécution. Pour plus d'informations sur le composant de service, consultez À propos de l'agent Cisco Terminal Services (TS) à la page 10.

1. Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.
2. Ouvrez **Start (Démarrer)** > **Administrative Tools (Outils d'administration)** > **Services**.
3. Localisez `CiscoTSAgent` (Agent TS Cisco) et consultez le **Status** (État).
4. (Facultatif) Si le composant du service de l'agent TS est arrêté, démarrez le service d'agent TS comme décrit dans Démarrage et arrêt des processus de l'agent TS à la page 36.

Démarrage et arrêt des processus de l'agent TS

Comment démarrer et arrêter le logiciel de l'agent TS.

Utilisez la procédure suivante pour démarrer ou arrêter le composant de service de l'agent TS.

1. Connectez-vous à votre serveur en tant qu'utilisateur avec des privilèges d'administrateur.
2. Ouvrez **Start** > **Administrative Tools** > **Services** (Démarrer, Outils administratifs, services).
3. Accédez au `CiscoTSAgent` et cliquez avec le bouton droit pour accéder au menu contextuel.
4. Choisissez **Start** (Démarrer) ou **Stop** (Arrêter) pour démarrer ou arrêter le service de l'agent TS

Visualisation des journaux d'activité des agents TS sur le serveur

Affichez les journaux d'activité de l'agent TS.

Si le service d'assistance vous le demande, utilisez la procédure suivante pour afficher les journaux d'activité du composant du service.

Ouvrez **Tools** > **Event Viewer** > **Applications and Services Log** > **Terminal Services Agent Log** (Outils, Visualisateur d'événement, Journal des applications et des services, Journal des agents des services de terminaux).

Désinstallation de l’agent TS

Comment désinstaller le logiciel de l’agent TS.

Utilisez la procédure suivante pour désinstaller l'Agent TS de votre serveur. La désinstallation de l'Agent TS supprime l’interface, le service et le pilote de votre serveur. La désinstallation de l'Agent TS met également fin aux sessions utilisateur actives, comme cela est signalé au Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou au On-Prem Firewall Management Center. La modification de la cryptographie forte n’est pas supprimée.

1. Connectez-vous à votre serveur en tant qu’utilisateur avec des privilèges d’administrateur.
2. Ouvrez **Start** > **Control Panel** (Démarrer, Panneau de contrôle).
3. Cliquez sur **All Control Panel Items** > **Programs and Features** (Tous les éléments du panneau de commande, Programmes et fonctionnalités).
4. Faites un clic droit sur **Terminal Services Agent** (Agent des services de terminaux) et choisissez **Uninstall** (Désinstaller).

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.