



IBM® Technical Support Appliance

Livre blanc sur la sécurité de la connectivité

Version 2.8.0.0

Janvier 2021

Table des matières

Introduction	1
Documentation utile	1
Termes et définitions	1
Connectivité de Technical Support Appliance	3
Connectivité sortante sans serveur proxy.....	3
Connectivité sortante avec votre serveur proxy.....	3
Protocoles de sécurité et chiffrement	5
Communication entre Technical Support Appliance et IBM.....	5
Communication entre votre navigateur et Technical Support Appliance	5
Informations de maintenance transmises à IBM	6
Les raisons pour lesquelles TSA se connecte à IBM.....	6
Données transmises à IBM.....	6
Manipulation des données par IBM.....	7
Annexe A	8
Configuration requise pour les connexions au support IBM	8

Introduction

La solution IBM® Technical Support Appliance (TSA) inclut l'appliance IBM qui découvre, et partage avec le support IBM, les informations des matériels et logiciels du centre de données, et les rapports de service proactifs corrélés qu'IBM partage avec le Client. Ce document décrit les informations de connectivité, de sécurité et de maintenance transmises par TSA lors de la communication avec IBM Service Delivery Center (SDC).

Pour les informations de sécurité et de connectivité relatives aux points de terminaison avec lesquels TSA communique à l'intérieur du réseau d'un client, reportez-vous au [Guide de configuration TSA](#) ou au [Guide du programme d'aide à la configuration de TSA](#).

Documentation utile

Le lien ci-dessous mène directement au site web d'information dédié à Technical Support Appliance sur IBM.com. Vous y trouverez tout ce dont vous avez besoin pour commencer à utiliser IBM Technical Support Appliance. Vous pourrez consulter les guides de configuration et la documentation relative à la sécurité, étudier des exemples de rapports et télécharger le code d'installation de TSA à partir d'IBM Fix Central.

Pour en savoir plus sur Technical Support Appliance : <https://ibm.biz/TSAdemo>

Termes et définitions

Les utilisateurs doivent avoir une connaissance de base des réseaux et des protocoles IP (Internet Protocol). Voici la liste des termes et acronymes utilisés dans le présent document.

Terme	Définition
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
NIST	National Institute of Standards and Technology
RFC	Requests for Comments
RSA	Système de cryptographie à clé publique
SDC	Service Delivery Center
SNAT	Conversion d'adresse réseau source
SHA	Secure Hash Algorithm

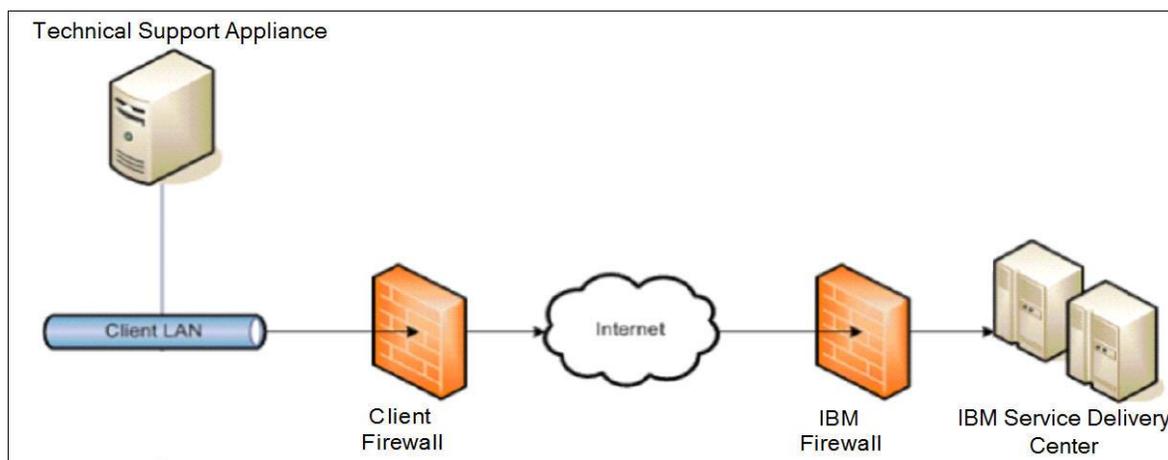
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSA	Technical Support Appliance
VPN	Virtual Private Network

Connectivité de Technical Support Appliance

TSA ne prend en charge que la connectivité Internet initiée de l'extérieur vers IBM. La connectivité avec les VPN et les modems ainsi que la connectivité entrante ne sont pas prises en charge.

Connectivité sortante sans serveur proxy

Le diagramme suivant montre la connexion de TSA à IBM sans serveur proxy. C'est la configuration par défaut.



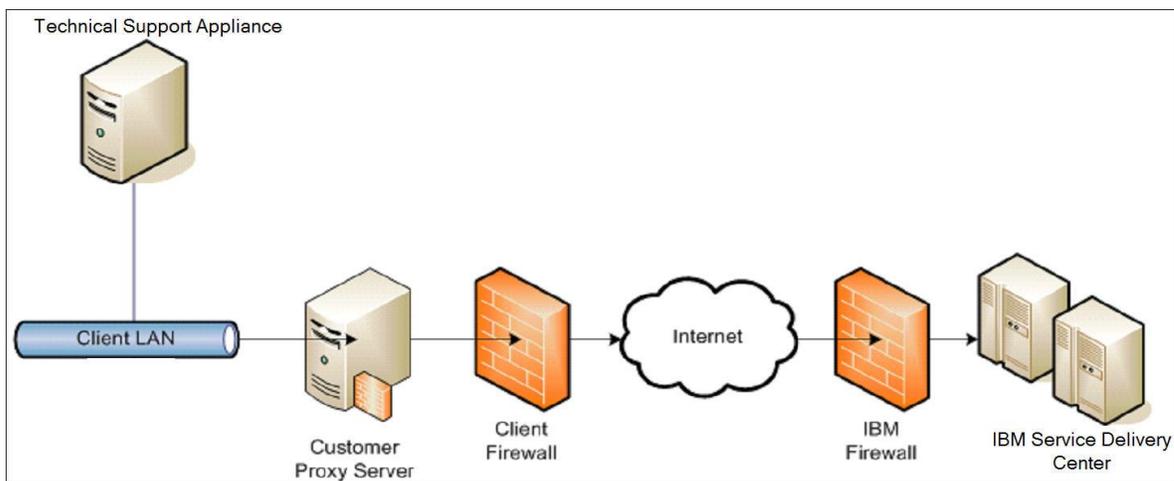
Dans cette configuration, TSA se connecte via votre connexion Internet en utilisant la route par défaut.

Pour que TSA communique sans problème, votre pare-feu externe doit permettre la libre circulation des paquets sortants via le port 443. Toutes les transactions utilisent le protocole HTTPS.

L'utilisation des règles SNAT (Conversion d'adresse réseau source) et celle de règles de masquage pour masquer l'adresse IP source de TSA sont toutes deux acceptables. Vérifiez que votre pare-feu autorise les connexions aux adresses IP IBM et aux ports spécifiés dans le tableau de l'[Annexe A](#).

Connectivité sortante avec votre serveur proxy

Le diagramme suivant montre la connexion de TSA à IBM avec un serveur proxy fourni par vous. Ce n'est pas la configuration par défaut et vous devrez configurer TSA pour utiliser votre proxy.



Pour transférer des paquets, le serveur proxy doit prendre en charge les fonctions d'en-tête proxy de base (telles que décrites dans la RFC #2616) et la méthode CONNECT. En option, l'authentification proxy de base (RFC #2617) peut être configurée pour que TSA s'authentifie avant de tenter de transférer des paquets via votre serveur proxy.

Pour configurer TSA pour l'utilisation d'un serveur proxy, voir « Configuration de la connectivité IBM » dans le Guide de configuration de TSA.

 L'inspection SSL n'est pas supportée ; si vous l'utilisez sur le proxy, désactivez-la pour ces flux.

Dans le cas des proxies Blue Coat, désactivez "Détection de protocole" pour les serveurs IBM. Ajoutez les règles de configuration suivantes :

- url.domain=esupport.ibm.com detect_protocol (none)
- url.address=129.42.54.189 detect_protocol (none)
- url.address=129.42.56.189 detect_protocol (none)
- url.address=129.42.60.189 detect_protocol (none)

Protocoles de sécurité et chiffrement

Communication entre Technical Support Appliance et IBM

TSA utilise le protocole HTTPS pour toutes les transactions, y compris la transmission des données d'inventaire entre votre site et IBM Service Delivery Center, le téléchargement des mises à jour logicielles et les informations de configuration. HTTPS est obtenu en encapsulant le protocole d'application HTTP dans le protocole cryptographique Transport Layer Security (TLS) version 1.2.

Communication entre votre navigateur et Technical Support Appliance

L'interface utilisateur web de TSA utilise le protocole HTTPS pour sécuriser les demandes administratives entre votre navigateur et TSA.

Informations de maintenance transmises à IBM

Cette section décrit les informations de maintenance transmises à IBM et les raisons pour lesquelles ces informations sont transmises lorsque TSA se connecte au Service Delivery Center IBM.

Les raisons pour lesquelles TSA se connecte à IBM

1. Transmission programmée et/ou manuelle des informations de maintenance, d'inventaire et de configuration système pour utilisation dans les rapports Client TSA
2. Tests de connectivité manuels et périodiques automatisés pour IBM
3. Vérifications manuelles et automatiques de la disponibilité des mises à jour du logiciel TSA
4. Téléchargements et mises à jour du logiciel TSA à l'initiative de l'utilisateur
5. Enregistrement des informations de contact et de localisation

Données transmises à IBM

Ce tableau présente les données transmises à IBM, le composant TSA qui collecte les informations et une description du contenu.

Type de données	Composant	Description
Informations de maintenance matérielle	Discovery Manager	TSA collecte des informations matérielles telles que le fabricant, le type de machine, le modèle, le numéro de série et certains éléments matériels tels que la mémoire, les unités centrales et le stockage connecté.
Informations de maintenance logicielle	Discovery Manager	TSA collecte des informations logicielles telles que le fabricant, l'identifiant du produit et des éléments logiciels sélectionnés tels que la version, le niveau de correction et les éléments prérequis.
Informations de base sur la configuration de l'appliance	Discovery Manager	Les informations relatives à l'ensemble de périmètres, la version de TSA et l'ID unique de TSA sont transmis afin d'associer les points de terminaison découverts à votre TSA spécifique. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Les informations d'identification de TSA et des points de terminaison ne sont jamais transmises.</div>
Informations de	Interface utilisateur	Les informations de contact client fournies

contact client	TSA	<p>dans l'interface utilisateur de TSA sont transmises et stockées de façon sécurisée par IBM. Ces informations sont utilisées pour associer les données d'inventaire à un client spécifique et ne sont utilisées que par le personnel de service IBM désigné pour contacter les clients au sujet de la maintenance et du support de leurs produits.</p> <div data-bbox="894 449 1425 537" style="border: 1px solid black; padding: 5px;">  Les informations de contact client sont facultatives. </div>
----------------	-----	---

Manipulation des données par IBM

Les données transmises sont stockées dans la base de données Client sécurisée d'IBM et protégées par un pare-feu. L'accès à ces données est limité au sein d'IBM, conformément aux politiques de sécurité d'IBM.

Les rapports TSA ne sont accessibles que par le personnel de support IBM désigné, par exemple votre équipe de compte. D'autres membres du support IBM peuvent y accéder pour vous aider si nécessaire.

Toutes les données sont associées à un identifiant unique et peuvent être purgées si nécessaire.

Annexe A

Configuration requise pour les connexions au support IBM

TSA se connecte au support IBM via une connexion directe ou via un proxy fourni par l'utilisateur qui doit être configuré pour permettre la communication avec IBM.

Toutes les transactions TSA vers le support IBM sont acheminées via un cluster de serveurs composé de plusieurs machines physiques dont la charge est répartie via un seul nom d'hôte. Cet environnement serveur est entièrement compatible NIST SP800-131A, prend en charge le protocole TLS 1.2, les fonctions de hachage SHA-256 ou supérieures et les clés RSA d'au moins 2048 bits.

Pour que TSA communique sans problème, le pare-feu externe doit permettre les connexions sortantes via le port 443. Vérifiez que votre pare-feu autorise les connexions aux adresses IP et aux ports du tableau ci-dessous.

Nom d'hôte	Adresses IP	Port(s)	Protocole
esupport.ibm.com	129.42.54.189	443	HTTPS (vers IBM)
	129.42.56.189		
	129.42.60.189		

Mentions légales

© IBM Corporation 2021
IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
Produit aux États-Unis
Janvier 2021.
Tous droits réservés

Ce document a été élaboré pour les produits et/ou services offerts aux États-Unis. IBM peut ne pas proposer les produits, fonctionnalités ou services décrits dans ce document dans d'autres pays.

Ces informations peuvent être modifiées sans préavis. Consultez votre interlocuteur IBM local pour obtenir des informations sur les produits, fonctionnalités et services disponibles dans votre région.

Toutes les déclarations concernant les orientations et intentions futures d'IBM peuvent être modifiées ou retirées sans préavis et ne représentent que des buts et des objectifs.

IBM, le logo IBM, POWER, System I, System p et i5/OS sont des marques ou des marques déposées d'International Business Machines Corporation aux États-Unis et/ou dans d'autres pays. La liste complète des marques détenues par IBM aux États-Unis se trouve à l'adresse <http://www.ibm.com/legal/copytrade.shtml>.

Blue Coat est une marque déposée de Blue Coat Systems.

Les autres noms de sociétés, de produits et de services peuvent être des marques de commerce ou des marques de service de tiers.

Les produits matériels IBM sont fabriqués à partir de pièces neuves ou de pièces neuves et de seconde main. Quel que soit le cas, nos conditions de garantie s'appliquent.

Cet équipement est soumis aux règles de la Federal Communications Commission (FCC). Il se conformera aux règles de la FCC avant la livraison finale à l'acheteur.

Les informations concernant les produits non IBM ont été obtenues auprès des fournisseurs de ces produits.

Les questions sur les capacités des produits non IBM doivent être adressées aux fournisseurs.

La page d'accueil d'IBM sur Internet se trouve à l'adresse <http://www.ibm.com>.