IBM® Technical Support Appliance Connectivity Security – Whitepaper

Version 2.7.0.0

August 2020

Inhaltsverzeichnis

Einführung

Die TSA-Lösung (Technical Support Appliance) von IBM® umfasst die IBM Appliance, die Informationen zu Hardware- und Softwareprodukten für Rechenzentren erkennt und für IBM Support freigibt, sowie die entsprechenden proaktiven Serviceberichte, die IBM für den Kunden freigibt. In diesem Dokument werden die Konnektivitäts-, Sicherheits- und Serviceinformationen beschrieben, die von TSA bei der Kommunikation mit dem IBM Service Delivery Center (SDC) übertragen werden.

Sicherheits- und Konnektivitätsinformationen, die TSA zu Endpunkten innerhalb eines Kundennetzes überträgt, finden Sie im TSA-Installationshandbuch oder im Leitfaden zum TSA-Konfigurationsassistenten.

Hilfreiche Dokumentation

Über den folgenden Link gelangen Sie direkt zur Website mit Informationen zur Technical Support Appliance auf IBM.com. Hier finden Sie alles, was Sie für den Einstieg in die IBM Technical Support Appliance brauchen. Sie können auf Installationshandbücher und sicherheitsspezifische Dokumentation zugreifen, Beispielberichte anzeigen und den Installationscode der virtuellen Appliance von IBM Fix Central herunterladen.

Weitere Informationen zur Technical Support Appliance: https://ibm.biz/TSAdemo

Begriffe und Definitionen

Benutzer sollten über ein grundlegendes Verständnis zu IP-Netzwerken und -Protokollen verfügen. Im Folgenden finden Sie eine Liste der in diesem Dokument verwendeten Begriffe und Akronyme.

Begriff	Definition
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
NIST	National Institute of Standards and Technology
RFC	Requests for Comments
RSA	Ein Verschlüsselungssystem mit öffentlichem Schlüssel
SDC	Service Delivery Center
SNAT	Source Network Address Translation

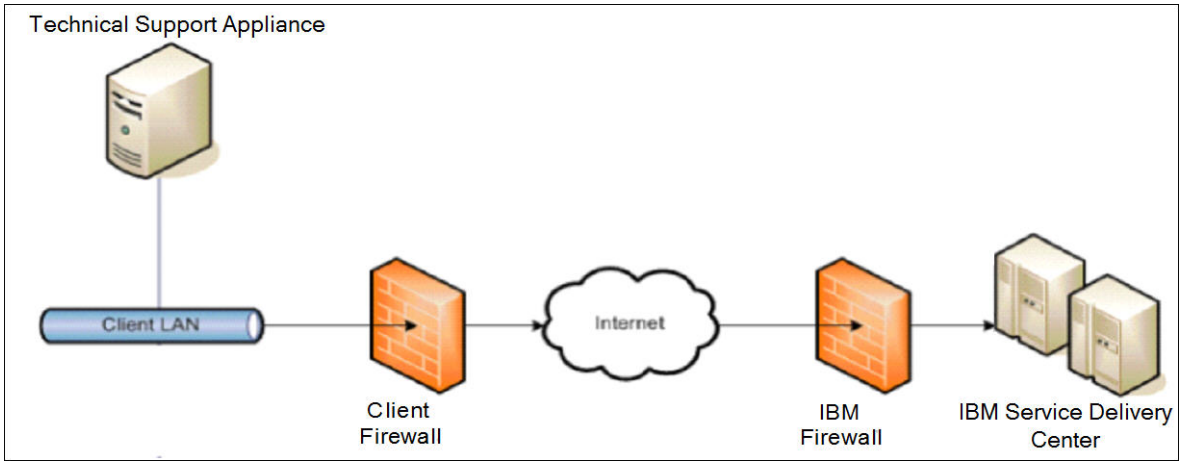
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSA	Technical Support Appliance
VPN	Virtual Private Network

Technical Support Appliance – Konnektivität

TSA unterstützt nur ausgehend initiierte Internetkonnektivität mit IBM. VPN, Modem und eingehende Konnektivität werden nicht unterstützt.

Ausgehende Konnektivität ohne Proxy-Server

In der folgenden Abbildung ist eine Verbindung zwischen TSA und IBM ohne Proxy-Server dargestellt. Dies ist die Standardkonfiguration.



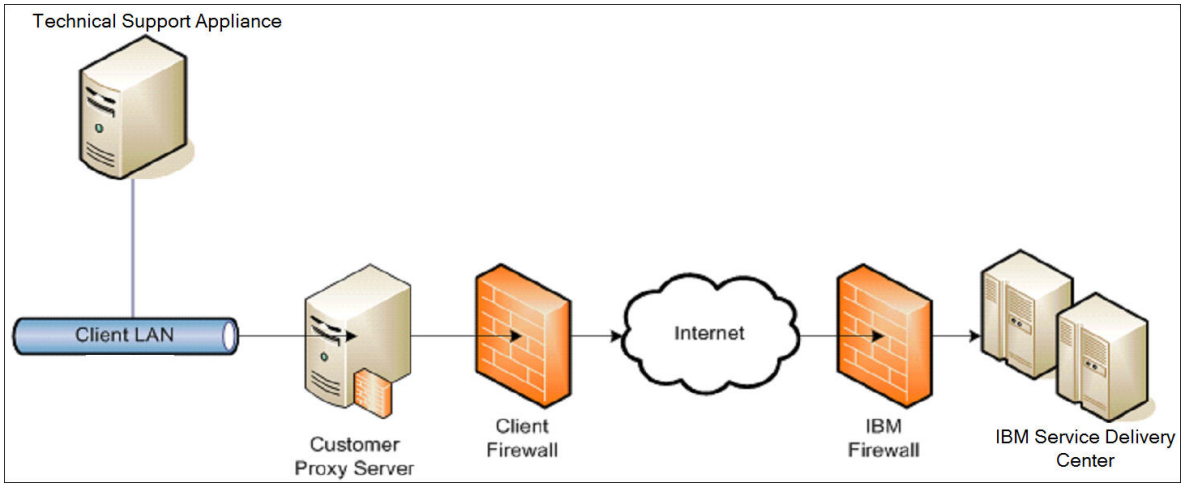
Bei dieser Konfiguration nutzt TSA Ihre Internetverbindung über die Standardroute.

Damit TSA erfolgreich kommunizieren kann, muss Ihre externe Firewall zulassen, dass ausgehende Pakete über Port 443 frei übertragen werden können. Für alle Transaktionen wird das HTTPS-Protokoll verwendet.

Es können SNAT-Regeln (Source Network Address Translation) und Maskierungsregeln zum Verbergen der IP-Quelladresse der TSA verwendet werden. Sorgen Sie dafür, dass Ihre Firewall Verbindungen mit den IP-Adressen und Ports von IBM in der Tabelle in Anhang A zulässt.

Ausgehende Konnektivität mit Proxy-Server

In der folgenden Abbildung ist eine Verbindung zwischen TSA und IBM mit einem von Ihnen bereitgestellten Proxy-Server dargestellt. Hierbei handelt es sich nicht um die Standardkonfiguration. Sie müssen TSA konfigurieren, wenn Ihr Proxy verwendet werden soll.



Zum Weiterleiten von Paketen muss der Proxy-Server die grundlegenden Proxy-Header-Funktionen (wie in RFC 2616 beschrieben) und die CONNECT-Methode unterstützen. Optional kann die grundlegende Proxy-Authentifizierung (RFC 2617) konfiguriert werden, sodass TSA vor dem Weiterleiten von Paketen über Ihren Proxy-Server eine Authentifizierung vornimmt.

Verwenden Sie zum Konfigurieren von TSA einen Proxy-Server. Informationen hierzu finden Sie im Abschnitt „IBM Konnektivität einrichten“ im TSA-Installationshandbuch.

Die SSL-Prüfung wird nicht unterstützt. Wenn Sie die SSL-Prüfung auf dem Proxy-Server verwenden, müssen Sie sie für diese Datenflüsse inaktivieren.

Wenn Sie Blue Coat-Proxys verwenden, inaktivieren Sie die Protokollerkennung für IBM Server. Fügen Sie die folgenden Konfigurationsregeln hinzu:

- 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)

Sicherheitsprotokolle und Verschlüsselung

Kommunikation zwischen der Technical Support Appliance und IBM

TSA verwendet für alle Transaktionen wie etwa bei der Übertragung von Bestandsdaten zwischen Ihrem Standort und dem IBM Service Delivery Center, beim Herunterladen von Software-Updates und Konfigurationsinformationen das HTTPS-Protokoll. HTTPS wird durch Einbinden des HTTP-Anwendungsprotokolls in das Verschlüsselungsprotokoll Transport Layer Security (TLS) Version 1.2 erreicht.

Kommunikation zwischen Ihrem Browser und der Technical Support Appliance

Die TSA-Webbenutzerschnittstelle verwendet das HTTPS-Protokoll für die Sicherheit von Verwaltungsanforderungen zwischen Ihrem Browser und der Appliance.

An IBM übertragene Serviceinformationen

In diesem Abschnitt wird beschrieben, dass Serviceinformationen an IBM übertragen werden, und es werden die Gründe für das Senden dieser Informationen beim Herstellen einer Verbindung zwischen TSA und IBM Service Delivery Center erläutert.

Gründe dafür, dass TSA eine Verbindung mit IBM herstellt

1. Geplante und/oder manuelle Übertragung von Service-, Bestands- und Systemkonfigurationsinformationen zur Verwendung in TSA-Kundenberichten
2. Manuelle und regelmäßige automatisierte Tests der Konnektivität mit IBM
3. Manuelle und automatische Überprüfung der Verfügbarkeit von TSA-Software-Updates
4. Vom Benutzer eingeleitete TSA-Software-Downloads und -Updates
5. Registrierung von Kontakt- und Standortinformationen

An IBM übertragene Daten

In dieser Tabelle sind die an IBM übertragenen Daten und die TSA-Komponenten aufgeführt, die diese Daten erfassen. Zudem enthält die Tabelle eine Beschreibung der jeweiligen Inhalte.

Datentyp	Komponente	Beschreibung
Informationen zum Hardware-Service	Discovery Manager	TSA erfasst Hardwareinformationen wie Hersteller, Systemtyp, Modell und Seriennummer sowie Informationen zu ausgewählten Hardwareelementen wie zu Hauptspeicher, CPUs und angeschlossenen Speichereinheiten.
Informationen zum Software-Service	Discovery Manager	TSA erfasst Softwareinformationen wie Hersteller und Produkt-ID sowie Informationen zu ausgewählten Softwareelementen wie zu Version, Fix-Level und Voraussetzungen.
Grundlegende Konfigurationsinformationen zur Appliance	Discovery Manager	Bereichsgruppeninformationen, Appliance-Version und die eindeutige Appliance-ID werden übertragen, um erkannte Endpunkte Ihrer jeweiligen TSA zuzuordnen. Berechtigungsnachweisinformationen für TSA und Endpunkt werden nicht übertragen.

Informationen zum Kundenkontakt	Die TSA-Benutzerschnittstelle	Informationen zum Kundenkontakt, die in der TSA-Benutzerschnittstelle bereitgestellt werden, werden übertragen und bei IBM sicher gespeichert. Diese Informationen werden verwendet, um Bestandsdaten einem bestimmten Kunden zuzuordnen. Sie werden nur von berechtigten IBM Service-Mitarbeitern zur Kontaktaufnahme mit Kunden im Rahmen von Service- und Supportleistungen für die entsprechenden Produkte verwendet.  Informationen zu Ansprechpartnern bei Kunden können optional angegeben werden.

Datenverarbeitung bei IBM

Übertragene Daten werden in der sicheren Kundendatenbank von IBM gespeichert und der Zugriff darauf wird durch eine Firewall eingeschränkt. Der Zugriff auf diese Daten ist innerhalb von IBM gemäß den IBM Sicherheitsrichtlinie eingeschränkt.

Auf TSA-Berichte können nur berechtigte IBM Support-Mitarbeiter wie etwa Mitarbeiter des Kundenteams und andere IBM Support-Mitarbeiter zugreifen, die Sie bei Bedarf unterstützen.

Allen Daten wird eine eindeutige ID zugewiesen. Und alle Daten können bei Bedarf gelöscht werden.

Anhang A

Konfigurationsanforderungen für Verbindungen zum IBM Support

TSA stellt eine Verbindung mit dem IBM Support über eine Direktverbindung oder über einen vom Benutzer bereitgestellten Proxy her, der so konfiguriert sein muss, dass er die Kommunikation mit IBM zulässt.

Alle TSA-Transaktionen an den IBM Support werden über einen Server-Cluster weitergeleitet, der aus mehreren physischen Maschinen besteht, bei denen das Load-Balancing über einen zentralen Hostnamen erfolgt. Die Serverumgebung ist vollständig kompatibel mit NIST SP800-131A, unterstützt das TLS-Protokoll 1.2, verwendet Hashfunktionen gemäß SHA-256 oder höher und RSA-Schlüssel mit einer Stärke von mindestens 2048 Bit.

Damit TSA erfolgreich kommunizieren kann, muss die externe Firewall über Port 443 ausgehende Verbindungen zulassen. Sorgen Sie dafür, dass Ihre Firewall Verbindungen mit den IP-Adressen und Ports in der folgenden Tabelle zulässt.

Hostname	IP-Adresse(n)	Port(s)	Protokoll
esupport.ibm.com	129.42.54.189	443	HTTPS (an IBM)
	129.42.56.189		
	129.42.60.189		

Bemerkungen

IBM Deutschland GmbH IBM-Allee
1 71139 Ehningen ibm.com/de
IBM Österreich Obere Donaustrasse
95 1020 Wien ibm.com/at
IBM Schweiz Vulkanstrasse 106 8010
Zürich ibm.com/ch

August 2020.

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem US-amerikanischen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an.

Die in dieser Dokumentation enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich.

Jegliche Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

IBM, das IBM Logo, POWER, System I, System p, i5/OS sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter http://www.ibm.com/legal/copytrade.shtml.

Blue Coat ist eine eingetragene Marke von Blue Coat Systems.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken oder Servicemarken anderer Hersteller sein.

IBM Hardwareprodukte sind aus fabrikneuen Teilen oder aus neuen und gebrauchten Teilen hergestellt. Unabhängig davon gelten die jeweiligen Bestimmungen zum Herstellerservice von IBM.

Dieses Produkt unterliegt den FCC-Vorschriften. Das Produkt wird auf die Einhaltung der entsprechenden FCC-Vorschriften geprüft, bevor es endgültig an den Käufer ausgeliefert wird.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte.

Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die IBM Homepage finden Sie im Internet unter http://www.ibm.com.