IBM® Technical Support Appliance

连接安全性白皮书

V2.7.0.0

2020 年 8 月

目录

简介

IBM® Technical Support Appliance (TSA) 解决方案包含用于发现并与 IBM 支持人员共享数据中心硬件和软件产品信息的 IBM 设备，以及 IBM 与客户共享的相关主动服务报告。本文档描述了 TSA 与 IBM Service Delivery Center (SDC) 通信时的连接性、安全性以及传输的服务信息。

有关客户网络中与 TSA 进行通信的端点的安全性和连接信息，请参考《TSA 设置指南》或《TSA 配置助手指南》。

文档

下面的链接会将您直接转至 IBM.com 上的 Technical Support Appliance 信息 Web 站点。您可在此处找到开始使用 IBM Technical Support Appliance 所需的所有内容。您可以访问设置指南和安全文档，查看样本报告，以及从 IBM Fix Central 下载虚拟设备安装代码。

了解有关 Technical Support Appliance 的更多信息：https://ibm.biz/TSAdemo

术语和定义

用户应该了解因特网协议（IP）网络和协议的基本知识。以下是在本文档中使用的术语和首字母缩略词的列表。

术语	定义
HTTP	超文本传输协议
HTTPS	安全超文本传输协议
IP	因特网协议
NIST	美国国家标准技术学会
RFC	请求评论
RSA	公钥密码体制
SDC	Service Delivery Center
SNAT	源网络地址转换

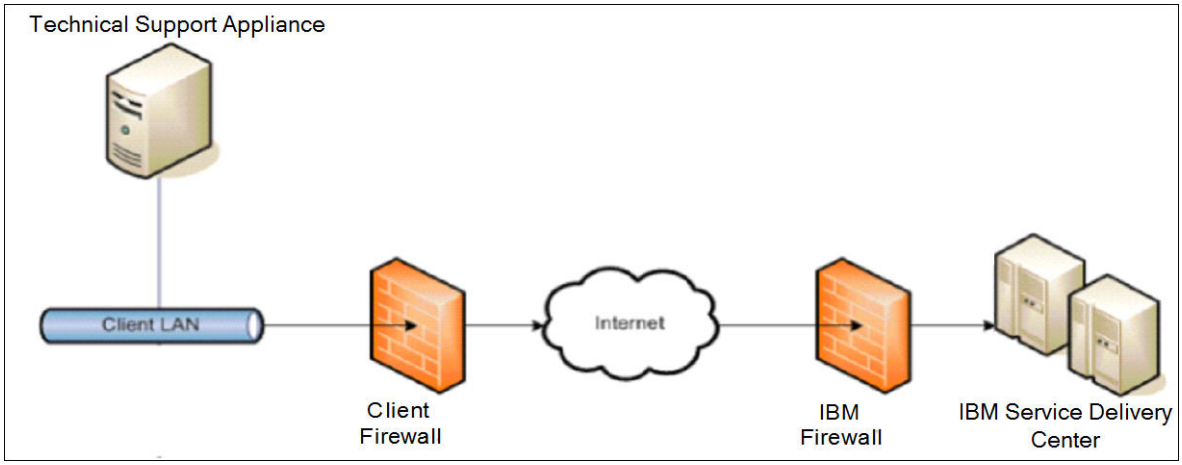
SHA	安全散列算法
SSL	安全套接字层
TCP	传输控制协议
TLS	传输层安全性
TSA	Technical Support Appliance
VPN	虚拟专用网

Technical Support Appliance 连接

TSA 仅支持到 IBM 的出站发起的因特网连接。不支持 VPN、调制解调器和入站连接。

无代理服务器的出站连接

下图展示了 TSA 在不使用代理服务器情况下连接到 IBM。这是缺省设置。



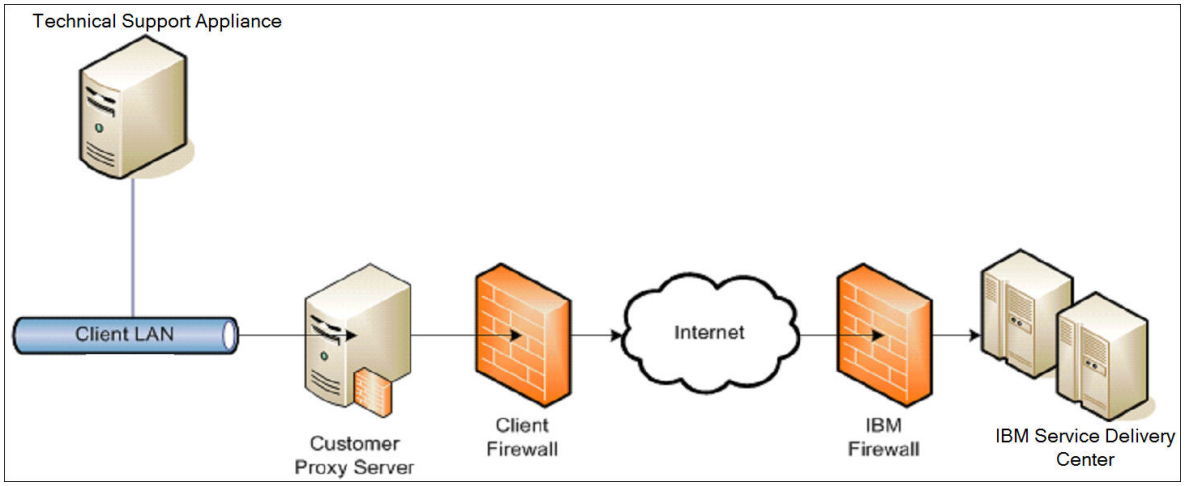
在此设置中，TSA 使用缺省路由通过因特网连接进行连接。

为使 TSA 成功通信，您的外部防火墙必须允许出站包自由流经端口 443。所有事务都使用 HTTPS 协议。

允许使用源网络地址转换 (SNAT) 和 masquerade 规则以隐藏 TSA 的源 IP 地址。确保防火墙允许连接到附录 A 的表中的 IBM IP 地址和端口。

使用代理服务器的出站连接

下图展示了 TSA 使用您提供的代理服务器连接到 IBM。这不是缺省设置，您将需要配置 TSA 以使用代理。



要转发数据包，代理服务器必须支持基本代理头函数（如 RFC #2616 中所述）和 CONNECT 方法。（可选）可以配置基本代理认证 (RFC #2617)，从而使 TSA 在尝试通过代理服务器转发数据包之前进行认证。

要配置 TSA 以使用代理服务器，请参阅《TSA 设置指南》中的“设置 IBM Connectivity”。

不支持 SSL 检查，如果在代理服务器上使用，请针对这些流禁用。

对于 Blue Coat 代理，禁用指向 IBM 服务器的“协议检测”。添加以下配置规则：

- 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)

安全协议和加密

Technical Support Appliance 与 IBM 之间的通信

TSA 将 HTTPS 协议用于所有传输，包括在您的站点和 IBM Service Delivery Center 之间传输库存数据、下载软件更新和配置信息。通过在传输层安全性 (TLS) V1.2 加密协议中封装 HTTP 应用协议，实现 HTTPS。

浏览器与 Technical Support Appliance 之间的通信

TSA Web 用户接口使用 HTTPS 协议来保护浏览器与设备之间的管理请求。

发送给 IBM 的服务信息

此部分概述了在 TSA 连接到 IBM Service Delivery Center 时传输给 IBM 的服务信息以及发送此信息的原因。

TSA 连接到 IBM 的原因

1. 计划安排和/或手动传输服务、库存和系统配置信息以供用于客户 TSA 报告
2. 手动和定期自动测试与 IBM 的连接
3. 手动和自动检查 TSA 软件更新可用性
4. 用户启动的 TSA 软件下载和更新
5. 注册联系人和位置信息

传输给 IBM 的数据

此表展示了传输给 IBM 的数据、收集信息的 TSA 组件以及内容的描述。

数据类型	组件	描述
硬件维护信息	发现作业管理器	TSA 收集硬件信息，例如，制造商、机器类型、型号、序列号，以及选定的硬件元素，例如，内存、CPU 和连接的存储器。
软件维护信息	发现作业管理器	TSA 收集软件信息，例如，制造商、产品标识，以及选定的软件元素，例如，版本、修订级别和必备条件。
基本设备配置信息	发现作业管理器	将传输范围集信息、设备版本和唯一设备标识，以便将发现的端点与特定 TSA 相关联。 从不传输 TSA 和端点凭证信息。
客户联系人信息	TSA 用户接口	将 TSA 用户界面中提供的客户联系人信息传输给 IBM 并进行安全存储。此信息用于将库存数据与特定客户相关联，并且仅供指定的 IBM 服务人员用来就产品

		服务和支持联系客户。 • 可以选择提供客户个人联系信息。

IBM 的数据处理

传输的数据存储在 IBM 的安全客户数据库中，并且受防火墙限制。仅限于依据 IBM 安全策略在 IBM 内访问此数据。

TSA 报告仅可供指定的 IBM 支持人员访问，例如，您的客户团队，以及供其他 IBM 支持人员在需要时访问，以便为您提供帮助。

所有数据都与唯一标识相关联，并且根据需要进行清除。

附录 A

连接到 IBM 支持人员的配置需求

TSA 通过直接连接或者通过用户提供的代理（必须配置为允许与 IBM 通信）连接到 IBM 支持人员。

所有 TSA 事务将通过服务器集群发送给 IBM 支持人员，此集群包含通过单个主机名进行负载均衡的多台物理机器。此服务器环境完全符合 NIST SP800-131A，支持 TLS 1.2 协议、SHA-256 或更加强大的散列功能，具备至少 2048 位强度的 RSA 密钥。

要使 TSA 成功通信，外部防火墙必须允许端口 443 上的出站连接。确保防火墙允许连接到下表中的 IP 地址和端口。

主机名	IP 地址	端口	协议
esupport.ibm.com	129.42.54.189	443	HTTPS（到 IBM）
	129.42.56.189		
	129.42.60.189		

声明

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
美国出版

2020 年 8 月。

本文档是为在美国国内供应的产品和/或服务而编写的。IBM 可能在其他国家或地区不提供本文档中讨论的产品、功能特性或服务。

本信息可随时更改而不另行通知。有关您所在区域可获取的产品、功能特性和服务的信息，请向您当地的 IBM 业务联系人咨询。

所有关于 IBM 未来方向和意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

IBM、IBM 徽标、POWER、System I、System p 和 i5/OS 是 International Business Machines Corporation 在美国和/或其他国家或地区的商标或注册商标。可在 http://www.ibm.com/legal/copytrade.shtml 中找到 IBM 拥有的美国商标的完整列表。

Blue Coat 是 Blue Coat Systems 的注册商标。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

IBM 硬件产品可能使用新部件制造而成，也可能同时使用了新部件和二手部件。无论属于何种情况，我们的保修条款均适用。

此设备遵守 FCC 规则。在最终交付给买方前，此设备将遵守相应的 FCC 规则。

涉及非 IBM 产品的信息是从这些产品的供应商处获取的。

有关非 IBM 产品功能的问题应与这些供应商联系。

IBM 因特网主页为 http://www.ibm.com。