

niagara remote™

Niagara Remote™ 提供基于 Web 的远程访问功能,用户可从任何连接互联网的设备上访问 Niagara 工作站。无需额外的硬件、网关或 VPN。

产品定义

Niagara 技术框架® 用户在日常生活中经常需要远程连接到基于 Niagara 的设备网络。Niagara Remote 是 Niagara Cloud Suite 中的一项服务,可帮助您提高用户对部署进行故障排查、执行定期工程和维护工作的效率,或只是通过图形用户界面检查基于 Niagara 网络的所有操作的状态。Niagara Remote™ 让您可以通过 Web 浏览器远程访问 Niagara Supervisor 或 JACE,无需额外的硬件、网关或 VPN。

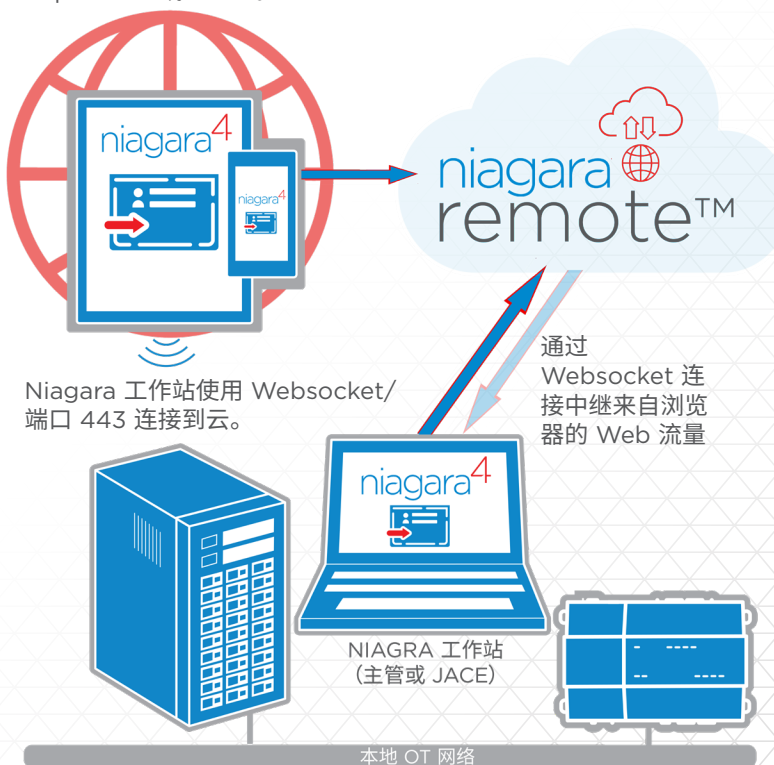
工作原理

Tridium 深知,在部署任何云解决方案时,网络安全往往是客户关心的一个关键问题。因此,Niagara Remote™ 的设计旨在执行以下程序:

- ▶ 在使用之前,用户要通过 Niagara Cloud Suite™ Management Portal 注册任何 Niagara Supervisor 或 JACE,以便进行远程管理。
- ▶ 注册完成后,Niagara 工作站会创建一个出站 Websocket 连接,通过 443 端口连接到 Niagara 技术框架。
- ▶ 要启动远程管理,用户需从浏览器登录 Niagara Cloud Suite™ Management Portal。
- ▶ 完成多因素身份验证 (MFA) 并应用最新的 TLS 加密后,Niagara Remote 将通过工作站的 Websocket 连接建立远程访问会话。

- ▶ 与工作站的远程访问会话建立后,用户必须使用其工作站凭证登录工作站。
- ▶ 要关闭远程会话,用户必须退出登录会话期间访问过的每个 Niagara Supervisor 或 JACE。

从任何配备浏览器的设备远程登录任何 Niagara Supervisor 或 JACE。



防火墙友好

- ▶ 所有用户和工作站之间的通信都在端口 443 上使用 HTTPS / WebSocket。
- ▶ Niagara 工作站启动与云的出站远程访问连接。不需要入站连接。
- ▶ 与工作站的所有通信均使用单个端点应用程序接口——api.niagara-cloud.com。

安全功能

- ▶ 远程访问工作站需要进行多因素身份验证。
- ▶ 基于角色的精细访问控制让您可以在工作站级别上管理用户访问。
- ▶ 所有通信均使用 TLS1.2 或更高版本。

先决条件

Niagara Remote 和其他 Niagara Cloud Suite 产品要求在整个订阅期间为每个 Niagara 实例提供有效的 Niagara 软件维护协议 (SMA)。最终用户应更新为 Niagara 技术框架的最新支持版本,并应用所有最新的网络威胁防护措施。这是 Tridium 针对所有 Niagara 技术框架产品的“默认安全”政策的另一个方面。

所有 Niagara Cloud Suite 产品的用户都可以访问 Niagara Cloud Management 门户。从此门户,用户可以设置和访问以下 Niagara Cloud Suite 服务:

对于系统集成商:

- ▶ 能够对客户唯一的云租户进行设备注册
- ▶ 能够创建合作伙伴视图层次结构,按主机 ID 描述客户、项目和订阅的设备
- ▶ 如果订阅了 Niagara Recover™,则能够创建和检索备份
- ▶ 能够分配客户用户

对于最终用户(建筑业主/物业经理):

- ▶ 查看其组织注册的设备
- ▶ 查看并检索备份(如果订阅了 Niagara Recover™)

订购信息

Niagara Remote 订阅可按 Niagara 实例(工作站)订购,订购价格为年度标价。

部件代码	说明
NCS-REMOTE	控制器级订阅
NCS-REMOTE-SUP	主管级订阅

要了解有关如何购买和开始使用 Niagara Remote™ 的更多信息,请联系您的 Tridium 客户经理或 Niagara 合作伙伴。



版权所有 © 2023 Tridium Inc. 保留所有权利。

tridium.com/cn/zh

本文发布的信息和/或规格截至本文发布之日为最新。Tridium, Inc. 保留更改或修改规格的权利,恕不另行通知。您可联系我们位于弗吉尼亚州里士满的公司总部,以获取最新版产品规格。本文所述产品或功能可能受一项或多项美国或外国专利的保护。仅在 Tridium 书面明确授权的情况下才可复制本文。不得以任何方式将本文全部或部分复制、复印、重现、翻译或删减为任何电子媒介或机器可读形式。

2023-0040CN