检查Umbrella Active Directory集成流程

目录

简介

本文档介绍Cisco Umbrella Active Directory(AD)集成中运营组件之间的通信流。

背景信息

了解Active Directory通信流有助于排除故障并确保部署前环境配置正确。

使用Umbrella Active Directory实施的通信流

AD连接器脚本在域控制器(DC)上运行时

Windows脚本使用HTTPS从域控制器(DC)到端口TCP/443上的云进行一次性连接，以将DC注册到仪表板。此对准允许连接器识别DC。使用特定参数对**https://api.opendns.com**进行调用。脚本成功注册DC后，它将显示在控制面板上。

问题有时可能与Windows上的根证书更新有关。要快速确定这一点，请导航到Internet Explorer并将浏览器指向：https://api.opendns.com/v2/OnPrem.Asset.**1005 Missing API key**.此操作将打印类似如下消息：如果任何证书错误或警告出现在该页面上，请确保已安装来自Microsoft的最新Root Certificates Update（根证书更新）。

AD连接器如何通信

AD连接器与Umbrella云服务或虚拟设备通信，如下所示：

- 云连接器

  如果发生更改，连接器使用端口443 TCP上的HTTPS连接每五分钟上传一次所有Active

Directory(AD)数据。仅上传有关组、用户和计算机的信息。不会上传密码，并且所有用户信息都会在本地进行哈希处理，从而使数据具有唯一性。

- 虚拟设备的连接器

  连接器使用端口443 TCP（未加密）持续向虚拟设备发送AD事件。 这是单向通信；设备无法与连接器进行通信。连接器和虚拟设备(VA)必须通过可信网络进行通信，这是必备条件。

- 与域控制器的连接器

  连接器使用端口389 TCP和3268 TCP/UDP与LDAP同步位于同一站点的所有域控制器通信。连接器还使用WMI/RPC与域控制器通信。端口135 TCP是RPC和WMI的标准端口。WMI还使用随机分配的端口，在Windows 2003及更早版本中，介于1024 TCP和65535 TCP之间，或在Windows 2008及更高版本中，介于49152 TCP和65535 TCP之间。自1.1.24版起，连接器还使用LDAP(LDAP over SSL)通过端口636 TCP和3269 TCP与域控制器通信。

如果发现通信问题，请检查可以阻止或丢弃数据的所有第7层应用代理。一个常见情况是基于DNS、HTTP或HTTPS等协议运行的Cisco设备上的检查功能。有关详细信息，请参阅我们的应用层协议检测文档。

虚拟设备(VA)到云

api.opendns.com虚拟设备经常通过端口443 TCP与端口53 TCP/UDP进行通信，以进行DNS查询或探测，并通过端口22、25、53、80、443或4766 TCP建立支持隧道。虚拟设备使用端口53 UDP/TCP、443 TCP、123 TCP和80 TCP与云通信。它们从端口443 TCP（非HTTPS连接）上的连接器接收数据，但不要求与它们进行回通信。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。