部署安全访问虚拟设备后脱机集成Active Directory

目录

问题

部署两个安全访问虚拟设备(VA)后，Active Directory(AD)集成在“安全访问”仪表板中停止运行。以前，AD集成运行正常，但在VA部署后，AD连接器现在在“安全访问”仪表板中显示为脱机状态。还原AD连接需要帮助。

环境

- 技术：解决方案支持（SSPT — 需要合同）
- 子技术：安全访问
- 软件版本:全部
- 安全访问(DNS-Advantage/Umbrella)
- 在总部部署两个安全访问虚拟设备(VA)
- 更改事件：在AD连接器故障之前立即安装VA
- AD连接器以前可正常运行，现在在安全访问门户中显示为脱机

分辨率

要解决VA部署后AD集成在Secure Access门户中显示为脱机的问题，请执行以下详细的故障排除步骤：

在连接器重新启动期间捕获网络流量

在重新启动连接器服务时，在AD连接器/域控制器的所有接口上运行Wireshark捕获。这有助于识别在连接器初始化期间的任何网络通信故障或未授权访问尝试。

第1步：在所有相关接口上开始Wireshark捕获

启动Wireshark并开始捕获所有AD连接器/域控制器接口。

第2步：通过Windows服务管理器重新启动连接器服务

打开services.msc，找到OpenDNS Connector service，然后单击Restart。

第3步：保存捕获文件以供进一步分析

停止捕获并导出.pcap文件。

收集连接器日志

从AD连接器收集日志，更深入地了解错误或身份验证问题：

1. 导航到日志目录。

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\vX.X.X
```

1. 收集相关日志文件并准备进行查看。将所有日志文件从上述目录复制到安全位置。

验证AD连接器帐户权限

引入虚拟设备后，AD连接器帐户需要特定权限才能正常工作。如果帐户缺少事件日志读取器角色，则可能会遇到未经授权的访问异常。

1. 为AD连接器帐户分配事件日志读取器权限。使用Active Directory用户和计算机(ADUC)或组策略将AD连接器帐户添加到事件日志读取器组。
2. 确认该帐户具有新权限。检查AD连接器帐户的组成员身份，以验证是否包含事件日志读取器。

发现常见异常

在故障排除过程中，日志或连接器状态输出中可能会观察到此异常：

```
* Exception type: system.unauthorizedaccessexception
message: Attempted to perform an unauthorized operation.
```

这表示AD连接器帐户没有足够的权限，尤其是事件日志读取器角色，该角色在引入VA后是必需的。

找不到CLI命令，显示从AD连接器状态脱机更改为联机。

原因

根本原因是在部署安全访问虚拟设备后，AD连接器帐户的权限不足。该帐户缺少事件日志读取器权限，这是正常AD连接器功能所必需的。这会导致“system.unauthorizedaccessexception”错误，并阻止连接器在安全访问门户中联机操作。

相关内容

- 思科技术支持和下载

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）。