排除Active Directory和VA的Umbrella错误

目录

简介

问题

环境

分辨率

- 虚拟设备
  - "此VA已注册，但从未同步"
  - “此VA一度同步，但后来停止了”
  - “此VA以前连接到一个或多个连接器，但现在未连接到任何连接器”
  - "此虚拟设备已连接到此站点的部分连接器，但并非所有连接器"
  - "此VA向Umbrella转发的DNS查询未加密"
  - "此VA未配置任何本地域"
  - “此VA在其站点内不是冗余的（每个站点需要2个以上的VA）”
  - "对此VA的大部分DNS查询失败"
- AD连接器
  - "此连接器已注册，但从未同步"
  - “此连接器曾同步过一次，但后来停止了”
  - "此连接器没有要连接的VA或直流电"
  - "此连接器没有要连接的DC"
  - “连接器可以连接一个或多个DC，但尚未连接到任何DC”
  - “连接器连接到某些（但不是全部）DC”
  - “连接器曾经连接过，但当前未连接到任何可用的DC”
  - “连接器可以连接一个或多个VA，但尚未连接到任何VA”
  - "连接器在尝试连接到某些VA时报告超时错误"
  - “连接器连接到某些（但不是全部）VA”
  - “连接器曾连接过，但当前未连接到任何可用的VA”
  - “连接器不会与VA并行同步事件。事件处理可能比预期慢”
  - "连接器正在报告在尝试向某些VA发送事件时发生的丢弃"
- 域控制器
  - “曾经连接到一个或多个连接器，但现在没有连接到任何连接器”
  - "此域控制器从未连接到连接器"
  - "此域控制器没有要连接的连接器"
  - "此域控制器已连接到某些但不是全部的连接器"
  - "此域控制器的WMI状态为关闭。域控制器未从连接器“ ”响应WMI连接

原因

相关内容

简介

本文档介绍Active Directory和虚拟设备的Umbrella错误故障排除。

问题

本文档概述了站点和Active Directory页面上的常见错误、警告和参考消息，并提供解决步骤。

虚拟设备、Active Directory(AD)连接器或域控制器(DC)的Umbrella Settings > Sites and AD页面上显示一个或多个错误、警告或信息消息。

环境

Umbrella Sites and Active Directory页面位于Settings > Sites and AD。

- 受影响的组件包括虚拟设备(VA)、AD连接器和DC。
- VA版本1.5.x或更高版本提供DNSCrypt支持。
- 如果连接器部署在Windows Server(WS)2012或更高版本上，并且已停止与Umbrella同步，请确保该连接器运行的是1.6.31或更高版本。
- 如果运行.NET 4.5.2或更高版本，则连接器版本1.6.31或更高版本在WS 2008/2008 R2上正常工作，但建议在支持的服务器上重新部署。
- 思科宣布传输层安全(TLS)1.0/1.1的寿命终止(EOL)。默认情况下，不支持的Windows版本（Windows Server 2008、2008 R2或Windows 7）不支持TLS 1.2。在支持的服务器版本（Windows Server 2012或更高版本）上重新安装连接器。
- 要将登录事件信息发送到虚拟设备，域控制器(DC)必须在同一站点中安装连接器。
- 站点必须至少包含消息所注明的每种组件类型之一。
- Umbrella Connector服务经过测试，每个CPU支持10个资产（域控制器和虚拟设备）。
- Umbrella连接器服务经测试可支持在Umbrella站点的所有域控制器中每秒约850个连续事件（无硬限制）。

分辨率

使用与设置 > 站点和AD上显示的组件类型匹配的部分，然后选择确切的消息文本。

- 虚拟设备:VA注册/同步状态、连接器关联、DNSCrypt、本地域、冗余和DNS查询失败消息。
- AD连接器:连接器注册/同步状态、DC/VA连接、超时、并行处理和事件丢弃消息。
- 域控制器:连接器关联和WMI连接消息。

虚拟设备

"此VA已注册，但从未同步"

1. 最多允许10分钟完成同步。
2. 确保满足网络要求。请参阅Active Directory通信流指南:Connectors > Virtual Appliances > DCs and the Cloud。
3. 如果问题仍然存在，请收集日志并打开支持案例。

“此VA一度同步，但后来停止了”

使用以下步骤恢复VA同步并确认所需的连接。

1. 如果删除了VA，请将其从Umbrella控制面板中删除：删除说明 — Umbrella Insights。
2. 确认网络要求。请参阅Active Directory通信流指南:Connectors > Virtual Appliances > DCs and the Cloud。
3. 如果问题仍然存在，请打开支持案例。

“此VA以前连接到一个或多个连接器，但现在未连接到任何连接器”

1. 如果删除了任何连接器，请忽略此消息并从控制面板中删除过时的连接器条目。
2. 确认网络要求。请参阅Active Directory通信流指南:Connectors > Virtual Appliances > DCs and the Cloud。
3. 如果问题仍然存在，请打开支持案例。

"此虚拟设备已连接到此站点的部分连接器，但并非所有连接器"

1. 如果删除了任何连接器，请忽略此消息并从仪表板中删除该连接器。
2. 确认必备条件：虚拟设备用户指南：先决条件.
3. 收集日志:提供AD连接器日志支持。
4. 如果问题仍然存在，请打开支持案例。

"此VA向Umbrella转发的DNS查询未加密"

DNSCrypt对从虚拟设备(VA)转发到Umbrella公共DNS解析器的DNS数据包进行加密，默认情况下处于启用状态。

1. 确认VA运行的是1.5.x版或更高版本。1.5.x或更高版本中提供DNSCrypt支持。如果只有一个VA且它未升级，请升级它：更新虚拟设备。
2. 检查防火墙和检查策略，确保端口53(UDP/TCP)上的DNSCrypt探测功能未被阻止或更改。如果入侵防御系统(IPS)或入侵检测系统(IDS)执行深度数据包检测并只期望DNS流量，则探测可能会失败。
3. 对于自适应安全设备(ASA)部署，请查看部署文档引用的数据包检测指南。

4. 如果警告仍然存在，请收集日志：通过AD连接器日志提供支持，然后打开支持案例。
5. 验证受影响的VA的Settings > Sites and AD上的警告是否已清除。

更多详情：新VA警告：在虚拟设备上启用DNSCrypt。

"此VA未配置任何本地域"

1. 确保本地域已配置：本地DNS转发。

“此VA在其站点内不是冗余的（每个站点需要2个以上的VA）”

1. 安装第二个VA以实现高可用性。有关每个站点运行两个虚拟设备的指导，请参阅Umbrella虚拟设备部署文档。

"对此VA的大部分DNS查询失败"

1. 收集相关的VA和连接器日志并打开支持案例。
2. 验证DNS查询失败率是否恢复正常，以及受影响的VA的Settings > Sites and AD上的错误是否清除。

AD连接器

"此连接器已注册，但从未同步"

使用以下检查确认初始同步已成功完成：

1. 最多允许10分钟完成同步。
2. 确保满足以下网络要求：身份集成：先决条件.
3. 收集日志:提供AD连接器日志支持。
4. 如果问题仍然存在，请打开支持案例。

“此连接器曾同步过一次，但后来停止了”

1. 确保满足网络要求。请参阅Active Directory通信流指南:Connectors > Virtual Appliances > DCs and the Cloud。
2. 思科宣布停用TLS 1.0/1.1。不支持的Windows版本（Windows Server 2008、2008 R2或Windows 7）默认不支持TLS 1.2。在支持的服务器版本（Windows Server 2012或更高版本

）上重新安装连接器。
3. 如果连接器部署在WS 2012或更高版本上，并且已停止与Umbrella同步，请确保连接器运行的是1.6.31或更高版本。
4. 如果运行.NET 4.5.2或更高版本，则连接器版本1.6.31或更高版本在WS 2008/2008 R2上正常工作，但建议在支持的服务器上重新部署。
5. 收集日志:提供AD连接器日志支持。
6. 如果问题仍然存在，请打开支持案例。

"此连接器没有要连接的VA或直流电"

1. 确保站点至少包含每种组件类型之一。
2. 查看安装文档：身份集成：必备条件和Active Directory集成>步骤2:准备Active Directory环境。

"此连接器没有要连接的DC"

1. 确保站点至少包含每种组件类型之一。
2. 查看安装文档：准备Active Directory环境。

“连接器可以连接一个或多个DC，但尚未连接到任何DC”

1. 最多允许10分钟完成同步。
2. 确保满足必备条件：身份集成：先决条件.
3. 收集日志:提供AD连接器日志支持。
4. 如果问题仍然存在，请打开支持案例。

“连接器连接到某些（但不是全部）DC”

1. 确认必备条件：身份集成：先决条件.
2. 收集日志:提供AD连接器日志支持。
3. 如果问题仍然存在，请打开支持案例。

“连接器曾经连接过，但当前未连接到任何可用的DC”

1. 确认必备条件：身份集成：先决条件.
2. 收集日志:提供AD连接器日志支持。
3. 如果问题仍然存在，请打开支持案例。

“连接器可以连接一个或多个VA，但尚未连接到任何VA”

1. 从控制面板中删除所有未使用的VA。
2. 删除后最多允许10分钟进行同步。
3. 确保满足以下网络要求：身份集成：先决条件.
4. 收集日志:提供AD连接器日志支持。
5. 如果问题仍然存在，请打开支持案例。

"连接器在尝试连接到某些VA时报告超时错误"

1. 如果虚拟设备与连接器不在相同的LAN上，请考虑使用Umbrella站点隔离部署：将多个Active Directory域连接到Umbrella。
2. 从控制面板中删除未使用的VA。
3. 删除后最多允许10分钟进行同步。
4. 确保满足以下网络要求：身份集成：先决条件.
5. 收集日志:提供AD连接器日志支持。
6. 如果问题仍然存在，请打开支持案例。

“连接器连接到某些（但不是全部）VA”

1. 从控制面板中删除未使用的VA。
2. 删除后最多允许10分钟进行同步。
3. 确保满足网络要求。请参阅Active Directory通信流指南:Connectors > Virtual Appliances > DCs and the Cloud。
4. 收集日志:提供AD连接器日志支持。
5. 如果问题仍然存在，请打开支持案例。

“连接器曾连接过，但当前未连接到任何可用的VA”

1. 从控制面板中删除未使用的VA。
2. 删除后最多允许10分钟进行同步。
3. 确保满足以下网络要求：Active Directory通信流指南:连接器>虚拟设备> DC和云。
4. 收集日志:提供AD连接器日志支持。
5. 如果问题仍然存在，请打开支持案例。

“连接器不会与VA并行同步事件。事件处理可能比预期慢”

1. 请注意，Umbrella Connector服务经过测试，每个CPU支持10个资产（域控制器和虚拟设备）。

2. 根据Umbrella站点中域控制器和虚拟设备的数量，使用所需的CPU数量升级服务器。
3. 收集日志:提供AD连接器日志支持。
4. 如果问题仍然存在，请打开支持案例。

"连接器正在报告在尝试向某些VA发送事件时发生的丢弃"

使用这些步骤可减少事件丢弃并恢复稳定的事件传输。

1. 检查Umbrella站点中所有域控制器的总事件速率是否超过每秒大约850个事件的已测试连续容量。
2. 如果事件速率超过此测试容量，请增加连接器主机上的CPU核心以提高处理吞吐量。
3. 如果丢弃持续存在，请启用具有两个或更多连接器的负载均衡以共享域控制器负载。必须通过Umbrella支持打开支持案例来启用此高级功能。

域控制器

“曾经连接到一个或多个连接器，但现在没有连接到任何连接器”

1. 如果连接器已移除，请重新部署连接器或移除域控制器。
2. 确认网络要求。请参阅Active Directory通信流指南:Connectors > Virtual Appliances > DCs and the Cloud。
3. 收集日志:提供AD连接器日志支持。
4. 如果问题仍然存在，请打开支持案例。

"此域控制器从未连接到连接器"

1. 要将有关登录事件的信息发送到虚拟设备，域控制器(DC)必须在同一站点中安装连接器。请参阅将Active Directory连接到Umbrella。
2. 收集日志:提供AD连接器日志支持。
3. 如果问题仍然存在，请打开支持案例。

"此域控制器没有要连接的连接器"

1. 要将有关登录事件的信息发送到虚拟设备，域控制器(DC)必须在同一站点中安装连接器。请参阅将Active Directory连接到Umbrella。
2. 如果重新安装连接器或将它从一台计算机移动到另一台计算机，请忽略此消息。

"此域控制器已连接到某些但不是全部的连接器"

1. 检查权限：Cisco_Connector用户所需的权限。
2. 收集日志:提供AD连接器日志支持。
3. 如果问题仍然存在，请打开支持案例。

"此域控制器的WMI状态为关闭。域控制器未从连接器“ ”响应WMI连接

1. 由于域控制器上的负载，这可能是一个临时问题。
2. 检查是否可以使用WBEMTest工具建立Windows Management Instrumentation(WMI)连接。
3. 通过停止监控安全事件的其他未使用的应用，减少DC上的负载。
4. 在减少DC负载后，重新启动连接器服务以启动新的WMI连接。
5. 收集日志:提供AD连接器日志支持。
6. 如果问题仍然存在，请打开支持案例。

原因

- DNSCrypt警告消息(VA):默认情况下，启用DNSCrypt以加密从虚拟设备(VA)转发到Umbrella公共DNS解析器的DNS数据包。如果防火墙或检查策略阻止或修改端口53(UDP/TCP)上的DNSCrypt探测，则探测失败。如果入侵防御系统(IPS)或入侵检测系统(IDS)执行深度数据包检测，并且只期望DNS流量，则探测失败。
- 连接器同步停止的消息（AD连接器）:思科宣布传输层安全(TLS)1.0/1.1的寿命终止(EOL)。不支持的Windows版本（Windows Server 2008、2008 R2或Windows 7）默认不支持TLS 1.2，这会导致连接器同步停止。
- 连接器性能消息（AD连接器）:Umbrella Connector服务经过测试，每个CPU支持10个资产（域控制器和虚拟设备）。超过此大小后，事件处理速度将比预期慢。
- 事件丢弃警告消息（AD连接器）:Umbrella连接器服务经测试可支持在Umbrella站点的所有域控制器中每秒约850个连续事件（无硬限制）。如果总速率超过此测试容量，则连接器会丢弃事件。
- WMI关闭错误消息（域控制器）:当域控制器处于负载下并且没有响应来自连接器的WMI连接时，WMI状态为关闭。

相关内容

- 检查Umbrella Active Directory集成流程
- 向Umbrella支持提交Active Directory连接器日志

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）。