了解Active Directory连接器性能

目录

简介

先决条件

- 要求
- 使用的组件

概述

每秒最大事件数

- 新功能

性能建议

- 连接器规格
- 专用连接器
- Umbrella站点
- 网络延迟
- 连接器数量
- 事件日志大小
- 第三方软件
- 防病毒软件
- 其他域控制器
- 服务帐户例外
- WMI修补程序
- WMI内存和句柄限制

DC负载均衡

虚拟设备并行通信

用户登录事件的加速传输

直接事件日志读取器连接

每秒事件数

简介

本文档介绍Umbrella DNS的Active Directory连接器性能。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Umbrella DNS。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

作为Umbrella Active Directory集成的一部分，Umbrella Connector服务用于监控用户/计算机登录事件。OpenDNS Connector服务从其站点中每个AD域控制器的安全事件日志读取登录信息。

在用户登录事件频率较高的环境中，必须查看这些性能指南。为了准确识别用户，连接器服务必须能够快速检索登录信息。

每秒最大事件数

可处理的事件数量没有硬性限制。Umbrella连接器服务经过测试，可支持在“站点”内的所有域控制器上每秒持续850个事件。 这基于不运行第三方软件的专用实验室环境。实际结果可能因网络延迟和其他瓶颈而异。

客户可以通过阅读本文后面的“每秒事件数”部分来确定大约事件数。

新功能

对于具有较高登录事件频率的较大型部署中的客户，Umbrella具有面向性能的新功能。除常规性能建议外，请阅读本文稍后有关负载均衡、并行通信和直接事件日志读取器连接方面的指南。

性能建议

连接器规格

运行Active Directory Connector服务的服务器必须具有Umbrella文档的“大小调整指南”中指定的CPU和内存资源。

专用连接器

虽然连接器服务可以直接安装在域控制器上，但Cisco Umbrella建议连接器安装在连接器服务专用的成员服务器上。此成员服务器必须未安装其他第三方软件。阅读Umbrella文档中有关安装过程的详细信息。

Umbrella站点

如果可能，Umbrella部署必须划分为“站点”，限制哪些组件在网络上通信。连接器服务只能与同一Umbrella站点中的组件通信。当用户部署分布在广阔的地理区域时，必须始终使用此功能。

通常为每个物理位置创建一个伞状站点。Umbrella站点必须在Umbrella文档中填写这些规则。

正确使用Umbrella站点可以极大地改善部署并防止组件通过广域网进行通信。

网络延迟

登录事件可以通过网络传输到连接器。 连接器和每个域控制器之间必须高速连接，以减少与网络相关的延迟。连接器可以尽可能靠近域控制器和虚拟设备。

连接器数量

每个Umbrella站点需要一个连接器。 在Umbrella站点中拥有多个连接器是可能的，但仅出于冗余目的而需要。添加连接器会增加域控制器上的负载，因为它们正在复制与第一个连接器相同的功能。Umbrella建议每个Umbrella站点最多2个连接器。

事件日志大小

大型Windows安全事件日志可能会对WMI操作的性能产生负面影响。 Umbrella建议限制事件日志大小。日志文件小于512MB时，可以获得最佳性能，但是，可根据日志保留要求调整该性能。可以使用以下说明调整日志文件大小：

1.打开Event Viewer应用程序(eventvwr.msc)。

2.转到Windows Logs > System

3.右键单击系统日志并选择属性。

4.根据需要调整日志文件的最大大小，然后选择确定。

第三方软件

许多其它软件产品也利用WMI，这可能会在域控制器上的WMI中造成瓶颈。这可能包括：

- 第三方安全/分析软件，用于监控事件日志
- Windows事件日志转发
- SIEM集成和监控事件日志的其他软件

如果不再需要任何此软件，我们建议将其禁用。 或者，可以使用附录中介绍的“Direct Event Log Reader Connection”方法缓解此问题。

防病毒软件

从防病毒扫描中排除此文件夹和以下可执行文件：

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\OpenDNSAuditService.exe
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>OpenDNSAuditClient.exe
```

其他域控制器

域控制器上的WMI通知系统将对每个事件日志条目进行队列和处理，并将它们发送到WMI订阅服务器。这实际上是一个推送机制，其中事件由DC发送。 因此，域控制器自身可能存在性能瓶颈，影响事件发送速度。

可以通过向AD环境添加其他域控制器来缓解此瓶颈。 Umbrella已经测试了单个域控制器，每秒最多850个事件。

服务帐户例外

通过排除服务帐户，减少Umbrella检测到的AD登录数。无论如何都必须排除这些帐户才能正确应用策略。 您还可以排除未使用AD用户策略但用户登录数量较大的服务器和其他设备。

WMI修补程序

请确保域控制器和连接器服务器使用最新的Microsoft修补程序。以下是解决已知WMI性能问题的修补程序示例。

WMI内存和句柄限制

WMI包含自己的内部限制，这可能会造成瓶颈。当其他软件也在执行密集的WMI操作时，情况尤其如此。有关如何增加这些限制的示例，请参阅Microsoft文档。

Umbrella支持无法针对您的环境建议正确的限制。请与Microsoft联系以获得帮助。

DC负载均衡

Umbrella现在支持负载均衡功能，此功能在站点具有多个域控制器和大量登录事件时非常有用。在这种情况下，将安装其他连接器，然后通过负载均衡组将域控制器分配给连接器。

在简单环境中，负载均衡的工作方式如下：

- 将DC_A和DC_B分配给由Connector_1处理的负载平衡Group_1。
- 将DC_C和DC_D分配给由Connector_2处理的负载平衡Group_2。
- 虚拟设备仍会从两个连接器接收事件，因此仍可感知所有登录事件。
- 如果需要冗余，则可以在每个负载均衡组中安装一个额外的连接器。

此功能具有以下优势：

- 每个连接器的工作量大大减少。每个连接器处理的域控制器数量更少。
- 在从DC接收事件存在高延迟的情况下，这通常会有所帮助。

负载均衡可以向上扩展，以应用于包含许多域控制器的复杂多站点环境。除了安装额外的连接器之外，使用负载均衡没有任何缺点。

此时，必须通过Umbrella支持启用负载均衡功能。请联系Umbrella支持讨论您的要求。

虚拟设备并行通信

连接器现在能够并行将登录事件发送到多个虚拟设备，而不是使用默认的串行方法。 当站点有多个虚拟设备和大量登录事件时，此功能非常有用。

此功能具有以下优势：

- 当有多个设备时，最大程度地减少发送登录信息过程中的任何延迟。 事件可以同时发送到所有设备。
- 防止与某个设备的通信问题或中断对其他设备具有连锁效应。 为每个事件维护一个单独的事件队列。

此功能现在自动启用，但仅在服务器满足CPU和内存建议时才启用。

用户登录事件的加速传输

连接器现在可以批量传输用户登录事件，这显着增加了每秒可发送到虚拟设备的事件数（每秒）。这对于与远程位置的虚拟设备通信的连接器尤为重要。

此功能现在可以自动启用，但具有以下要求：

- 必须启用并行通信（上述）。 服务器必须符合CPU和内存建议。
- 需要ADC版本1.8+
- 需要3.2.0+版连接器

直接事件日志读取器连接

Active Directory连接器版本1.4+支持直接连接到域控制器安全事件日志的新方法，无需使用WMI查询。这使WMI成为“中间人”，并在WMI成为瓶颈的情况下显着提高了性能。这在各个域控制器处理大量登录事件的场景中特别有用。

此功能使用拉取机制工作，连接器每5秒拉取一次新事件，因此识别出的正确用户存在短延迟（例如5秒）。

此优化现在默认启用。 有关此功能的详细信息，请联系Umbrella支持部门。

每秒事件数

可以统计域控制器上最近的事件数来估计每秒钟的事件。Umbrella建议在高峰时间执行此任务：

1.打开Event Viewer应用程序(eventvwr.msc)。

2.转到Windows Logs > System。

3.选择筛选当前日志，然后选择Last hour(上一小时记录的事件)。

4.选择确定。

加载过滤器后，事件日志可以显示上一小时内的事件数。此值可以除以3600来估计每秒事件。

360024901511

360024894112

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）。