

Understand Active Directory Connector Performance

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Overview](#)

[Maximum Events/Second](#)

[New Features](#)

[Performance Recommendations](#)

[Connector Sizing](#)

[Dedicated Connector](#)

[Umbrella Sites](#)

[Network Latency](#)

[Number of Connectors](#)

[Event Log Size](#)

[Third Party Software](#)

[Anti-Virus Software](#)

[Additional Domain Controllers](#)

[Service Account Exceptions](#)

[WMI Patches](#)

[WMI Memory and Handle Limits](#)

[DC Load Balancing](#)

[Virtual ApplianceParallel Communication](#)

[Accelerated Transmission of User Login Events](#)

[Direct Event Log Reader Connection](#)

[Events Per Second](#)

Introduction

This document describes Active Directory connector performance for Umbrella DNS.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Umbrella DNS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

The Umbrella Connector service is used to monitor User/Computer login events as part of Umbrella's Active Directory integration. The OpenDNS Connector service reads login information from the Security Event Log of each AD Domain Controller in its site.

In environments with a high frequency of user login events it is important to review these performance guidelines. For accurate user identification, the Connector service must be able to retrieve login information quickly.

Maximum Events/Second

There is no hard limit on the number of events that can be processed. The Umbrella Connector service is tested to support a continuous **850 events per second** across all Domain Controllers in a "Site". This is based on a dedicated lab environment with no third-party software running. Real world results can differ based on network latency and other bottlenecks.

Customers can determine an approximate number of events/s by reading the "Events Per Second" section later in this article.

New Features

For customers in larger deployments with a high frequency of login events, Umbrella has new performance orientated features. In addition to the general Performance recommendations please read the guidelines later in this article on Load Balancing, Parallel Communication, and the Direct Event Log Reader Connection.

Performance Recommendations

Connector Sizing

The server running the Active Directory Connector service must have CPU and Memory resources as specified in the Umbrella documentation's [Sizing Guide](#).

Dedicated Connector

Although the Connector service can be installed on a Domain Controller directly, Cisco Umbrella recommend that the Connector is installed on a member server dedicated to the Connector service. This member server must have no other third-party software installed. Read more about the [installation process in the Umbrella documentation](#).

Umbrella Sites

Where possible, Umbrella deployments must be segregated into "Sites" that restrict which components communicate across the network. The Connector service can only communicate with components in the same Umbrella site. This feature must always be used when users have a deployment distributed over large

geographical areas.

Typically an Umbrella site is created for each physical location. Umbrella sites must these [rules in the Umbrella documentation](#).

Proper use of Umbrella sites can greatly improve the deployment and prevent components communicating over the Wide Area Network.

Network Latency

Login events can be transferred to the Connector across the network. It is important that there is high-speed connection between the Connector and each Domain Controller to reduce network-related delays. The Connector can be positioned as close possible to the Domain Controller(s) and Virtual Appliance(s).

Number of Connectors

One Connector is required for each Umbrella site. Having multiple Connectors in an Umbrella site is possible, but is only required for redundancy purposes. Having additional Connectors places extra load on the Domain Controllers as they are duplicating the same function as the first Connector. Umbrella recommends a maximum of 2 Connectors for each Umbrella site.

Event Log Size

Large Windows Security Event logs can have an adverse impact on the performance of this WMI operation. Umbrella recommend limiting the event log size. The best performance is found with a log file < 512MB, however, this can be adjusted in line with your log retention requirements. The log file size can be tuned using these instructions:

1. Open the **Event Viewer** application (**eventvwr.msc**).
2. Go to **Windows Logs > System**
3. Right-click on the System log and select **Properties**.
4. Tune the maximum log file size as desired and select **OK**.

Third Party Software

A number of other software products also utilize WMI which can create a bottleneck in WMI on the Domain Controller. This can include:

- Third-Party Security / Analytic software which monitors event logs
- Windows Event Log Forwarding
- SIEM integration and other software which monitors event logs

If any of this software is no longer required we recommend to disable it. Alternatively this issue can be mitigated using the 'Direct Event Log Reader Connection' method described in the Appendix.

Anti-Virus Software

Exclude this folder and these executables from Anti-Virus scanning:

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

Additional Domain Controllers

The WMI notification system on the Domain Controller queues and processes each Event Log entry, and sends them to WMI subscribers. This is effectively a push mechanism where the events are sent by the DC. As such, there can be a performance bottleneck on the Domain Controller itself affecting how quickly events are sent.

This bottleneck can be mitigated by adding additional Domain Controllers to your AD environment. Umbrella has tested a single Domain Controller up to **850 events/s**.

Service Account Exceptions

Reduce the number of AD logins detected by Umbrella by excluding Service accounts. These accounts must be excluded anyway for correct policy application. You can also exclude servers and other devices which are not using AD User policies but can have a high volume of user logons.

WMI Patches

Please ensure the Domain Controller and connector server are up to date with the latest Microsoft patches. Examples of hotfixes which resolve known WMI performance issues are [here](#).

WMI Memory and Handle Limits

WMI contains its own internal limits which can create a bottleneck. This is particularly true when other software is also performing intensive WMI operations. An example of how to increase these limits is found in Microsoft documentation.

Umbrella support is unable to advise the correct limits for your environment. Please contact Microsoft for assistance.

DC Load Balancing

Umbrella now support a load-balancing feature which is useful when a site has multiple domain controllers and a large number of logon events. In this scenario, additional Connectors are installed, and Domain Controllers are then assigned to a Connector via a Load-Balancing group.

In a simple environment, Load Balancing would work like this:

- **DC_A** and **DC_B** are assigned to load-balancing **Group_1** which is handled by **Connector_1**.
- **DC_C** and **DC_D** are assigned to load-balancing **Group_2** which is handled by **Connector_2**.
- **Virtual Appliances** still receive events from both Connectors so are still aware of all logon events.
- If **redundancy** is required an additional Connector can be installed in each Load Balancing Group.

This feature has these benefits:

- The workload of each Connector is greatly reduced. Each Connector is handling a smaller number of Domain Controllers.
- This typically helps in scenarios where there is a high delay **receiving** events from a DC.

Load Balancing can scale up to be used in complex multi-site environments with many Domain Controllers. There is no drawback to using Load Balancing beyond the installation of additional Connectors.

At this time the Load Balancing feature must be enabled by Umbrella support. Please contact Umbrella support to discuss your requirements.

Virtual Appliance Parallel Communication

The Connector is now able to send login events to multiple Virtual Appliances in parallel, rather than using the default serial method. This is useful when a site has multiple virtual appliances and a large number of logon events.

This feature has these benefits:

- Minimizes any delay in sending login information when there are multiple appliances. An event can be sent to all appliances at once.
- Prevents a communication issue or outage with one appliance having a knock-on effect for other appliances. A separate event queue is maintained for each.

This feature is now enabled automatically, but only when the server meets the CPU and memory recommendations .

Accelerated Transmission of User Login Events

The Connector is now able to transmit User Login Events in Batches, which significantly increases the number of events per second which can be sent to the Virtual Appliance (per-second). This is particularly important for connectors communicating with virtual appliances at remote locations.

This feature can now be enabled automatically but has these requirements:

- Parallel Communication (above) must be enabled. The server must meet the CPU and memory recommendations.
- ADC Version 1.8+ Required
- Connector Version 3.2.0+ Required

Direct Event Log Reader Connection

Version 1.4+ of the Active Directory connector supports a new method to connect directly to the Security Event Log of the Domain Controller(s) without using a WMI query. This cuts out WMI as a "middle man" and significantly improves performance in cases where WMI is a bottleneck.. This is particularly useful in scenarios where individual domain controllers are processing a large number of login events.

This feature works using a pull mechanism where the Connector pulls new events every 5 seconds, as such there is a short (for example, 5 second) delay in the correct user being identified.

This optimization is now enabled by default. For more information on this feature please contact Umbrella support.

Events Per Second

It is possible to count the number of recent events on a Domain Controller to estimate the events per second. Umbrella recommends doing this at peak time:

1. Open the **Event Viewer** application (**eventvwr.msc**).
2. Go to **Windows Logs > System**.
3. Select **Filter current log** and select events logged in **Last hour**.
4. Select **OK**.

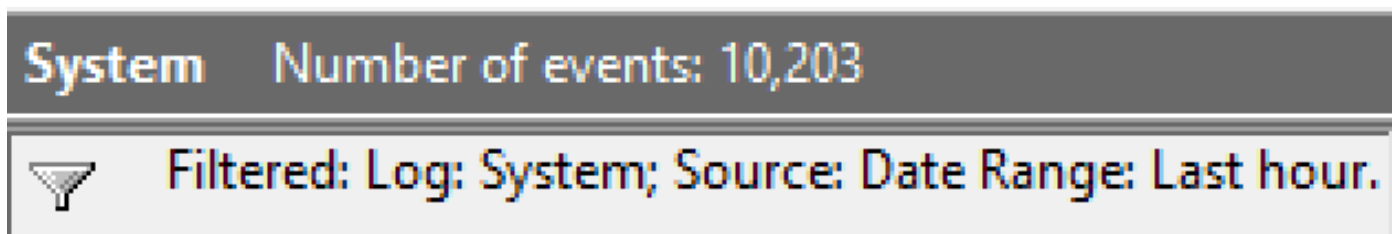
Once the filter has loaded, the **Event log** can show the number of events in the last hour. This value can be divided by 3600 to estimate the events per second.

Filter Current Log



The screenshot shows the 'Filter Current Log' dialog box. It has two tabs: 'Filter' and 'XML'. The 'Filter' tab is active. Below the tabs, there is a 'Logged:' label followed by a dropdown menu. The dropdown menu is currently set to 'Last hour'.

360024901511



The screenshot shows the Windows Event Viewer interface for the 'System' log. The header bar displays 'System' and 'Number of events: 10,203'. Below the header, there is a filter bar with a funnel icon and the text 'Filtered: Log: System; Source: Date Range: Last hour.'

360024894112