Citrix Always On Tracing 2507 LTSR

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Introduction 2

Architecture Overview 2

Centralized AOT Log Server 6

Installing and Configuring Log Server 8

Uploading the AOT logs from CVAD Core Components 13

Best Practices for Using AOT 17

Uninstall Log Server 17

Troubleshooting with AOT and Log Server 18

FAQ 19

General Response Code for Log Server API 20

Known Issues and Limitations 21

Third party notice 21

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Introduction

July 25, 2026

Always On Tracing (AOT) is a modern diagnostic framework from Citrix designed to continuously capture relevant log data across the Citrix Virtual Apps and Desktops (CVAD) environment. Always on Tracing (AOT) is a subset of CDF traces that can be helpful when troubleshooting common failures (for example, VDA registrations and application/desktop launches).
Unlike traditional tools that require manual intervention, AOT runs in the background by default, ensuring that critical information is available when issues occur, even if the problem cannot be reproduced.

AOT is built to simplify troubleshooting for IT administrators and Citrix® support teams to improve the mean-time-to-resolution by:

- Automatically capturing log data for user sessions and system events.
- Eliminating the need to reproduce issues.
- Making logs easily accessible and readable without engineering-level expertise.
- Enabling self-service diagnostics to reduce dependency on Citrix Support.

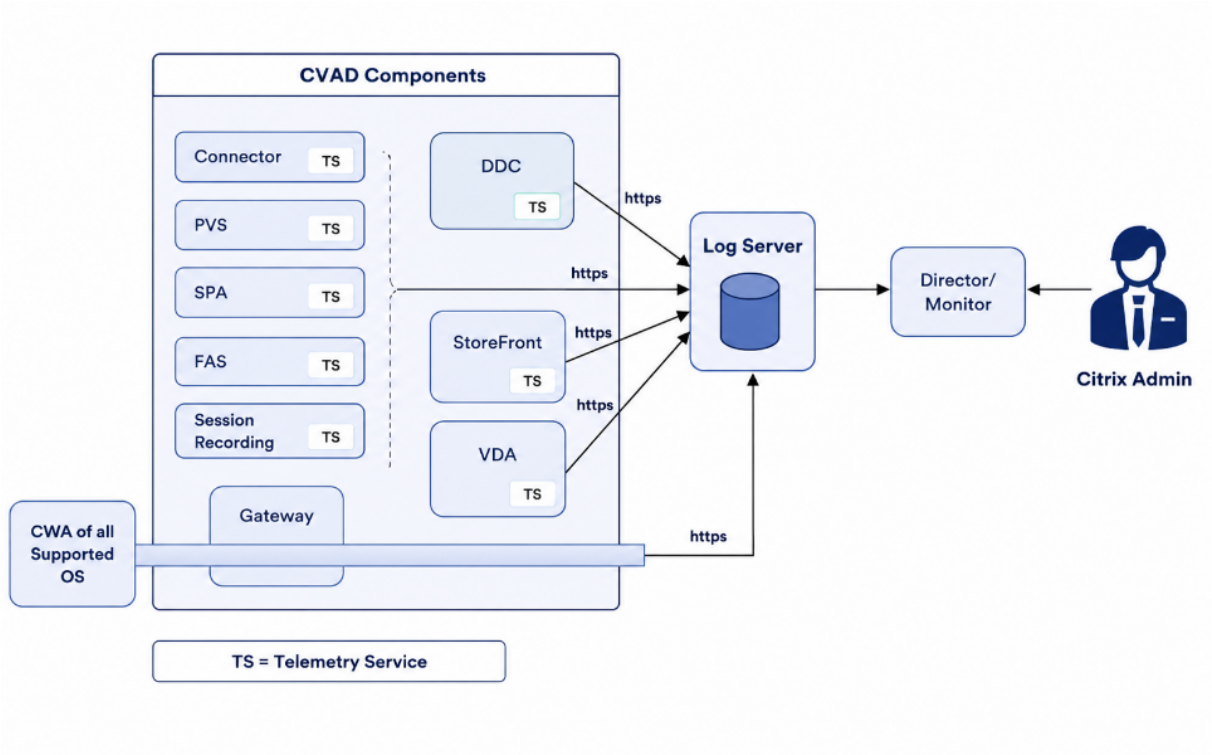
Key Benefits

- Faster MTTR (Mean Time to Resolution)
- Always-on, no manual trace initiation needed
- Self-diagnosis for common issues
- Streamlined escalation to Citrix Support with full context
- Secure, compliant log handling with sensitive data redaction

Architecture Overview

July 25, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The Always On Tracing (AOT) architecture is designed to provide continuous, real-time trace collection across the Citrix Virtual Apps and Desktops™ (CVAD) environment. It enables IT administrators and Citrix Support to troubleshoot user and infrastructure issues without requiring manual trace initiation or issue reproduction.

The AOT system is built on several integrated components working in sequence to capture, transfer, and store telemetry logs from multiple Citrix infrastructure layers into a centralized repository.

Key Components and Workflow

1. **AOT Log Generators (Citrix Core Components):** Citrix components such as the Virtual Delivery Agent (VDA), Delivery Controller™ (DDC), StoreFront, and others act as log generators. These components are equipped with the Telemetry Service, which uses the AOT API to capture trace data, record pre-defined step traces, and log error events relevant to user sessions and transactions.
2. **Enable Log Collection:** When an administrator initiates a request to collect logs (typically through a powershell command), instructions are sent to the broker, which orchestrates the log collection process across the relevant components, including broker and VDA; the administrator initiates the request to collect logs (through a powershell command) from Storefront™ Server separately.
3. **Telemetry Service:** After configuring the Log Server address and port in Storefront and DDC,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the Telemetry Service then activates the new real-time AOT listener, which collects logs based on predefined events, failures, or trigger points.

4. **Log Transfer to Centralized Log Server:** Once the logs are collected, the Telemetry Service transfers them securely to a centralized log server directly. In environments where endpoints are connected from external networks through a Citrix Gateway, the transfer typically occurs over a SOCKS tunnel to ensure secure and seamless transfer.
5. **Log Storage and Organization:** The Centralized Log Server receives, parses, and stores the AOT logs in a structured and searchable format using an indexed database backend (OpenSearch by default). Logs are tagged by session, component, and timestamp, enabling easy access and efficient troubleshooting.

Logs in the Citrix AOT system are stored in a structured and searchable format, tagged with various fields to enable easy access and efficient troubleshooting. These tags include:

- **MachineName:** The name of the machine where the log originated.
- **MachineIP:** The IP address of the machine.
- **Role:** The role of the Citrix component (e.g., VDA, DDC, StoreFront).
- **TimeStamp:** The UTC timestamp when the log event occurred.
- **Message:** The actual log message content. Could be searched/filtered by words.
- **Level:** The severity level of the log (e.g., info, warning, error).
- **Module:** The specific software module that generated the log.
- **ProcessName:** The name of the process that generated the log.
- **ProcessId:** The ID of the process.
- **Thread:** The thread ID within the process.
- **Cpu:** Information related to CPU id at the time of the log.
- **SessionId:** The ID of the user session associated with the log.
- **Class:** The class or component within the module.

These detailed tags allow administrators to quickly filter, search, and analyze logs based on specific criteria, facilitating the identification and resolution of issues.

In summary, the AOT workflow begins with Citrix components generating diagnostic logs. A centralized request is initiated to collect these logs, which the Telemetry Service gathers from the relevant components. The collected logs are then securely transferred to a centralized log server for indexing, storage, and later analysis.

How AOT Works

Citrix Always On Tracing (AOT) continuously captures diagnostic data from key components in your environment. When triggered, logs are collected automatically, securely transferred to a centralized

© 1997–2026 Citrix Systems, Inc. All rights reserved.

log server, and retained for analysis. This eliminates the need for manual tracing and simplifies troubleshooting.

Tracing Triggers and Log Collection: Citrix components such as VDA, DDC, StoreFront and other components are equipped with the AOT API to track critical steps and errors. These components serve as AOT log generators. When an administrator initiates a log collection request from the Delivery Controller:

The DDC sends the instruction to relevant Citrix components. Each component forwards the request to its local Telemetry Service.

The Telemetry Service starts the real-time AOT listening program to collectAOT logs, and forwards the logs to the Centralized Log Server.

Log Storage and Retention: Once the AOT logs are received, the Centralized Log Server formats and indexes them into a structured, searchable database. Logs are retained based on a defined retention policy to optimize storage usage. By default, AOT logs are retained for 7 days, after which they are automatically purged to conserve space.

AOT vs Traditional Logging

Aspect	AOT	Traditional CDF Tracing
Activation	Automatic, continuous	Manual, issue reproduction required
Complexity	User-friendly, readable logs	Engineering-level parsing
Diagnostic Speed	Immediate logs available	Delayed by reproduction effort
Resource Usage	Low overhead with optimized buffers	Moderate to high if used incorrectly

Traditional tracing tools require manual effort and only work if you catch the problem while it's happening. With Always On Tracing (AOT), logging runs continuously in the background, so issues are captured as they happen —even if you're not watching. This saves time and makes troubleshooting much easier.

AOT Highlights

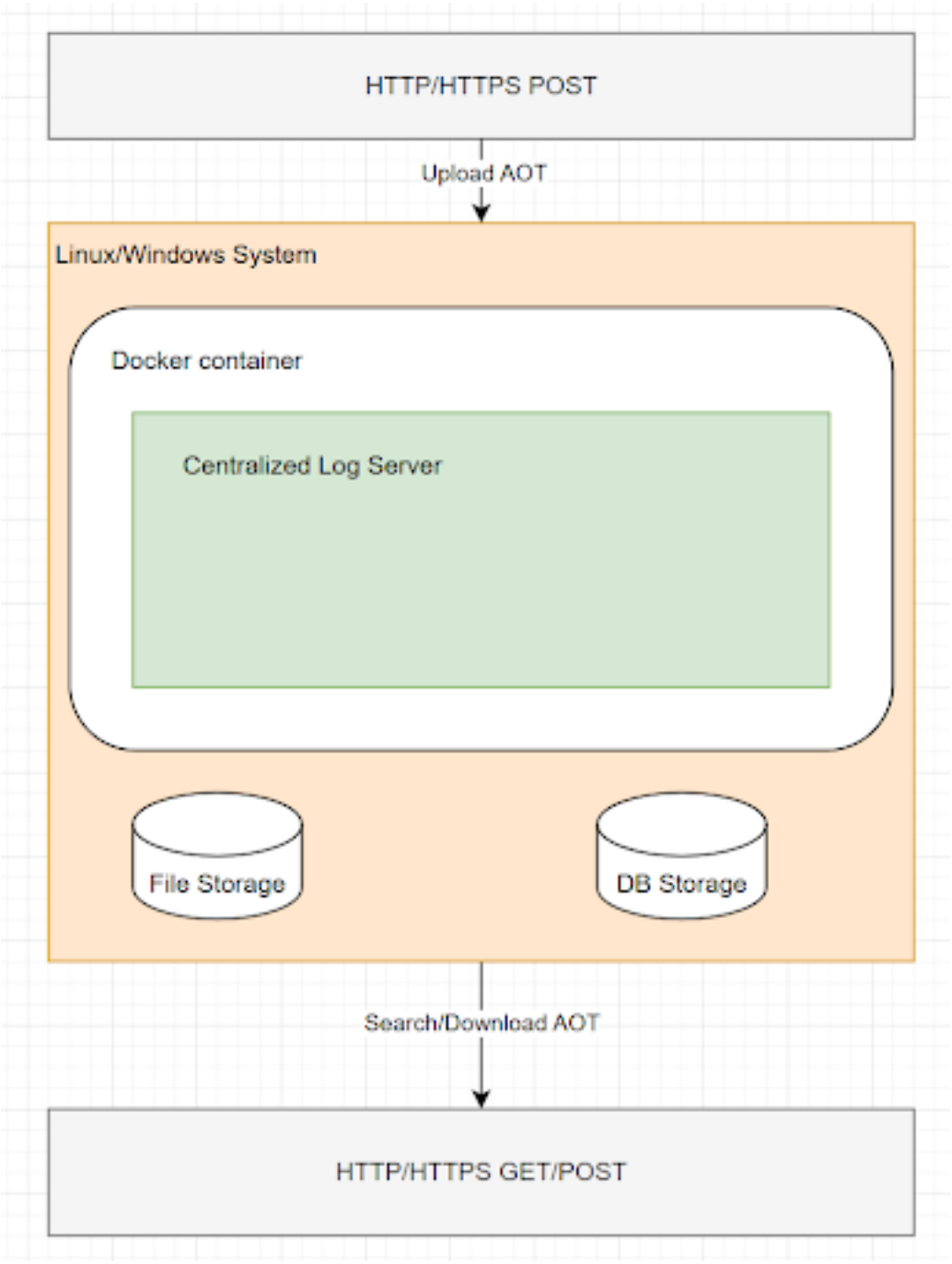
- **Always On:** Tracing runs all the time, no need to turn it on manually.
- **Auto Capture:** Logs are collected always when issues occur.
- **Central Log Server:** All logs are stored in one place for easy access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Easier Troubleshooting:** Helps quickly pinpoint common failures.
- **No Reproduction Needed:** No need to recreate the issue, it's already captured.

Centralized AOT Log Server

July 25, 2026



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The AOT Log Server acts as a centralized destination for collecting and storing Always On Tracing (AOT) logs from various Citrix® components. It is containerized using Docker technology and is preferably deployed on Linux, though it also supports Windows environments via Docker Desktop.

Key Features of the AOT Log Server

- **Centralized Log Storage:** Aggregates diagnostic logs from multiple Citrix components into a unified and searchable location.
- **Retention Policy:** Logs are retained based on a configurable policy (default: 7 days) to optimize storage usage and performance.
- **Deployment:** The Log Server is deployed using packaged installer scripts and Docker containers. The setup requires compatible hardware and a Docker runtime environment.
- **Secure Log Access:** Logs can be retrieved using CLI tools included with the Log Server. All access requires proper authentication to ensure security and compliance.
- **Integration with Citrix Core Components:** The AOT Telemetry Service is embedded within core Citrix components, enabling them to act as log generators. Telemetry Service ensures seamless and automated log capture across these components, enabling consistent diagnostic visibility throughout the Citrix infrastructure.

AOT Log Server Deployment and Configuration

AOT Prerequisites

The AOT Log Server is deployed using Docker container technology. Linux is the preferred operating system, though it can also be installed on Windows using Docker Desktop.

Linux

- **Supported OS:** Ubuntu 24.04, Ubuntu 22.04 and RHEL 8.10, 9.4 with Docker installed.
- **Hardware requirements:** Minimum 4 cores CPU, 16 GB RAM, and 500 GB free disk space.
- **Software Requirements:** Install Docker Engine for Linux or Docker Desktop for Linux.
- **User permissions:** Ensure the user can start Docker without requiring root.

Windows

- **Supported OS:** Windows 11, Windows 10, Windows Server 2022 and Windows Server 2025. For Azure VMs see recommendations here.
- **Hardware requirements:** Minimum 8 cores, 24 GB RAM, and 500 GB free disk space.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Software requirements:** Install Docker Desktop (subscription may be required) for Windows.
  - **WSL version 2.1.5** or later is required.
  - Enable **Hyper-V** and **Containers** Windows features.

Installing and Configuring Log Server

July 25, 2026

1. Download the log server docker container image from Citrix downloads.
2. Place the downloaded files in the same directory.
3. Run the installer in the directory with terminal (Linux) or command prompt (Windows) and follow the instructions:

> **Note:**
>
> - For secure deployment, HTTPS is strongly recommended as it ensures encrypted communication between clients and servers. The use of HTTP is at the customer's discretion.
> - Ensure the selected port is not already in use.
> - Avoid using privileged ports (0–1023) as they require administrator or system-level permissions.
> - Verify that firewall rules allow traffic on the chosen port.
> - Use a port number within the valid range (0–65535), but avoid ports commonly used by system services to prevent conflicts.

Linux Installation

```
chmod +x ./InstallLogServer

# Install with https mode with port 8443 with default path
./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port 8443

# Install with http mode, with port 8080 with default path
./InstallLogServer --port 8080

# Command to change the config path and data path of your choice with https mode
./InstallLogServer --https --cert </path/your_private_cert_key.pfx> --port 8443 --config /Path/LogServer/Config --database /Path/LogServer/Data

# Command to change the config path and data path of your choice with http mode
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
./InstallLogServer --port 8080 --config /Path/LogServer/Config --
    database /Path/LogServer/Data
```

After the installation, some useful script files are generated:

```
# In Linux, sh scripts will be generated

DownloadLogsByTime.sh
DownloadLogsByWords.sh
GetAuthKey.sh
ListMachines.sh
StartLogServer.sh
```

Use ./StartLogServer.sh to start the server.
Check your configpath/weblogs.txt to confirm LogServer started successfully.

If the LogServer starts successfully you will see the below message in the weblogs file. Port 5000 is used by LogServer internally in docker containers with selected http or https protocol.

```
Now listening on: https://[::]:5000
```

If the log server was installed in HTTP mode, successful logs should show the below:

```
Now listening on: http://[::]:5000
```

> **Note:**
>
> - The port configured in the installation step (8080 or 8443 or any port specified) should be used when configuring LogServer url in DDC, Storefront™, VDA, etc.
> - Usually it takes 30s to 60s to start on Linux.

Windows Installation

Step 1: Install Docker Desktop (subscription may be required) for Windows on the log server VM.

Step 2: Run the below commands to continue the installation.

> **Note:**
>
> The default location of Config and Database (Data) folders are created under C:\Users<username>\LogServer.You can change them with the commands below:

```
#Install with https mode with port 8443 with default path
InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443

#Install with http mode, with port 8080 with default path
InstallLogServer.exe --port 8080
#Command to change the config path and data path of your choice with
    https mode
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
InstallLogServer.exe --https --cert <c:\path\cert.pfx> --port 8443 --
    config C:\LogServer\Config --database C:\LogServer\Datacmd

#Install with specific config path and data path
InstallLogServer.exe --port 8080 --config C:\LogServer\Config --
    database C:\LogServer\Datacmd
```

After the installation, a few useful script files are generated in the same directory where you saved the installer files.

> **Note:**
>
> You may move these files to a different location. However, remember the new location, as they will be required again when configuring the Log Server.

```
#In Windows, bat scripts will be generated in the same directory where
    you saved the installer files.

DownloadLogsByTime.bat
DownloadLogsByWords.bat
GetAuthKey.bat
ListMachines.bat
StartLogServer.bat
```

Use `StartLogServer.bat` to start the log server.

Check your **configpath\weblogs.txt** to confirm LogServer started successfully

When the logs show the below, it means to say the Log Server has started successfully.

If the LogServer starts successfully you will see the below message in the weblogs file. Port 5000 is used by LogServer internally in docker containers with selected http or https protocol.

```
Now listening on: https://[::]:5000
```

If the log server was installed in HTTP mode, successful logs should show the below:

```
Now listening on: http://[::]:5000
```

> **Note:**
>
> - The port configured in the installation step (8080 or 8443 or any port specified) should be used when configuring LogServer url in DDC, Storefront, VDA, etc.
> - Usually it takes 1~10 minutes depending upon the hardware in Windows.

Verify the Log Server

Open your browser on Log Server or VDA or DDC, visit http://YourLogServerFQDN:8080/Ping
A response string “Pong UTC:08/19/2025 01:03:29“will show in the browser.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Change port 8080 to your configured port if not using the default port, and change http to https if installed with HTTPS mode:
>
> If the log server verification fail, please check the following logs:
> Run `docker logs logserver` to check docker logs.
> For Linux – `$HOME/LogServer/Config/weblogs.txt`
> (change $HOME/LogServer to your real installed path if not using default one)
>
> For Windows - `C:\Users\YourUserName\LogServer\Config\weblogs.txt`
> (Change YourUserName to real username. Change C:\Users\YourUserName\LogServer to your real installed path if not using default one)

Advanced Configuration of Log Server

Run `docker stop logserver` to stop the logserver

By default, the log server is configured with the below values. To make the changes, edit the `StartLogServer.sh` or `StartLogServer.bat` if installed in windows.

-e MAX_RESERVE_DAYS=7
-e MAX_DISK_USAGE_PERCENTAGE=90
-e LOCAL_DOWN_ONLY=true
-e OPENSEARCH_JAVA_OPTS=”-Xms2G -Xmx2G”

LogServer Configuration Options	Default Value	Value Range	Description
MAX_RESERVE_DAYS	7	1~30	Log Server stores log entries max days based on the TimeStamp field. Logs that were inserted 7 days ago will be deleted. Check every 10 minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LogServer Configuration Options	Default Value	Value Range	Description
MAX_DISK_USAGE_PERCENTAGE	90	10~90	Log Server monitors the data storage percentage. If the usage percentage is more than 90%, Log Server will delete old logs day by day until the usage percentage is less than 90%. Check every 10 minutes.
LOCAL_DOWN_ONLY	true	true/false	If true, only the machine installed Log Server can visit the `/Download/*` APIs. If false, then other machines with AuthKey could visit the `/Download/*` APIs.
OPENSEARCH_JAVA_OPTS	Xms2G -Xmx2G”	2G ~ MaxMem/2	Opensearch memory configurations. Provide more memory if there are a lot of machines that would send logs to Log Server.

Start the log server, using `./StartLogServer.sh` on Linux
Start the log server using `StartLogServer.bat` on Windows.

To check if the changes are considered

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Uploading the AOT logs from CVAD Core Components

July 25, 2026

If you have configured the log server in HTTPS mode `https://<LogServerFQDN>:port`, make sure the necessary certificate is properly installed and trusted on your system.

1. **Uploading AOT logs from Storefront™**

```
#Enable uploading in HTTP

Set-STFDiagnosticsLogServer -Server LogServerFQDN:8080

#Or to use HTTPS

Set-STFDiagnosticsLogServer -Server https://LogServerFQDN:8443

#Disable

Clear-STFDiagnosticsLogServer

#The configuration will take effect in one hour. To apply the
    changes immediately, restart the Citrix Telemetry Service.
```

2. **Uploading AOT logs from DDC:**

```
#Enable uploadng in HTTP
Set-ConfigSite -LogServerEnabled $true -LogServerName
    LogServerFQDN -LogServerPort 8080

#Or enable HTTPS
Set-ConfigSite -LogServerEnabled $true -LogServerName https://
    LogServerFQDN -LogServerPort 8443
#Disable HTTP
Set-ConfigSite -LogServerEnabled $false -LogServerName
    LogServerFQDN -LogServerPort 8080
#Disable HTTPS
Set-ConfigSite -LogServerEnabled $false -LogServerName https://
    LogServerFQDN -LogServerPort 8443
```

3. **Enable AOT on Windows VDA:**

From the machine where you installed DDC, run the below commands and after this you need to restart Citrix Desktop Service to make it take effect immediately.

```
```bash
#Initiate, run following commands in DDC powershell
$configSlot = New-BrokerConfigurationSlot -Name VdaAotTracing -
    Description VdaAotTracing -SettingsGroup G=Telemetry

```

© 1997–2026 Citrix Systems, Inc. All rights reserved.
```

```
#If using HTTPS, parameter of -Endpoint should be "https://logserverFQDN:8443"
$policy = New-BrokerLogServerAddress -Enabled $true -Endpoint "logserverFQDN:8080"
$mc = New-BrokerMachineConfiguration -ConfigurationSlotUid $configSlot.Uid -LeafName VdaAotTracing -Policy $policy


# Using the real DeliverygroupName of your VDA.
$dg = Get-BrokerDesktopGroup -Name "DeliverygroupName"
Add-BrokerMachineConfiguration -InputObject $mc -DesktopGroup $dg


#Restart Citrix Desktop Service in your VDA to make it take effect immediately.
```

Update when the log server address or port changed:

```bash
#Update, run following commands in DDC powershell
#If using HTTPS, parameter of -Endpoint should be "https://NewLogServerFQDN:8443"


$policy = New-BrokerLogServerAddress -Enabled $true -Endpoint "NewLogServerFQDN:8443"
Set-BrokerMachineConfiguration -Name "VdaAotTracing\VdaAotTracing" -Policy $policy
$mc=Get-BrokerMachineConfiguration -Name "VdaAotTracing\VdaAotTracing"

# Using the real DeliverygroupName of your VDA.
$dg = Get-BrokerDesktopGroup -Name "DeliverygroupName"
Add-BrokerMachineConfiguration -InputObject $mc -DesktopGroup $dg
#Restart Citrix Desktop Service in your VDA to make it take effect immediately.
```

How to disable:

```bash
#Disable, run following commands in DDC powershell


#If using HTTPS, parameter of -Endpoint should be "https://LogServerFQDn:8443"
$policy = New-BrokerLogServerAddress -Enabled $false -Endpoint "LogServerFQDN:8080"
Set-BrokerMachineConfiguration -Name "VdaAotTracing\VdaAotTracing" -Policy $policy
$mc=Get-BrokerMachineConfiguration -Name "VdaAotTracing\VdaAotTracing"

# Using the real DeliverygroupName of your VDA.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$dg = Get-BrokerDesktopGroup -Name "DeliverygroupName"
Add-BrokerMachineConfiguration -InputObject $mc -DesktopGroup $dg

#Restart Citrix Desktop Service in your VDA to make it take effect
    immediately.

```
```

1. **Enable AOT on WindowsVDA directly:**

Run the command directly on the machine(WindowsVDA) where you want to upload AOT. This will only take effect on the machine where the command is applied.

```
```bash
# Enable AOT uploading for Windows VDA
#If using HTTPS, parameter of -AotDataStoreEndpoint should be "https://
    LogServerFQDN:8443"

Enable-CitrixAOTUpload -AotDataStoreEndpoint LogServerFQDN:8443 -Role
    WVDA

# Disable AOT uploading
Disable-CitrixAOTUpload
```
```

## Viewing and Using AOT Logs

### Accessing Logs via Log Server

To keep your logs secure, you will need an **AuthKey before** downloading them. Here is what to do:

1. Get your AuthKey –Use your own role-name/name to generate it.
2. Run locally –Scripts can only run on the machine where the Docker container is installed.
3. Windows users –Use the GetAuthKey.bat scripts instead of shell scripts.
4. Download logs –Once authenticated, you can safely retrieve your logs.

```
For Linux
./GetAuthKey.sh role-name
{
 "key":"ebac9b7726cb4be597c92c6769134d25","role":"role-name","
    status":"DONE" }


For Windows
GetAuthKey.bat role-name
{
 "key":"ebac9b7726cb4be597c92c6769134d25","role":"role-name","
    status":"DONE" }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.
```

```
11
12
13  #Save the key: ebac9b7726cb4be597c92c6769134d25 by yourself. It's
       the only way to get the key.
```

List machine names that have already sent their AOT logs to the logserver:

```
1  ```bash
2  #The parameter is the key get from GetAuthKey.sh
3  For linux:
4  ./ListMachines.sh ebac9b7726cb4be597c92c6769134d25
5  {
6   "machines":["MachineName"] }
7
8  #Empty machines means that there has no log
9
10 For Windows:
11 ListMachines.bat ebac9b7726cb4be597c92c6769134d25
12 {
13  "machines":["MachineName"] }
14
15 #Empty machines means that there has no log
16 ```
```

Download logs by Machine name and Time range. Time is in UTC format.

```
1  ```bash
2  #Usage: ./DownloadLogsByTime.sh [AuthKey] [MachineName] [StartTime] [
       EndTime] [OutputFile]
3  #Example:
4
5  For Linux
6  ./DownloadLogsByTime.sh ebac9b7726cb4be597c92c6769134d25 MachineName
       2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
7
8  For Windows
9  DownloadLogsByTime.bat ebac9b7726cb4be597c92c6769134d25 MachineName
       2025-01-01T00:00:00Z 2025-01-02T00:00:00Z logs.csv
10 ```
```

Download logs by keyword/s filter. Time is in UTC format:

> **Note:**
>
> - A keyword can be a single word or a combination of words.
> - Keywords can match anywhere within the log message.
> - A **Transaction ID** can also be used as a keyword.

```
1  ```bash
2  #Usage: ./DownloadLogsByWords.sh [AuthKey] [StartTime] [EndTime] [
       SearchWords] [OutputFile]
3
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
#Example:
For Linux:
./DownloadLogsByWords.sh authkey 2025-01-01T00:00:00.000Z 2025-12-31T23:59:59.999Z "session launch" logs.csv

For Windows:
DownloadLogsByWords.bat authkey 2025-01-01T00:00:00.000Z 2025-12-31T23:59:59.999Z "failed vda" logs.csv
```

Best Practices for Using AOT

July 25, 2026

Time-Based Log Analysis: Download logs based on the estimated timeframe of the issue using /Download/TimeRange. Analyze the logs to identify failures or anomalies tied to that timeframe.

Keyword-Based Log Search: Use /Download/SearchLog with relevant **keywords or transaction ID** to locate specific error messages, events, or patterns. This is effective for known issues or symptoms.

Combine Time and Keyword Search: For complex issues, start with a time-based search and refine results using keywords within the identified timeframe.

Uninstall Log Server

July 25, 2026

1. Uninstall Log Server in Linux

Run the below commands in terminal:

```
docker rm -f logserver
docker rmi logserver

# List containers and images to make sure

docker ps -a
docker images

# Delete Log Server config and data files if not needed any more, change $HOME/LogServer to real installed path if not installed with the default one
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
10
11 rm -r $HOME/LogServer
```

2. Uninstall Log Server in Windows

Run the below commands in powershell:

```
1  docker rm -f logserver
2  docker rmi logserver
3
4  # List containers and images to make sure
5
6  docker ps -a
7  docker images
8
9  # Delete Log Server config and data files if not needed any more,
       change ~/LogServer to real installed path if not installed with the
       default one
10
11 Remove-Item -Recurse -Force ~/LogServer
```

Troubleshooting with AOT and Log Server

July 25, 2026

Top challenges addressed by AOT

1. Availability of AOT logs from a centralized log server for DDC, StoreFront™ and VDA components.
2. Improve log collection time and reduce repetitive log iterations.
3. Increase customer self-troubleshooting capabilities.
4. Accelerate issue resolution time (MTTR)
5. Quick search for logs based on various parameters/keywords.

Ways to download AOT logs

1. When the Timestamp is Known:
    - Use the /Download/TimeRange interface within the powershell script to download logs for the timeframe when the issue occurred.
    - Collect logs from all relevant components (DDC, StoreFront, VDA) involved in the issue.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Review the logs to identify failures or anomalies and take corrective action based on log details.

2. When the Problem Description is known:

   - Use the /Download/SearchLog interface with relevant keywords (error messages, components, events).
   - Identify specific log entries related to the issue.
   - Further refine the search by time or component as necessary.

3. When the logs have to shared with Citrix Tech Support with further troubleshooting

   - If the logs do not clearly indicate the root cause, or if the available information is insufficient to resolve the issue.
   - Package the logs and share them with Citrix Support for further analysis.

FAQ

July 25, 2026

1. **How can I check the running log server configurations, like MAX_RESERVE_DAYS?**
   You can check the container environment values using either of the following commands:

```
docker inspect logserver |findstr MAX_RESERVE_DAYS
```

Or by checking the container environment:

```
docker exec -it logserver env |grep MAX_RESERVE_DAYS
```

If nothing is returned, it means the log server is using the default value:
MAX_RESERVE_DAYS=7

1. **Do I need to purchase Docker Desktop licenses when installing the log server container image on Windows?**

Yes. A valid Docker Desktop license is required.

1. **Should I use a new server for log server installation?**

Yes. It is recommended to use a dedicated server for the log server installation to ensure performance and isolation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

General Response Code for Log Server API

July 25, 2026

This table outlines the standard HTTP response codes used by the Log Server's API to communicate the result of client requests. These codes help clients understand whether their requests were successful or if errors occurred, and what kind of errors were encountered. Understanding these response codes is crucial for diagnosing issues, debugging API calls, and ensuring smooth integration with the Log Server.

Error	Status	Description
200	OK	The request was successful.
400	Bad request.	The server could not process the request due to missing parameters, malformed syntax, or absence of required HTTP headers. For example, if fields like MachineName or Role are missing in the request headers, this response is triggered.
401	Not Authorized.	The request was denied because the client is not authorized. This usually occurs when the IP address or the authentication key (AuthKey) used is not permitted to access the Log Server.
404	Not found.	The API path requested does not exist. This response is returned when the endpoint is invalid or mistyped.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Error	Status	Description
500	Internal error.	Indicates that the Log Server encountered an unexpected condition preventing it from fulfilling the request. This is commonly caused by server-side issues such as resource exhaustion (e.g., memory or disk space).

Known Issues and Limitations

July 25, 2026

In the CVAD 2507 LTSR release, Always On Tracing (AOT) is designed to capture logs from the following three primary components: Delivery Controllers (DDCs), StoreFront™ and Virtual Delivery Agents (VDAs)

This initial scope targets a subset of the most common and recurring issues. The current implementation helps reduce the need for issue reproduction in a few scenarios but not all, specifically for problems related to DDCs, StoreFront, and VDAs.

All remaining components and their corresponding AOT logs will be introduced in future iterations.

Third party notice

July 25, 2026

This release of Citrix AOT Log Server may include third-party software licensed under the terms defined in the following documents:

- Citrix Centralized Log Server Third Party Notices

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.