

EUM Server Requirements

On this page:

- [Hardware Requirements](#)
- [Filesystem Requirements](#)
- [Controller Version](#)
- [Open File Descriptor and User Process Limits](#)
- [Network Settings](#)
- [libaio Requirement](#)
- [Configure User Limits in Linux](#)

This page lists the EUM Server requirements, offers sizing guidance, and shows you how to use configuration to modify the default settings.

Hardware Requirements

The requirements and guidelines for the EUM Server machine (basic usage) are as follows:

- Minimum 50 GB extra disk space. See [Disk Requirements Based on Resource Timing Snapshots](#) to learn when more disk space is needed.
- 64-bit Windows or Linux operating system
- Processing: 4 cores
- 10 Mbps network bandwidth
- Minimum 8 GB memory total (4 GB is defined as max heap in JVM). See [RAM Requirements Based on the Beacon Load](#) to learn when more RAM is required.
- NTP enabled on both the EUM Server host and the Controller machine. The machine clocks need to be able to synchronize.



A machine with these specs can be expected to handle around 10K page requests a minute or 10K simultaneous mobile users. Adding on-premises Analytics capability requires increasing these requirements—particularly disk space—considerably, depending on the use case.

RAM Requirements Based on the Beacon Load

Beacons are sent to the EUM Server every 10 seconds, and each beacon can contain data for multiple events. You can configure the JavaScript Agent to [limit the number of Ajax requests](#).

The table below specifies the required RAM based on your beacon load per minute and lists the content of a typical beacon.

Peak Beacons Per Minute	Typical Beacon Composition	RAM
~3K	<ul style="list-style-type: none">• 600 sessions• 1K base pages• 2K virtual pages• 7K Ajax requests	8 GB
~16K	<ul style="list-style-type: none">• 1.8K sessions• 5K base pages• 10K virtual pages• 40K Ajax requests	16 GB

~26K	<ul style="list-style-type: none"> • 3.6K sessions • 8K base pages • 17K virtual pages • 62 Ajax requests 	16 GB
~33K	<ul style="list-style-type: none"> • 3.9K sessions • 10K base pages • 20K virtual pages • 74K Ajax requests 	32 GB
>40K	12K base pages	32 GB

Disk Requirements Based on Resource Timing Snapshots

By default, the EUM Server accepts a maximum of 1K resource timing snapshots per minute and retains those snapshots for 15 days. On average, each snapshot takes 3 KB of disk space. You can configure the JavaScript Agent to [modify and limit the number of resources to monitor](#) and use the EUM Server configuration `onprem.resourceSnapshotAllowance` to specify the maximum disk space allotted for storing resource snapshots. See [EUM Server Configuration File](#) for a complete list of configurations.

Because of the number of resource timing snapshots impact disk usage, you should follow the guidelines in the table below.

Number of Resource Timing Snapshots	Recommended Disk Space
~500	40 GB
~1000	64 GB
~1500	96 GB
~2000	128 GB

Filesystem Requirements

The filesystem of the machine on which you install EUM should be tuned to handle a large number of small files. In practical terms, this means that either the filesystem should be allocated with a large number of inodes or the filesystem should support dynamic inode allocation.

Controller Version

The AppDynamics Platform you use with the EUM server must have a supported Controller version installed. Controllers only work with the same or later versions of the EUM Server. For example, the 4.2 EUM Server works with the AppDynamics Controller version 4.2 or earlier.

Open File Descriptor and User Process Limits

On Linux, also ensure that open file descriptor and user process limits on the EUM Server machine are set to a sufficient value. For the EUM Server, the hard and soft limits should be as follows:

- Open file descriptor limit (nofile): 65535
- Process limit (nproc): 65535

See [Prepare the Controller Host](#) for information on how to check and set user limits.

Network Settings

The network settings on the operating system need to be tuned for high performance data transfers. Incorrectly tuned network settings can manifest themselves as stability issues on the EUM Server.

The following command listing demonstrates tuning suggestions for Linux operating systems. As shown, AppDynamics recommends a TCP/FIN timeout setting of 10 seconds (the default is typically 60), the TCP connection keepalive time to 1800 seconds (reduced from 7200, typically), and disabling TCP window scale, TCP SACK, and TCP timestamps.

```
echo 5 > /proc/sys/net/ipv4/tcp_fin_timeout
echo 1800 > /proc/sys/net/ipv4/tcp_keepalive_time
echo 0 > /proc/sys/net/ipv4/tcp_window_scaling
echo 0 > /proc/sys/net/ipv4/tcp_sack
echo 0 > /proc/sys/net/ipv4/tcp_timestamps
```

The commands demonstrate how to configure the network settings in the /proc system. To ensure the settings persist across system reboots, be sure to configure the equivalent settings in the etc/sysctl.conf, or the network stack configuration file appropriate for your operating system.

libaio Requirement

The EUM processor requires the libaio library to be on the system. This library facilitates asynchronous I/O operations on the system. Note if you have a NUMA based architecture, then you are required to install the numactl package.

Install libaio on the host machine if it does not already have it installed. The following table provides instructions on how to install libaio for some common flavors of Linux operating system.

Linux Flavor	Command
Red Hat and CentOS	Use <code>yum</code> to install the library, such as: <ul style="list-style-type: none">• <code>yum install libaio</code>• <code>yum install numactl</code>
Fedora	Install the library RPM from the Fedora website : <ul style="list-style-type: none">• <code>yum install libaio</code>• <code>yum install numactl</code>
Ubuntu	Use <code>apt-get</code> , such as: <ul style="list-style-type: none">• <code>sudo apt-get install libaio1</code>• <code>sudo apt-get install numactl</code>
Debian	Use a package manager such as APT to install the library (as described for the Ubuntu instructions above).

Configure User Limits in Linux

AppDynamics recommends the following hard and soft per-user limits in Linux:

- Open file descriptor limit (nofile): 65535
- Process limit (nproc): 8192

The following log warnings may indicate insufficient limits:

- Warning in database log: "Could not increase number of max_open_files to more than xxxx".
- Warning in server log: "Cannot allocate more connections".

To check your existing settings, as the root user, enter the following commands:

```
ulimit -S -n
ulimit -S -u
```

The output indicates the soft limits for the open file descriptor and soft limits for processes, respectively. If the values are lower than recommended, you need to modify them.

Where you configure the settings depends upon your Linux distribution:

- If your system has a `/etc/security/limits.d` directory, add the settings as the content of a new, appropriately named file under the directory.
- If it does not have a `/etc/security/limits.d` directory, add the settings to `/etc/security/limits.conf`.
- If your system does not have a `/etc/security/limits.conf` file, it is possible to put the `ulimit` command in `/etc/profile`. However, check the documentation for your Linux distribution for the recommendations specific for your system.

To configure the limits:

1. Determine whether you have a `/etc/security/limits.d` directory on your system, and take one of the following steps depending on the result:
 - If you *do not* have a `/etc/security/limits.d` directory:
 - a. As the root user, open the `limits.conf` file for editing:

```
/etc/security/limits.conf
```
 - b. Set the open file descriptor limit by adding the following lines, replacing `<login_user>` with the operating system username under which the EUM Server runs:

```
<login_user> hard nofile 65535
<login_user> soft nofile 65535
<login_user> hard nproc 8192
<login_user> soft nproc 8192
```
 - If you *do* have a `/etc/security/limits.d` directory:
 - a. As the root user, create a new file in the `limits.d` directory. Give the file a descriptive name, such as the following:

```
/etc/security/limits.d/appdynamics.conf
```
 - b. In the file, add the configuration setting for the limits, replacing `<login_user>` with the operating system username under which the EUM Server runs:

```
<login_user> hard nofile 65535
<login_user> soft nofile 65535
<login_user> hard nproc 8192
<login_user> soft nproc 8192
```
2. Enable the file descriptor and process limits as follows:
 - a. Open the following file for editing:

```
/etc/pam.d/common-session
```
 - b. Add the line:

```
session required pam_limits.so
```
3. Save your changes to the file.

When you log in again as the user identified by `login_user`, the limits will take effect.