Scheduler for Nuix

Installation Guide

Version 3.0

For eDiscovery professionals ...
by eDiscovery professionals

Table of Contents

Disclaimer

The material in this manual is for informational purposes only. The products it describes are subject to change without prior notice, due to the manufacturer’s continuous development program. Rampiva Inc. makes no representations or warranties with respect to this manual or with respect to the products described herein. Rampiva Inc. shall not be liable for any damages, losses, costs or expenses, direct, indirect or incidental, consequential or special, arising out of, or related to the use of this material or the products described herein.

==

1. Architecture

1.1. Components

Several components are required as part of a Rampiva Scheduler deployment:

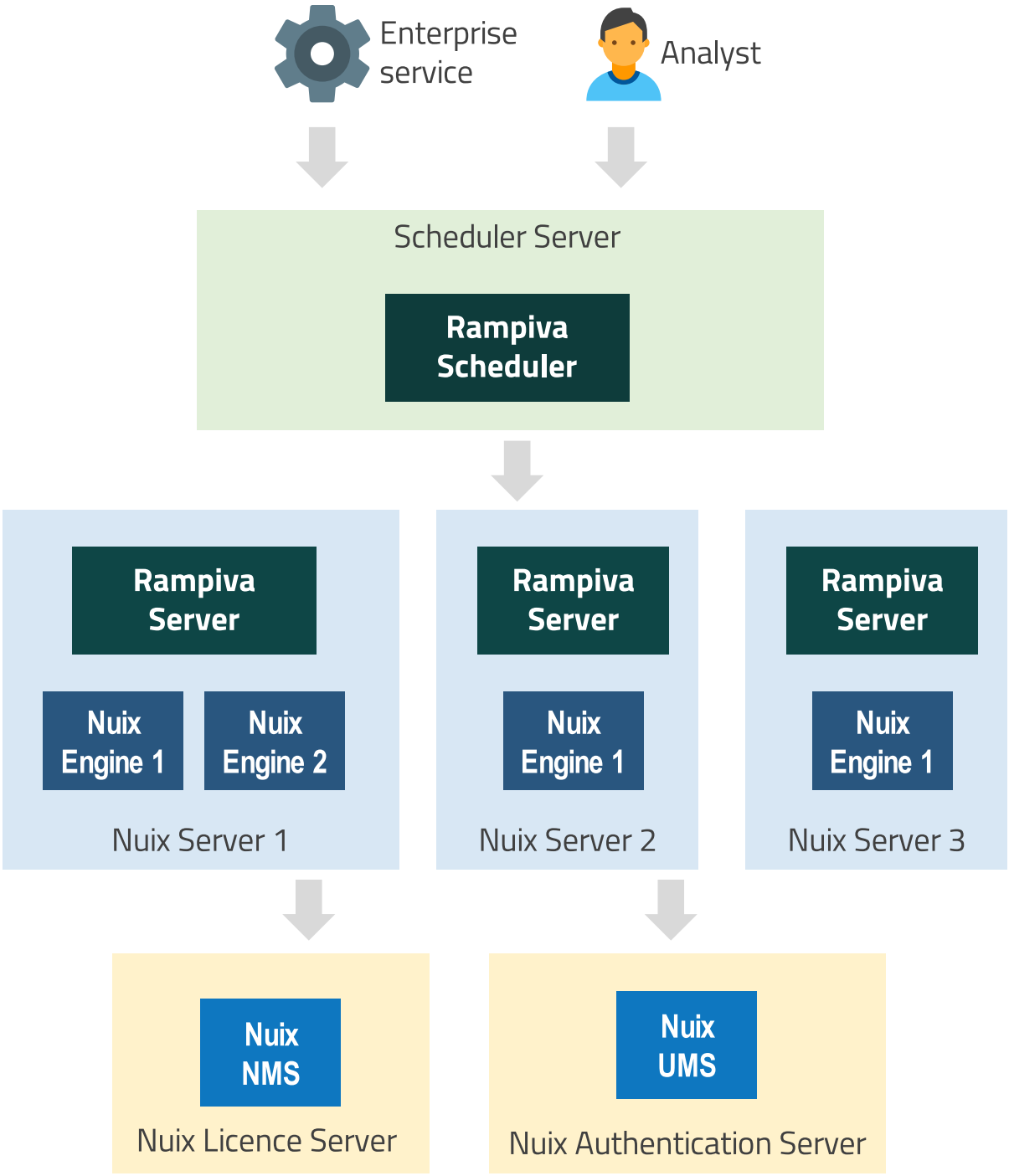
- **Rampiva Scheduler**: Receives requests from the Nuix analysts or from enterprise services for queuing workflows and dispatches the workflows to the Rampiva Servers.
- **Rampiva Server**: Receives workflows from Rampiva Scheduler, starts Nuix Engines and runs workflows.
- **Nuix Engine**: The Nuix Engine creates/opens Nuix cases and performs the required work in the cases.
- **Nuix NMS**: The Nuix licence server, used by the Nuix Engines to acquire licences.
- **Nuix UMS**: The Nuix User Management server, used by Rampiva Scheduler and Rampiva Server to validate user credentials.

1.2. Deployment

With the exception of Rampiva Server which needs to be installed on each Nuix server that will be part of the Ramiva Scheduler deployment, all remaining components can be deployed either on the same server or on dedicated servers.

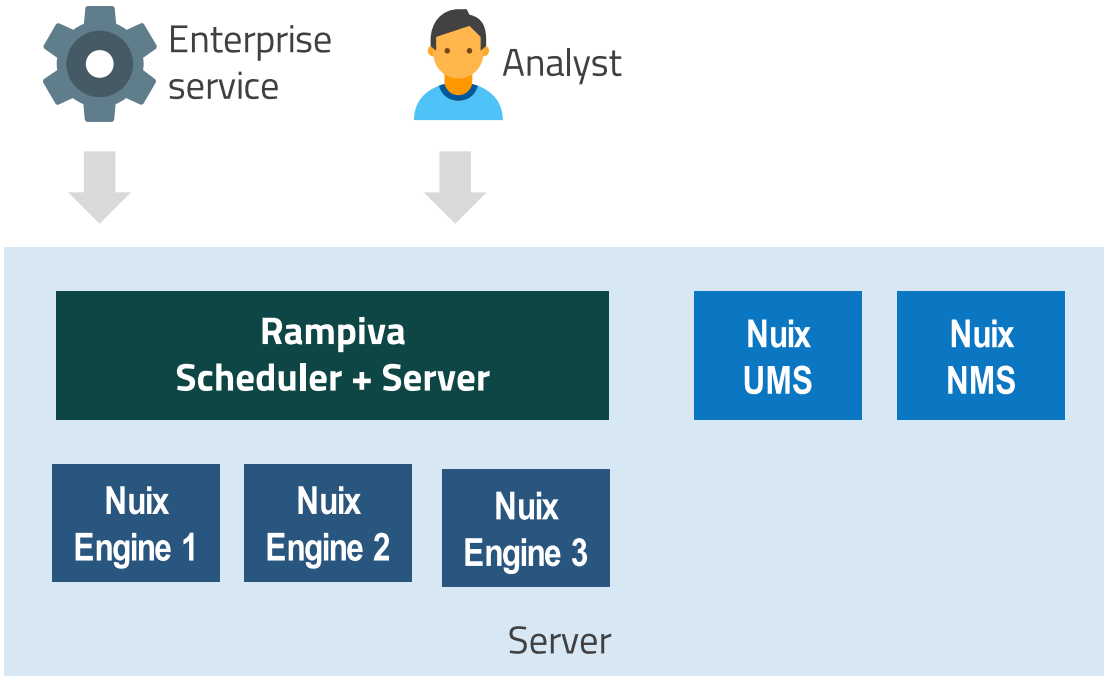
1.2.1. Sample distributed architecture

This sample architecture consists in a dedicated server which hosts Rampiva Scheduler, several servers which host Rampiva Server and Nuix Engines, as well as dedicated servers for the Nuix NMS and Nuix UMS.



1.2.2. Sample standalone architecture

This sample architecutre consists in a single server which hosts the Rampiva Scheduler + Server, several Nuix Engines, as well as the Nuix NMS and Nuix UMS.



1.3. Network Traffic Flow

Components in a Rampiva Scheduler deployment communicate over HTTP. To configure the TCP ports and TLS certificates, please see section Configuration.

Source	Destination	Protocol (Port)
Analyst Web Browser	Rampiva Scheduler	HTTPS (TCP/443)
Rampiva Scheduler	Rampiva Server	HTTPS (TCP/443)
Rampiva Scheduler	Nuix UMS	HTTPS (TCP/443)
Rampiva Server	Nuix UMS	HTTPS (TCP/443)
Nuix Engine	Nuix NMS	HTTPS (TCP/27443)

2. Prerequisites

Each of Rampiva Scheduler and Rampiva Server, require the following components to be installed on the server on which they are deployed:

- **Nuix Engine**, version 7.6.0 or later. Download the latest version of the Nuix Engine from https://download.nuix.com/releases/engine and extract the contents of the engine zip package to C:\Program Files\Nuix\Nuix Engine.
- **Nuix Workstation**, version 7.6.0 or later. Download the latest version of the Nuix Workstation from https://download.nuix.com/releases/desktop.
- **Rampiva Workflow for Nuix**, version 3.0.0 or later, with a valid Rampiva licence. Download the latest version of Rampiva Workflow from https://rampiva.com/products/workflow-for-nuix/download.

Additionally, the following Nuix components must be deployed on any server:

- **Nuix UMS**, version 7.6.3 or later. Download the latest version of the Nuix UMS as part of Nuix Web Review from https://download.nuix.com/releases/web-review and only install the UMS component.
- **Nuix NMS**, or a physical Nuix dongle.

3. Configuration

3.1. Authentication and Privileges

Rampiva Scheduler authenticates users against Nuix UMS. The following privileges can be assigned from the Nuix UMS, from the Web Review section:

- **View Workflows**: Allows user to log in to Rampiva Scheduler and view queued, running and finished workflows, as well as the list of servers and engines.
- **Execute Workflows**: Allows user to submit new workflows to the queue and modify the properties of the workflows submitted by the same user.
- **Manage Workflows**: Allows user to modify the properties of workflows submitted by any user and to configure the servers and engines.

3.2. Service Settings

The Rampiva Scheduler and Rampiva Server configuration file is located at `C:\ProgramData\Rampiva\Scheduler for Nuix\config\config.yml`. This file follows the YAML Syntax and contains the following parameters:

- **runScheduler**: `true` or `false` indicating whether the Rampiva Scheduler component will run on the server;
- **runServer**: `true` or `false` indicating whether the Rampiva Server component will run on the server;

Either one or both of these components can be configured to run on a specific server, but only instance of Rampiva Scheduler should run in the entire deployment.

- **nuixEnginePath**: The location of the Nuix Engine deployment. This folder should contain **bin**, **lib**, and **user-data** subfolders directly.
- **rampivaWorkflowLibPath**: The location of the Rampiva Workflow deployment.
- **nuixFlags**: The flags to start Nuix with, similarly to how they would be submitted in a Nuix batch file.
- **log4jConfigurationFile**: The log4j configuration file.
- **nuixUserManagementServer**: The URL of the Nuix UMS service.

If an HTTPS URL is provided, ensure that the Java Runtime Environment from the latest version of Nuix Workstation deployed on each server trusts the TLS certificate. See section Managing Certificates for more details.

- **server**: Indicates the IP/ports to listen on and the TLS certificate for HTTPS connections.

By default, the service listens on HTTP on port 80, and on HTTPS on port 443, only all IP addresses. To restrict the server to listen on a specific IP address, change `0.0.0.0` to the required IP address in the config.yml file.

- **logging**: Indicates the parameters of the logging performed by the service. These logs will also contain the information that is typically logged by Nuix Workstation. The location of the worker logs is specified in the **nuixFlags** parameter.

3.3. Memory

3.3.1. Nuix Workers

The memory of Nuix Workers can be specified either in the workflow `Configuration` operation, or explicitly as a batchfile parameter in the `config.yml` file of each Rampiva Server instance, for example:

```
nuixFlags: -Dnuix.worker.jvm.arguments="-Xmx8g"
```

3.3.2. Nuix Engine

The memory of the Nuix Engine, equivalent to the memory of the Nuix Workstation is specified as a batchfile parameter, in `C:\Program Files\Rampiva\Scheduler for Nuix\runService.bat`

All Nuix Engines will run under the same JVM and will share the memory allocated to the Rampiva Scheduler deployment on that specific server. Ensure enough memory is allocated to the Rampiva Scheduler JVM to support all instances of the Nuix Engine that will run on that server.

3.4. Shared Data Sources

Rampiva workflows are executed on the servers running the Rampiva Server component. To ensure that workflows cases and source data from a shared location, provide a UNC path or a mapped drive letter path which is accessible from all servers running the Rampiva Server component.

By default, the Rampiva Scheduler service runs under the Local System account. Change this to a domain account with privileges to the shared data sources, as required.

4. Troubleshooting

4.1. Rampiva Scheduler service does not start

Rampiva Scheduler/Controller runs as a Windows service. If the service is not started, inspect the log file at `C:\Temp\Log\rampiva-scheduler.log`.

4.2. Adding Rampiva Server throws `javax.net.ssl.SSLHandshakeException` error

Ensure that the Java Runtime Environment from the latest version of Nuix Workstation deployed on each the Rampiva Scheduler server trusts the TLS certificate of the Rampiva Server. See section Managing Certificates for more details.

4.3. Engine is stuck in INITIALIZING state

When using a NMS licence, the Nuix Engine will prompt the user for confirmation if the TLS certificate is not trusted. Because the Engine runs under the Rampiva Scheduler service which does not have a dekstop user interface, the TLS certificate warning is logged but there is no way for the user to accept the warning. To resolve this, ensure that the Java Runtime Environment from the latest version of Nuix Workstation deployed on each server trusts the TLS certificate of the NMS. See section Managing Certificates for more details.

5. Managing Certificates

5.1. Generate certificate for Rampiva Scheduler/Server

To generate a self-signed certificate for Rampiva Scheduler or Rampiva Server, run the batch file `C:\Program Files\Rampiva\Scheduler for Nuix\ generateCertificate.bat` with administrative privileges.

5.2. Import existing certificate for Rampiva Scheduler/Server

1. Open an administrative command prompt
2. Run `del "C:\ProgramData\Rampiva\Scheduler for Nuix\config\keystore.jks"` to delete the previous certificate store
3. Run `cd "C:\Program Files\Nuix\Nuix 7.6\jre"`
4. Run `bin\keytool -importkeystore -srckeystore C:\temp\myCertificate.pfx -srcstoretype pkcs12 -destkeystore "C:\ProgramData\Rampiva\Scheduler for Nuix\config\keystore.jks" -deststoretype JKS -storepass defaultPassword1234` where `C:\temp\myCertificate.pfx` corresponds to the existing certificate.

5.3. Add the Rampiva Server certificate to trust store

On the server running the Rampiva Scheduler module, perform the following steps:

1. Navigate to `https://SERVERNAME` where `SERVERNAME` is the computer name on which Rampiva Server is installed
2. Save the certificate
   a. In Google Chrome, open the Developer Tag using `F12`
   b. Open the `Security` tab
   c. Select `View certificate`
   d. Open the `Details` tab
   e. Click on `Copy to File…`
   f. Save the certificate in DER encoded binary format
3. Open an administrative command prompt
4. Run `cd "C:\Program Files\Nuix\Nuix 7.6\jre"`
5. Run `bin\keytool -import -alias rampiva-server-name -storepass changeit -keystore lib\security\cacerts -file C:\Temp\serverCertficate.cer` where `C:\Temp\serverCertficate.cer` corresponds to the certificate file saved at the previous step, and `rampiva-server-name` is a unique name for each Rampiva Server.

6. Type `yes`
7. Confirm message `Certificate was added to keystore` is displayed
8. Restart the Rampiva Scheduler service
9. In the Settings page, add the server with the URL `https://SERVERNAME` where `SERVERNAME` is the computer name on which Rampiva Server is installed, as displayed when running the command `echo %COMPUTERNAME%` in a command prompt.

5.4. Add the Nuix NMS certificate to the trust store

On each server running the Ramiva Scheduler or the Rampiva Server module, perform the following steps:

1. Navigate to `https://NMS:27443` where `NMS` is the computer name on which the NMS is installed
2. Save the certificate
    a. In Google Chrome, open the Developer Tag using `F12`
    b. Open the `Security` tab
    c. Select `View certificate`
    d. Open the `Details` tab
    e. Click on `Copy to File…`
    f. Save the certificate in DER encoded binary format
3. Open an administrative command prompt
4. Run `cd "C:\Program Files\Nuix\Nuix 7.6\jre"`
5. Run `bin\keytool -import -alias nuix-nms -storepass changeit -keystore lib\security\cacerts -file C:\Temp\nmsCertficate.cer` where `C:\Temp\nmsCertficate.cer` corresponds to the certificate file saved at the previous step.
6. Type `yes`
7. Confirm message `Certificate was added to keystore` is displayed
8. Restart the Rampiva Scheduler service

6. Filepaths Inventory

- `C:\Program Files\Rampiva\Scheduler for Nuix`: default installation folder
- `%programdata%\Rampiva\Scheduler for Nuix\config`: configuration folder
- `%appdata%\Rampiva\Scheduler for Nuix\Workflows`: persistence and archival of workflow details folder (under the user account running the Rampiva Scheduler service)
- `C:\Temp\logs\rampiva-scheduler.log`: current log file
- `C:\Temp\logs\rampiva-scheduler.%d.log.zip`: previous log files
- `C:\Temp\logs\Rampiva Scheduler.wrapper.log`: service wrapper logs