NVIDIA License System

Release Notes

RN-10194-001 _v3.4.1 | February 2025

Table of Contents

Chapter 1. Release Notes

This document summarizes current status, information on supported platforms, and known issues with NVIDIA® License System release 3.4.1.

1.1. Updates in this Release

New Features in this Release

- Added validity of 3 years to the license file downloaded for the DLS license server.
  - If you are using NLS version 3.3 3.3.x or earlier, the client VMs running vGPU software driver 18.0 or later or NVAIE version 6.0 or later will fail to acquire a license from the license server. NVIDIA strongly recommends that you upgrade to NLS version 3.4.x as soon as possible, to support existing and upcoming vGPU and NVAIE software releases.
- DLS release 3.4.1 displays the License Server file validity on Dashboard.
- DLS release 3.4.1 displays alerts on the Dashboard starting 90 days ahead of end of the License Server File's validity period.
- NVIDIA Licensing Portal displays alerts on the DLS bound License Server Details starting 90 days ahead of License Server File's validity period.
- The ability to add a from-email address in a DLS SMTP configuration.
- The ability to access DLS using your principal name.
- Security updates as listed in Security Updates
- Miscellaneous bug fixes as listed in Resolved Issues

1.2. Supported Platforms

1.2.1. Supported Hypervisors

For deployment in a virtual machine, the Delegated License Server (DLS) component of the NVIDIA License System is supplied as a virtual appliance. The virtual appliance must be installed on a supported hypervisor software release.

The following hypervisor software releases are supported:

- Xenserver 8
- MS Azure Stack HCI support - AHCI 2023
- Citrix Hypervisor 8.2
- Linux Kernel-based Virtual Machine (KVM) hypervisors with one of the following QEMU releases:
  - QEMU 4.2.0
  - QEMU 2.12.0 (`qemu-kvm-2.12.0-64.el8.2.27782638`)
- Microsoft Windows Server with Hyper-V 2019 Datacenter edition
- Red Hat Enterprise Linux Kernel-based Virtual Machine (KVM) 9.2, 9.1, 9.0, and 8.8
- Red Hat Virtualization 4.3
- Ubuntu Hypervisor 22.04
- VMware vSphere Hypervisor (ESXi)) 8.0.3, 8.0.2, 8.0.1, 8.0, 7.0.3, 7.0.2, and 7.0.1

1.2.2. Supported Container Orchestration Platforms

For deployment on a supported container orchestration platform, the Delegated License Server (DLS) component of the NVIDIA License System is supplied as a containerized software image.

The following container orchestration platform releases are supported:

- Docker version 27.4.0 with docker-compose version v2.31.0
- Docker 24.0.2 with Docker Compose 2.18.1
- Kubernetes 1.23.8
- Red Hat OpenShift Container Platform 4.10.67 with Kubernetes 1.23.17
- Podman 4.4.2 with Podman Compose 1.0.7
- VMware Tanzu Application Platform 1.1 with Kubernetes 1.23.6

1.2.3. Supported Operating Systems

For installation on a supported operating system, the Delegated License Server (DLS) component of the NVIDIA License System is supplied as an installable package. The package includes the containerization software and container images that are required to run the NVIDIA Licensing application on the operating system. The operating system can be running in a virtualized server environment on your choice of hypervisor or on a bare-metal server.

Any Red Hat Enterprise Linux 8 or 9 release that is supported by Red Hat is supported.

1.2.4. Licensed Client Support

NVIDIA License System supports specific releases of several NVIDIA software products as licensed clients.

Software Product	Supported Releases
NVIDIA® vGPU™ software graphics drivers	NVIDIA vGPU software starting with release 13.0 **Note:** Support for node-locked licensing was introduced in NVIDIA vGPU software 15.0. It is **not** supported in earlier NVIDIA vGPU software releases.

1.2.5. Web Browser Requirements

NVIDIA License System and NVIDIA Licensing Portal were tested with Google Chrome version 86.0.4240.111 (Official Build) (64-bit).

Chapter 2. Limitations of Containerized DLS Software Images

A container orchestration platform cannot control or restrict access to the OS on which the platform is running. Therefore, containerized DLS software images cannot support the features of VM-based DLS virtual appliances that rely on the ability of the appliance to control the underlying OS.

Containerized DLS software images do not support the following features, for which equivalent functionality is available through standard OS interfaces:

- Log archive settings
- NTP configuration
- Static IP address configuration
- DLS diagnostics user configuration
- Disk expansion

Because a container orchestration platform cannot control the underlying OS, the following limitations also apply to containerized DLS software images:

- Online migration from a VM-based DLS virtual appliance to a containerized DLS software image is **not** supported because the destination containerized DLS software image retains its IP address even after data migration.

  Instead, you must use offline migration when migrating from a VM-based DLS virtual appliance to a containerized DLS software image.
- When the secondary node is removed from an HA cluster, the containerized DLS software image that hosts the node is **not** shut down.

  Instead, you must shut down the DLS software container manually.

Chapter 3. Security Updates

To address vulnerabilities that were discovered through security scans of the DLS, new releases of third-party software components are included in the delegated license service (DLS) component of NVIDIA License System.

Component	Release	Scope	Third-Party Security Information
Docker	27.4.0	DLS 3.4.1.0	Docker Engine Release Notes
PostgreSQL	15.9	DLS 3.4.1.0	PostgreSQL Security Information
Python	3.12.8	DLS 3.4.1.0	Python Security Information
Nginx	1.27.1	DLS 3.4.1.0	Nginx Security Information

Chapter 4. Resolved Issues

Only resolved issues that have been previously noted as known issues or had a noticeable user impact are listed. The summary and description for each resolved issue indicate the effect of the issue on NVIDIA License System **before the issue was resolved**.

Bug ID	Summary
4922619	Vulnerability for below packages in DLS is remediated: 1. Vulnerability for below packages in DLS is remediated 2. libarchive vulnerabilities (USN-7070-1) 3. AppArmor vulnerability (USN-7035-1)
4992156	Events are only triggered for NVIDIA RTX Virtual Workstation-2.0 when set for all leases
5012610	[US Space Force (USSF)] Vulnerabilities found on DLS 3.4.
4894255	Customer not able to access appliance via IPv6
5019817	Errors in log bundle class 'pg8000.exceptions.InterfaceError "network error on write" - fail to renew.

Chapter 5. Known Issues

None.

Appendix A. Updating the Ubuntu GPL/LGPL v3 Licensed OSS Libraries Within the DLS Virtual Appliance

To comply with the terms of the GPL/LGPL v3 license under which the GPL/LGPL v3 licensed Open Source Software (OSS) libraries within the DLS virtual appliance are released, the `rsu_admin` user has the elevated privileges required to update and upgrade these libraries.

> **CAUTION:** Any changes to the Ubuntu GPL/LGPL v3 licensed OSS libraries within the DLS virtual appliance might impair the performance of the DLS virtual appliance or prevent it from functioning as required. If you make any changes to these libraries, the affected DLS instance is no longer eligible for support from NVIDIA. It is **your** responsibility to ensure that the DLS instance continues to perform and function as required.

Ensure that the `sudo` DLS user account `rsu_admin` has been created.

1. Log in as the `rsu_admin` user to the VM that hosts the DLS virtual appliance.
2. Edit the `/etc/apt/sources.list` .
   a). Add this repository list:

```
$ sudo nano /etc/apt/sources.list
```

```
deb http://archive.ubuntu.com/ubuntu/ jammy main universe restricted
 multiverse
deb-src http://archive.ubuntu.com/ubuntu/ jammy main universe restricted
 multiverse
deb http://archive.ubuntu.com/ubuntu/ jammy-updates main universe restricted
 multiverse
deb-src http://archive.ubuntu.com/ubuntu/ jammy-updates main universe
 restricted multiverse
deb http://security.ubuntu.com/ubuntu jammy-security main universe restricted
 multiverse
deb-src http://security.ubuntu.com/ubuntu jammy-security main universe
 restricted multiverse
```

   b). Update the apt list.

```
$ sudo apt update
```

3. Determine whether your existing network configuration allows the DLS virtual appliance to reach the Ubuntu package repositories.

For example, download information from all configured sources about the latest versions of the packages.

```
$ sudo apt update
```

4. If the DLS virtual appliance cannot reach the Ubuntu package repositories, modify your network configuration to allow access to these repositories.
   a). Ensure that your DNS server has the entries required to resolve the domain names of the Ubuntu package repositories.
   b). Delete the symbolic link `/etc/resolv.conf`.

   ```
   $ sudo rm -f /etc/resolv.conf
   ```

   c). Copy the default `resolv.conf` file at `/run/NetworkManager` to `/etc/resolv.conf`.

   ```
   $ sudo cp /run/NetworkManager/no-stub-resolv.conf /etc/resolv.conf
   ```

5. Use the Advanced Packaging Tool (APT) of the Ubuntu OS to check for and install any available updates to the Ubuntu GPL/LGPL v3 licensed OSS libraries.
6. After installing the updates, restore your original network configuration.
   a). Delete the `/etc/resolv.conf` file that you copied earlier.

   ```
   $ sudo rm -f /etc/resolv.conf
   ```

   b). Re-create the symbolic link `/etc/resolv.conf`.

   ```
   $ sudo ln -s /run/NetworkManager/no-stub-resolv.conf /etc/resolv.conf
   ```

7. Once the package upgrade is complete, remove sources.list created in Step 2.

   ```
   $ sudo rm /etc/apt/sources.list
   ```

The file `/var/dls/sudouser` is created to indicate that the Ubuntu GPL/LGPL v3 licensed OSS libraries within the DLS virtual appliance have been updated or upgraded. If the DLS virtual appliance is hosting a node in an HA cluster, this file is automatically copied to the other node in the cluster.

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation ("NVIDIA") makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

VESA DisplayPort

DisplayPort and DisplayPort Compliance Logo, DisplayPort Compliance Logo for Dual-mode Sources, and DisplayPort Compliance Logo for Active Cables are trademarks owned by the Video Electronics Standards Association in the United States and other countries.

HDMI

HDMI, the HDMI logo, and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.

OpenCL

OpenCL is a trademark of Apple Inc. used under license to the Khronos Group Inc.

Trademarks

NVIDIA, the NVIDIA logo, NVIDIA Maxwell, NVIDIA Pascal, NVIDIA Turing, NVIDIA Volta, Quadro, and Tesla are trademarks or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

Copyright

© 2021-2025 NVIDIA Corporation. All rights reserved.

NVIDIA Corporation | 2788 San Tomas Expressway, Santa Clara, CA 95051
http://www.nvidia.com