



# NVIDIA License System

## Release Notes

# Table of Contents

Chapter 1. Release Notes.....	1
1.1. Updates in this Release.....	1
1.2. Supported Platforms.....	1
1.2.1. Supported Hypervisors.....	1
1.2.2. Supported Container Orchestration Platforms.....	2
1.2.3. Supported Operating Systems.....	2
1.2.4. Licensed Client Support.....	3
1.2.5. Web Browser Requirements.....	3
Chapter 2. Limitations of Containerized DLS Software Images.....	4
Chapter 3. Security Updates.....	5
Chapter 4. Resolved Issues.....	6
Chapter 5. Known Issues.....	9
5.1. The DLS appliance has an expired SSL certificate and weak code cipher suites.....	9
5.2. CLS denies license requests from clients named localhost.....	10
5.3. With Windows DNS, internal DLS services cannot be restarted from the DLS management interface.....	11
5.4. NTP configuration changes from the DLS management interface are ignored.....	12
5.5. LDAP user account names for DLS logins are case sensitive.....	13
5.6. Heartbeat-generated failover events are missing from the Events page.....	14
5.7. USN-6420-1: Vim vulnerabilities affect VM-based DLS appliances.....	14
5.8. Self-signed SSL certificates expire on November 14, 2023.....	15
5.9. Heavy traffic on the CLS instance resulting in network communication failures.....	16
5.10. Cannot use Log Archival to mount the network file share.....	16
5.11. Service instances might be unable to reclaim unused licenses on clients with an invalid or empty MAC address.....	17
5.12. Users configured in LDAP Additional Details cannot log in to a DLS virtual appliance VM.....	18
5.13. Multiple VMs fail to acquire license with an invalid origin environment error.....	19
5.14. HA cluster node is not synchronized while its virtual NIC is removed or its network is partitioned.....	19
5.15. Windows clients fail to return leases to the upgraded DLS node.....	20
5.16. VM-based DLS appliance has security vulnerabilities.....	21
5.17. Client fails to acquire offline license when rebooted.....	22
Appendix A. Updating the Ubuntu GPL/LGPL v3 Licensed OSS Libraries Within the DLS Virtual Appliance.....	23

---

# Chapter 1. Release Notes

This document summarizes current status, information on supported platforms, and known issues with NVIDIA® License System release 3.2.0.

## 1.1. Updates in this Release

### New Features in this Release

- ▶ Support for the DLS on the operating system releases listed in [Supported Operating Systems](#)
- ▶ New APIs for retrieving system metrics, listing failovers, and updating the retention period of system metrics on DLS appliances that can be used with API keys.  
For information about the API specifications, see [NVIDIA License System Virtual Appliance APIs](#).
- ▶ Enhanced Heartbeat Service to monitor DLS appliances in a high-availability environment for optimal performance.
- ▶ New email alerts for service availability and system resources, including CPU, memory, and disk space.
- ▶ 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:

- ▶ 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) 8.0.1, 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 20.10.17 with Docker Compose 2.6.0
- ▶ 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	<div>NVIDIA vGPU software starting with release 13.0</div> <div> <b>Note:</b> Support for node-locked licensing was introduced in NVIDIA vGPU software 15.0. It is <b>not</b> supported in earlier NVIDIA vGPU software releases.</div>

## 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
Nginx	1.25.0	All DLS appliances	<a href="#">Nginx security advisories</a>
PostgreSQL	15.4	All DLS appliances	<a href="#">PostgreSQL Security Information</a>
Python	3.11.5	All DLS appliances	<a href="#">Change log for Python 3.11.5 final</a>
RabbitMQ	3.11.10	All DLS appliances	<a href="#">Rabbit MQ Security Advisories</a>
Ubuntu OS	22.04 LTS	VM-based DLS appliances only	<a href="#">Ubuntu Security Notices - Search Results for Ubuntu 20.04</a>

---

# 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
	<p><b>DLS instance displays benign warning message about clients with an invalid or empty MAC address</b></p> <p>When a DLS instance detects one or more clients with an invalid or empty MAC address, the instance displays a warning message in a banner on the web GUI of the instance's NVIDIA Licensing application indicating that some clients are in an unhealthy state.</p>
4361477	<p><b>Second NTP Server to be configured is not listed on the Service Instance Settings page</b></p> <p>If a second NTP server is configured for a DLS instance for which NTP is already configured, it is not listed on the <b>Service Instance Settings</b> page. This issue occurs only if the NTP servers are configured in separate operations in the DLS management interface in quick succession (within 15-20 seconds of each other).</p>
4247340	<p><b>The DLS appliance is vulnerable to click jacking</b></p> <p>A Rapid7 scan of the DLS appliance reveals that the DLS appliance is vulnerable to click jacking, which is also known as a UI redress attack.</p> <div> <b>Note:</b> The resolution of this issue does not address the issue with weak ciphers that the Rapid7 scan also revealed. These weak ciphers remain enabled because SSL certificates are preinstalled on the DLS appliance.</div>
4242954	<p><b>Security vulnerabilities affect the DLS appliance</b></p> <p>ACAS scans on the DLS appliance reveal that the DLS appliance is affected by several security vulnerabilities.</p>
4222881	<p><b>Clients fail to obtain node-locked licenses from license file containing multiple license types</b></p> <p>If a node-locked license file is generated with multiple types of licenses, for example NVIDIA RTX Virtual Workstation licenses and NVIDIA Virtual Application licenses, licensed clients fail to obtain licenses from that file.</p>



Bug ID	Summary
4192413	<p><b>Licensing data is not replicated between the nodes in an HA cluster</b></p> <p>In an HA cluster of DLS instances, licensing data is not replicated between the nodes in the cluster. As a result:</p> <ul style="list-style-type: none"> <li>▶ Checked out licenses fail to be renewed from the secondary node after a failover because they are not replicated on secondary node.</li> <li>▶ The DLS shows that overage allowances are being used even when licenses are available.</li> <li>▶ Licensed clients fail to obtain a license even when licenses are available.</li> </ul>
4174438	<p><b>Security vulnerabilities affect the DLS appliance</b></p> <p>Security scans on the DLS appliance reveal that the DLS appliance is affected by several security vulnerabilities.</p>
4151346	<p><b>Login access to a DLS instance cannot be restricted to specific LDAP users</b></p> <p>After a DLS instance has been integrated with an LDAP server, login access to the web GUI of the instance cannot be restricted to specific user accounts in the LDAP directory on the server. Even if an LDAP search filter is configured, all users in the LDAP directory can log in to the DLS instance.</p>
4101673	<p><b>Name resolution fails during startup if a name is used instead of an address for an NTP or <code>syslog</code> server</b></p> <p>If a DLS virtual appliance is reconfigured to specify an external NTP server or <code>syslog</code> server through the server's fully qualified domain name instead of its IP address, name resolution fails during startup of the DLS virtual appliance or the <code>rsyslog</code> service.</p>
3966221	<p><b>BadRequestError error is displayed on the Events page of a DLS instance</b></p> <p>When a licensed client requests a license from a DLS instance, the following error is displayed on the Events page of the DLS instance:</p> <pre>BadRequestError(origin reference reference already in use by different fingerprint)</pre>
3961380	<p><b>Migration of a DLS instance fails</b></p> <p>Migration of a DLS instance can fail if a large quantity of data is to be migrated. This issue affects both online and offline migration of a DLS instance. When this issue occurs, the NVIDIA Licensing application on the new DLS virtual appliance is affected in one of the following ways:</p> <ul style="list-style-type: none"> <li>▶ The NVIDIA Licensing Dashboard does not show license server details.</li> <li>▶ The <b>ACKNOWLEDGE MIGRATION</b> button is absent from Maintenance page.</li> </ul>
3931610	<p><b>HA cluster creation fails after migration of a DLS instance</b></p> <p>HA cluster creation after migration of a DLS instance can fail if a large quantity of data is to be migrated.</p>

Bug ID	Summary
3917695	<p><b>Events cannot be exported from a DLS instance on a Kubernetes platform</b></p> <p>Events cannot be exported from a DLS instance hosted by a container-based DLS appliance running on Kubernetes, Red Hat OpenShift Container Platform, or VMware Tanzu Application Platform. When a user tries to export events, the attempt fails and the error message Export file generation failed. Please try again. is displayed.</p>
3741535	<p><b>VM hosting a DLS appliance cannot be reached</b></p> <p>After a VM-based DLS appliance has been installed, the VM that is hosting the DLS appliance cannot be reached after it has been started. This issue occurs when a static IP address has been assigned to the VM that is hosting the DLS appliance and the subnet mask of the VM's network was specified in an incorrect format. The subnet mask of the VM's network must be specified in classless inter-domain routing (CIDR) format without the leading slash character (/).</p>
3718863	<p><b>Validation of the client configuration token fails</b></p> <p>When Network Time Protocol (NTP) servers are configured for a VM-based DLS instance, the system times on the DLS instance and the licensed client might still be different. In this situation, validation of the client configuration token fails.</p>

---

## Chapter 5. Known Issues

### 5.1. The DLS appliance has an expired SSL certificate and weak code cipher suites

#### Description

A security scan of the DLS appliance reveals that the DLS appliance has an expired SSL certificate and weak message authentication code cipher suites.

By default, a DLS virtual appliance is configured with a self-signed X.509 SSL server certificate that is included in the DLS virtual appliance image from which the DLS virtual appliance is created. This certificate expired on November 14, 2023.

The DLS appliance supports Transport Layer Security (TLS) version 1.2 but the weak message authentication code cipher suites have not been removed. The TLS/SSL server in the DLS appliance also supports the use of static key ciphers.

#### Workaround

To address the issue of the expired SSL certificate, install a new SSL certificate. You can use a self-signed SSL certificate or a certificate that is signed by a third party, such as a certificate authority (CA), for this purpose.

To address the issue of weak code cipher suites, customize the ciphers that the DLS appliance should use.

Ensure that the sudo DLS user account **rsu\_admin** has been created.

1. Use the hypervisor management console of the appliance to log in as the user **rsu\_admin** to the VM that hosts the DLS virtual appliance.
2. As root, open the file `/var/lib/docker/volumes/configurations/_data/ui/dls-web-ui.conf.template` for editing in the nano plain-text editor.

```
$ sudo nano /var/lib/docker/volumes/configurations/_data/ui/dls-web-ui.conf.template
```

3. In the file `/var/lib/docker/volumes/configurations/_data/ui/dls-web-ui.conf.template`, remove the weak message authentication code cipher suites and add the directive `ssl_ciphers` followed by the ciphers that you want to use.

For example, to use the `TLS_RSA_WITH_AES_128_CCM_8` cipher, add the following directive:

```
ssl_ciphers "TLS_RSA_WITH_AES_128_CCM_8";
```

4. Save your changes to the `/var/lib/docker/volumes/configurations/_data/ui/dls-web-ui.conf.template` file and quit the editor.
5. Restart the DLS appliance.

## Status

Open

## Ref. #

4016523

# 5.2. CLS denies license requests from clients named `localhost`

## Description

Cloud License Server (CLS) instances deny license requests from clients the host name of which is `localhost`. This behavior is the expected behavior for the CLS. For security reasons, the CLS denies requests from clients the host name of which is `localhost`.

## Workaround

- Avoid assigning the host name `localhost` to licensed clients of CLS instances.
- Use Delegated License Service (DLS) instances to serve licenses to clients that have the host name `localhost`.

## Status

Not a bug

## Ref. #

4036980

## 5.3. With Windows DNS, internal DLS services cannot be restarted from the DLS management interface

### Description

If a Windows DNS server is used for name resolution, and the DLS instance is accessed through the fully qualified domain name of its VM, the internal DLS services of the instance cannot be restarted from the management interface of the **NVIDIA Licensing** application of the DLS instance. On the **Service Instance** page, the **RESTART** button remains deactivated even if the status of the services is displayed as inactive.

You can restart these services from the management interface only if you are logged in to the specific instance whose services must be restarted. The DLS determines the instance by matching the fully qualified domain name of the instance with browser's URL origin property.

This issue occurs when the case of the fully qualified domain name in the DNS entry that maps the default host name to the fully qualified domain name is different from the case of the browser's URL origin property. This issue occurs with Windows DNS servers because the fully qualified domain name is in uppercase but the browser's URL origin property is typically in lowercase.

### Workaround

Use any one of the following workarounds for this issue.

- ▶ When logging in to the DLS appliance, specify the IP address of the VM on which the DLS virtual appliance is installed instead of its fully qualified domain name or CNAME.
- ▶ Modify the DNS entry that maps the default host name to the fully qualified domain name to use a lowercase fully qualified domain name.
- ▶ Restart the services from the hypervisor management console of the appliance.

Before using this workaround, ensure that the `sudo` DLS user account **rsu\_admin** has been created.

1. Use the hypervisor management console of the appliance to log in as the user **rsu\_admin** to the VM that hosts the DLS virtual appliance.
2. Restart the critical services.

```
$ sudo docker exec -it config-nls-si-0-1 supervisorctl \
restart auth lease
```

3. Restart the other noncritical services.

- ▶ For a node in an HA cluster, run the following command:

```
$ sudo docker exec -it config-nls-si-0-1 supervisorctl \
restart admin fileInstallation rabbitmq orchestrator:orchestrator_00
```

- For a standalone DLS instance, run the following command:

```
$ sudo docker exec -it config-nls-si-0-1 supervisorctl \
restart admin fileInstallation rabbitmq
```

## Status

Open

## Ref. #

4351000

# 5.4. NTP configuration changes from the DLS management interface are ignored

## Description

When the Network Time Protocol (NTP) configuration of a DLS instance is changed from the management interface of the **NVIDIA Licensing** application of the DLS instance, the changes are not applied to the instance. This issue occurs because both the `systemd-chrond` service and the `systemd-timesyncd` service are active in the DLS instance and the instance uses the `systemd-timesyncd` service for synchronization with an NTP server. However, when NTP is configured from the DLS management interface, only the settings for the `systemd-chrond` service are changed.

## Workaround

Disable the `systemd-timesyncd` service or use standard OS interfaces to configure the `systemd-timesyncd` service.

Before attempting either workaround, ensure that the `sudo` DLS user account **rsu\_admin** has been created.

To disable the `systemd-timesyncd` service:

1. Use the hypervisor management console of the appliance to log in as the user **rsu\_admin** to the VM that hosts the DLS instance.
2. As root, run the `systemctl` command to disable the `systemd-timesyncd` service.

```
$ sudo systemctl disable systemd-timesyncd
```

When the `systemd-timesyncd` service is disabled, the DLS instance uses the `systemd-chrond` service for synchronization with an NTP server.

To use standard OS interfaces to configure `systemd-timesyncd` service:

1. Use the hypervisor management console of the appliance to log in as the user **rsu\_admin** to the VM that hosts the DLS instance.
2. As root, open the file `/etc/systemd/timesyncd.conf` for editing in the nano plain-text editor.

```
$ sudo nano /etc/systemd/timesyncd.conf
```

3. In the `/etc/systemd/timesyncd.conf` file, specify the NTP servers that you want to use.
4. Save your changes to the `/etc/systemd/timesyncd.conf` file and quit the editor.
5. As root, restart the `systemd-timesyncd` service.

```
$ sudo systemctl restart systemd-timesyncd
```

## Status

Open

## Ref. #

4399804

# 5.5. LDAP user account names for DLS logins are case sensitive

## Description

When a lightweight directory access protocol (LDAP) directory is used for managing user access to a DLS appliance, user account names for logging in to the DLS appliance are case sensitive. However, this behavior is inconsistent with the default behavior of an LDAP directory: By default, LDAP distinguished names and attributes are case insensitive.

## Status

Open

## Ref. #

4399814

## 5.6. Heartbeat-generated failover events are missing from the Events page

### Description

Failover events are omitted in error from the **Events** page of the **NVIDIA Licensing** application on the DLS instances in a High Availability (HA) cluster of DLS instances. These events are generated by the Heartbeat service in the cluster and are written to the log files for the DLS appliance as expected.

### Workaround

- ▶ Configure email alerts for failover events from the Heartbeat service.
- ▶ Examine the log files on the DLS appliance for failover events from the Heartbeat service.

### Status

Open

## 5.7. USN-6420-1: Vim vulnerabilities affect VM-based DLS appliances

### Description

Critical security vulnerabilities in the Ubuntu package `xxd_2:8.1.2269-1ubuntu5.17` affect VM-based DLS appliances. This issue does **not** affect the functionality of these DLS appliances. For more information, refer to the Ubuntu security notice [USN-6420-1: Vim vulnerabilities](#).

### Workaround

Install an updated version of the `xxd` package that addresses these vulnerabilities.



**Note:** All other packages that are affected by this issue have been removed from the DLS appliance image.

Ensure that the `sudo` DLS user account **rsu\_admin** has been created.



1. Use the hypervisor management console of the appliance to log in as the user **rsu\_admin** to the VM that hosts the DLS appliance.
2. Add the Ubuntu jammy software repositories to the list of configured APT resources in the main APT sources configuration file `/etc/apt/sources.list`.

```
$ sudo sh -c 'echo "deb http://us.archive.ubuntu.com/ubuntu/ jammy main restricted
deb http://us.archive.ubuntu.com/ubuntu/ jammy-updates main restricted
deb http://us.archive.ubuntu.com/ubuntu/ jammy universe
deb http://us.archive.ubuntu.com/ubuntu/ jammy-updates universe
deb http://us.archive.ubuntu.com/ubuntu/ jammy multiverse
deb http://us.archive.ubuntu.com/ubuntu/ jammy-updates multiverse
deb http://us.archive.ubuntu.com/ubuntu/ jammy-backports main restricted universe
multiverse
deb http://security.ubuntu.com/ubuntu jammy-security main restricted
deb http://security.ubuntu.com/ubuntu jammy-security universe
deb http://security.ubuntu.com/ubuntu jammy-security multiverse" > /etc/apt/sources.list'
```

3. Download information from all configured sources about the latest versions of the packages available from those sources.

```
$ sudo apt update
```

4. Install the `xxd` package.

```
$ sudo apt install -yq xxd
```

## Status

Open

# 5.8. Self-signed SSL certificates expire on November 14, 2023

## Description

The self-signed SSL certificates that are installed on the DLS appliance expire on November 14, 2023. This issue does **not** affect the functionality of the DLS appliance.

## Workaround

**Optional:** Replace the installed certificates with custom certificates.

## Status

Open

## 5.9. Heavy traffic on the CLS instance resulting in network communication failures

### Description

Due to heavy traffic on the CLS instance, the response time for some requests exceed the three-second timeout limit, resulting in network communication failures on the client. This issue happens intermittently for the lease operations because the subsequent service request launched by the retry logic from the client driver will be more likely to succeed.

### Status

Open

### Ref. #

4235254

## 5.10. Cannot use Log Archival to mount the network file share

### Description

In a Unix environment, when you use the Log Archival feature to mount a network file share, the following error message is displayed on the Basics Setting page:

```
Cannot mount the network file share, something went wrong, please check your credentials.
```

This issue occurs in the following situations:

- ▶ If you are using DLS version 3.1 or an earlier version and you configure log archival for the Unix platform on the DLS virtual appliance.
- ▶ If an in-place upgrade is performed from DLS version 3.1 or an earlier version to DLS version 3.2 and you configure Log Archival for the Unix platform on the DLS virtual appliance.

### Workaround

The workaround is for the situation in which you want to perform an in-place upgrade on a Unix platform using Log Archival. Follow these instructions after an in-place upgrade:

1. Log in as the **rsu\_admin** user.
2. Run the `sudo apt-get update` command.
3. Run the `sudo apt-get install -yq nfs-common` command.



**Note:** This workaround is applicable only after the in-place upgrade is complete.

## Status

Open

## Ref. #

4223357

# 5.11. Service instances might be unable to reclaim unused licenses on clients with an invalid or empty MAC address

## Description

When a client with an invalid or empty MAC address requests a license, the service instance grants the request and locates the client through the client's IP address. In an environment where the clients are VM instances with reused MAC addresses, the service instance might have granted licenses to multiple clients with invalid or empty MAC addresses. If a client in such an environment is abruptly shut down and cannot return the license, the service instance cannot locate the VM to reclaim the unused license on it. The license remains checked out until it expires, when the service instance can reclaim it.

## Workaround

Forcibly release licenses acquired by client VMs with invalid or empty MAC addresses that have greater than usual longevity.

## Status

Open

## Ref. #

4163388

## 5.12. Users configured in LDAP Additional Details cannot log in to a DLS virtual appliance VM

### Description

After a DLS instance has been integrated with an LDAP server, users configured in the **Additional Details** section of the LDAP configuration cannot log in to the VM that hosts DLS virtual appliance for the instance. This issue occurs whenever a search filter in the **Additional Details** section contains white space, for example, in the `binddn` value. When the DLS instance writes the search filter to the file `/etc/ldap.conf`, the search filter is split into two lines in `/etc/ldap.conf`. As a result, the LDAP server can no longer parse the file `/etc/ldap.conf`.

### Workaround

1. Use the hypervisor management console of the appliance to log in as the user **dls\_admin** to the VM that hosts the DLS virtual appliance.
2. Open the file `/etc/ldap.conf` for editing in a plain-text editor, such as `vi`.  

```
$ vi /etc/ldap.conf
```
3. Remove all unwanted line breaks from the file `/etc/ldap.conf`.
4. Save your changes and quit the editor.
5. Restart the VM that hosts the DLS virtual appliance.

### Status

Open

### Ref. #

4135514

## 5.13. Multiple VMs fail to acquire license with an invalid origin environment error

### Description

In an environment where the clients are VM instances with reused MAC addresses, an issue with the NVIDIA vGPU software graphics driver might prevent clients with an invalid or empty MAC address from acquiring a license. Whenever this issue causes a VM to fail to acquire a license occurs, the following message is written to the licensing event logs on the client:

```
Tue May 23 03:04:05 2023:<1>:Failed to acquire license from  
api.cls.licensing.nvidia.com  
Info: NVIDIA Virtual PC - Error: invalid origin environment)
```

### Version

This issue affects the following releases of NVIDIA vGPU software:

- ▶ NVIDIA vGPU software 13.0 through 13.8
- ▶ NVIDIA vGPU software 15.0 through 15.3

### Status

Resolved in NVIDIA vGPU software 16.0

### Ref. #

4137753

## 5.14. HA cluster node is not synchronized while its virtual NIC is removed or its network is partitioned

### Description

If a virtual network interface card (NIC) is removed from a node in an HA cluster or its network is partitioned, the node cannot reach other nodes in the cluster. The affected node handles the inability to reach other nodes as a failure of those nodes and assumes the primary role. While the NIC is removed or its network is partitioned, the node cannot

be updated with information about operations that other nodes in the cluster have performed.

### Workaround

After the virtual NIC is attached again or the network is no longer partitioned, the node assumes a role that depends on its uptime. When a node is restarted, it is synchronized with the primary node and assumes the secondary role. Therefore, how to synchronize the nodes in the cluster depends on the role that the node assumes when is able to reach other nodes in the cluster again:

- ▶ **Primary:** All other nodes in the cluster must be restarted.
- ▶ **Secondary:** The node itself must be restarted.

### Status

Closed

### Ref. #

4097705

## 5.15. Windows clients fail to return leases to the upgraded DLS node

### Description

Windows clients cannot return leases to the upgraded DLS node. The failure happens only if the first operation performed by a Windows client is returning leases to an upgraded DLS node. Currently, the DLS upgrade operation does not maintain the auth tokens issued by the existing DLS node. As a result, when the client provides the auth token that was issued before the DLS upgrade, the upgraded node does not acknowledge that token and issues the following error message:

```
Failed to return license to dhcp-10-24-129-182.nvidia.com (Error: invalid token:
Signature verification failed.)
```

After a reboot of the Windows client, the lease that was not returned previously will be assigned to the client. This lease will be returned to the server if the client initiates a lease return after at least one successful lease renewal.

If the virtual machine is shut down, you can manually release the lease by choosing the **Force Release** option using the License Server GUI or wait until the license expires.

### Status

Open

## Ref. #

4092741

## 5.16. VM-based DLS appliance has security vulnerabilities

### Description

The VM-based DLS appliance for each supported hypervisor has security vulnerabilities related to options set for file-system partitions and access permissions for some files.

The vulnerabilities are as follows:

- ▶ The `nodev` option is **not** set on the `/boot/efi` partition.
- ▶ Every time the VM that hosts the DLS appliance is started, Docker creates the following files with the mode `-rwxrwxrwx`, which allows write access by other users (world):
  - ▶ `/home/dls_admin/device`
  - ▶ `/home/dls_admin/dns`
  - ▶ `/home/dls_admin/gateway`
  - ▶ `/home/dls_admin/ip_address`
  - ▶ `/home/dls_admin/static-ip-ova-logs`

### Workaround

You can mitigate these vulnerabilities by setting the `nodev` option on the affected file-system partition and restricting write access to the affected files.

You need to change the affected partition only once. The change persists when the VM that hosts the DLS appliance is restarted.

1. Use the hypervisor management console of the appliance to log in as the user `rsu_admin` to the VM that hosts the DLS appliance.
2. Add the `nodev` mount option to the entry in `/etc/fstab` for the `/boot/efi` partition.
3. Restart the VM that hosts the DLS appliance.

Restrict write access to the affected files that are recreated after every reboot of the VM every time the VM is rebooted.

1. Use the hypervisor management console of the appliance to log in as the user `dls_admin` to the VM that hosts the DLS appliance.

2. Set the mode of the affected files that are recreated after every reboot of the VM to allow access only by owner and root.

- a). Change to the `/home/dls_admin` directory.

```
$ cd /home/dls_admin
```

- b). Change the mode of the affected files in this directory to `-rwxr-xr-x`.

```
$ sudo chmod 755 \
device dns gateway ip_address static-ip-ova-logs
```

## Status

Not a bug

## Ref. #

3923943

# 5.17. Client fails to acquire offline license when rebooted

## Description

When a licensed client that is configured with an offline license is rebooted, the client might fail to acquire a license. When this issue occurs, the following message is written to the licensing event log file on the client:

```
Client fingerprint mismatch - No valid lease found in local trusted store
```

This issue occurs when the MAC addresses of the network adapters for a client change when the client is rebooted. When the MAC addresses change, the NVIDIA vGPU software graphics driver treats the client as a new client and the offline license in the client's trusted storage database is discarded.

Typically, the MAC addresses change because the network configuration of the client has been explicitly changed by an administrator. However, the MAC address of a client can unexpectedly change when the client is rebooted for several reasons, for example:

- ▶ The client requests a license before the client's network interfaces are initialized.
- ▶ Docker or the NVIDIA Container Runtime for Docker is installed on the client and the `ifconfig` command lists it as a network interface.

## Status

Open

## Ref. #

200665895



---

# 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. 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
```
3. 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
```
4. 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.

5. 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
```

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 NON-INFRINGEMENT, 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

© 2021-2024 NVIDIA Corporation. All rights reserved.

