TABLE OF CONTENTS

Chapter 1. NGC Container Registry Overview ............................................................. 1
  1.1. About the NGC Container Registry ..................................................................... 1
  1.2. General Workflow for Using the NGC Container Registry ................................. 1
  1.3. NGC Container Registry Spaces and User Roles .................................................. 2
      1.3.1. NGC Container Registry Account Types....................................................... 2
      1.3.2. NGC Container Registry Spaces .................................................................. 2
      1.3.3. NGC Container Registry User Roles ............................................................ 3
Chapter 2. Setting Up and Activating Your NGC Account ............................................. 4
  2.1. Preparing the NGC Enterprise Account ............................................................... 4
  2.2. Signing Up for an NGC Account .......................................................................... 4
  2.3. Activating Your NGC Account ........................................................................... 5
Chapter 3. Overview of the NGC Website ................................................................... 6
Chapter 4. Generating Your NGC API Key .................................................................. 9
Chapter 5. Using the NGC Container Registry ............................................................. 11
  5.1. Using the NGC Website ..................................................................................... 11
      5.1.1. Browsing the NGC Website ....................................................................... 11
  5.2. Using NGC Container Registry from the Docker Command Line .......................... 14
      5.2.1. Accessing the NGC Container Registry ....................................................... 14
      5.2.2. Uploading an NVIDIA Container Image onto Your System .......................... 15
      5.2.3. Tagging and Pushing a Container Image ..................................................... 16
  5.3. Automated Scanning for NGC Private Registry .................................................... 16
      5.3.1. Using Image Scanning ............................................................................. 17
      5.3.2. NGC Security Scan Failure Remedies ........................................................ 21
Chapter 6. Managing Users and Teams ..................................................................... 23
  6.1. Creating Users .................................................................................................... 23
  6.2. Creating Teams .................................................................................................. 24
  6.3. Adding Users to Teams ..................................................................................... 25
  6.4. Changing User Roles ......................................................................................... 25
Chapter 7. Getting Support for NGC container registry ................................................ 26
Chapter 1.
NGC CONTAINER REGISTRY OVERVIEW

This document describes how to use the NVIDIA® GPU Cloud (NGC) private registry. This guide assumes the user is familiar with Linux and Docker, and has access to an NVIDIA GPU-based computing solution, such as an NVIDIA DGX system, that is configured for internet access and prepared for running NVIDIA GPU-accelerated Docker containers.

1.1. About the NGC Container Registry

Docker containers simplify deployment of data center applications, such as those used for deep learning. Through the NVIDIA® GPU® Cloud (NGC) container registry, NVIDIA provides a collection of "containerized" deep learning applications that have been optimized for use with NVIDIA GPUs.

For more information about NVIDIA containers and frameworks, see the NVIDIA Containers and Deep Learning Frameworks User Guide.

1.2. General Workflow for Using the NGC Container Registry

Using the NGC container registry involves accessing the NGC website and using the Docker command line, as described in this general workflow:

1. Obtain an NGC account.
2. Log on to the NGC website and obtain your API Key so you can access the NGC container registry.
3. Access the NGC container registry from the Docker command line to push, pull, and run the containers.
1.3. NGC Container Registry Spaces and User Roles

1.3.1. NGC Container Registry Account Types

There are two types of NGC accounts available:

- NGC accounts associated with the organization that purchased a DGX system.
  NVIDIA creates accounts for the initial administrators.
  If you are part of that organization, your NGC organization administrator will need to add you to the account. Once you are added, you will receive an invitation email and will be able to activate the account.

- Personal NGC accounts
  You can also sign up for your own NGC account. To set up a personal NGC account, see Getting Started Using NVIDIA GPU Cloud for instructions.

1.3.2. NGC Container Registry Spaces

The following are the registry spaces available to NGC container registry for users:

- **NVIDIA Repositories**
  Example Paths:
  - `nvcr.io/nvidia/`
  - `nvcr.io/hpc`
  - `nvcr.io/nvidia-hpcvis`
  - `nvcr.io/partners`
  These spaces contain images provided by NVIDIA and other developers. All users can pull images from these spaces.
  NVIDIA also provides a CUDA container image within the following public repository that is available to anyone without an NGC account: `nvcr.io/public`

- **Enterprise Organization**
  Path: `nvcr.io/org/`
  This space is created for a DGX customer organization during the initial NGC container registry setup.

- **Team**
  Path: `nvcr.io/org/team`
  This space is created by the organization administrator for use by other users within their organization who have been added to the team.
1.3.3. NGC Container Registry User Roles

The NGC container registry supports three different user roles:

- **Organization Administrator**
  Capabilities:
  - Create teams
  - Add or remove users to or from organizations
  - Add or remove users to or from teams
  - Push, pull, and run Docker images to and from all customer registry spaces
  - Pull and run Docker images from the NVIDIA public registry.

- **Team Administrator**
  Capabilities:
  - Add or remove users to or from teams
  - Pull, push, and run Docker images to and from any organization or team spaces of which the user is a member
  - Pull and run Docker images from the NVIDIA public registry.

- **User**
  Capabilities:
  - Pull, push, and run Docker images from any organization or team spaces of which the user is a member
  - Pull and run Docker images from the NVIDIA public registry
Chapter 2.
SETTING UP AND ACTIVATING YOUR NGC ACCOUNT

2.1. Preparing the NGC Enterprise Account

At least one person from an enterprise must be assigned as the organization administrator for the NGC account. Make sure that the following information for your organization has been provided to NVIDIA Enterprise Support:

- **Organization name**
  This name identifies the organization registry space that is available to all users in your organization.

- **Organization administrator name and email**
  This is the person responsible for adding users and team spaces to the registry.

- **Authentication method for user accounts (IT-managed by SAML, or DGX account)**
  IT-managed by SAML method integrates with your domain login as a single sign-on.
  NGC accounts are independent of your organization’s IT structure.

2.2. Signing Up for an NGC Account

**Signing Up as the Initial Organization Administrator**

Once NVIDIA has received the information described in *Preparing the NGC Enterprise Account*, the NVIDIA NGC team will set up the organization’s space within the NGC container registry, set up the administrator account and authentication method, and
then send a welcome email to the administrator to inform that the NGC container registry is available for use.

**Signing Up as a User within the Organization**

If you are part of the organization, your organization administrator will need to add you to the account. Once you are added, you will receive an invitation email and will be able to activate the account.

### 2.3. Activating Your NGC Account

After NVIDIA or your organization administrator sets up your account, you will receive a welcome email.

1. Click the link in the email to launch the NGC sign-in screen in a browser.

![NGC Sign-in Screen](image)

2. Enter your organization email, then click **Sign In**.
3. Set up a password, depending on the authentication method set up by your organization.
   
   You may need to create a password or you may need to log in using your organization’s single sign-on credentials.

4. Click **Accept** at the NVIDIA GPU Cloud Terms of Use screen.
5. At the **Set Your Organization** screen, select the organization that you want to set for this session, then click **Sign In**.

   This sets the organization or team registry space view for this login to the website.

   You can switch to other organization or team views of which you are a member once you are logged in.
Chapter 3. 
OVERVIEW OF THE NGC WEBSITE 

The NGC website may open to an intro page that helps you get started finding the software of interest.

Explore Our Accelerated Software 

What are you interested in starting?

Industry Select ▼  AI Application Select ▼  Technology Select ▼

[ ] Skip Intro Next Session

Search for software using the options, or click X in the top corner to close the intro page and open the **Accelerated Software** page.
In the upper right corner is an icon representing you, the user, and the current registry space view.

The left side menu lists the functional pages that are available to you:

- **Accelerated Software**: Shows the software provided by NVIDIA.
- **Containers**: Shows the container images provided by your org and team.
- **Models**: Shows the deep learning models provided by your org or team.
- **Teams**: Shows the teams that are available to the user, and lets administrators add or remove users from specific teams. Organization administrators can also add (create) teams.
- **Users**: (Available only to administrators) Shows all active and invited members of the current team or organization view. Organization administrators can also add (invite) users.
- **Setup**: Provides setup functions, such as generating an API key and installing the NGC Registry CLI.

These are explained more fully in the chapters Using the NGC Container Registry and Administrator Instructions.

Click from the top menu options to specify the type of software to view.

Select a category from the top ribbon to see the associated catalog of software.
Click one of the software cards to view information about the software.
This section describes how to obtain an API key to access locked container images from the NGC Registry.

1. Sign in to the NGC website.
   From a browser, go to https://ngc.nvidia.com/signin/email and then enter your email and password.
2. In the top right corner, click your user account icon and select Setup.
3. Click Get API key to open the Setup > API Key page.
   The API Key is the mechanism used to authenticate your access to the NGC container registry.
4. Click Generate API Key to generate your API key.
   A warning message appears to let you know that your old API key will become invalid if you create a new key.
5. Click Confirm to generate the key.
Your API key appears.

You only need to generate an API Key once. NGC does not save your key, so store it in a secure place. (You can copy your API Key to the clipboard by clicking the copy icon to the right of the API key.)

Should you lose your API Key, you can generate a new one from the NGC website. When you generate a new API Key, the old one is invalidated.
Chapter 5.
USING THE NGC CONTAINER REGISTRY

Before using NGC container registry from the Docker command line, you need to log on to the NGC website and obtain your API Key. Your API Key authenticates you to use the registry.

The NGC website also provides useful information, such as:

- The NGC container registry spaces that are available to you
- The Docker repositories in each space
- Guidance on Docker push and pull commands

5.1. Using the NGC Website

This section describes sections of the website that are of interest to users who will be accessing containers from the Docker command line.

5.1.1. Browsing the NGC Website

The NGC website opens to the catalog of GPU-optimized accelerated software.
Click from the top menu options to specify the type of software to view.

You can also select a different category from the top ribbon to see the associated catalog of software.

Click one of the software cards to view information about the software.

The example images below show information for the PyTorch repository.
What Is PyTorch?

PyTorch is a GPU accelerated tensor computational framework with a Python front end. Functionality can be easily extended with common Python libraries such as NumPy, SciPy and Cython. Automatic differentiation is done with a tape-based system at both a functional and neural network layer level. This functionality brings a high level of flexibility and speed as a deep learning framework and provides accelerated NumPy-like functionality.

Running PyTorch

Before running the container, use docker pull to ensure an up-to-date image is installed. Once the pull is complete, you can run the container image.

Procedure

1. Under the Pull Command tab, click the icon to copy the docker pull command.

2. Open a command prompt and paste the pull command. The pulling of the container image begins. Ensure the pull completes successfully before proceeding to the next step.

3. Run the container image. To run the container, choose interactive mode or non-interactive mode.
5.2. Using NGC Container Registry from the Docker Command Line

5.2.1. Accessing the NGC Container Registry

You can access the NGC container registry by running a Docker command from your client computer. You are not limited to using your NVIDIA DGX platform to access the NGC container registry. You can use any Linux computer with Internet access on which Docker is installed.

Before accessing the NGC container registry, ensure that the following prerequisites are met:

- Your NGC account is activated.
- You have an NGC API key for authenticating your access to NGC container registry. For more information, see Generating Your NGC API Key.
- You are logged in to your client computer as an administrator user.

An alternate approach for enabling other users to run containers without giving them sudo privilege, and without having to type sudo before each docker command, is to add each user to the docker group, with the command:

```
sudo usermod -aG docker $USER
```

While this approach is more convenient and commonly used, it is less secure because any user who can send commands to the docker engine can escalate privilege and run root level operations. If you choose to use this method, only add users to the docker group who you would trust with root privileges.

1. Log in to the NGC container registry.

```
sudo docker login nvcr.io
```
2. When prompted for your user name, enter the following text:

```
$oauthtoken
```

The `$oauthtoken` user name is a special user name that indicates that you will authenticate with an API key and not a user name and password.

3. When prompted for your password, enter your NGC API key as shown in the following example.

```
Username: $oauthtoken
Password: my-api-key
```

Tip When you get your API key as explained in Generating Your NGC API Key, copy it to the clipboard so that you can paste the API key into the command shell when you are prompted for your password.

### 5.2.2. Uploading an NVIDIA Container Image onto Your System

No container images are preloaded onto a DGX system. Instead, containers are available for download from the NGC container registry. NVIDIA has provided a number of containers for download from the NGC container registry. If your organization has provided you with access to any custom containers, you can download those as well.

Before loading an NGC container image, ensure that the following prerequisites are met:

- You have read access to the registry space that contains the container image.
- You are logged in to nvcr.io as explained in Accessing the NGC Container Registry.

Tip To browse the available containers in the NGC container registry, use a web browser to log in to your NGC account on the NGC website (http://ngc.nvidia.com/).

1. Run the command to download the container that you want from the registry.

```
sudo docker pull registry/registry-space/repository:tag
```

- `registry`  
  The URL of the container registry, which for the NGC container registry is nvcr.io.
- `registry-space`  
  The name of the space within the registry that contains the container. For example, nvidia is the registry space for containers provided by NVIDIA.
- `repository`  
  Repositories are collections of containers of the same name, but distinguished from each other by their tags. Think of it as the main container name.
- `tag`  
  A tag that identifies the version of the container.

2. To confirm that the container was downloaded, list the Docker images on your system.
The following are several examples of pulling container images.

- Example of pulling `tensorflow:18.06-py3` from the `nvidia` registry space.
  ```
  ~$ sudo docker pull nvcr.io/nvidia/tensorflow:18.06-py3
  ```

- Example of pulling a custom container image tagged `v2.0` from the `acme` organization registry space.
  ```
  ~$ sudo docker pull nvcr.io/acme/custom-image:v2.0
  ```

- Example of pulling a custom container image tagged `v2.0` from the `acme/team` team registry space.
  ```
  ~$ sudo docker pull nvcr.io/acme/zoom/custom-image:v2.0
  ```

### 5.2.3. Tagging and Pushing a Container Image

You can upload custom images to the registry if you have write access to the registry space. Uploading a container image involves first tagging the image and then pushing the image to the registry space.

In the following examples, the user is a member of the Acme organization and the Zoom team within the Acme organization.

- **Tagging Example**
  This example tags a local container image `mycaffe` in the `acme/zoom` team space with "v1.5".
  ```
  ~$ sudo docker tag mycaffe nvcr.io/acme/zoom/mycaffe:v1.5
  ```

- **Pushing Example**
  This example pushes version `v1.5` of the `mycaffe` local container image to the `acme/zoom` team space:
  ```
  ~$ sudo docker push nvcr.io/acme/zoom/mycaffe:v1.5
  ```

### 5.3. Automated Scanning for NGC Private Registry

NGC Private Registry provides enterprises with the ability to push, store, share, and deploy their own custom-built images to their on-premises, cloud, or hybrid environments.

NVIDIA now supports Image Scanning for NGC Private Registries. Image scanning is an automated vulnerability assessment feature in NGC Private Registry that helps improve security early in the build process of developments by scanning a broad range of system vulnerabilities. The scan automatically checks against an aggregated set of Common Vulnerabilities and Exposures (CVE's), crypto keys, private keys, meta-data scans, and exposes the results in the NGC UI.
With Image Scanning:

- Security teams can audit and verify compliance in real time.
- Users can perform detailed analysis of container images, producing reports with defined policies for images to be used in production environments.

5.3.1. Using Image Scanning

Scanning is a microservice provided to NGC users. Once the image is pushed to a private registry, the image joins the NGC scan queue requests. The scan may take several minutes (typically 5 mins - 30 mins) based on the scan queue or the size of the image.

Activate Automated Scanning

NVIDIA enables the automated scanning feature upon the request of an Enterprise who owns a Private Registry. The activation of scanning can take place both at an organization and at team level. The organization may choose to integrate their own scanning tools manually or can leverage this feature as provided by NVIDIA.

Scanning Tool Integration

When a new container image is pushed, it triggers the Anchore engine scan based on the permission setting allocated to that NGC Private Registry. If email notification is activated, scan status notifications are triggered. If scan permissions are activated in your Private Registry settings, users can review the scan findings for information about the security of the container images that are being pushed.

Email Notifications

Once the scan is complete, the user who pushes the image receives an email notification stating the result of the status of scans.

The following is an example email notification for an image that has passed the scan policy:
The following is an example email notification for an image that has failed the scan policy:

Dear Monika,
nvidia/ngc-product-team/test_nginx:latest has been **scanned** at 2020/03/10 22:48 PM

**Scan Summary**

**Scan Action:** PASS

Reason:
No critical or high severity issues found

Review Details within NVIDIA GPU Cloud

Copyright © 2020 NVIDIA Corporation. All rights reserved.
NVIDIA Corporation, 2701 San Tomas Expressway, Santa Clara, CA 95050.
Review Scan Results

Having received the email notification, the user can now log in to the private registry with NGC credentials. The following screenshot shows the UI tab “Security Report” (highlighted in red) on the container page:
On the left, users can navigate through tags to view different security reports. The example shows the scan result of tag 0.5. (highlighted in green)

The UI indicates all details on the scan results which are bucketed as critical, high, medium and low severities. As previously stated and in accordance with best practices, the user must ensure the image does not have any high or critical severities before deployment.

Since the CVE’s database is updated each hour and scan results can vary over time, the “Rescan Image” (highlighted in black) shows the latest scan results before deployment. Also, this could be leveraged for images in production as over time the packages in the images can become outdated and they tend to collect vulnerabilities which could be a security threat in the future. The scan timestamp is also made available.

Finally, the “NGC Security Scan Failure Remedies” is a recommendation guide for NGC users to tackle frequently occurring security threats.
5.3.2. NGC Security Scan Failure Remedies

NGC Container Registry performs automated security scans on containers pushed to the NGC registry. The scanning tool checks against the content of a dockerfile if provided, or a derived dockerfile based on the docker layer history if the dockerfile is not provided.

The Security Scan tab is displayed on the description page for the specific container and shows the results of the scan. The following are some remedies for select security scan failures:

**CVE Failures**

These failures typically occur for one of two reasons:

- Your container image is built from an older base image which has now been found to have security vulnerabilities.
  
  New CVEs are reported every month, so a base image even a few months old is likely no longer secure.

- Your container is built from a recent base image, but a new CVE has been found since its release.
  
  The NGC scanning tool picks up known CVE updates daily, so an image that passed yesterday may fail today.

In both cases the remedy is usually the same; look for the most recent tag for your base image (**FROM** line in your dockerfile) and rebuild your container.

The following is an example of a base image CVE and the remedy.

**Issue**


**Fix**

Rebuild the image and include the latest package which fixes the identified code flaw.

For example:

- Use the latest base image which includes the latest package:

  ```
  FROM ubuntu:19.04
  ```

  or

- Include the specific run command to update the old package:

  ```
  apt update && apt install --only-upgrade linux-libc-dev
  ```

CVE failures can also be triggered by other packages/binaries that you install in your container after the base image. The CVE Failure message should have identified the
package or binary that triggered it. Look for a more recent version of that package or binary, update your dockerfile and rebuild your docker image.

**Denied/Exposed Port Failures**

NGC has a list of ports which should not be opened in an NGC Container Image.

An example of a denied port is port 80, the default port for HTTP. HTTP connections (as opposed to HTTPS) are not encrypted and are insecure. Modern browsers will warn against an open HTTP connection and is a bad user experience. Port 443 and HTTPS should be used instead - no warnings will appear and the connection is secure.

The following is the list of denied ports:

- 20 - FTP (there are more secure ways to file transfer)
- 23 - Telnet (recommend using a more secure service than telnet)
- 25 - SMTP (email service isn’t a common service to be exposed for NGC containers)
- 80 - HTTP (recommend using https on port 433 instead)
- 115 - FTP (there are more secure ways to file transfer)

For all denied ports, the remedy is to use a secure alternative that provides the same functionality whose default port is not on the list of denied ports.

**Private Key Failures**

The NGC Security Scan identifies any private key crypto files in the image, and fails the scan if it finds them. Private keys are dangerous to leave in a published container image, as they may be used by others to authenticate on private or public services and gain access as an imposter.

The remedy is to remove the private keys and resubmit the container image.

There are cases where a container image includes private test keys to allow users to run tests on the container. These are generally harmless and can be whitelisted if the publisher requests.
Chapter 6.
MANAGING USERS AND TEAMS

This chapter applies to organization and team administrators, and explains the tasks that an organization or team administrator can perform from the NGC website.

As the NGC administrator for your organization, you can invite other users to join your organization’s NGC account. Users can then be assigned as members of teams within your organization. Teams are useful for keeping custom work private within the organization.

The general workflow for building teams of users is as follows:

1. The organization admin invites users to the organization’s NGC account.
2. The organization admin creates teams within the organization.
3. The organization admin adds users to appropriate teams, and typically assigns at least one user to be the team admin.
4. The organization or team admin can then add other users to the team.

6.1. Creating Users

As the organization administrator, you must create user accounts to allow others to use the NGC container registry within the organization.

2. Click Users from the left side menu, then click the ‘+’ icon at the bottom of the screen and then click the ‘invite new user’ icon.
It doesn’t matter which organization or team view is enabled; the new user is added only to the organization if they are assigned the *User* role. After adding the user, you can add them to individual teams as needed. If you assign the new user the *Admin* role, the user is added to all teams within the organization.

3. Fill out the **Invite New User** form for the new user as follows:
   a) Enter the display name and email where indicated.
   b) Click the **Role Type** list arrow and then select one of the user types.

   If you select *Admin*, the user will be added to all teams within the organization.

4. Click **Add User** when done.

   An invitation email is automatically sent to the user.

### 6.2. Creating Teams

Creating teams is useful for allowing users to share images within a team while keeping them invisible to other teams in the same organization. Only organization administrators can create teams.

To create a team,

1. Log on to the [https://ngc.nvidia.com](https://ngc.nvidia.com).
2. Select *Teams* from the left side menu, then click the ‘+’ icon at the bottom of the screen and then click the ‘create teams’ icon.

3. Enter a team name and description, then click **Add Team**.
6.3. Adding Users to Teams

Organization administrators can add users to any team in the organization. Team administrators can add users to their teams.

2. Click Teams from the left side menu, then select the team that you want to add a user.
3. In the Active Members section, click Add User.
4. In the Add User dialog, select one of the available users, select a role, then click Add User.

Users can be members of more than one team. To add a user to another team, repeat these steps for any additional teams.

6.4. Changing User Roles

You can change user roles for any users you created.

2. Select the registry space (org and team) for which you want to change the user role.
   Click your user icon to select from the list of orgs, and then click Select a Team and choose the appropriate team.
3. Click Users from the left side menu.
   A list of all the users in the current registry space appears.
4. Select the user whose role you want to change.
   The User Information form appears.
5. Click Edit User.
6. Click the Role Type list arrow and then select the new user type.
7. Click Save when done.
Chapter 7.
GETTING SUPPORT FOR NGC CONTAINER REGISTRY

For additional information on using the NGC container registry and for getting help if you encounter issues, send an email to enterprisesupport@nvidia.com with a description of your issue and a ticket will be created for you.
Notice

THE INFORMATION IN THIS GUIDE AND ALL OTHER INFORMATION CONTAINED IN NVIDIA DOCUMENTATION REFERENCED IN THIS GUIDE IS PROVIDED “AS IS.” NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE INFORMATION FOR THE PRODUCT, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA’s aggregate and cumulative liability towards customer for the product described in this guide shall be limited in accordance with the NVIDIA terms and conditions of sale for the product.

THE NVIDIA PRODUCT DESCRIBED IN THIS GUIDE IS NOT FAULT TOLERANT AND IS NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE IN CONNECTION WITH THE DESIGN, CONSTRUCTION, MAINTENANCE, AND/OR OPERATION OF ANY SYSTEM WHERE THE USE OR A FAILURE OF SUCH SYSTEM COULD RESULT IN A SITUATION THAT THREATENS THE SAFETY OF HUMAN LIFE OR SEVERE PHYSICAL HARM OR PROPERTY DAMAGE (INCLUDING, FOR EXAMPLE, USE IN CONNECTION WITH ANY NUCLEAR, AVIONICS, LIFE SUPPORT OR OTHER LIFE CRITICAL APPLICATION). NVIDIA EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH HIGH RISK USES. NVIDIA SHALL NOT BE LIABLE TO CUSTOMER OR ANY THIRD PARTY, IN WHOLE OR IN PART, FOR ANY CLAIMS OR DAMAGES ARISING FROM SUCH HIGH RISK USES.

NVIDIA makes no representation or warranty that the product described in this guide will be suitable for any specified use without further testing or modification. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to ensure the product is suitable and fit for the application planned by customer and to do 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 guide. NVIDIA does not accept any 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 guide, or (ii) customer product designs.

Other than the right for customer to use the information in this guide with the product, no other license, either expressed or implied, is hereby granted by NVIDIA under this guide. Reproduction of information in this guide is permissible only if reproduction is approved by NVIDIA in writing, is reproduced without alteration, and is accompanied by all associated conditions, limitations, and notices.

www.nvidia.com
Trademarks

NVIDIA, the NVIDIA logo, and Volta are trademarks and/or registered trademarks of NVIDIA Corporation in the United States and other countries.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries.

Other company and product names may be trademarks of the respective companies with which they are associated.

Copyright

© 2020 NVIDIA Corporation. All rights reserved.