NVIDIA CloudXR AMI Introductory Offer
Quick Start Guide

This guide walks through getting started using the NVIDIA CloudXR AMI Introductory Offer - WinServer 2019 offering available from the AWS Marketplace.

What's included

Using the NVIDIA CloudXR AMI Introductory Offer - WinServer 2019 eases installation and delivery of NVIDIA CloudXR to developers. Deploying the Marketplace offering provides the following software and AWS instance configurations:

- CloudXR Server installer and documentation
- NICE DCV remote desktop access for developers and non-VR users
- NICE DCV virtual audio driver--used by CloudXR
- AWS Security Group settings for the EC2 instance.

What's excluded

The post-deployment applications and configurations that are required but **not** included are:

- Steam & SteamVR
- AWS IAM configuration
- CloudXR clients

**Steam and SteamVR**

CloudXR uses StreamVR's OpenVR SDK as an interface between head-mounted displays and VR software by installing a plugin to SteamVR. It is not distributed with the image and must be downloaded directly from Valve and installed manually after the EC2 instance launches.

**AWS IAM**

IAM roles are not created or assigned during the marketplace launch process. After the marketplace instance is deployed, you must assign an IAM role with an S3 read-only policy to the EC2 instance to validate the NICE DCV license.

**CloudXR test/sample clients**


AWS Configuration Prerequisites

Before getting started, you must have an AWS Account that meets the following prerequisites:

- Deployment rights for G4 EC2 instances
- Creation rights for EC2 Security Groups and ability to attach them to EC2 instances
- Operational rights within a designated or default AWS Virtual Private Cloud (VPC)
An EC2 IAM role with a S3 read-only policy for NICE DCV licensing or ability to create such a role and policy.

You also should be comfortable operating within the AWS Management Console. The instructions describe methods for using the prepared AWS Marketplace, but direct access to the Amazon Machine Instance is also available for advanced configurations.

**Marketplace Deployment Steps**

The steps described below are for launching an EC2 instance within the AWS Marketplace. Advanced customizations such as VPC networking specifics, more robust security-group settings, and public/private subnetting placement are beyond the scope of this document.

1. Navigate to [AWS Marketplace](https://aws.amazon.com/marketplace/) and search for CloudXR to find the latest listing. Review the details and make a note of the instance size, AWS Pricing, usage, and other details. Select **Continue to Subscribe**.
2. **Accept** the Terms and Conditions to activate the subscription (this may take a few minutes). When finished, an effective date will be displayed. Select **Continue to Configuration**.

3. Select the region closest to your client user. If you’re not sure which region that is, AWS provides a **Connection Health Check** tool to check. When satisfied, select **Continue to Launch**.

4. If you're not familiar with the AWS EC2 management console, make sure **Choose Action** is set to **Launch from Website** (this is the recommended method of getting started quickly). Select the proper **EC2 Instance Type** for your application, **VPC Settings**, and **Subnet Settings**.
5. Within **Security Group Settings**, select **Create New Based on Seller Settings** which populates the required Security Group ports.

![Security Group Settings](image)

6. Within **Key Pair Settings**, select your AWS EC2 Key Pair to assign it to this instance or create a new one. **If you proceed without a key pair, you will not be able to log in to the instance.**

7. Verify the above settings and select **Launch**.

Note: AWS instances are billed based on usage. Consider configuring AWS CloudWatch alarms and/or rules to prevent charges when not in use.

### Connecting to GPU-Accelerated CloudXR Workstation

You must attach an IAM role with read-only rights to S3 on your launched instance for proper NICE DCV licensing. Not doing so significantly increases initialization times, causes DCV licensing errors, and may prevent DCV client access to your launched instance.

1. Navigate to the **EC2 Console** within the selected AWS Region region your instance. Locate the launched CloudXR instance within the **Instances** panel.

2. Select your instance and add the IAM role by selecting **Actions > Security > Modify IAM Role**. A menu will appear; select the proper IAM role and select **Save**. If you do not have a service-specific role, you will need to create one following these instructions: [https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-service.html)
3. Select the **Connect** button. This brings up a panel; select **RDP Client** (Note: Even though you’ll be using NICE DCV to connect, the password retrieved is the same). Select **Get password** and another menu will open.

4. **Browse** and select the PEM key pair identified during marketplace creation. Once selected, it will populate the textbox with the key. Select **Decrypt Password** to view the instance password and copy this value.

5. Open a web browser to connect to the NICE DCV web-client. Navigate to **https://YOUR-PUBLIC-IP-ADDRESS:8443** (you must include **HTTPS** and :8443). The public IP address assigned to your instance can be found within the EC2 Console instance **Details** panel.

6. NICE DCV uses a default self-signed certificate and most browsers will display a security warning regarding this. Acknowledge the notice and continue to log in. (For details on how to use your own certificate, see this link: [https://docs.aws.amazon.com/dcv/latest/adminguide/manage-cert.html](https://docs.aws.amazon.com/dcv/latest/adminguide/manage-cert.html))

7. Log in using the following credentials:
   - Username: **Administrator**
   - Password: **Retrieved from EC2 Console, Step #3**

8. The browser client session will start and display the a Window's Desktop when connected

**NOTE:** The instance executes several initialization scripts the very first time it is ever booted. This only happens this one time and can take up to 10 minutes to complete. **Your password will NOT work during this time**. If you're attempting to connect and receiving login errors (and have verified your credentials entered correctly), wait 10 minutes and try again.
Installing and using CloudXR on AWS EC2

At this point, you should be connected to the remote EC2 instance from a web browser. The EC2 instance comes configured with (most) Windows firewall settings, CloudXR server installer, and SDK documentation. It does not come with an OpenVR SDK (Steam and SteamVR) which you need to download and install manually.

1. Open the README file on the desktop and review.
2. Open a web-browser on the EC2 instance. Navigate to https://www.steamvr.com to first install Steam followed by SteamVR.
3. After SteamVR has been installed, open the folder CloudXR-SDK_2.1 on the desktop. Navigate to Installer and run CloudXR-Setup.exe
4. Ensure all CloudXR Server options remain selected and client options are NOT selected. Select **Install**. (Note: SteamVR must be already installed else the CloudXR installer will NOT complete successfully.)

5. Once completed, select the **Launch SteamVR** from the Windows Desktop. If not done already, you will be prompted to log into Steam.

6. SteamVR will launch and display a messaging asking you to connect a headset. This can be ignored. If you also see a notice regarding App Container permissions, select **Update Permissions**.
7. Validate CloudXR's plugin is installed by opening SteamVR's **settings** panel. Enable **Advanced Setting** and select **Manage Add-ons**. The addon **CloudXRRRemoteHMD** should be listed and **On** selected.

8. On the Desktop, double-click **vrserverallowadd.bat** to add a Windows Firewall rule to allow **VRServer.exe** to send and receive network traffic.
9. Verify the rule has been added by launching Run > wf.msc to open Windows Defender Firewall with Advanced Security. Look for a rule named CloudXR VR Server Path. (Also note the CLOUDXR RTSP TCP entries that were added by the CloudXR Server installer).

10. Server installation and configuration is now complete. 

   Note: AWS instances are billed based on usage. Consider configuring AWS CloudWatch alarms and/or rules to prevent charges when not in use.

   **Connecting to CloudXR Server from CloudXR Client**

   The latest CloudXR sample/test clients help developers learn how to develop their own client applications. It is strongly advised to acquire the latest samples from the NVIDIA Developer portal at [https://developer.nvidia.com/nvidia-cloudxr-sdk](https://developer.nvidia.com/nvidia-cloudxr-sdk). The instructions below may change at any time. These instructions also do not discuss methods of loading and launching client applications on HMD devices. For these details, consult the CloudXR documentation.

   1. Ensure firewalls are configured to allow access for the specified ports for CloudXR. These include your local network firewall and remote AWS VPC ACL and Security Group settings. Specific ports and their values are located with the CloudXR documentation.

   2. Launch SteamVR. It may display warning about a disconnected headset which can be ignored.

   3. Launch the CloudXR Client application on your client device and use the public IP address of your EC2 instance for its connection endpoint. Once connected, SteamVR will display icons indicating a device is connected. You will also see the SteamVR “void” within the headset. You can also open the VR view within SteamVR and validate images between the server and headset.

   4. Launch any OpenVR application and use as you normally would.

   5. Shut down / STOP the EC2 Instance when your session is over else AWS EC2 charges will continue to accumulate.