DEPLOYMENT QUICK GUIDE

TriCaster® Vectar AWS Marketplace AMI Quick Deployment Guide

Unlock the full potential of live production with the TriCaster® Vectar AWS Marketplace AMI Quick Deployment Guide. This straightforward guide provides step-by-step instructions to swiftly launch TriCaster® Vectar on AWS, ensuring you leverage cutting-edge live broadcasting technology with ease. Whether you're a seasoned broadcaster or new to cloud deployments, this guide demystifies the setup process and equips you with the tools to get your live production up and running in no time. Dive in to transform your live event broadcasting into a seamless, scalable, and secure experience.

AUGUST 2024

Contents

1 Welcome

This guide is crafted to streamline the setup of your TriCaster® Vectar using the AWS Marketplace AMI, ensuring a quick and efficient deployment. Whether integrating TriCaster® Vectar into your existing AWS infrastructure or establishing a new live production setup, the steps provided here will guide you through a hassle-free installation.

Before You Begin:

- Ensure you have an active AWS account. New to AWS? Check out the AWS Getting Started Resource Center for guidance.
- Familiarize yourself with basic AWS services concepts to smoothly follow along with the deployment steps.

About This Guide:

- **Quick Setup:** Ready to get started? You'll be operational in just about 30 minutes! Perfect for grabbing a coffee while setting up.
- **Experiment with a Complete Workflow:** Set up a small live cloud production pipeline to experiment and understand the end-to-end workflow in a live production setting, enhancing your practical knowledge for streamlining operations.
- **Free Version Notice:** The free version outputs a watermark on your production. If satisfied and seeking a watermark-free experience, please see the chapter on acquiring a license for details on upgrading.
- **Why Manual?** This guide focuses on manual deployment for those who appreciate detailed control. Prefer a faster setup? Contact us about Viz Now—our automated tool for setting up live production environments. Viz Now offers a seamless, efficient way to configure your setup, perfect for those who prefer immediate results.

For more comprehensive information and best practices beyond this quick setup, refer to the full **TriCaster® Vectar AWS Deployment Guide** here. It includes detailed sections on deployment, security, and maintenance to help you maximize your TriCaster® Vectar experience.

Let's dive into the world of live production with TriCaster® Vectar on AWS!

2 Prerequisites

Before diving into the deployment of TriCaster® Vectar via AWS Marketplace, there are a few things you'll need to ensure are in place. This chapter outlines the essential requirements needed to get started.

2.1 AWS Account Requirements

- **AWS Account:** You must have an active AWS account. If you don't have one, sign up at aws.amazon.com.
- **Permissions:** Ensure you have administrative access or sufficient permissions within your AWS account to create and manage EC2 instances, AMIs, and related resources.

2.2 Knowledge and Skills Required

- **AWS Basics:** Familiarity with navigating the AWS Management Console is crucial. You should know how to locate and use services like EC2 (Elastic Compute Cloud) and IAM (Identity and Access Management).
- **Networking Fundamentals:** Understanding of basic networking concepts such as subnets, security groups, and IP addressing will be helpful.

2.3 Software and Tools Preparations

- **Web Browser:** Ensure you have a modern web browser installed, as you will manage AWS services through the AWS Management Console, which is web-based.
- **Secure Network:** Ensure your internet connection is secure and stable, as you'll be setting up and managing cloud resources.
- **NDI Tools**: Ensure latest version of NDI Tools are installed on your local machine or any machine intended for use as a transcoder.
- **AMAZON DCV Client Installation:** To access your TriCaster® Vectar instance remotely and manage its graphical user interface, you will need to install the AMAZON DCV client. Download and install the client software from the official AWS page: AMAZON DCV Download.

2.4 AWS Service Quotas

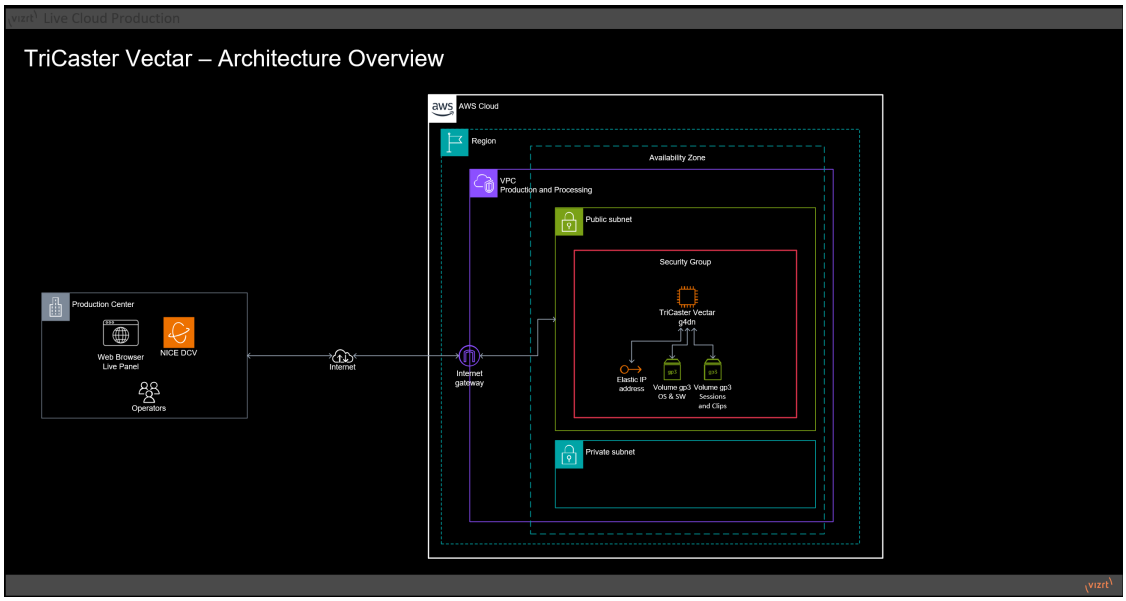
- **GPU Instance Availability**: TriCaster® Vectar requires EC2 instances equipped with GPUs. Check your AWS Service Quotas to ensure you have the capacity to launch EC2 instances with GPUs, such as the G and VT instance families.
- **Adjust Quotas if Necessary**: If the default quotas do not meet your needs, you may need to request an increase. This can be done through the AWS Management Console under the Service Quotas section. Keep in mind that approval might take some time, so it's advisable to manage this well before your planned deployment.

2.5 Security Responsibilities and Best Practices

The deployment process involves setting up various AWS resources. While this guide includes security tips and recommendations, it is ultimately your responsibility to ensure the security of your cloud resources. We strongly advise referring to the AWS security documentation and best practices for each resource deployed in the TriCaster Vectar AMI.

3 TriCaster Vectar Architecture Overview

This chapter provides a high-level overview of the AWS architecture you'll deploy using the TriCaster Vectar AMI, ensuring a secure, scalable, and efficient live production environment:



- **Virtual Private Cloud (VPC):** Your dedicated VPC isolates your network within AWS, creating a secure space for your resources that's disconnected from other networks.
- **Subnet Configuration:** One public subnet within your VPC hosts your EC2 instance. This subnet facilitates direct internet connectivity, enhancing the interaction with external content and services.
- **Internet Gateway:** An integral component that connects your VPC to the internet, enabling your instances in public subnets to communicate outwardly, essential for real-time content distribution.
- **EC2 Deployment:** EC2 instances are strategically deployed in public subnets to optimize accessibility and performance for your live production needs.
- **Elastic IP Allocation:** A static public IP address is assigned to your EC2 instance, ensuring a consistent point of access for incoming and outgoing internet traffic.
- **Security Group Configuration:** Security groups are meticulously configured to allow connections only from whitelisted IP addresses, safeguarding access to your instances.

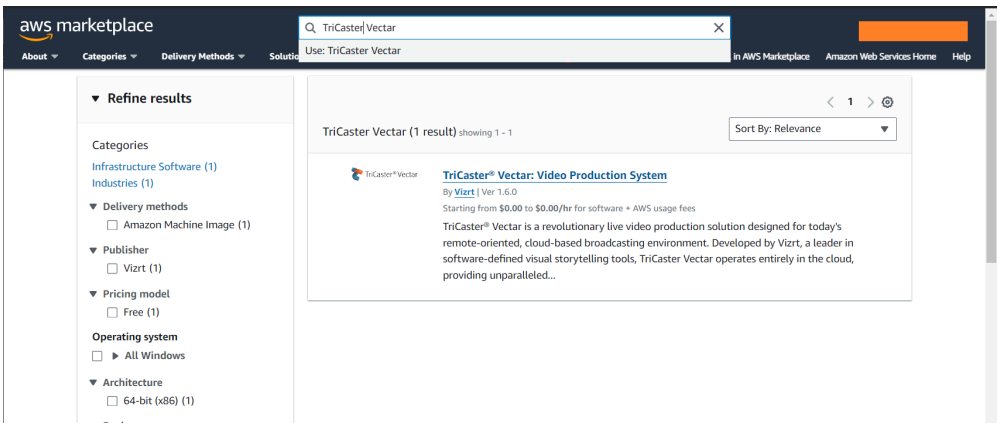
- **Remote Access via AMAZON DCV:** For high-quality, low-latency remote access, AMAZON DCV is utilized, providing a superior PCoIP experience that ensures smooth, secure, and responsive interaction with your TriCaster Vectar environment.

4 AMI Deployment Process

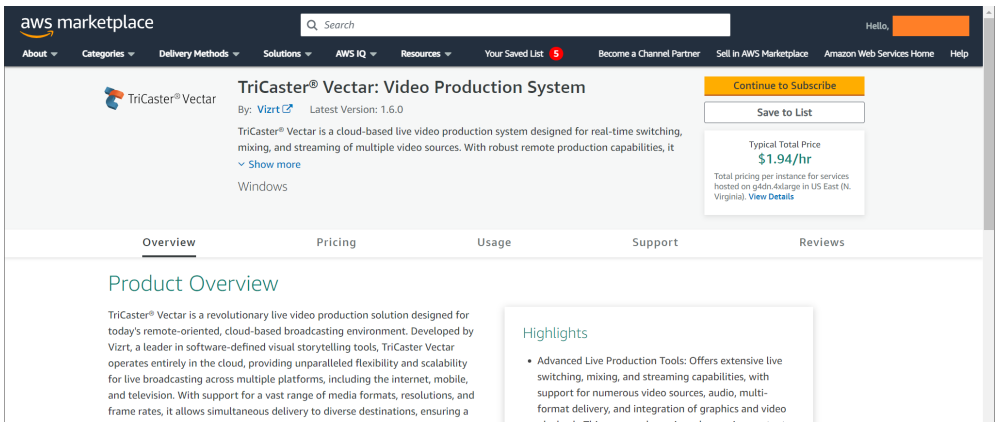
Deploying TriCaster® Vectar from the AWS Marketplace is straightforward. This chapter walks you through each step from finding the AMI to launching your EC2 instance with TriCaster® Vectar installed.

4.1 Accessing the AWS Marketplace

- **Search for TriCaster® Vectar:** Log into your AWS Management Console. Navigate to the AWS Marketplace and enter “TriCaster® Vectar” in the search bar. Select the official AMI provided by Vizrt.

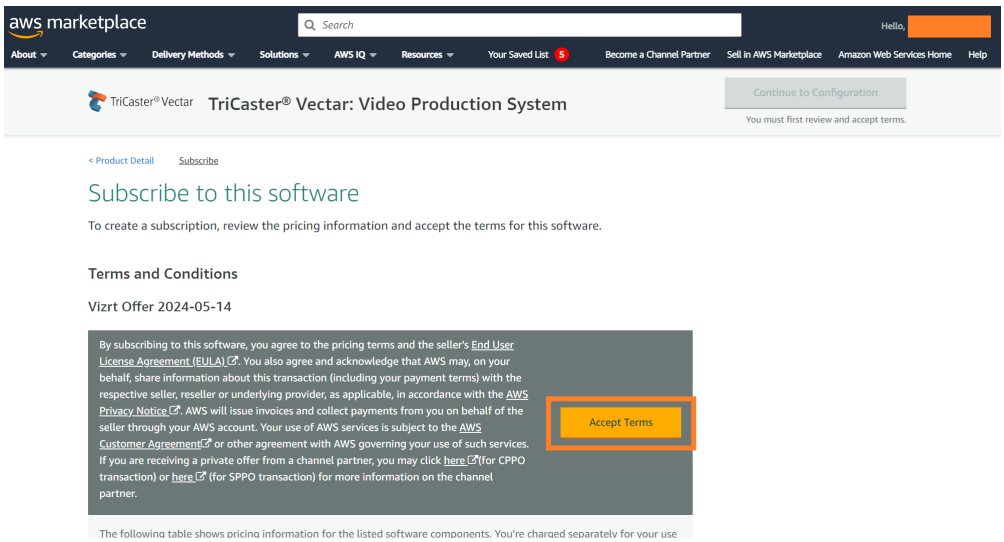


- **Review AMI Details:** On the product page, review the details of the AMI, including pricing, configuration options.

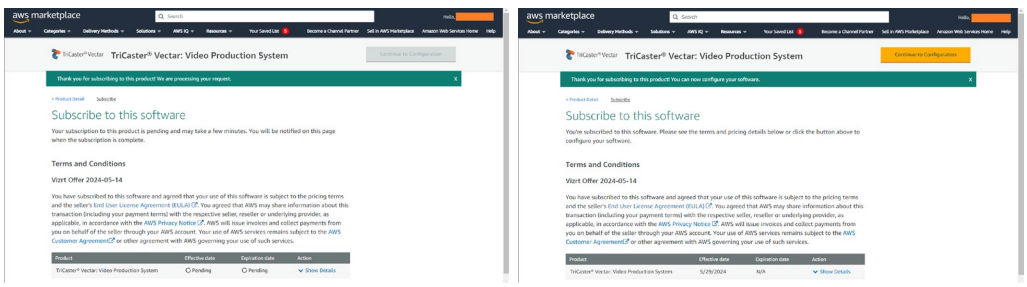


4.2 Selecting the TriCaster® Vectar AMI

- **Choose an AMI:** Click on ‘Continue to Subscribe’ to review the terms and accept them if you agree. After subscribing, it may take a moment for the AMI to become available for configuration.



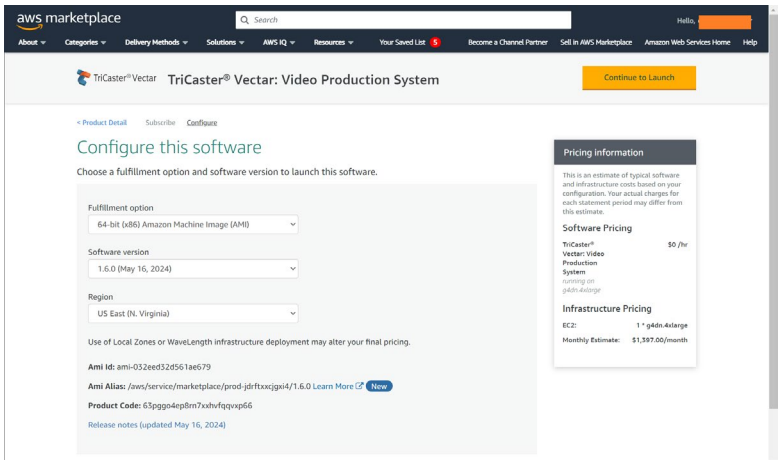
- **Proceed with Configuration:** Once the AMI is available, click on ‘Continue to Configuration’ to proceed with setting up your instance.



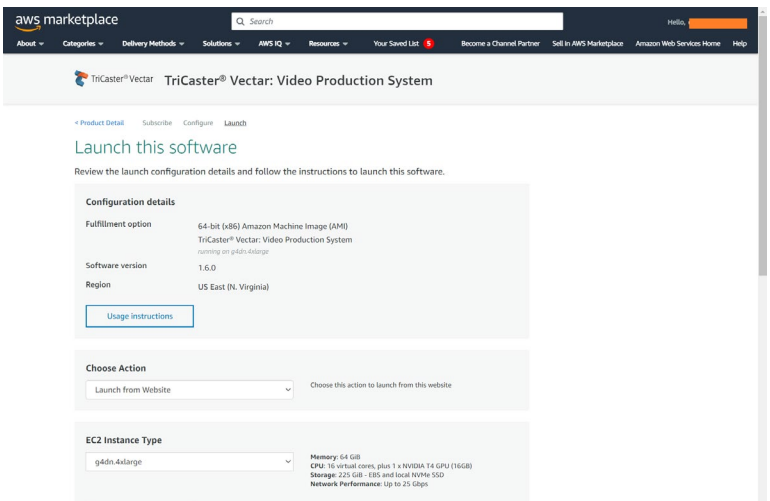
4.3 Configuring Instance Details

- **Choose the Version:** Select the software version of TriCaster® Vectar you wish to deploy.
- **Select the Region**: Choose the AWS region where your EC2 instance will be deployed. Selecting a region close to your operators can reduce latency and improve performance.

- **Continue to Launch:** After selecting your desired region, click the ‘Continue to Launch’ button to move forward in the deployment process.



- **Click on Usage Instructions**: Before proceeding, access the available documentation by clicking on 'Usage Instructions' to understand all features and deployment considerations.
- **Confirm Launch Method**: Ensure that 'Launch from Website' is selected in the 'Choose Action' dropdown menu.
- **Select the Appropriate EC2 Instance Type**: Choose an EC2 instance type that meets the requirements of your deployment. If you are unsure which instance type to select, refer to the 'Optimizing EC2 Instances' section in the **TriCaster® Vectar AWS Deployment Guide** for detailed guidance. This guide provides insights into selecting instance types with the necessary capabilities. If still in doubt, opt for the recommended instance type.



4.4 Network and Security Settings

Configure Virtual Private Cloud (VPC)

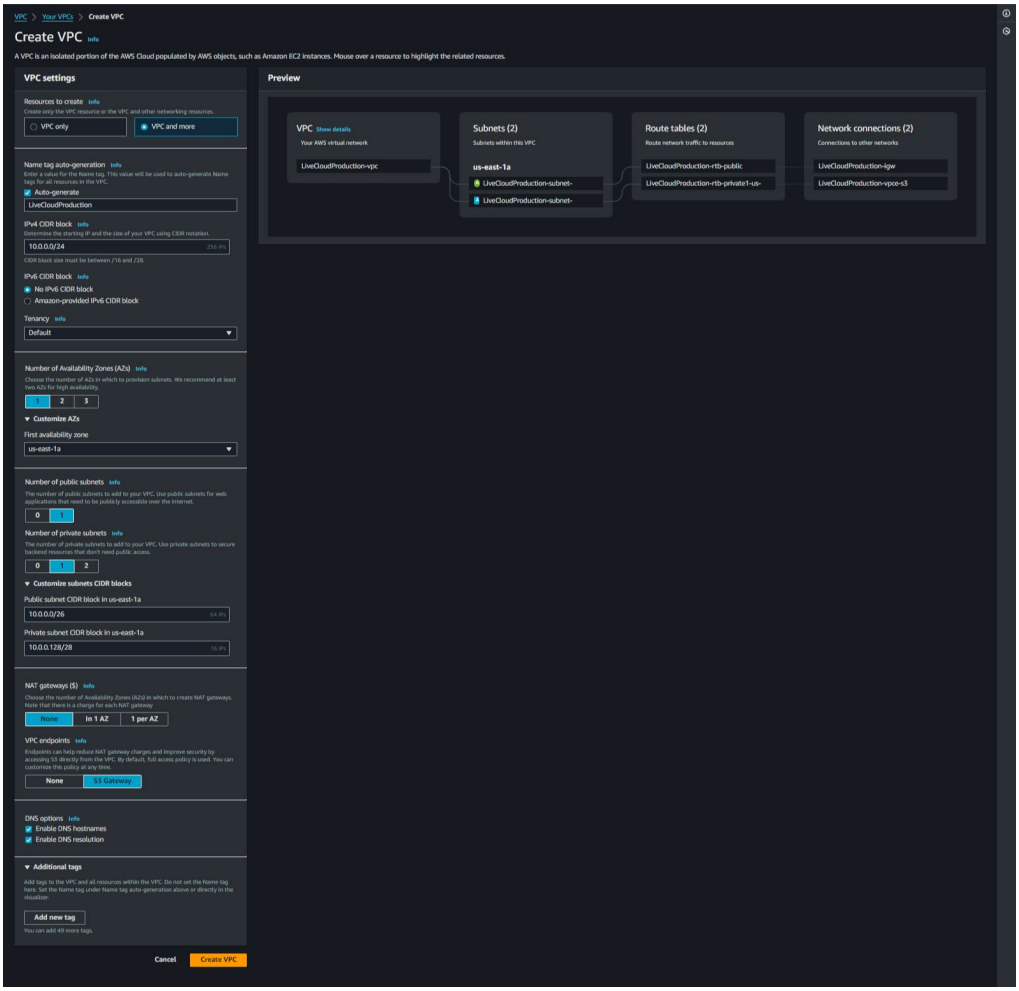
When deploying TriCaster® Vectar, you'll need to decide whether to integrate it into an existing VPC or set up a new one. This choice depends on whether you want to utilize your current network infrastructure or create a dedicated environment for your live production.

- **Select an Existing VPC**: If you choose to deploy TriCaster® Vectar within an existing network, simply select the appropriate VPC from the dropdown list in the AWS Marketplace setup.

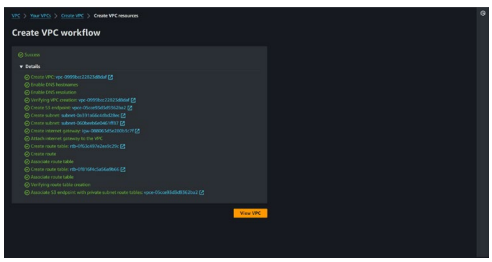
To set up a new VPC for your TriCaster Vectar deployment, follow these detailed steps to ensure proper configuration:

- **Navigate to VPC Creation:** click **'Create a VPC in EC2**' to open the VPC dashboard in the AWS Management Console.
- Click on **Create VPC** in the top right corner of the VPC dashboard and select **VPC and More** to proceed with a detailed setup process.
- **Name tag:** Assign a descriptive name to your VPC, such as ***LiveCloudProduction***, to easily identify it later.
- **Set IPv4 CIDR block:** Use a CIDR block like **10.0.0.0/24** for the VPC. This block size is generally sufficient for most deployment scenarios unless specific larger or segmented networking setups are required. See Appendices for best practice.
- **Number of Availability Zones**: Choose 1 to specify the number of Availability Zones you want to include in your VPC.
- **Customize Public subnets CIDR blocks**: Enter 10.0.0.0/26 for the public subnet within your chosen Availability Zone.

- Review your settings to make sure everything is correct.

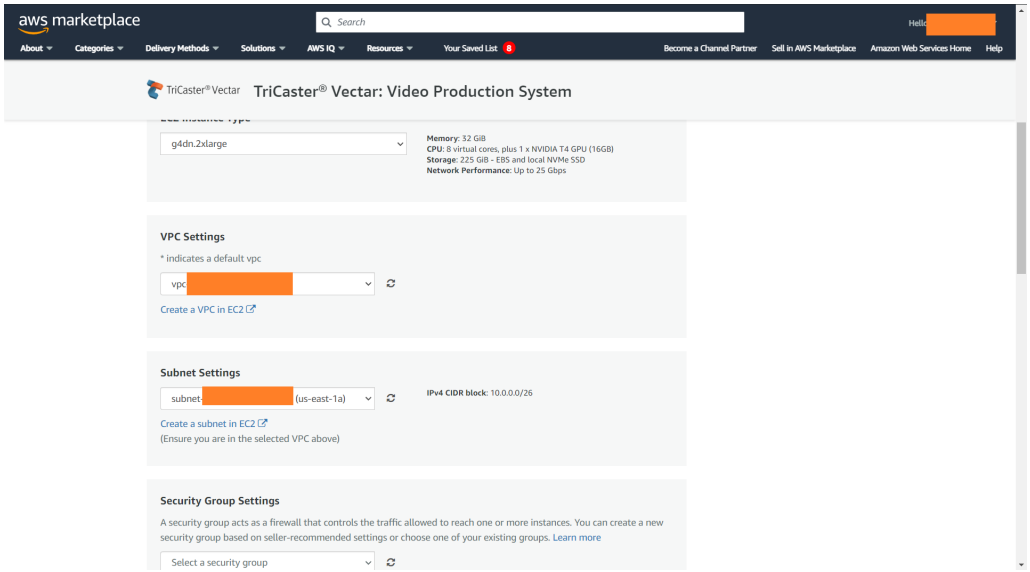


- Click **Create VPC** to establish your new VPC with the specified configurations.



- Click **View VPC** to return to the VPC dashboard

- **Return to AWS Marketplace:** go back to the AWS Marketplace, refresh the VPC list, and select the newly created VPC from the dropdown.
- Select the newly created **public subnet** from the dropdown.

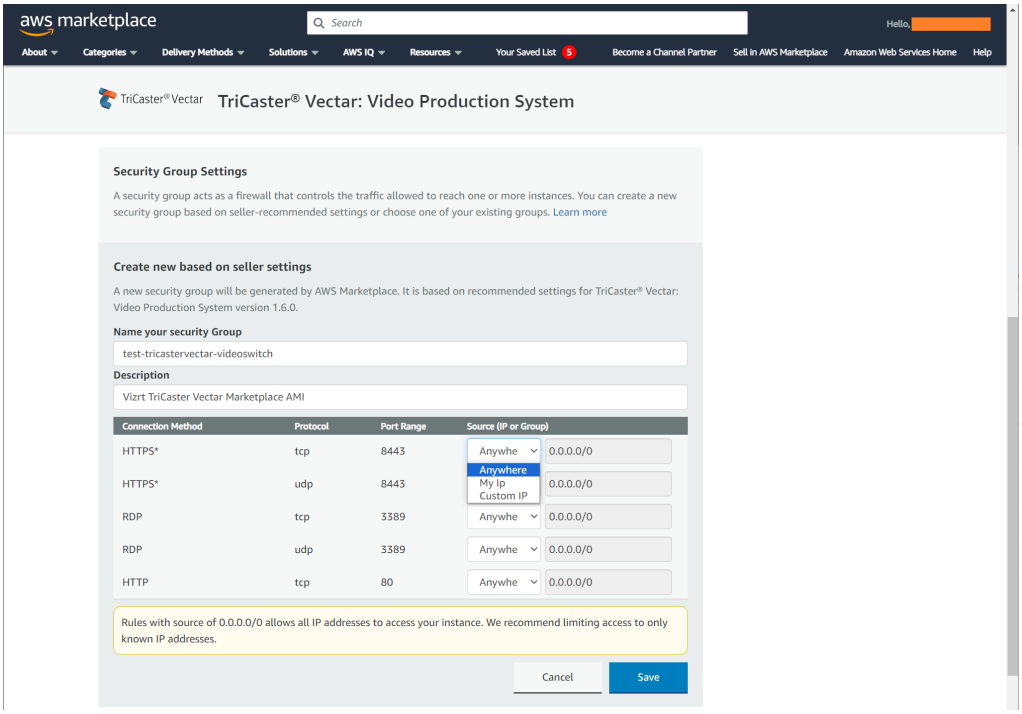


Configure Security Group

Security groups act as a virtual firewall that controls the traffic allowed to and from your EC2 instance. You have the option to use an existing security group or create a new one that meets the specific needs of your TriCaster® Vectar deployment.

- **Select an Existing Security Group:** If an appropriate security group already exists in your account, you can select it from the 'Security Group' dropdown menu. Ensure that this security group has the necessary ports open as required for your deployment. For guidance on which ports need to be opened based on your intended usage (such as specific video and audio protocols), refer to the 'Configuration and Customization Options' chapter in the TriCaster® Vectar Deployment Guide.
- **Create a New Security Group using Use Seller Settings:** click the 'Create New Based on Seller Setting' button.
- **Naming Your Security Group:** provide a name for instance, name it ‘test-tricastervectar-videoswitch’, add a brief description such as 'Vizrt TriCaster Vectar Marketplace AMI' helps identify the purpose of the security group.

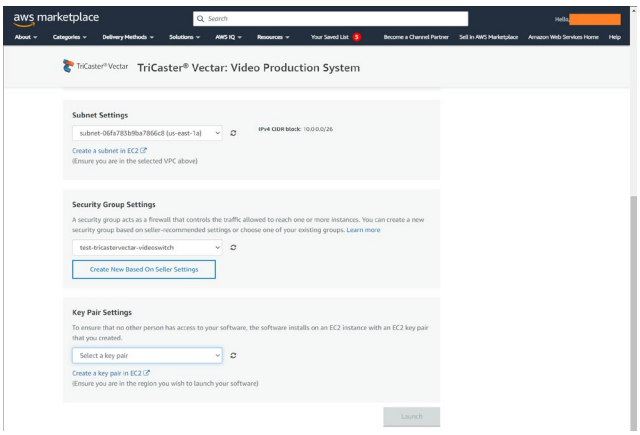
- **Customize IP Restrictions:** To enhance security, You can restrict access to your current IP or a custom list of IPs to ensure that only authorized users can connect to your instance.



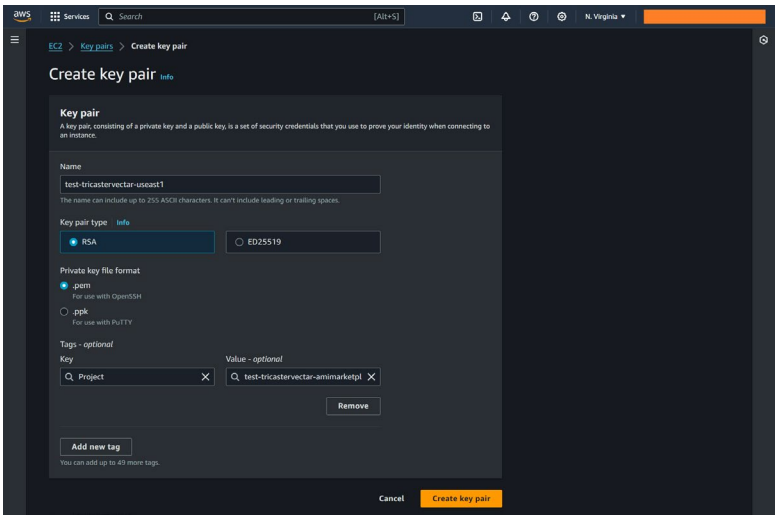
Setting Up Key Pairs

Key pairs are essential for securely accessing your EC2 instances. They are used to decrypt the administrator password and ensure secure SSH access. You'll need to create a key pair if you don't already have one suitable for this deployment.

- **Navigate to Key Pair Creation:** Click on '**Create a key pair in EC2**', which will direct you to the EC2 console's Key Pairs section.



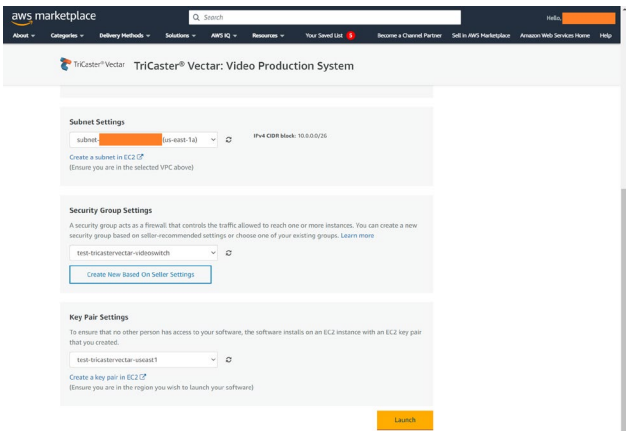
- **Region Selection:** Ensure you are in the correct AWS region where you plan to launch TriCaster® Vectar. This is crucial as key pairs are specific to the region they are created in.
- **Name Your Key Pair:** Assign a descriptive name to your key pair, such as **'test-tricastervectar-useast1'**, indicating the purpose and the region it is intended for.
- **Select File Format**: Choose **.pem** from the file format options.
- **Optional Tagging:** Assign tags to your key pair if needed.
- **Download Key Pair:** Upon creation, download the key pair file. AWS provides the private key file in a .ppk format.
- **Secure Storage:** Store the downloaded key pair file in a secure location. This file is crucial for accessing your EC2 instance and cannot be downloaded again; AWS does not retain a copy of it.



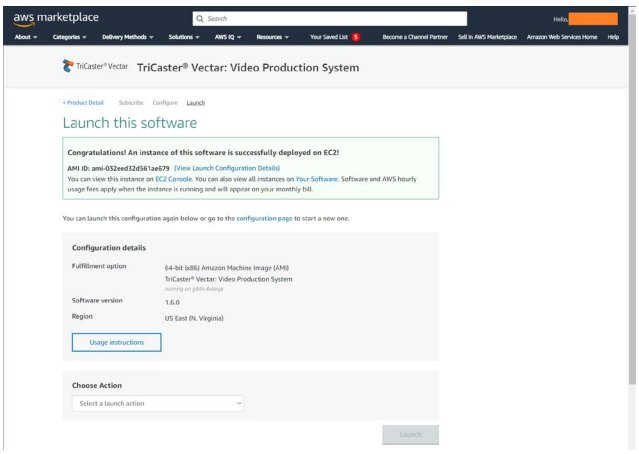
- **Refresh Key Pair List:** downloading your key pair, return to the AWS Marketplace where you initiated the instance setup.
- **Select the New Key Pair:** Refresh the list of key pairs to see the newly created one. Select your new key pair, test-tricastervectar-useast1, from the dropdown menu.

4.5 Launching the Instance

- **Review Configuration:** Carefully review all configurations to ensure everything is set correctly according to your requirements. This includes the EC2 instance type, VPC, subnet, security group settings, and any other configurations you have made.

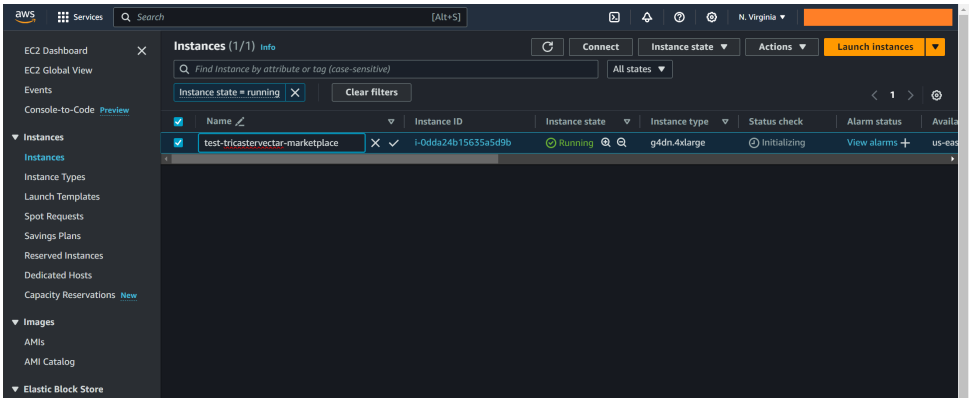


- **Initiate Launch:** Click on the 'Launch' button to start the deployment of your TriCaster® Vectar instance.

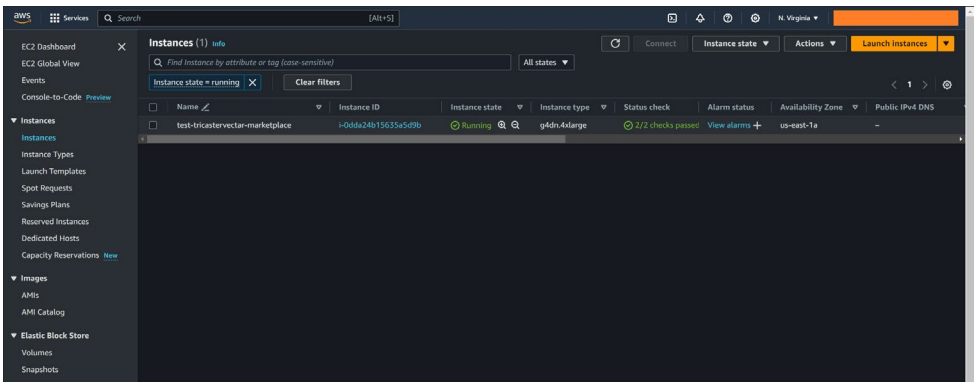


- **Navigate to EC2 Dashboard:** open the AWS Console and select the EC2 service from the services menu.
- **Access Instances Section:** Click on 'Instances' to view the list of your EC2 instances. This will display all your instances, including the newly launched TriCaster® Vectar instance.

- **Name Your Instance:** Select your new instance, click the ‘Name’ column, and assign a clear name such as **test-tricastervectar-marketplace**, to easily identify it among other resources.



- **Monitor the Deployment:** After initiating the launch, monitor the status of your EC2 instance in the AWS EC2 Management Console. It might take a few minutes for the instance to be fully set up and operational.



5 Initial Setup and Configuration

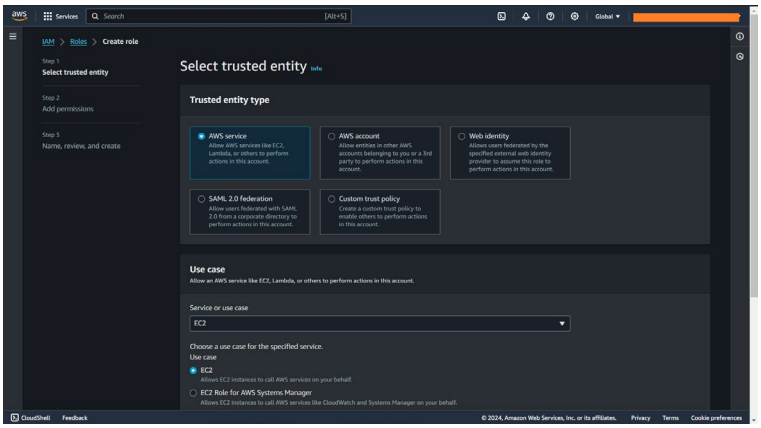
5.1 Associating an IAM Profile for Amazon DCV Licensing

Setting up the proper IAM profile is crucial for licensing Amazon DCV on your Amazon EC2 instance. Follow these steps to ensure the correct IAM profile is associated with your EC2 instance (reference AMAZON DCV licensing requirements):

1. **Stop the Running Instance:**
    - Navigate to the EC2 console in your AWS Management Console.
    - Select the EC2 instance running TriCaster Vectar.
    - Click the **Actions** button, and under the **Instance State** dropdown, choose **Stop** to halt the instance. This step is necessary to apply the new IAM role.
2. **Create an IAM Role:**

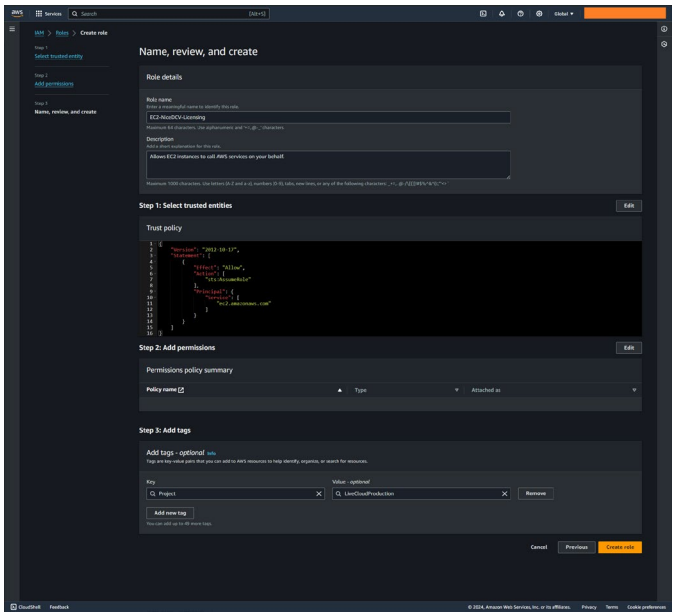
If a suitable role already exists, you can skip role creation and use the existing role. Ensure that the role has the necessary permissions as outlined in the Amazon DCV Administrator Guide.

- Open a new tab in your browser and go to the IAM service in the AWS console.
- Click on **Roles** on the left sidebar, then click the **Create role** button.
- For the trusted entity type, choose **AWS service**.
- Under **Common use cases**, select **EC2**. This allows EC2 instances to call AWS services on your behalf.
- Click **Next** twice to proceed with the role configuration.



3. **Name and Review:**

   - Give your role a meaningful name, such as ***EC2-NiceDCV-Licensing***.
   - Optionally, add a description to remind you of the role's purpose.
   - Review the role details to ensure everything is configured correctly and then click Create role.



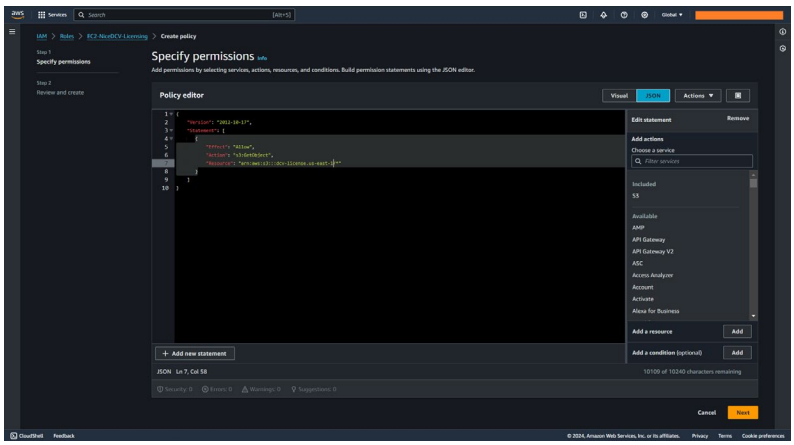
4. **Configure Permissions:**

   - **Access the Created Role:** Navigate back to the IAM console.
   - Under the Roles section, find and click on the role you previously created (e.g., ***EC2-NiceDCV-Licensing***).
   - **Add Permission to the Role:** Click on the Add permissions button.
   - Choose **Create inline policy** to directly attach custom permissions.
   - **Define the Policy:** Click on the JSON tab to manually edit the policy.
   - Copy and paste the following policy into the JSON editor:

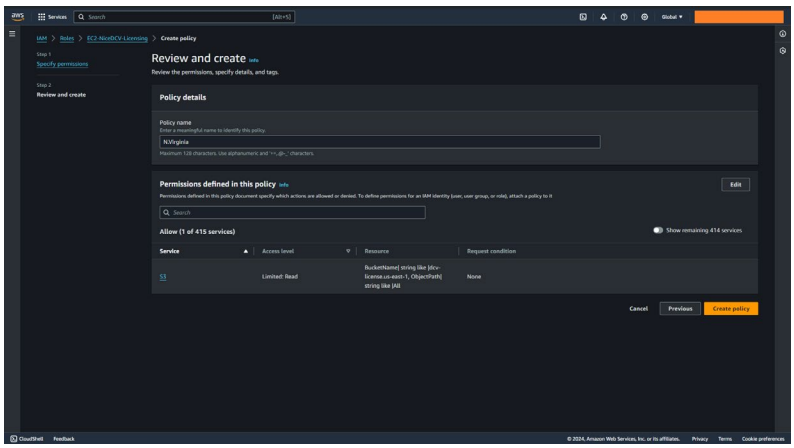
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::dcv-license.region/*"
        }
    ]
}
```

- **Replace <region>** in the Resource path with your AWS Region, such as **us-east-1**. This ensures that the policy is correctly configured for your specific geographic area.

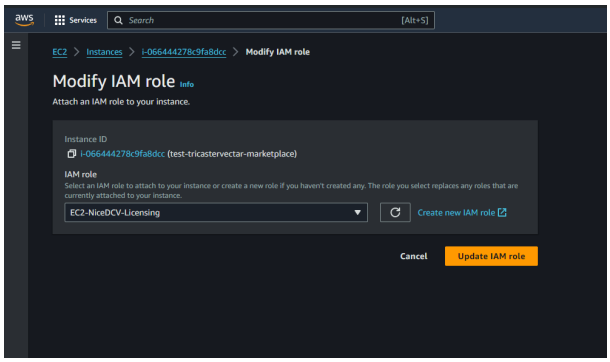


- **Review and Create Policy:** After inputting the policy, click Next to proceed.
- Review the policy settings to ensure everything is correct.
- Provide a descriptive name for the policy, such as ***NiceDCV-License-Policy-N.Virginia***, to easily identify it later.
- Click **Create policy** to finalize the setup.



5. **Associate the IAM Role with the EC2 Instance:** Return to the EC2 console where your instance is listed. Select the instance, click on **Actions**, navigate to **Security**, and select **Modify IAM role**.

6. Choose the IAM role you just created from the dropdown list and apply it to the instance.



5.2 Setting Auto-assigned IP Address in the EC2 Console

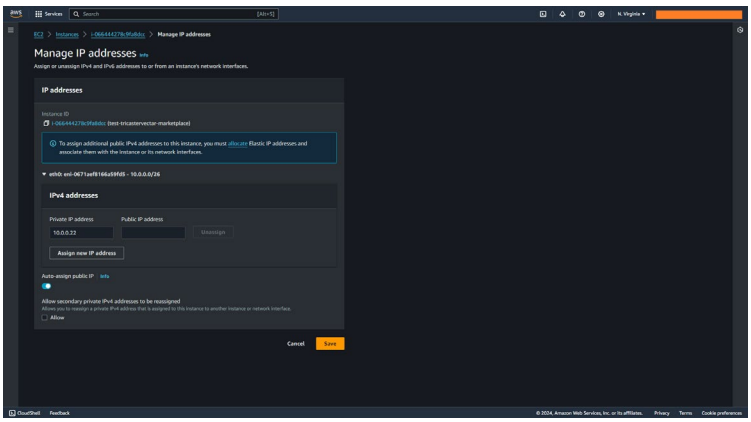
To ensure your EC2 instance can communicate effectively with the internet, you need to enable auto-assignment of public IP addresses, especially if your instance operates within a public subnet. Follow these steps to configure this setting:

1. **Navigate to EC2 Management Console: go back to the AWS** Management Console and open the EC2 service dashboard and select the EC2 instance by clicking the checkbox next to it.

2. **Modify Network Interface:** look for the **Actions** dropdown menu, navigate to **Networking** > **Manage IP addresses**.

3. **Configure Auto-assign Public IP:** In the network interfaces section, find the primary network interface (usually labeled as eth0) and click on it.

4. Look for the option labeled **Auto-assign Public IP** and set to **Enable**. Confirm your changes by clicking **Save**.



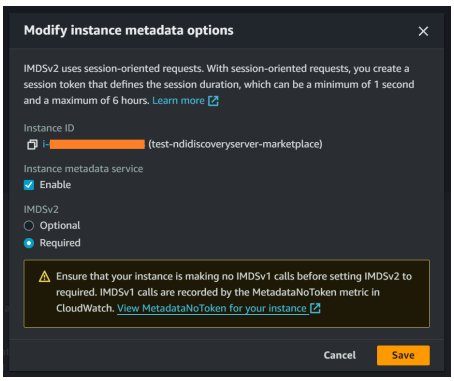
With this option, the setup is straightforward and cost-effective as it does not incur any additional charges for the IP address. However, it's important to note that with auto-assigned IP addresses, the IP will change every time the machine is stopped and restarted.

Considering a Fixed IP? If your workflow requires a stable IP address, you might want to consider allocating an Elastic IP address. To learn how to allocate and associate an Elastic IP address to your EC2 instance, refer to the AWS documentation.

5.3 Enabling IMDSv2 Metadata

For enhanced security, it's important to enable the Instance Metadata Service Version 2 (IMDSv2) on your EC2 instances. Follow these steps to configure IMDSv2:

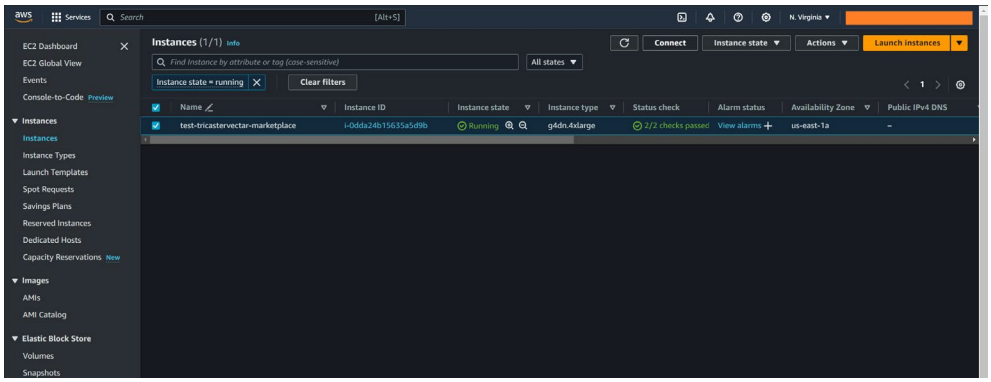
1. **Navigate to EC2 Management Console**: Open the AWS Management Console and access the EC2 service dashboard.
2. **Instance Details**: Locate the EC2 instance, select the instance by clicking the checkbox next to it.
3. **Modify Instance Setting**: find and click on the 'Actions' dropdown menu. Choose 'Instance Settings' and select 'Modify Instance Metadata Options'.
4. **Enable IMDSv2**: Set the state to 'Required'. Click 'Save' to apply the changes.



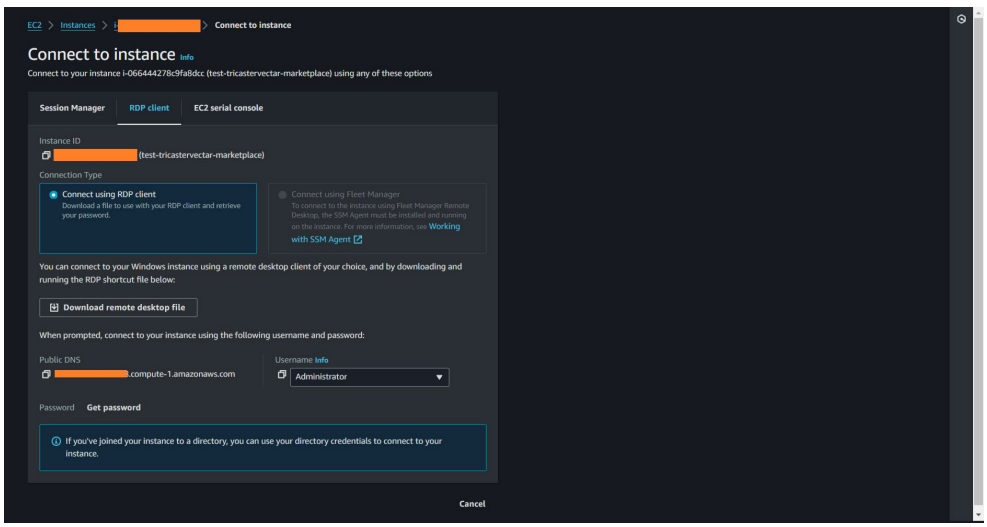
5.4 Starting and Connecting to Your EC2 Instance

Follow these steps to start your EC2 instance and connect to it using an RDP client, such as Amazon DCV, which allows for secure and high-performance remote access.

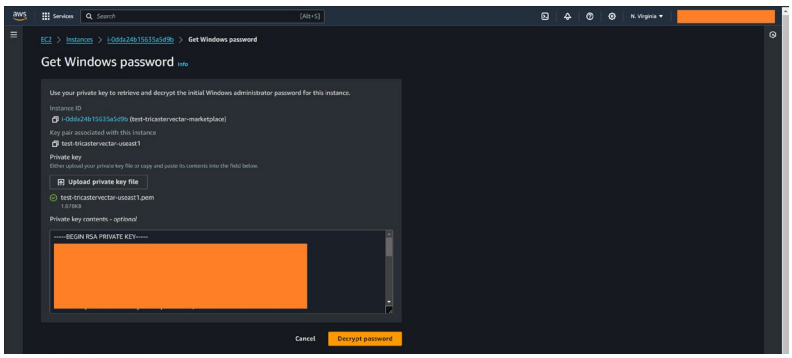
1. **Start the EC2 Instance:** Go to the AWS EC2 Console, navigate to the **Instances** section. Select the instance by checking the box next to it, click on the **Instance State** button, then select **Start instance**.



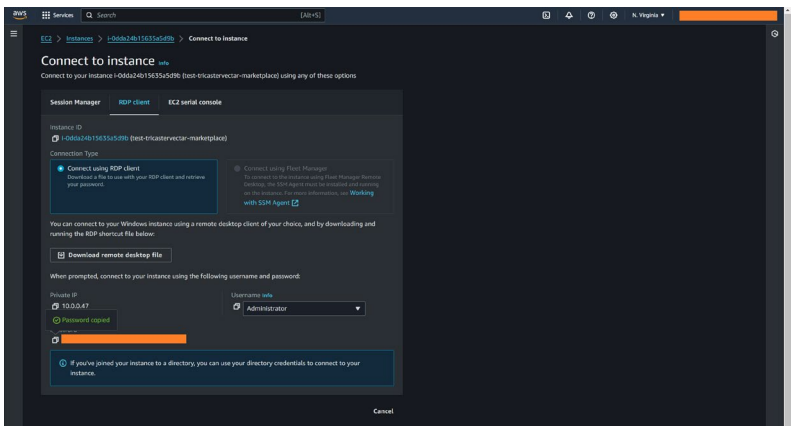
2. **Connect Using RDP Client:** Once the instance is running, click on the **Connect** button at the top of the EC2 console. In the **Connect to instance** page, select the **RDP client** tab.



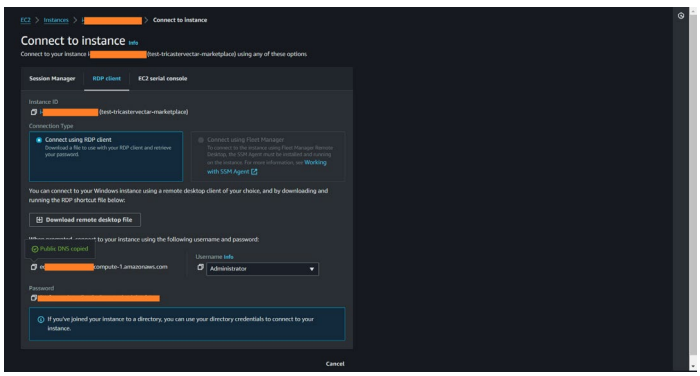
3. **Decrypt the Administrator Password:** click on **Get password**, upload the private key file that you saved securely during the key pair creation step.



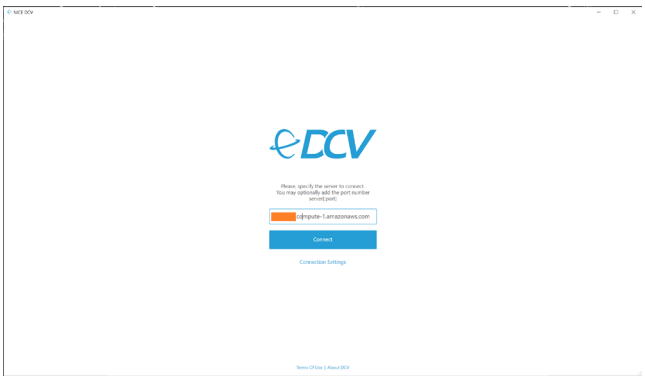
4. Click on **Decrypt password** to reveal the administrator password. Make sure to copy this password as you will need it to log in.



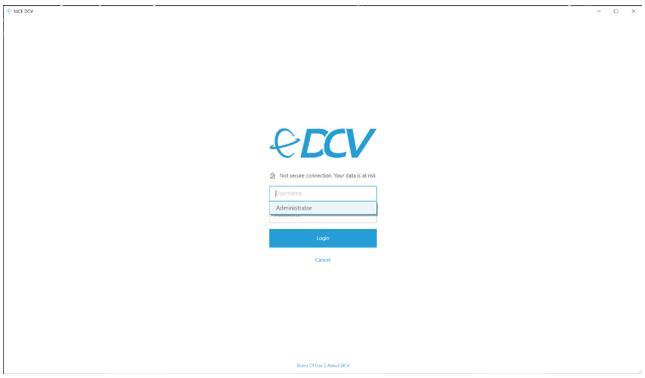
5. **Copy the Public DNS:** Locate and copy the **Public DNS** address displayed. This address is needed to connect to your instance via AMAZON DCV.



6. **Launch Amazon DCV Client:** Open the Amazon DCV client on your local machine. In the connection window, paste the public IP address of your EC2 instance.

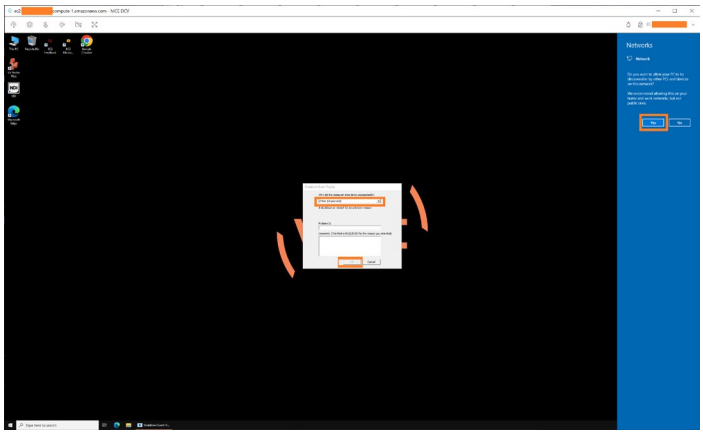


7. Enter the username Administrator and the decrypted administrator password. Click **Connect** to initiate the remote desktop session.



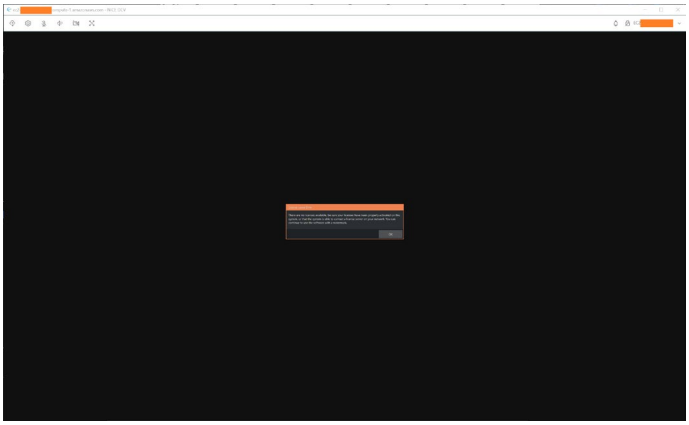
8. **Launch TriCaster Vectar:**
    - **Resolve Shutdown Event Tracker Modal:** you may encounter the Shutdown Event Tracker modal due to the way the instance was previously. Select the appropriate reason, then click **OK** to proceed.

- **Confirm Network Discoverability:** Windows may prompt you to make your network discoverable. Click **Yes** to ensure that your instance can communicate effectively with other services.

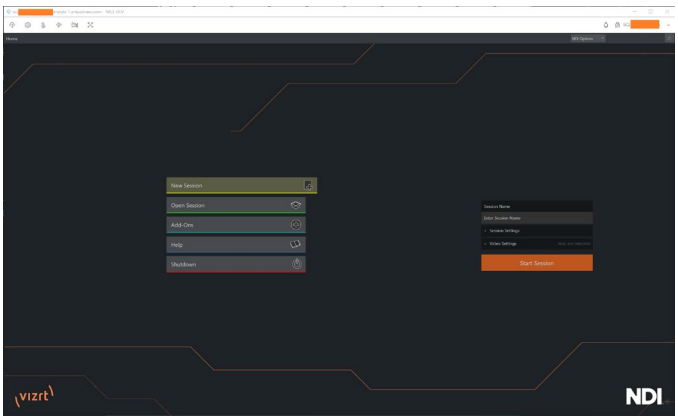


- **Optional Customer Engagement Form**: Upon the first launch, you have the option to fill out a brief customer engagement form. This step is designed to facilitate communication between you and our product experts. While filling out this form is not mandatory, it offers significant benefits for enhancing your user experience.
- **Exclusive Benefit for Registrants**: After registering, you will receive a free trial of Viz Flowics, our advanced HTML graphics SaaS solution. Viz Flowics is fully compatible with TriCaster® Vectar and enhances your production with dynamic, real-time graphics.

- **License Notification:** Upon starting TriCaster Vectar, a notification may appear indicating that a valid license is not detected. Click **OK** to acknowledge this message. Note that without a valid license, the output from TriCaster Vectar will include a watermark, indicating unlicensed usage.



- **TriCaster Vectar Main Screen:** After handling initial configurations and notifications, the main screen of TriCaster Vectar will appear. This screen is your primary interface for managing and executing live production tasks.



- Take a moment to familiarize yourself with the layout and available tools. From here, you can begin setting up your production environment according to your specific needs.

6 Next Steps: Establishing Your Live Cloud Production Pipeline

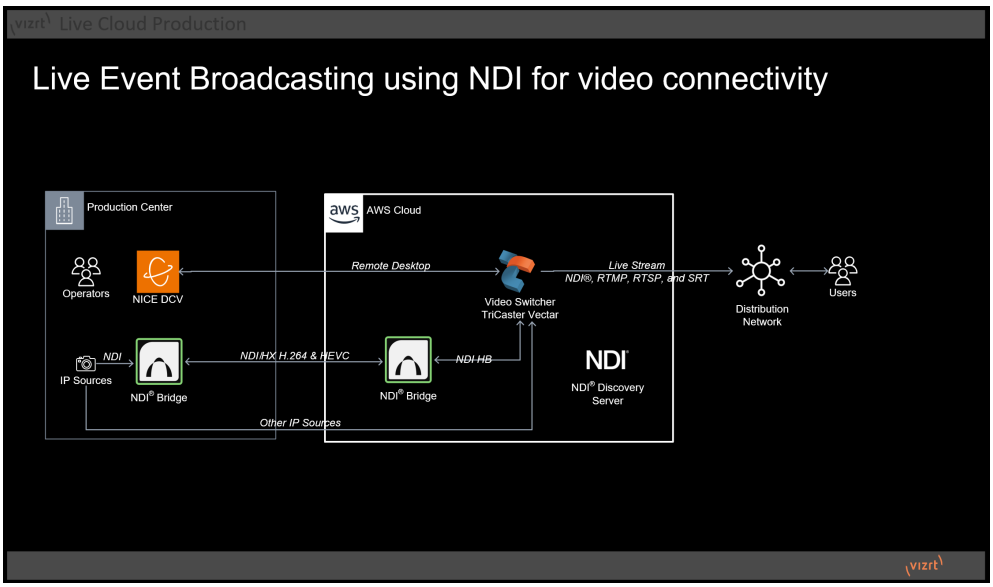
Having successfully deployed TriCaster® Vectar via the AWS Marketplace, you are now equipped to broaden your live production capabilities. TriCaster® Vectar is versatile enough to support a wide range of scenarios, including live event broadcasting for sports, concerts, and conferences, scaling remote distributed productions, or enhancing your disaster recovery strategies. Descriptions of these use cases are available in the TriCaster® Vectar AWS Deployment Guide.

This chapter introduces one of the many potential use cases. We will show you how to set up a small production pipeline using NDI technology, although other protocols like SRT are also supported, offering flexible production configurations.

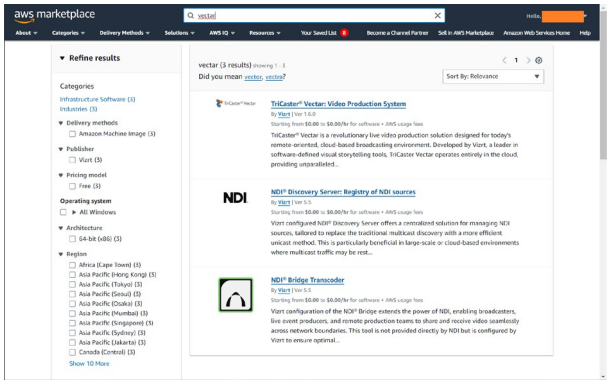
We have provided two additional AMIs featuring NDI technology, configured by Vizrt to complement our suite of products. These AMIs, although not provided directly by NDI, are optimized for use with Vizrt live production workflows, ensuring enhanced integration and performance when used alongside other Vizrt solutions.

Please note that this setup is optional and TriCaster® Vectar can function effectively without it.

6.1 Live Event Broadcasting Solution leveraging NDI



Search 'Vectar' on AWS Marketplace to find all the necessary products for your production pipeline.



Here's how to get started:

1. Deploy NDI Discovery Server:

- **Purpose:** The NDI Discovery Server acts as a central repository for all NDI sources, making it easier to manage and access feeds across your network.
- **Deployment:** Also available on the AWS Marketplace, the NDI Discovery Server should be set up within the same VPC as your TriCaster Vectar and NDI Bridge.

2. Deploy NDI Bridge:

- **Purpose:** NDI Bridge connects NDI networks securely over the internet, facilitating the exchange of NDI feeds between on-premises production environments and your AWS-hosted TriCaster Vectar.
- **Setup:** Search for the NDI Bridge on the AWS Marketplace and follow the deployment instructions similar to those you used for TriCaster Vectar. Ensure it is configured to communicate with your TriCaster Vectar instance for seamless feed integration.

3. Finalizing Your TriCaster Vectar:

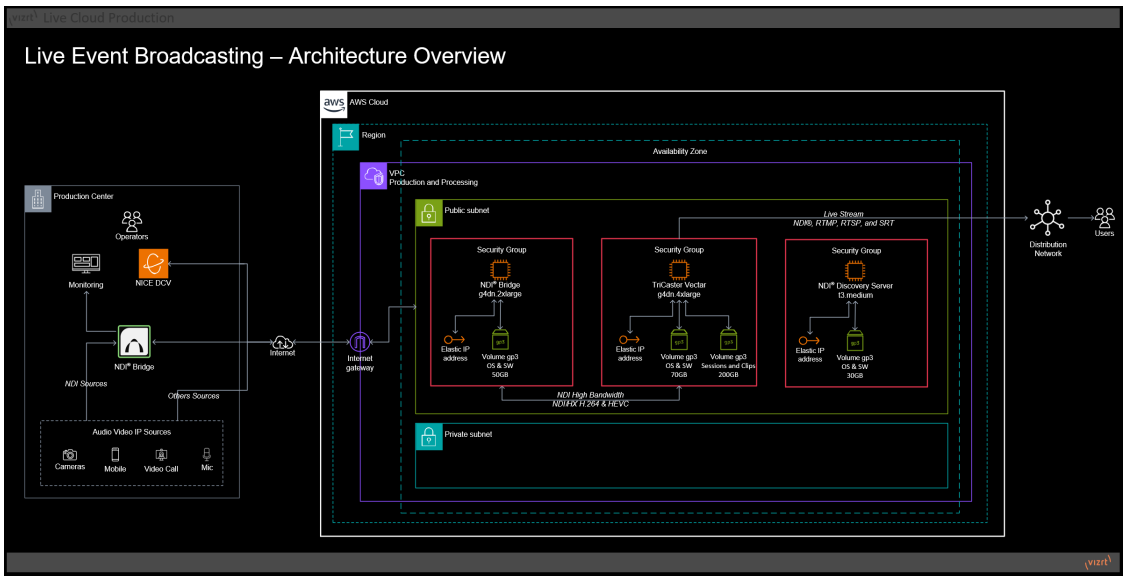
- **Integration:** With NDI Bridge and Discovery Server in place, configure your TriCaster Vectar to receive and send NDI feeds to/from your ground facilities.
- **Settings:** Adjust your TriCaster Vectar's settings to utilize the Discovery Server for feed management and configure your Live Session.

4. Set Up CDN Publishing:

- **Connection:** Configure your TriCaster Vectar to stream directly to your chosen CDN. This involves setting up the streaming outputs within TriCaster Vectar's interface and ensuring your CDN credentials and endpoints are correctly configured.
- **Testing:** Conduct a series of test streams to ensure stability and quality before going live.

5. Go Live:

- **Monitoring:** Utilize TriCaster Vectar to monitor live feeds and production performance.
- **Adjustments:** Make real-time adjustments as needed to maintain quality and address any issues that arise during live streaming.



By following these steps, you can create a robust, scalable, and secure live cloud production pipeline that leverages the full capabilities of TriCaster Vectar, NDI Bridge, and Discovery Server. This setup not only enhances your production flexibility but also ensures high-quality live-streaming delivery to audiences worldwide.

6.2 Deploy NDI Discovery Server

Deploying the NDI Discovery Server in your AWS environment can be streamlined by using the resources and configurations already established for TriCaster® Vectar. Follow the steps below to integrate the NDI Discovery Server into the same ecosystem efficiently.

Search and deploy from AWS Marketplace:

1. **Search for NDI Discovery Server in AWS Marketplace.** Navigate to the AWS Marketplace and enter "NDI Discovery Server" in the search bar to find the appropriate AMI.
2. **Follow the AMI Deployment Process.** Use the deployment instructions provided in this guide. Remember to adjust the selections to fit the deployment of the NDI Discovery Server:
    - **Network and Security Settings:** Choose the existing VPC and the subnet that was used for TriCaster® Vectar to ensure that both systems are within the same network environment.
    - **Security Group:** Create a new security group specifically for the NDI Discovery Server to ensure it has the appropriate security settings. This ensures that the security settings are tailored to the needs of the NDI Discovery Server while maintaining a secure network environment.
    - **Key Pairs:** You have the option to create a new key pair or reuse an existing one. Ensure you decrypt and save the new password for the NDI Discovery Server, as it will differ from that of TriCaster® Vectar.

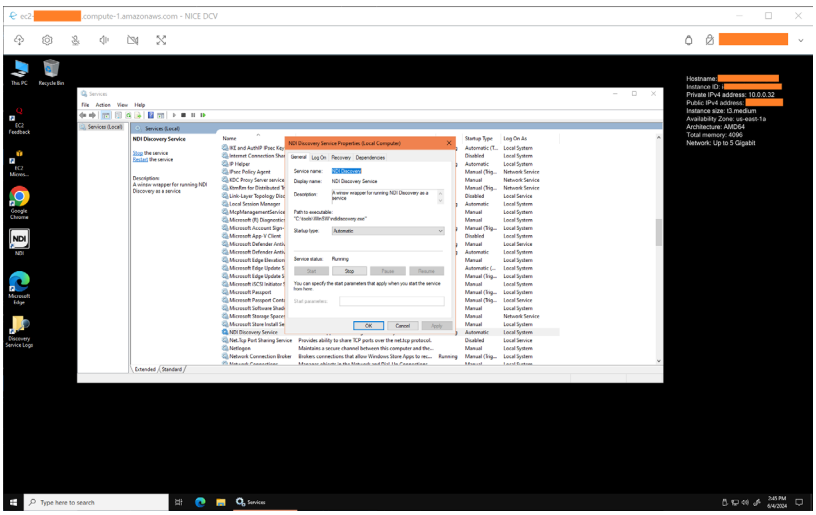
Initial Setup and Configuration:

3. **Initial Configuration:** Follow the setup steps similar to those for TriCaster® Vectar. You can skip duplicating some of the AWS resource creations:
    - **Associating an IAM Profile:** If you have already set up an IAM profile for Amazon DCV Licensing with TriCaster® Vectar, reuse this role. Directly associate it with the new EC2 instance of the NDI Discovery Server without creating a new one.
    - **Launch and Connect:** Once the instance is running, retrieve and save the administrator password.

Post-Deployment:

4. **Check Service Status:** Once connected, you can verify the NDI Discovery Server is running properly by using the Services application in Windows. Search for the "NDI Discovery Server" to see if it is active and running.

5. **Note the Private IP Address:** Document the private IP address displayed either on the Windows desktop or in the AWS EC2 console. This IP address will be crucial for configuring NDI Bridge and TriCaster® Vectar to communicate with the Discovery Server.

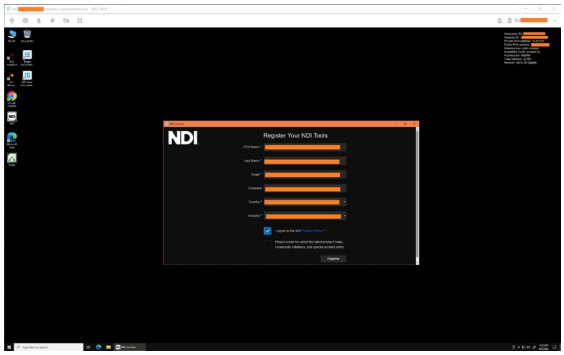


6.3 Deploy NDI Bridge

The deployment process for NDI Bridge builds upon the setup used for the NDI Discovery Server, with additional steps to pair two NDI Bridges for effective video feed contribution between local and cloud environments. Follow these steps to configure and deploy NDI Bridge effectively:

1. **Step 1: Deploy NDI Bridge**
    - **Search for NDI Bridge**: Go to AWS Marketplace and search for "NDI Bridge".
    - **Follow Deployment Instructions**: Refer to the steps outlined in the "Deploy NDI Discovery Server " section of this guide to deploy NDI Bridge similarly. Ensure you follow the same procedures for selecting the instance, configuring network settings, and setting security measures.
2. **Set the NDI Discovery Server IP**:

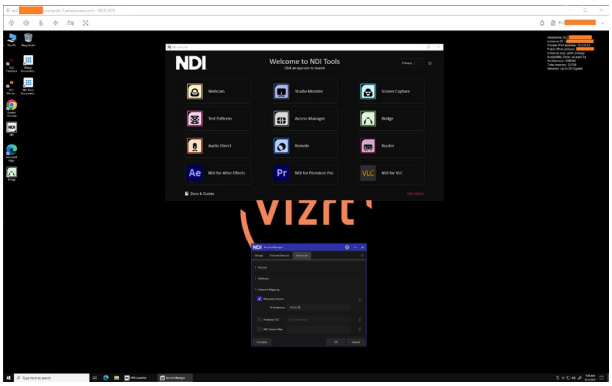
- **Register NDI Tools**: Ensure NDI Tools are registered on your system.



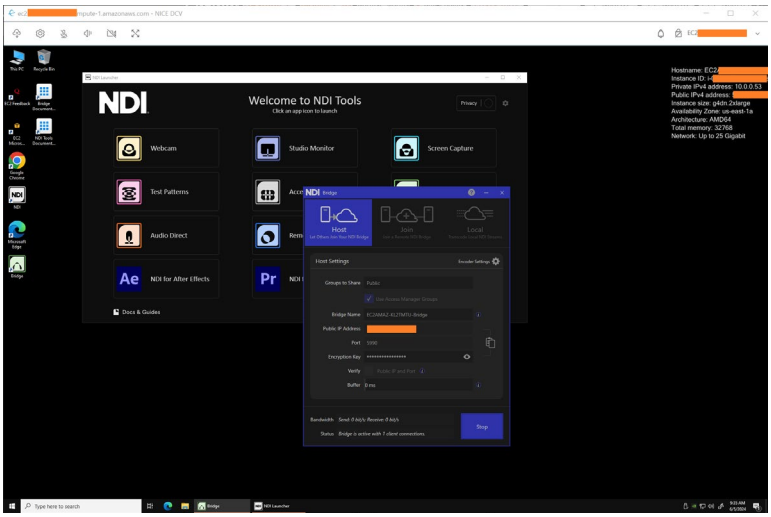
- **Configure NDI Access Manager**: Launch the NDI Access Manager and navigate to the 'Advanced' tab. Enter the **Private IP address** of your NDI Discovery Server in the 'Discovery Servers' field.

3. **Pair Two NDI Bridges**:

   - **Setup Host Bridge:** On your cloud EC2 instance, configure the NDI Bridge to operate in Host mode.
   - **Generate Encryption Key:** Create an encryption key that will be used to secure the connection between the two bridges.
   - **Record Important Information**: Document the Public IP Address and Encryption Key from the EC2 instance where the NDI Bridge is hosted; these details are essential for setting up the Join bridge.



- **Activate Host Bridge**: Start the NDI Bridge in Host mode to begin accepting connections.



- **Configure the Local NDI Bridge:** Open NDI Bridge on your local machine and set it to Join mode.
- Enter the **Public IP address** of the remote Bridge Host hosted on the EC2 instance in the Server IP Address field.
- Enter the **Encryption Key** you noted earlier and start the NDI Bridge

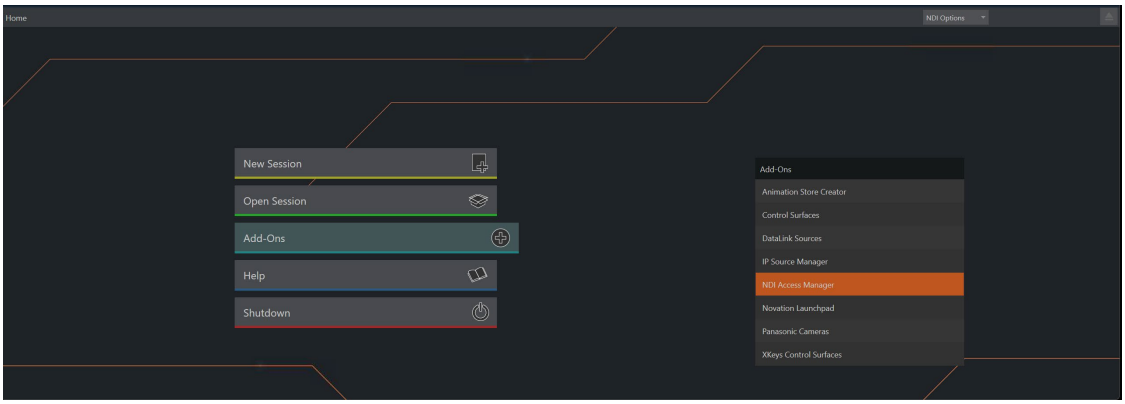
4. **Test NDI Flow**:
   - Test an NDI flow from your local machine to the cloud using the NDI Test Patterns to ensure everything is configured correctly.
5. **Additional Information**:

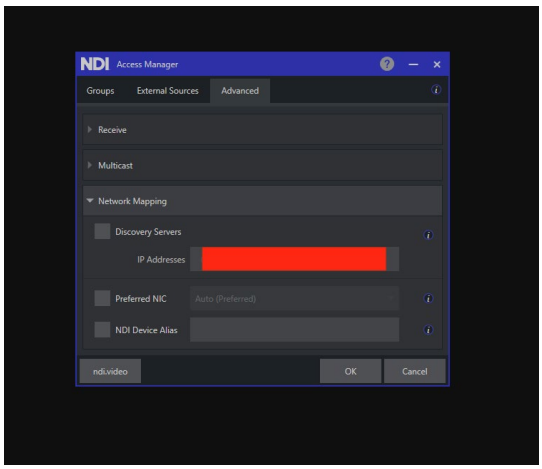
- For more detailed information and troubleshooting, refer to the NDI Bridge documentation.

6.4 Finalizing Your TriCaster Vectar

With the NDI Discovery Server and NDI Bridge in place, you can now finalize the setup of TriCaster Vectar:

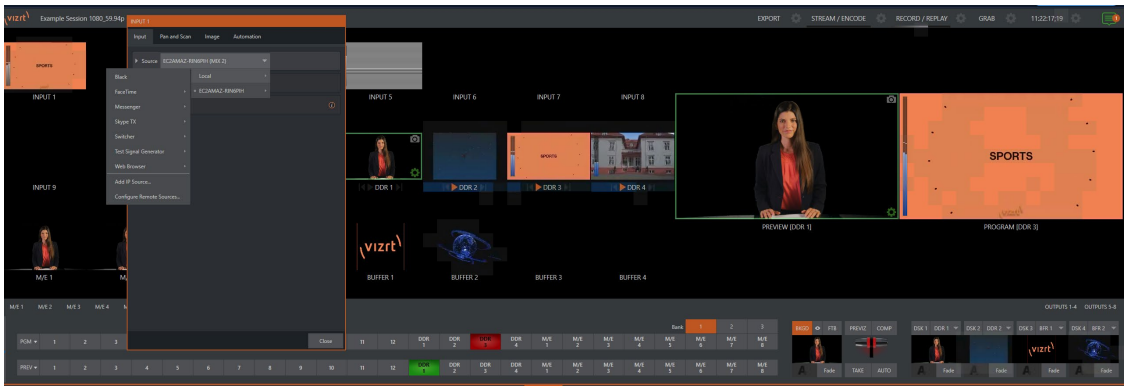
- **Configure NDI Access Manager:** On the TriCaster Vectar home page, navigate to Add-Ons and select NDI Access Manager. Enter the Private IP of your NDI Discovery Server to link it with your TriCaster Vectar.





- **Create a New Session or Use an Existing Session Template:** You can start a fresh session by following the guidelines in the "Starting a Session" section of the TriCaster Vectar User Guide, or opt to use one of the pre-configured session templates available on your system.

- **Configure Your Inputs:** To set up your video inputs, refer to the "Configure Video Inputs" section in the TriCaster Vectar User Guide. Ensure all connections and settings match your production requirements.



- **Prepare Content for Production:** Load your digital video recorders (DDR) files, buffers, effects, and graphics such as Viz Flowics Graphics. Ensure your audio mixer is configured correctly; check and unmute inputs as necessary to suit your production's audio requirements.

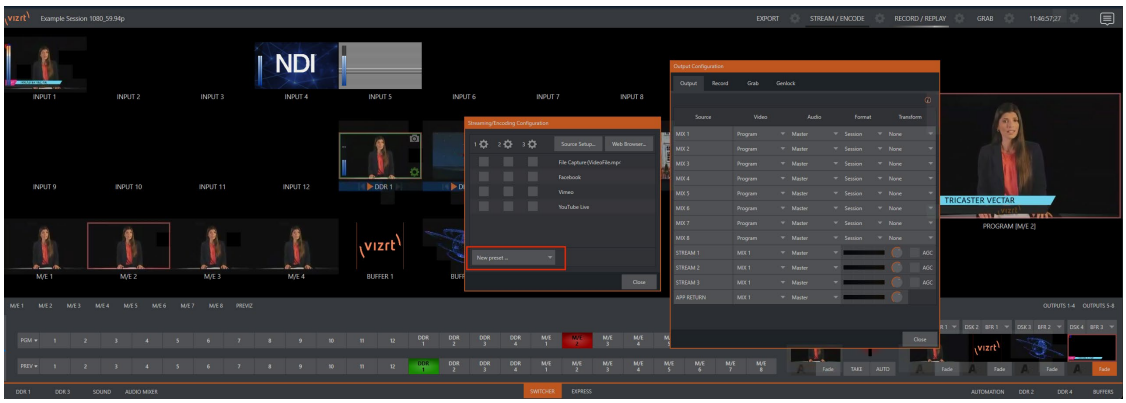
- **Configure Your Outputs:** For detailed instructions on setting up your audio and video outputs, consult the "Configure A/V Output" section in the TriCaster Vectar User Guide. Verify that output effects and graphics are functioning correctly and set up transitions such as fades to your preference.

6.5 Set Up CDN Publishing

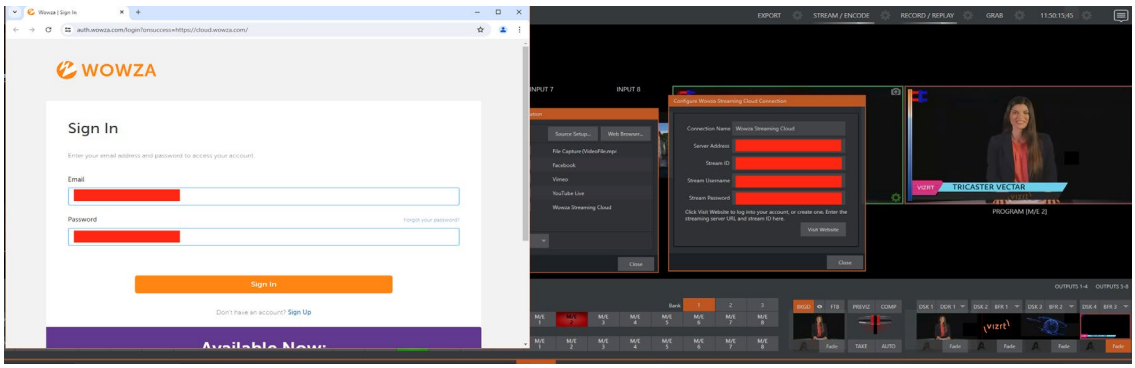
TriCaster Vectar supports various content delivery networks (CDNs) to stream your live production to a broad audience. For this setup, we'll focus on integrating with Wowza Streaming Cloud. For additional CDN configurations and use cases tailored to your production needs, consult the "Stream/Encode Live" section in the TriCaster Vectar User Guide.

Steps to Configure Wowza Streaming Cloud:

1. **Access Stream/Encode Settings:**
    - Navigate to the Stream/Encode panel in your TriCaster Vectar interface.
    - Click on the gear icon to open the settings.
2. **Create a New Preset:**
    - Click 'New Preset' to start setting up your CDN streaming options.



    - Input the CDN settings provided by your cloud provider. This includes server URLs, stream keys, and any other necessary configuration details.



3. **Configure the Encoder:**

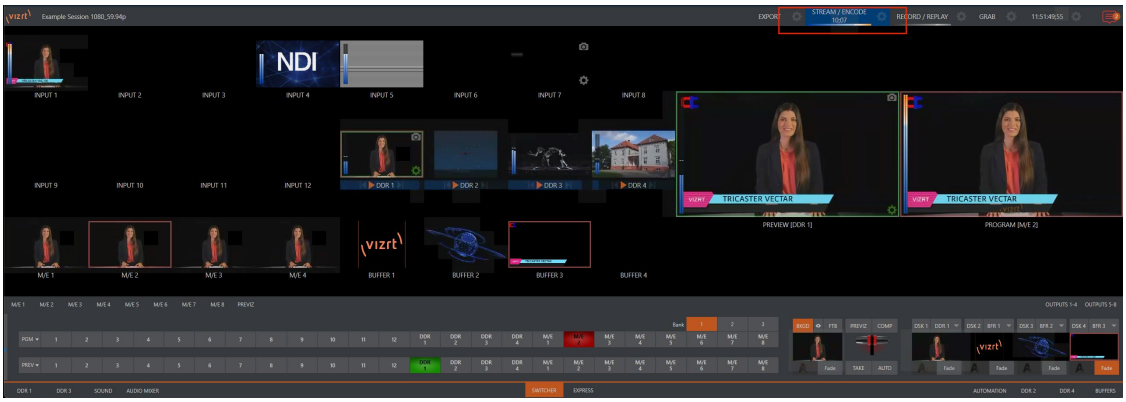
- After saving your CDN settings, click on the gear icon next to your new preset.
- Configure the encoder settings for both video and audio according to your production requirements. Ensure that the bitrate, resolution, and audio settings are optimized for the best streaming performance.
- Close the settings window.

6.6 Go Live

Now that your CDN publishing setup is complete, you are just a few clicks away from broadcasting your live production. Here's how to go live:

1. **Start Broadcasting:**
   - Navigate to the 'Stream/Encode' button on your TriCaster Vectar interface.
   - Click on 'Stream/Encode' to initiate the live stream to your chosen CDN.
2. **Enjoy Your Live Production:**
   - Monitor your stream and enjoy the process of live broadcasting. Engage with your audience and manage your production seamlessly.
3. **Post-Production Reminder:**
   - After concluding your live session, remember to stop all your AWS EC2 instances. Leaving instances running will incur ongoing charges, even if they are not actively being used.

- As a best practice, set up cost controls and alerts in AWS to manage expenses and avoid unexpected costs. This proactive measure helps keep your budget in check and ensures you only pay for the resources you need.



7 Additional Consideration

This chapter discusses additional considerations to enhance the security and functionality of your TriCaster Vectar deployment. These suggestions provide alternatives to the default settings and enhance your operational security and storage management.

Public vs. Private Subnets:

- **Default Setup:** For simplicity, the initial deployment of TriCaster Vectar is configured in a public subnet. This setup facilitates easier access and initial configuration.
- **Enhanced Security:** To significantly improve security posture, consider moving your EC2 instances into a private subnet. This reduces direct exposure to the internet and enhances your network's security. Detailed guidance on configuring private subnets for your instances can be found in the "TriCaster Vectar AWS Deployment Guide."

VPC recommendation VPC Security is a complex and crucial topic that can be daunting to tackle. We strongly recommend you check the best practices document offered by AWS (link) and cover as many of these practices when deploying our AMIs into your VPCs.

Elastic Block Store (EBS) Configuration:

- **Default Disk Setup:** By default, the EC2 instances come with two EBS volumes: a 70 GiB volume for the operating system (C drive) and a 200 GiB volume designated for media storage and recording.
- **Customization Options:** Depending on your specific storage needs, particularly if you anticipate a higher volume of media production or require longer retention periods, you may find it necessary to adjust the size of these volumes. For recommendations on sizing and configuring your EBS volumes to optimize performance and cost, please refer to the storage optimization section in the "TriCaster Vectar AWS Deployment Guide."

Customer-Managed Encryption:

- **Data at Rest**: Customers are responsible for configuring encryption on EBS volumes to secure data at rest. Amazon EBS supports encryption across all volume types, offering transparent encryption and decryption processes that do not require manual intervention. Performance metrics, such as IOPS, remain consistent between encrypted and unencrypted volumes, with minimal impact on latency. For detailed guidance, refer to Amazon EBS encryption.
- **Data in Transit**: The encryption of data in transit is also managed by the customer. This includes ensuring that any audio or video streams are securely encrypted, with

the methods varying based on the transport stream utilized. Adhering to industry best practices for the encryption of data in transit is essential for maintaining the confidentiality and integrity of broadcast content.

Monitoring

- **Enable Logging:** Enable AWS CloudWatch for logging and monitoring the instance. This will help you track usage and performance and troubleshoot any potential issues.

Bringing Additional Video Feeds into the Cloud

To enhance your live production capabilities, you may want to bring additional video feeds into the cloud to be utilized within TriCaster Vectar. While this guide focuses on using NDI for streamlined video and audio exchange, TriCaster Vectar also supports a variety of other transport streams, such as SRT, to accommodate diverse production needs.

When incorporating additional feeds, ensure you review and adjust your security group settings to allow the necessary incoming and outgoing traffic, as detailed in the "TriCaster Vectar AWS Deployment Guide." For guidance on configuring these feeds within your TriCaster Vectar video switcher, refer to the "TriCaster Vectar User Guide." This flexibility allows you to tailor your setup to meet the specific demands of your production environment, ensuring a robust and versatile live production setup in the cloud.

8 Additional Resources

For those new to AWS or needing a refresher, consider the following resources to get up to speed:

- AWS Training and Certification: Offers courses to enhance your understanding of AWS services.
- AWS Documentation: Provides comprehensive guides and tutorials on using AWS services.

For those looking to deepen their knowledge and skills in operating TriCaster® Vectar and other related technologies, the following resources are invaluable:

- **Vizrt Documentation and User Manuals:** Comprehensive product documentation for TriCaster® Vectar is available at TriCaster Vectar User Guide. This includes user manuals that detail common operations, deeper reference sections, and step-by-step guides for various functionalities.
- **Self-Service Knowledge Base:** For additional support and troubleshooting, visit our Self-Service Knowledge Base at Vizrt Support Portal.
- **Viz University:** Enhance your expertise by signing up at Viz University as a freelancer or media professional. Viz University offers a range of courses specifically tailored to mastering TriCaster and live production techniques. Courses related to TriCaster are available, helping you become proficient in utilizing this powerful tool for live broadcasting.
- **Vizrt Official YouTube Channel:** For visual learners, the Vizrt Official YouTube Channel provides a wealth of tutorial videos. These tutorials cover various aspects of setup, operation, and creative uses of Vizrt products, offering practical insights and tips.
- Join the conversation at the **Vizrt Community forum**: https://forum.vizrt.com/
- **NDI Documentation and Setup Help:** For more detailed information and advanced configurations, visit the official NDI documentation at NDI Tools Documentation (https://docs.ndi.video/tools).

This guide assumes a basic level of familiarity with AWS. If you find any of the steps challenging, referring to the detailed **TriCaster® Vectar AWS Deployment Guide** or AWS's official documentation may provide additional clarity and guidance.

Expand Your Skills with Viz University Courses

To help you maximize your TriCaster Vectar experience, Viz University offers a selection of free courses that delve into various aspects of operating TriCaster systems. These courses are designed to enhance your knowledge and skills, whether you're new to vision mixing or looking to master more advanced features.

1. **Introduction to Vision Mixing with TriCaster**: Gain foundational knowledge on vision mixing and learn the basics of video switching, media playback, audio mixing, and output configuration using TriCaster. This course starts with the computer interface and extends to control panel operations. Enroll Here
2. **Advanced Vision Mixing with TriCaster**: Explore the advanced capabilities of TriCaster, including M/E operation, chroma keying, macros, automation, and more. The course covers both the user interface and control panel operations. Enroll Here
3. **TriCaster Production Graphics**: Understand the crucial role of graphics in live production. This course covers creating titles, transitions, animated logos, and virtual sets, providing practical examples and focusing on various graphics workflows within TriCaster. Enroll Here
4. **Live Story Creator In-Depth**: Discover how to produce scripted shows efficiently using TriCaster's Live Story Creator. Learn to set up a teleprompter, control it from various devices, and automate production elements directly from a Microsoft Word script. Enroll Here
5. **NDI and Performance Media Networking Class**: Master the essentials of video over IP networking, tailored for the high-performance requirements of live production. This course covers everything from network hardware to detailed insights into NDI protocol operations, organization, and troubleshooting. Enroll Here

These courses are designed to be accessible for users at different skill levels and provide a structured learning path to enhance your live production capabilities with TriCaster Vectar.

9 Purchasing a License

If you are ready to purchase a license for TriCaster® Vectar to unlock its complete capabilities without a watermark, we encourage you to contact a Vizrt Certified reseller or Vizrt sales representative. Our licensing solutions are designed to cater to various operational sizes and specific production needs.

Contact a Certified Reseller: To explore the licensing options that best fit your requirements, please visit our reseller locator here (https://www.vizrt.com/reseller-locator). Our global network of certified partners is equipped to provide you with detailed information, including pricing, features, and current promotions, ensuring you receive tailored advice for your setup.

Why Purchase a License? Acquiring a license grants you access to the full, watermark-free version of TriCaster® Vectar, along with regular updates and dedicated support. This investment not only enhances your production quality but also ensures you are equipped with the latest technology to maximize your live production's impact and efficiency.

10 Support

While the free version of TriCaster Vectar on AWS Marketplace does not include full access to our support services, users can still take advantage of a variety of resources to ensure they are effectively utilizing the product. Here's what's available to help you maximize your use of TriCaster Vectar:

1. **Self-Service Knowledge Base**: Access our comprehensive knowledge base at Vizrt Self Service Knowledge Base for troubleshooting, tips, and detailed guidance on common queries and technical challenges.
2. **Viz University**: Benefit from a limited selection of courses and tutorials at Viz University, designed to enhance your skills and understanding of live production processes.
3. **Vizrt Community Forum**: Join the community at the Vizrt Community Forum to connect with other users, share experiences, and get answers from the broader Vizrt user base.

These resources are designed to provide you with the tools and knowledge needed to resolve issues and improve your live production capabilities, ensuring you get the most out of your TriCaster Vectar experience, even without a full support package.

Additionally, it's important to note that the two additional AMIs featuring NDI technology are not provided by NDI and are not included in any support level provided by NDI.

11 Appendices

11.1 Best Practice for VPC Design

When choosing a CIDR block for an Amazon VPC that will host about 5 to 6 EC2 instances, you want to consider both immediate needs and potential future growth. It's always a good idea to design your network to accommodate more resources than you currently anticipate needing, to allow for scalability and the addition of other services or instances without requiring major changes later.

Recommended CIDR Range

For a VPC intended to host 5 to 6 EC2 instances, a good starting point could be a /28 or /27 subnet within your VPC. Here's why:

- **/28 Subnet:**
    - Offers 16 IP addresses (14 usable, as AWS reserves the first 4 and the last address in each subnet).
    - Suitable for very small, tightly controlled deployments but offers little room for expansion.
- **/27 Subnet:**
    - Provides 32 IP addresses (30 usable).
    - Offers more flexibility and space for adding additional instances or services.
- **/24 Subnet:**
    - Provides 256 IP addresses (251 usable after AWS reservations).
    - This is a more commonly recommended size for a small VPC, as it provides ample room for future expansion without being overly large.

Considerations for VPC and Subnet Planning

- **IP Address Utilization**: AWS reserves the first four IP addresses and the last IP address in every subnet for its own use. These addresses are used for networking services such as the VPC router, DNS, future AWS services, and for broadcast addressing in the subnet.
- **Future Growth**: Even if you only plan for 5 to 6 instances now, consider potential future needs for additional instances, auxiliary services, or other AWS resources like RDS databases, ELB load balancers, and more.

- **Network Segmentation**: If you anticipate different types of resources or applications, consider creating multiple subnets for different purposes, such as public-facing web servers in one subnet and backend databases in another. This enhances security and traffic management.
- **VPC Size**: While you can choose a smaller subnet for immediate needs, the overall VPC CIDR block should be larger to accommodate potential subnet additions. A common practice is to start with a larger CIDR block for the VPC (e.g., /16 or /20) and carve out smaller subnets as needed.

11.2 Best Practice for Subnet Design

When configuring public and private subnets within a VPC using a **/24** CIDR block (such as **10.0.0.0/24**), it's crucial to design the network to optimize both functionality and security. The **/24** CIDR block provides up to 256 IP addresses, which, after AWS reserves certain addresses, leaves you with approximately 251 usable IPs. Here are some best practices and a proposed configuration:

Best Practices for Subnet Design:

1. **Separation of Concerns:** Divide your resources between public and private subnets based on their exposure needs and roles within your architecture.
    - **Public Subnet:** Hosts resources that need to be accessible from the internet, like public web servers, load balancers, etc.
    - **Private Subnet:** Hosts resources that should not be directly accessible from the internet, like databases, application servers, etc.
2. **Security:** Utilize Network Access Control Lists (NACLs) and security groups to tightly control inbound and outbound traffic. Public subnets typically have more permissive rules to allow web traffic, whereas private subnets have restrictive rules to block unnecessary access.
3. **Size Appropriately:** Allocate IP ranges keeping future scalability in mind. Avoid making your subnets too small, as resizing them later can be complex.
4. **Reserve Space for Expansion:** Even within a limited address space, it's wise to plan for growth either by reserving additional subnet space or ensuring subnet sizes can accommodate additional resources without reconfiguration.

Example Configuration:

Assuming a base CIDR block of **10.0.0.0/24**, you might divide this block into smaller subnets:

Public Subnet:

- **CIDR: 10.0.0.0/26**
- **Usable IP Range: 10.0.0.1** to **10.0.0.62** (61 usable IPs)
- **Purpose:** This subnet can be used for placing your NAT gateway, internet-facing load balancers, and public web servers. The size allows for scalability and the addition of more public resources if needed.

Private Subnet:

- **CIDR: 10.0.0.64/26**
- **Usable IP Range: 10.0.0.65** to **10.0.0.126** (61 usable IPs)
- **Purpose:** This subnet is ideal for backend servers, application servers, and databases that do not require direct internet access but can communicate with the public subnet.

Reserved for Future Use:

- **CIDR 1: 10.0.0.128/26**
- **CIDR 2: 10.0.0.192/26**
- These blocks can be reserved for future expansion, additional isolated environments, or specific services that may need segregated networks.

Network Infrastructure:

- **NAT Gateway:** Place a NAT Gateway in the public subnet to enable instances in the private subnet to access the internet for updates, while still blocking incoming traffic from the outside.
- **Internet Gateway:** Attach an Internet Gateway to the VPC and route it through the public subnet for outbound and inbound internet traffic.
- **Route Tables:** Create distinct route tables for public and private subnets. The public subnet's route table should direct traffic to the Internet Gateway, while the private subnet's route table should point to the NAT Gateway for outbound traffic.

Additional Considerations:

- **Elastic IP:** Assign an Elastic IP to your NAT Gateway for a stable outbound IP.
- **Backup and Recovery:** Plan for backup and disaster recovery scenarios by perhaps using additional regions or reserved IPs for critical services.

This structure ensures that your network is not only secure and functional but also scalable and adaptable to changing needs.