Viz Now Administrator Guide

Version 2.0

Viz Now

Disclaimer

Vizrt provides this publication “as is” without warranty of any kind, either expressed or implied. This publication may contain technical inaccuracies or typographical errors. While every precaution has been taken in the preparation of this document to ensure that it contains accurate and up-to-date information, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained in this document.

Vizrt’s policy is one of continual development, so the content of this document is periodically subject to be modified without notice. These changes will be incorporated in new editions of the publication. Vizrt may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time. Vizrt may have patents or pending patent applications covering subject matters in this document. The furnishing of this document does not give you any license to these patents.

Antivirus Considerations

Vizrt advises customers to use an AV solution that allows for custom exclusions and granular performance tuning to prevent unnecessary interference with our products. If interference is encountered:

- **Real-Time Scanning:** Keep it enabled, but exclude any performance-sensitive operations involving Vizrt-specific folders, files, and processes. For example:
  - C:\Program Files\[Product Name]
  - C:\ProgramData\[Product Name]
  - Any custom directory where [Product Name] stores data, and any specific process related to [Product Name].
- **Risk Acknowledgment:** Excluding certain folders/processes may improve performance, but also create an attack vector.
- **Scan Scheduling:** Run full system scans during off-peak hours.
- **False Positives:** If behavior-based detection flags a false positive, mark that executable as a trusted application.

Technical Support

For technical support and the latest news of upgrades, documentation, and related products, visit the Vizrt web site at www.vizrt.com.

Created on

2025/11/14

Contents

1 Users

1.1 Working with Users

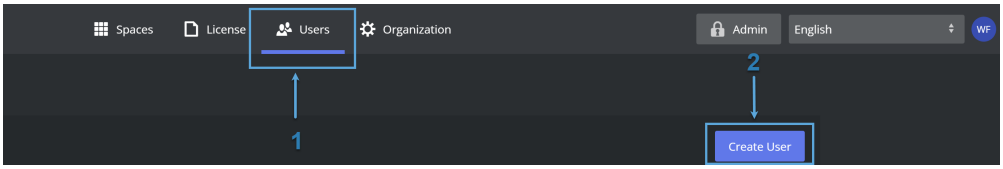
Only admins can create, delete, and assign privileges to users. This page describes:

- Creating a New User
- Managing Users
- User Privileges

1.1.1 Creating a New User

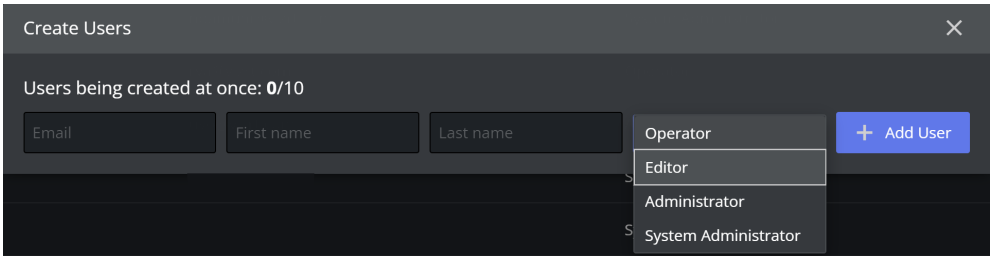
To Create New Users in Your Organization

1. Navigate to the **Users** tab in the top menu.
2. Click **Create User**.



3. Fill out the form with the new user's email, first and last name, and assign their privileges (see User Privileges below).

> **Note:** Up to ten users can be added at a time.



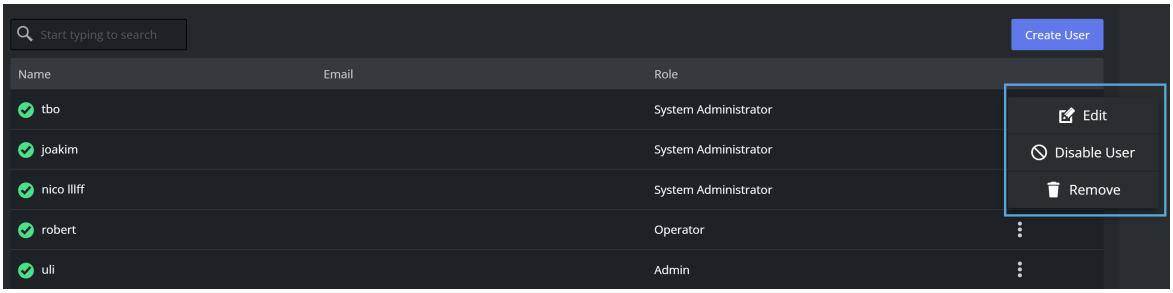
4. Click **Confirm** to finish creating the new user(s).

1.1.2 Managing Users

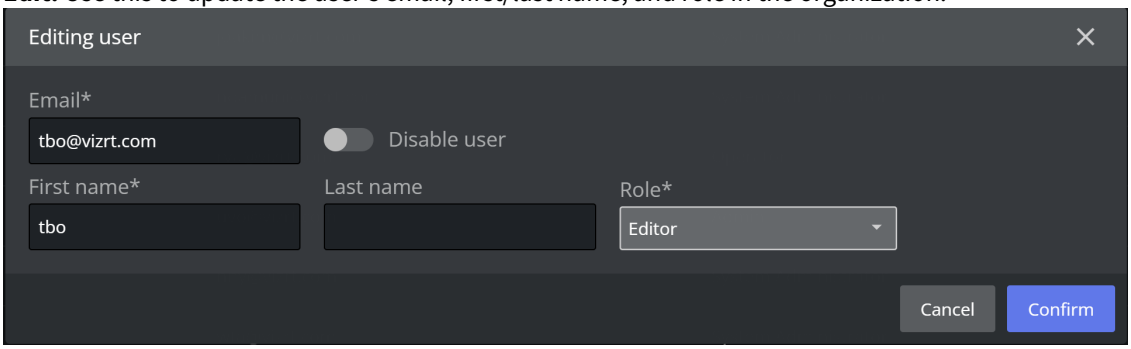
All users in the organization are displayed in the **Users** tab.

To Manage a Single User

1. Click on the three dots to the right of their name to see a list of options.



a. **Edit:** Use this to update the user's email, first/last name, and role in the organization.



You can also disable the user by turning on the **Disable User** toggle.

b. **Disable User:** Use this to prevent the user from accessing the organization, whilst retaining their details.
c. **Remove:** Use this to remove the user from the organization and delete their information.

1.1.3 User Privileges

There are three different user roles within an Organization:

- **Admin:** Full edit and access privileges for all spaces, and can configure the organization, manage users, change credentials, and assign roles.
- **Editor:** Create, deploy, and destroy spaces, and can only view spaces that they have created themselves or been assigned to. Ability to start and stop spaces, add themselves to the whitelist, and access apps.
- **Operator:** Access spaces that have been assigned to them and retrieve login information for apps within those spaces.

Summary of User Privileges

Privilege	Admin	Editor	Operator
Access a deployed space that they are assigned to	✅	✅	✅
Start and stop a space they own or are assigned to	✅	✅	✅
Start any space within their organization	✅	⛔	⛔

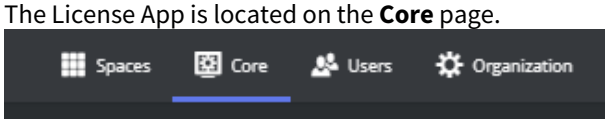
Privilege	Admin	Editor	Operator
Access any space not within their organization	⛔	⛔	⛔
Create a new space	✅	✅	⛔
Deploy a space they own or are assigned to	✅	✅	⛔
Deploy any space within their organization	✅	⛔	⛔
Deploy any space	⛔	⛔	⛔
Destroy a space they own or are assigned to	✅	✅	⛔
Destroy any space within their organization	✅	⛔	⛔
Destroy any space not within their organization	⛔	⛔	⛔
Delete a space they are assigned to	✅	⛔	⛔
Delete any space not within their organization	⛔	⛔	⛔
Assign users to a space they own	✅	✅	⛔
Assign users to any space within the organization	✅	⛔	⛔
Assign users to any space not within their organization	⛔	⛔	⛔
Whitelist themselves to any space they have access to	✅	✅	✅
Edit the whitelist on any space they have access to	✅	✅	✅
Add new users to the organization and assign roles	✅	⛔	⛔
Create new organizations	⛔	⛔	⛔
Invite other users to a space	✅	✅	⛔

2 Licenses

2.1 Working with Licenses

2.1.1 The Core Page

The License App is located on the **Core** page.



From here you can manage all Vizrt product licenses.

Tip: Refer to the *Vizrt Licensing Administrator Guide* for further details.

To Access the License App

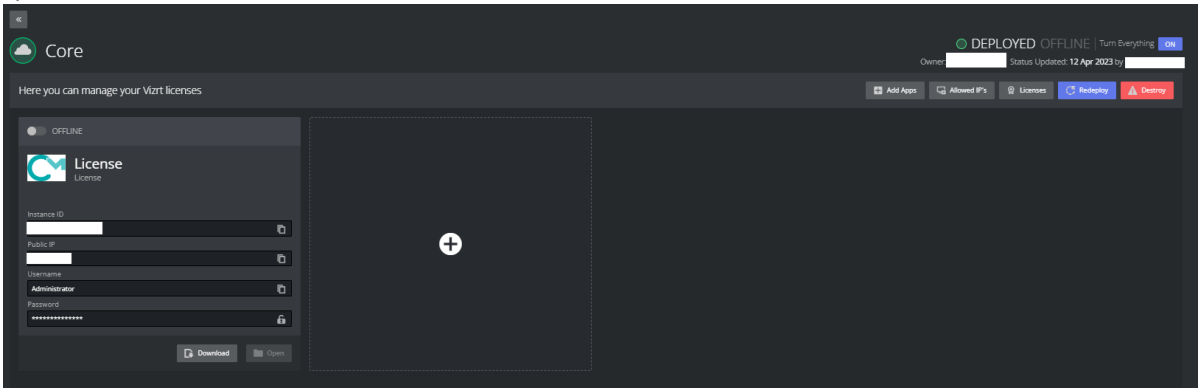
- Ensure that the License App is turned on and simply access it like any other App.

Note: Only the Organization Administrator has the privilege to access licenses.

Licenses are required for all Vizrt products, however, for third-party products, different license systems may be utilized. Please refer to the documentation for those specific products for more detailed information.

To Access Licenses within Any Other Space

- The License App must be running.
  It serves as the central hub for managing all Vizrt product licenses and needs to be accessible to other spaces in order for them to access the licenses



To View Available Licenses

- Click on the **Licenses** button on the **Core Space** menu. The right side list shows available licenses (if any) with its Container ID.

2.1.2 SSL Certificate Validation

If the certificate has expired, a warning message is displayed.

- Click the button to renew it. This process takes a few minutes.

2.1.3 Accessing the License Server

To Access the License Server

1. Download the DCV link. If your IP address is not on the list of allowed IPs, it is added to the list when you click the **Download** or **Open** button.
2. Only users with IP addresses on the allowed list are able to access the license virtual machine.

2.1.4 Destroying the License Server

Warning: You should avoid destroying the License server unless instructed to do so by Vizrt Support.

If you destroy the License server:

- All licenses are lost and you need to go through the onboarding process for your organization again and deploy a new License server.
- All existing spaces lose their connection to the License server and need to be removed.

2.1.5 Redeploying the License Server

- In rare cases, you may be asked to redeploy the License server to update critical changes.

3 Introduction

This document provides detailed guidance on how to configure and operate Viz Now as an Organization Administrator. As an Organization Administrator, you have access to advanced features and controls that allow you to manage and customize Viz Now to suit the specific needs of your organization. By following the instructions in this guide, you can optimize your use of Viz Now and ensure that your cloud production workflows are deployed and configured efficiently and effectively.

3.1 Related Documents

Visit the Vizrt Documentation Center for documentation for related products, including:

- Viz Vectar Plus
- Media Service
- Graphic Hub
- Viz Trio
- Media Sequencer
- Viz Engine
- Pilot Data Server*
- Viz Libero*
- Viz Arena*

Note: Documentation marked * is available to customers with a valid Support Agreement, from Vizrt Support. Please contact your Account Manager.

3.2 Quick Start

3.2.1 Getting Started

Starting a Session

You need access to an authenticator app like MS Authenticator or Google Authenticator on your phone.

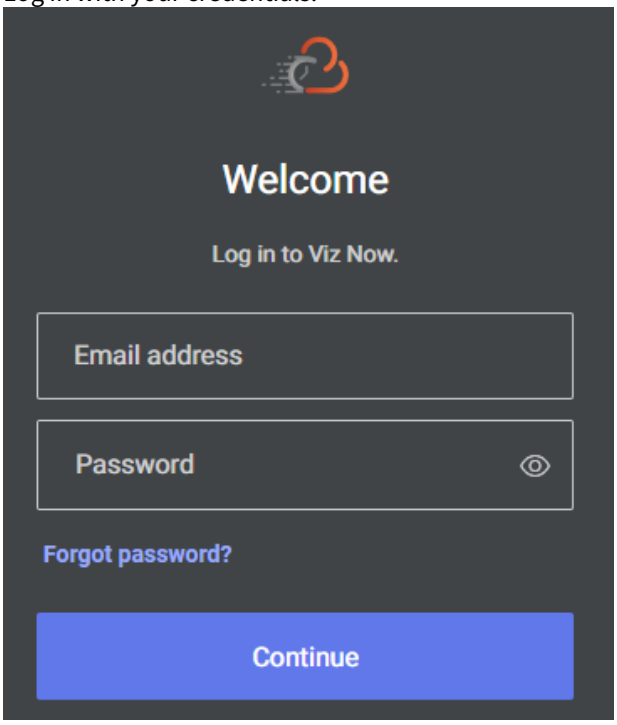
To Obtain an Authenticator App

- **For Android:** *https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en_US&gl=US*
- **For iOS:** *https://apps.apple.com/us/app/microsoft-authenticator/id983156458*

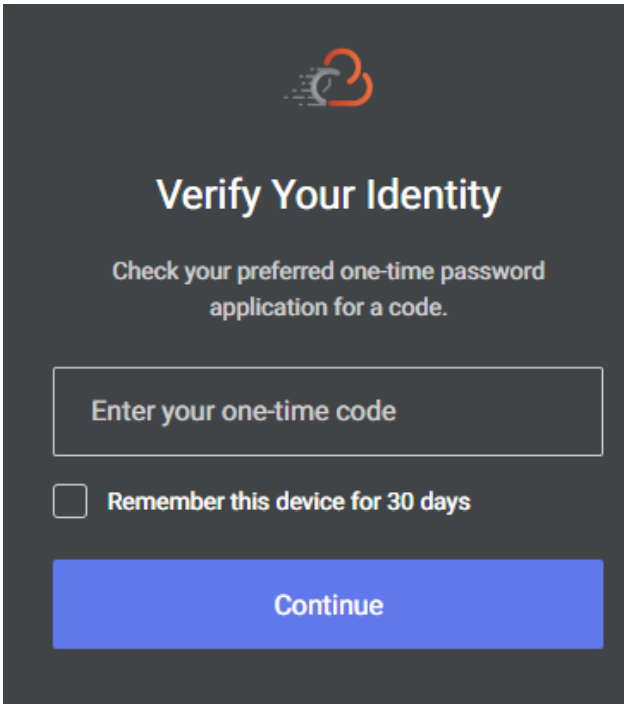
To Start a Session

Viz Now runs in a standard web browser.

1. Type the Viz Now address *https://now.vizrt.com/*. A log in menu appears.
2. Log in with your credentials.



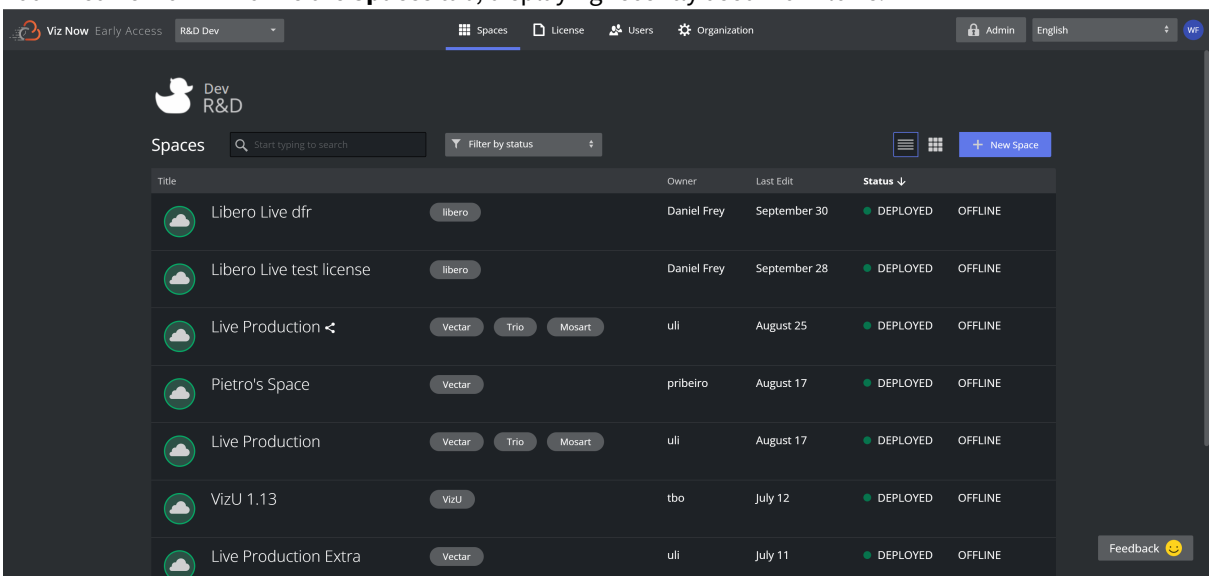
3. Sign in with the Authenticator app and provide the OTP (One Time Password).



Note: For security reasons, your session times out and automatically closes when inactive for a prolonged period, after which you need to log in again.

Home Screen

- Your first view of Viz Now is the **Spaces** tab, displaying recently used workflows.



- Select the required workflow.

To Access Your Apps

- To log into your deployed apps in a workflow, first install the remote desktop client, Amazon DCV client: Amazon DCV > Download.

For further details see section Remote Access to Deployed Viz Now Apps.

See Also

- Organizations
- Templates
- Users
- Licenses
- Spaces

3.3 Onboarding

3.3.1 Introduction to Onboarding

This section provides an overview to the onboarding process and clarifies the terms used.

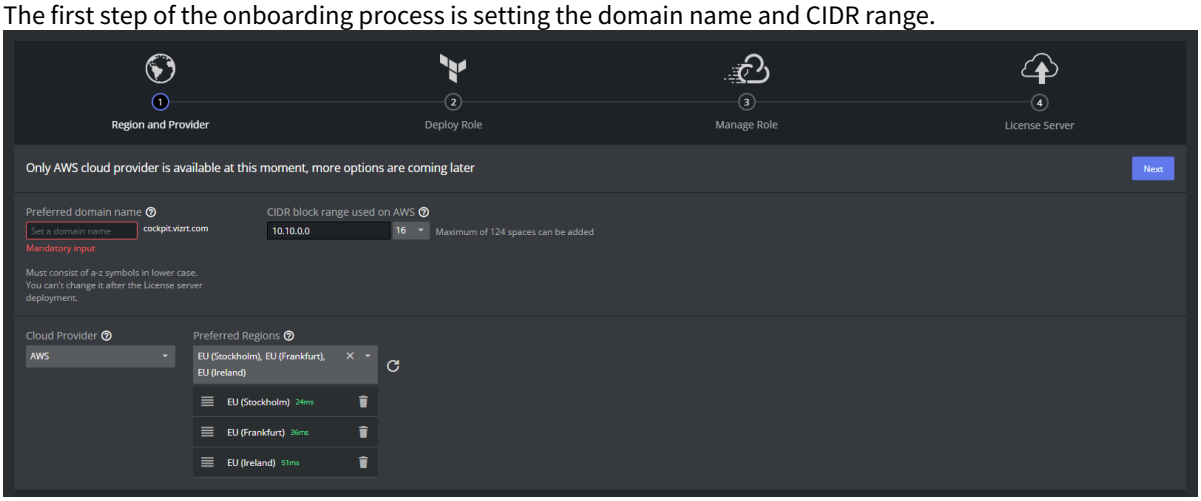
- Region and Provider
- Deploy Role and Manage Role

Once a new organization is set up and an organization admin assigned, the new admin has to go through the onboarding process to set up the Viz Now account.

- Vizrt Support does not have login access to the target AWS account, the user needs to perform this action.
- During onboarding, Viz Now is granted access to the target account using IAM roles that it is allowed to assume. This enables Viz Now to deploy infrastructure on the AWS account.
- These steps are described in detail in the UI and it should be possible for most users with the necessary AWS privileges to complete this. If issues or problems occur during onboarding, please contact Vizrt Support.

Region and Provider

1. The first step of the onboarding process is setting the domain name and CIDR range.



2. Use only lowercase letters a-z and avoid using any special characters.
3. The domain name is used to automatically issue domain certificates for apps within your organization.
4. The CIDR range should be specified using CIDR block notation.

> **Info:** What is CIDR? - CIDR Blocks and Notation Explained - AWS (amazon.com)

5. Viz Now selects unique IP addresses within this range when deploying.
6. You need to select the *regions* where Viz Now should deploy its content.
    a. Viz Now deploys spaces on your AWS account to any of the selected regions, depending on the availability of the necessary instance types.
    b. You can order the regions by preference, with the topmost region being the first choice.
    c. With the **Refresh** button, you can automatically select the three closest regions.

Deploy Role and Manage Role

The AWS integration for Viz Now allows it to assume an IAM role in your AWS account and generate temporary credentials to perform tasks such as installing and configuring a new space.

The Deployment agent is used by a third party tool and you should not need to refer to its documentation, as everything is handled by Viz Now. It performs tasks like:

- Creating infrastructure using VPC and EC2.
- Configuring domain routes using Route53.
- Creating S3 buckets with associated IAM users.
- Creating NACLs and Security Groups.
- Creating Cloudwatch log groups used by VPCs

The Manage role is used by Viz Now to simplify deployments on your behalf. The AWS integration for Viz Now allows it to perform tasks like:

- Increasing the quota.
- Reserving EC2 instance types.
- Managing S3 buckets and security groups.
- Creating and accepting VPC peerings.
- Starting and stopping EC2 instances, and destroying EC2 instances.

To Set up the Integration

The deployment Agent needs to assume an IAM role in your organization's AWS account.

1. Make sure you have an AWS account set up and are logged in as a user with the necessary AWS rights.
2. You need to create this role in the AWS Console and provide Viz Now with the necessary information. The roles needs privileges to manage iam, s3, kms, route53, sts, ec2, tag, and logs. The policy needed can be found as part of the guide on the site.

> ⚠ **Note:** If this role requirement conflicts with your company policy, contact Vizrt Support for advice on how to proceed with more granular AWS policies.

3. Follow the steps in the Viz Now onboarding UI and click the link to create a new IAM roles in your AWS account.
4. Once the roles are created, copy the ARN code and paste it into the Viz Now form to enable Viz Now to deploy instances in your environment.

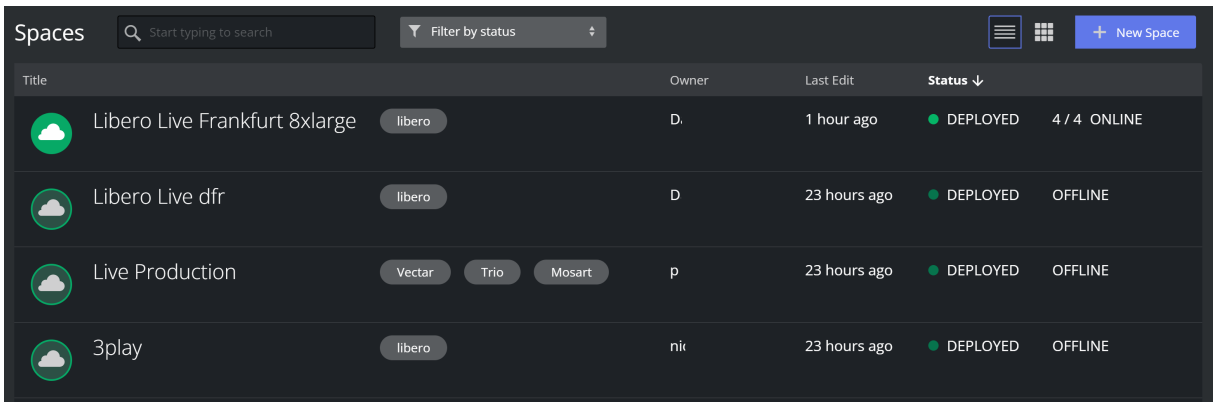
Licensing

The final step of the onboarding process involves deploying a License server. Once this is successful, your Viz Now account is ready for use.

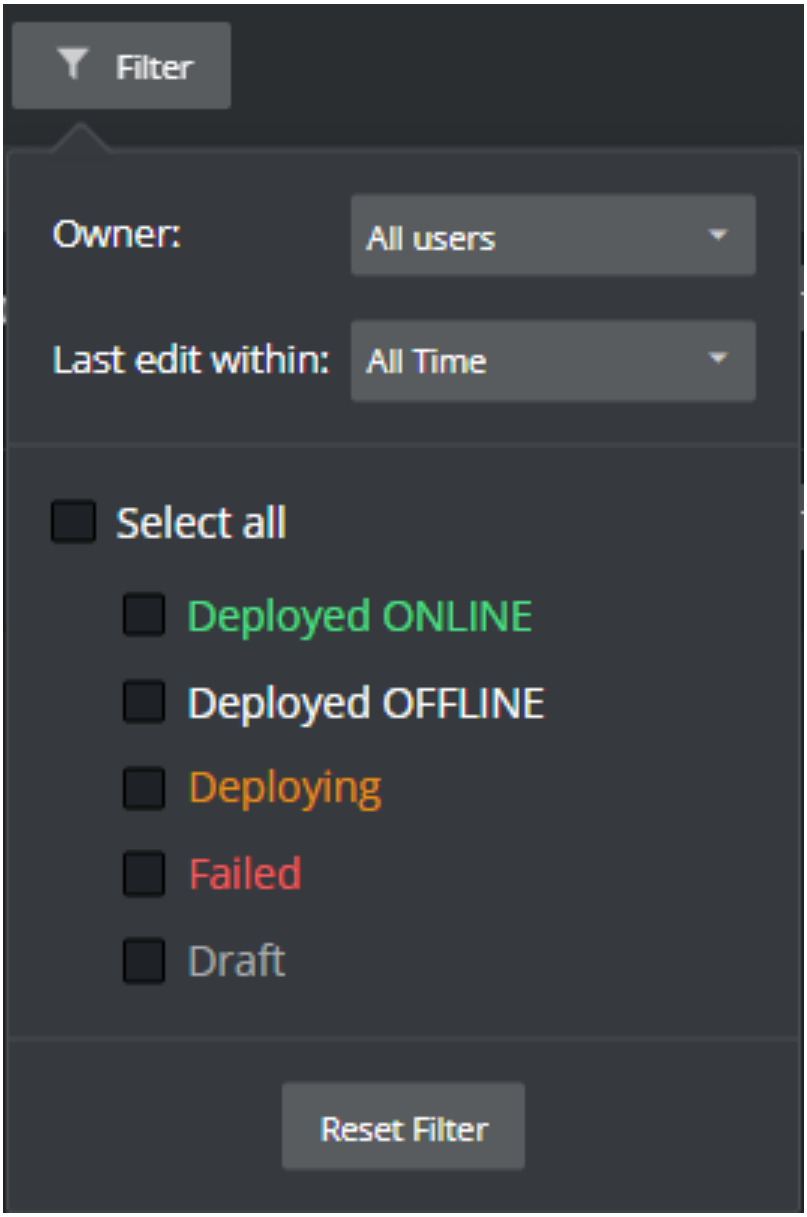
4 Spaces

4.1 Spaces

All spaces created in the organization are listed under the **Spaces** tab. Each space has details such as the title, list of available apps, owner, last edit and status.



- To find a space, use the search box on the left by typing the name of the space title or its owner.
- Use the **Filter** menu to filter the search results by status.



4.1.1 Space Status

The space status is displayed together with an icon.

Icon	Status
	Deployed Online Space.
	Deployed Offline Space.

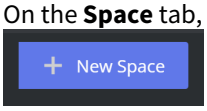
Icon	Status
	Validating (Space is deploying).
	Validating failed or Deployment failed.
	A draft space.

4.1.2 Managing a New Space

Only Users with the *editor* and/or *admin* roles (assigned by the admin) are allowed to create and deploy new space templates.

To Create a New Space Template

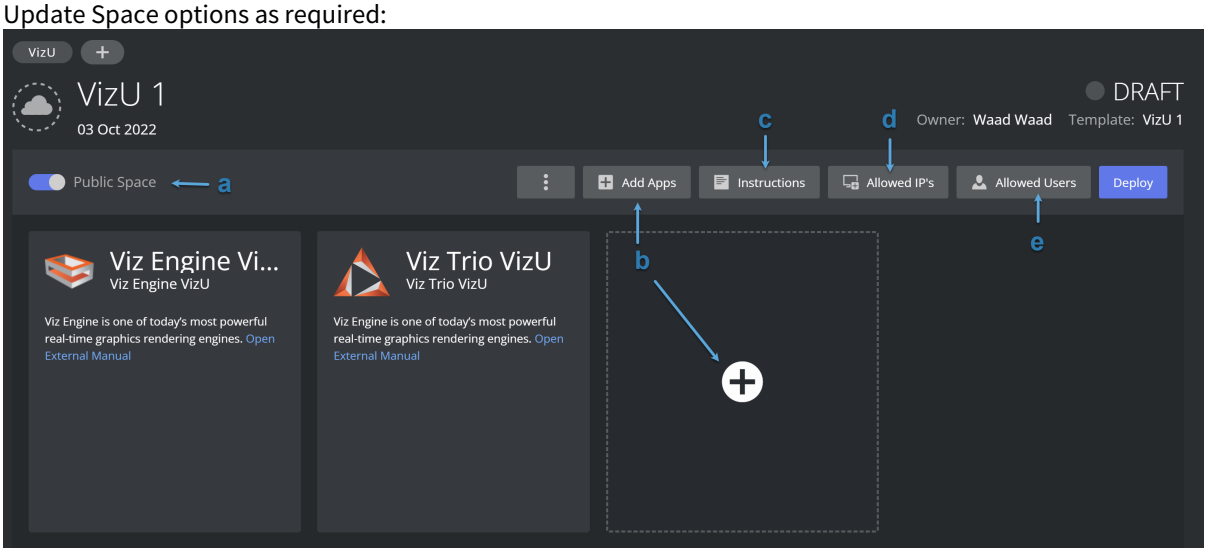
1. On the **Space** tab, click on the **+ New Space** button to the right.



A list of all available Templates is displayed. Each template belongs to a different package (Essential or Premium) and has a set of Vizrt products.

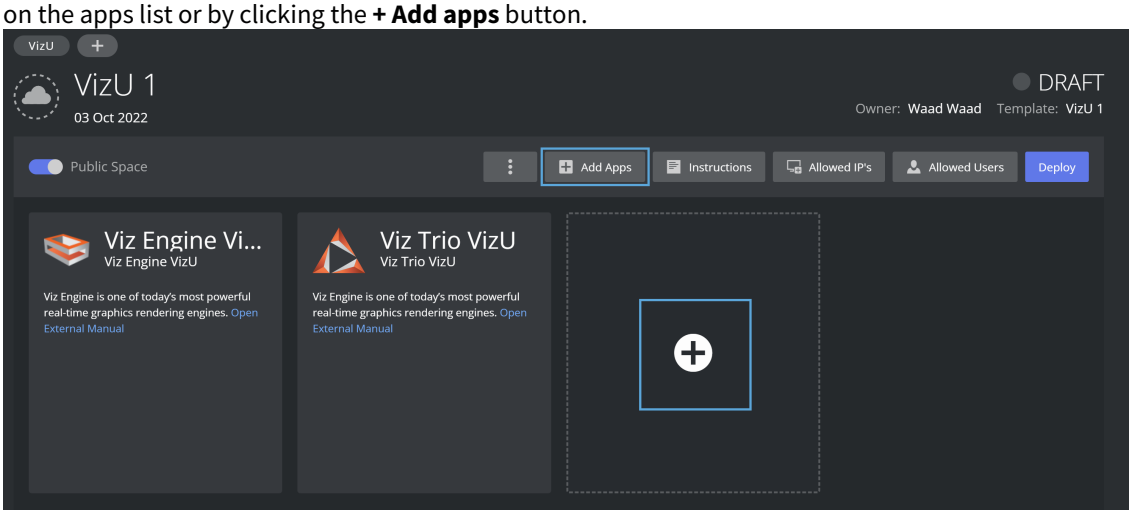
> **Note:** The list of templates may vary between Organizations. Some templates are only available for certain organizations.

2. Click on the template you want to deploy or search for it by typing the template name in the Search box on the right.
3. Update Space options as required:

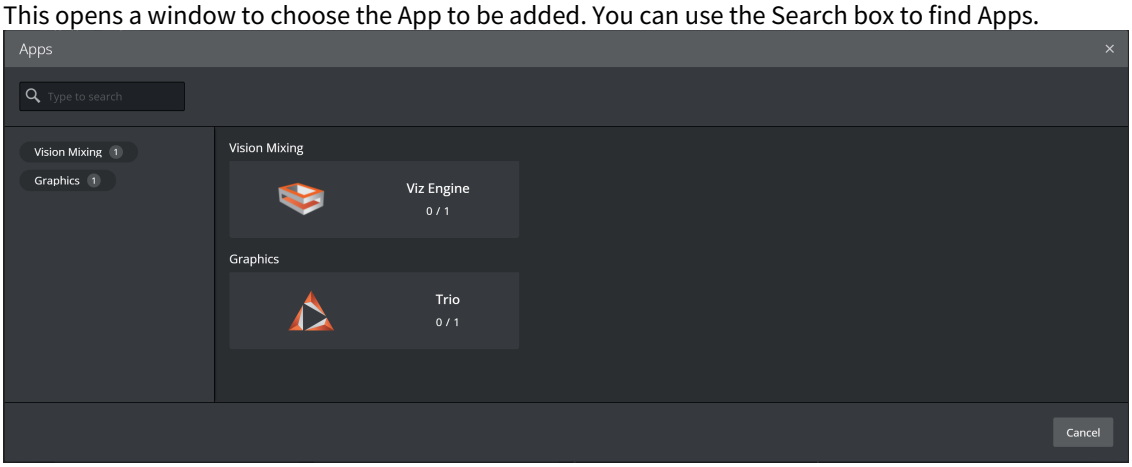


a. **Space visibility:** You can make the space template public (visible to all in the organization) by turning on the **Public Space** toggle under the template's name (Default *off* - only visible to assigned users and admin).

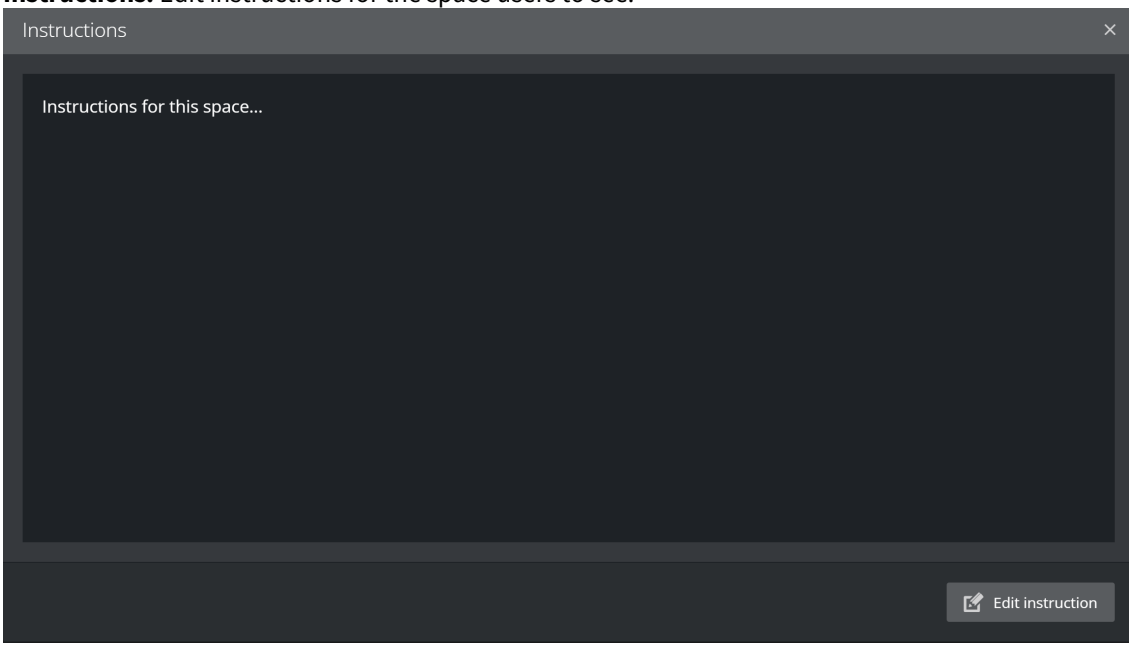
b. **Add Apps:** You can add more apps to the predefined apps in the template by either clicking the **+** sign on the apps list or by clicking the **+ Add apps** button.



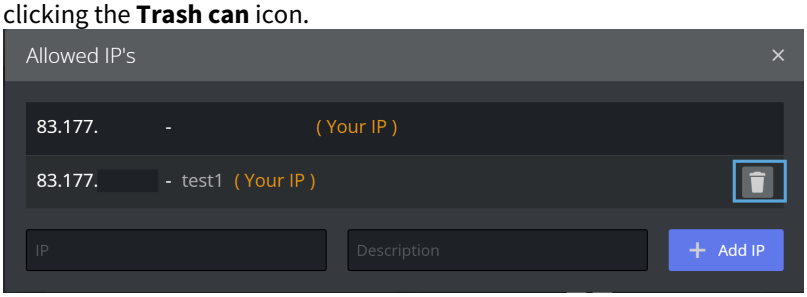
This opens a window to choose the App to be added. You can use the Search box to find Apps.



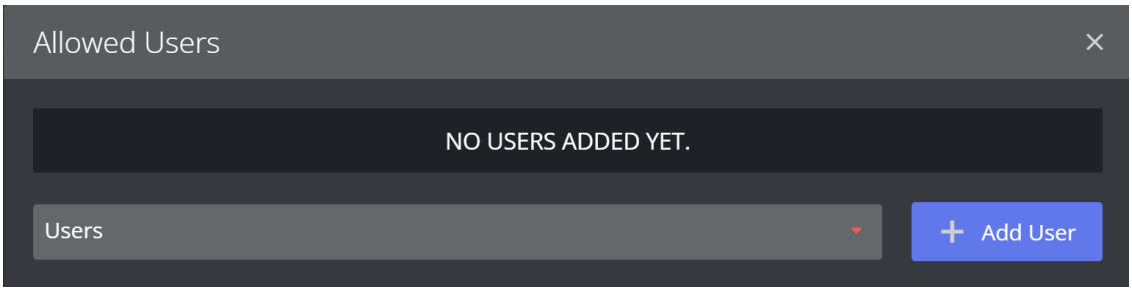
c. **Instructions:** Edit instructions for the space users to see.



d. **Allowed IP's:** You can a list of allowed IPs to access this space. You can *remove* an IP from the list by clicking the **Trash can** icon.

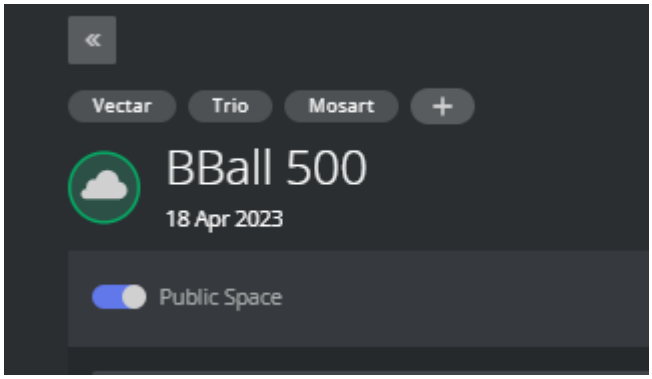


e. **Allowed Users:** Add users from the organization to access and use the space. Click on the dropdown list of users to add a new user.
To remove a user click the **Trash can** icon.



Note: Your IP is automatically added when you click the **Download** or **Open** button (to access any App within the Space).

Public Space: Click the switch to toggle between sharing the Space with anyone within the organization, or restricting access to only Admin, Owner and assigned Users.



4.1.3 Deploying a Space

To Deploy a Space

- To start deploying the Space to your AWS Account, click **Deploy**.

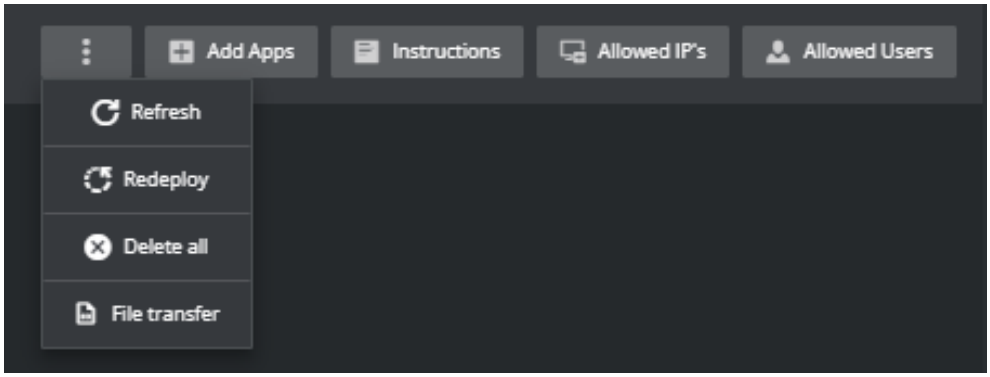
Note: This action cannot be canceled and takes approximately 10 minutes.

4.1.4 Deleting Apps and Resources

To Delete Apps and Resources

- To delete all the Apps and deployed resources, select **Delete All** from the menu.

> **Note**: This action is irreversible and permanently removes all resources associated with the Apps.



- Click **Refresh** to ensure the Space is in sync with the current status
- To ensure that all changes have been correctly applied, click **Redeploy**.

> **Note**: This action cannot be canceled and takes approximately ten minutes.

See Also

- Users
- Templates

4.2 Remote Access to Deployed Viz Now Apps

From Viz Now, you can remote in to one of the deployed apps. This is done on the **Space** page.

4.2.1 Remote Connection to Apps

- Prerequisites
- Remote Desktop Client
- The QUIC Protocol

Prerequisites

- You need the Amazon DCV client and to add your IP to Viz Now's *allowed* list. Follow the one-time configuration procedure below.

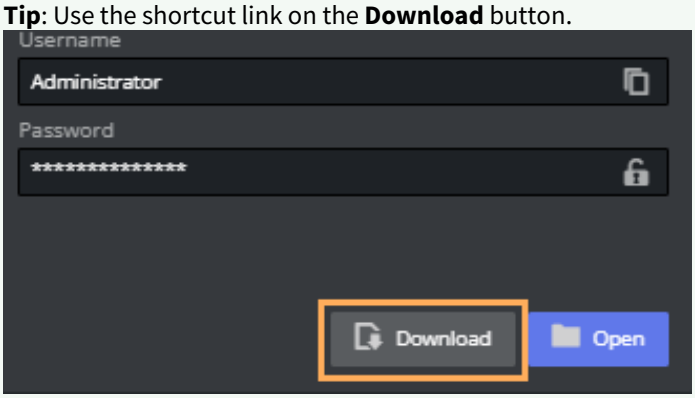
Remote Desktop Client

To Download and Enable the Amazon DCV Client

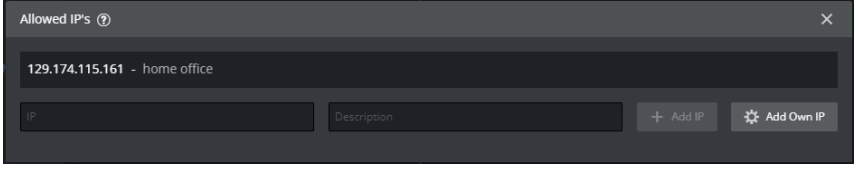
This is a one-time, initial configuration.

1. The latest Amazon DCV client is from Amazon DCV > Download.

Tip: Use the shortcut link on the **Download** button.



2. Your IP needs to be added to the *Allowed IP* list, before attempting to access any of the apps within a space. On first run, this can either be done by:
   a. Clicking **Download** or **Open**
   or
   b. Edit the **Allowed IP's** list. Add the IP in the field with a description then click **Add IP**.

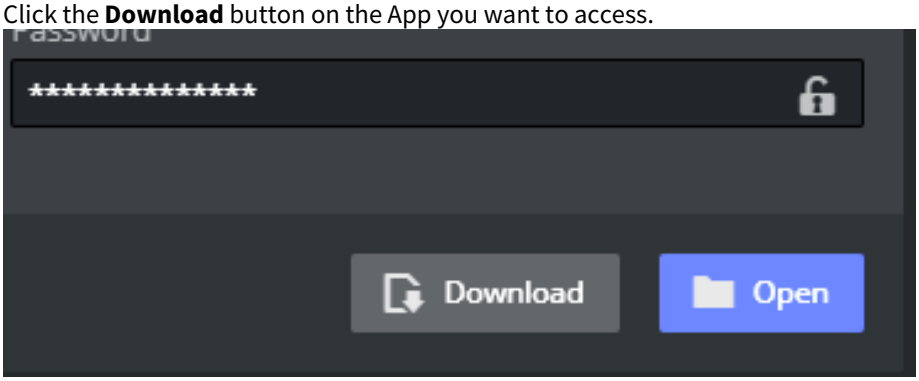


More information on using the Amazon DCV client App is provided here, *Using Amazon DCV*.

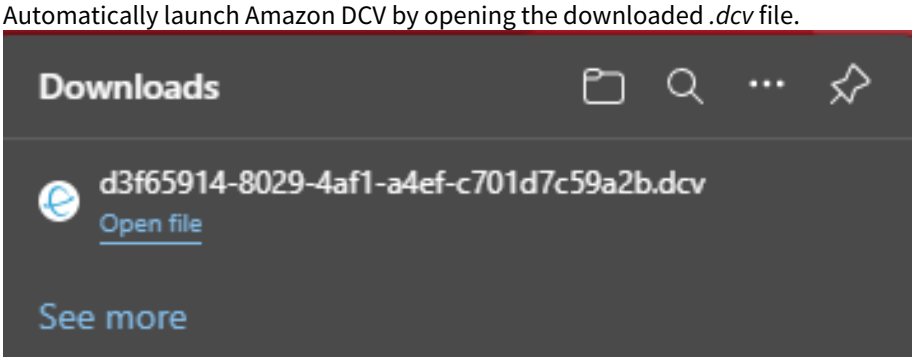
To Access a Viz Now App with the Amazon DCV Client

You can access any of your deployed apps remotely.

1. Ensure you have performed the one-off configuration described in To download and enable the Amazon DCV client above.
2. Click the **Download** button on the App you want to access.



   A *.dcv* file is saved to your browser's Downloads folder.
3. Automatically launch Amazon DCV by opening the downloaded *.dcv* file.

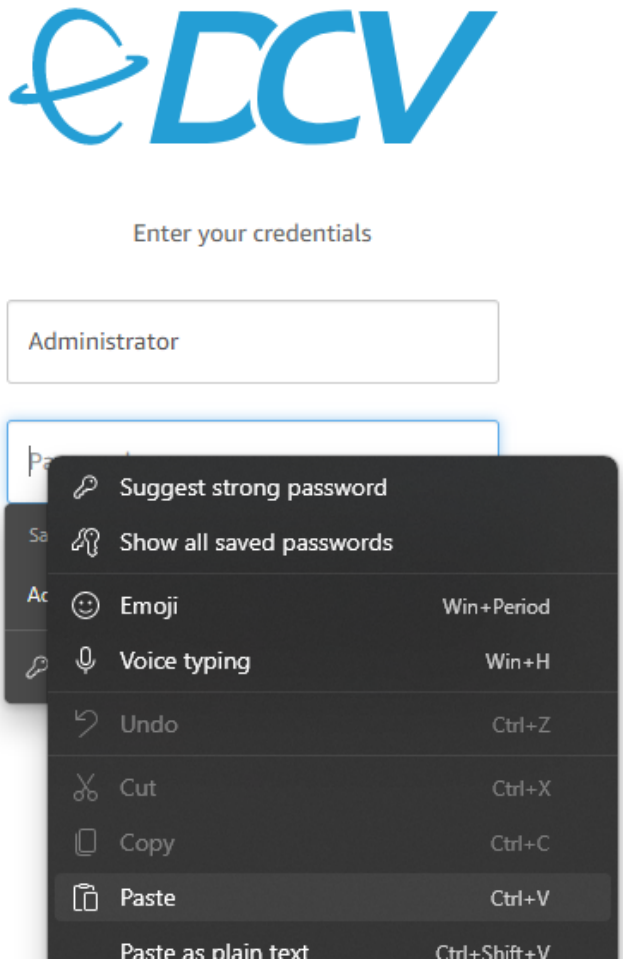


To Access a Viz Now App from Your Web Browser

You can also open the App access utility, Amazon DCV, from within your browser.

> **Note**: Be aware that this alternative method will *not* have the best quality and lowest possible latency. You are recommended to use the Amazon DCV client.

1. Click the **Open** button.
2. If a system *enable copying* pop-up appears, click affirmative to allow pasting to the clipboard.
   The Viz Now app password is copied to your windows clipboard.
3. In the **Enter your credentials menu**, right-click in the **Password** field and select *Paste*.



The QUIC Protocol

The QUIC Protocol uses UDP traffic, which can potentially improve performance and reduce latency.

- In order to use it, traffic will need to be allowed through the default port (8443). This is discussed in the documentation for Amazon DCV:
  - *Enabling the QUIC UDP transport protocol - Amazon DCV (amazon.com)*
  - *Changing the Amazon DCV Server TCP/UDP ports and listen address - Amazon DCV (amazon.com)*

4.3 Tags

For each Space, it is possible assist Space management by adding *tags*. The various types of tag are described below:

- Custom Tags
- Mandatory Tags
- Organization Tags
- Cost Allocation Tags

4.3.1 AWS Tags

All tags are applied as AWS Tags on all resources deployed by Viz Now.

- AWS Tags are key-value pairs that can be attached to AWS resources, providing a flexible way to manage, organize, and track costs.
- AWS Tags facilitate efficient resource filtering and discovery, enhancing operational efficiency.
- In AWS, *tag policies* enforce consistent tagging across resources, which is crucial for regulatory compliance and effective resource management and cost tracking.

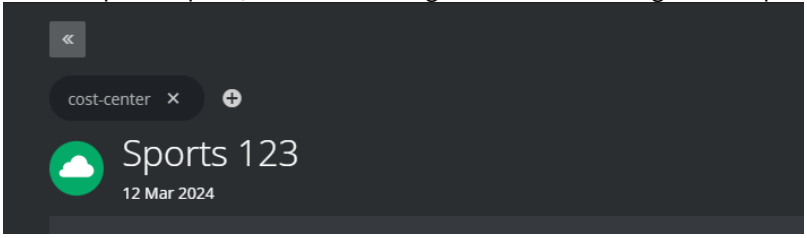
> **Note**: The Organization Administrator can define *mandatory* Tags to comply with AWS Tag Policies and ensure that specific tags are always included.
> See the Viz Now Administrator Guide, section *Organization*.

4.3.2 Adding a Tag

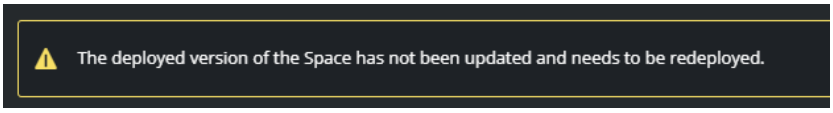
Custom Tags

Adding custom tags to a Space enables distinguishing a particular Space from other resources. It also clarifies what the Space is used for.

To add a custom tag

1. In the required Space, click the **Plus** sign above the heading for the Space.


2. Enter the Tag name and click or press **Enter**.
3. (Optional) Provide a value if required.
4. To add the new tag, click .
5. Once the Tag is added, a *redeploy* is required to add the Tag to any existing AWS resources.
   The Tag is highlighted until this is done.

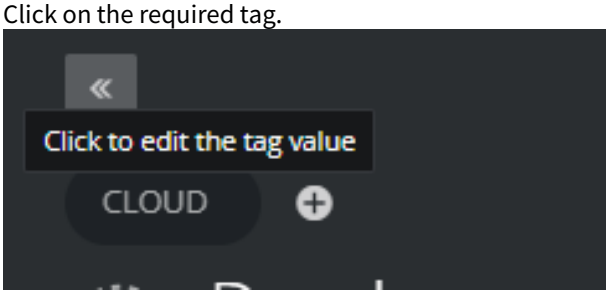


Mandatory Tags

If your administrator has marked an Organization Tag as mandatory, it will appear in all new Spaces. It is not possible to remove this tag and there is no '**X**' button to remove it. However, you add *values* to it.

To select values for a mandatory Tag

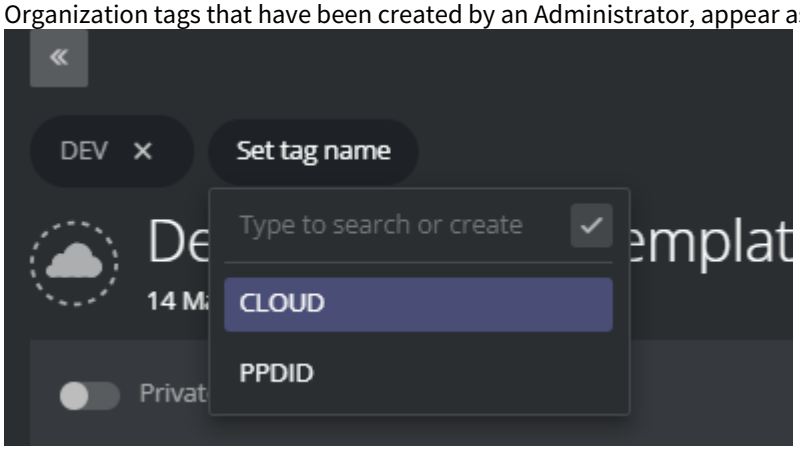
1. Click on the required tag.



2. Enter a value and save by clicking or pressing **Enter**.

Organization Tags

Organization tags that have been created by an Administrator, appear as selectable suggestions.



To add organization tags to a Space

- Simply select them from the list to add.

Cost Allocation Tags

- Cost allocation tags are labels that you or AWS assign to an AWS resource. Each tag consists of a *key* and a *value*.
- These tags enable you to organize your resources and track costs on a detailed level.

There are two types of cost allocation tags:

AWS-generated tags: These are created by AWS or AWS Marketplace ISVs for you and are prefixed with "*aws:*".

User-defined tags: You can add these tags yourself through Viz Now, as described above.

Why use Cost Allocation Tags?

Accountability: Allocate costs to those responsible for the resource usage.
Financial transparency: Provide clear visibility into cash allocations toward IT spending.
Informed IT investments: Track ROI based on projects, applications, or business lines.

How Do Cost Allocation Tags Work?

- After activating cost allocation tags, AWS organizes your resource costs on a *cost allocation report*. This report groups your usage and costs based on your active tags.
- You can apply tags that represent business categories (for example, cost centers, application names) to organize costs across services.

Example Scenario:

- You tag two Amazon EC2 instances:
  - **Cost Center**: Engineering
  - **Stack**: Production
- You have an AWS-generated tag: **createdBy** (that tracks who created the resource)

The *cost allocation report* will show costs associated with these tags.

> ⚠ **Note**: *Cost allocation tags* enhance cloud accountability and empower better decision making.
>
> - Activate them to gain insights into your AWS costs.
>
> Read more about this topic here: Using AWS cost allocation tags - AWS Billing (amazon.com)

4.4 Deployment Stages (AWS)

The deployment workflow starts when the user clicks the **Deploy** button.

- Stage 1 - Initialize
- Stage 2 - Pre-deploy
- Stage 3 - Deploy
- Stage 4 - Post Deploy

4.4.1 Stage 1 - Initialize

First, Viz Now checks that the selected apps are available and that no resources are missing.

4.4.2 Stage 2 - Pre-deploy

Viz Now adopts a role in the target AWS account and performs the following actions:

1. Check and increase quota if needed. Quota is used by AWS to assess how many resources are needed (Read more here - AWS service quotas - AWS General Reference).
2. Reserve the instances to be deployed in the target region. Viz Now checks if the instance types configured are available. If not, it attempts other instance options if any alternatives are listed in the app and other regions if more are listed.

> ⚠ **Note**: Capacity reservations are handled by Viz Now and should *not* be interfered with during deploy (Read more here - On-Demand Capacity Reservations - Amazon Elastic Compute Cloud).

3. Once Viz Now successfully reserves the instances required for the deployment, it continues.
4. Share the AMIs that are needed for the deploy with the target AWS account (Read more here - Share an AMI with specific AWS accounts - Amazon Elastic Compute Cloud).

4.4.3 Stage 3 - Deploy

Viz Now depends on third parties to handle the deploy process. This requires the longest wait time, but should be done within 15 minutes. This party also assumes a role in the target account and runs the deployment scripts. Technologies used for the deploy are:

- **Spacelift:** Spacelift Documentation
- **Docker:** Docker Documentation | Docker Documentation
- **Terraform:** Terraform by HashiCorp
- **Powershell:** PowerShell Documentation - PowerShell | Microsoft Learn
- **Windows RM:** Windows Remote Management - Win32 apps | Microsoft Learn

4.4.4 Stage 4 - Post Deploy

Viz Now gathers data from the deploy process and stores it in its database.

4.5 Apps

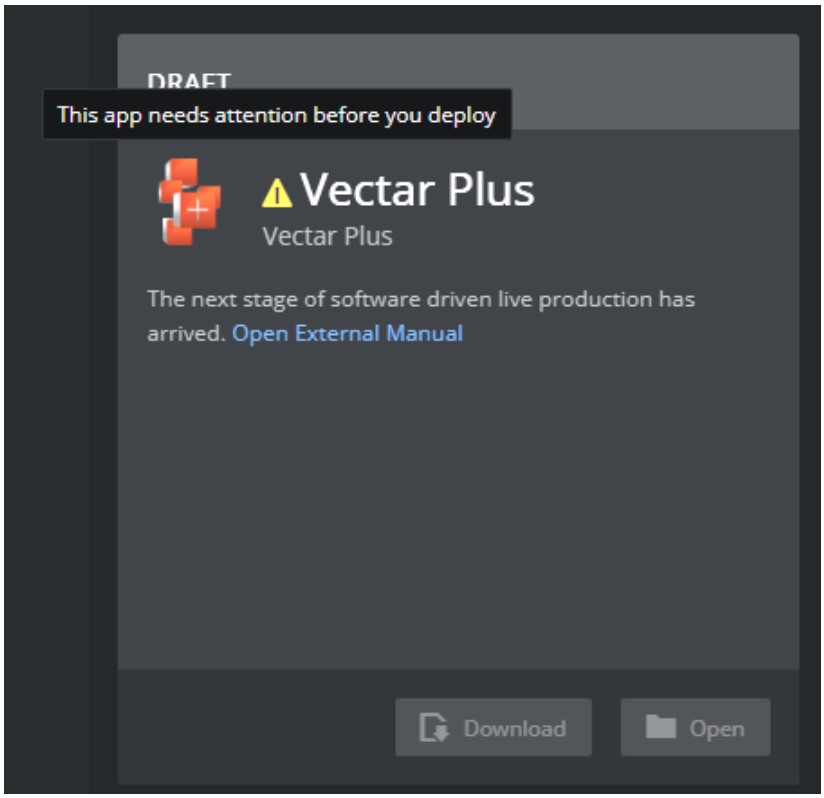
An *App* is a deployed application and is part of a Space. In Viz Now, the App box provides information and tools for accessing the app.

- Accessing App Details
- Configuring App Deployment Settings
- Offline or Online

4.5.1 Working with Apps

Accessing App Details

This is usually done with the Amazon DCV client or with a web URL.

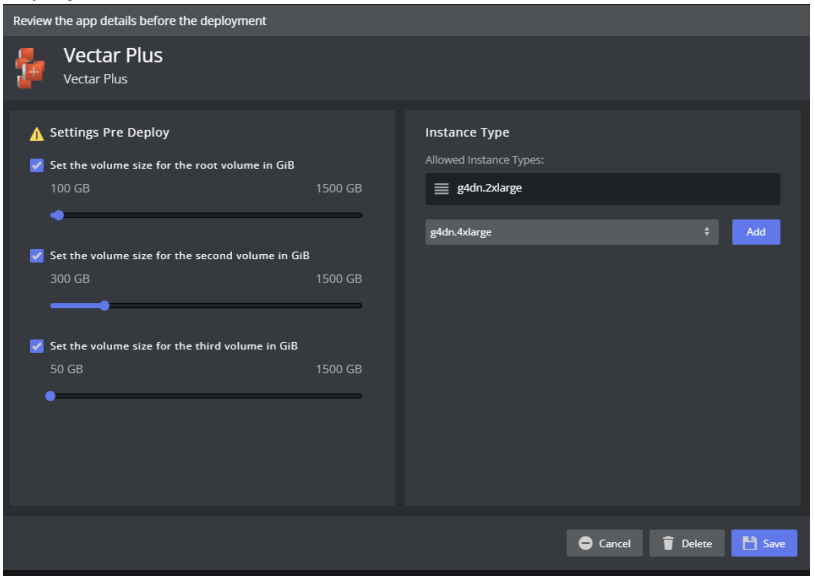


Configuring App Deployment Settings

- For some Apps it is possible to do some configuration options *before* deploying the product.
- For some Apps there are settings that *only* can be set before the first deploy. These are indicated with a warning symbol and tooltip.

To Configure App Deployment Characteristics

- Click the App
  A detailed view of the App is presented, where you can optionally perform further customization before deployment.



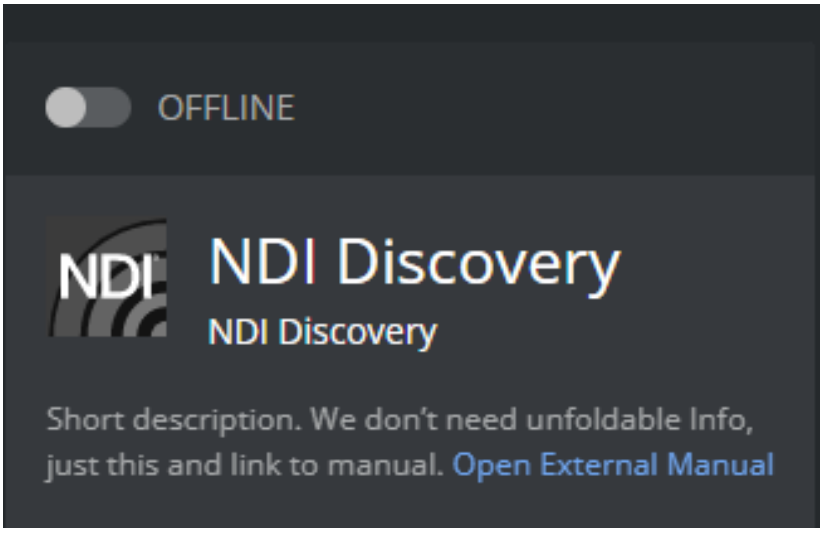
To Configure First-time only App Deployment Characteristics

Selections in the panel with **Settings Pre Deploy** can only be set when the app is deployed for the *first time*. If you need to later change these setting, you must:

1. Manually back up all your changes.
2. Remove the App and redeploy it.
3. Re-add the App, configure and save your pre-deployment settings.
4. Deploy the App.
5. Restore your backup manually, if needed.

Offline or Online

- Each App can be turned on or off by toggling its switch.



- Switching *on* starts the virtual machine that the app is running on.
- If the cloud provider does not have the resources available an error message is shown.

Note: The cost of the instance is greatly reduced while offline, but it has a cost as long as it is not removed and the space is redeployed. Viz Now does not currently provide any indications of the cost of the Space or individual Apps.

4.6 Templates

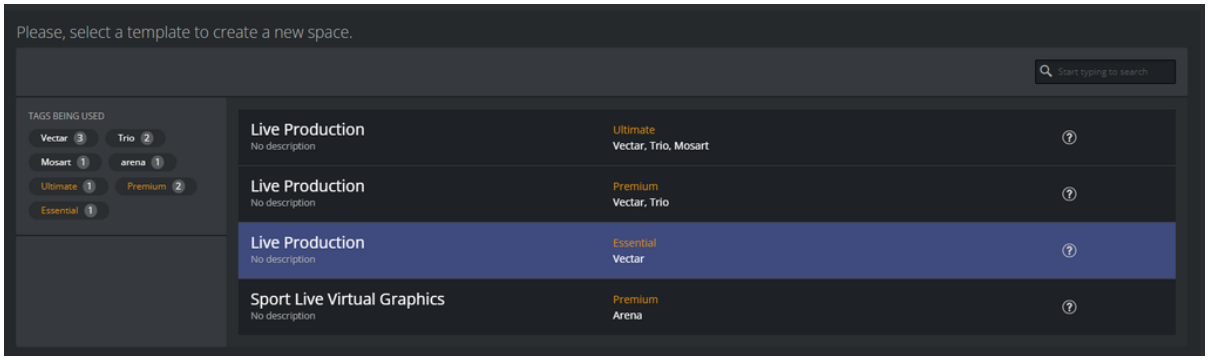
4.6.1 Space Templates

A space template is a set of Vizrt products that have been configured and prepared by Vizrt for deployment in the cloud. It can be used in your Viz Now organization to address a particular workflow, and may offer some customization options for the user.

Template Types

It's possible that your organization won't have access to certain template types.

Specific apps such as Viz Vectar Plus, Viz Trio and Viz Mosart are pre-tagged by default with some templates.



4.7 VPC Peering

4.7.1 Working with VPC Peering

Viz Now allows you to connect different spaces or VPCs using the VPC peering service in AWS. This allows network traffic to be exchanged between the applications running within different spaces. This can also be used to let Viz Now spaces communicate with VPCs that are manually created within AWS.

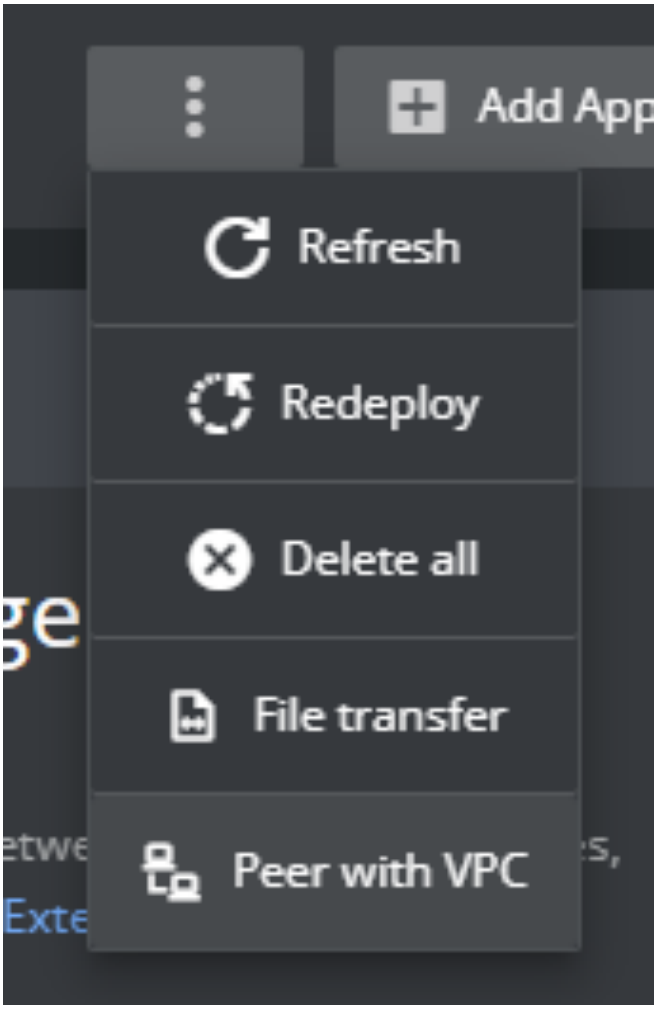
> **Note:** Peering can only be set up by the Organization Admin user or a Editor user with access to the Spaces to be peered. If a peering with a VPC that is not created by Viz Now some manual configuration is required. See AWS documentation regarding this.

Space Peering

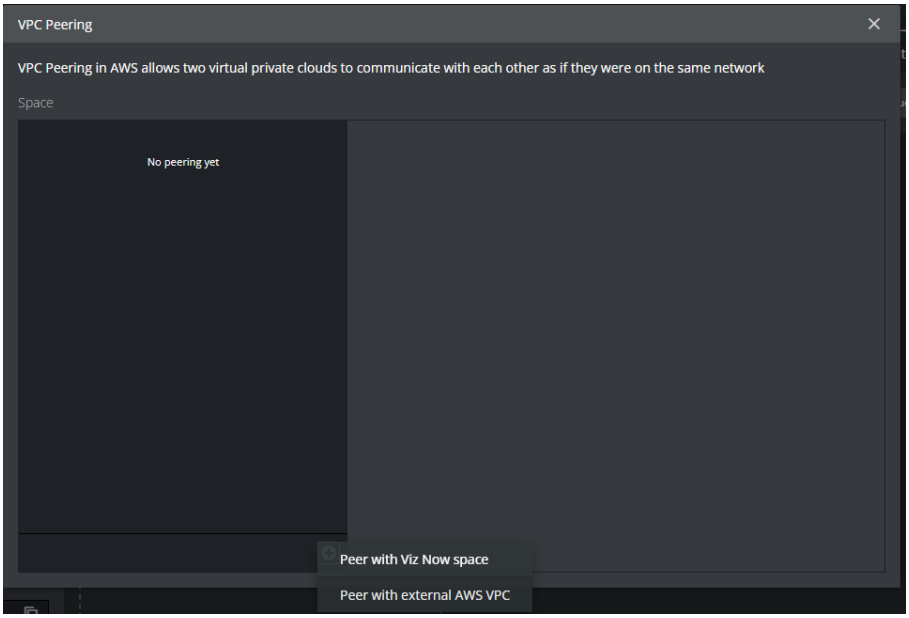
You must have the necessary access rights to both spaces. In addition, you must have minimum Viz Now *Editor* or *Admin* privileges. It is possible to peer with several other Spaces. This can be useful if you want to have dedicated Spaces for contribution or limit for different Operators access into different Spaces. When peering spaces some manual configuration of the App configurations are usually required if you want them to communicate. This is depending on the Apps you use.

To peer with another Space

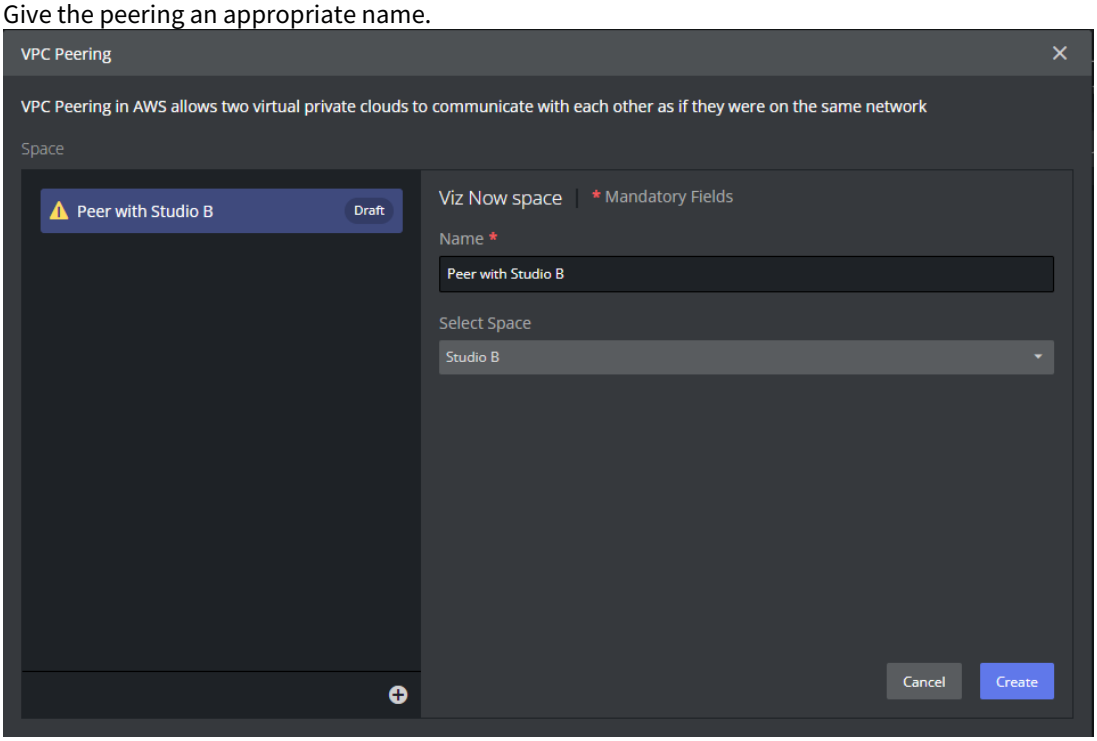
1. Navigate to one of the Spaces.
2. Click the **dotted** button.



3. Select *Peer with VPC*.
4. The **VPC Peering** dialogue appears. Click the **+** icon at the bottom of the list and select *Peer with Viz Now space*.



5. From the list of available spaces, select the Space you want to connect to.
6. Give the peering an appropriate name.

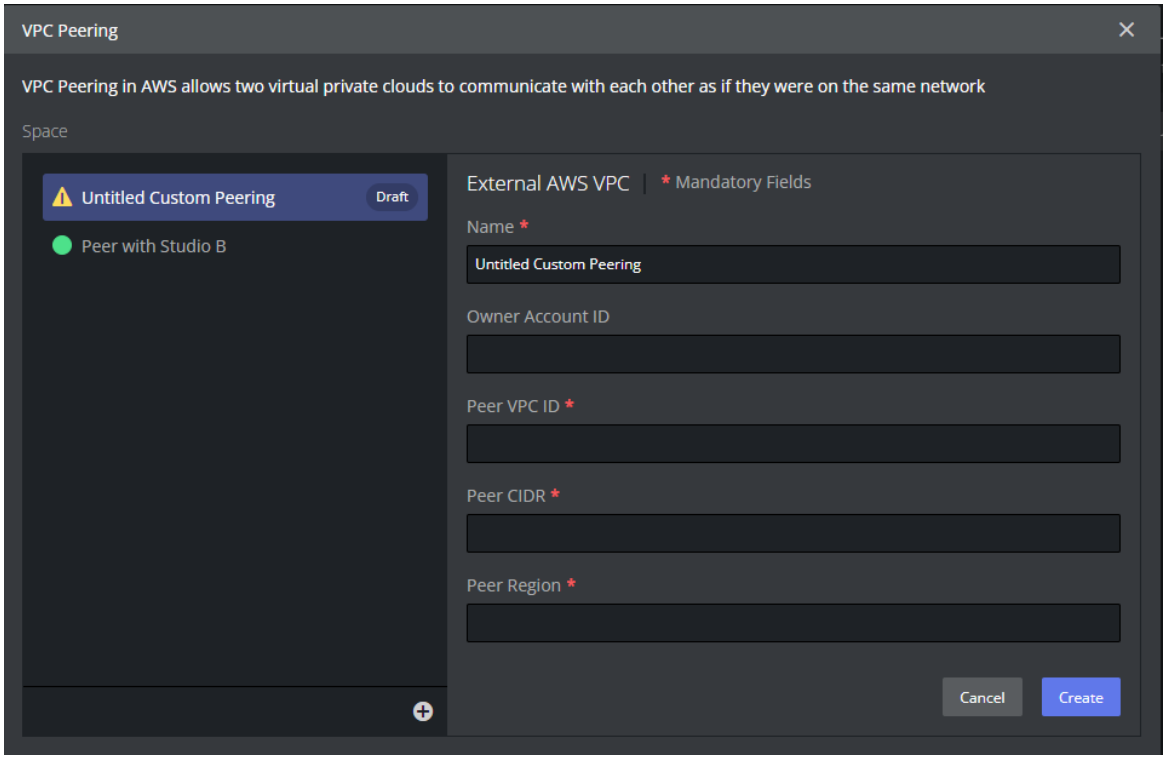


7. Click **Create** to start the peering.
8. The peering should be automatically accepted within minutes.

Note: If the Space you want to connect to is not in the list, most likely you lack access rights or the space is unsuitable for peering.

To peer with an external account or custom VPC

Warning: If you wish to establish peering with custom Virtual Private Clouds (VPCs), ensure that the target VPC falls within the CIDR range defined for the organization, usually 10.0.0.0/8. Alternatively, you can consider using the 172.16.0.0/12 range, although this holds a lower priority and network traffic will be deprioritized.

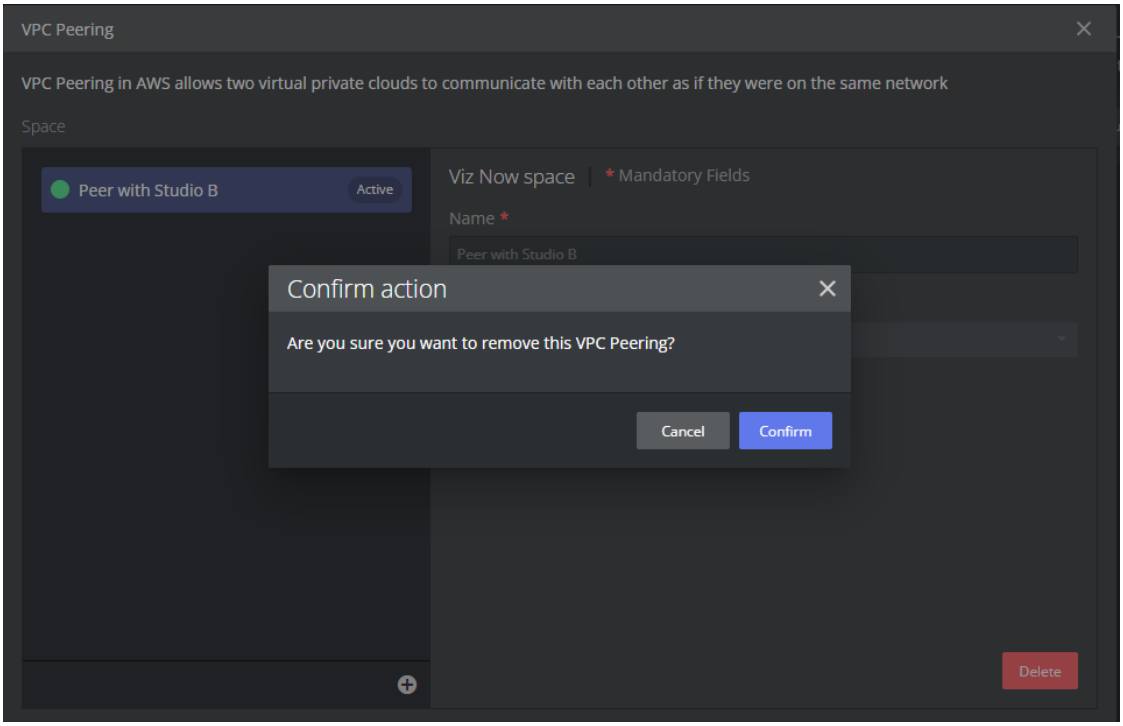


1. From the **VPC Peering** dialogue - select *Peer with external AWS* VPC.
2. Fill in the required fields.
3. Click **Create**.
   This creates the peering request
4. When connecting to *custom VPC*s some additional configuration from within the AWS Console is required for the peering to work.
   - Accepting the peering request.
   - Setting up the route table on the custom VPC to route traffic to the Viz Now VPC.
5. Once the peering is complete, you should see the peering status below the title of the Space.

Warning: If the two spaces are in different regions, AWS transfer costs are added to your AWS bill.

To delete a VPC peering

1. Open the Space where the peering is configured.
2. Open the **VPC Peering** dialogue.
3. Select the *Active peering* and click the red **Delete** button.



4. Click **Confirm** to delete the peering.

5 Organizations Explained

During the onboarding process, your *organization* is set up to allow Viz Now to access your cloud vendor.

- Each Organization has its own administrator user who can create more users and assign different privileges.
- For each Cloud Account, a separate organization is required.
- Each customer organization receives a unique Organization from Vizrt.

> **Note:** Your admin user is provided by the Vizrt administrator via email.

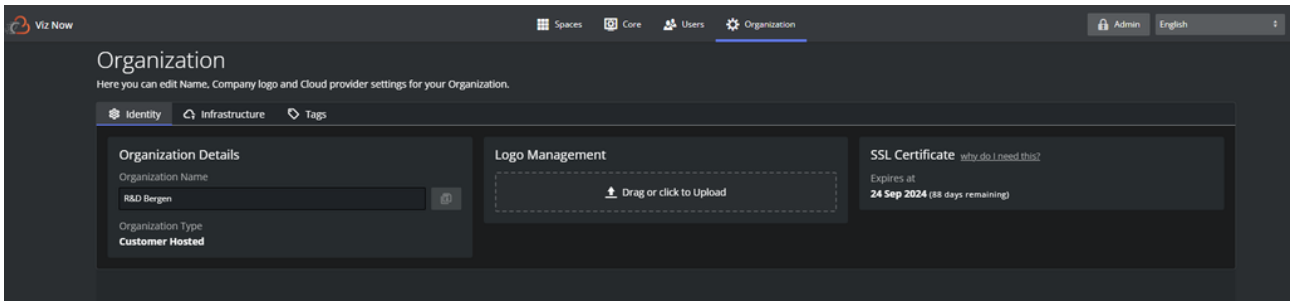
5.1 The Organization Page

- As an Admin, you reach the Organization page by clicking the **Organization** tab on the top menu bar.

Tabs enable you to edit and update the following settings in your organization:

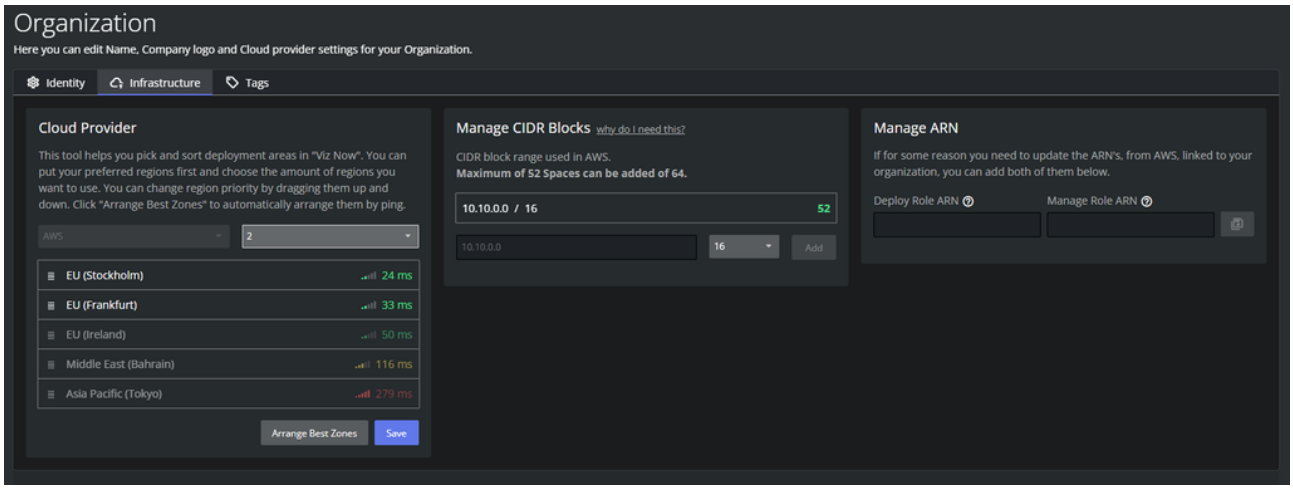
- Identity
- Infrastructure
- Tags

5.1.1 Identity



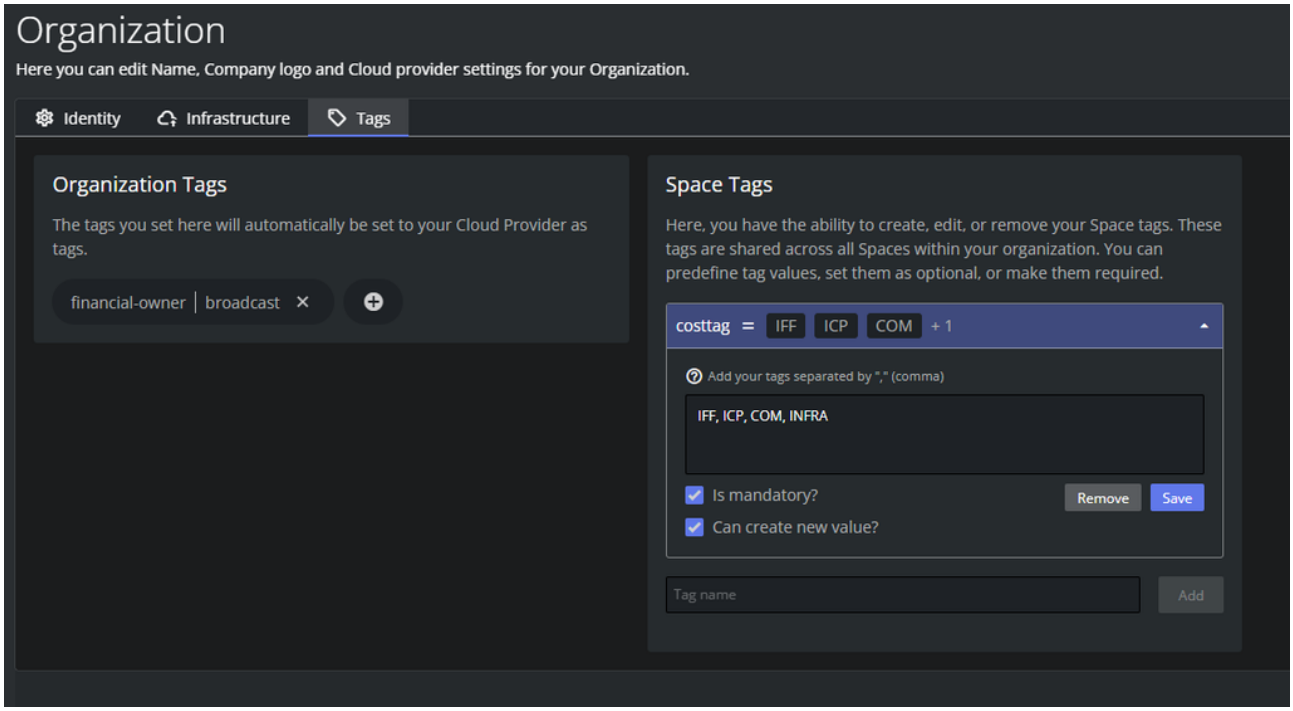
- **Organization Details:** The initial organization name is provided during the onboarding process and can be updated only by the organization admin.
  Organization Type is currently always *Customer Hosted*.
- **Logo Management:** You can upload/update a company logo by clicking on **Drag or Click to Upload**, selecting a logo file and clicking **OK**, then **Save**.
- **SSL Certificate** (expiration date)**:** SSL certificates secure Viz Now-deployed apps and protect user data, verify ownership of the app, prevent attackers from creating fake versions, and establish trust with users. If expiration date is near, you can renew the certificate here.

5.1.2 Infrastructure



- **Cloud Provider:** Viz Now requires access to your cloud providers, which you can alternate between. Currently only the AWS (Amazon Web Services) cloud provider is available.
    - **Preferred Cloud Provider Regions:**
        - The first region in the list is the Cloud Provider region where the spaces are usually deployed.
        - If deployment to the first region fails, the second in the list is attempted.
          From the drop-down on the right, you select how many regions will be attempted until failing the deployment (1-5 selections).
        - The regions that are enabled appear in the list of selections that the user can choose from, if they want to specify the region for their space.
- **Manage CIDR Blocks:** Define additional CIDR blocks to extend the range used in AWS, as required.
- **Manage ARN:** Here you can update the ARN linked to the user roles used to manage your organization. It is not possible to view the current role ARNs due to security constraints.

Tags



- **Organization Tags**: Lets you define tags that will be attached to all spaces deployed by Viz Now. This is particularly useful if you're implementing AWS Tag Policies and/or aiming to monitor expenses via Tags.
- **Space Tags:** Administer tags that are either optional or mandatory for Spaces. Tags applied to Spaces also appear as tags on all AWS resources that Viz Now deploys for that particular Space.
    - **Is mandatory?**: The tag will be pre-added to all spaces and not possible to remove. Usually the user then needs to choose from some options or fill in a value.
      For a user, setting this tag is mandatory before deploying any new space.
      This is particularly useful if you're implementing AWS Tag Policies and/or aiming to monitor expenses via Tags.
    - **Can create new value?:** When checked, users can also add their own custom values to the tag (in addition to the tags made here or exclusively).

6 Best practices - How to Configure Your AWS Accounts for Viz Now

6.1 Introduction

This is a guide to creating a specific AWS account tailored for Viz Now. By creating a dedicated AWS account, users can benefit from enhanced security and isolation.

6.1.1 Main Benefits of a Dedicated AWS Account

- **Security Isolation:** By creating a dedicated AWS account, users can isolate resources and services, ensuring that potential security breaches or vulnerabilities in one environment do not affect the other.
- **Cost Management:** A dedicated AWS account allows for better cost tracking and management. Users can easily monitor and control costs associated with the Viz Now deployment without interference from other services.
- **Customization:** A dedicated AWS account allows users to customize settings, policies, and permissions specifically for the Viz Now deployment. This provides greater flexibility in managing and optimizing the application's performance and security.

6.1.2 AWS Account Considerations

On the other hand, there are several AWS account requirements essential for Viz Now to achieve seamless deployment:

- **On-demand Capacity reservations:** Viz Now requires that the IAM entities used for Viz Now do not have limitations on their permissions to create on-demand Capacity reservations. This is necessary to ensure that the capacity required for a Space is available and that the Space created by Viz Now can be fully deployed in a single request.
  Reference: On-Demand Capacity Reservations - Amazon Elastic Compute Cloud

- **Service Quota limits:** These limits are described and defined by AWS, and in the case of Viz Now, must ensure that there are some minimum safe limits to guarantee that the deploys are carried out correctly. Reference: What is Service Quotas? - Service Quotas (amazon.com)

6.2 On-Demand Capacity Reservations

On-Demand Capacity Reservations enable you to reserve compute capacity for your Amazon EC2 instances in a specific Availability Zone for any duration. Capacity Reservations mitigate against the risk of being unable to get On-Demand capacity in case there are capacity constraints. If you have strict capacity requirements, and are running business-critical workloads that require a certain level of long or short-term capacity assurance, we recommend that you create a Capacity Reservation to ensure that you always have access to Amazon EC2 capacity when you need it, for as long as you need it.

This ensures that the required resources are always available when needed, providing predictable performance and the ability to launch instances immediately.

6.2.1 Main Benefits of On-Demand Capacity Reservations

- **Guaranteed Capacity:** On-Demand Capacity Reservations ensure that the required capacity is available when needed, avoiding potential delays and ensuring the successful execution of the workload by having the necessary AWS resources.
- **Flexible Pricing:** Unlike Reserved Instances, On-Demand Capacity Reservations do not require long-term commitments. Users pay for the reserved capacity on an hourly basis, providing more flexibility in managing costs.
- **Customizable Reservations:** Users can create Capacity Reservations with different instance types, sizes, and tenancies, allowing for a tailored solution that meets the specific requirements of the Viz Now deployment.

6.2.2 AWS Account Considerations

In an AWS account, there are several factors that could prevent the use of Capacity Reservations:

- **Insufficient permissions:** The IAM entities (users, groups, or roles) might not have the necessary permissions to create or manage Capacity Reservations. Ensure that the appropriate permissions are granted in the IAM policies.
    a. Sign in to the AWS Management Console and navigate to the IAM service.
    b. Check the permissions for a specific IAM user, group, or role, select the corresponding section in the left navigation pane (Users, Groups, or Roles).
    c. Find and select the IAM entity you want to check
    d. Click on the **Permissions** tab and then the **Simulate** button.
    e. In IAM Policy Simulator, in the search bar, enter *EC2* service and select the following actions:
        i. CreateCapacityReservation
        ii. CancelCapacityReservation
- **Service limits:** AWS imposes default limits on the number of Capacity Reservations per region. If the limit is reached, you may be unable to create new reservations. In such a case, you can request a limit increase through the AWS **Service Quotas** console or through AWS Support.
    - See section AWS Service Quotas for how his is checked.

- **Availability zone restrictions:** Capacity Reservations are specific to an Availability Zone (AZ). If the desired Availability Zone is constrained or has limited capacity, it may impact your ability to use Capacity Reservations.
    - This is managed by Viz Now selecting another AZ or region on the preferred ones for the Viz Now organization.
- **Instance type restrictions:** Some instance types might not be available for Capacity Reservations in certain regions or Availability Zones. Check the AWS documentation for instance type availability.
    - This is managed by Viz Now selecting another Instance type in the preferred ones for the Viz Now application.

To address these issues, ensure that the necessary permissions are in place, monitor service limits, choose appropriate Availability Zones and instance types, and maintain a sufficient account budget.

6.3 AWS Service Quotas

AWS Service Quotas are limits applied to the number of resources that can be created or used within an AWS account. These quotas help prevent unintentional resource consumption and enable AWS to provide a reliable service to all users. If your business needs are not met by the default limit of service resources or operations that apply to an AWS account or an AWS Region, you might need to increase your Service Quota values. Service Quotas enable you to look up your service quotas and to request increases. AWS Support might approve, deny, or partially approve your requests.

Viz Now automatically requests a service quota increase during the deployment process. However, since the approval process for these requests can take up to 48 hours, there is also a manual method for increasing service quotas. Manually performing this action in advance can help ensure that your deployment proceeds smoothly without waiting for quota increases approval.

6.3.1 Top Service Quotas Related to Viz Now

This technical guide outlines various AWS service quotas that may impact the deployment of Viz Now. Each section presents a service quota, its default value, scope, and adjustability, as well as a brief description of the corresponding AWS service or resource.

Running On-Demand G and VT Instances (L-DB2E81BA)

> ⚠ **Note:** It is strongly recommended to make a manual request (48 hours in advance) to AWS for this type of deployment.

vCPUs (virtual CPUs) allocate computing resources to instances in AWS.

- Quota: *Maximum number of vCPUs assigned* to running On-Demand G and VT instances
- Quota code: *L-DB2E81BA*
- Default quota value: *0*
- Adjustable: *Yes*
- Scope: *Regional.*

EC2-VPC Elastic IPs (L-0263D0A3)

Elastic IP addresses are static IPv4 addresses designed for dynamic cloud computing in EC2. The IP address is assigned to the instance and retained till it is destroyed.

- Quota: *Maximum number of Elastic IP addresses* allocated for EC2-VPC
- Quota code: *L-0263D0A3*
- Default limit: *5* per region
- Adjustable: *Yes*
- Scope: *Regional*.

VPCs (L-F678F1CE)

A Virtual Private Cloud (VPC) is an isolated section of the AWS Cloud where a user can launch resources within a virtual network.

- Quota: *Maximum number of VPCs per region* (tied to the maximum number of internet gateways per region)
- Quota code: *L-F678F1CE*
- Default limit: *5*
- Adjustable: *Yes*
- Scope: *Regional*.

Inbound or Outbound Rules per Security Group (L-0EA8095F)

Security groups serve as virtual firewalls for EC2 instances, controlling inbound and outbound traffic.

- Quota: *Maximum number of inbound or outbound rules per VPC security group* (120 rules in total, enforced separately for IPv4 and IPv6)
- Quota code: *L-0EA8095F*
- Default limit: *60 inbound and 60 outbound rules* per security group
- Adjustable: *Yes*
- Scope: *Regional*.

Security Groups per Network Interface (L-2AFB9258)

Network interfaces facilitate communication between instances and networks.

- Quota: *Maximum number of security groups per network interface* (cannot exceed 1000 when multiplied by the quota for rules per security group)
- Quota code: *L-2AFB9258*
- Default limit: *5* per network interface
- Adjustable: *Yes* (max 16)
- Scope: *Regional*.

VPC Peerings (L-7E9ECCDB)

VPC peering allows a user to connect VPCs across different AWS accounts or regions.

- Quota: *Maximum number of active VPC peering connections per VPC* (can be increased up to a maximum of 125)
- Quota code: *L-7E9ECCDB*
- Default limit: *50*
- Adjustable: *Yes* (max 125)
- Scope: *Regional*.

6.3.2 Examples of Quota Service Numbers

Explanation of Service Quotas related with Viz Now on an AWS account:

Service Quota	Default Value	Viz Now considerations about the Service Quota	Reason	Calculations
G On-demand running	0	Default template: *Live Production Vision Mixing* with default Apps	2 instances from G family InstanceType (g4dn.2xlarge Instances) are needed. Since the default value is 0, this requires an increase request.	2 x 8 vCPU = 16 vCPU
VPC	5	Viz Now makes a VPC per Space	An Organization has 1 mandatory Space, a *License* Space. With default settings, *4* spaces could be deployed before reaching the limit.	4 Spaces + License = 5 VPC
Elastic IP	5	Each App has an attached elasticIP	A template with 6 Applications needs 6 Elastic IP.	Each App deployed needs one Elastic IP.
Security Groups (SG) Rules	60 in 60 out	Each IP allowed to access a Space's apps has a number of rules it applied to it, based on the workflow.	Each IP will apply 10 rules per allowed IP.	All rules are *inbound* rules so max allowed IP is around *20*, unless this limit is increased.
SG per Network Interface	5	4 SG per Network Interface	With the default number of Security Groups no extra security groups need be added.	
VPC Peerings	50	By default, each deployed space needs (one) peering with the License server.	By default an Organization could have 50 Spaces with default Peering between the Space VPC and the License VPC.	

6.3.3 Service Quota by Template

Below you see the relationship between a Template and its configurations. Some examples are shown to provide an understanding of how Viz Now deployments impacts a service quota.

Template Title	G On demand Quota	Elastic IP Quota	Comments

Live Production Vision Mixing	**Default Specs:** 16 *(8+8)*
	Max Specs: 112 *(32*4 +16)*
		Default Specs: 3
		Max Specs: 6
			Defaults Specs:
			• There are two G family instances:
			  • Viz Vectar and NDI Bridge
			  • g4dn.2xlarge requires 8 vCPU
			• There are 3 apps by default: 3 IPs are needed.
			Max Specs:
			• 3 potential G family instance:
			  • Vectar - g4dn.8xlarge - 32 vCPU
			  • NDI Bridge - g4dn.4xlarge - 16 vCPU
			  • Windows (3x) - g4dn.8xlarge - 32 vCPU x3
			• Max of 6 Apps : 6 IPs are needed.

Template Title	G On demand Quota	Elastic IP Quota	Comments

Live Production Vision Mixing and Advanced Graphics	**Default Specs:** 24 *(8+8+8)*
	Max Specs: 272 *(160 + 16 +96)*
		Default Specs: 4
		Max Specs: 12
			Defaults Specs:
			• There are three G family instance:
			  • Viz Vectar, Viz Engine & NDI Bridge
			  • g4dn.2xlarge requires 8 vCPU
			• There are 4 apps by default: 4 IPs are needed.
			Max Specs:
			• 7 potential G family instance:
			  • Vectar - g4dn.8xlarge - 32 vCPU
			  • Vectar Live Prod - g4dn.8xlarge - 32 vCPU
			  • 3Play - g4dn.8xlarge - 32 vCPU
			  • Viz Engine - g4dn.8xlarge - 32 vCPU
			  • Viz Trio - g4dn.8xlarge - 32 vCPU
			  • NDI Bridge - g4dn.4xlarge - 16 vCPU
			  • Windows (3x) - g4dn.8xlarge - 96 vCPU
			• Max of 6 Apps : 6 IPs are needed.

Template Title	G On demand Quota	Elastic IP Quota	Comments

Sports Analysis File-base	**Default Specs:** 16
	Max Specs: 48 *(32 + 32)*
		Default Specs: 1
		Max Specs: 2
			Defaults Specs:
			• There are 1 G family instance:
			  • Viz Libero
			  • g4dn.4xlarge requires 16 vCPU
			• There are 1 apps by default: 1 IP needed.
			Max Specs:
			• 2 potential G family instance:
			  • Viz Libero - g4dn.8xlarge - 32 vCPU
			  • Windows - g4dn.8xlarge - 32 vCPU
			• Max of 2 Apps : 2 IPs are needed.

6.3.4 Increasing Service Quotas

Deployment Timeout

Viz Now will automatically request an increase in service quotas during the deployment process. This is usually executed on the AWS side in 15-20 minutes.

- However, if the request is not approved by AWS after 20 minutes, the deployment is canceled.

At timeout and cancel, you will be notified, with a reference to the canceled service quota.

The request is retained in the AWS Management console, where you can monitor status of the request.

It can take up to 48 hours for AWS to increase service quotas. For this reason, we recommend submitting a manual service quota increase, 48 hours in advance of intended deployment.

To manually increase a Service Quota

Performing this action in advance can help ensure that your deployment proceeds smoothly without waiting for quota increases.

- Refer to the guide Requesting a quota increase - Service Quotas (amazon.com)

After submitting the request, AWS will review and respond to the request within 48 hours, although the response time may vary depending on the complexity of the request and the justification provided. AWS may request additional information or deny the request if the justification is not deemed sufficient. Status is available in your AWS Management console.

6.4 Conclusion

By following this guide, users can create an AWS account tailored for the Viz Now deployment application, taking advantage of security isolation, cost management, and customization.

Understanding *Reserved Instances* and *AWS Service Quotas* helps with optimizing the application's performance and resource usage.