



Viz Now User Guide

Version 2.0



Viz Now



Copyright ©2025 Vizrt. All rights reserved.

No part of this software, documentation or publication may be reproduced, transcribed, stored in a retrieval system, translated into any language, computer language, or transmitted in any form or by any means, electronically, mechanically, magnetically, optically, chemically, photocopied, manually, or otherwise, without prior written permission from Vizrt. Vizrt specifically retains title to all Vizrt software. This software is supplied under a license agreement and may only be installed, used or copied in accordance to that agreement.

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	Introduction to Viz Now	6
1.1	Related Documents	6
2	Creating First IAM Role	7
2.1	Creating an IAM Role.....	7
2.1.1	Defining a new IAM Role	7
3	Working with Deployed Apps	18
3.1	Region and Availability Zone	18
3.1.1	To select a Region and Availability Zone	18
3.2	Allowed IP	19
3.3	Virtual Windows Instance Apps.....	19
3.3.1	Amazon DCV Client Software	19
3.4	Web Apps.....	20
4	Working with Users	21
4.1	Assigning Users	21
4.1.1	To assign a User to your Space	21
5	Working with Spaces.....	22
5.1	Space Details	22
5.2	Creating and Deleting a Space	23
5.2.1	Creating a Space.....	23
5.2.2	Deleting a Space.....	24
5.3	Session Scheduling.....	25
5.3.1	Start and End Times.....	25
5.3.2	Auto-Shutdown	26
5.4	AWS Tags.....	27
5.4.1	Custom Tags	28
5.4.2	Mandatory Tags.....	28
5.4.3	Organization Tags	29
5.4.4	Cost Allocation Tags.....	29
6	Capacity Management.....	31
6.1	Best Practices for Instance Provisioning and Workflow Resilience	31
6.2	Capacity Management Strategies for Resilient Cloud Deployments:	31
6.3	Default Behavior: Targeted Capacity Reservations	32
6.3.1	Why This Matters	32

6.3.2	Important Notes	32
6.4	Guided Retry and Fail-Fast Deployment	33
6.4.1	Capacity Check & Reservation Feedback	33
6.4.2	What the User Sees	33
6.4.3	Your Options: Guided Response	33
6.4.4	Why It Matters	34
6.5	Visual Indicators for Capacity Status	35
6.5.1	App-Level Indicators	35
6.5.2	Space-Level Summary Indicator	35
6.6	Bring Your Own Capacity (BYOC)	36
6.6.1	Overview	36
6.7	Changing EC2 Instance Type of an Application.....	39
6.7.1	Overview	39
6.7.2	Why Change the EC2 Instance Type?.....	39
6.7.3	How to Change EC2 Instance Type in Viz Now	39
6.7.4	Important Notes	40
6.7.5	Summary	41
6.8	Switching Availability Zone or Region to Resolve EC2 Scarcity	42
6.8.1	Overview	42
6.8.2	Options for Relocating Workloads.....	42
6.8.3	Considerations and Tradeoffs	42
6.8.4	Summary	43
7	Security Overview	44
7.1	Introduction	44
7.1.1	Our Commitment to Secure Defaults	44
7.2	Viz Now IAM Role Setup & Permissions Guide.....	45
7.2.1	Overview	45
7.2.2	Prerequisites.....	45
7.2.3	Update Existing IAM Roles	45
7.2.4	Permissions Explained	50
7.3	Network Security and Default Port Configuration	53
7.3.1	Viz Now Security Environment	53
7.3.2	Volatility of Manual Changes	54
8	Feedback & Support	56
8.1	How to Access Support and Submit Ideas	56
8.1.1	Accessing the Support Portal	56
8.2	Got an Idea?	56

8.2.1	How to Submit an Idea.....	56
8.3	Need Help?	57

1 Introduction to Viz Now

Viz Now is a powerful tool for automating deployment and configuration of Cloud production workflows.

This guide presents the following topics:

- [Security Overview](#)
 - [Working with Deployed Apps](#)
 - [Working with Users](#)
 - [Working with Spaces](#)
 - [Feedback & Support](#)
-

1.1 Related Documents

See the [Vizrt documentation center](#) for documentation for related products, including:

- TriCaster Vector *
- Media Service
- Graphic Hub
- Viz Trio
- Media Sequencer
- Viz Engine
- Pilot Data Server*
- Viz Libero*
- Viz Arena*



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

2 Creating First IAM Role

2.1 Creating an IAM Role

If you have not defined any IAM roles for Viz Now, follow these guidelines.

Info: Where you already have defined Viz Now IAM roles in your AWS account, see [Update Existing IAM Roles](#).

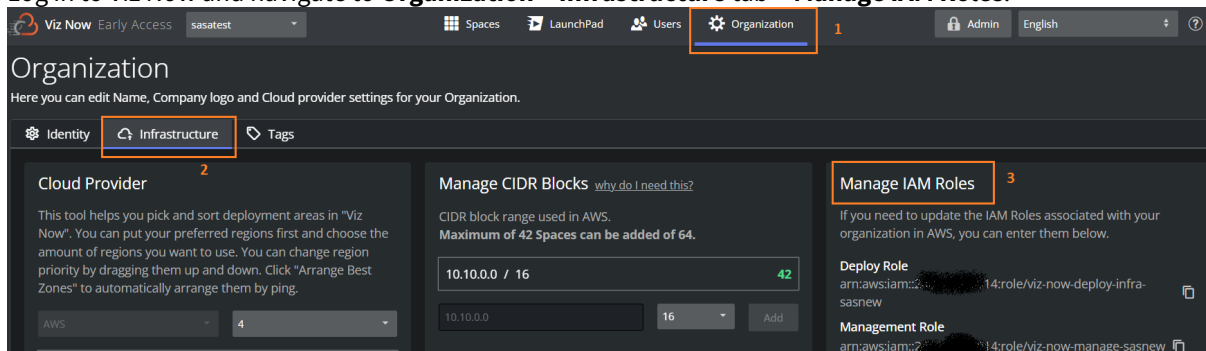
2.1.1 Defining a new IAM Role

You will create both a *Deploy* role and a *Management* role, and associate customized Viz Now trust relationships and policies.

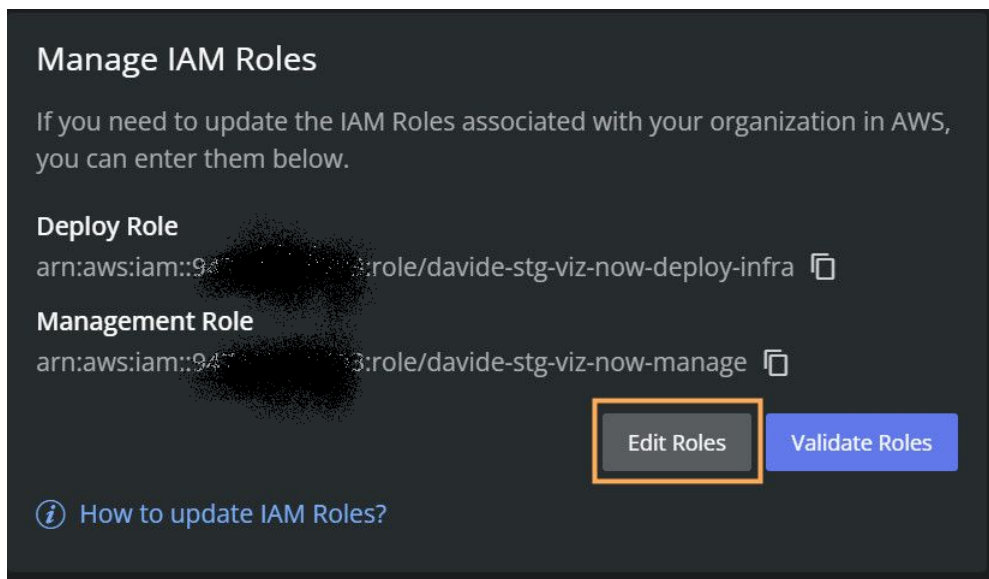
Tip: For a comprehensive explanation of roles, refer to the [Permissions Explained](#) section.

To define an IAM role in Viz Now

1. Log in to Viz Now and navigate to **Organization > Infrastructure tab > Manage IAM Roles**.



2. You'll see a screen like the one below, where you define the IAM Roles ARNs needed for a *Deploy* role.



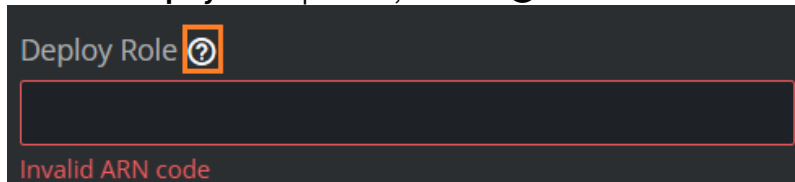
Deploy Role

The role *viz-now-deploy-infra* allows deploying infrastructure in your AWS Account.

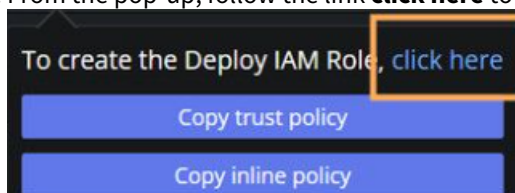
3. Log in to the AWS Management Console with IAM Administrator rights.
4. Back in Viz Now, click **Edit Roles**.



5. Next to the **Deploy Role** input field, click the **?** icon.



6. From the pop-up, follow the link **click here** to open the AWS console.



7. The AWS console opens in a new tab (if not logged-in, you will need to authenticate).

Step 1: Select trusted entity

Step 2: Add permissions

Step 3: Name, review, and create

Select trusted entity

Trusted entity type

- ☐ AWS service: Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☒ AWS account: Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web identity: Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation: Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy: Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- ☐ This account (248967558014)
- ☒ Another AWS account

Account ID
Identifier of the account that can use this role

324880187172

8. Click **Next** twice to skip the **Add permissions** step and arrive at **Name, review, and create**. **Role Name** is pre-populated as: *viz-now-deploy-infra*.

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

viz-now-deploy-infra

Maximum 64 characters. Use alphanumeric and '+', '=', '@', '-', '_' characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+ = @ - _ ' " , . / [] ! % ^ & * ~

9. Click **Create Role**.
A confirmation message is displayed.

Role viz-now-deploy-infra-sas created. [View role](#)

Note: If a warning indicates that the name already exists, update it by adding a suffix, for example: *viz-now-deploy-infra-something else*.

8. Click **View role**, AWS opens with the **Summary** page of the new role:

viz-now-deploy-infra-sas

Summary

Creation date: May 16, 2025, 10:50 (UTC+01:00)

ARN: arn:aws:iam::248967558014:role/viz-now-deploy-infra-sas

Last activity: -

Maximum session duration: 1 hour

Link to switch roles in console: <https://signin.aws.amazon.com/switchrole?roleName=viz-now-deploy-infra-sas&account=viznowtest>

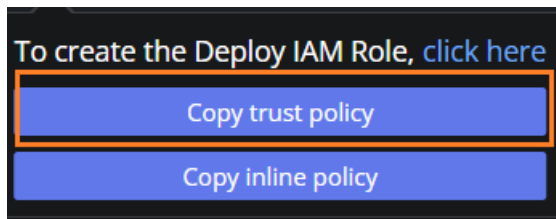
Permissions policies (0)

You can attach up to 10 managed policies.

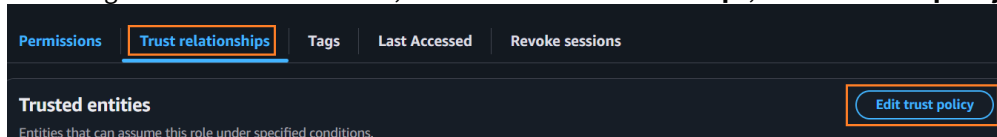
[Simulate](#) [Remove](#) [Add permissions](#)

Update the Trust Policy

9. Back in Viz Now, click **Copy trust policy**.



10. Switching back to the AWS console, on the tab **Trust relationships**, click **Edit trust policy**.



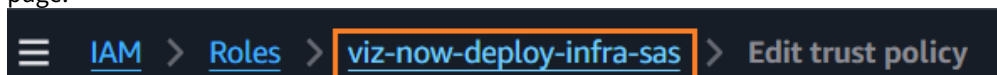
11. Paste the trust policy and click **Update Policy**.

12. The JSON code, shown below and which you can copy, is verified.

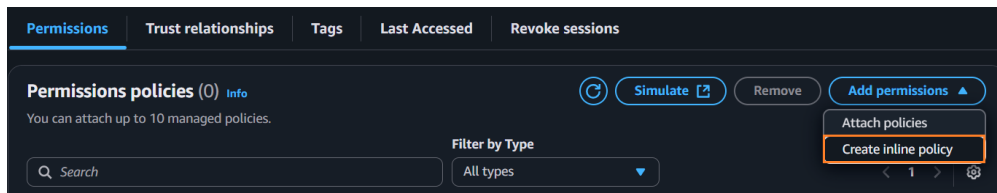
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::324880187172:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "sts:ExternalId": "SpaceliftIntegration*"
        }
      }
    }
  ]
}
```

Code	Explanation
Principal	Allows the Deployment Agent's AWS account (here <code>324880187172</code>) to assume the role.
Condition	Ensures the external ID starts with <code>SpaceliftIntegration@</code> .

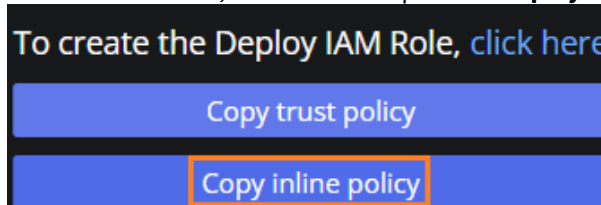
13. Continue in the AWS console by clicking the role's name in the breadcrumbs to reach the role's **Summary** page:



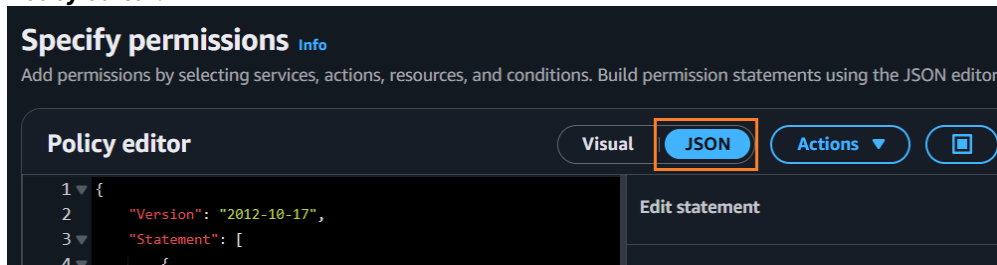
14. From the **Permissions** tab, click **Add permissions > Create inline policy**.



15. Go back to Viz Now, and from the input field **Deploy Role**, click **Copy inline policy**.



16. Back to the AWS console, in the **Policy editor**, click the **JSON** button and then paste the inline policy into the **Policy editor**.



17. The pasted JSON looks like:



18. Click **Next**, and in the input field **Policy name**, name the policy (for example use, *viz-now-deploy-infra-inline-policy*) and click **Create policy**.



Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

19. Associate the IAM Role in Viz Now:
 - a. Copy the role's ARN from the AWS Console.

viz-now-deploy-infra Info Delete Edit

Summary Creation date July 06, 2023, 12:14 (UTC+01:00) Last activity -	ARN  arn:aws:iam::[redacted]:role/viz-now-deploy-infra	Link to switch roles in console  https://signin.aws.amazon.com/switchrole?roleName=viz-now-deploy-infra&account=viznowtest
	Maximum session duration 1 hour	

- b. Over in Viz Now, in **Manage IAM Roles**, paste the ARN from the clipboard into the field **Deploy Role**.

Deploy Role ?

Management Role ?

Invalid ARN code

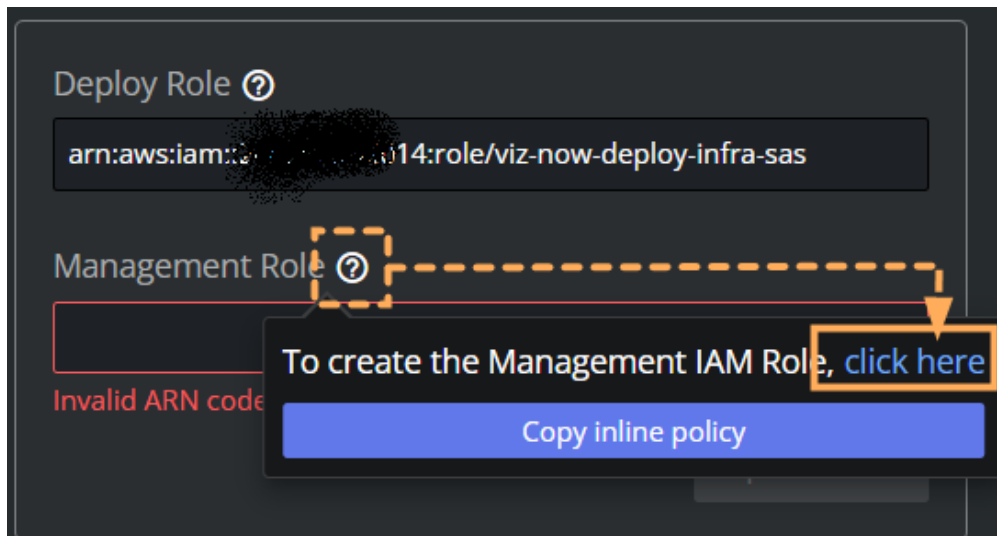
Cancel Update Roles

(The **Update Roles** button will be enabled only after filling the **Management Role** ARN in the next steps).

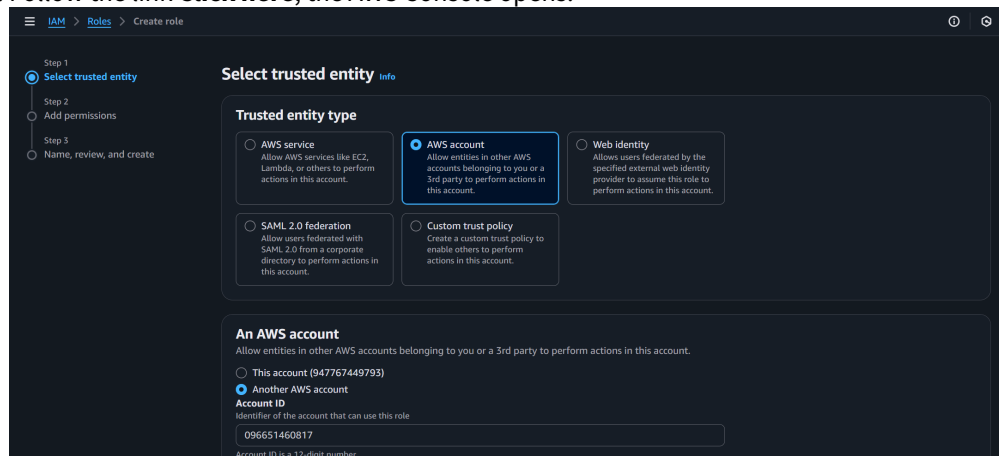
Management Role

The *viz-now-manage* role enables Viz Now to manage deployed instances and perform operational tasks.

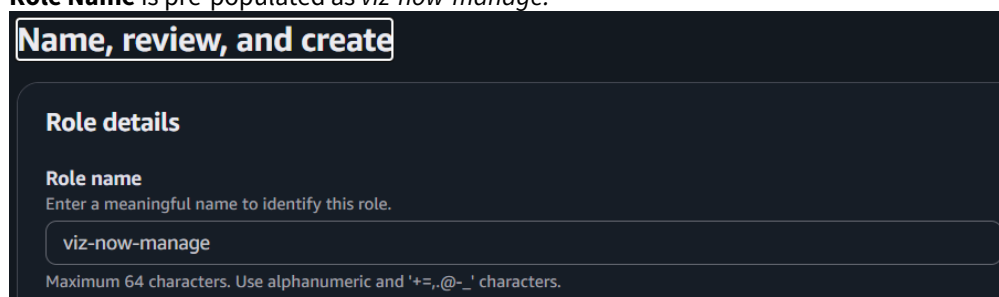
20. Still in the **Manage IAM Roles** menu, click the ? icon next to the input field **Management Role**.



- a. Follow the link **Click here**, the AWS Console opens.



- b. Click **Next** twice to skip the **Add permissions** step and arrive at the **Name, review, and create** menu. **Role Name** is pre-populated as *viz-now-manage*.

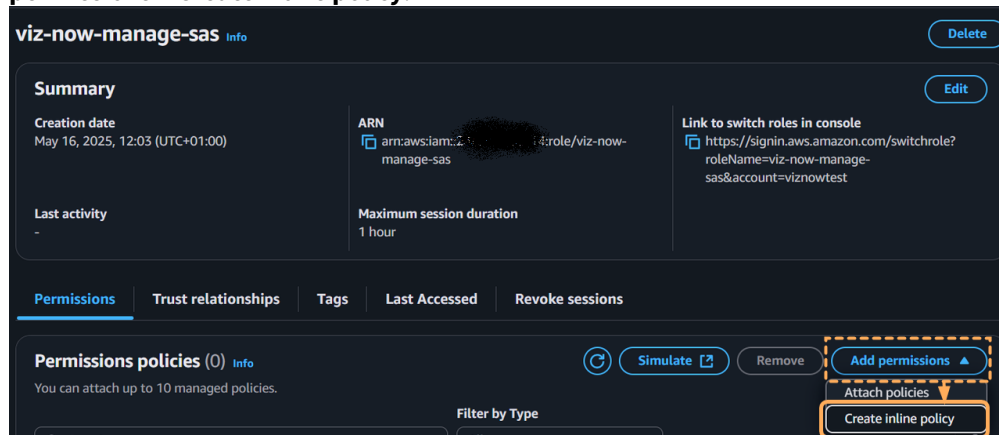


- c. Click **Create Role**.
Note: If a warning indicates that the name already exists, update it by adding a suffix, for example: *viz-now-manage-something else*.
d. Click **View role**.
A confirmation message is displayed:

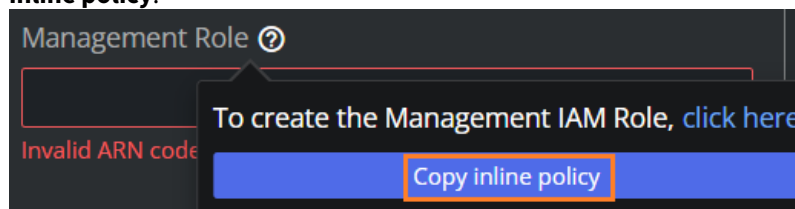


21. Add Inline permissions:

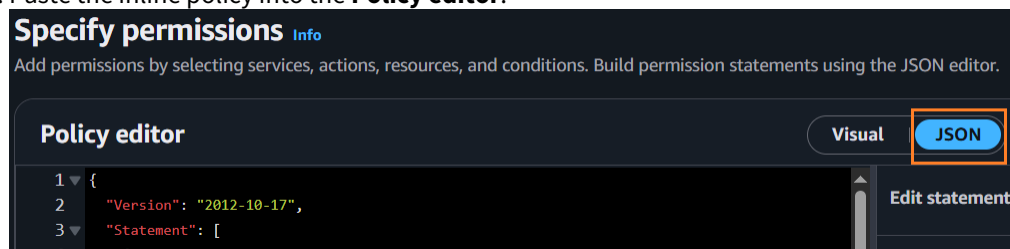
- a. Switch to the AWS console, and from the role's **Summary** page, click **Permissions** tab > **Add permissions** > **Create inline policy**.



- b. Go back to Viz Now, and next to the input field **Management Role**, click the **?** icon, then, **Copy inline policy**.



- c. Switch to the AWS console and click the **JSON** button.
- d. Paste the inline policy into the **Policy editor**.



- e. In the Editor, the pasted-in the JSON code will look like:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VizNowManage0",
      "Effect": "Allow",
      "Action": [
        "iam:*",
        "kms:*",
        "route53:*",
        "servicequotas:*",
        "s3:*",
        "ec2:*",
        "tag:*",

```

```

        "sts:*",
        "logs:*"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowSSMDocumentsForSendCommand",
    "Effect": "Allow",
    "Action": "ssm:SendCommand",
    "Resource": "arn:aws:ssm:*:*:document/*"
},
{
    "Sid": "AllowSendCommandToVizNowInstances",
    "Effect": "Allow",
    "Action": ["ssm:SendCommand"],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
        "StringEquals": {
            "ssm:ResourceTag/VizNow": "true"
        }
    }
},
{
    "Sid": "AllowCommandInvocationChecks",
    "Effect": "Allow",
    "Action": ["ssm:ListCommandInvocations",
"ssm:GetCommandInvocation"],
    "Resource": "*"
},
{
    "Sid": "AllowSSMInventoryReadOnly",
    "Effect": "Allow",
    "Action": ["ssm:ListInventoryEntries",
"ssm:DescribeInstanceInformation"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "ssm:ResourceTag/VizNow": "true"
        }
    }
},
{
    "Sid": "AllowCreateMediaConnectFlows",
    "Effect": "Allow",
    "Action": ["mediaconnect:CreateFlow"],
    "Resource": "*"
},
{
    "Sid": "AllowManageVizNowFlowsByName",
    "Effect": "Allow",
    "Action": [
        "mediaconnect:DeleteFlow",
        "mediaconnect:UpdateFlow",

```

```

        "mediaconnect:StartFlow",
        "mediaconnect:StopFlow",
        "mediaconnect:AddFlowOutputs",
        "mediaconnect:RemoveFlowOutput",
        "mediaconnect:UpdateFlowOutput",
        "mediaconnect:AddFlowSources",
        "mediaconnect:RemoveFlowSource",
        "mediaconnect:UpdateFlowSource",
        "mediaconnect:AddFlowVpcInterfaces",
        "mediaconnect:RemoveFlowVpcInterface",
        "mediaconnect:GrantFlowEntitlements",
        "mediaconnect:UpdateFlowEntitlement",
        "mediaconnect:DescribeFlow",
        "mediaconnect:ListEntitlements"
    ],
    "Resource": "arn:aws:mediaconnect:*:*:*VizNow-*"
  },
  {
    "Sid": "AllowListMediaConnectFlows",
    "Effect": "Allow",
    "Action": [
      "mediaconnect:ListFlows",
      "mediaconnect:DescribeFlow",
      "mediaconnect:ListTagsForResource"
    ],
    "Resource": "*"
  }
]
}

```

- f. Click **Next**, and in **Policy name**, provide an identity for the policy (for example, use: *viz-now-manage-inline-policy*), and then click **Create policy**.

Policy details


Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.

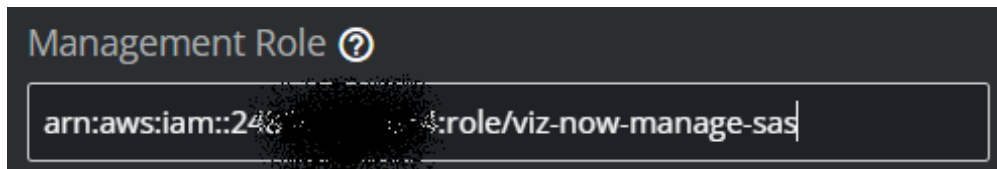
22. Associate and update the IAM Role in Viz Now:

- a. Copy the role's ARN from the AWS Console on the **Summary** page.

Summary

Creation date May 16, 2025, 12:03 (UTC+01:00)	ARN  arn:aws:iam::241111111111:role/viz-now-manage-sas
Last activity -	Maximum session duration 1 hour

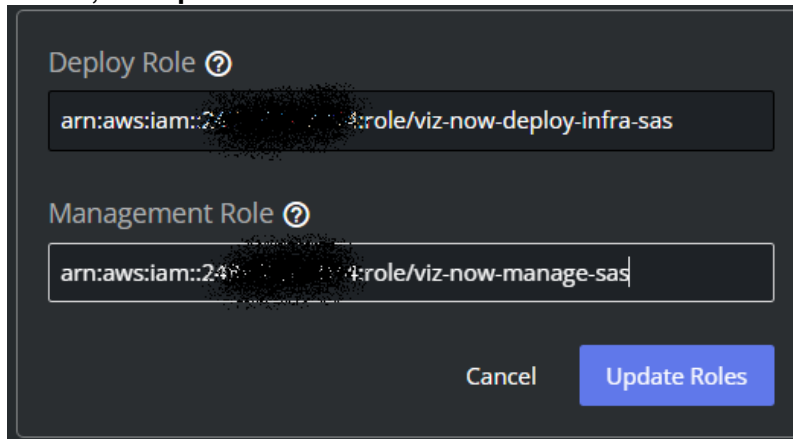
- b. In Viz Now **Manage IAM Roles** panel, paste the ARN in **Management Role** field.



Management Role ?

arn:aws:iam::246...:role/viz-now-manage-sas

c. To save, click **Update Roles**.



Deploy Role ?

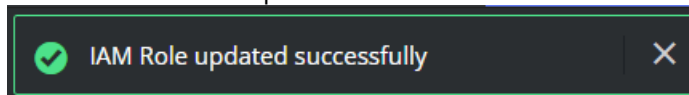
arn:aws:iam::246...:role/viz-now-deploy-infra-sas

Management Role ?

arn:aws:iam::246...:role/viz-now-manage-sas

Cancel Update Roles

d. Viz Now validates the updated roles:



✓ IAM Role updated successfully ✕

3 Working with Deployed Apps

Any user can access the Apps within a Space that they created or are assigned to. There are different ways to interact with an App depending on the defined App properties.

- [Region and Availability Zone](#)
- [Allowed IP](#)
- [Virtual Windows Instance Apps](#)
- [Web Apps](#)

3.1 Region and Availability Zone

It can be useful to specify region and zone to

- Peer with an internal VPC
- Use a region that is not the default one.

If you have Editor rights, the target Region and Availability Zone for the deployment can be specified before its deployed.

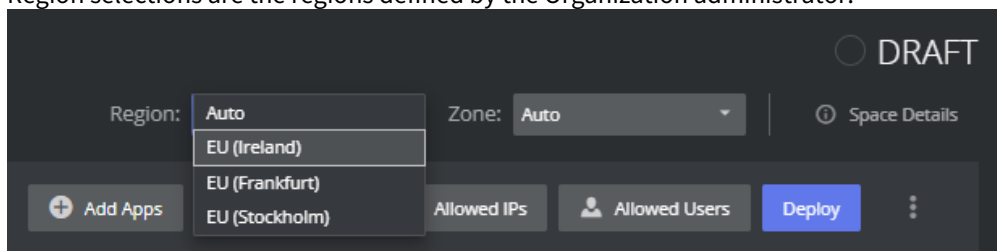
Note: Specifying Region and Availability Zone only works for spaces in DRAFT mode.

- If no selection is made, the deployment uses the prioritized list already configured by the administrator.

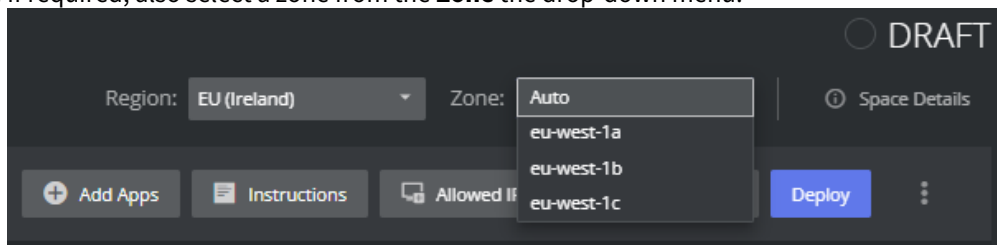
3.1.1 To select a Region and Availability Zone

This is an *optional* procedure.

1. While in DRAFT mode, select a *region* from the **Region** drop-down menu. Region selections are the regions defined by the Organization administrator.



2. If required, also select a zone from the **Zone** the drop-down menu.



If no specific Zone is defined the first in the list is used.

3.2 Allowed IP

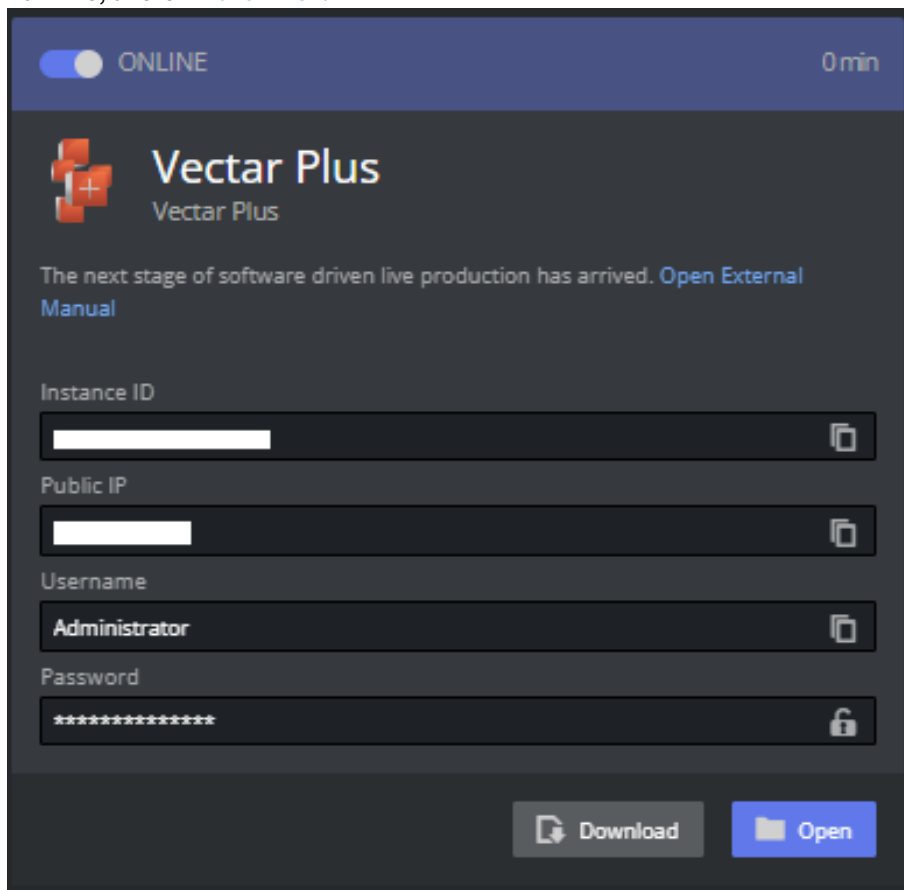
To be able to access any app your public IP must be whitelisted. This should happen automatically when clicking the buttons on the App.

- If you have Editor rights to a Space, the IPs that have been allowed, can be viewed and edited by selecting the **Allowed IP** menu from the Space.
- If an IP is removed, the user behind the IP will no longer have access.

3.3 Virtual Windows Instance Apps

Apps that are installed on virtual windows instances (for example, Viz Vector Plus), require the user to log into the App session, using a third party remote desktop client.

- For AWS, this is [Amazon DCV](#).



3.3.1 Amazon DCV Client Software

The Amazon DCV client software has to be installed on the local machine before the user is able to access the instance. If the software is installed the user can download a small shortcut script that opens the remote session.

1. Click the download button. This will download a *.dcv* shortcut file that can be saved (for example, onto your desktop). If the Amazon DCV client application is installed on your machine, this automatically logs you in. You may rename it to something that makes sense to you.



Note: Keep the *.dcv* file *secure*, it contains the credentials needed to log into the App.

2. Click **Open file** in the browser (usually upper right corner).

Web Browser-based Amazon DCV

Amazon DCV can also be opened in a browser window. You will not get the same low latency benefit with this approach but works well when inspecting Apps.

1. Click the **Open** button
2. Viz Now will copy the password to your clipboard (you might need to allow this)
3. A new browser will be opened
4. Paste the password into the Log in menu and connect

3.4 Web Apps

For apps that are accessible via a browser, a corresponding link is displayed.

See Also

- [Amazon DCV | Download \(Amazon-dcv.com\)](#)

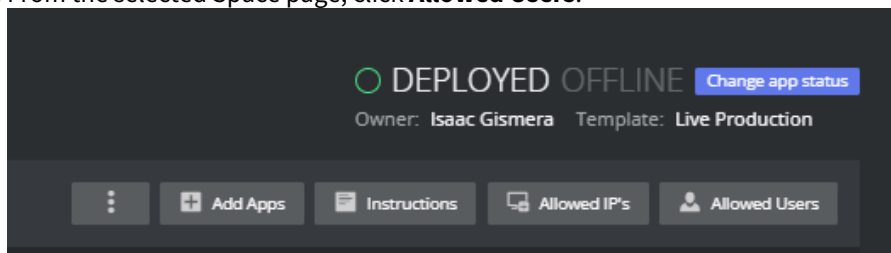
4 Working with Users

4.1 Assigning Users

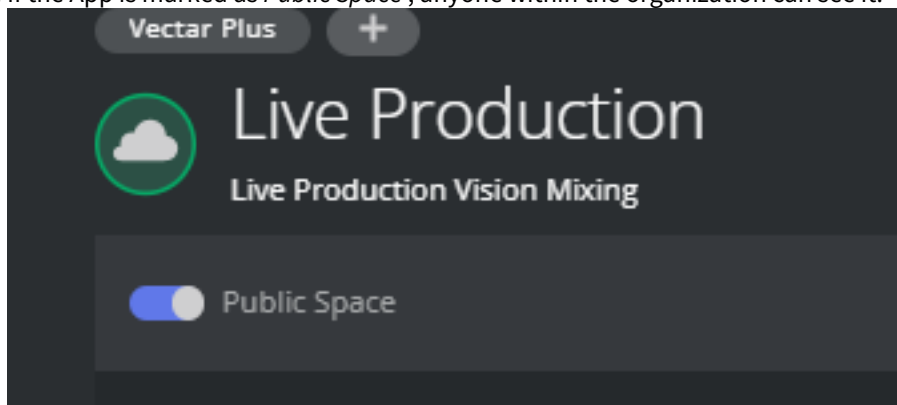
When you create a Space it is by default only visible to you and the Administrators, but it is possible to assign other users to your Space.

4.1.1 To assign a User to your Space

1. From the selected Space page, click **Allowed Users**.



2. You can add and remove other users to let them see and access your installed Apps.
If the user is an *Operator*, they can only access the Apps and can not change your Space.
3. If the App is marked as *Public Space*, anyone within the organization can see it.

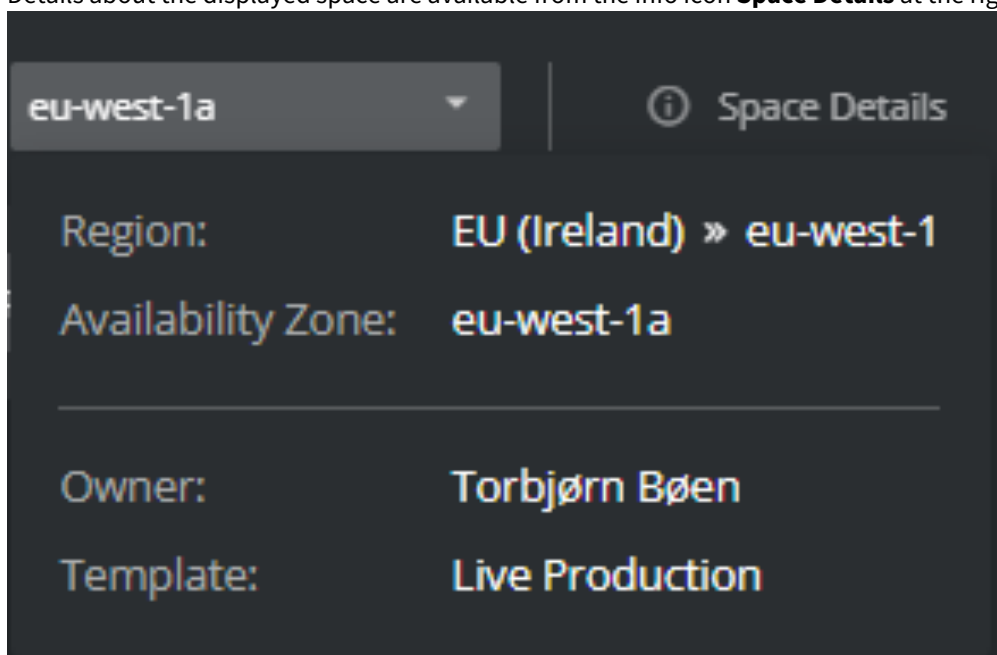



5 Working with Spaces

- [Space Details](#)
 - [Creating and Deleting a Space](#)
 - [Creating a Space](#)
 - [Deleting a Space](#)
 - [Session Scheduling](#)
 - [Start and End Times](#)
 - [Auto-Shutdown](#)
 - [AWS Tags](#)
 - [Custom Tags](#)
 - [Mandatory Tags](#)
 - [Organization Tags](#)
 - [Cost Allocation Tags](#)
-

5.1 Space Details

- Details about the displayed space are available from the info icon **Space Details** at the right corner.



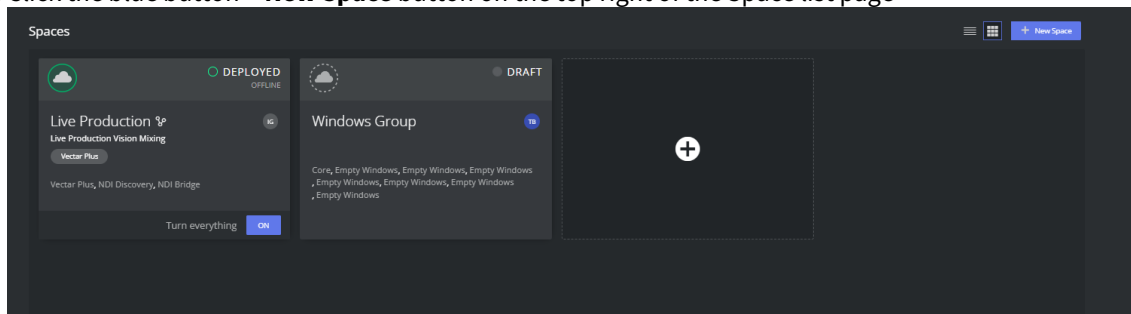
 **Note:** Users with the Editor role can select the desired region to deploy, as described in section [Region and Availability Zone](#).

5.2 Creating and Deleting a Space

5.2.1 Creating a Space

To create a new Space

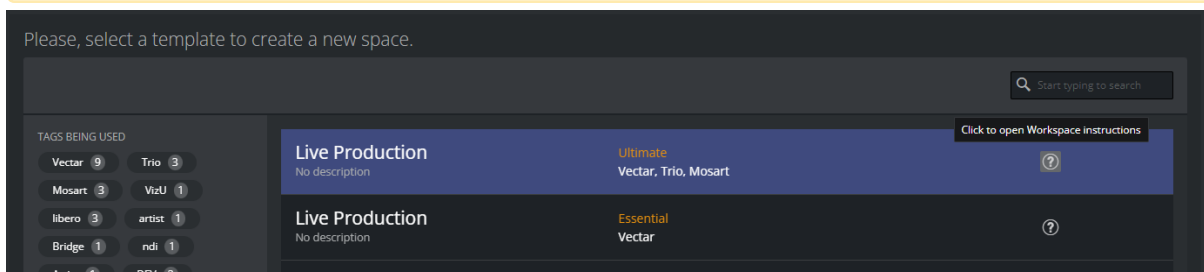
1. Either
 - a. Click the blue button **+ New Space** button on the top right of the Space list page



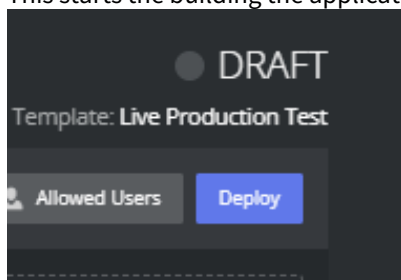
or

- b. Click on the big **+** (**Plus sign**) within a box if you are using the *box* view.
2. Choose your template.
The template determines which apps can be deployed.

Note: Refer to the [Viz Now Administrator Guide](#) for more details about *Templates*.



3. Click the **Question mark** to open instructions for the template.
4. When the Space is created select which apps should be part of the Space by clicking the **Add Apps** menu.
5. From the popup menu the available apps can be selected.
6. When the all required apps are selected, click **Deploy**.
This starts the building the application on your account.



7. The operation takes 10-15 minutes.

5.2.2 Deleting a Space

A space that has been created and deployed incurs costs. Instances that are *running* are much more costly than when they are off. However there are *still* charges for instances that are off, especially if they have large disks.

It is therefore recommended that instances are destroyed when they are no longer in use.

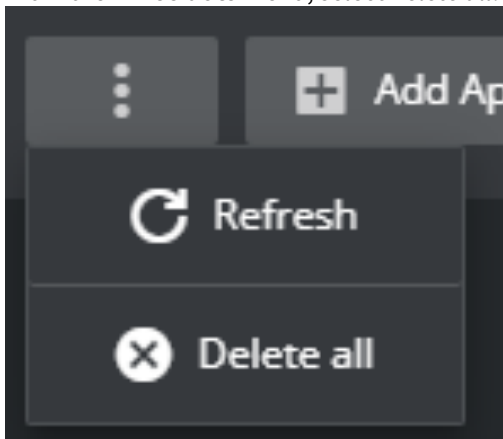
Note: You must first perform a **Delete all** before a deployed space can be deleted.

- **Delete all:** All virtual instances that Viz Now has deployed are deleted from the Cloud Account. All configurations are lost but the space itself is not yet deleted from Viz Now database.
- **Delete:** The space is deleted from the Viz Now database.

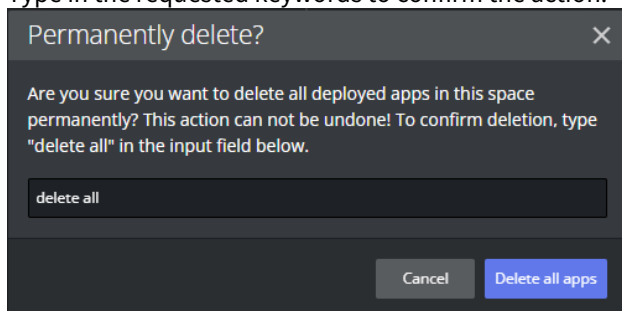
To delete all content deployed in a Space

This removes all virtual machines and storage. Make sure you have saved any work elsewhere before doing this.

1. Open the space you want to delete (must be *Deployed*).
2. From the **Three dots** menu, select *Delete all*.

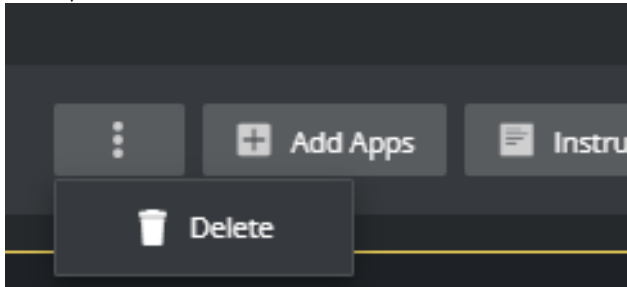


3. A popup box warns about permanent actions. Type in the requested keywords to confirm the action.

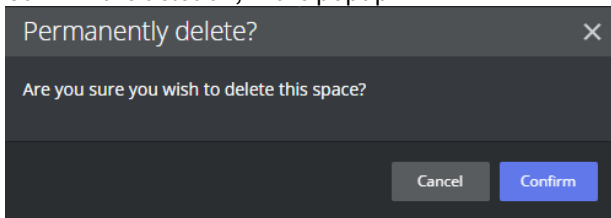


To delete a Space

1. To completely delete the Space references from Viz Now, select **Delete** (available if the Space is in *Draft* mode).



2. Confirm the deletion, in the popup



5.3 Session Scheduling

Viz Now users with *Editor* or *Administrator* roles can define their spaces' up-time. This feature ensures that the apps are accessible during specific hours on designated days and helps prevent unexpected costs that may arise from users forgetting to turn off their apps.

This feature covers *all* apps within a space, it does address the individual apps in a space.

Both assigned users and the space owner receive a notification 30 minutes prior to Viz Now forcibly shutting down the apps.

This advance notice is intended to provide users with ample time to manually shut down their systems, the recommended course of action.

5.3.1 Start and End Times

By predetermining the activation and deactivation time of a space, users can plan in advance exactly when the space should be operational or not available.

To schedule space start time and end time

1. Navigate to the target Viz Now Space for scheduling.
2. From the **Scheduler settings** menu, fill-in the checkbox **Schedule session**.
Select **Start time** and **End time** by clicking the **Calendar** icon.
The estimated shutdown time is displayed.

Scheduler settings

☒ **Schedule session**

You can program a start date so the space goes online automatically and an end date so it goes offline.

Start time: 07 Nov 2024 13:00 07 Nov 2024, 12:00 UTC

End time: 07 Nov 2024 16:00 07 Nov 2024, 15:00 UTC

☐ **Enable auto-shutdown**

Auto-shutdown helps you control your infrastructure cost. The service will go offline after the period defined.

Estimated shutdown: After 3h 0min of uptime

Cancel Confirm

3. Click **Confirm** to apply your settings.

5.3.2 Auto-Shutdown

An unused space that is still running, generates unnecessary operating costs on the users' AWS account. Auto-shutdown provides an optional safeguard to autonomously place unused resources offline.

Users can:

- Specify the duration that a Space is expected to remain active.
- Optionally enable the advanced auto-detect feature *Shutdown only when inactivity is detected over 30 minutes*, for added security.

When this feature is activated, the instance remains operational until there is no outgoing data detected for 30 minutes.

- If there are no active streams or remote connections to the app within this timeframe, the system will automatically shut down.
- This helps ensure that the instance does not power-off while still in use.

To schedule auto-shutdown

Users that will only run Apps for a certain amount of hours, can configure the Auto-shutdown feature. This feature initiates a stopwatch after the last App is turned on and then turns off everything after the chosen time elapses.

1. Navigate to the target Viz Now space.
2. From the **Scheduler settings** menu, fill-in the checkbox **Enable auto-shutdown**.

Scheduler settings

☒ **Schedule session**

You can program a start date so the space goes online automatically and an end date so it goes offline.

Start time: 07 Nov 2024 13:00 07 Nov 2024, 12:00 UTC

End time: 07 Nov 2024 16:00 07 Nov 2024, 15:00 UTC

☐ **Enable auto-shutdown**

Auto-shutdown helps you control your infrastructure cost. The service will go offline after the period defined.

Estimated shutdown: After 3h 0min of uptime

Cancel Confirm

3. In section **Shutdown after *n:nn* hrs of uptime**, use the slider to specify how many hours your space is expected to run.
The estimated shutdown time is displayed.
4. Optionally enable the **Shutdown only when inactivity is detected over 30 minutes** safeguard option mentioned above.
5. Click **Confirm** to apply your settings.

Note: It is advised to avoid using this option during a live broadcast, to prevent unexpected shutdowns if the show runs longer than anticipated.

5.4 AWS 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](#).

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.

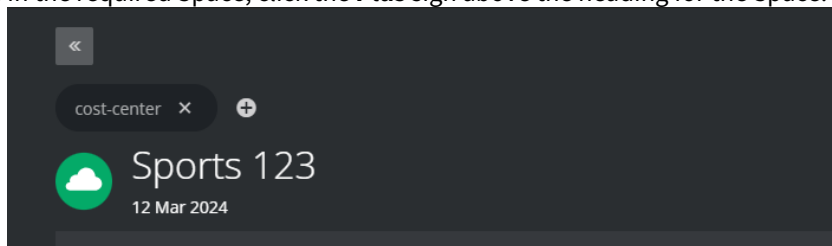
Note: The Organization Administrator can define *mandatory* Tags to comply with AWS Tag Policies and ensure that specific tags are always included. See the [Viz Now Administrator Guide](#), section *Organization*.

5.4.1 Custom Tags

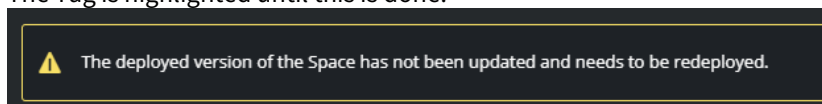
Adding custom tags to a Space enables distinguishing a particular Space from other resources. It also clarifies what the Space is used for.

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.

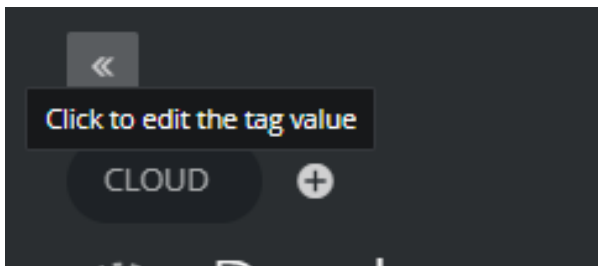



5.4.2 Mandatory Tags

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

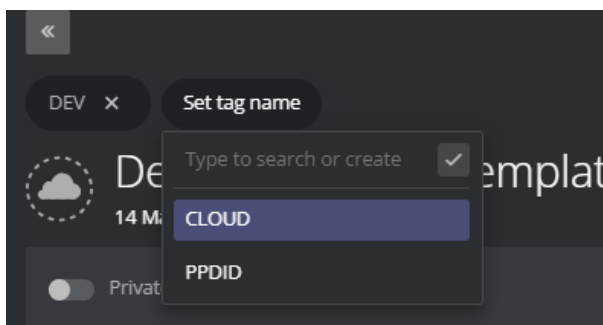
1. Click on the required tag.



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

5.4.3 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.

5.4.4 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 \(amazon.com\)](https://aws.amazon.com/billing/latest/using-cost-allocation-tags/)

6 Capacity Management

6.1 Best Practices for Instance Provisioning and Workflow Resilience

Efficient management of cloud infrastructure is critical for maintaining performance, cost control, and operational predictability in live production environments.

Viz Now introduces tools and flexibility to give users greater visibility and control over how compute resources such as EC2 instances are provisioned and consumed.

While Viz Now automates much of the heavy lifting during deployment, cloud infrastructure behaves differently than traditional on-prem setups. Instance availability can fluctuate, quotas may be limited, and GPU resources are often region-specific or subject to supply constraints. Therefore, proactively managing your capacity strategy is essential.

In this section, we'll walk through key strategies to:

- Plan and reserve compute capacity for mission-critical workflows using default Viz Now Targeted Capacity Reservations
 - Understand Guided Retry and Fail-Fast Deployment to avoid mid-process launch failures
 - Interpret Visual Indicators to assess deployment capacity status in real time
 - Leverage BYOC (Bring Your Own Capacity) to manually assign long-term reserved capacity
 - Change EC2 Instance Types dynamically to adapt to availability and cost constraints
 - Switch Regions or Availability Zones to bypass regional shortages
 - Collaborate with AWS TAMs to understand capacity trends and proactively plan deployments.
-

6.2 Capacity Management Strategies for Resilient Cloud Deployments:

- [Default Behavior: Targeted Capacity Reservations](#)
- [Guided Retry and Fail-Fast Deployment](#)
- [Visual Indicators for Capacity Status](#)
- [Bring Your Own Capacity \(BYOC\)](#)
- [Changing EC2 Instance Type of an Application](#)
- [Switching Availability Zone or Region to Resolve EC2 Scarcity](#)

These best practices are designed to help you make informed decisions when deploying Viz Now spaces and ensure your production is not impacted by unexpected resource shortages.

6.3 Default Behavior: Targeted Capacity Reservations

To increase reliability during deployments and lifecycle operations (such as scaling or relaunching), Viz Now use **Targeted Capacity Reservations (CRs)**. These are short-lived reservations created and managed by Viz Now to secure the required EC2 capacity at launch time.

6.3.1 Why This Matters

EC2 GPU instances are in high demand and can be scarce, especially in select regions or during peak usage periods. By default, Viz Now improves your chances of successful launches by creating temporary, targeted capacity reservations scoped specifically to the instance types, availability zone, and resource needs of your space.

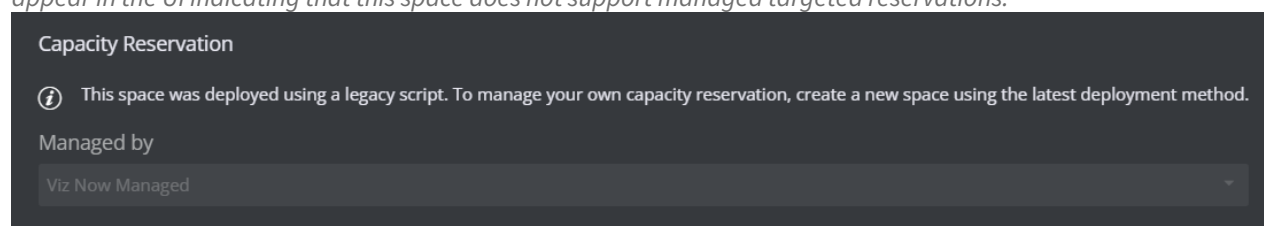
These targeted CRs:

- Provide **isolation from general on-demand pools**, reducing deployment failure risk
- Attempt to secure **resource availability at the moment of launch**, however success depends on the ability to create the targeted reservation. If capacity is not available, Viz Now will inform the user and allow them to decide how to proceed (details covered later).
- Are **ephemeral**, typically retained for a short duration (for example, 20 minutes) to support post-launch stability and cleanup.

6.3.2 Important Notes

- This feature only applies to **spaces deployed using the latest deployment packages**.
- Spaces created using **legacy deployment scripts** (prior to this feature rollout) rely on open reservation pools, which may lead to **contention** or **misallocation**.

i *If a user attempts to configure capacity reservation options in an unsupported (legacy) space, a warning will appear in the UI indicating that this space does not support managed targeted reservations.*



To take full advantage of these capacity reservation improvements, we recommend **creating new spaces** using the latest deployment packages.

6.4 Guided Retry and Fail-Fast Deployment

6.4.1 Capacity Check & Reservation Feedback



In Viz Now, the deployment process includes a smarter pre-launch validation step that checks whether **Targeted Capacity Reservations (CRs)** were successfully allocated for all required EC2 instances.

Rather than proceeding blindly and encountering AWS errors midway through deployment, Viz Now now enters a **deploy-pending** state whenever CR issues are detected **before EC2 launch**.

This proactive step improves transparency and control.

6.4.2 What the User Sees




When capacity reservation issues are detected, Viz Now displays a **Capacity Check** dialog that includes:

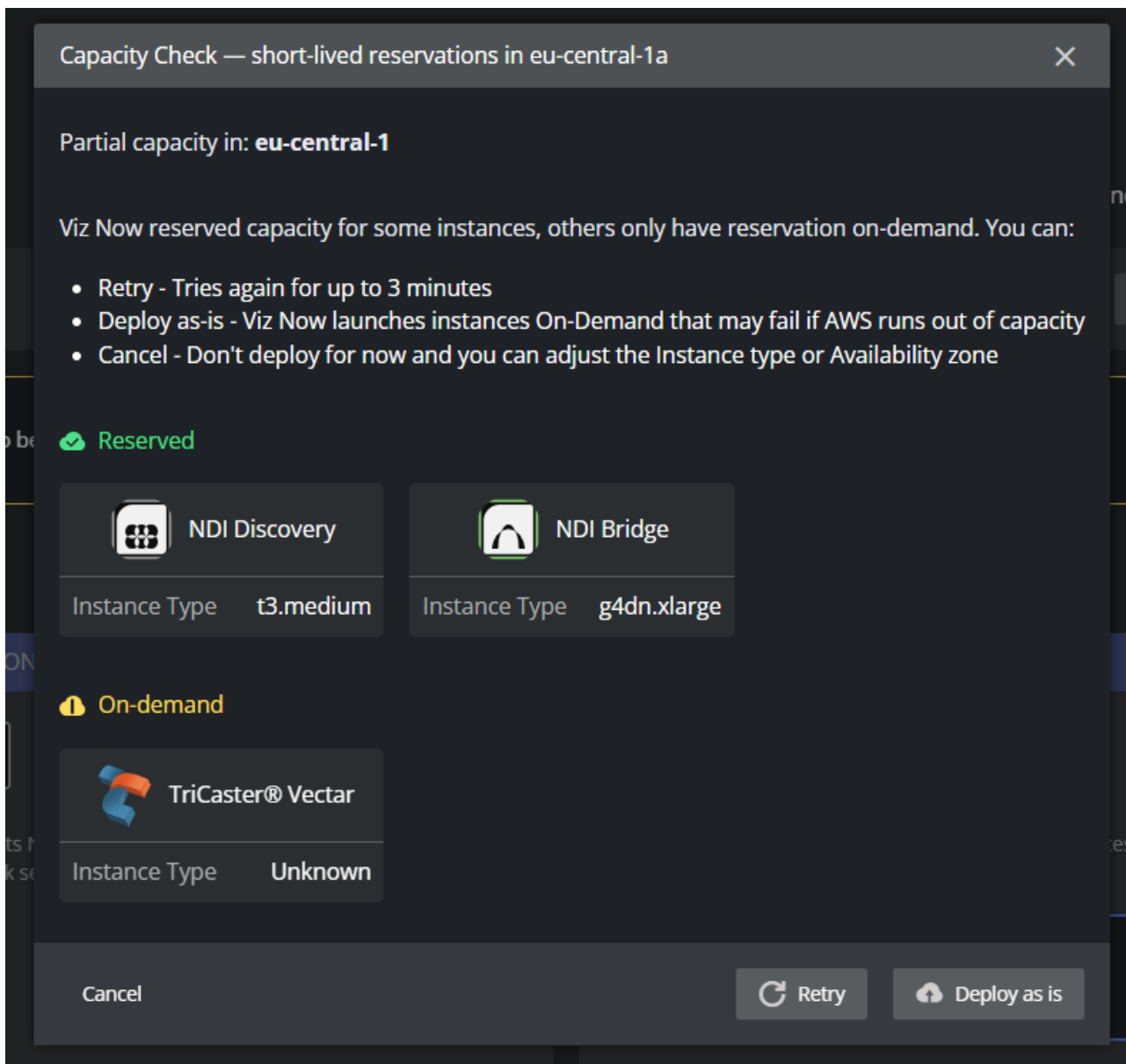
-  A list of **instances successfully matched** to short-lived reservations
-  A list of **instances that could not secure a reservation** (e.g., due to regional capacity constraints)

Each instance is clearly marked with its reservation status (*Reserved / On-Demand fallback*), along with the **instance type** and **function**.

6.4.3 Your Options: Guided Response

Users can choose how to proceed based on current availability:

-  **Retry**: Viz Now will attempt to reserve capacity again for up to 3 minutes
-  **Cancel**: Stop the deployment and return to the Configuration phase
-  **Deploy as-is**: Proceed using On-Demand EC2 instances for any unmatched components
(Note: This increases the risk of AWS capacity errors during launch).



6.4.4 Why It Matters

This approach removes guesswork and avoids silent deployment failures by:

- Making the **reservation status visible** before launch
- Providing users with **informed control** over how to handle shortages
- Supporting fast troubleshooting without manual digging through AWS logs or support tickets.

6.5 Visual Indicators for Capacity Status

To improve transparency and operational awareness, Viz Now uses **visual indicators** at both **App** and **Space** levels, that reflect the capacity status of your deployment.

These indicators help you quickly understand whether apps are backed by reserved capacity or are relying on standard On-Demand EC2 behavior.

6.5.1 App-Level Indicators

Each deployed app displays:

- **Reserved:** Indicates the instance is covered by an active targeted capacity reservation
- **On-Demand:** Indicates the instance is running without a reservation (higher risk of AWS capacity failure)
- **Time Remaining:** If reserved, the UI shows how long the reservation remains valid.

This provides users with precise insight into which components of their workflow are most secure from capacity interruptions.

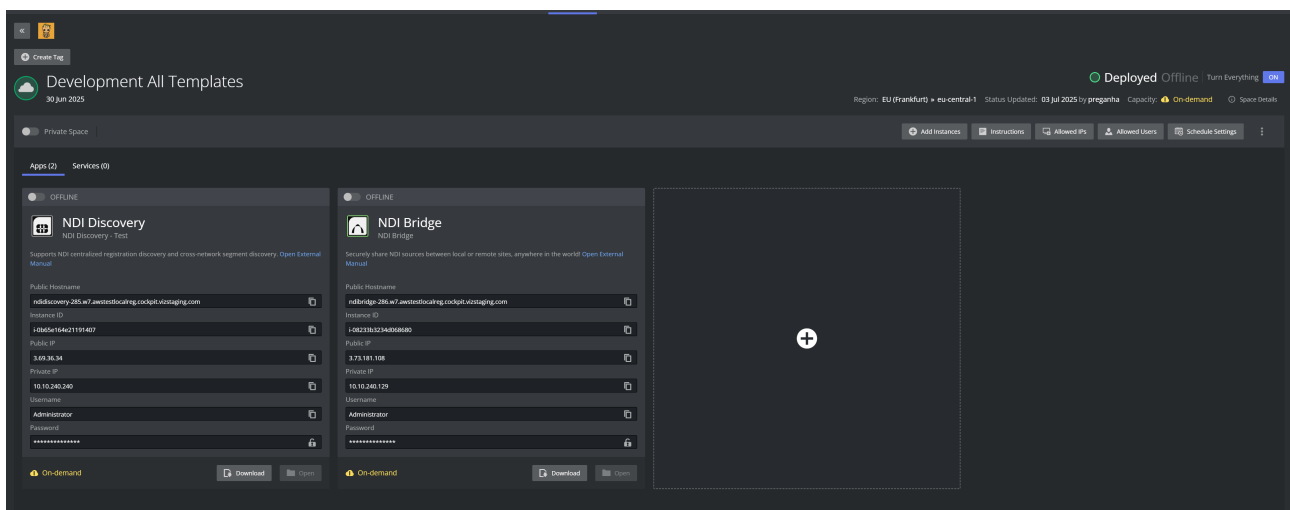
6.5.2 Space-Level Summary Indicator

At the top-right of the Space, a unified status label summarizes overall capacity:

- **On-Demand:** All apps in the space are running without capacity reservations
- **Partially Reserved:** Some apps are running with active reservations, others are not
- **Fully Reserved:** All apps are backed by active reservations.

This top-level overview allows users to:

- Assess deployment risk at a glance
- Know when action might be needed (for example, re-reserve capacity, relaunch with fallback)
- Track improvements from retry logic or new reservation attempts.



6.6 Bring Your Own Capacity (BYOC)

6.6.1 Overview

Viz Now supports **Bring Your Own Capacity (BYOC)**, enabling users to override the default short-lived capacity reservation mechanism and instead attach **pre-existing AWS Capacity Reservations** directly to individual apps.

This is especially beneficial for:

- Customers with **long-term Reserved Capacity** (for example, one or three year term CRs)
- Workloads that rely on **scarce or highly requested instance types**
- Organizations with internal **cost tracking, security policies, or lifecycle governance** that require tighter control over cloud allocation.

How It Works

For each app, within the **App Details** window, in the **Instance Type** section, users can select:

- *Viz Now Managed* (default, using ephemeral CRs)
- *Use my reservation* (manual assignment of an existing CR ID).

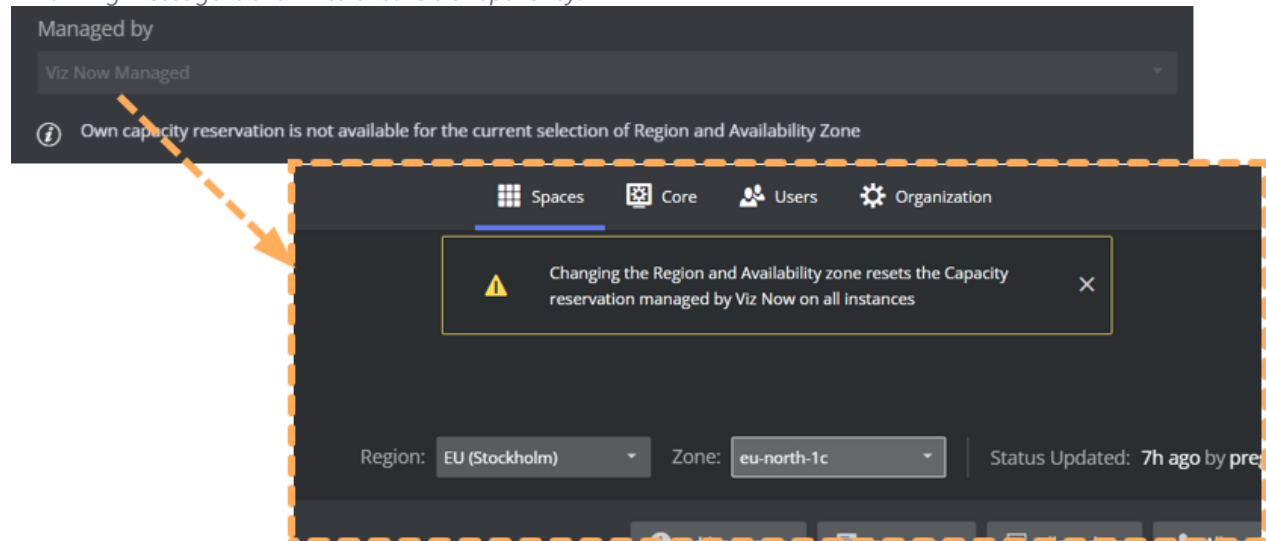
When BYOC is selected:

- A dropdown menu will show compatible reservations filtered by Region, Availability Zone, and Instance Type
- If no valid CR is found, Viz Now will alert the user and fallback to On-Demand.

Requirements

- ☒ **Region and Availability Zone must be explicitly set** in the space configuration, since CRs are zone-specific.
- **!** This feature is only available for **draft spaces that have both Region and Availability Zone explicitly specified**. Draft spaces without this configuration will not support BYOC.

Note: If you later change the Region or AZ of the space, any BYOC configuration will reset to **Viz Now Managed**. A warning message is shown to ensure transparency.



UI Behavior

- When no CRs are detected for the selected parameters, the message: *There's no available reservations for the Region, Availability Zone and Instance type configured* is displayed
- If the Region/AZ combination doesn't support BYOC, the selector will be disabled with a message: *Own capacity reservation is not available for the current selection of Region and Availability Zone*.

Creating a Compatible Capacity Reservation in AWS

To bring your own Capacity Reservation into Viz Now, you must create a **targeted CR** in AWS that meets specific **tagging and configuration requirements**.

Tagging and Configuration Requirements Overview

Requirement	Description
Targeted CR	Reservation must target a specific Availability Zone (AZ)
Tag: VizNow:true	Required to make the reservation visible in Viz Now
Matching Instance Type	Must match the instance type used by the Viz Now app (e.g., g4dn.xlarge)
Matching Platform	Must match platform (e.g., Windows, Linux/UNIX)
Region	Must be in the same region selected in Viz Now

Requirement	Description
Availability Zone	Must match the one selected in the Viz Now UI
Instance Count	Should match or exceed the number of app instances expected

i **Info:** Creating reservations is done through the AWS Console / AWS CLI. For step-by-step AWS instructions, consult the AWS documentation on EC2 Capacity Reservations.
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/capacity-reservations-create.html>

Verifying the Reservation

To verify a reservation in Viz Now

Once your CR is created:

1. Open Viz Now and navigate to your **Space**
2. Select the relevant **App**
3. Change **Managed by** from *Viz Now Managed* to *Use my reservation*
4. Select your CR from the dropdown menu.

If your reservation does **not appear**, check:

- Tag is present (`VizNow:true`)
- Region and Availability Zone match
- Instance Type and Platform are correct
- The CR is in **active** state.

6.7 Changing EC2 Instance Type of an Application

6.7.1 Overview



Viz Now applications are certified to run on multiple EC2 instance types, giving users flexibility when responding to **capacity scarcity** or tuning performance to match their production needs.

Each certified instance type is evaluated for:

- Functional compatibility with the application
- Expected performance and bandwidth usage
- Cost-efficiency for different workloads.

6.7.2 Why Change the EC2 Instance Type?

When EC2 capacity is limited or reservations cannot be allocated, switching to a different instance type is a viable strategy. You can:

-  **Upsize** to a more powerful instance to increase availability (higher cost)
-  **Downsize** to a more accessible instance, but you may need to reduce workload or disable features.

Best Practice

Live production workloads benefit from continuous performance monitoring. AWS provides CloudWatch and other observability tools to:

- Track CPU, memory, network throughput
- Identify bottlenecks in real-time
- Trigger alerts for performance degradation.

This data can inform instance size decisions based on actual load.

6.7.3 How to Change EC2 Instance Type in Viz Now

Viz Now makes instance switching easy; no need to redeploy the space. Just follow the steps below:

To change EC2 instance type

1. Go to your deployed **Application** panel
2. Click **Manage Instance Types**
3. In the **Add Instance Type** field, select a compatible type (for example, *g4dn.2xlarge*, *g4dn.8xlarge*)
4. To add the instance type to the list, press the **+ Plus** button
5. In the list, click **Choose to deploy** on the instance type you want to activate
6. Click **Save & Deploy** to apply the change.

The app will automatically redeploy itself on the new instance type.

Review the app details before the deployment

TriCaster@ Vectar
TriCaster@ Vectar

Pre-deployment settings

☐ Customize root volume C: size in GB (default 100 GB)

☒ Set the volume size for the clip drive (D:) in GB
5 GB 500 GB

☒ Set the volume size for the recording drive (E:) in GB
5 GB 500 GB

Instance Type

You can add new Instance types or set the deployed instance here. After making and saving changes, the app will automatically deploy.

Instance Types

g4dn.2xlarge

Manage Instance Types

Capacity Reservation

This space was deployed using a legacy script. To manage your own capacity reservation, create a new space using the latest deployment method.

Managed by
Viz Now Managed

Capacity **On-demand**

Settings

☒ Live Panel Password

Username: admin

*2RbfzTnHvfwveCmzRz

Cancel Delete Save

Review the app details before the deployment

TriCaster@ Vectar
TriCaster@ Vectar

Pre-deployment settings

☐ Customize root volume C: size in GB (default 100 GB)

☒ Set the volume size for the clip drive (D:) in GB
160 GB 500 GB

☒ Set the volume size for the recording drive (E:) in GB
300 GB 500 GB

Instance Type

You can add new Instance types or set the deployed instance here. After making and saving changes, the app will automatically deploy.

Instance Types

g4dn.2xlarge Choose to deploy

g4dn.8xlarge Choose to deploy

Add Instance Type

Cancel Save & Deploy

Capacity Reservation

This space was deployed using a legacy script. To manage your own capacity reservation, create a new space using the latest deployment method.

Managed by
Viz Now Managed

Capacity **On-demand**

Settings

☒ Live Panel Password

Username: admin

*2RbfzTnHvfwveCmzRz

Cancel Delete Save

6.7.4 Important Notes

- You can change instance types **before or after deployment**
- Compatibility is validated by Viz Now - only certified instance types are accepted
- If using **BYOC**, make sure your reservation matches the newly selected instance type
- Switching instance types can trigger **billing changes**; be sure to review AWS pricing.

6.7.5 Summary

Instance type flexibility in Viz Now gives you another tool to ensure production continuity, even under regional cloud capacity stress. Monitor performance, choose wisely, and adapt dynamically.

6.8 Switching Availability Zone or Region to Resolve EC2 Scarcity

6.8.1 Overview

When EC2 instance capacity is unavailable in the selected Availability Zone (AZ) or Region, Viz Now users have the option to move their workloads to an alternate location where resources are available.

This strategy can help maintain service continuity by avoiding congested zones or regions, especially when dealing with GPU-intensive or high-demand instance types.

6.8.2 Options for Relocating Workloads

Move Entire Deployment

Viz Now does not currently support changing the Region or AZ for an existing space. To move your entire deployment, you must:

- Create a **new Viz Now space** in the target Region and Availability Zone
- Re-deploy all required applications in the new space
- Manually reconfigure capacity applications and reservations.

Move a Single Application

You may also split your workload across locations:

- Deploy a new Viz Now space in a different AZ or Region
- Use the **VPC Peering Tool** to connect the new space with your existing one
- Allow inter-space communication between apps (for example, using *NDI Discovery*)

 **Note:** When separating apps across zones or regions, ensure connectivity requirements are fully validated.

6.8.3 Considerations and Tradeoffs

Network Latency

- Performance-sensitive apps (for example, live video, replay) may experience latency if apps are spread across distant locations
- Delay settings may need to be adjusted.

Cost Implications

- **Intra-region AZ traffic** may incur additional data transfer charges from AWS
- Long distance Region-to-Region traffic is usually billed at a higher rate.

Best Practices

- Monitor performance after migration
 - Use availability forecasts or historical insights from AWS to guide decisions - consider leveraging your AWS Technical Account Manager (TAM) to gain early visibility into capacity trends and regional constraints
 - Keep production-critical services together in the same location whenever possible.
-

6.8.4 Summary

Choosing an alternate AZ or Region is a valuable fallback strategy when managing scarce EC2 resources in Viz Now. With proper configuration and awareness of the tradeoffs, this can help ensure smooth, uninterrupted production workflows.

7 Security Overview

7.1 Introduction

The deployment of cloud-based live production workflows using Viz Now involves the automated provisioning of various AWS resources, such as EC2 instances, security groups, IAM roles, VPCs, and storage components. These resources are created directly in your AWS account, enabling and maintaining full customer control and ownership.

While Viz Now provides a strong foundation and starting point in terms of security posture, it is ultimately the responsibility of you, the customer, to ensure that these resources are properly secured according to organizational security policies and operational needs.

We **strongly recommend** referring to AWS security best practices and documentation for each service involved in a Viz Now deployment. Customers should review and, if necessary, adapt the configurations post-deployment, to align with their internal security standards, compliance frameworks, and threat models.

7.1.1 Our Commitment to Secure Defaults

Viz Now is being continuously improved to offer:

- **More secure-by-default templates** for deployments.
- **Optional security configurations** during setup.
- **Transparent documentation** of ports, protocols, IAM permissions, and network exposure.


This section presents

- [Viz Now IAM Role Setup & Permissions Guide](#)
- [Network Security and Default Port Configuration](#)

It provides:

- A detailed list of **network ports and protocols** opened by default.
- An overview of **IAM permissions** used by Viz Now roles.
- Important **warnings about manual changes** that may be overwritten during redeployment.
- Suggestions for **enhancing your security posture** based on your infrastructure setup and use case.

We will continue to evolve this section with updated recommendations, configurable options, and integration best practices.

 **Info:** If you have specific security requirements or constraints, we encourage you to contact our team to discuss how Viz Now can best be configured for your environment.

7.2 Viz Now IAM Role Setup & Permissions Guide

This section guides you through management of AWS IAM roles needed for operating Viz Now with your AWS account.

Secure, reliable operations are ensured by first clarifying permissions and adopting these best practices.

- [Overview](#)
- [Prerequisites](#)
- [Update Existing IAM Roles](#)
- [Permissions Explained](#)

7.2.1 Overview

Viz Now requires *two* IAM roles:

IAM Role Name	Purpose	Used By
<code>viz-now-deploy-infra</code>	Provisions infrastructure via Terraform	Deployment Agent
<code>viz-now-manage</code>	Manages deployed instances	Control Plane


These roles are assumed using AWS STS (Security Token Service), and their ARNs are stored securely in Viz Now.

7.2.2 Prerequisites

- An active AWS account.
- IAM Administrator access to AWS.
- Administrator access to the Viz Now platform.

7.2.3 Update Existing IAM Roles

If your AWS account already has Viz Now IAM roles defined, follow these guidelines to update them.

 **Note:** If your AWS account has no Viz Now IAM roles defined, first see section [Creating First IAM Role](#).

IAM Roles

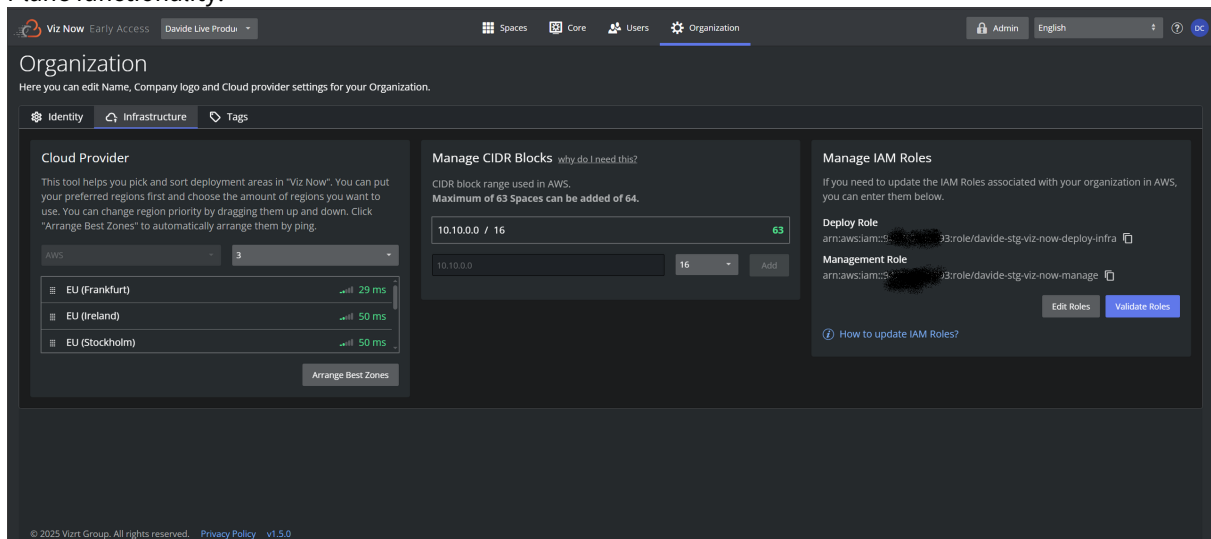
You will update both the *Deploy* and *Management* IAM roles and their associated inline policies.

To update an IAM role in Viz Now

This procedure assumes that your Viz Now user details are already setup in AWS. See the **Note** above.

1. Log in to your AWS Management Console with IAM Administrator permissions.
Keep this tab active in your browser.

- Log in to the Viz Now and navigate to the panel **Organization > Infrastructure** tab > **Manage IAM Roles**. You'll see a screen like the one below, where you can define the IAM Role ARNs for the Deploy and Control Plane functionality.

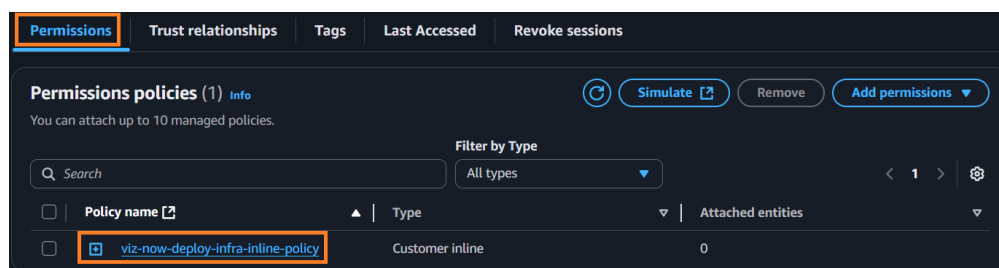
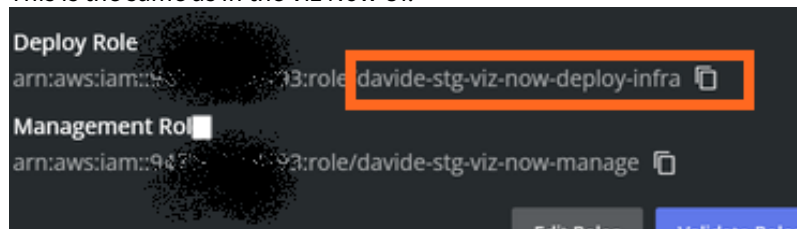


Keep this tab active in your browser.

Deploy role

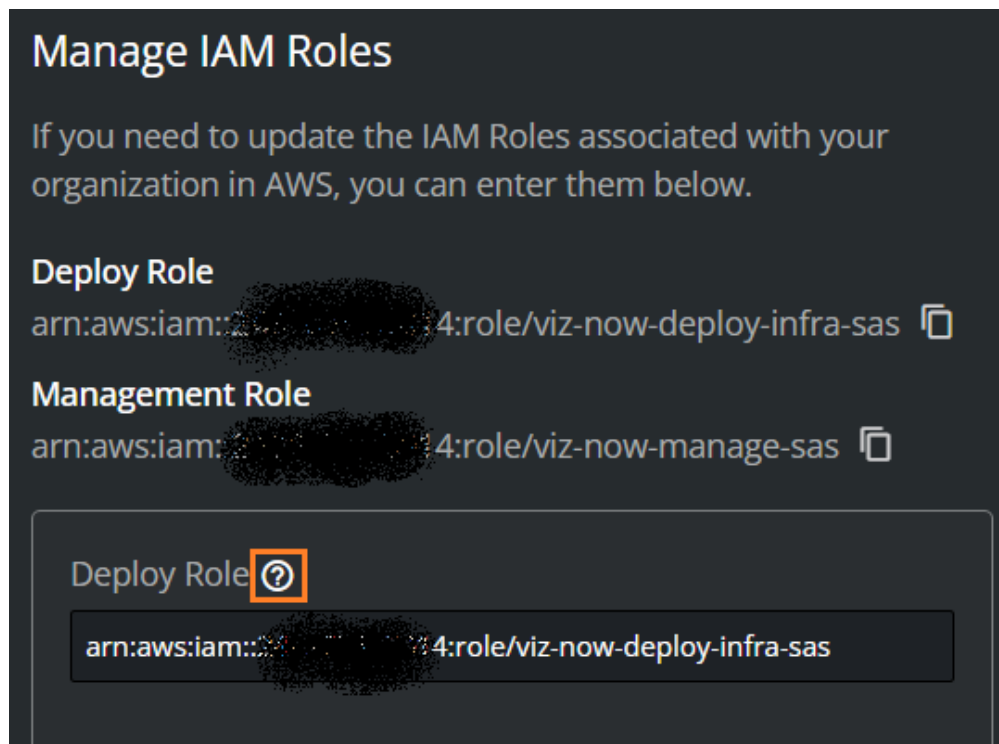
- Update the inline policy:
 - Switch to the AWS console **IAM > Roles** and from the **Permissions** tab, you can search for required inline policy.

This is the same as in the Viz Now UI:

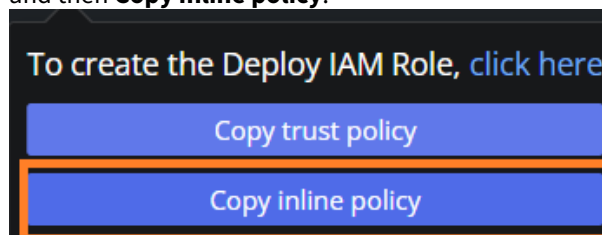


Click it to open.

- Go back to Viz Now and in the **Manage IAM Roles** panel, next to **Deploy Role**, click the **Question mark** icon (?).

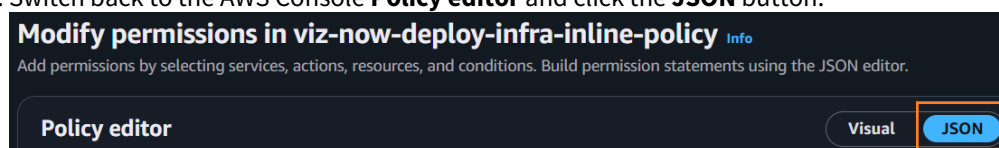


and then **Copy inline policy**.

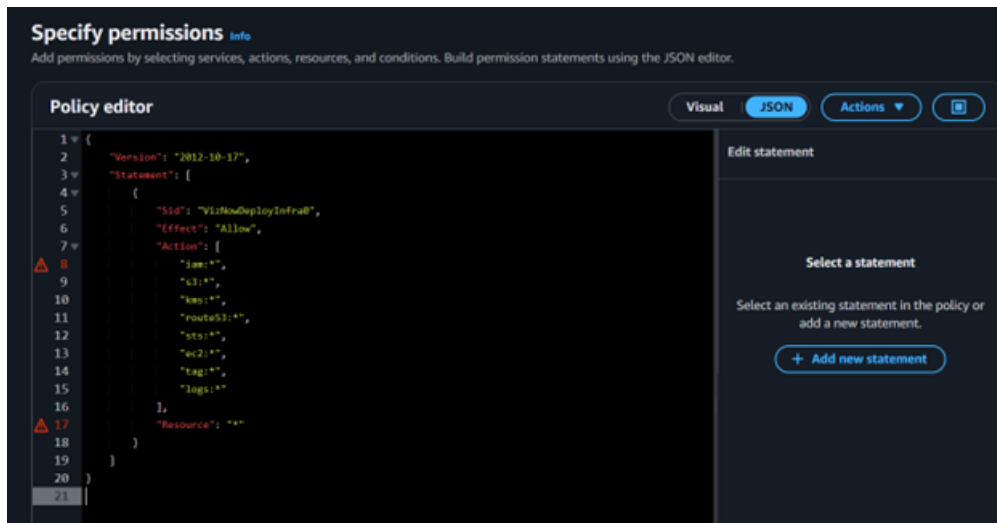


(This saves the policy details to the clipboard).

- c. Switch back to the AWS Console **Policy editor** and click the **JSON** button.



- d. In the **Policy editor**, paste-in the inline policy from the clipboard.



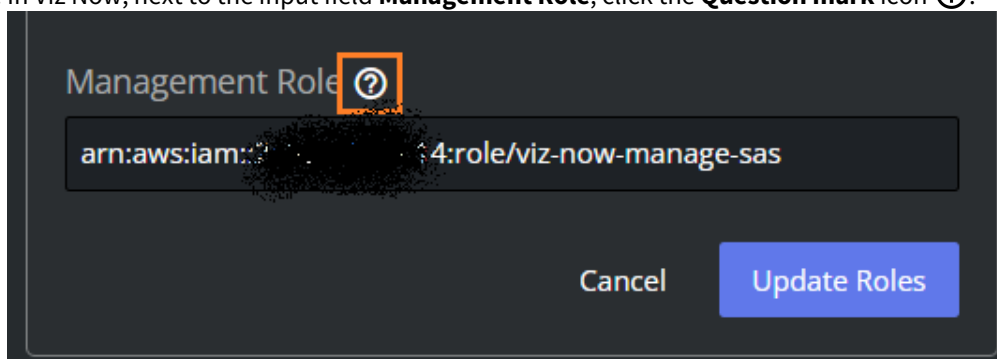
- e. Click **Next** and then click **Save changes**.
- f. A confirmation message is displayed.

✔ Policy viz-now-deploy-infra-inline-policy updated.

Management Role

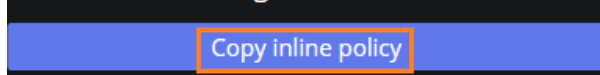
You now repeat the same steps for the Management role.

4. In Viz Now, next to the input field **Management Role**, click the **Question mark** icon (?).



- a. From the pop-up, click **Copy inline policy**.

To create the Management IAM Role, click here



- b. In the AWS Console, search for the required *manage* role, in this example, *viz-now-manage*, and click on it to display a **Summary** page.

viz-now-manage-sas Info Delete

Summary Edit

Creation date
May 16, 2025, 12:03 (UTC+01:00)

ARN
arn:aws:iam::248967558014:role/viz-now-manage-sas

Link to switch roles in console
<https://signin.aws.amazon.com/switchrole?roleName=viz-now-manage-sas&account=viznowtest>

Last activity
4 hours ago

Maximum session duration
1 hour

Permissions Trust relationships Tags Last Accessed Revoke sessions

Permissions policies (1) Info Simulate Remove Add permissions

You can attach up to 10 managed policies.

Search Filter by Type All types

Policy name	Type	Attached entities
viz-now-manage-inline-policy	Customer inline	0

- c. Select the **Permissions** tab and then its contained policy.
The **Policy editor** page opens:

Modify permissions in viz-now-manage-inline-policy Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor Visual JSON Actions Edit statement Remove

Edit statement
VizNowManage0

Add actions
Choose a service

Included
CloudWatch Logs
EC2
IAM
KMS
Resource Group Tagging
Route 53
S3
STS

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VizNowManage0",
6       "Effect": "Allow",
7       "Action": [
8         "iam:*",
9         "kms:*",
10        "route53:*",
11        "servicequotas:*",
12        "s3:*",
13        "ec2:*",
14        "tag:*",
15        "sts:*",
16        "logs:*"
17      ],
18      "Resource": "*"
19    },
20    {
21      "Sid": "AllowSSMDocumentsForSendCommand",
22      "Effect": "Allow",
23      "Action": "ssm:SendCommand"
24    }
25  ]
26 }



```

- d. Paste-in the *inline policy* that you copied to your clipboard, to update the JSON code.
For an example, see the [code below](#).
- e. Click **Save changes**.
5. Validate IAM Role in Viz Now:
- Click **Cancel**.
 - In Viz Now **Manage IAM Roles** panel, click **Validate Roles**.

[How to update IAM Roles?](#)

Edit Roles Validate Roles

- c. A confirmation message is displayed.

 IAM Role validation completed successfully
 

7.2.4 Permissions Explained

Deploy Role (*viz-now-deploy-infra*)

The Deploy role grants broad permissions to allow Spacelift to deploy infrastructure using Terraform. All permissions apply to all resources (`"Resource": "*"`).

Permission	Purpose	Resource Scope
<code>iam:*</code>	Manages IAM roles/users	Scope to specific roles
<code>s3:*</code>	Manages S3 buckets	Scope to specific buckets
<code>kms:*</code>	Manages encryption keys	Scope to specific keys
<code>route53:*</code>	Configures DNS	Scope to specific zones
<code>sts:*</code>	Assumes roles	Necessary for Spacelift
<code>ec2:*</code>	Provisions EC2 resources	Scope to specific VPCs
<code>tag:*</code>	Applies tags	All (<code>*</code>)
<code>logs:*</code>	Manages CloudWatch logs	Scope to specific log groups

Manage Role (*viz-now-manage*)

The *Manage* role enables Viz Now to perform operational tasks on deployed instances. Permissions are scoped to specific resources whenever possible.

Key Tasks Enabled by Manage Role

- Increase service quotas for AWS resources.
- Reserve specific EC2 instance types.
- Create S3 buckets for file storage.
- Manage security groups for IP-based access.
- Handle VPC peering.

- Start, stop, or destroy instances.
- Manage MediaConnect flows for streaming.

Permission	Purpose	Resource Scope
<code>iam:*</code>	Manages IAM configurations	All (*)
<code>kms:*</code>	Manages encryption keys	All (*)
<code>route53:*</code>	Updates DNS	All (*)
<code>servicequotas:*</code>	Increases quotas	All (*)
<code>s3:*</code>	Manages S3 buckets	All (*)
<code>ec2:*</code>	Manages instances	All (*)
<code>tag:*</code>	Manages tags	All (*)
<code>sts:*</code>	Assumes roles	All (*)
<code>logs:*</code>	Manages CloudWatch logs	All (*)
<code>ssm:SendCommand</code>	Executes commands	SSM documents & tagged EC2 instances (<code>VizNow=true</code>)
<code>ssm:ListCommandInvocations</code> , etc.	Checks command status	All (*)
<code>ssm:ListInventoryEntries</code> , etc.	Retrieves instance details	Tagged resources (<code>VizNow=true</code>)
<code>mediaconnect:CreateFlow</code>	Creates MediaConnect flows	All (*)
<code>mediaconnect:*</code> (multiple)	Manages MediaConnect flows	Flows named <code>VizNow-*</code>

Permission	Purpose	Resource Scope
<code>mediaconnect:ListFlows</code> , etc.	Lists flows	All (*)

Additional Resources

- [Spacelift AWS Integration](#)
- [AWS IAM Documentation](#)

7.3 Network Security and Default Port Configuration

Viz Now automatically sets up secure and functional network environments for your cloud deployments.

This section helps you understand how your instances are protected and what changes are safe with the following topics:

- [Viz Now Security Environment](#)
 - [Default Open Ports and Services](#)
- [Volatility of Manual Changes](#)
- [Recommendations](#)

7.3.1 Viz Now Security Environment

Viz Now uses a *layered security model* combining:

- **Network Access Control Lists (NACL):** Control which ports are open at the subnet level.
- **Security Groups:** Control which IP addresses can reach each instance.

This dual approach ensures both flexibility and safety:

- NACLs open the ports needed for applications to work.
- Security Groups limit access to specific IPs that *you* define.

Default Open Ports and Services

Depending on the application and services deployed, Viz Now enables by default the following ports:

Application / Service	Protocol(s)	Port(s)	Direction	Notes
TriCaster Vector API	TCP	5951 – 5952	Ingress	For switcher control
Controls Panels	TCP	5958	Ingress	For Control Surface interface
Amazon DCV	TCP/UDP	8443	Ingress	For remote desktop access
NDI Bridge	TCP/UDP	5990	Ingress	For video/audio streaming
Comprimato Live Transcoder	TCP	1935	Ingress	For RTMP AV streaming

Application / Service	Protocol(s)	Port(s)	Direction	Notes
Comprimato Live Transcoder	TCP / UDP	5960 - 9000	Ingress	For NDI
Comprimato Live Transcoder	UDP	30000	Ingress	For JPEGXS
Telos Infinity VIP	TCP / UDP	7001 - 7016	Ingress	Audio
Harrison Mixbus	TCP / UDP	5004 - 5005	Ingress	RTP MIDI
SRT Streaming protocol	TCP/UDP	9000 - 9020	Ingress	Secure video transport
Ephemeral Ports	TCP/UDP	49152 - 65535	Ingress	Dynamic and temporary connections
Ephemeral Ports	TCP/UDP	1024 - 65535	Egress	Dynamic and temporary connections
ICMP	ICMP	All	Bi-directional	For ping and diagnostics

Info: Some ports are opened only if specific services like Comprimato, Telos Infinity, or Mixbus are enabled during deployment.

7.3.2 Volatility of Manual Changes

Manual changes may be overwritten!

If you manually add or change firewall rules directly in the AWS Console:

- Viz Now will *not track* those changes.
- If you *redeploy* your space, manual changes may be lost and default settings restored.

Recommendations

- Whenever possible, always use the Viz Now UI for managing access.

- If you must make manual changes, document them outside of Viz Now and plan to reapply them after updates or redeployments.


8 Feedback & Support

- [How to Access Support and Submit Ideas](#)
 - [Got an Idea?](#)
 - [Need Help?](#)
-

8.1 How to Access Support and Submit Ideas

We want Viz Now to serve your production needs in the best possible way. Whether you are seeking help or eager to share ideas, we have made it simple to connect with our support ecosystem.

8.1.1 Accessing the Support Portal

1. In Viz Now, click  close to your user icon (top-right corner).
2. Select **Viz Now – Feedback & Support** from the dropdown.
3. You will be redirected to the **Vizrt Global Support page**.
4. From here, you can log in to the **Vizrt Community Portal**.

What You'll Find in the Vizrt Community

Once logged in, you can access:

- **Support Portal** – Submit and manage technical support requests.
 - **Documentation** – Explore user guides and reference material.
 - **Viz University** – Access self-paced training and certification resources.
 - **License Portal** – View and manage product licenses.
 - **Vizrt Customer Ideas Portal** – Suggest, vote, and track product ideas.
-

8.2 Got an Idea?

At Vizrt, we value your feedback and ideas to shape the future of our products. Whether a small feature request or a big innovation, we want to hear from you!

8.2.1 How to Submit an Idea

1. Log in to the [Vizrt Community Portal](#).
2. From the main menu, click **Ideas**.
3. Submit your suggestion, vote on others, and help influence the product roadmap.

► **Watch this video** to learn how it works: <https://vimeo.com/766541626/d21a6c6ab5>

Why Your Input Matters


Your ideas help us:

- Prioritize the right improvements

- Understand evolving workflows
 - Build tools that truly support your creativity and efficiency.
-

8.3 Need Help?

If you are having trouble accessing the Vizrt Support Portal or the Vizrt Community:

- In the Viz Now menu, click the top-right  icon and **Viz Now – Feedback & Support**.
- On the Vizrt Global Support page, under the **Visit Support Portal** button and *Do not have Vizrt Support Portal access?*, click **Submit Ticket**.
- Our Support team will assist you in gaining access and resolving your request.