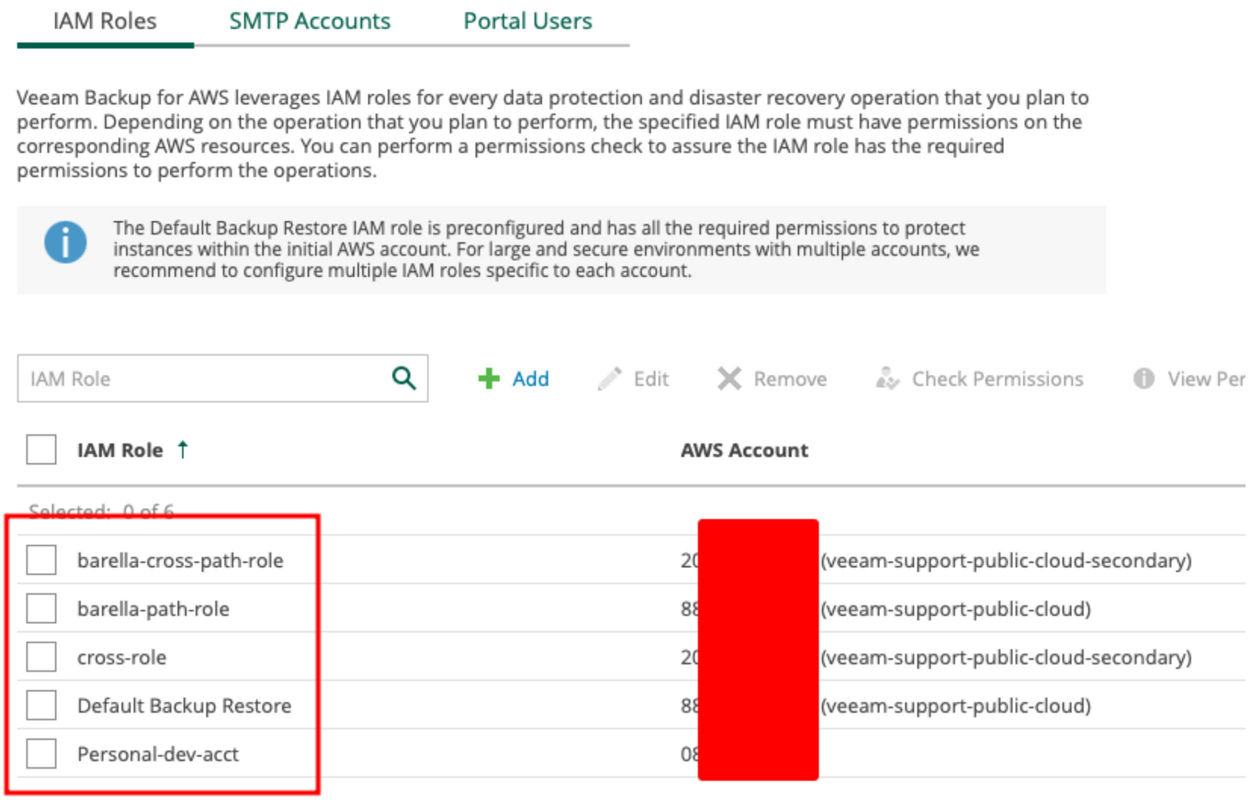
Steps to test SQS communication.

This Python script will launch an Amazon Linux 2023 VM with necessary resources to test the SQS communication.
Install Python3 first:
https://www.python.org/downloads/
Download the python script here:
https://github.com/barellag/scripts/blob/main/launch_instances.py

For the script you will need to provide:

- Role ARN with the Backup permissions (same configured in VBAWS)

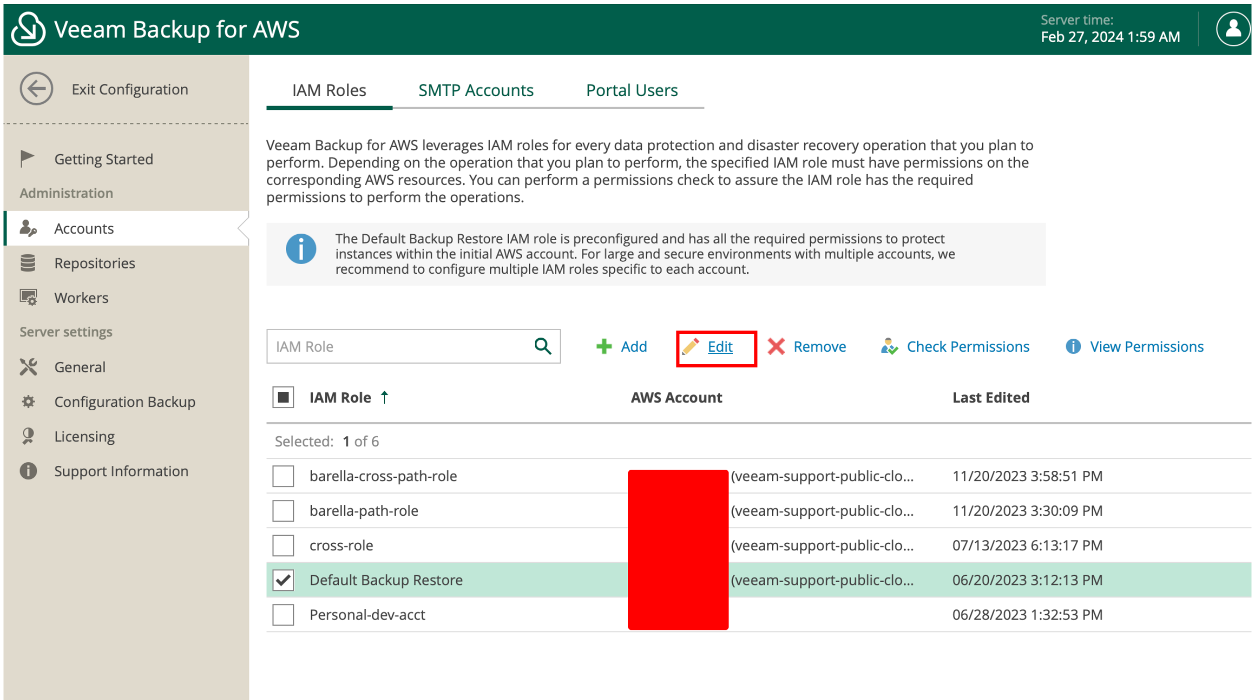


Veeam Backup for AWS leverages IAM roles for every data protection and disaster recovery operation that you plan to perform. Depending on the operation that you plan to perform, the specified IAM role must have permissions on the corresponding AWS resources. You can perform a permissions check to assure the IAM role has the required permissions to perform the operations.

The Default Backup Restore IAM role is preconfigured and has all the required permissions to protect instances within the initial AWS account. For large and secure environments with multiple accounts, we recommend to configure multiple IAM roles specific to each account.

Selected: 0 of 6

□	IAM Role ↑	AWS Account
□	barella-cross-path-role	[redacted] (veeam-support-public-cloud-secondary)
□	barella-path-role	[redacted] (veeam-support-public-cloud)
□	cross-role	[redacted] (veeam-support-public-cloud-secondary)
□	Default Backup Restore	[redacted] (veeam-support-public-cloud)
□	Personal-dev-acct	[redacted]



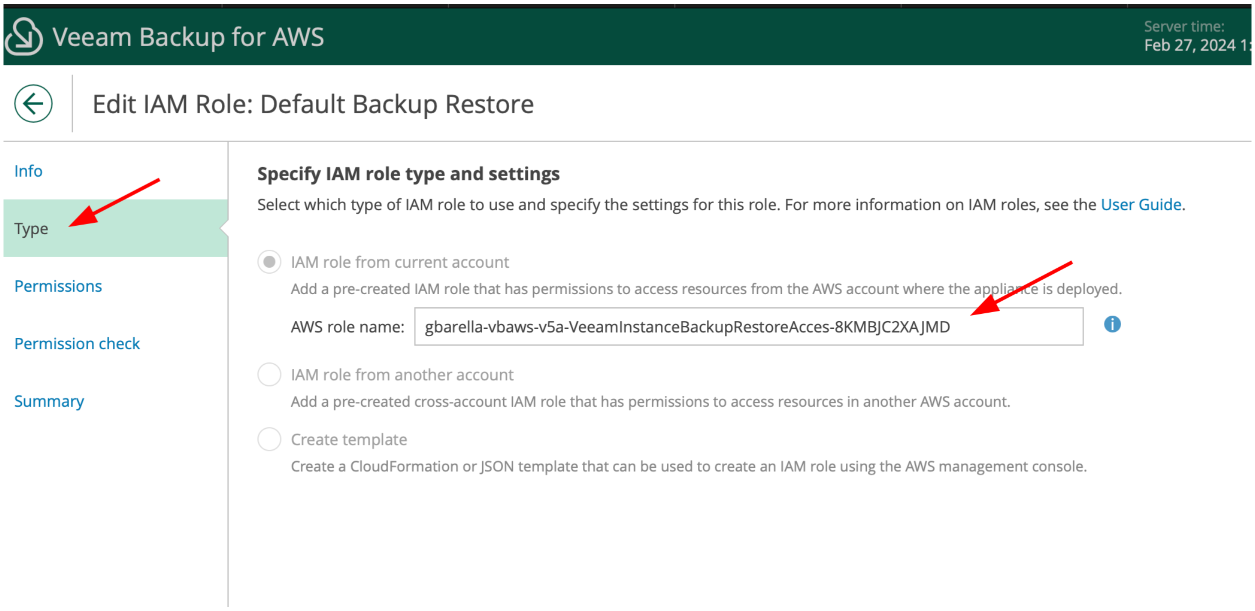
Veeam Backup for AWS leverages IAM roles for every data protection and disaster recovery operation that you plan to perform. Depending on the operation that you plan to perform, the specified IAM role must have permissions on the corresponding AWS resources. You can perform a permissions check to assure the IAM role has the required permissions to perform the operations.

The Default Backup Restore IAM role is preconfigured and has all the required permissions to protect instances within the initial AWS account. For large and secure environments with multiple accounts, we recommend to configure multiple IAM roles specific to each account.

Selected: **1** of 6

	IAM Role ↑	AWS Account	Last Edited
□	barella-cross-path-role	[redacted] (veeam-support-public-clo...	11/20/2023 3:58:51 PM
□	barella-path-role	[redacted] (veeam-support-public-clo...	11/20/2023 3:30:09 PM
□	cross-role	[redacted] (veeam-support-public-clo...	07/13/2023 6:13:17 PM
☑	Default Backup Restore	[redacted] (veeam-support-public-clo...	06/20/2023 3:12:13 PM
□	Personal-dev-acct	[redacted]	06/28/2023 1:32:53 PM

This is the Role Name:



Edit IAM Role: Default Backup Restore

Specify IAM role type and settings

Select which type of IAM role to use and specify the settings for this role. For more information on IAM roles, see the User Guide.

● IAM role from current account

Add a pre-created IAM role that has permissions to access resources from the AWS account where the appliance is deployed.

AWS role name: gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD

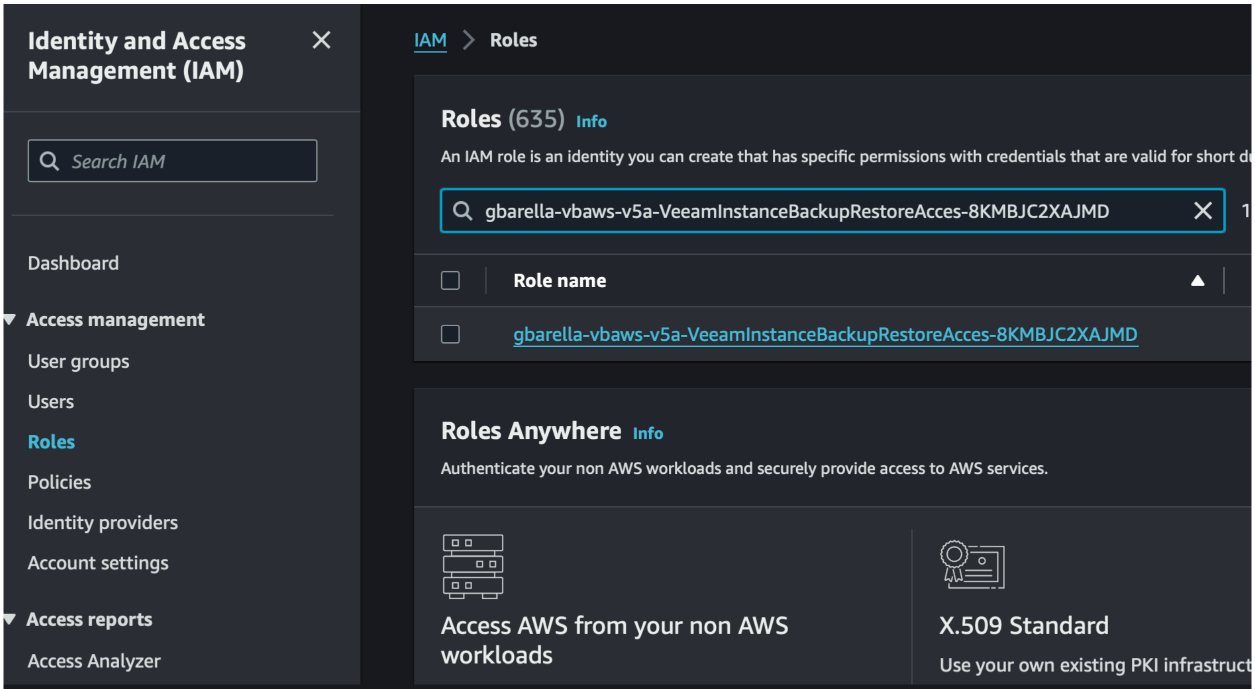
○ IAM role from another account

Add a pre-created cross-account IAM role that has permissions to access resources in another AWS account.

○ Create template

Create a CloudFormation or JSON template that can be used to create an IAM role using the AWS management console.

Find this role in AWS:



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

IAM > Roles

Roles (635) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short d

gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD

□	Role name ▲
□	gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD

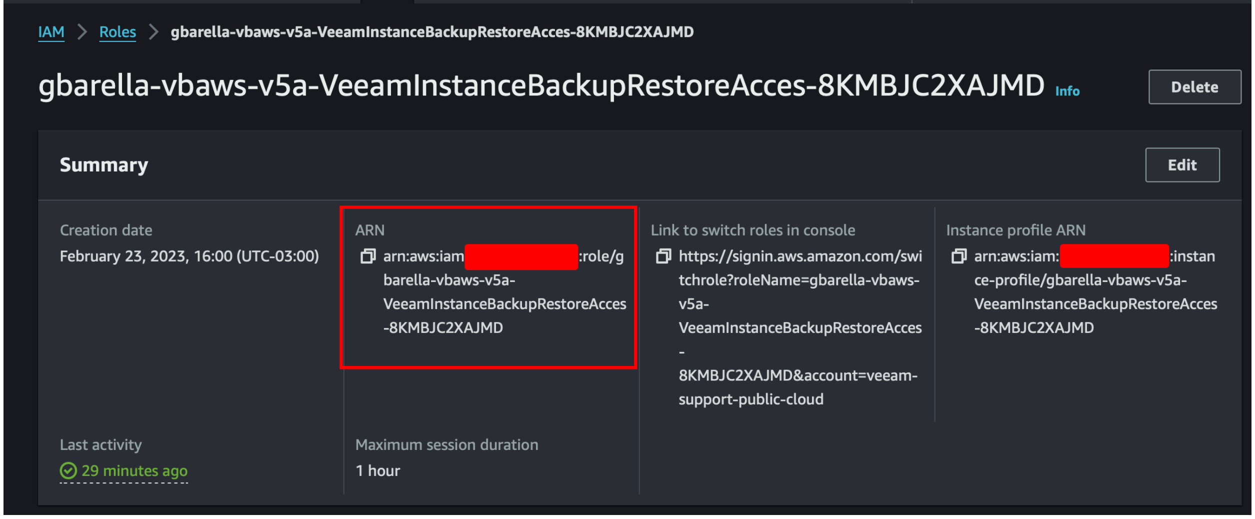
Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

X.509 Standard

Use your own existing PKI infrastruct



IAM > Roles > gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD

gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD Info

Summary

Creation date
February 23, 2023, 16:00 (UTC-03:00)

ARN
arn:aws:iam[redacted]:role/gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD

Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD&account=veeam-support-public-cloud

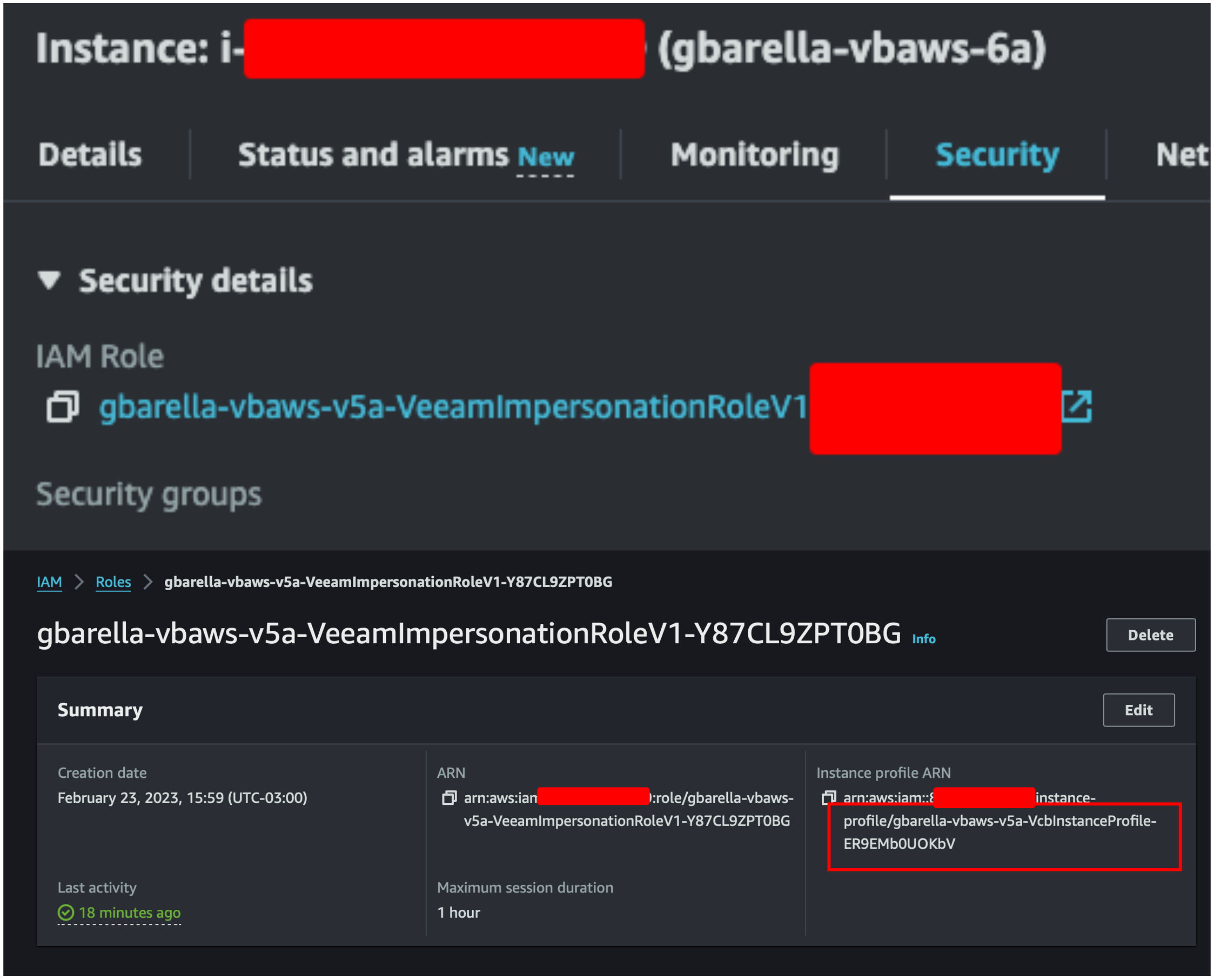
Instance profile ARN
arn:aws:iam:[redacted]:instance-profile/gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD

Last activity
29 minutes ago

Maximum session duration
1 hour

- Name for the test VM (this will play the worker role)
- Region name
- Instance Profile ARN (same as the workers are assuming for cross account, if you are testing same account, you need to identify the instance profile name that is associated to the appliance, in the Security Tab of the instance you can find the Role name).

To find the instance profile name, you click on the Role name and then you will see the instance profile name:



Instance: i-[redacted] (gbarella-vbaws-6a)

Security details

IAM Role
gbarella-vbaws-v5a-VeeamImpersonationRoleV1[redacted]

gbarella-vbaws-v5a-VeeamImpersonationRoleV1-Y87CL9ZPT0BG

Summary

Creation date
February 23, 2023, 15:59 (UTC-03:00)

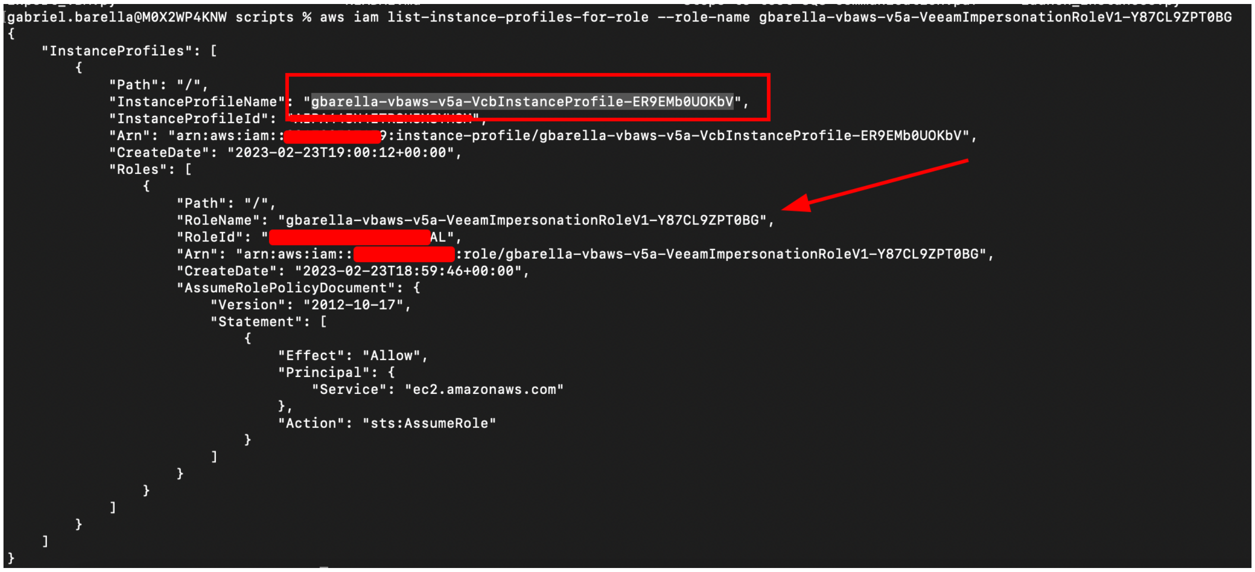
ARN
arn:aws:ian[redacted]:role/gbarella-vbaws-v5a-VeeamImpersonationRoleV1-Y87CL9ZPT0BG

Instance profile ARN
arn:aws:iam::[redacted]instance-profile/gbarella-vbaws-v5a-VcbInstanceProfile-ER9EMb0UOKbV

Last activity
18 minutes ago

Maximum session duration
1 hour

You can also use the AWS CLI:
Use the following command to find out the instance profile name:
aws iam list-instance-profiles-for-role --role-name rolenamehere

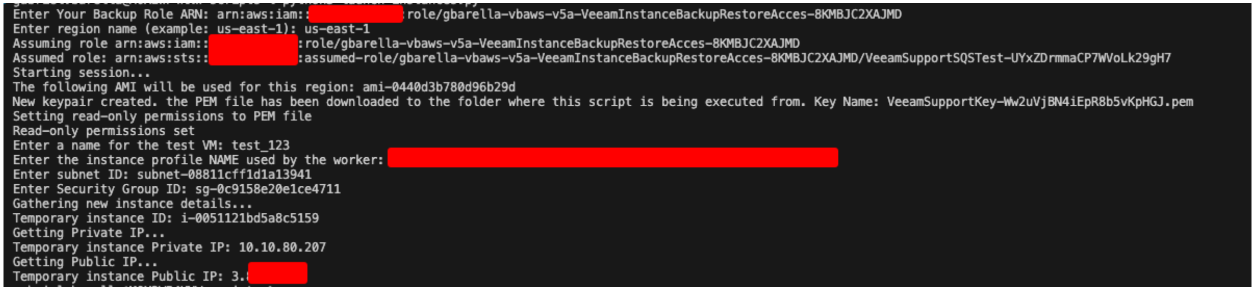


```
gabriel.barella@M0X2WP4KNW scripts % aws iam list-instance-profiles-for-role --role-name gbarella-vbaws-v5a-VeeamImpersonationRoleV1-Y87CL9ZPT0BG
{
    "InstanceProfiles": [
        {
            "Path": "/",
            "InstanceProfileName": "gbarella-vbaws-v5a-VcbInstanceProfile-ER9EMb0UOKbV",
            "InstanceProfileId": "[redacted]",
            "Arn": "arn:aws:iam::[redacted]9:instance-profile/gbarella-vbaws-v5a-VcbInstanceProfile-ER9EMb0UOKbV",
            "CreateDate": "2023-02-23T19:00:12+00:00",
            "Roles": [
                {
                    "Path": "/",
                    "RoleName": "gbarella-vbaws-v5a-VeeamImpersonationRoleV1-Y87CL9ZPT0BG",
                    "RoleId": "[redacted]AL",
                    "Arn": "arn:aws:iam::[redacted]:role/gbarella-vbaws-v5a-VeeamImpersonationRoleV1-Y87CL9ZPT0BG",
                    "CreateDate": "2023-02-23T18:59:46+00:00",
                    "AssumeRolePolicyDocument": {
                        "Version": "2012-10-17",
                        "Statement": [
                            {
                                "Effect": "Allow",
                                "Principal": {
                                    "Service": "ec2.amazonaws.com"
                                },
                                "Action": "sts:AssumeRole"
                            }
                        ]
                    }
                }
            ]
        }
    ]
}
```

In case you see the error "An error occurred (InvalidClientTokenId)", remove the credentials set to file ~/.aws/credentials. Simply delete the file credentials located at your home folder /.aws/

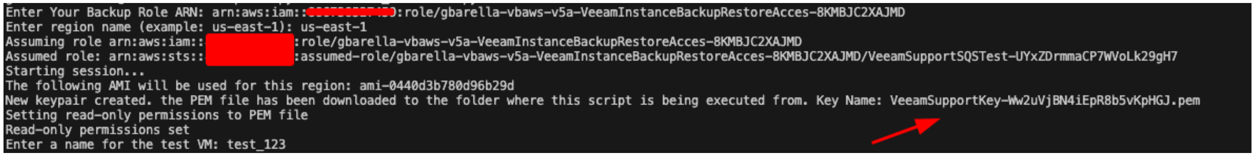
- Subnet ID (Same as configured for workers)
- Security Group ID (Same as used by workers)

This is the expected output:



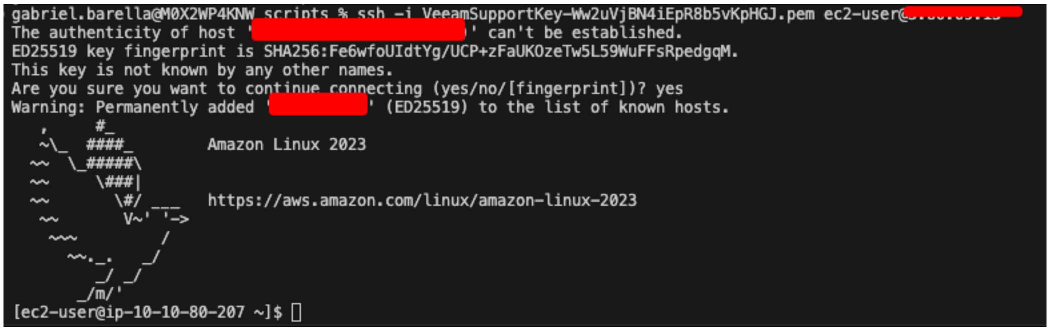
```
Enter Your Backup Role ARN: arn:aws:iam::[redacted]:role/gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD
Enter region name (example: us-east-1): us-east-1
Assuming role arn:aws:iam::[redacted]:role/gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD
Assumed role: arn:aws:sts::[redacted]:assumed-role/gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD/VeeamSupportSQSTest-UYxZDrmmaCP7WVoLk29gH7
Starting session...
The following AMI will be used for this region: ami-0440d3b780d96b29d
New keypair created. the PEM file has been downloaded to the folder where this script is being executed from. Key Name: VeeamSupportKey-Ww2uVjBN4iEpR8b5vKpHGJ.pem
Setting read-only permissions to PEM file
Read-only permissions set
Enter a name for the test VM: test_123
Enter the instance profile NAME used by the worker: [redacted]
Enter subnet ID: subnet-08811cff1d1a13941
Enter Security Group ID: sg-0c9158e20e1ce4711
Gathering new instance details...
Temporary instance ID: i-0051121bd5a8c5159
Getting Private IP...
Temporary instance Private IP: 10.10.80.207
Getting Public IP...
Temporary instance Public IP: 3.[redacted]
```

The SSH PEM file will be downloaded to the folder where the script was executed.



```
Enter Your Backup Role ARN: arn:aws:iam::[redacted]:role/gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD
Enter region name (example: us-east-1): us-east-1
Assuming role arn:aws:iam::[redacted]:role/gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD
Assumed role: arn:aws:sts::[redacted]:assumed-role/gbarella-vbaws-v5a-VeeamInstanceBackupRestoreAcces-8KMBJC2XAJMD/VeeamSupportSQSTest-UYxZDrmmaCP7WVoLk29gH7
Starting session...
The following AMI will be used for this region: ami-0440d3b780d96b29d
New keypair created. the PEM file has been downloaded to the folder where this script is being executed from. Key Name: VeeamSupportKey-Ww2uVjBN4iEpR8b5vKpHGJ.pem
Setting read-only permissions to PEM file
Read-only permissions set
Enter a name for the test VM: test_123
```

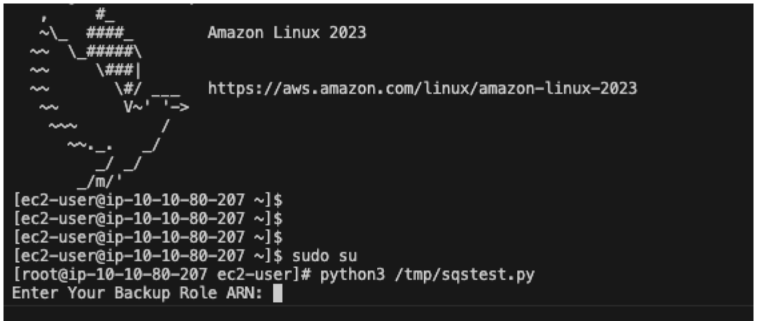
From the same terminal you should be able to ssh into the temp VM:



```
gabriel.barella@M0X2WP4KNW scripts % ssh -i VeeamSupportKey-Ww2uVjBN4iEpR8b5vKpHGJ.pem ec2-user@[redacted]
The authenticity of host '[redacted]' can't be established.
ED25519 key fingerprint is SHA256:Fe6wfoUIdtYg/UCP+zFaUKOzeTw5L59WuFFsRpedgqM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[redacted]' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-10-80-207 ~]$ 
```

Run the following commands:

sudo su
python3 /tmp/sqstest.py

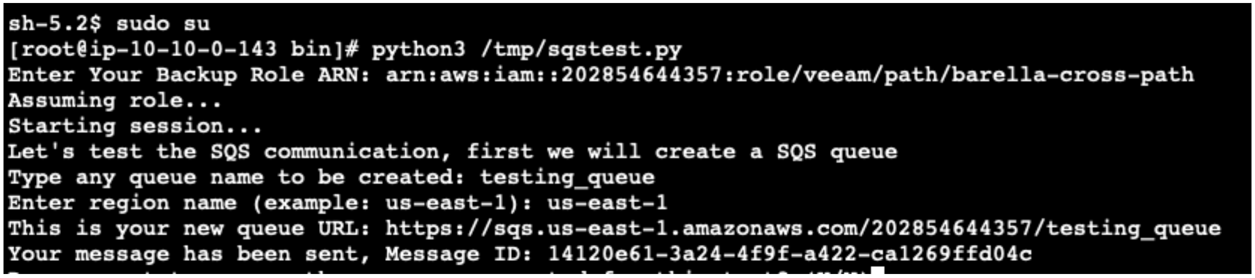


```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-10-80-207 ~]$
[ec2-user@ip-10-10-80-207 ~]$
[ec2-user@ip-10-10-80-207 ~]$
[ec2-user@ip-10-10-80-207 ~]$ sudo su
[root@ip-10-10-80-207 ec2-user]# python3 /tmp/sqstest.py
Enter Your Backup Role ARN: 
```

For this part you will need to enter:

- Backup Role ARN (the same used in the first step)
- Any name for the test queue
- Region Name (us-east-1 for example)

Expected output:



```
sh-5.2$ sudo su
[root@ip-10-10-0-143 bin]# python3 /tmp/sqstest.py
Enter Your Backup Role ARN: arn:aws:iam::202854644357:role/veeam/path/barella-cross-path
Assuming role...
Starting session...
Let's test the SQS communication, first we will create a SQS queue
Type any queue name to be created: testing_queue
Enter region name (example: us-east-1): us-east-1
This is your new queue URL: https://sqs.us-east-1.amazonaws.com/202854644357/testing_queue
Your message has been sent, Message ID: 14120e61-3a24-4f9f-a422-ca1269ffd04c
```

If you see this, it means it was able to connect to the SQS endpoint. Then the script will ask if you want to delete the resources.
The test instance will not be terminated, only the SQS queue and the credentials will be deleted.