Hystax Acura

Installation Guide (AWS)

Overview

Hystax is a cloud migration and Disaster Recovery company focusing on consistent replication of IT workloads and providing real-time migration and Best-In-Class Disaster Recovery.

To deploy Hystax Acura solution a customer needs to request Hystax (info@hystax.com) to provide AMI with the solution and follow the steps described in this document.

Installation requirements

- AMI with Hystax Acura (provided by request).
- Deploy Hystax Acura AMI with not less than t2.large (2/8) flavour
- Use default VPC for the deployment
- AMI with Hystax Acura cloud agent. Cloud agent is a service virtual machine responsible for preparing EBS volumes / snapshots and AMIs from migrated machines.
- Security groups allowing the following traffic:
    - Hystax Acura host:
        - Ingress – tcp/443;
        - Ingress – tcp/4443;
        - Ingress – udp/12201.
    - Hystax Cloud Agent (spawned automatically in the Target Project):
        - Ingress – tcp/80;
        - Ingress – tcp/3260.

Required permissions for the IAM user

Add the following permissions to the IAM policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
```

```
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource": ["arn:aws:s3:::mys3bucket","arn:aws:s3:::mys3bucket/*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CancelConversionTask",
        "ec2:CancelExportTask",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:ImportInstance",
        "ec2:ImportVolume",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ImportImage",
        "ec2:ImportSnapshot",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeImportSnapshotTasks",
        "ec2:CancelImportTask"
      ],
      "Resource": "*"
    }
  ]
}
```

A user must create a role named vmimport with a trust relationship policy document that allows VM Import to assume the role, and attach an IAM policy to the role.

To create the service role:

1. Create a file named trust-policy.json with the following policy:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "Service": "vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals":{
               "sts:Externalid": "vmimport"
            }
         }
      }
   ]
}
```

The file can be saved anywhere on your computer. Take note of the location of the file, because it will be specified in the next step.

2. Use the create-role command to create a role named vmimport and give VM Import/Export access to it. Ensure that the full path to the location of the trust-policy.json file is specified, and that you prefix file:// to it:

```
aws iam create-role --role-name vmimport --assume-role-policy-document
file://trust-policy.json
```

Note

If you encounter an error stating that "This policy contains invalid Json," double-check that the path to the JSON file is provided correctly.

3. Create a file named role-policy.json with the following policy, where disk-image-file-bucket is the bucket where the disk images are stored:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetBucketLocation",
            "s3:GetObject",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::disk-image-file-bucket",
            "arn:aws:s3:::disk-image-file-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
```

```
            ],
            "Resource":"*"
        }
    ]
}
```

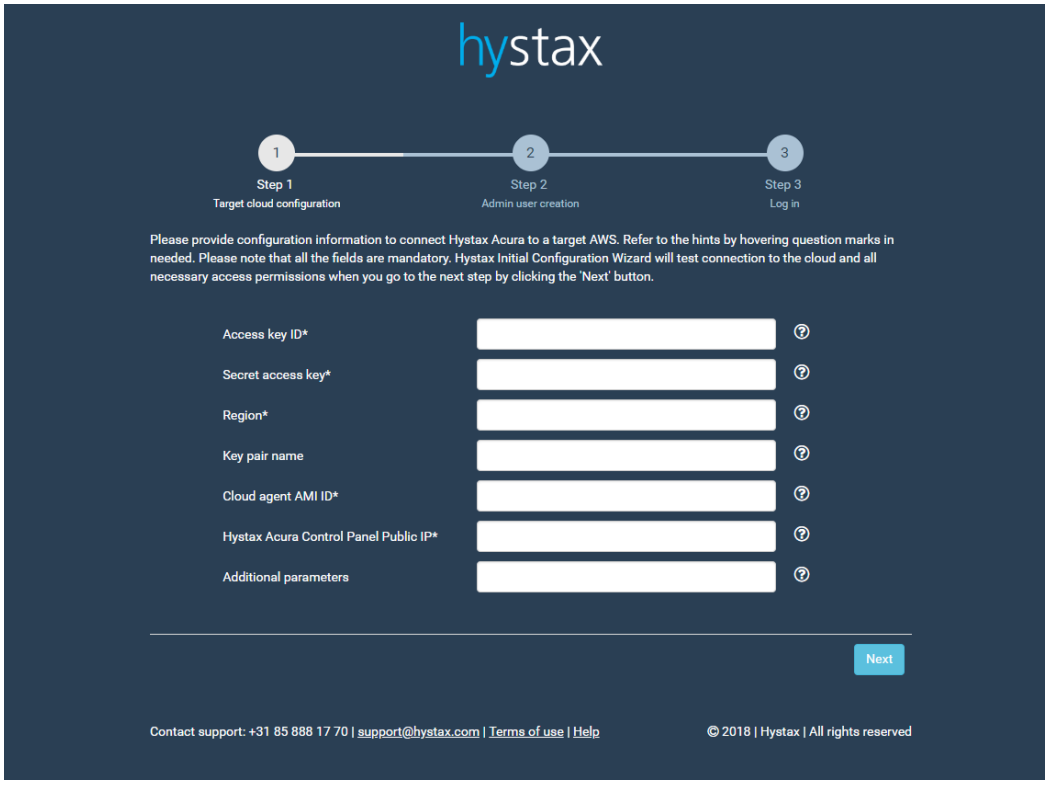
4. Use the following put-role-policy command to attach the policy to the role created above. Ensure that the full path to the location of the role-policy.json file is specified.

```
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json
```

Attach created policy to the IAM user that will be used for Hystax Acura.

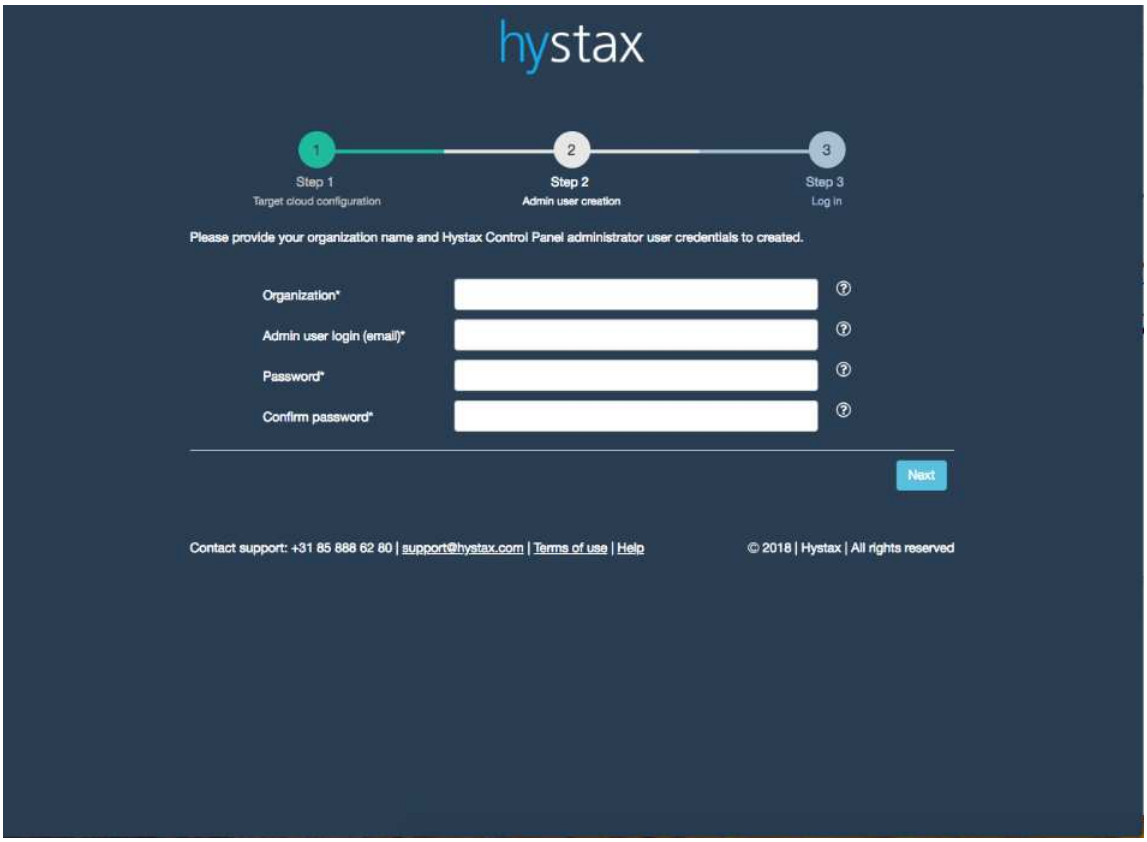
Installation steps

1. Create a machine from an AMI with Hystax Acura.
2. Associate an Elastic IP with the created machine.
3. Open a web browser and go to https://<ip_address of the machine>/. You will be redirected to the Hystax Setup Wizard. When you complete all the steps, the installation will be done and you can start using Hystax Acura.
4. Step 1 - Fill all the fields on the first step providing cloud configuration details. Please use question mark icons to get hints on the fields. When you click 'Next', the Hystax Setup Wizard will validate the data entered and notify you in case of error.

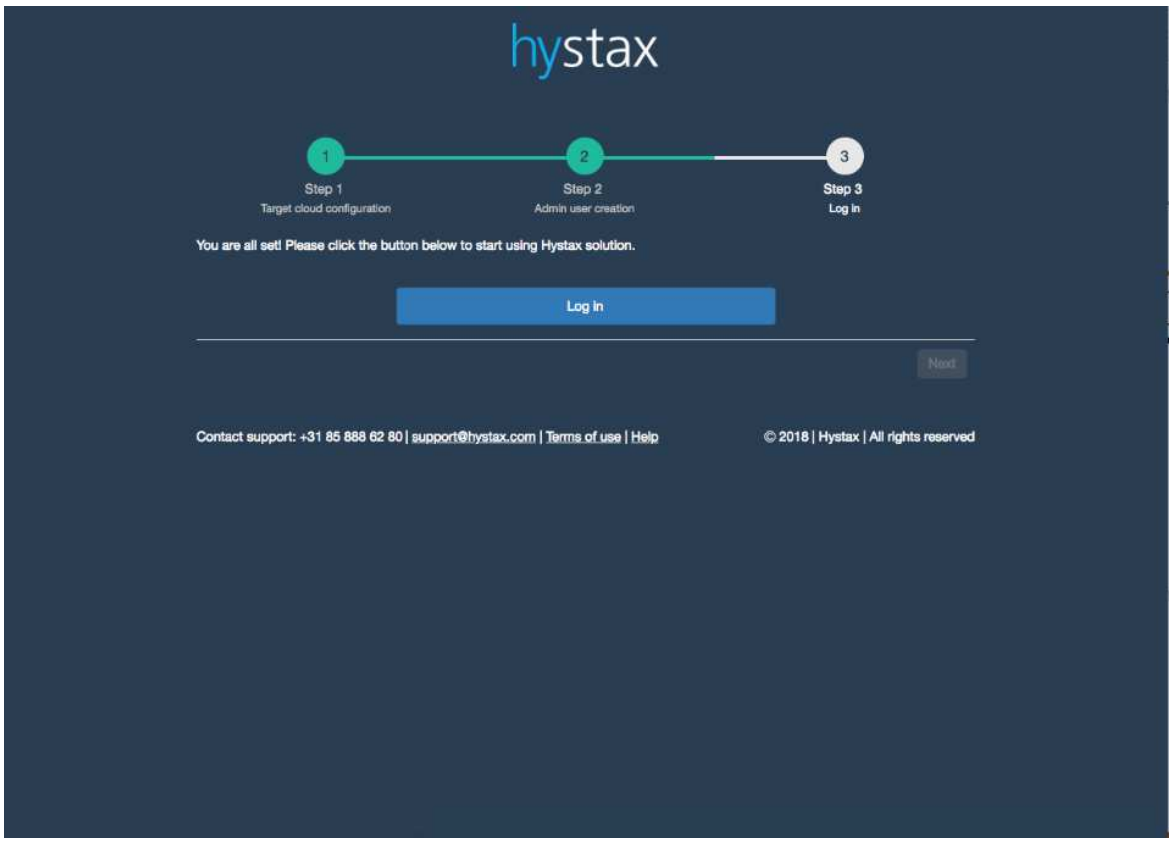


Field	Description	Example
AWS access key id	AWS account access key id	AKIAIH2FFMEUAFAOF4A
AWS secret key	AWS account secret key	MkhJX0j7FQ//T0xCUZJtJ3 jwZsXAzAddzaszz
Region	AWS region name	us-west-2
Key pair name	Key pair name to access the cloud agent	aws-key
Cloud agent AMI ID	The image ID from which cloud agent instances will be spun up	ami-06004e6d7b9cda28b
Hystax Acura Control Panel Public IP	Public IP which will be used to access the Hystax Control Panel via web browser and by replication agents	18.5.123.6
Additional parameters	Other additional parameters in JSON format, for example: {"parameter":"value"}	{"availability_zone": "zone-1"}

5. Step 2 – Enter the organization name and Hystax Admin User credentials into Hystax Setup Wizard. This is the user which you can use to log in to Hystax Acura Control Panel and administer the system. If there are any errors the system will notify you.



6. Step 3 – Installation is complete and you can log in to the system using credentials entered on the second step.



Troubleshooting

Hystax Acura automatically checks cloud access and necessary permissions for successful operation. It provides detailed error messages describing causes of problems. In case of an error, please check correctness of data entered and necessary permissions.

Use contact details below to reach Hystax support in case you have any questions or problems with the installation process.

Contacts

Email: info@hystax.com

Phone: +31 85 888 62 80Address: Kingsfordweg 151, Amsterdam, 1043 GR, Netherlands.