Déploiement de l’ensemble du cloud privé chez AWS

Ce document a pour but de permettre à un administrateur qualifié de pouvoir redéployer l’ensemble de l’infrastructure en cas de sinistre.

Dans un premier temps, il convient de se procurer les images des machines virtuelles.

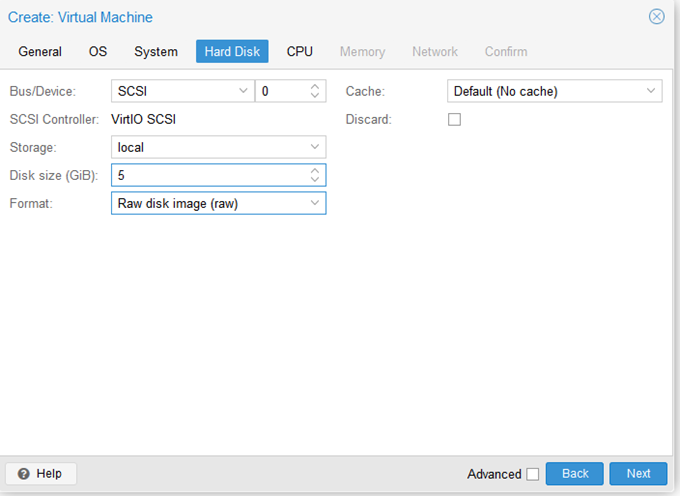
Celles-ci sont normalement backupées de manière journalière sur le FTP prévu à cet effet.

Il est important de s’assurer que cette procédure de backup est fonctionnelle, dans le cadre du PRA.

Les images sont au format raws et peuvent être importées dans l’infrastructure d’Amazon.

Nous allons décrire la procédure ci-dessous.

Pour faciliter l’explication, voici comment générer une image au format raw lors de la création d’une VM sous proxmox.

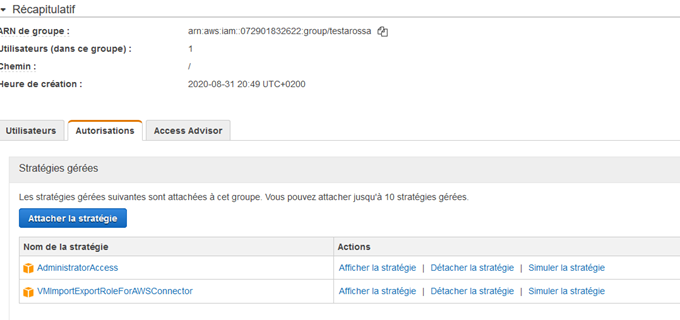


Pour la suite de la procédure, nous allons utiliser l’API CLI AWS.

Il est nécessaire pour cela de créer un utilisateur et un groupe depuis IAM (si cela n’est pas déjà le cas)

<https://console.aws.amazon.com/iam/home?#/users>

Ensuite il vous faudra ajouter les droits d’administrateur au groupe concerné.



Puis récupérer les clés API permettant son utilisation en CLI.

Vous aurez besoin de :

* AWS Access Key ID
* AWS Secret Access Key



Configurez ensuite les clés d’accès API sur l’outil CLI.

Choisir la région **eu-west-1**

epitech@Testarossa:~/client1$ aws configure

AWS Access Key ID [\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*UN5O]:

AWS Secret Access Key [\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*ofgn]:

Default region name [eu-west-1]:

Default output format [None]:

Une fois l’outil CLi correctement configuré, vous serez en mesure de communiquer avec l’API.

Vous devrez ensuite créer un rôle IAM « vmimport »

Doc AWS: <https://docs.aws.amazon.com/vm-import/latest/userguide/vmie_prereqs.html#vmimport-role>

Pour ce faire, exécutez les commandes suivantes (ajustez si besoin en fonction de l’évolution de l’infrastructure)

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

trust-policy.json :

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": { "Service": "vmie.amazonaws.com" },

"Action": "sts:AssumeRole",

"Condition": {

"StringEquals":{

"sts:Externalid": "vmimport"

}

}

}

]

}

$> aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document <file://role-policy.json>

role-policy.json :

{

"Version":"2012-10-17",

"Statement":[

{

"Effect": "Allow",

"Action": [

"s3:GetBucketLocation",

"s3:GetObject",

"s3:ListBucket"

],

"Resource": [

"arn:aws:s3:::epivmimg",

"arn:aws:s3:::epivmimg/\*"

]

},

{

"Effect": "Allow",

"Action": [

"s3:GetBucketLocation",

"s3:GetObject",

"s3:ListBucket",

"s3:PutObject",

"s3:GetBucketAcl"

],

"Resource": [

"arn:aws:s3:::epivmimg",

"arn:aws:s3:::epivmimg/\*"

]

},

{

"Effect": "Allow",

"Action": [

"ec2:ModifySnapshotAttribute",

"ec2:CopySnapshot",

"ec2:RegisterImage",

"ec2:Describe\*"

],

"Resource": "\*"

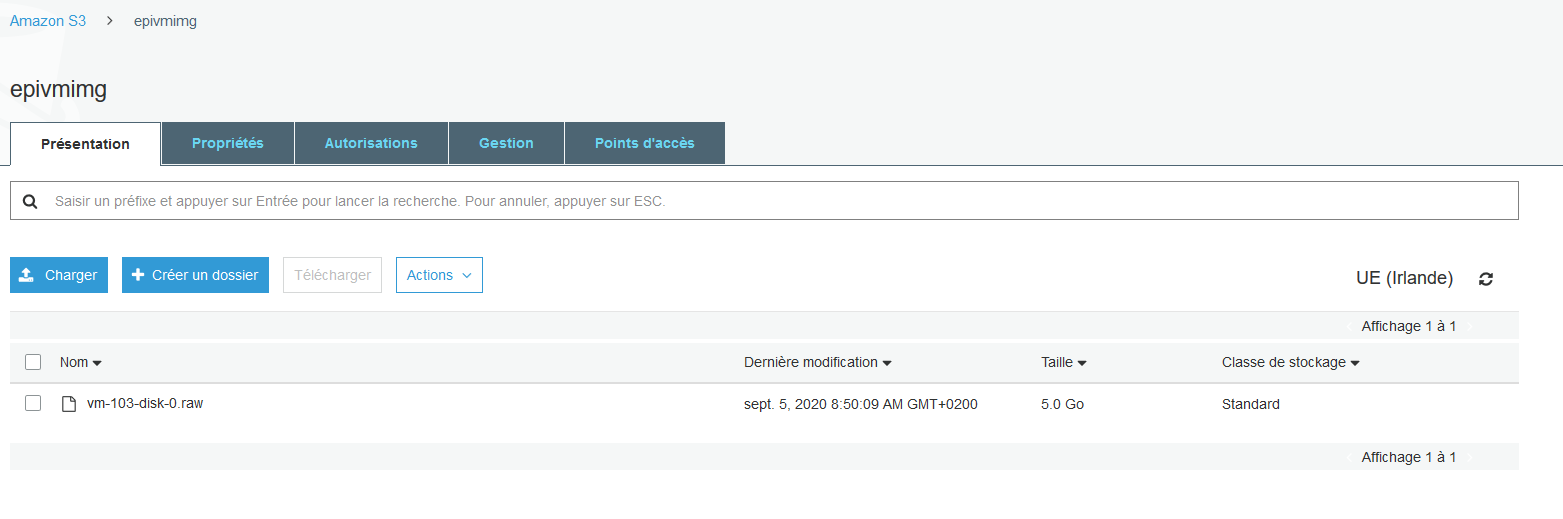
}

]

}

Afin de recevoir les images des machines virtuelles, nous devons tout d’abord créer un bucket destiné au stockage de ces images.

Nom du bucket : epivmimg



Pour « pousser » une image locale (ex : vm-103-disk-0.raw) sur le bucket epivmimg, exécutez la commande suivante :

$> aws s3 cp /mnt/pve/vm-storage/images/103/vm-103-disk-0.raw s3://epivmimg/

Enfin, une fois les images stockées dans le bucket, il est possible de les importer dans l’AMI (Amazon Machine Images) à l’aide de la commande suivante :

aws ec2 import-image --description “My server VM” --disk-containers <file://containers.json>

containers.json :

[

{

"Description": "First disk",

"Format": "raw",

"UserBucket": {

"S3Bucket": "epivmimg",

"S3Key": "vm-103-disk-0.raw"

}

}

]

Vous pouvez monitorer l’import d’une VM à l’aide de la commande suivante :

aws ec2 describe-import-image-tasks --import-task-ids import-ami-id

Une fois l’image importée, il vous sera ensuite possible de la piloter depuis l’interface de gestion d’EC2.

<https://aws.amazon.com/premiumsupport/knowledge-center/launch-instance-custom-ami/>

Nous espérons que ce document vous permettra de reprendre le contrôle de l’infrastructure en cas de sinistre.

Si vous avez des questions en lien avec le document, n’hésitez pas à vous rapprocher de ses auteurs.

* Thomas HENON ([thomas.henon@epitech.eu](mailto:thomas.henon@epitech.eu))
* Aurélien DARRAGON (aurelien.darragon@epitech.eu)