Major changes after forked:

1. remove acl in the bucket since aws makes new standard of s3 bucket since April 2023
2. fixed broken crontab for certain distributions of linux, for instance amazon linux 2 & 2023
3. add a feature to copy pem private keys & place them in the bastion
4. add ec2-ssm-role to the default profile.
5. upgraded to aws 5.0
6. remove bucket_public_keys_readme
7. add support for one single instance (without the ELB)
8. add public IP and private ip for one single instance
9. fix a bug in the context of "var.bastion_security_group_id == "" ? 1 : 0"
10. add additional input "bastion_security_group_used" boolean variable

AWS Bastion Terraform module

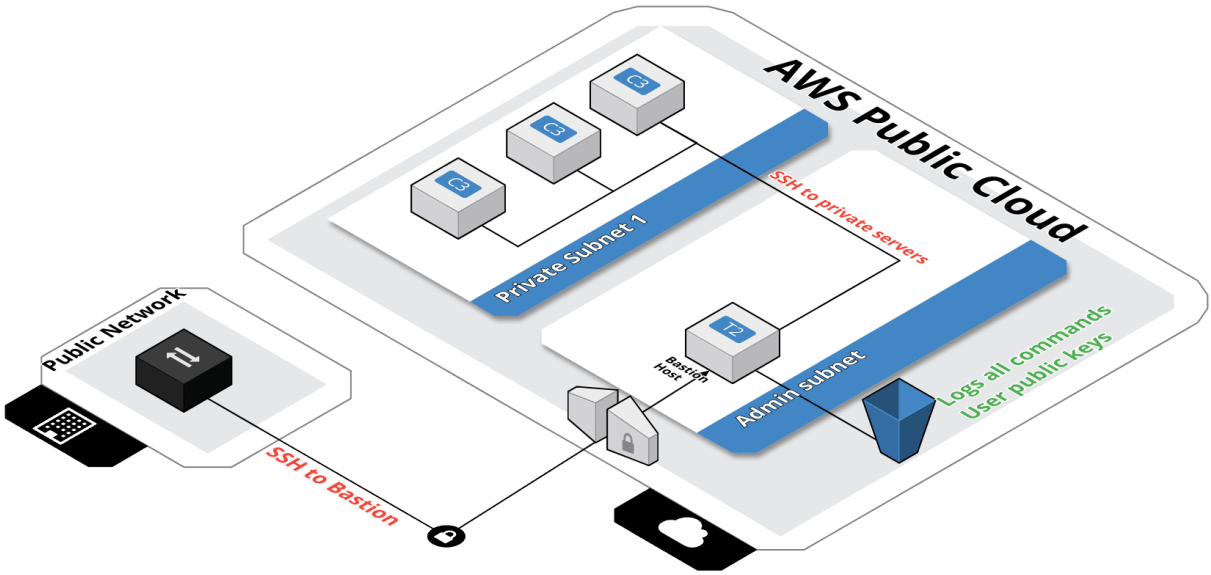
code helpers 2

Terraform module which creates a secure SSH bastion on AWS.

Mainly inspired by Securely Connect to Linux Instances Running in a Private Amazon VPC

Features

This module will create an SSH bastion to securely connect in SSH to your private instances.



All SSH commands are logged on an S3 bucket for security compliance, in the /logs path.

SSH users are managed by their public key, simply drop the SSH key of the user in the /public-keys path of the bucket. Keys should be named like 'username.pub', this will create the user 'username' on the bastion server. Username must contain alphanumeric characters only.

Then after you'll be able to connect to the server with :

```
ssh [-i path_to_the_private_key] username@bastion-dns-name
```

From this bastion server, you'll able to connect to all instances on the private subnet.

If there is a missing feature or a bug - open an issue.

Usage

```
module "bastion" {
  source = "Guimove/bastion/aws"
  bucket_name = "my_famous_bucket_name"
  region = "eu-west-1"
  vpc_id = "my_vpc_id"
  is_lb_private = "true|false"
  bastion_host_key_pair = "my_key_pair"
  create_dns_record = "true|false"
  hosted_zone_id = "my.hosted.zone.name."
  bastion_record_name = "bastion.my.hosted.zone.name."
  bastion_iam_policy_name = "myBastionHostPolicy"
  elb_subnets = [
    "subnet-id1a",
    "subnet-id1b"
  ]
  auto_scaling_group_subnets = [
    "subnet-id1a",
    "subnet-id1b"
  ]
  tags = {
    "name" = "my_bastion_name",
    "description" = "my_bastion_description"
  }
}
```

Requirements

Name	Version
terraform	~> 1.0
aws	~> 4.0

Providers

<<<<<<< HEAD

Name	Version
aws	~> 5.0

=======

Name	Version
aws	~> 4.0

Modules

No modules.

Resources

Name	Type
aws_autoscaling_group.bastion_auto_scaling_group	resource
aws_iam_instance_profile.bastion_host_profile	resource
aws_iam_policy.bastion_host_policy	resource
aws_iam_role.bastion_host_role	resource
aws_iam_role_policy_attachment.bastion_host	resource
aws_kms_alias.alias	resource
aws_kms_key.key	resource
aws_launch_template.bastion_launch_template	resource
aws_lb.bastion_lb	resource
aws_lb_listener.bastion_lb_listener_22	resource
aws_lb_target_group.bastion_lb_target_group	resource
aws_route53_record.bastion_record_name	resource
aws_s3_bucket.bucket	resource
aws_s3_bucket_acl.bucket	resource
aws_s3_bucket_lifecycle_configuration.bucket	resource
aws_s3_bucket_ownership_controls.bucket-acl-ownership	resource

Name	Type
aws_s3_bucket_server_side_encryption_configuration.bucket	resource
aws_s3_bucket_versioning.bucket	resource
aws_s3_object.bucket_public_keys_readme	resource
aws_security_group.bastion_host_security_group	resource
aws_security_group.private_instances_security_group	resource
aws_security_group_rule.egress_bastion	resource
aws_security_group_rule.ingress_bastion	resource
aws_security_group_rule.ingress_instances	resource
aws_ami.amazon-linux-2	data source
aws_iam_policy_document.assume_policy_document	data source
aws_iam_policy_document.bastion_host_policy_document	data source
aws_kms_alias.kms-ebs	data source
aws_subnet.subnets	data source

Inputs

Name	Description	Type	Default	Required
allow_ssh_commands	Allows the SSH user to execute one-off commands. Pass true to enable. Warning: These commands are not logged and increase the vulnerability of the system. Use at your own discretion.	`bool`	`false`	no
associate_public_ip_address	n/a	`bool`	`true`	no
auto_scaling_group_subnets	List of subnets where the Auto Scaling Group will deploy the instances	`list(string)`	n/a	yes

Name	Description	Type	Default	Required
bastion_additional_security_groups	List of additional security groups to attach to the launch template	`list(string)`	`[]`	no
bastion_ami	The AMI that the Bastion Host will use.	`string`	`""`	no
bastion_host_key_pair	Select the key pair to use to launch the bastion host	`string`	n/a	yes
bastion_iam_permissions_boundary	IAM Role Permissions Boundary to constrain the bastion host role	`string`	`""`	no
bastion_iam_policy_name	IAM policy name to create for granting the instance role access to the bucket	`string`	`"BastionHost"`	no
bastion_iam_role_name	IAM role name to create	`string`	`null`	no
bastion_instance_count	n/a	`number`	`1`	no
bastion_launch_template_name	Bastion Launch template Name, will also be used for the ASG	`string`	`"bastion-lt"`	no
bastion_record_name	DNS record name to use for the bastion	`string`	`""`	no
bastion_security_group_id	Custom security group to use	`string`	`""`	no
bucket_force_destroy	The bucket and all objects should be destroyed when using true	`bool`	`false`	no
bucket_name	Bucket name where the bastion will store the logs	`string`	n/a	yes
bucket_versioning	Enable bucket versioning or not	`bool`	`true`	no

Name	Description	Type	Default	Required
cidrs	List of CIDRs that can access the bastion. Default: 0.0.0.0/0	`list(string)`	`[ "0.0.0.0/0" ]`	no
create_dns_record	Choose if you want to create a record name for the bastion (LB). If true, 'hosted_zone_id' and 'bastion_record_name' are mandatory	`bool`	n/a	yes
create_elb	Choose if you want to deploy an ELB for accessing bastion hosts. Only select false if there is no need to SSH into bastion from outside. If true, you must set elb_subnets and is_lb_private	`bool`	`true`	no
disk_encrypt	Instance EBS encryption	`bool`	`true`	no
disk_size	Root EBS size in GB	`number`	`8`	no
elb_subnets	List of subnets where the ELB will be deployed	`list(string)`	`[]`	no
enable_http_protocol_ipv6	Enables or disables the IPv6 endpoint for the instance metadata service	`bool`	`false`	no
enable_instance_metadata_tags	Enables or disables access to instance tags from the instance metadata service	`bool`	`false`	no

Name	Description	Type	Default	Required
enable_logs_s3_sync	Enable cron job to copy logs to S3	`bool`	`true`	no
extra_user_data_content	Additional scripting to pass to the bastion host. For example, this can include installing PostgreSQL for the `psql` command.	`string`	`""`	no
hosted_zone_id	Name of the hosted zone where we'll register the bastion DNS name	`string`	`""`	no
http_endpoint	Whether the metadata service is available	`bool`	`true`	no
http_put_response_hop_limit	The desired HTTP PUT response hop limit for instance metadata requests	`number`	`1`	no
instance_type	Instance size of the bastion	`string`	`"t3.nano"`	no
ipv6_cidrs	List of IPv6 CIDRs that can access the bastion. Default: ::/0	`list(string)`	`[ "::/0" ]`	no
is_lb_private	If TRUE, the load balancer scheme will be "internal" else "internet-facing"	`bool`	`null`	no
kms_enable_key_rotation	Enable key rotation for the KMS key	`bool`	`false`	no
log_auto_clean	Enable or disable the lifecycle	`bool`	`false`	no
log_expiry_days	Number of days before logs expiration	`number`	`90`	no

Name	Description	Type	Default	Required
log_glacier_days	Number of days before moving logs to Glacier	`number`	`60`	no
log_standard_ia_days	Number of days before moving logs to IA Storage	`number`	`30`	no
private_ssh_port	Set the SSH port to use between the bastion and private instance	`number`	`22`	no
public_ssh_port	Set the SSH port to use from desktop to the bastion	`number`	`22`	no
region	n/a	`string`	n/a	yes
tags	A mapping of tags to assign	`map(string)`	`{}`	no
use_imds_v2	Use (IMDSv2) Instance Metadata Service V2	`bool`	`false`	no
vpc_id	VPC ID where we'll deploy the bastion	`string`	n/a	yes
bastion_security_group_used	Use the external or existing security group or not	`bool`	`true`	yes

Outputs

Name	Description
bastion_auto_scaling_group_name	The name of the Auto Scaling Group for bastion hosts
bastion_elb_id	The ID of the ELB for bastion hosts
bastion_host_security_group	The ID of the bastion host security group
bucket_arn	The ARN of the S3 bucket
bucket_kms_key_alias	The name of the KMS key alias for the bucket
bucket_kms_key_arn	The ARN of the KMS key for the bucket
bucket_name	The ID of the S3 bucket
elb_arn	The ARN of the ELB for bastion hosts

Name	Description
elb_ip	The DNS name of the ELB for bastion hosts
private_instances_security_group	The ID of the security group for private instances
target_group_arn	The ARN of the target group for the ELB
public_ip	The public ip of ELB or one single instance
private_ip	The private ip of ELB or one single instance

Known issues

Tags are not applied to the instances generated by the auto scaling group do to known terraform issue : terraform-providers/terraform-provider-aws#290

Change of disk encryption isn't propagate immediately. Change have to trigger manually from AWS CLI: Auto Scaling Groups -> Instance refresh . Keep in mind all data from instance will be lost in case there are temporary or custom data.

Authors

Module managed by Guimove.

License