Table of Contents

In-Account Scanning

Configure In-Account Scanning

To configure in-account scanning, create and onboard a dedicated account, and then grant Tenable Cloud Security permissions to provision the necessary infrastructure resources in the target account.

To configure in-account scanning:

1. Create one or more dedicated account/s for scanning purposes.

    - Only one scanning account can be defined per **scope** in Tenable Cloud Security. A scanning account can only be mapped to a single scope.
    - Customers are responsible for any relevant compute costs associated with such accounts (estimated at about $300 per region). See **Resources Provisioned per Region** for more information.

2. Onboard the account in Tenable Cloud Security.

3. Depending on your cloud provider, add the following to the account to grant Tenable the necessary permissions required to manage compute resources:

    - **AWS**. Add the following custom, inline policy to the IAM role you created during onboarding:

      JSON Copy

      ```json
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": [
              "autoscaling:UpdateAutoScalingGroup",
              "ec2:*",
              "eks:*",
              "iam:AttachRolePolicy",
              "iam:CreateOpenIDConnectProvider",
      ```

```
        "iam:CreateRole",
        "iam:CreateServiceLinkedRole",
        "iam:DeleteOpenIDConnectProvider",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:TagRole",
        "iam:UpdateAssumeRolePolicy",
        "kms:CreateAlias",
        "kms:CreateGrant",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:DescribeKey",
        "kms:EnableKeyRotation",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "kms:ScheduleKeyDeletion",
        "kms:TagResource",
        "license-manager:ListReceivedLicenses",
        "resource-groups:*"
      ],
      "Resource": "*"
    }
  ]
}
```

- **Azure**. Assign the following roles to the Tenable Cloud Security Connector app:
  - *Built-in roles*:
    - `Azure Kubernetes Service RBAC Cluster Admin`
    - `Contributor`
    - `Key Vault Crypto Officer`
    - `Role Based Access Control Administrator`
  - *Custom role*:

JSON Copy

```json
{
    "properties": {
        "roleName":
"WorkloadAnalysisInAccountStorageRole",
        "description": "",
        "assignableScopes": [
            "/subscriptions/SubscriptionID"
        ],
        "permissions": [
            {
                "actions": [

"Microsoft.Authorization/roleDefinitions/write",

"Microsoft.Compute/disks/delete",

"Microsoft.Compute/disks/read",

"Microsoft.Compute/disks/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listkeys/action"
                ],
                "notActions": [],
                "dataActions": [

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"
                ],
                "notDataActions": []
            }
        ]
    }
}
```

- **GCP**. Add the following roles to the Tenable Cloud Security service account you created during onboarding:
    - `Cloud KMS Admin`
    - `Editor`
    - `Kubernetes Engine Admin`
    - `Service Account Admin`

4. Contact Support for help completing the process. At this point:

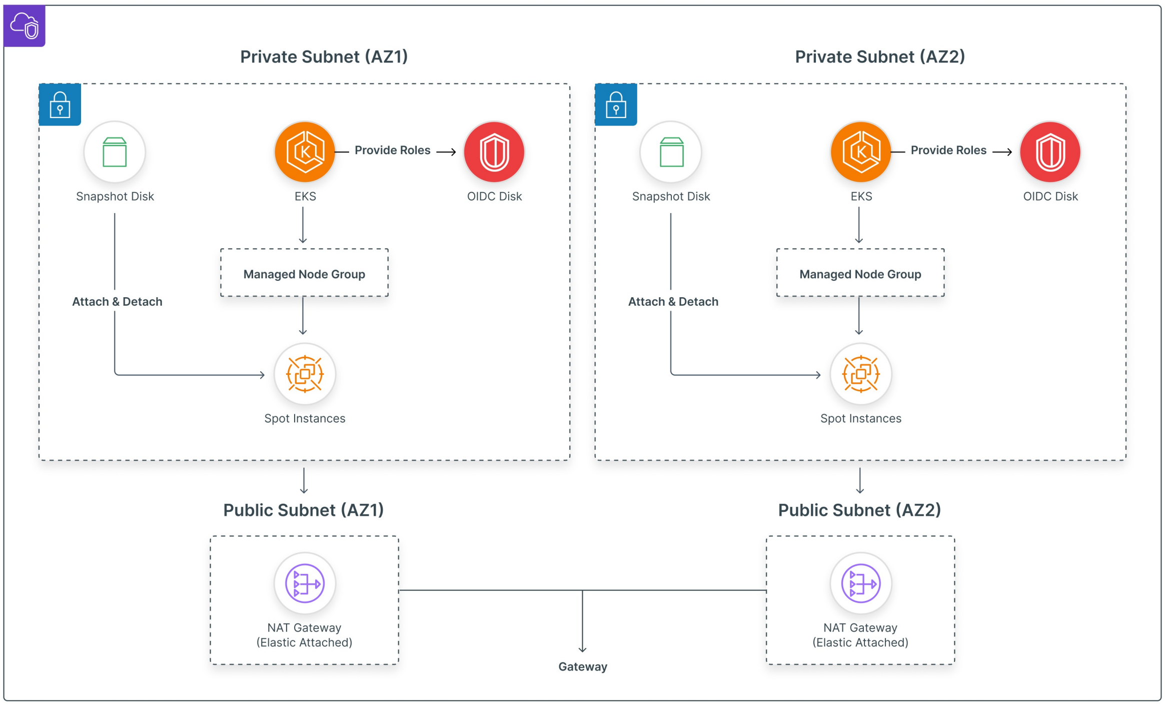
    - Tenable will provision the necessary compute resources for each region in which you have virtual machines. See Resources Provisioned per Region for more information.
    - Tenable will orchestrate the scanning on a regular basis.

Resources Provisioned per Region

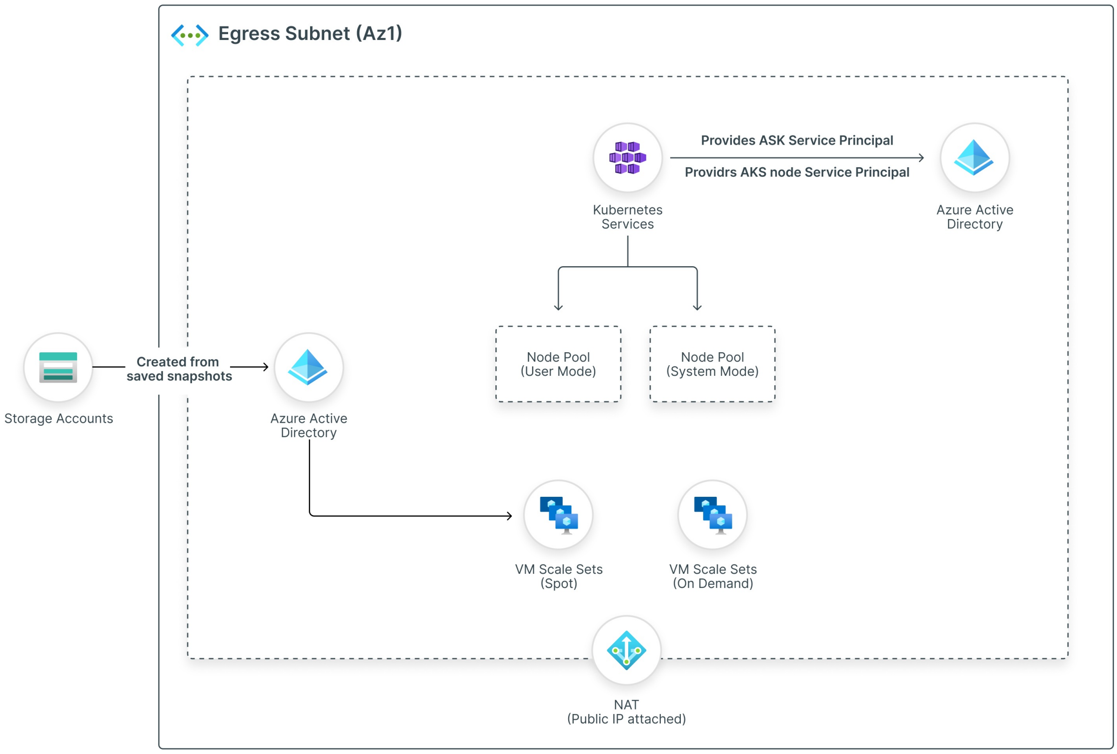
	AWS	Azure	GCP
Compute	• 1 EKS cluster • Nodes[1]	• AKS cluster • 1 On demand virtual machine, 2 CPU and 8 GB RAM • 1 Spot virtual machine, 2 CPU and 8 GB RAM	• 1 GKE cluster • 1 Spot machine - e2-standard-2 (2vCPU and 8 GB RAM)
Identities	• 3 IAM roles • 1 OIDC identity provider	2 User Managed Identities	1 service account (per project)
Storage	n/a	• 1 Storage Account • 1 Storage account blob container	n/a
Network	• 2 Elastic IPs • 1 Internet Gateway • 2 NAT Gateways • 4 Route tables • 4 Security Groups • 4 Subnets • 1 VPC	• 2 Network Security Groups • 1 NAT gateway • 1 Public IP • 1 Virtual Network • 1 Subnet	• 1 Subnet • 1 Router • 1 VPC (per project)
Cost (per month)	$300	$300	$300
Capacity (per day)	5,000 VMs	5,000 VMs	5,000 VMs

[1] The number and size of provisioned nodes is automatically managed by Tenable Cloud Security to simultaneously minimize costs while meeting scanning demands.

Sample AWS Architecture



Sample Azure Architecture



Frequently Asked Questions

Q: How does Tenable Cloud Security deploy multiple clusters in multiple datacenters?

A: Tenable will provision the necessary compute resources for each region in which you have virtual machines. See Resources Provisioned per Region and Sample AWS Architecture for more information.

Q: Can I use the AWS outpost to deploy this on an on-premises virtualized data center?

A: No. The outpost is only available for scanning cloud-hosted virtual machines.

Powered by Document360