Tenable Cloud Security Quick Reference Guide: Agentless Assessment

Last Revised: September 06, 2023

Table of Contents

Tenable Cloud Security Quick Reference Guide: Agentless Assessment 3

Overview 4

Workflows 6

Learn More About Agentless Assessment 7

Create a Project 8

AWS Agentless Assessment Workflow 9

Agentless Assessment Requirements for AWS 11

AWS IAM Role for Agentless Assessment 14

Set Up Read-Only Access to the AWS Account 16

Onboard AWS Accounts 25

Onboard an AWS Organization 26

Onboard an AWS Account 31

Create an AWS Snapshot 32

Create AWS Snapshot Manually 33

Automate Snapshot Creation with AWS Data Lifecycle Manager (DLM) 36

Configure Vulnerability Scan using Agentless Assessment for AWS 37

Azure Agentless Assessment Workflow 40

Agentless Assessment Requirements for Azure 42

Create an Azure Service Principal Role 44

Register an application with Azure 46

Create a custom role and assign it to the service principal 47

Assign the Reader role to the service principal 54

Create a client secret 58

Onboard an Azure Account 60

Create an Azure Virtual Machine Snapshot 61

Create Azure Virtual Machine Snapshot Manually 63

Automate Azure Virtual Machine Snapshot Creation 65

Configure Vulnerability Scan using Agentless Assessment for Azure 66

Run a Cloud Scan 68

View Vulnerabilities 69

Tenable Cloud Security Quick Reference Guide: Agentless Assessment

This Quick Reference Guide provides information about using Agentless Assessment in Tenable Cloud Security (formerly known as Tenable.cs).

Overview

Agentless Assessment allows you to scan and analyze short-lived cloud instances on your cloud environments. You can scan both online and offline systems with Agentless Assessment. Agentless Assessment relies on API data and snapshots and does not depend on data from Tenable or other cloud-vendor agents.

Agentless Assessment supports the following:

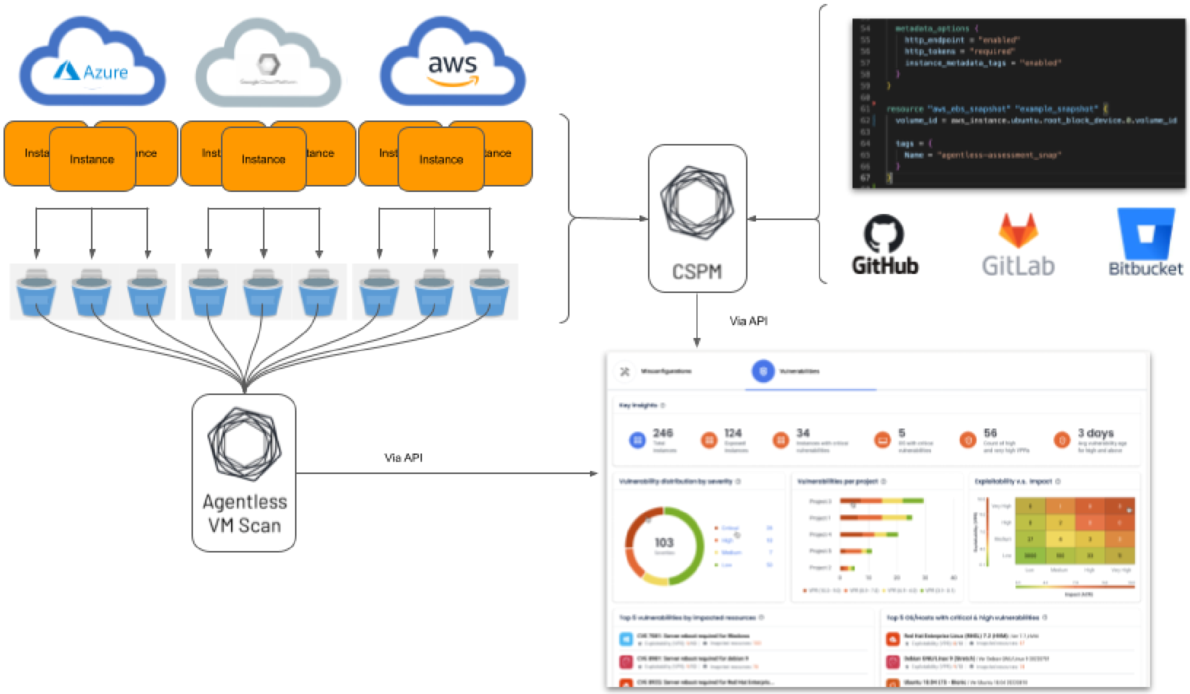
- AWS EC2 Instances.
- Azure Virtual Machines.

The following are the key benefits of vulnerability scanning using Agentless Assessment:

- No need for any software installation on scan targets.
- No impact on system resources.
- No need for any system credentials to perform the scans. Agentless Assessment requires read-only access to your AWS EBS.
- Live Results feature that always give you the latest Tenable threat updates without running a new scan.

Agentless Assessment is based on Amazon EBS snapshots of your workload EC2 instances. For Azure, Agentless assessment is based on snapshots of your virtual machines. When you trigger a cloud scan in Tenable Cloud Security, along with detecting your cloud resources and mis-configurations, Tenable Cloud Security also detects vulnerabilities in your AWS EC2 workload instances and Azure virtual machines. You can view these vulnerabilities on the **Findings > Vulnerabilities** page in Tenable Cloud Security and the **Findings** page in Tenable Vulnerability Management.

The following image shows a high-level overview of Agentless Assessment:



```
    metadata_options {
      http_endpoint = "enabled"
      http_tokens = "required"
      instance_metadata_tags = "enabled"
    }
  }

  resource "aws_ebs_snapshot" "example_snapshot" {
    volume_id = aws_instance.ubuntu.root_block_device.0.volume_id

    tags = {
      Name = "agentless-assessment_snap"
    }
  }
```

> **Note:** Agentless Assessment supports only root volume scanning and scans software installed at the operating system level.

Why Agentless Assessment

Agentless Assessment makes it easier to onboard and manage cloud accounts and is best suited for cloud-native environments. Key benefits include:

- **Agentless is Region Agnostic**: Agentless does not require any deployment in any cloud region. Agentless Assessment requires no SSM agents, Azure runbooks, or local commands and their associated performance costs; and it provides more detailed visibility into the cloud inventories.
- **Agentless Assessment is API Based**: Agentless Assessment uses APIs to gather data from block storage snapshots. As a result, Agentless Assessment collects more data, allows lighter-weight cloud instances, and can automatically discover new workloads.

Workflows

Use the following workflows and steps to set up and run Agentless Assessment:

- Agentless Assessment for AWS
- Agentless Assessment for Azure

Learn More About Agentless Assessment

- Tenable Cloud Security Documentation
- Tenable Blog: Introducing Tenable Cloud Security with Agentless Assessment and Live Results
- Tenable Blog: Accelerate Vulnerability Detection and Response for AWS with Tenable Cloud Security Agentless Assessment

Create a Project

In Tenable Cloud Security Console, you can group resources, such as repositories and cloud accounts, into projects. Projects allow you to monitor, analyze, and manage all your resources at once.

To create a project:

1. In the left navigation bar, click ⊕ > **Project**.
2. In the **Give the project a name** section, type a name for your project.

   > **Note:** A project name can have a maximum of 25 characters.

3. Click **Continue**.
4. Click **Create**.

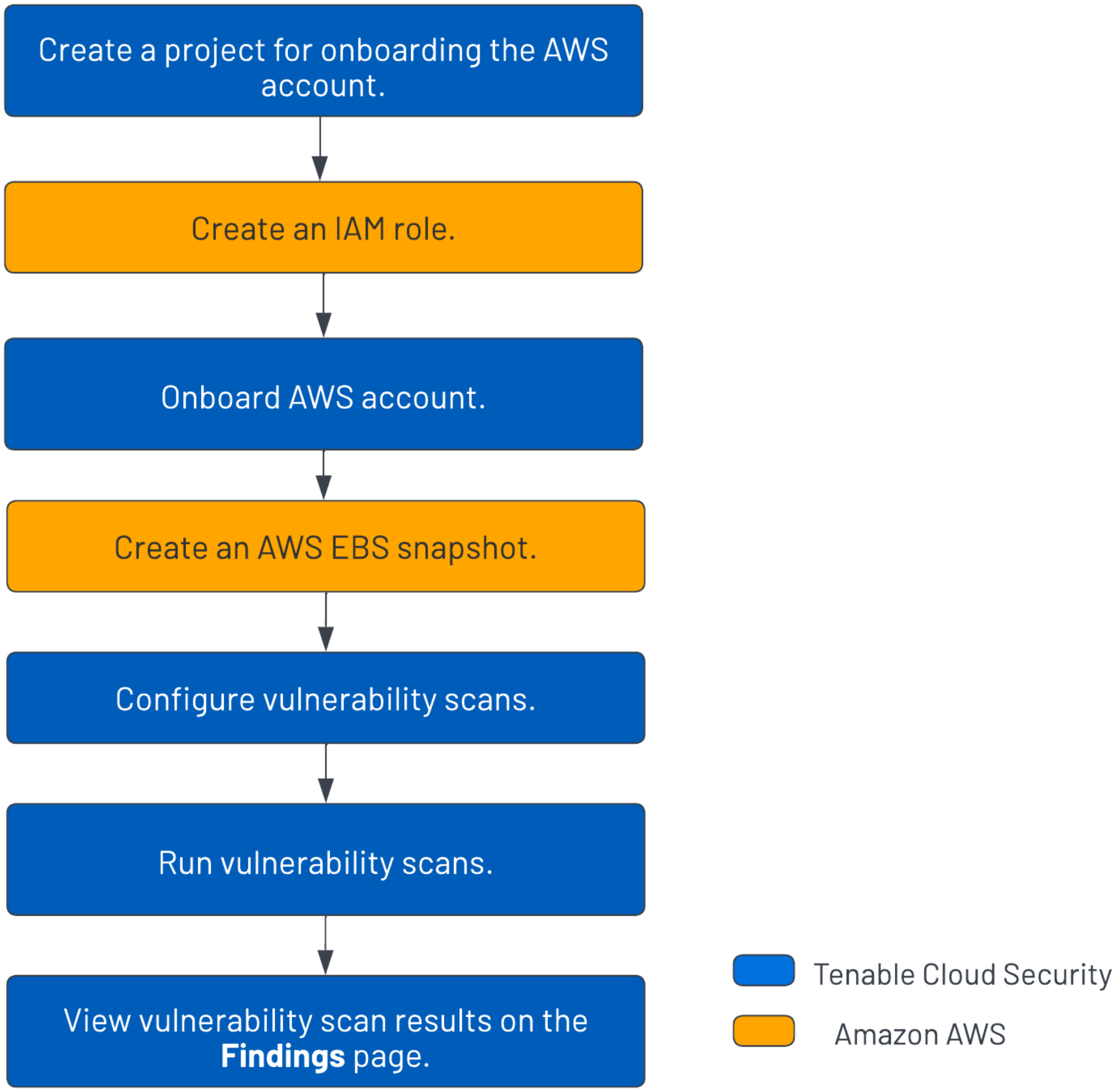
   A confirmation message appears and Tenable Cloud Security creates the project. You can view the new project on the **Projects & Connections** page.

   What to do next:

   - AWS Agentless Assessment Workflow
   - Azure Agentless Assessment Workflow

AWS Agentless Assessment Workflow

The following workflow shows the process to set up Agentless Assessment and view the results:


Create a project for onboarding the AWS account.
Create an IAM role.
Onboard AWS account.
Create an AWS EBS snapshot.
Configure vulnerability scans.
Run vulnerability scans.
View vulnerability scan results on the **Findings** page.
Tenable Cloud Security
Amazon AWS

To set up Agentless Assessment for AWS:

1. Create a project for onboarding the AWS account.

2. Create an IAM role.

3. Onboard AWS account.

4. Create an AWS EBS snapshot.
5. Configure vulnerability scans using Agentless Assessment.
6. Run cloud scans.
7. View cloud scan results on the Tenable Cloud Security **Findings > Vulnerabilities** page and the **Findings** page on Tenable Vulnerability Management.

Agentless Assessment Requirements for AWS

The following requirements must be met for performing Agentless Assessment:

- IAM Role for Tenable Cloud Security
- AWS Snapshots
- Supported Operating Systems for AWS
- Supported File Systems
- Supported Regions for AWS

AWS IAM Role

Agentless Assessment of EC2 instances requires an IAM role that grants Tenable Cloud Security permission to read block data from Elastic Block Store (EBS) volumes. The role must provide Tenable Cloud Security the following EBS permissions:

- ebs:ListSnapshotBlocks
- ebs:ListChangedBlocks
- ebs:GetSnapshotBlock

Follow the instructions on the Set Up Read-Only Access to the AWS Account page to configure your IAM role with the appropriate permissions for Agentless Assessments.

Snapshots encrypted with Key Management Service (KMS) must grant the IAM role with access to the KMS key(s) used to encrypt these snapshots. Modify the KMS key's resource policy to include the following permissions:

- kms:Decrypt
- kms:DescribeKey

For more information, see Required AWS KMS key policy for use with encrypted volumes in AWS documentation.

AWS Snapshots

Agentless Assessment utilizes Amazon EBS snapshots of your workload EC2 instances. Ensure snapshots have been created for the EC2 instances that you want to scan. For more information, see Create an AWS Snapshot. AMIs do not require any additional preparation to initiate Agentless Assessment.

Supported Operating Systems for AWS

- Amazon Linux 2023
- Amazon Linux 2
- CentOS 7
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES) 11.4 to 15.2
- Ubuntu
- Debian

Supported File Systems

- XFS
- ext4

Supported Regions for AWS

You can perform Agentless scans on the following AWS regions:

- `us-east-1`
- `us-west-1`
- `us-east-2`
- `us-west-2`
- `ap-southeast-1`
- `ap-southeast-2`
- `ap-northeast-1`

- `ap-northeast-2`
- `ap-northeast-3`
- `ap-south-1`
- `eu-central-1`
- `eu-north-1`
- `ca-central-1`
- `eu-west-1`
- `eu-west-2`
- `eu-west-3`
- `sa-east-1`

AWS IAM Role for Agentless Assessment

Agentless Assessment of AMIs and EC2 instances requires an IAM Role that grants the Tenable Cloud Security role access to the AWS-Managed Policy **ReadOnlyAccess** as well as permissions to read block data from Elastic Block Store (EBS) volumes.

The role must provide Tenable Cloud Security the following permissions:

- ReadOnlyAccess (AWS-Managed Policy)
- ebs:ListSnapshotBlocks
- ebs:ListChangedBlocks
- ebs:GetSnapshotBlock

For the EBS requirement with Agentless Assessment, create an inline policy with the following JSON to provide EBS permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ebs:List*",
                "ebs:Get*"
            ],
            "Resource": "*"
        }
    ]
  }
```

For additional instructions on configuring the AWS IAM Role, see Set Up Read-Only Access to the AWS Account.

Snapshots encrypted with Key Management Service (KMS) must grant the IAM role access to the KMS key(s) used to encrypt these snapshots. Modify the KMS key's resource policy to include the following permissions:

- kms:Decrypt
- kms:DescribeKey

The following example shows a custom inline policy that is assigned to the Tenable Cloud Security IAM Role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:[REGION]:[ACCOUNT-ID]:key/[KEY]"
    }
  ]
}
```

Note: In the JSON, replace the **Resource:** value with either ***** or with a list of the KMS keys used to encrypt volumes or snapshots for each region in the AWS account.

If preferred, you can add the Tenable Cloud Security IAM Role as a Key User instead of creating a custom KMS inline IAM policy. Navigate to the AWS KMS Service, find the KMS key used to encrypt the EBS Volumes and Snapshots, and add the Tenable Cloud Security IAM Role as a Key User.

Set Up Read-Only Access to the AWS Account

To read the resources in the Amazon Web Services (AWS) cloud account, Tenable Cloud Security requires appropriate permissions. Tenable Cloud Security recommends provisioning an IAM (Identity and Access Management) role in the target AWS cloud account and configuring it for Tenable Cloud Security to read the resources in the same account. When onboarding an AWS organization account, create an IAM role for the management account.

You can create the role in the following ways:

- Create a read-only role manually
- Create a read-only role using a script
- Create a read-only role using a CloudFormation Template

Create a read-only role manually

You can create a read-only role manually from the AWS management console.

Before you begin:

- Log in to the AWS web console with a user account with permission to create IAM roles.

  For more information about IAM roles, see Amazon's AWS Identity and Access Management User Guide.

To create a read-only role manually:

1. In the AWS web console, go to **Identity and Access Management (IAM)**.
2. On the left navigation pane, click **Roles**.

   The **Roles** page appears.
3. Click **Create Role**.

   The Create Role wizard appears.
4. In the **Select trusted entity** page, do the following:

a. In the **Trusted entity type** section, select **AWS Account**.

b. In the **An AWS Account** section, select **Another AWS Account**.

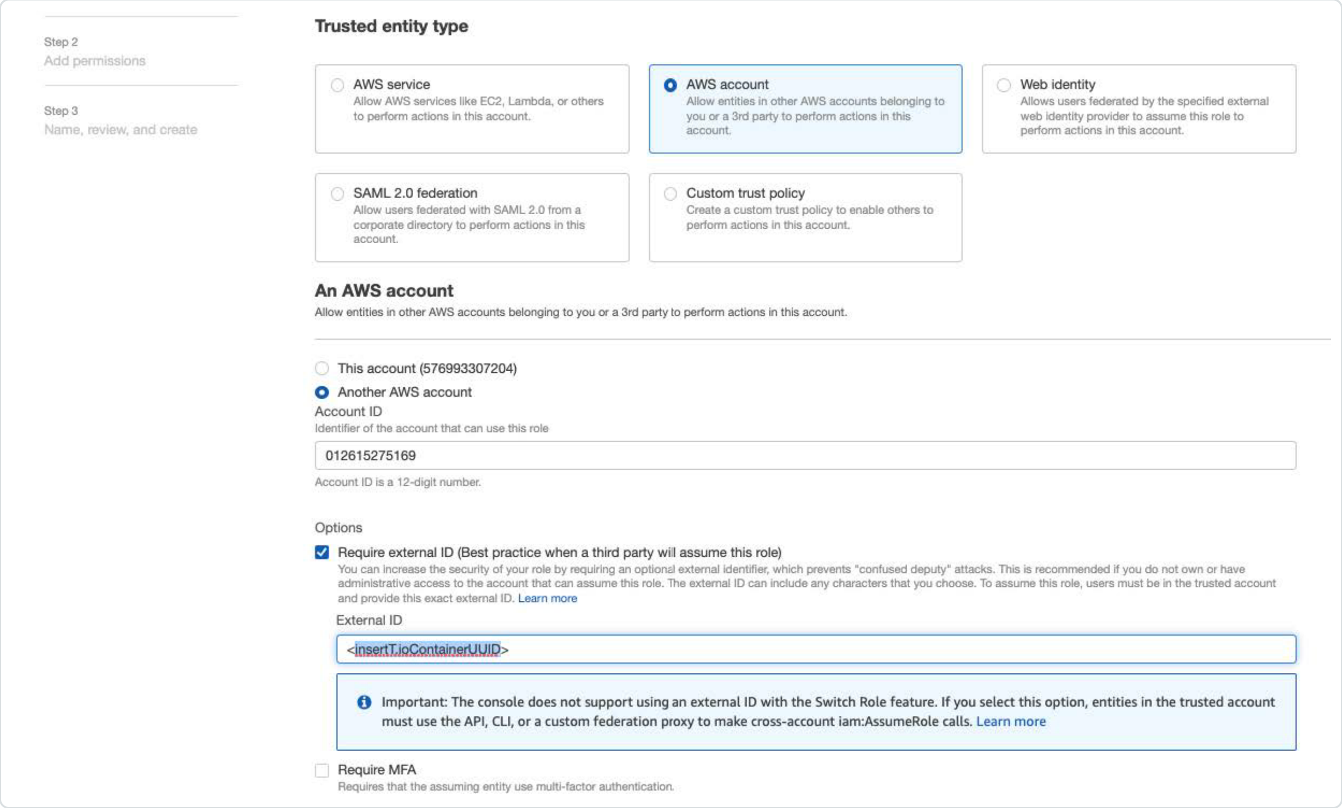
c. In the **Account ID** box, type **012615275169**.

> **Note:** 012615275169 is the account ID of the Tenable AWS account that you are establishing a trust relationship with to support AWS role delegation.

d. Under **Options**, click the **Require External ID** check box and type your Tenable Vulnerability Management Container UUID in the External ID box.

> **Note:** In Tenable Vulnerability Management, navigate to **Settings > License** to get your container UUID. For more information, see View Information about Your Tenable Vulnerability ManagementInstance.

e. Click **Next**.



Step 2
Add permissions

Step 3
Name, review, and create

Trusted entity type

○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

● AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ This account (576993307204)
● Another AWS account
Account ID
Identifier of the account that can use this role
012615275169
Account ID is a 12-digit number.

Options
☑ Require external ID (Best practice when a third party will assume this role)
You can increase the security of your role by requiring an optional external identifier, which prevents "confused deputy" attacks. This is recommended if you do not own or have administrative access to the account that can assume this role. The external ID can include any characters that you choose. To assume this role, users must be in the trusted account and provide this exact external ID. Learn more
External ID
<insertT.ioContainerUUID>

Important: The console does not support using an external ID with the Switch Role feature. If you select this option, entities in the trusted account must use the API, CLI, or a custom federation proxy to make cross-account iam:AssumeRole calls. Learn more

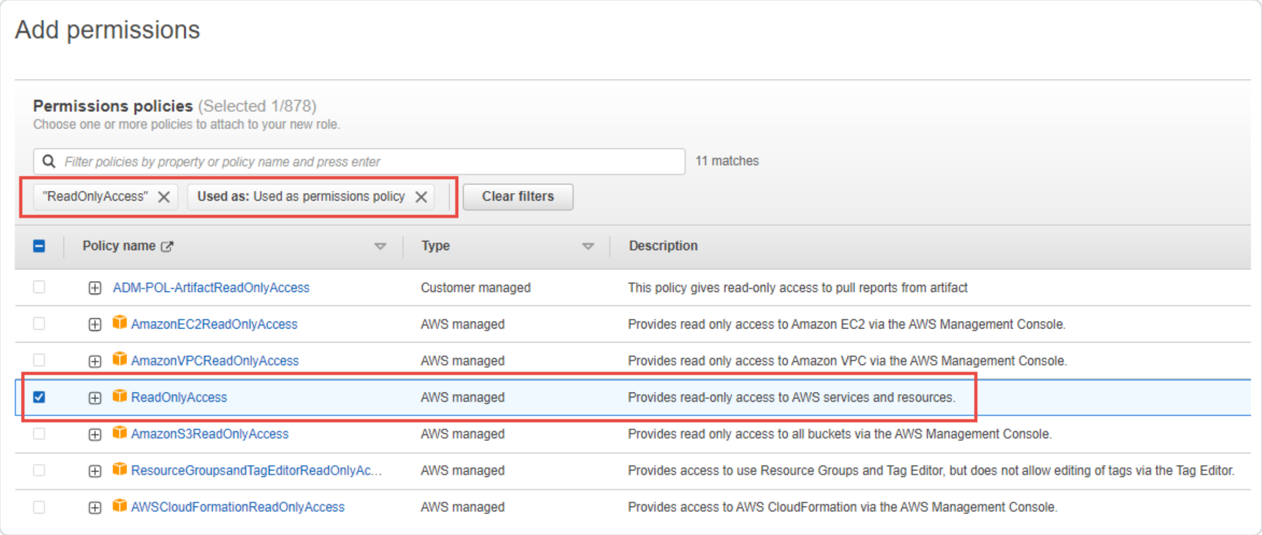
☐ Require MFA
Requires that the assuming entity use multi-factor authentication.

5. On the **Add permissions** page, perform the following:

a. Search for **ReadOnlyAccess** in the search box.

> **Tip:** Filtering for “ReadOnlyAccess” by role name might return many entries. Apply the ”Used as: Used as permissions policy" filter along with the role name “ReadOnlyAccess" to narrow down the search results.

b. Select the **ReadOnlyAccess** check box.



Add permissions

Permissions policies (Selected 1/878)
Choose one or more policies to attach to your new role.

Filter policies by property or policy name and press enter — 11 matches

"ReadOnlyAccess" ✕ | **Used as:** Used as permissions policy ✕ | Clear filters

	Policy name	Type	Description
☐	ADM-POL-ArtifactReadOnlyAccess	Customer managed	This policy gives read-only access to pull reports from artifact
☐	AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon EC2 via the AWS Management Console.
☐	AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon VPC via the AWS Management Console.
☑	ReadOnlyAccess	AWS managed	Provides read-only access to AWS services and resources.
☐	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all buckets via the AWS Management Console.
☐	ResourceGroupsandTagEditorReadOnlyAc...	AWS managed	Provides access to use Resource Groups and Tag Editor, but does not allow editing of tags via the Tag Editor.
☐	AWSCloudFormationReadOnlyAccess	AWS managed	Provides access to AWS CloudFormation via the AWS Management Console.

For the list of permissions and AWS resources scanned by Tenable Cloud Security with this policy, see Permissions and Supported Resources for AWS ReadOnlyAccess Policy.

c. For vulnerability scanning with Agentless Assessment, create an inline policy with the following JSON to provide Elastic Block Store permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ebs:List*",
                "ebs:Get*"
            ],
            "Resource": "*"
        }
    ]
  }
```

   d. Select the required policies for the IAM role and click **Next**.

   > **Note:**The new policy might take some time to get created. Refresh your browser if you do not see the policy in the list of policies.

   For information about creating IAM policies, see the [AWS documentation](#).

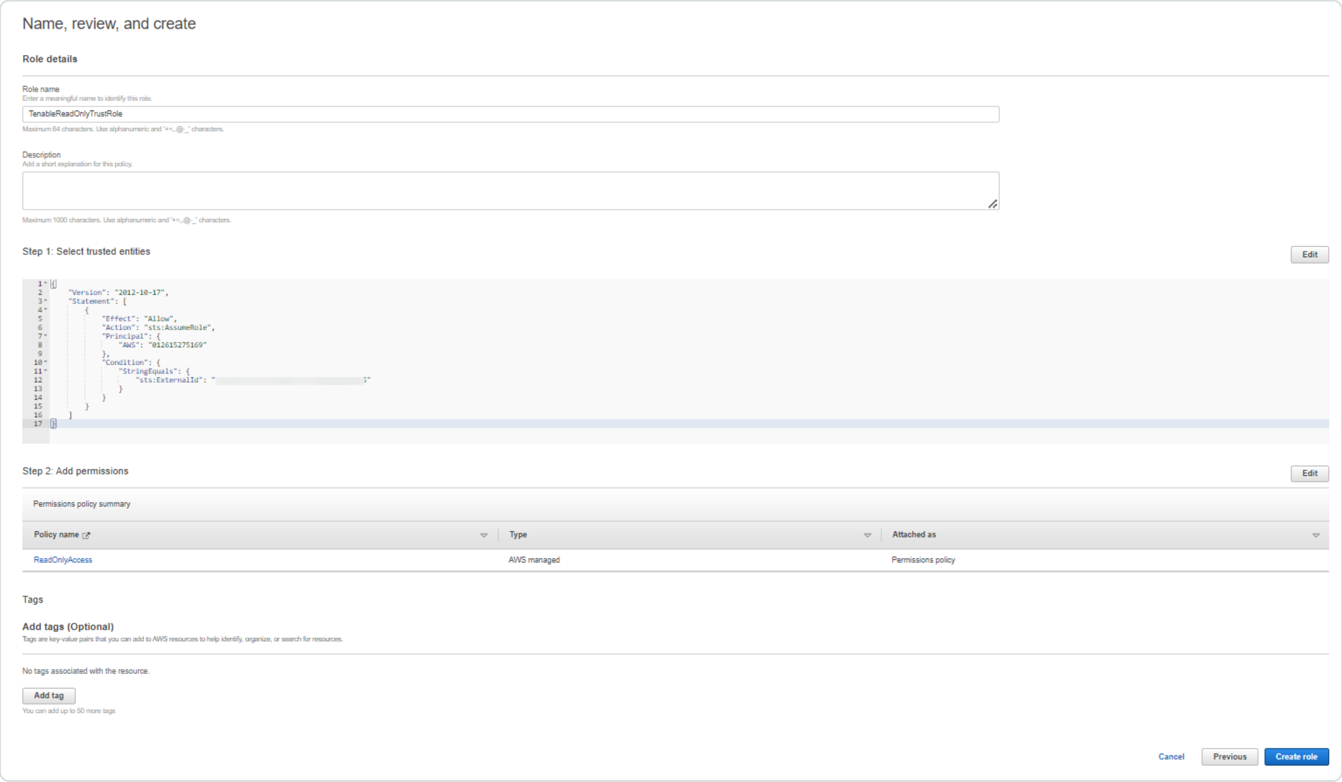
6. In the **Name, review, and create** page, do the following:

   a. In the **Role Details** section, type a **Role Name** for the role.

   b. (Optional) Add a role description in the **Description** box.

   c. (Optional) Click **Add Tags** to add key-value pairs to AWS resources.

   d. Click **Create Role**.



Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
TenableReadOnlyTrustRole
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this policy.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": "012615275169"
            },
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "[redacted]5"
                }
            }
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
ReadOnlyAccess	AWS managed	Permissions policy

Tags

Add tags (Optional)
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags

Tenable Cloud Security now has read-only access to your AWS account.

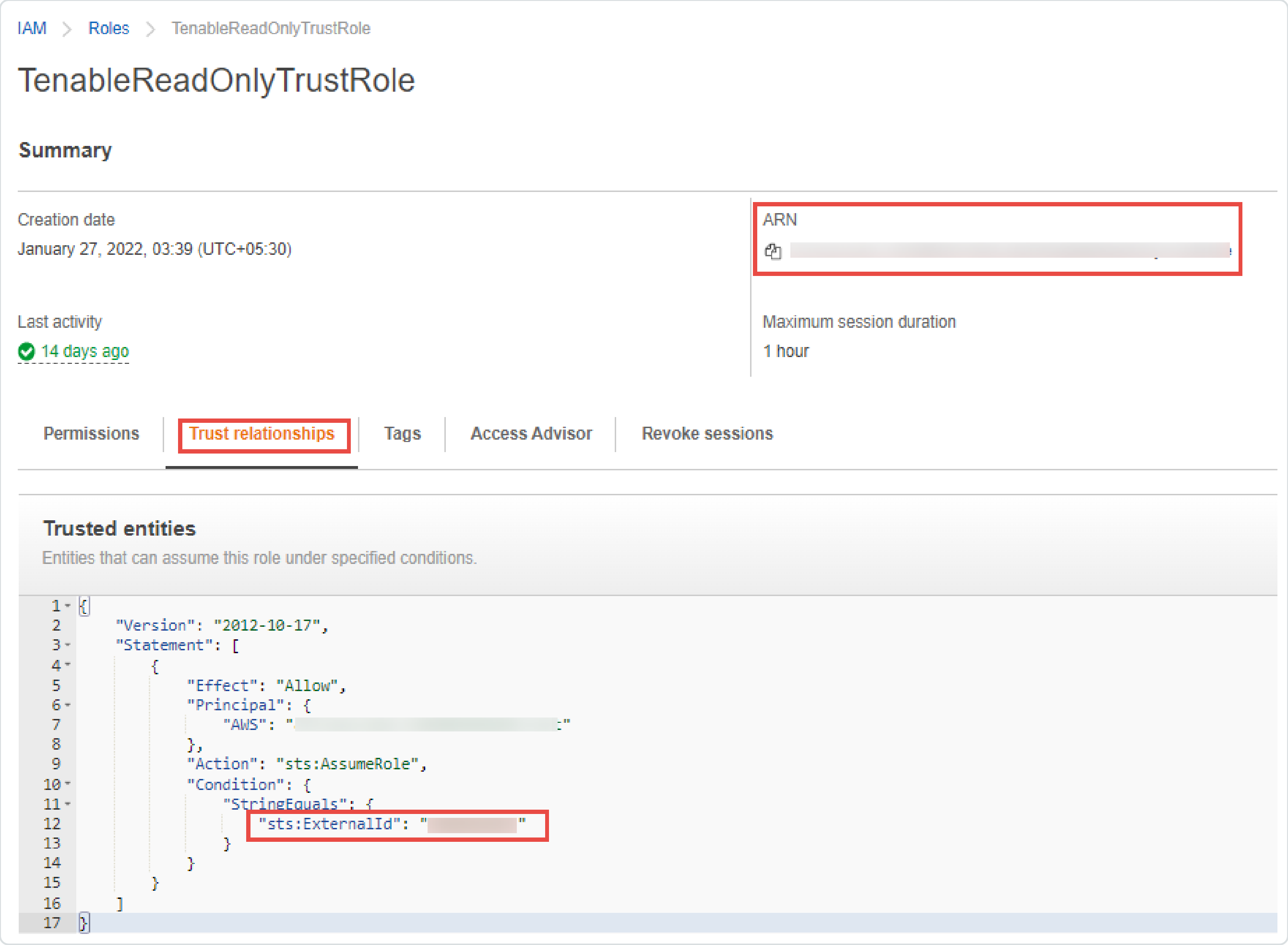
7. To get the **Role ARN** and **External ID** of this new role for Tenable Cloud Security, do the following:

a. On the left navigation pane, click **Roles**.

b. Search for the role that you created.

c. In the **Summary** section, note the **Role ARN** value.

d. Click the **Trust Relationships** tab and note the value of the **ExternalId** field.



TenableReadOnlyTrustRole

Summary

Creation date
January 27, 2022, 03:39 (UTC+05:30)

ARN
[redacted]

Last activity
14 days ago

Maximum session duration
1 hour

Trusted entities
Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "[redacted]"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "[redacted]"
                }
            }
        }
    ]
}
```

8. Note down the following values:

    - **Role ARN**
    - **External ID**

    You need these values when onboarding AWS accounts in Tenable Cloud Security.

Create a Read-Only Role Using a Script

You can run the script provided by Tenable Cloud Security to create an AWS read-only role.

Before you begin:

- You must have the following:
  - Terraform version 12 or higher
  - AWS access key
  - AWS secret key

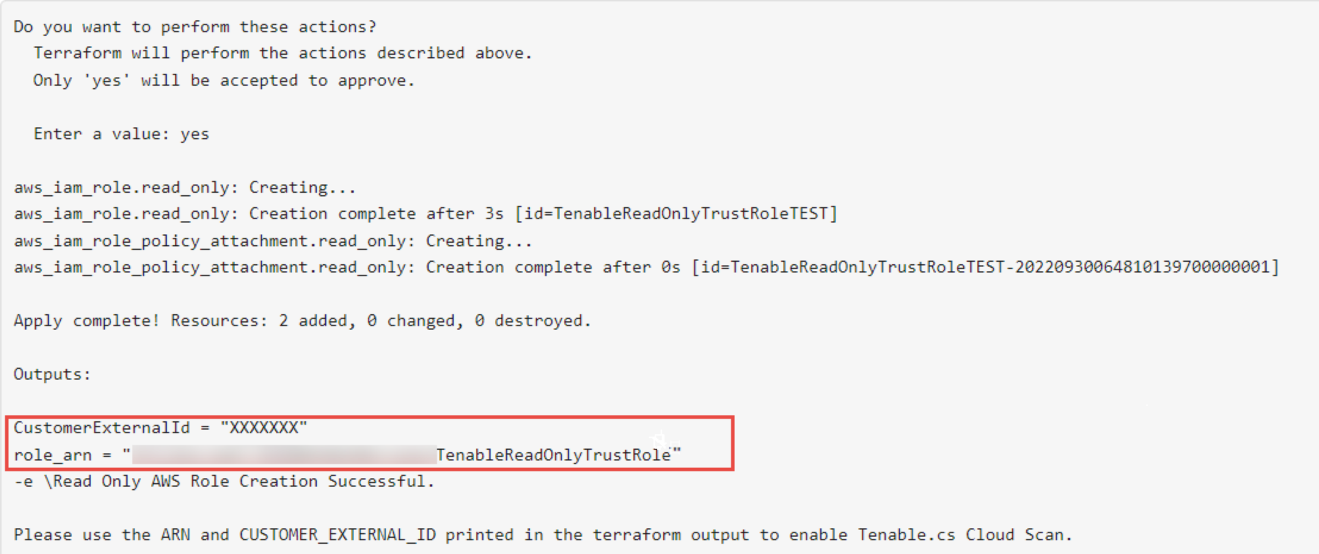
To create a read-only role using a script:

1. Run the following command:

   ```
   /bin/bash -c "$(curl https://downloads.accurics.com/downloads/io/create_tcs_aws_readonly_
   role.sh)"
   ```

2. Provide values for the following parameters, when prompted:
   - (Required) **AWS_ACCESS_KEY_ID**: Access key of the AWS account.
   - (Required) **AWS_SECRET_ACCESS_KEY**: Secret key of the AWS account.
   - (Optional) **Role name suffix**: By default, Tenable Cloud Security creates a role with the name *TenableReadOnlyTrustRole*. Provide an optional suffix to append to this role name. For example, if you provide ACME, the role name is TenableReadOnlyTrustRoleACME.
   - (Required) **ExternalId**: Provide an alphanumeric string to be used as the External ID of the role. The External ID can contain a minimum of 4 chars and a maximum of 1224 characters. Tenable recommends providing your Tenable Vulnerability Management Container UUID for the External ID.
3. When prompted **"Do you want to perform these actions?"**, type **yes** to continue.

   Tenable Cloud Security executes the script and creates the read-only role.



```
Do you want to perform these actions?
  Terraform will perform the actions described above.
  Only 'yes' will be accepted to approve.

  Enter a value: yes

aws_iam_role.read_only: Creating...
aws_iam_role.read_only: Creation complete after 3s [id=TenableReadOnlyTrustRoleTEST]
aws_iam_role_policy_attachment.read_only: Creating...
aws_iam_role_policy_attachment.read_only: Creation complete after 0s [id=TenableReadOnlyTrustRoleTEST-20220930064810139700000001]

Apply complete! Resources: 2 added, 0 changed, 0 destroyed.

Outputs:

CustomerExternalId = "XXXXXXX"
role_arn = "[redacted]TenableReadOnlyTrustRole"
-e \Read Only AWS Role Creation Successful.

Please use the ARN and CUSTOMER_EXTERNAL_ID printed in the terraform output to enable Tenable.cs Cloud Scan.
```

4. Note down the following values:

   - Role ARN
   - External ID

     You need these values when onboarding accounts in AWS.

Create a read-only role using a CloudFormation Template

You can deploy the Tenable Cloud Security stackset to create a read-only role.

Before you begin:

- Log in to the AWS web console.

To create a read-only role using a CloudFormation Template:

1. Click here to open the CloudFormation template to deploy a read-only role in AWS.

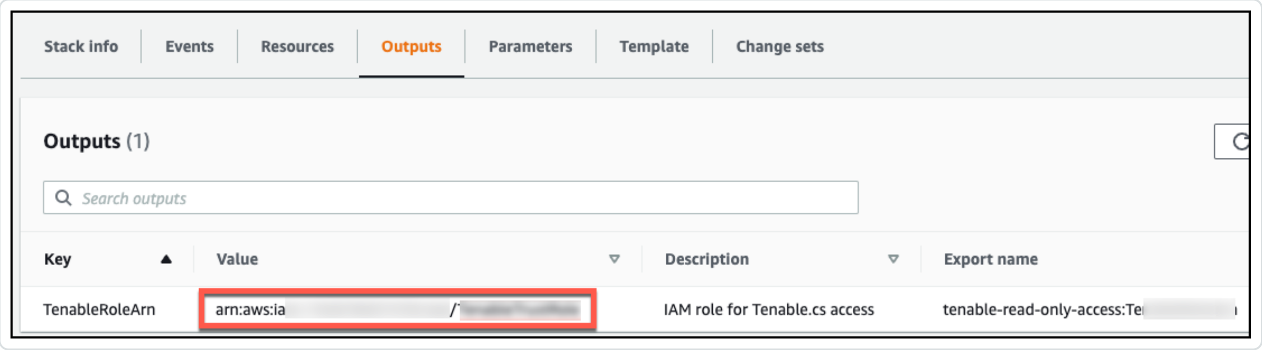
   Tenable Cloud Security redirects you to the **Quick create stack** page in AWS.

2. Review the parameters in the stack template and update, if required.
3. In the **Capabilities** section, select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names.** check box to confirm creating the IAM resources with required permissions.
4. Click **Create stack**.

Wait for the stack to get created and its status to become **CREATE_COMPLETE**.

5. Note down the following values:

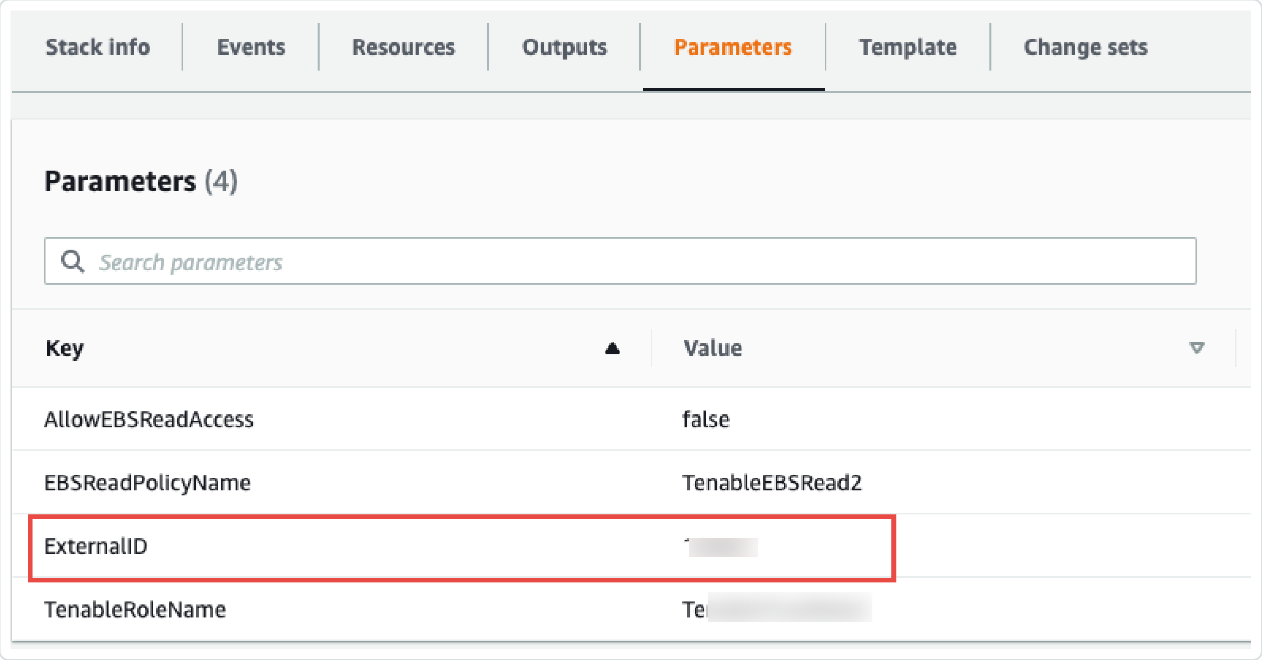
   - **Role ARN**: Copy the stack ARN of the deployed stack from the **Outputs** tab.



Outputs (1)

Key	Value	Description	Export name
TenableRoleArn	arn:aws:ia[redacted]/[redacted]	IAM role for Tenable.cs access	tenable-read-only-access:Te[redacted]

   - **External ID**: Copy the **ExternalID** from the **Parameters** tab.



Parameters (4)

Key	Value
AllowEBSReadAccess	false
EBSReadPolicyName	TenableEBSRead2
ExternalID	[redacted]
TenableRoleName	Te[redacted]

You need these values when onboarding AWS accounts in Tenable Cloud Security.

What to do next:

Onboard AWS Accounts

You must have the following values for onboarding the AWS account in Tenable Cloud Security:

- Role ARN
- External ID

Onboard AWS Accounts

You can connect your single, multiple or all Amazon Web Services (AWS) accounts as a part of your AWS project. For a detailed workflow for onboarding AWS accounts, see the Tenable Cloud Security Quick Reference Guide: Onboarding AWS Accounts.

To onboard AWS accounts in Tenable Cloud Security, each AWS account being onboarded must be associated with a role granting the **ReadOnlyAccess** policy to the Tenable AWS account. Tenable Cloud Security requires the Role ARN and External ID to onboard the AWS account. When onboarding an AWS Organization, Tenable Cloud Security provides you with a StackSet that recursively adds that role to all accounts under the organization. Tenable Cloud Security requires the StackSet ARN to onboard the organization. For more information, see the following topics:

- To connect multiple or all AWS accounts, see Onboard an AWS Organization.
- To connect a single AWS account, see Onboard an AWS Account.

Onboard an AWS Organization

Tenable Cloud Security can connect to your AWS organization's management account to discover all the member accounts under that account. This is the recommended method when you want to onboard all of your AWS accounts in Tenable Cloud Security Tenabfor security assessment. You must have the required permissions to deploy a CloudFormation stack for setting up access roles in each of the member accounts.

> **Tip:** For more information about AWS organizations, see Amazon's AWS Organizations User Guide.

Before you begin:

You must have the following details for the read-only role in your AWS account:

- Role ARN
- External ID

For more information, see Set Up Read-Only Access to the AWS Account.

To connect to an AWS organization account:

1. In the left navigation bar, click ⊕ > **Connection** > **AWS account**.
2. In the **Choose a workflow to discover AWS account(s)** section, select **Onboard AWS organization**.
3. Click **Continue**.

   The **Configure management account** section appears.
4. Type the appropriate **Read Only Role ARN** and **External ID**.
5. Click **Continue**.

   The **Configure member accounts** section appears.
6. Configure member accounts by performing the following actions:

a. In the **Configure member accounts** section, in the first step, click **here**.

   Tenable Cloud Security redirects you to the **Create StackSet** wizard in the AWS Management Console. Follow these steps to deploy the stackset that creates the role for all member accounts.

   To deploy the StackSet to create a read-only role for a member account:

   a. Sign in to the AWS management account of the target organization.

   b. Copy the appropriate URL from the **Configure member accounts** section.

   c. On the **Choose a template** page, do the following:

      i. In the **Permissions** section, ensure that the **Service-managed permissions** option is selected.

      ii. In the **Prerequisite - Prepare template** section, ensure that the **Template is ready** option is selected.

      iii. In the **Template source** section, click **Amazon S3 URL**.

      iv. In the **Amazon S3 URL** box, copy the template URL from the Tenable Cloud Security Console and paste it.

      v. Click **Next**.

   d. On the **Specify StackSet details** page, do the following:

      i. In the **StackSet name** section, type a name for the StackSet.

         Tip: Choose a meaningful name because the Tenable Cloud Security role name is used for all the member accounts of the organization.

      ii. In the **StackSet description** section, type a description for the current StackSet.

      iii. In the **Parameters** section, type the appropriate management account ID.

      iv. Click **Next**.

   e. On the **Configure StackSet Options** page, do the following:

   i. (Optional) In the **Tags** section, click **Add new tag** and provide a **Key** and a **Value** to specify the tag.

      Tags are arbitrary key-value pairs that can be used to identify your stack. Tags that you apply to stack sets are applied to all resources created by your stacks.

   ii. For **Execution configuration**, choose **Active** so that StackSets performs non-conflicting operations concurrently and queues conflicting operations. After conflicting operations finish, StackSets starts queued operations in request order.

   iii. Click **Next**.

f. On the **Set deployment options** page, do the following:

   i. In the **Deployment targets** section, click one of the following:

      - **Deploy to organization** — Creates the role in all the member AWS accounts for the organization.
      - **Deploy to organizational units (OUs)** — Creates the role in all the member AWS accounts for selected organizations.

   ii. In **Automatic deployment**, click **Enabled**.

   iii. In **Account removal behavior**, click the required option.

g. In the **Specify regions** section, add a region available across all member accounts.

   > **Caution:** Select only one region. If you specify multiple regions, stack deployment succeeds only for one region and fails for others and can cause issues.

   > **Note:** If the selected region is not available under a particular member account, the stackset deployment fails.

h. In the **Deployment options** section, do the following:

i. In the **Maximum concurrent accounts - optional** drop-down box, select **Percentage**, and set the value to **100**.

ii. In the **Failure tolerance - optional** drop-down box, select **Percentage**, and set the value to **100**.

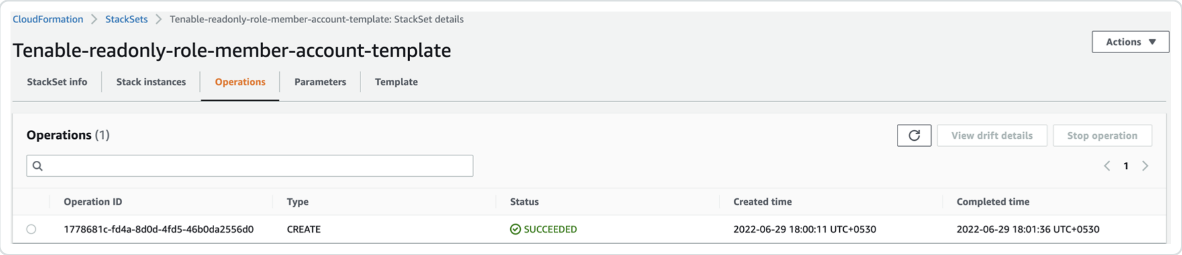
iii. In the **Regional Concurrency** section, click **Sequential**.

iv. Click **Next**.

i. In the **Capabilities** section, select the **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**check box to confirm.

j. Click **Submit**.

The **StackSet details** page appears. Wait for the status of the StackSet to change to **Succeeded**.



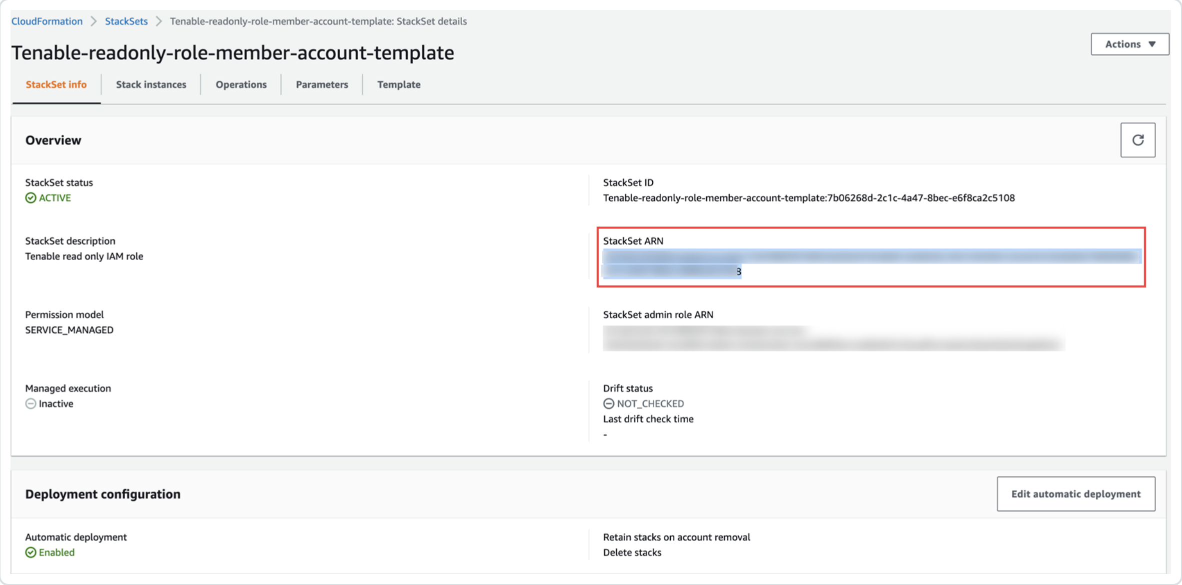
CloudFormation > StackSets > Tenable-readonly-role-member-account-template: StackSet details

Tenable-readonly-role-member-account-template

Operations (1)

	Operation ID	Type	Status	Created time	Completed time
○	1778681c-fd4a-8d0d-4fd5-46b0da2556d0	CREATE	✓ SUCCEEDED	2022-06-29 18:00:11 UTC+0530	2022-06-29 18:01:36 UTC+0530

k. Click the **StackSet Info** tab and copy the **StackSet ARN**.



CloudFormation > StackSets > Tenable-readonly-role-member-account-template: StackSet details

Tenable-readonly-role-member-account-template

Overview

StackSet status
✓ ACTIVE

StackSet ID
Tenable-readonly-role-member-account-template:7b06268d-2c1c-4a47-8bec-e6f8ca2c5108

StackSet description
Tenable read only IAM role

StackSet ARN
[redacted]

Permission model
SERVICE_MANAGED

StackSet admin role ARN
[redacted]

Managed execution
⊖ Inactive

Drift status
⊖ NOT_CHECKED
Last drift check time
-

Deployment configuration

Automatic deployment
✓ Enabled

Retain stacks on account removal
Delete stacks

b. In the Tenable Cloud Security Console, paste the Stacksets ARN copied in the previous step in the **Stacksets ARN** box.

c. Click **Continue**.

The **Discover and onboard member accounts** section appears. Tenable Cloud Security deploys the StackSet used to create a Tenable Cloud Security role for each member account.

7. Onboard member accounts.

a. In the **Discover and onboard member accounts** section, in the list, select the cloud member accounts that you want to onboard.

> **Tip:** You can also search for specific cloud accounts and filter the list by organizations.

b. (Optional) To create a new project automatically for the AWS organization, select the **Map accounts automatically** check box.

Tenable Cloud Security creates a new project for the AWS organization and links all AWS member accounts with the project.

8. In the **Choose prerequisites** section, select the check boxes:

- Ensure that you have granted all permissions.
- Ensure that you already have snapshots or or followed the provided instructions to create snapshots for the instances you wish to scan.

Click the links to view documentation for providing permissions to Tenable Cloud Security for scanning and creating snapshots for Agentless Assessment.

9. Click **Onboard accounts**.

On the **Projects & Connections** page, the AWS project links to the connected AWS organization's account and the selected VPCs.

Onboard an AWS Account

You can connect your Amazon Web Services (AWS) account as part of your AWS project. Use this method if you want to onboard each of your AWS account manually without deploying a CloudFormation template.

Before you begin:

You must have the following details for the read-only role in for your AWS account:

- Role ARN
- External ID

For more information, see Set Up Read-Only Access to the AWS Account.

To connect an AWS account:

1. In the left navigation bar of the Tenable Cloud Security page, click ⊕ > **Connection** > **AWS account**.
2. In the **Choose a workflow to discover AWS accounts** section, click **Onboard AWS account**.
3. Click **Continue**.

   The **Configure AWS account** section appears.
4. Type the appropriate **Read Only Role ARN** and **External ID**.
5. Click **Continue**.
6. In the **Choose projects to add the AWS account(s) to** section, select the project that you created for the AWS account.

   For more information, see Create a Project.
7. In the **Choose prerequisites** section, select the check boxes:
   - Ensure that you have granted all permissions.
   - Ensure that you already have snapshots or or followed the provided instructions to create snapshots for the instances you wish to scan.

Click the links to view documentation for providing permissions to Tenable Cloud Security for scanning and creating snapshots for Agentless Assessment.

8. Click **Connect Cloud Account**.

   You can view the AWS project linked to the connected AWS account and the selected VPCs on the **Projects & Connections** page.

Create an AWS Snapshot

EBS snapshots must be created and accessible for EC2 instances that you want to scan with Agentless Assessment.

> **Note:** Agentless Assessment scans AWS Instance snapshots, and not AWS volume snapshots.

You can create snapshots manually or you can automate the process using AWS Data Lifecycle Manager (DLM). Tenable recommends that you automate this process.

- Create a snapshot manually
- Automate snapshot creation with AWS DLM

> **Note:** AWS Backup's snapshot automation feature is not currently compatible with Elastic Block Storage (EBS) service's list and describe APIs. Therefore, it is not possible to create automated EBS snapshots that are readable by Agentless Assessment using AWS Backup.

Tenable recommends that you follow these best practices for snapshots:

- Take snapshots frequently.
- Do not share snapshots between accounts.
- Ensure snapshots are not visible publicly.
- Ensure snapshots have appropriate life-cycle management for creation, archiving, and deletion.
- Encrypt all snapshots.

Create AWS Snapshot Manually

To create a snapshot manually:

1. Log in to the AWS console.
2. In the left navigation bar, select **EC2 Service** dashboard.

   The **EC2 Service Dashboard** page appears.
3. In the left navigation bar, click **Elastic Block Store** > **Snapshots**.

The **Create Snapshot** page appears.

4. In the **Snapshot Settings** section, under **Resource Type**, select **Instance**.
5. In the **Instance ID** box, select the EC2 Instance ID for which you want to create a snapshot.
6. Click **Create snapshot**.

   AWS creates the snapshot, which takes around 10 minutes to complete.

Automate Snapshot Creation with AWS Data Lifecycle Manager (DLM)

You can use the Data Lifecycle Manager (DLM) service to automate the creation of snapshots from EC2 instances according to a schedule. For more information, see Amazon Data Lifecycle Manager.

To get you started, an example is provided to deploy DLM automatically on Tenable GitHub.

Configure Vulnerability Scan using Agentless Assessment for AWS

Tenable Cloud Security triggers vulnerability scans on AMIs and EC2 instances as part of the cloud scanning process.

Before you Begin:

- Onboard cloud accounts in Tenable Cloud Security. For more information about onboarding your AWS accounts, see Onboard AWS Accounts.
- Create an IAM role that provides Tenable Cloud Security the following permissions:
    - Elastic Block Store:
        - ebs:ListSnapshotBlocks
        - ebs:ListChangedBlocks
        - ebs:GetSnapshotBlock
    - Key Management Service (KMS):

      Snapshots encrypted with KMS must grant the IAM role used by Tenable Cloud Security with access to the KMS key used to encrypt the snapshot. Modify the KMS key's resource policy to include the following permissions:

        - kms:Decrypt
        - kms:DescribeKey
- Create snapshots in AWS console.

To set up Agentless Assessment:

1. In Tenable Cloud Security, initiate a cloud scan:

    a. On the home page, click **Projects & Connections**.

       Tenable Cloud Security displays the list of projects in the **Projects** tab.

    b. In the row for the project that you want to scan, click ⋮ **> Manage cloud scan profiles**.

       The **Manage scan profiles** window appears.

c. Click **New Scan Profile**.

The **Create new scan profile for cloud** window appears.

> **Note:** You can also use the default scan profile. Vulnerability scan with agentless assessment is enabled by default for the default scan profile.

d. In the **Scan profile name** box, type a name for the scan profile or retain the default name.

e. In **Step 1 Cloud config assessment options**, retain the default selections or do one of the following:

- Select the check box next to the option to select all the options within a category.
- Click the drop-down arrow ⌄ to show all the available options in the category. Select the check boxes as needed.

> **Note**: The count next to the drop-down arrow ⌄ shows: Number of options available / Number of options selected.

> **Tip:** Ensure EC2 AMI and EC2 Instance resources are selected to take full advantage of AWS Agentless Assessment scans.

f. In **Step 2**, click the **Enable Vulnerability Scan (optional)** toggle to enable vulnerability scan.

> **Note**: Tenable Cloud Security scans EC2 AMI and EC2 instances for vulnerabilities after it completes the Misconfiguration Scan. The EC2 resources are available under the **Compute** category.

g. (Optional) Click **Preview** to view all the selected assessment options.

h. Click **Create Scan Profile**.

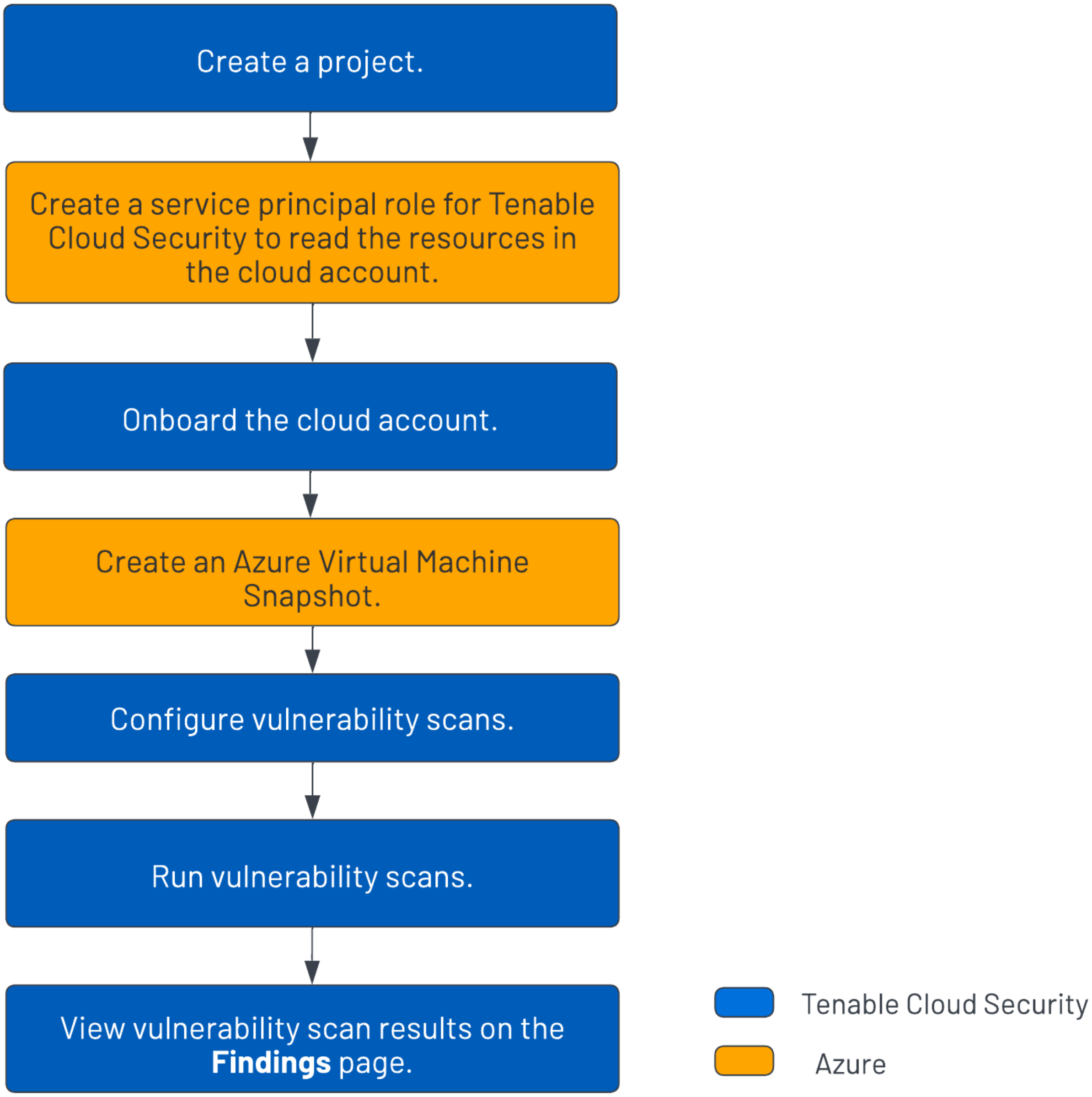
Tenable Cloud Security creates the scan profile and the newly created scan profile appears on the **Configure cloud scan** window.

i. In the row of the scan profile that you created for a vulnerability scan, click **Run Scan**.

Tenable Cloud Security runs the vulnerability scan and you can view the vulnerability scan results on the Tenable Cloud Security **Vulnerabilities** page and also on the Tenable Vulnerability Management **Findings** page.

Azure Agentless Assessment Workflow

The following workflow shows the process to set up Agentless Assessment and view the results:


Create a project.
Create a service principal role for Tenable Cloud Security to read the resources in the cloud account.
Onboard the cloud account.
Create an Azure Virtual Machine Snapshot.
Configure vulnerability scans.
Run vulnerability scans.
View vulnerability scan results on the **Findings** page.
🟦 Tenable Cloud Security
🟧 Azure

To set up Agentless Assessment for Azure virtual machines:

1. Create a project for onboarding the cloud account.
2. Create a service principal role for Tenable Cloud Security.

3. Onboard the Azure cloud account.

4. Create an Azure Virtual Machine snapshot.

5. Configure vulnerability scans using Agentless Assessment.

6. Run cloud scan.

7. View cloud scan results on the Tenable Cloud Security **Findings > Vulnerabilities** page and the **Findings** page on Tenable Vulnerability Management.

Agentless Assessment Requirements for Azure

The following requirements must be met for performing Agentless Assessment:

- Azure Role
- Azure Snapshots
- Supported Operating Systems for Azure
- Supported File Systems
- Supported Regions for Azure

Azure Service Principal Role

This is a prerequisite before setting up Agentless Assessment. Agentless Assessments requires a role that grants Tenable Cloud Security permissions to read data from Azure virtual machine snapshots.

The following permissions are required for a vulnerability scan of Azure VMs:

- Reader
- Disk Snapshot Contributor

Follow the instructions on the Create an Azure Service Principal Role page to create a role for Tenable Cloud Security.

Azure Snapshots

Agentless assessment for Azure is based on snapshots of your virtual machines. To configure an Agentless Assessment, you must first create a snapshot. For more information, see Create an Azure Virtual Machine Snapshot.

Supported Operating Systems for Azure

- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES) 11.4 to 15.2

- Ubuntu
- Debian

Supported File Systems

- XFS
- ext4

Supported Regions for Azure

- `australiacentral`
- `australiacentral2`
- `australiaeast`
- `australiasoutheast`
- `brazilsouth`
- `brazilsoutheast`
- `canadacentral`
- `canadaeast`
- `centralindia`
- `centralus`
- `eastus`
- `eastus2`
- `francecentral`
- `francesouth`
- `germanynorth`
- `germanywestcentral`
- `japaneast`
- `northcentralus`

- `northeurope`
- `norwayeast`
- `norwaywest`
- `southcentralus`
- `southeastasia`
- `southindia`
- `swedencentral`
- `swedensouth`
- `uksouth`
- `ukwest`
- `westcentralus`
- `westeurope`
- `westus`
- `westus2`
- `westus3`

Create an Azure Service Principal Role

Tenable Cloud Security requires adequate permissions to read the resources in your Azure subscription. Provision a service principal role in the target Azure subscription and configure it for Tenable Cloud Security to read the resources in the same account.

The following permissions are required for a vulnerability scan of Azure virtual machines:

- Reader
- Disk Snapshot Contributor

Follow these steps to create a service principal and assign a role to it:

1. Register an application with Azure to create the service principal.

2. Choose one of the following options to assign a role to the service principal for accessing the resources in your subscription:

    - Create and assign a custom role with expanded Read access (comprehensive) to the service principal.

    - Assign the built-in Reader role (limited) to the service principal.

3. Create a client secret for authenticating the service principal from Tenable Cloud Security.

Register an application with Azure

When you register an application through the Azure portal, Azure automatically creates an application object and service principal in your tenant. For more information on the relationship between application registration, application objects, and service principals, see [Application and service principal objects in Microsoft Entra ID](#).

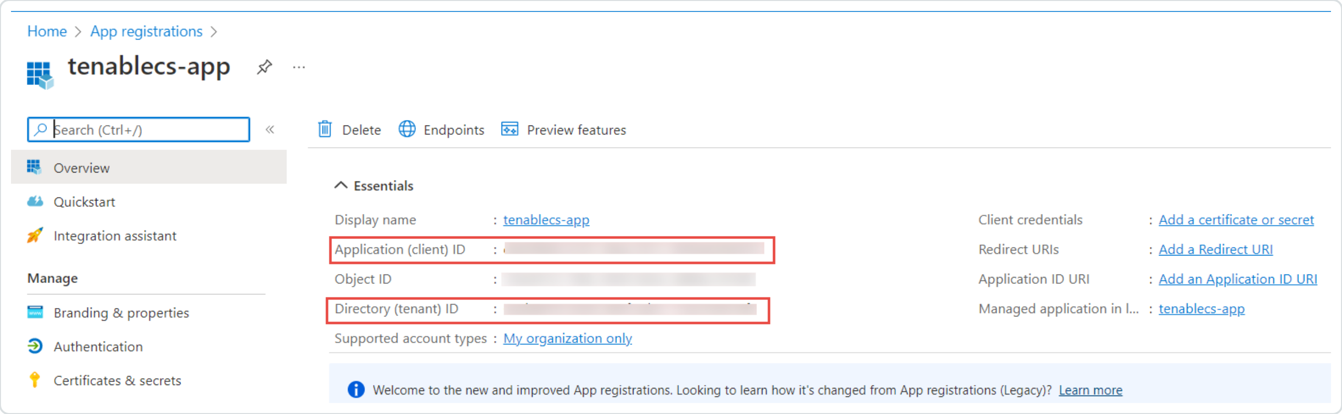
To create a service principal role in Azure:

1. Log in to the [Microsoft Azure portal](#).
2. In the home page, click **App registrations**.

   The **App registrations** page appears.
3. Click **New registration**.

   The **Register an application** page appears.
4. Type a name for the application you want to register.
5. Click **Register**.

   The application details page appears.

   Display name : tenablecs-app
   Application (client) ID : [redacted]
   Object ID : [redacted]
   Directory (tenant) ID : [redacted]
   Supported account types : My organization only

   Client credentials : Add a certificate or secret
   Redirect URIs : Add a Redirect URI
   Application ID URI : Add an Application ID URI
   Managed application in l... : tenablecs-app

   Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more
6. Note down the following values. You need these values when onboarding the service account in Tenable Cloud Security:
   - **Application (client) ID**: This is the client ID requested by Tenable Cloud Security.
   - **Directory (tenant) ID**: This is the Tenant ID requested by Tenable Cloud Security.

Create a custom role and assign it to the service principal

For a comprehensive Azure cloud scan for resources such as Storage Account, Kubernetes Cluster, Cosmos DB, Function App resources, create a custom role with expanded read access including the list APIs access. Additionally, Agentless Assessment requires the Disk Snapshot Contributor role along with the Reader role for scanning virtual machine snapshots.

For more information about these permissions, see Azure built-in roles in Azure documentation.

To create a custom role and assign it to the service principal:

1. On the home page of the Azure portal, do one of the following:

   - To create a role for a management group, click **Management groups**.

     The **Management groups** page appears.

   - To create a role for a subscription, click **Subscriptions**.

     The **Subscriptions** page appears.

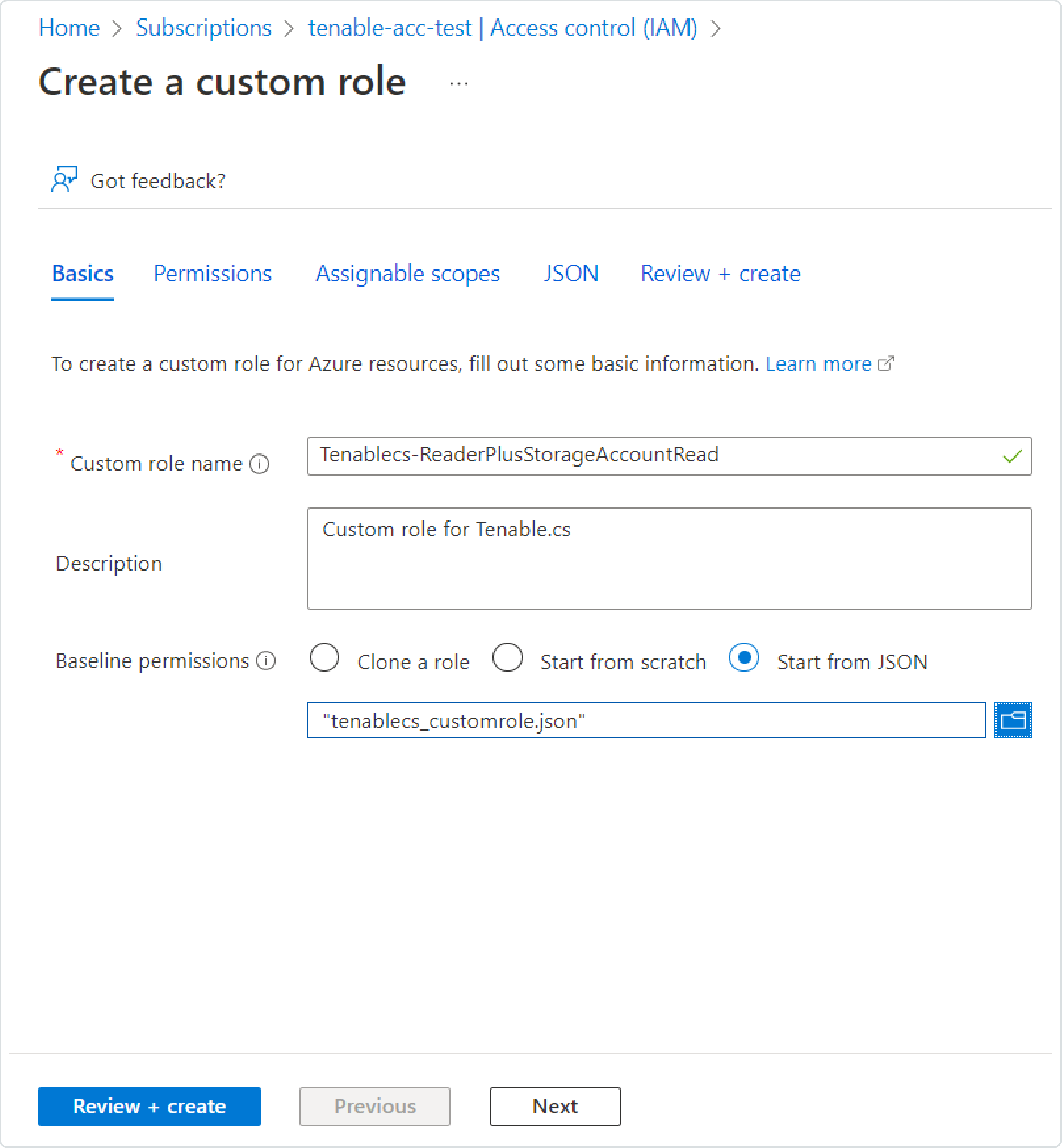
   > **Note:** To enable Tenable Cloud Security to discover all subscriptions under a management group, ensure that the service principal role is assigned to the management group. You can also assign the role to a root management group to discover all subscriptions under the root management group.

2. On the left navigation bar, click **Access Control (IAM)**.

   The **Access control (IAM)** page for your subscription appears.

3. In the **Create a custom role** section, click **Add**.

   The **Create a custom role** page appears.



Home > Subscriptions > tenable-acc-test | Access control (IAM) >

Create a custom role ...

Got feedback?

To create a custom role for Azure resources, fill out some basic information. Learn more

* Custom role name: Tenablecs-ReaderPlusStorageAccountRead ✓

Description: Custom role for Tenable.cs

Baseline permissions: ○ Clone a role ○ Start from scratch ● Start from JSON

"tenablecs_customrole.json"

4. In **Baseline permissions**, select the **Start from JSON** option.

   You can create a custom role in the following ways:

   - **Clone a role**: Create a custom role by cloning an existing role and modifying the role, as required.

- **Start from scratch**: Create a custom role by using the Azure user interface.
- **Start from JSON**: Create a custom role by uploading a JSON file with the required permissions.

For more information about these methods, see Create or update Azure custom roles using the Azure portal in Azure documentation.

> **Note:** This procedure describes how to create a custom role using a JSON file.

5. Click 📂 to upload a JSON file that has the required permissions.

   Azure validates the JSON file and uploads the file for role creation.

   The following sample JSON file creates a role with read permissions along with the list APIs for the Storage Accounts, Kubernetes cluster, Cosmos DB, and Function App services for a **subscription**:

```
{
    "properties": {
        "roleName": "Tenablecs-ReaderPlusStorageAccountRead",
        "description": "Custom role for Tenable Cloud Security",
        "assignableScopes": [
            "/subscriptions/<subscription-id>"
        ],
        "permissions": [
            {
                "actions": [
                    "*/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/storageAccounts/listServiceSas/action",
                    "Microsoft.Storage/storageAccounts/localusers/listKeys/action",
                    "Microsoft.ContainerService/managedClusters/accessProfiles/listCredential/action",
                    "Microsoft.DocumentDB/databaseAccounts/listKeys/action",
                    "Microsoft.DocumentDB/databaseAccounts/readonlykeys/action",
                    "Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/action",
                    "Microsoft.Web/sites/config/list/action"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

The following sample JSON file creates a role with read permissions along with the list APIs for the Storage Accounts, Kubernetes cluster, Cosmos DB, and Function App services for a **management group**:

```
{
    "properties": {
        "roleName": "Tenablecs-ReaderPlusStorageAccountRead",
        "description": "Custom role for Tenable Cloud Security",
        "assignableScopes": [
            "/providers/Microsoft.Management/managementGroups/<management-group-ID>"
        ],
        "permissions": [
            {
                "actions": [
                    "*/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/storageAccounts/listServiceSas/action",
                    "Microsoft.Storage/storageAccounts/localusers/listKeys/action",
                    "Microsoft.ContainerService/managedClusters/accessProfiles/listCredential/a-
ction",
                    "Microsoft.DocumentDB/databaseAccounts/listKeys/action",
                    "Microsoft.DocumentDB/databaseAccounts/readonlykeys/action",
                    "Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/action",
                    "Microsoft.Web/sites/config/list/action"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

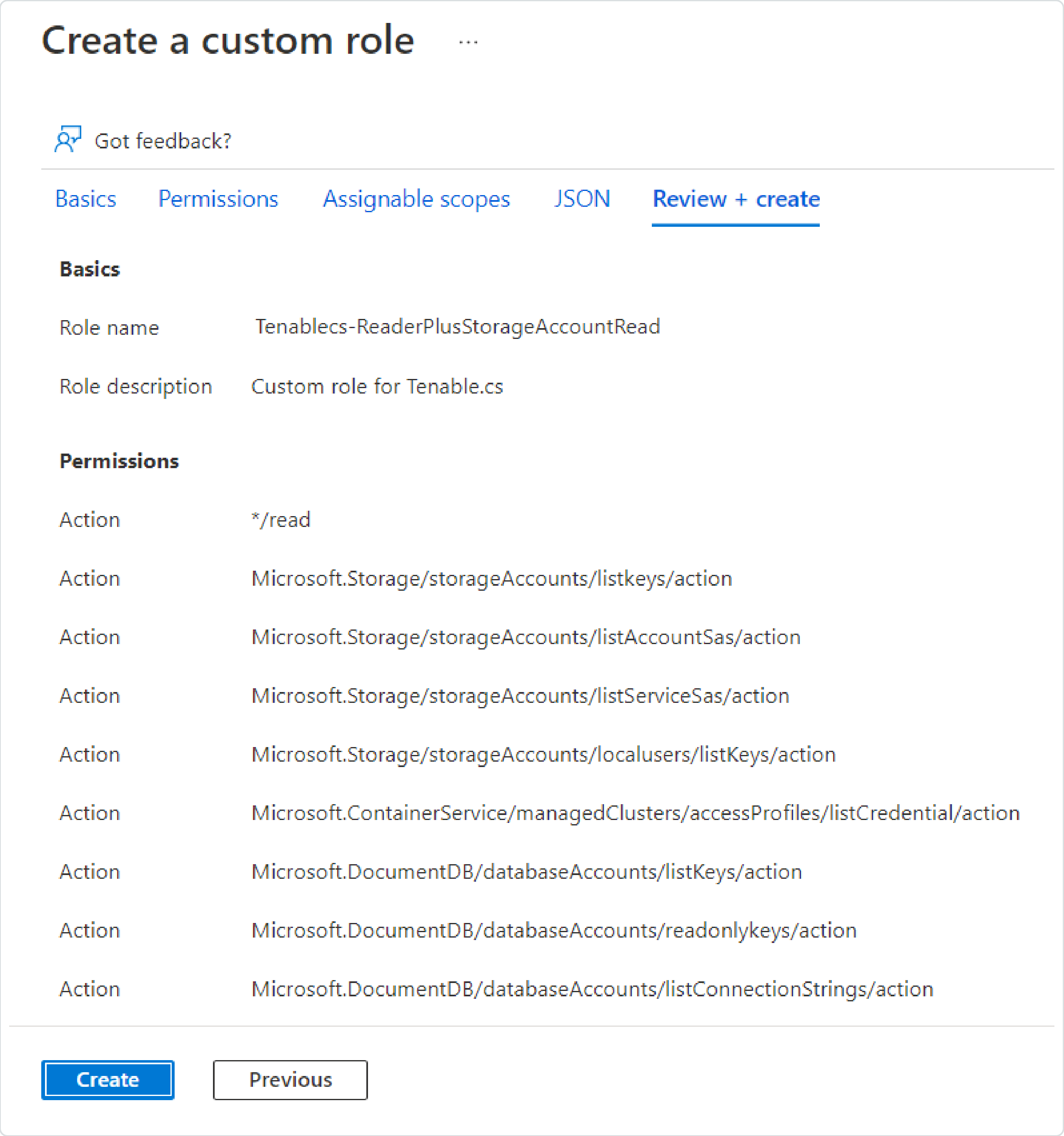
The following sample JSON file creates a custom role with read permissions along with permissions to access snapshots at a subscription-level, which is required for Agentless Assessment:

```
{
    "properties": {
        "roleName": "Tenablecs-ReaderPlusDiskSnapshotContributor",
        "description": "Custom role for Tenable Cloud Security",
        "assignableScopes": [
            "/subscriptions/<subscription-id>"
        ],
        "permissions": [
            {
                "actions": [
                    "*/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/storageAccounts/listServiceSas/action",
                    "Microsoft.Storage/storageAccounts/localusers/listKeys/action",
                    "Microsoft.Compute/snapshots/beginGetAccess/action"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

where `<subscription-id>` is your Azure subscription ID.

6. Click **Review + create**.

   The **Review + create** tab appears.



Basics

Role name	Tenablecs-ReaderPlusStorageAccountRead
Role description	Custom role for Tenable.cs

Permissions

Action	*/read
Action	Microsoft.Storage/storageAccounts/listkeys/action
Action	Microsoft.Storage/storageAccounts/listAccountSas/action
Action	Microsoft.Storage/storageAccounts/listServiceSas/action
Action	Microsoft.Storage/storageAccounts/localusers/listKeys/action
Action	Microsoft.ContainerService/managedClusters/accessProfiles/listCredential/action
Action	Microsoft.DocumentDB/databaseAccounts/listKeys/action
Action	Microsoft.DocumentDB/databaseAccounts/readonlykeys/action
Action	Microsoft.DocumentDB/databaseAccounts/listConnectionStrings/action

7. Click **Create**.

   Azure creates the custom role and redirects you to the **Access control (IAM)** page.

8. In the **Grant access to this resource** section, click **Add role assignment** to assign the custom role to the service principal.

   The **Add role assignment** page appears.

9. On the **Role** tab, search for the custom role you created.

10. Select the custom role and click **Next**.

    The **Members** tab appears.

11. On the **Members** tab, do the following:

    a. Click **Select Members**.

    b. In the **Select members** window, search for the application you created.

    c. Select the application.

       The application appears under **Selected members**.

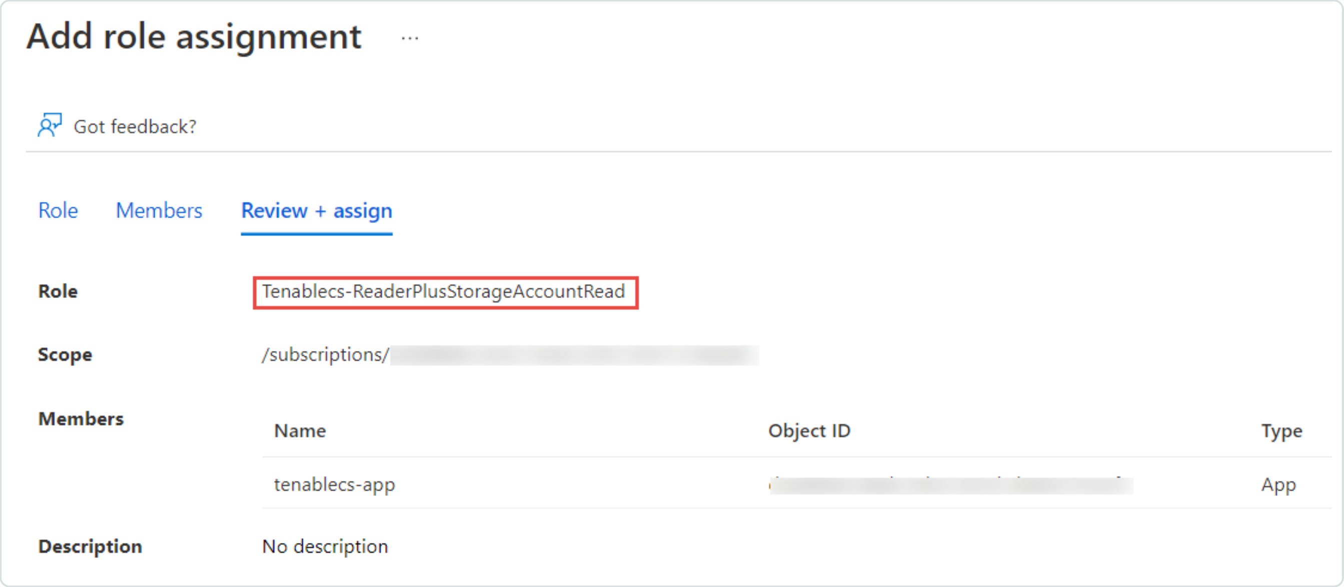
    d. Click **Select**.

       Azure adds the application for assigning the selected custom role.

    e. Click **Next**.

       The **Review + assign** tab appears.

12. Review the details of the role and click **Review + assign**.



Role Tenablecs-ReaderPlusStorageAccountRead

Scope /subscriptions/[redacted]

Members

Name	Object ID	Type
tenablecs-app	[redacted]	App

Description No description

Azure assigns the custom role to the service principal of the application and redirects you to the **Access control (IAM)** page.

Assign the Reader role to the service principal

Tenable Cloud Security requires the **Reader** role for accessing the resources for a cloud scan. This role provides limited permissions to the service principal. If you want to perform a comprehensive scan including managed clusters and storage accounts, create a custom role with expanded read permissions.

1. On the home page of the Azure portal, do one of the following:

    - To assign the role to a management group, click **Management groups**.

      The **Management groups** page appears.

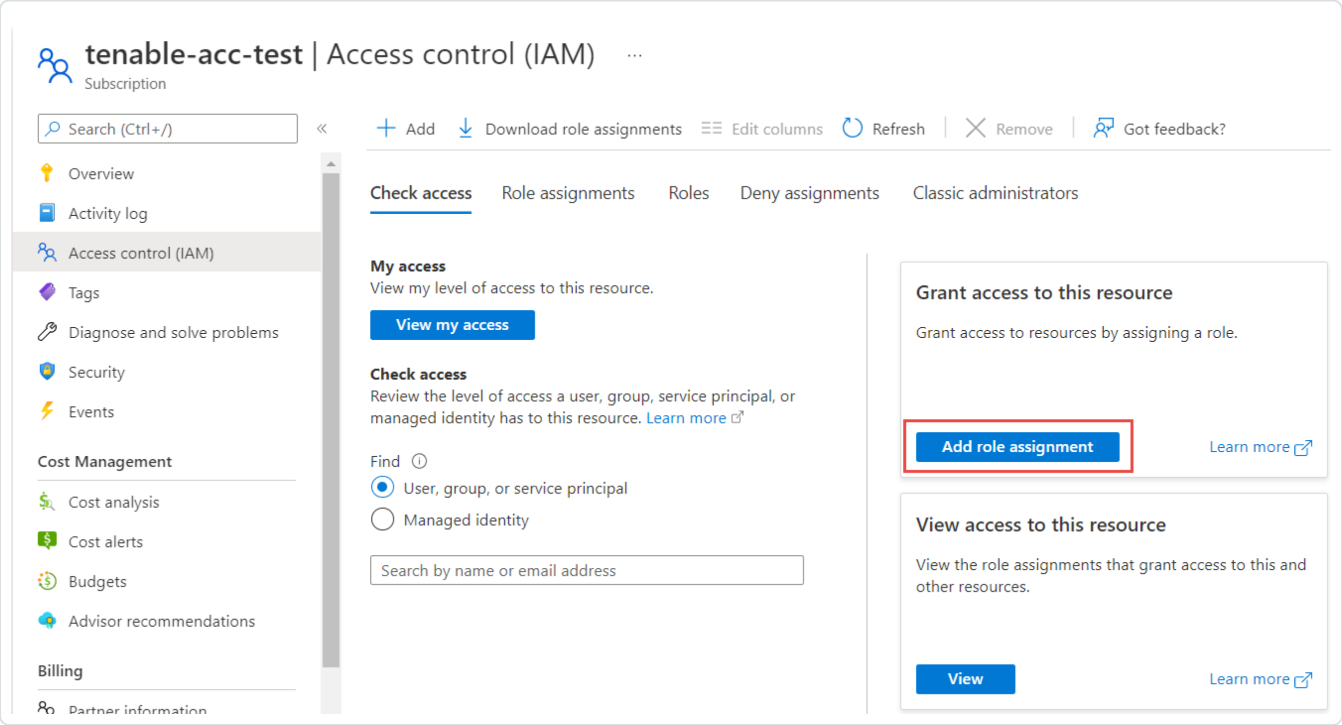
      > **Note:** To enable Tenable Cloud Security to discover all subscriptions under a management group, ensure that the service principal role is assigned to the management group. You can also assign the role to a root management group to discover all subscriptions under the root management group.

    - To create a role for a subscription, click **Subscriptions**.

      The **Subscriptions** page appears.

2. On the left navigation bar, click **Access Control (IAM)**.

   The **Access control (IAM)** page for your subscription appears.



My access
View my level of access to this resource.

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find
● User, group, or service principal
○ Managed identity

Search by name or email address

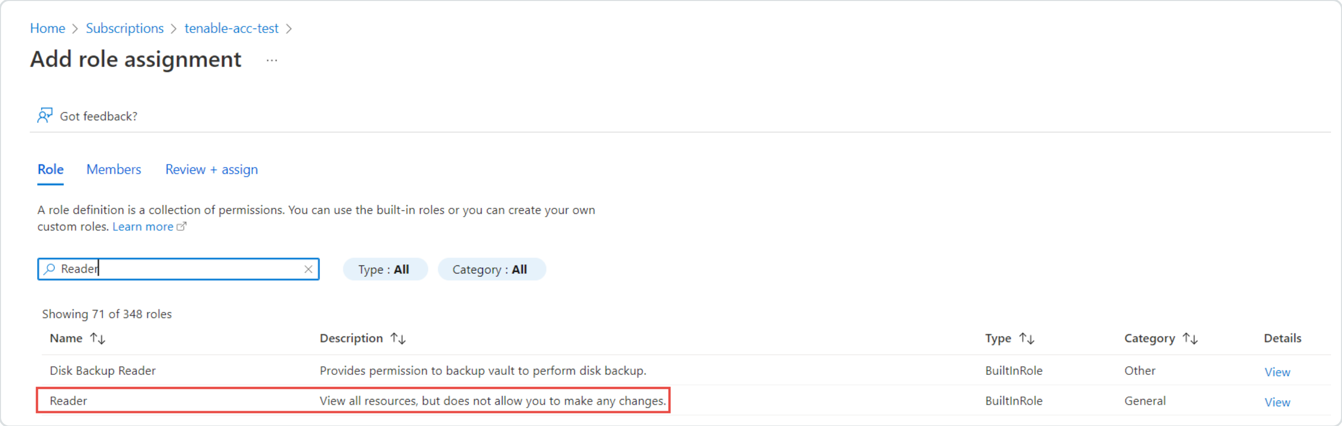
Grant access to this resource
Grant access to resources by assigning a role.

View access to this resource
View the role assignments that grant access to this and other resources.

3. In the **Grant access to this resource** section, click **Add role assignment**.

   The **Add role assignment** page appears.

4. On the **Role** tab, search for the **Reader** role.



A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Reader

Showing 71 of 348 roles

Name	Description	Type	Category	Details
Disk Backup Reader	Provides permission to backup vault to perform disk backup.	BuiltInRole	Other	View
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View

5. Select the **Reader** role and click **Next**.

   The **Members** tab appears.

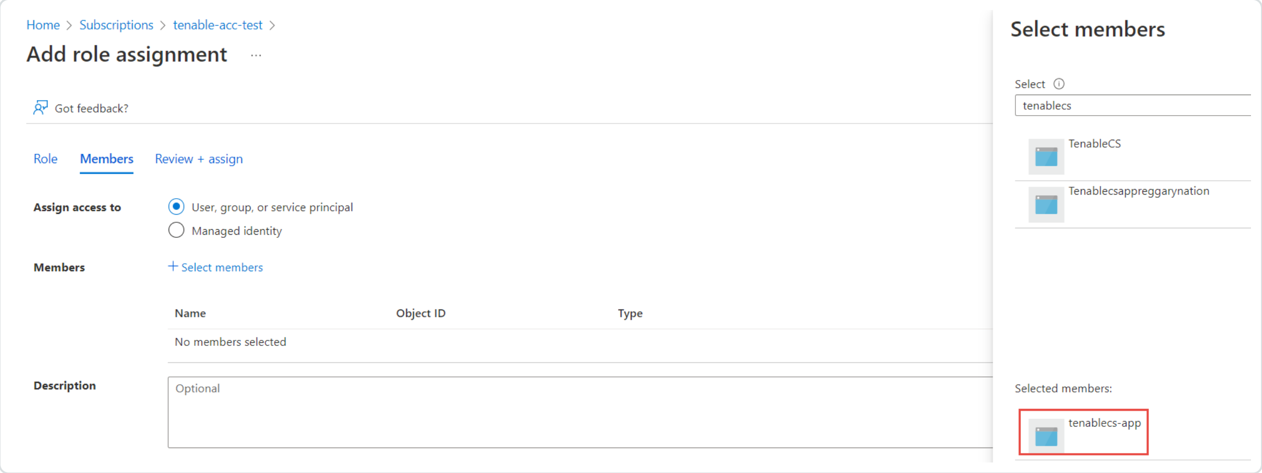
6. On the **Members** tab, do the following:

a. Click **Select Members**.

b. In the **Select members** window, search for the application you created.

c. Select the application.

The application appears under **Selected members**.



Home > Subscriptions > tenable-acc-test >

Add role assignment ...

Got feedback?

Role | Members | Review + assign

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

Name	Object ID	Type
No members selected		

Description: Optional

Select members

Select ⓘ tenablecs

TenableCS

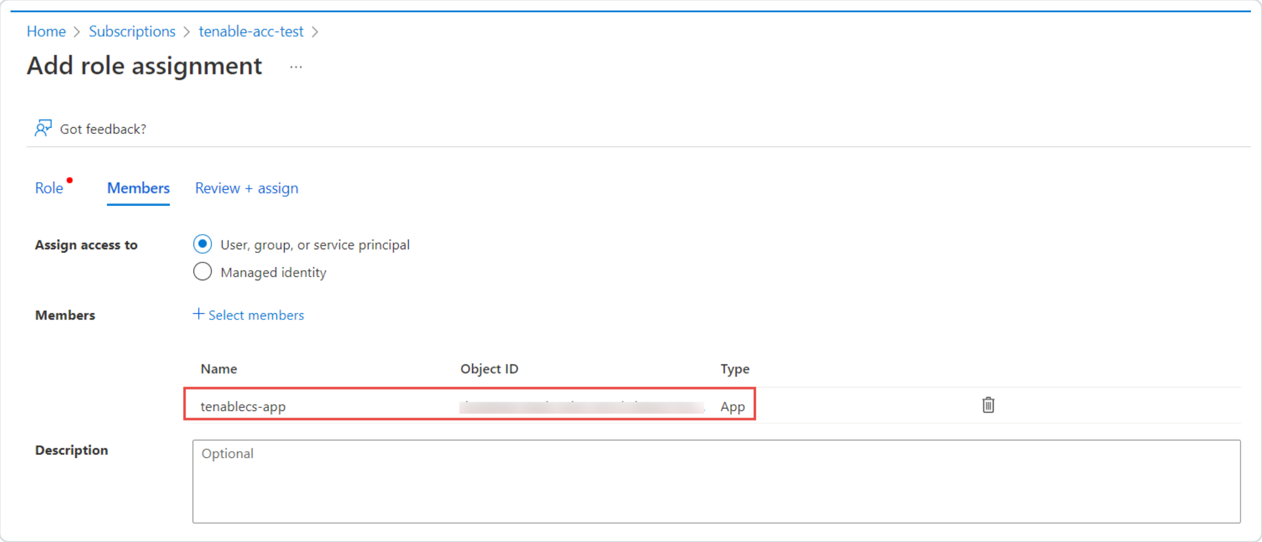
Tenablecsappreggarynation

Selected members:

tenablecs-app

d. Click **Select**.

Azure adds the application for assigning the **Reader** role.



Home > Subscriptions > tenable-acc-test >

Add role assignment ...

Got feedback?

Role | Members | Review + assign

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

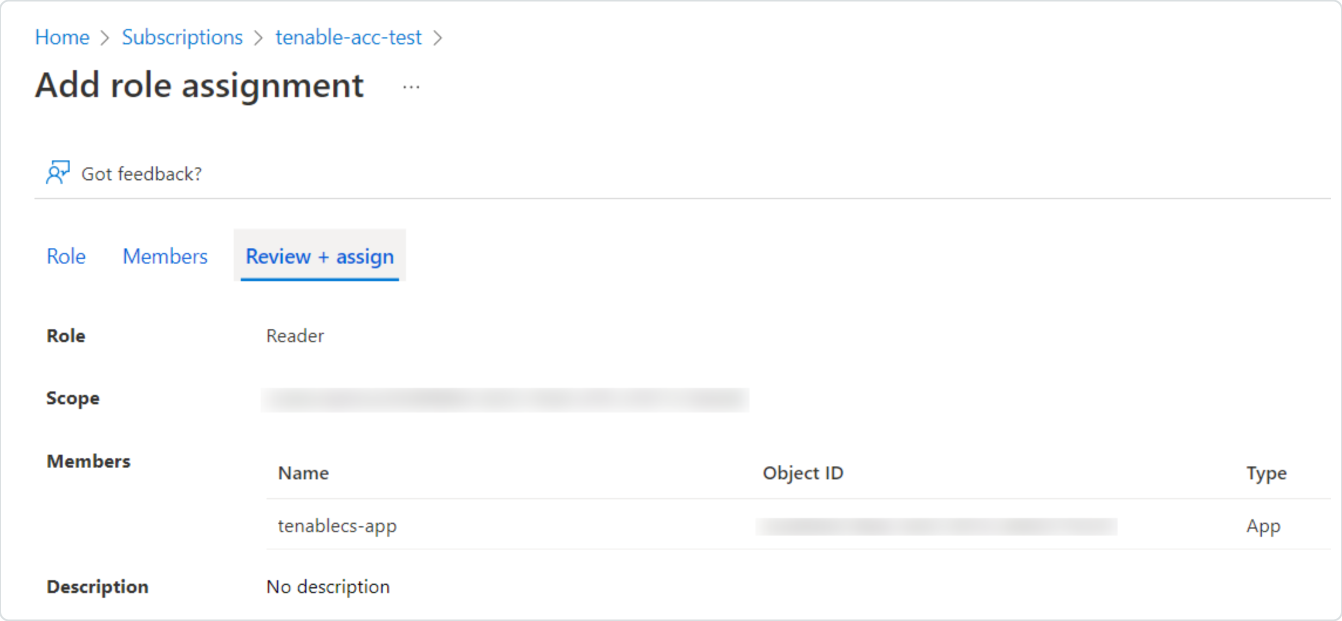
Name	Object ID	Type
tenablecs-app	[redacted]	App

Description: Optional

e. Click **Next**.

The **Review + assign** tab appears.

7. Review the details of the role and click **Review + assign**.



Role Reader

Scope [redacted]

Members

Name	Object ID	Type
tenablecs-app	[redacted]	App

Description No description

Azure assigns the role to the service principal of the application and redirects you to the **Access control (IAM)** page.

Create a client secret

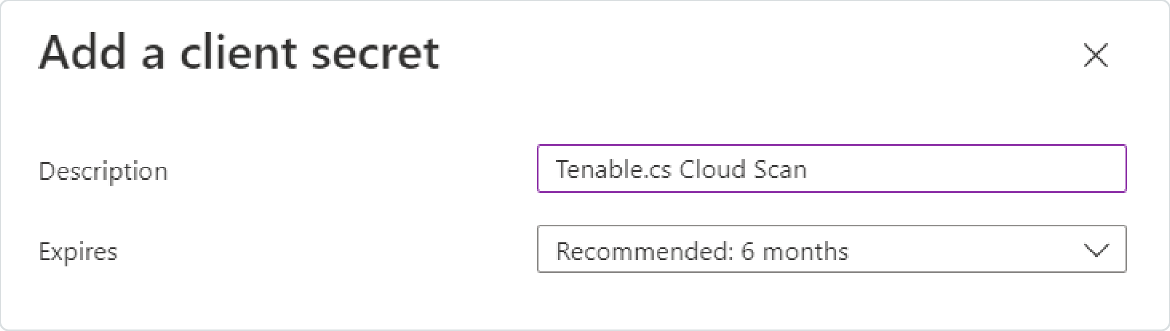
You can create a new application secret to authenticate the service principal.

1. On the home page of the Azure portal, click **App Registrations**.
2. Click the application that you created for Tenable Cloud Security.
3. On the left navigation bar, click **Certificates & secrets**.

   The **Certificates & secrets** page appears.

4. Click **New client secret**.

   The **Add a client secret** page appears.

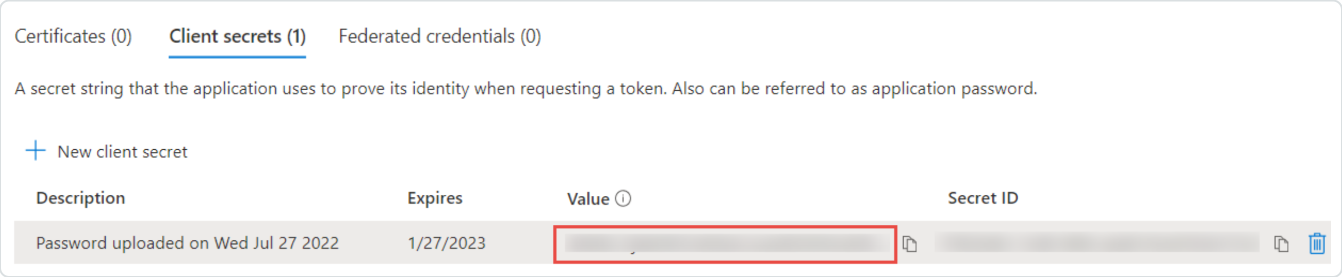
   Add a client secret

   Description: Tenable.cs Cloud Scan

   Expires: Recommended: 6 months

5. Provide a relevant description for the secret. For example, Tenable Cloud Security Scan.
6. Set an expiration for the client secret.
7. Click **Add**.

   The client secret value and ID appear.

   A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID
Password uploaded on Wed Jul 27 2022	1/27/2023	[redacted]	[redacted]

8. Record the **Value** of this client secret.

> **Note:** You cannot view this value again because Azure masks this value.

What to do next:

Onboard an Azure Account

You must have the following values for onboarding the Azure account in Tenable Cloud Security:

- Client ID
- Tenant ID
- Secret value

Onboard an Azure Account

In Tenable Cloud Security, you can connect your Microsoft Azure cloud account using a service principal. In Microsoft Azure, a service principal is an entity that requires access to the resources secured by a Microsoft Entra ID tenant.

Before you begin:

- Ensure you have the following Azure values:
  - Client ID
  - Secret value
  - Tenant ID

  For more information, see Create an Azure Service Principal Role.

To connect an Azure subscription with a service principal:

1. In the left navigation bar, click ⊕ > **Connection** > **Azure subscription**.
2. In the **Choose a workflow to discover Azure subscriptions** section, click **Service principal (recommended)**.
3. Click **Continue**.
4. In the **Discover Azure subscription(s)** section, enter your **Client ID**, **Secret value**, and **Tenant ID**.
5. Click **Continue**.

   Tenable Cloud Security connects to your Microsoft Azure account using the specified credentials, and displays the list of subscriptions.
6. In the **Choose Azure subscription(s)** section, select the required subscriptions.
7. Click **Continue**.
8. For the selected subscriptions, in the **Choose resource group(s)** section, do one of the following:

- To select all available resource groups, click **All (recommended)**.
- To select specific resource groups, click **Specific**, and select a resource group in the list.

> **Tip:** You can search for specific resource groups, and filter the list by subscriptions.

9. Click **Continue**.
10. (Optional) In the **Choose projects to add the Azure project(s) to** section, create or select a project for the Azure subscription.

    - To create a new project for your Azure account, click **Add a project**. For more information, see Create a Project.
    - Select a project from the list.

    > **Tip:** You can also search for specific projects.

11. In the **Choose prerequisites** section, select the check boxes:

    - Ensure that you have granted all permissions.
    - Ensure that you already have snapshots or or followed the provided instructions to create snapshots for the instances you wish to scan.

      Click the links to view documentation for providing permissions to Tenable Cloud Security for scanning and creating snapshots for Agentless Assessment.

12. Click **Connect Cloud Account**.

    On the **Projects & Connections** page, you can view the Azure project with the connected Azure account and view the selected VPCs.

Create an Azure Virtual Machine Snapshot

Tenable Cloud Security Agentless Assessment performs scans on Azure Virtual Machines through the assessment of virtual hard disk snapshots. Snapshots can be created manually or automatically through the use of Azure Backup Vault. Tenable recommends that you automate this process.

- Create a snapshot manually
- Automate Azure Virtual Machine Snapshot Creation

Create Azure Virtual Machine Snapshot Manually

To create a snapshot manually:

1. In the Azure portal, select **Create a resource**.
2. Search for and select **Snapshot**.

   The **Snapshot** window appears.
3. Click **Create**.

   The **Create snapshot** window appears.
4. In the **Basics** tab, do the following:

   a. For **Resource group**, select an existing resource group or enter the name of a new one.

   b. In the **Instance details** section, provide the following information:

      - **Name** — Name of the snapshot.
      - **Region** — The Azure region into which the resource should be deployed. For the list of supported regions, see Agentless Assessment Requirements for Azure.
      - **Snapshot type** — The type of snapshot determines its pricing and functionality.
        - Full: Make a complete read-only copy of the selected disk.
        - Incremental: Save on storage costs by making a partial copy of the disk based on the difference between the last snapshot.
      - **Source subscription** — The subscription that contains the managed disk to be backed up.
      - **Source disk** — The disk to use as the source of this new snapshot.
      - **Storage type** — Select **Standard HDD**, unless you require zone-redundant storage or high-performance storage (Premium HDD) for your snapshot.
5. Click the **Encryption** tab and ensure that Key management is set to **Platform-managed key**.

   Platform-managed keys (PMKs) are key encryption keys that are generated, stored, and managed entirely by Azure.

6. Click the **Networking** tab and ensure that **Network access** is set to **Enable public access from all networks**.

7. Click the **Advanced** tab and ensure that the **Enable data access authentication mode** is disabled.

8. (Optional) Configure the **Tags** tab by providing name/value pairs for your resources.

9. Click **Review + create**.

   Azure validates the snapshot and shows a summary of the snapshot.

10. Click **Create** to create the snapshot.

Automate Azure Virtual Machine Snapshot Creation

To get you started, an automated solution is provided on Tenable GitHub.

Configure Vulnerability Scan using Agentless Assessment for Azure

Workload vulnerability scans are triggered as part of the cloud scan process in Tenable Cloud Security. Tenable Cloud Security supports agentless workload scanning for Azure Virtual Machines.

Before you Begin:

- Onboard cloud accounts in Tenable Cloud Security. For more information about onboarding your cloud accounts, see Onboard an Azure Account.
- Create an Azure service principal role that provides Tenable Cloud Security the following permissions:
  - Reader
  - Disk Snapshot Contributor
- Create an Azure Virtual Machine Snapshot.

To set up Agentless Assessment:

1. In Tenable Cloud Security, initiate a cloud scan:
   a. On the home page, click **Projects & Connections**.

      Tenable Cloud Security displays the list of projects in the **Projects** tab.

   b. In the row for the project that you want to scan, click ⋮ **> Manage cloud scan profiles**.

      The **Manage scan profiles** window appears.

   c. Click **New Scan Profile**.

      The **Create new scan profile for cloud** window appears.

      > **Note:** You can also use the default scan profile. Vulnerability scan with agentless assessment is enabled by default for the default scan profile.

   d. In the **Scan profile name** box, type a name for the scan profile or retain the default name.

e. In **Step 1 Cloud config assessment options**, retain the default selections or do one of the following:

   - Select the check box next to the option to select all the options within a category.
   - Click the drop-down arrow ⌄ to show all the available options in the category. Select the check boxes as needed.

     > **Note**: The count next to the drop-down arrow ⌄ shows: Number of options available / Number of options selected.

f. In **Step 2**, click the **Enable Vulnerability Scan (optional)** toggle to enable vulnerability scan.

   > **Note**: Tenable Cloud Security scans Azure Virtual Machines for vulnerabilities after it completes the Misconfiguration Scan. These resources are available under the **Compute** category.

g. (Optional) Click **Preview** to view all the selected assessment options.

h. Click **Create Scan Profile**.

   Tenable Cloud Security creates the scan profile and the newly created scan profile appears on the **Configure cloud scan** window.

i. In the row of the scan profile that you created for a vulnerability scan, click **Run Scan**.

   Tenable Cloud Security runs the vulnerability scan and you can view the vulnerability scan results on the Tenable Cloud Security **Vulnerabilities** page and also on the Tenable Vulnerability Management **Findings** page.

Run a Cloud Scan

You can create a scan profile to include the resource types that you want to scan and trigger a scan for that profile.

To start a scan:

1. Click **Projects & Connections**.

   Tenable Cloud Security displays the list of projects in the **Projects** tab.

2. In the row for the project for the cloud scan, click ⋮ and do one of the following:

   - **Run default scan profile** — Select this option to run a scan on the default scan profile. If there are no other scan profiles, Tenable Cloud Security runs a scan on the system default scan profile.

     > **Note:** Vulnerability scan with agentless assessment is enabled by default for the default scan profile.

   - **Manage cloud scan profiles** — Select this option to create a new scan profile or use a scan profile that you created earlier.

     The **Manage scan profile** window appears and lists all the scan profiles.

   Tenable Cloud Security runs the scan and updates the scan status column of the project on completion of the scan.

   > **Note:** You can view or edit other scan profiles of a project when the cloud scan is running with one of the scan profiles.

What to do next:

After running a cloud scan, you can view a summary of issues, critical security insights, remediation insights, number of cloud and IaC drifts, failing policies, and impacted resources for your project. For more information, see View Tenable Cloud Security Dashboards and Reports.

View Vulnerabilities

The **Vulnerabilities** tab of the **Findings** page displays the vulnerabilities detected during the Agentless Assessment of EC2 instances and Azure virtual machines.

1. Access Tenable Cloud Security.

   The **Dashboard** page appears.

2. In the left navigation pane, click **Findings**.

   The **Misconfigurations** tab appears.

3. Click the **Vulnerabilities** tab.

   The **Vulnerabilities** tab appears with the list of vulnerabilities. The **Vulnerabilities** table displays the following details:

Column	Description
Severity	This is the severity level of the vulnerability whether **Critical**, **High**, **Medium**, **Low**, and **Info**. For more information about how Tenable calculates severity, see CVSS vs. VPR.
Name	The name of the vulnerability.
CVSS3 Score	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Cloud Security shows a Tenable-predicted score.
Plugin family	The plugin family for the vulnerability.
Impacted resources	The number of impacted resources.
VPR Score	The Vulnerability Priority Rating (VPR) assigned to the vulnerability.
Last detected	This is the time when the vulnerability was last detected.

4. To view the details of a vulnerability, click the vulnerability name.

   The **Vulnerability details** plane appears with the following information:

Section	Description
Vulnerability information	Includes the details about the vulnerability such as the severity, plugin family, plugin ID, the ease of exploitation, and the patch publication date.
VPR Key Drivers	Gives the key drivers that Tenable uses to calculate the VPR of a vulnerability.
Description	Provides a description of the vulnerability.
Solution	Provides the solution to fix the vulnerability.
Impacted Resources	Lists the impacted resources and the detection date of the vulnerability on the resource.

5. To view specific vulnerabilities on the **Vulnerabilities** tab, do one of the following:

   - Use the **Search** box to search by CVE or Plugin ID.
   - Use the following filters:

     a. Click the ⏷ **Filters** icon to open the **Filter Vulnerabilities** box.

     b. Select the following filters as needed.

Filter	Description
Severity	Filters the list by severity: critical, high, medium, or low.
Plugin family	Filters the list of vulnerabilities by plugin family name. Use the search box to search for a specific plugin family.
VPR	Filters by the vulnerability priority rating (VPR) score.
Projects	Filters the list by projects.
Cloud provider	Filters the list by cloud providers.
Cloud	Filters the list by cloud accounts.

accounts	
Source	Filters by the source of the vulnerability — Cloud or Image.

   c. Click **Apply Filters**.

      Tenable Cloud Security applies the filters and displays the filtered vulnerabilities.

6. To export the list of vulnerabilities as a CSV, click ⤓ **Export** > **CSV**.

7. To add or remove columns from the **Vulnerabilities** table:

   a. Click ▥ to display the column names.

   b. Select or deselect the check boxes next to the column name as needed.

      Tenable Cloud Security displays the selected columns.

      > **Note**: You cannot remove the **Severity** and **Name** columns from the table and these are disabled.

8. Click ⟳ to refresh the vulnerabilities list.