Managed Threat Detection

FAQs

Issue 08

Date 2022-07-16

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 About the Product

1.1 What Is Managed Threat Detection (MTD)?

Powered by an AI engine, threat intelligence, and detection policies, MTD intelligently examines access behavior in logs of cloud services to detect threats, generate alarms, and provide remediation. With MTD, you can respond to alarms, handle potential threats, and harden service security in a timely manner to prevent major losses such as information leakage, keeping your accounts and service secure and stable.

Detection Types

Table 1-1 lists the MTD detection types supported in each region.

Table 1-1 Detection types

Region	IAM Detection	DNS Detection	CTS Detection	OBS Detection	VPC Detection
AP-Bangkok	√	-	√	√	√
AP-Singapore	√	√	√	√	√
LA-MexicoCity	-	-	√	-	-
CN-Hong Kong	√	√	-	√	-

1.2 What Are Data Sources of MTD?

The data sources are cloud service logs. Currently, IAM, VPC, DNS, OBS, and CTS logs can be accessed and analyzed using MTD. Other types of files are not supported.

1.3 What Are the Detection Objects of MTD?

MTD examines cloud workloads (cloud resources or services) of your account.

1.4 How Is MTD Distinct from Other Security Services?

MTD can detect security risks of IAM accounts and DNS attacks, as well as risks of being intruded by checking CTS logs. These security risks cannot or barely can be detected by other security services.

1.5 What Threats Can MTD Detect?

MTD collects logs from IAM, VPC, DNS, CTS, and OBS and uses an AI engine, threat intelligence, and detection policies to continuously detect potential threats, malicious activities, and unauthorized behaviors, such as brute-force cracking, penetration attacks, and mining attacks. You can view alarms on a graphical dashboard.

MTD uses an elastic profile model, unsupervised model, and supervised model to detect abnormal behaviors in seven high-risk scenarios, including risky passwords, credential leakage, token exploitation, abnormal delegation, remote logins, unknown threats, and brute-force cracking. Therefore, MTD can detect distributed brute-force attacks even if they occur with low frequency. MTD can effectively detect the Linux.Ngioweb botnet, SystemdMiner Trojans, WatchBog Trojans, and Bad Rabbit ransomware.

1.6 How Do I Get Started with MTD After Purchasing It?

Before you use MTD, you need to create a detector and configure a tracker.

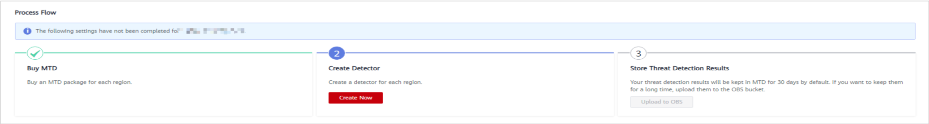
Step 1: Create a Detector

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the left navigation pane and choose **Security & Compliance** > **Managed Threat Detection**.

Figure 1-1 Home page of the MTD console



Process Flow

The following settings have not been completed fo [redacted]

✓ Buy MTD

Buy an MTD package for each region.

2 Create Detector

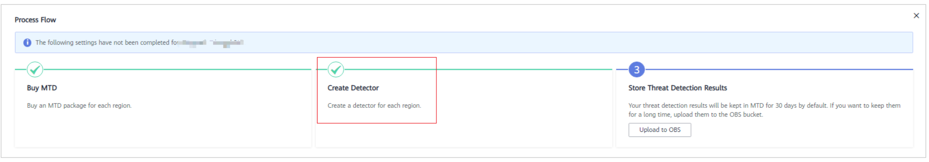
Create a detector for each region.

3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

Step 4 Click **Create Now** in the **Create Detector** pane. After the creation is complete, **Detector created.** is displayed. The page is automatically refreshed. Click in the upper left corner of the page to show the **Process Flow**. If **Create Detector** is checked as shown in **Detector created successfully**, the detector is created.

Figure 1-2 Detector created successfully



Process Flow

The following settings have not been completed for [redacted]

Buy MTD

Buy an MTD package for each region.

Create Detector

Create a detector for each region.

3 Store Threat Detection Results

Your threat detection results will be kept in MTD for 30 days by default. If you want to keep them for a long time, upload them to the OBS bucket.

----End

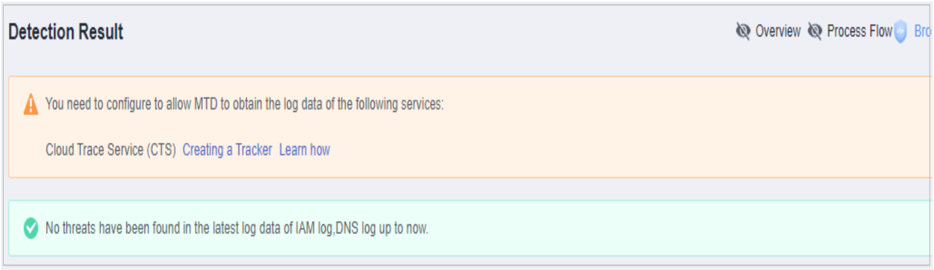
Step 2: Create a Tracker

NOTE

CTS threat detection is not supported for **CN-Hong Kong**. The tracker does not work in **CN-Hong Kong**.

Step 1 View the notice on the **Detection Result** page. The notice asks you to create a tracker.

Figure 1-3 Notice on the detection result page



Detection Result

You need to configure to allow MTD to obtain the log data of the following services:

Cloud Trace Service (CTS) Creating a Tracker Learn how

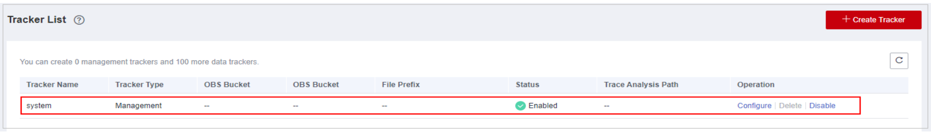
No threats have been found in the latest log data of IAM log,DNS log up to now.

Step 2 Click **Creating a Tracker** to switch to the CTS **Tracker List** page. In the tracker list, locate the only default tracker which is of the **Management** type.

NOTE

You do not need to create the **Management** tracker as it is created by the system.

Figure 1-4 Management tracker



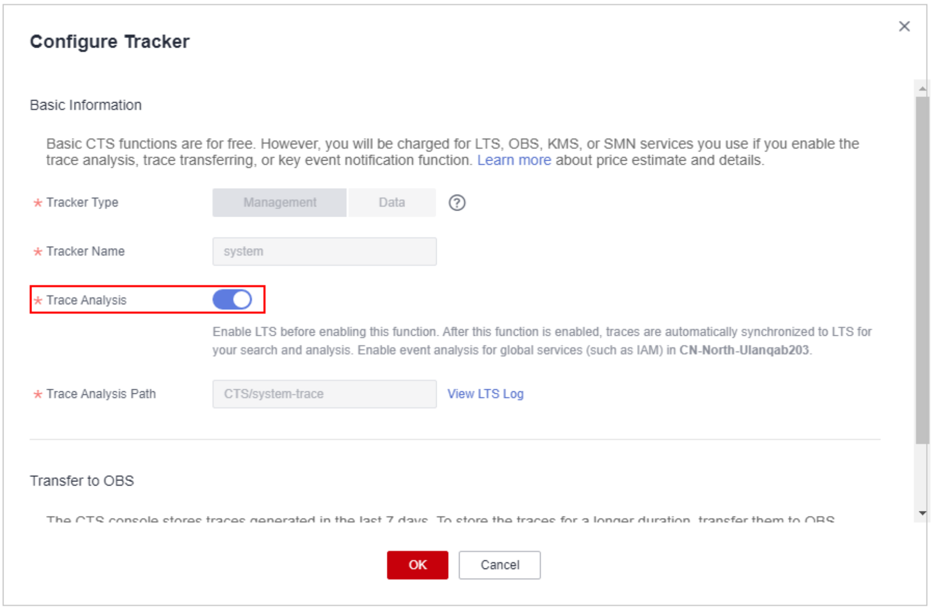
Tracker List

You can create 0 management trackers and 100 more data trackers.

Tracker Name	Tracker Type	OBS Bucket	OBS Bucket	File Prefix	Status	Trace Analysis Path	Operation
system	Management	--	--	--	Enabled	--	Configure | Delete | Disable

Step 3 Click **Configure** in the **Operation** column of the target tracker. In the displayed **Configure Tracker** dialog box, enable **Trace Analysis** and set other parameters as required.

Figure 1-5 Enabling event analysis



Basic Information

Basic CTS functions are for free. However, you will be charged for LTS, OBS, KMS, or SMN services you use if you enable the trace analysis, trace transferring, or key event notification function. Learn more about price estimate and details.

* Tracker Type: Management | Data

* Tracker Name: system

* Trace Analysis: enabled

Enable LTS before enabling this function. After this function is enabled, traces are automatically synchronized to LTS for your search and analysis. Enable event analysis for global services (such as IAM) in **CN-North-Ulanqab203**.

* Trace Analysis Path: CTS/system-trace

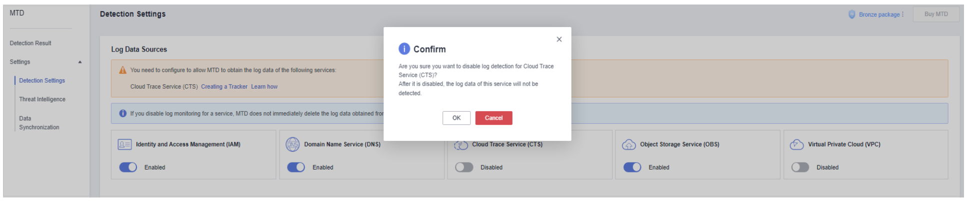
Transfer to OBS

The CTS console stores traces generated in the last 7 days. To store the traces for a longer duration, transfer them to OBS

Step 4 Click ☰ in the left navigation pane and choose **Security & Compliance** > **Managed Threat Detection**.

Step 5 In the left navigation pane, choose **Settings > Detection Settings**. On the **Detection Settings** page, click next to **Cloud Trace Service (CTS)**. In the displayed dialog box, click **OK** to temporarily disable CTS threat detection. **Operation successfully!** is displayed in the upper right corner.

Figure 1-6 Disabling CTS



You need to configure to allow MTD to obtain the log data of the following services:

Cloud Trace Service (CTS) Creating a Tracker Learn how

If you disable log monitoring for a service, MTD does not immediately delete the log data obtained fro

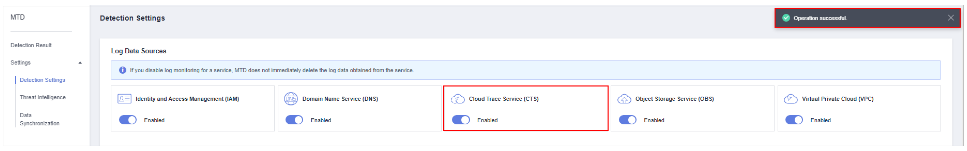
Confirm

Are you sure you want to disable log detection for Cloud Trace Service (CTS)?
After it is disabled, the log data of this service will not be detected.

Identity and Access Management (IAM)	Domain Name Service (DNS)	Cloud Trace Service (CTS)	Object Storage Service (OBS)	Virtual Private Cloud (VPC)
Enabled	Enabled	Disabled	Enabled	Disabled

Step 6 Click behind **Cloud Trace Service Log (CTS)** to enable CTS threat detection. **Operation successfully!** is displayed in the upper right corner.

Figure 1-7 Enabling CTS detection



Operation successful.

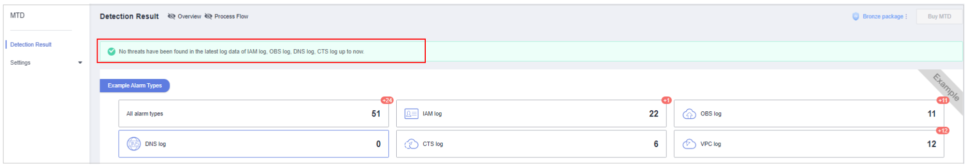
If you disable log monitoring for a service, MTD does not immediately delete the log data obtained from the service.

Identity and Access Management (IAM)	Domain Name Service (DNS)	Cloud Trace Service (CTS)	Object Storage Service (OBS)	Virtual Private Cloud (VPC)
Enabled	Enabled	Enabled	Enabled	Enabled

Step 7 In the navigation pane on the left, choose **Detection Result**. On the displayed page, check that the notice asking you to create a tracker disappears, and that CTS log is enabled. The tracker is configured successfully.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Figure 1-8 Tracker configured



No threats have been found in the latest log data of IAM log, OBS log, DNS log, CTS log up to now.

----End

2 Regions and AZs

2.1 What Are Regions and AZs?

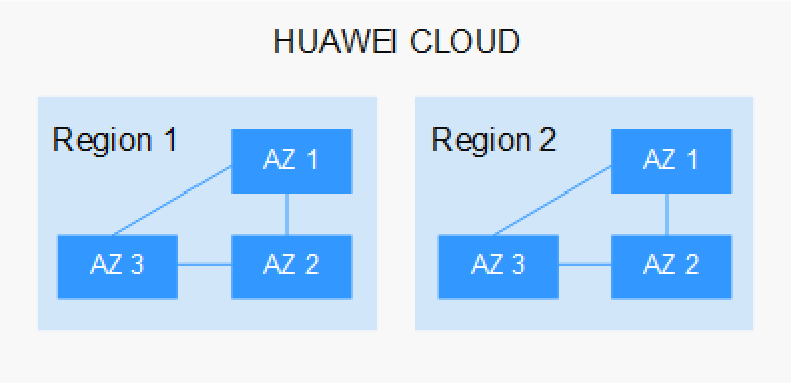
Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

Figure 2-1 shows the relationship between the regions and AZs.

Figure 2-1 Region and AZ



Huawei Cloud provides services in many regions around the world. You can select a region and AZ as needed.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces network latency and improves access rate.

  - If you or your users are in the Asia Pacific region and outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your users are in Africa, select the **AF-Johannesburg** region.
  - If you or your users are in Latin America, select the **LA-Santiago** region.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

2.2 Can MTD Be Used Across Regions?

No.

MTD is a region-level service and can be used only in the region you select when purchasing it.

3 Purchase Consulting

3.1 Will I Be Charged If I Disable All Log Data Sources After Purchasing MTD?

You have paid for the package when purchasing the MTD service. After you disable all log data sources, you will not be charged.

After you purchase a package, you will be billed on a pay-per-use basis only when the detected log data exceeds the purchased package capacity. For details about the billing mode, see **Pay-Per-Use**.

3.2 How Will I Be Billed for Using MTD?

You will be charged based on the service specifications, usage duration, and the volume of scanned logs that exceed the pre-purchased specifications.

MTD provides bronze, silver, gold, and platinum packages and will charge you on a yearly/monthly basis for using any one of them. If the volume of detected logs exceeds the purchased package, the system buys an add-on package for you and charges you on a pay-per-use basis.

NOTE

If the purchased specifications (bronze, silver, gold, and platinum packages) expire and you do not renew them, MTD will charge you on a pay-per-use basis.

For details about MTD billing mode, see **Billing**.

For pricing details, see **MTD Pricing Details**.

3.3 How Can I Unsubscribe from MTD?

MTD cannot be unsubscribed from on the management console.

You can unsubscribe from it by creating a service ticket. For details, see **Creating a Service Ticket**.

Copyright © Huawei Cloud Computing Technologies Co., Ltd.

3.4 How Do I Renew MTD After It Expires?

You can renew the purchased MTD service only when the validity period ends. The service specifications cannot be changed during the renewal. After the renewal, you can continue to use MTD.

Before the service expires, the system sends an SMS message or email to remind you that the service is about to expire.

If you do not renew MTD after it expires, your resources will enter a retention period. The resources will be automatically deleted and cannot be restored. The service cannot be renewed after the retention period ends. For details about the retention period, see **Service Suspension and Resource Release**.

Procedure

Step 1 **Log in to the management console.**

Step 2 In the top navigation pane, choose **Billing & Costs** > **Renewal**. The **Renewals** page of the Billing Center is displayed.

Step 3 On the **Renewals** page, click the **Manual Renewals** tab.

Step 4 Select all items to be renewed of the **Managed Threat Service**, and click **Renew**. The **Renew** page is displayed.

Step 5 Configure the **Renewal Duration**, for example, **9 months**.

Step 6 Complete the payment.

Step 7 Return to the **Renewals** page. The service has been renewed. Confirm the validity period.

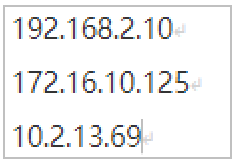
----End

4 About Functions

4.1 How Do I Edit Objects in Plaintext Format?

To upload whitelist and intelligence file to the OBS bucket, the file can only be in the plaintext format. A maximum of 10,000 IP addresses or domain names can be written into the file.

Ensure that each IP address or domain name in the whitelist or intelligence list occupy a line. The format is as follows.



```
192.168.2.10
172.16.10.125
10.2.13.69
```

Save the edited object file in .txt format.

4.2 Does MTD Support Automatic Defense?

No, MTD does not defend against attacks automatically. MTD generates alarms for access threats by detecting logs of cloud services (including IAM, CTS, OBS, VPC, and DNS).

4.3 How Do I Use My IAM Account to Grant MTD Permissions to a User of the Account?

When you use an IAM user to create a detector or perform other operations on the MTD console, you need to grant the user related permissions using the IAM account.

Prerequisites

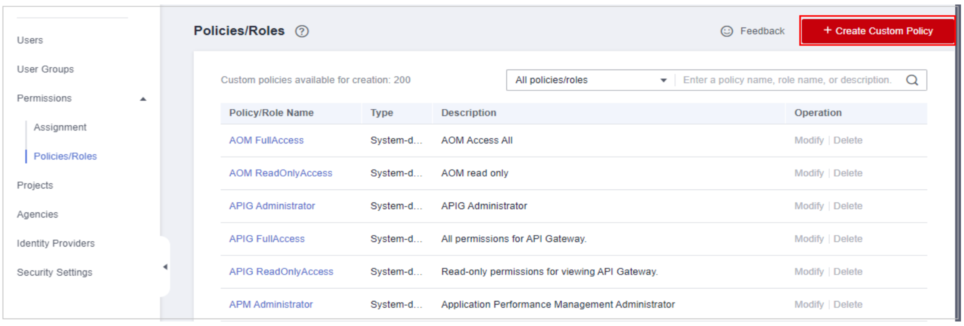
An IAM user has been created and added to the user group.

Step 1: Create a Custom Policy

Step 1 Log in to the IAM console.

Step 2 On the IAM console, choose **Permissions** > **Policies/Roles** from the navigation pane, and click **Create Custom Policy** in the upper right corner.

Figure 4-1 Creating a custom policy



Custom policies available for creation: 200

Policy/Role Name	Type	Description	Operation
AOM FullAccess	System-d...	AOM Access All	Modify | Delete
AOM ReadOnlyAccess	System-d...	AOM read only	Modify | Delete
APIG Administrator	System-d...	APIG Administrator	Modify | Delete
APIG FullAccess	System-d...	All permissions for API Gateway.	Modify | Delete
APIG ReadOnlyAccess	System-d...	Read-only permissions for viewing API Gateway.	Modify | Delete
APM Administrator	System-d...	Application Performance Management Administrator	Modify | Delete

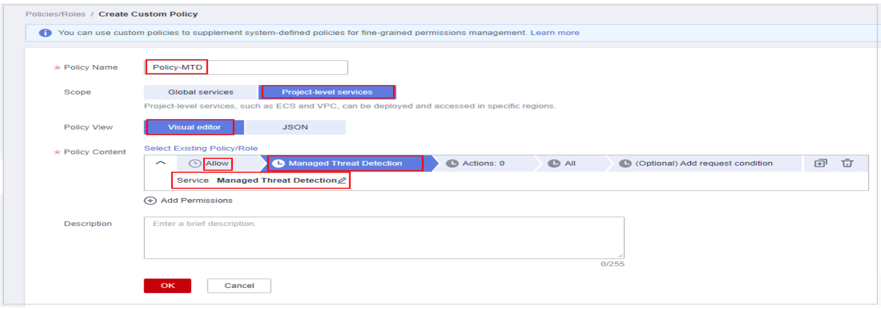
Step 3 On the **Create Custom Policy** page, configure required parameters as needed.

- **Policy Name**: Enter a policy name.
- **Scope**: Select **Project-level services**.
- **Policy View**: Select **Visual editor**.
- **Policy Content**: Select **Allow**.

  a. On the **Allow** tab, select **Allow**.

  b. On the **Select service** tab, enter **MTD** in the search box and select **Threat Detection Service (MTD)**.

Figure 4-2 Entering a policy name



You can use custom policies to supplement system-defined policies for fine-grained permissions management. Learn more

* Policy Name: Policy-MTD

Scope: Project-level services

Project-level services, such as ECS and VPC, can be deployed and accessed in specific regions.

Policy View: Visual editor

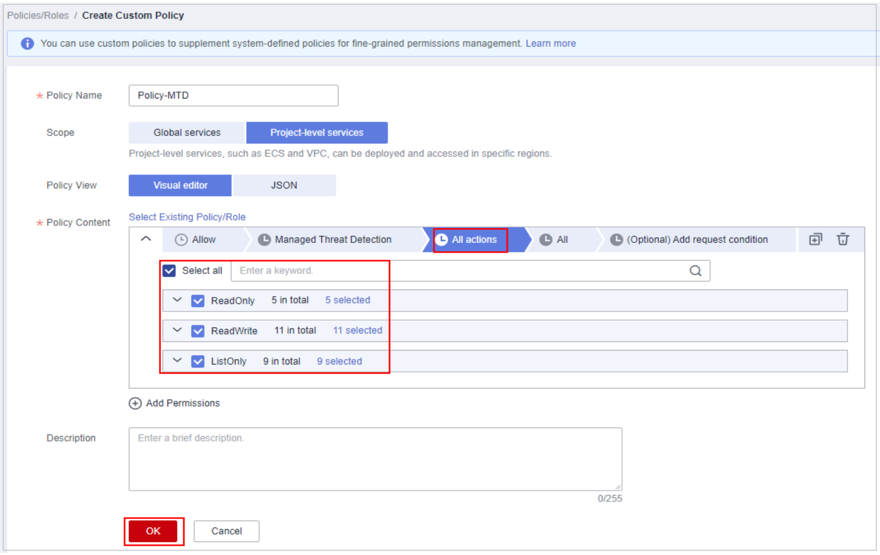
* Policy Content

Service Managed Threat Detection

Description

  c. On the **Actions** tab, click **Select all**.

Figure 4-3 Selecting all actions



Policies/Roles / Create Custom Policy

You can use custom policies to supplement system-defined policies for fine-grained permissions management. Learn more

* Policy Name: Policy-MTD

Scope: Global services | Project-level services

Project-level services, such as ECS and VPC, can be deployed and accessed in specific regions.

Policy View: Visual editor | JSON

* Policy Content: Select Existing Policy/Role

Allow | Managed Threat Detection | All actions | All | (Optional) Add request condition

☑ Select all — Enter a keyword.

☑ ReadOnly	5 in total	5 selected
☑ ReadWrite	11 in total	11 selected
☑ ListOnly	9 in total	9 selected

Add Permissions

Description: Enter a brief description. 0/255

OK | Cancel

Step 4 Click **OK**.

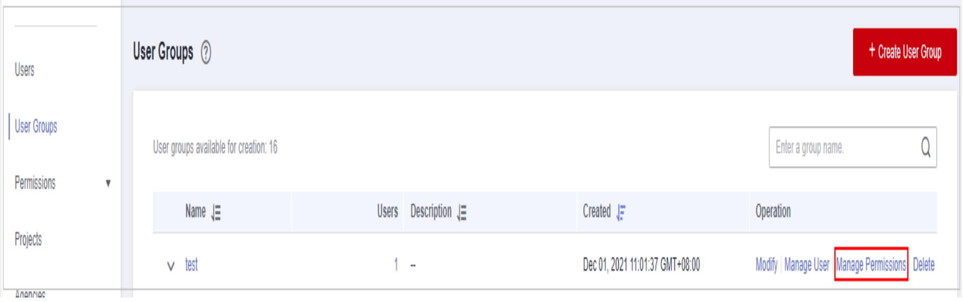
----End

Step 2: Grant Permissions to the User Group

Step 1 On the IAM console, choose **User Groups** from the navigation pane.

Step 2 In the row containing the target user group, click **Manage Permissions** in the **Operation** column.

Figure 4-4 Managing permissions



User Groups

+ Create User Group

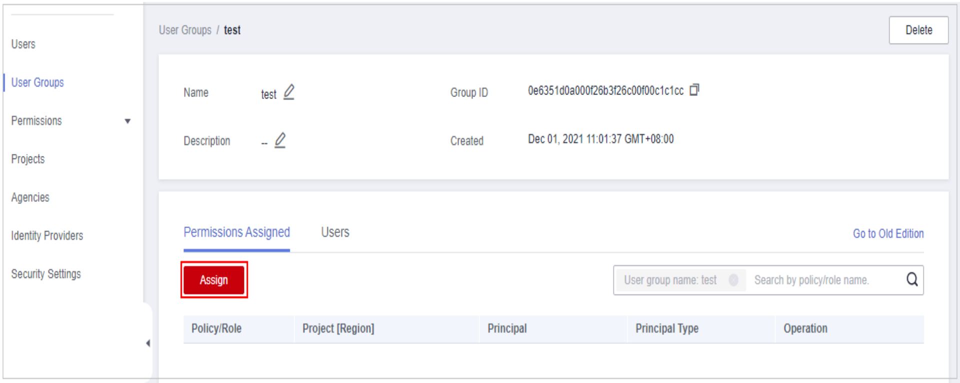
User groups available for creation: 16

Enter a group name.

Name	Users	Description	Created	Operation
test	1	--	Dec 01, 2021 11:01:37 GMT+08:00	Modify | Manage User | Manage Permissions | Delete

Step 3 On the **Permissions Assigned** tab, click **Assign**.

Figure 4-5 Assigning permissions



Name test

Group ID 0e6351d0a000f26b3f26c00f00c1c1cc

Description --

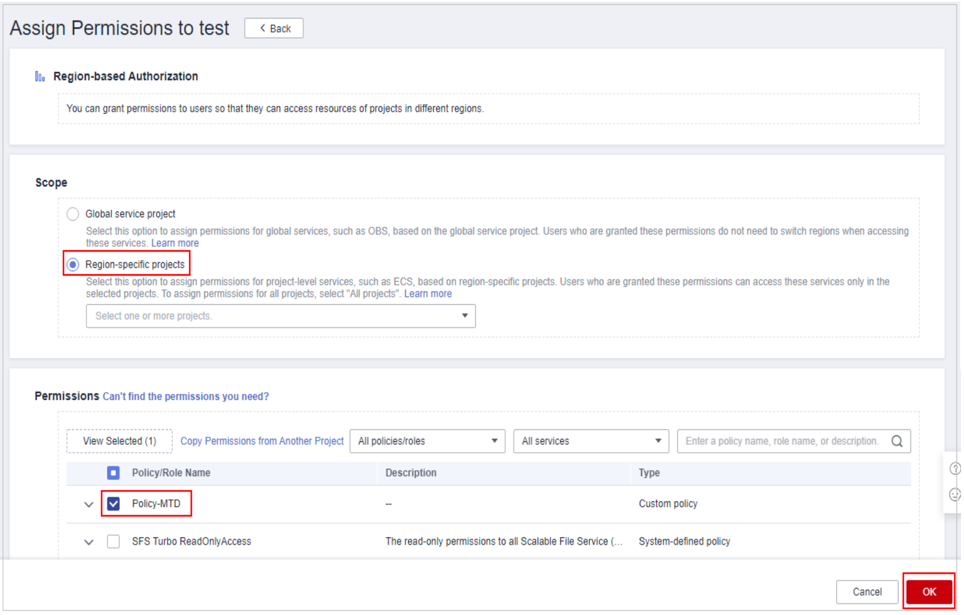
Created Dec 01, 2021 11:01:37 GMT+08:00

Policy/Role	Project [Region]	Principal	Principal Type	Operation

Step 4 In the **Scope** pane, select **Region-specific projects**.

Step 5 In the **Permissions** pane, select the policy create in **Step 1: Create a Custom Policy**.

Figure 4-6 Granting a policy to the user group


Assign Permissions to test
Back
Can't find the permissions you need?
View Selected (1)
Copy Permissions from Another Project
All policies/roles
All services
Enter a policy name, role name, or description.
Cancel
OK

Region-based Authorization

You can grant permissions to users so that they can access resources of projects in different regions.

Scope

○ Global service project

Select this option to assign permissions for global services, such as OBS, based on the global service project. Users who are granted these permissions do not need to switch regions when accessing these services. Learn more

● Region-specific projects

Select this option to assign permissions for project-level services, such as ECS, based on region-specific projects. Users who are granted these permissions can access these services only in the selected projects. To assign permissions for all projects, select "All projects". Learn more

Select one or more projects.

Permissions

	Policy/Role Name	Description	Type
☑	Policy-MTD	--	Custom policy
□	SFS Turbo ReadOnlyAccess	The read-only permissions to all Scalable File Service (...	System-defined policy

Step 6 Click **OK**.

----End

A Change History

Date	Description
2022-07-16	This issue is the eighth official release. Added the following FAQs: **How Will I Be Billed for Using MTD?** **How Can I Unsubscribe from MTD?** **How Do I Renew MTD After It Expires?**
2022-04-26	This issue is the seventh official release, which incorporates the following change: Added the **CN-Hong Kong** region. IAM, DNS, CTS, OBS, and VPC detection is supported in the **CN-Hong Kong** region.
2022-03-28	This issue is the sixth official release. Provisioned DNS detection for AP-Bangkok, and IAM, DNS, CTS, OBS, and VPC detection for AP-Singapore.
2022-03-08	This issue is the fifth official release. Modified **What Is Managed Threat Detection (MTD)?**
2022-01-14	This issue is the fourth official release. Added VPC threat detection and optimized the description.
2021-12-03	This issue is the third official release. Added **How Do I Use My IAM Account to Grant MTD Permissions to a User of the Account?** Deleted "Is MTD Free?" Deleted "What Can I Do If Token Verification Fails When I Use Other Services After Purchasing MTD?"
2021-11-30	This issue is the second official release. Added **Can MTD Be Used Across Regions?**
2021-11-17	This issue is the first official release.