

Guidance to detect Anomalous activity

Step 1: Check resources that had exposure

- a) Go to your Automation account in [Azure Portal](#). Navigate to the Identity tab under "Account Settings". Take note of the Id of your automation account on top left corner (The Id in the example below is 'test 38'). Then click on the "Azure role assignments".

Dashboard > test38

test38 | Identity

Automation Account

Search (Ctrl+ /)

Connections

Certificates

Variables

Related Resources

Linked workspace

Event grid

Start/Stop VM

Account Settings

Properties

Networking

Keys

Pricing

Source control

Run as accounts

Identity

Settings

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Azure AD, so you don't have to store any credentials in code. [Learn more about Managed identities.](#)

Save Discard Refresh Got feedback?

Status

Off On

Object (principal) ID

Permissions

Azure role assignments

This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures. [Learn more](#)

- b) The page will list all Azure resources that are linked to [Managed identities](#).

Dashboard > Automation Accounts > test38 >

Azure role assignments

+ Add role assignment (Preview) Refresh

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *

Role	Resource Name	Resource Type	Assigned To	Condition
Contributor		Resource Group	test38	None
Contributor		Subscription	test38	None

Step 2: Scan Logs for anomalous activity

a) For the previous step (Step 1b), click on the resource to be redirected to the portal page of that resource

[Dashboard](#) > [Automation Accounts](#) > [test38](#) >

Azure role assignments

...

+

Add role assignment (Preview)



↺

Refresh

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)


Subscription *

Oaas-SubLib-039

Role	Resource Name	Resource Type	Assigned To	Condition
Contributor	 [REDACTED]	Resource Group	test38	None
Contributor	 Oaas-SubLib-039	Subscription	test38	None

b) On the resource portal page, navigate to the “Activity logs”

[Dashboard](#) > [Automation Accounts](#) > [test38](#) > [Azure role assignments](#) > [Oaas-SubLib-039](#)



Oaas-SubLib-039

Subscription

Activity log

...

Search (Ctrl+ /)

«

Activity

Edit columns

Refresh

Diagnostics settings

Download as CSV

Logs

Pin current filters

Reset filters

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Events

Cost Management

Cost analysis

Cost alerts

Budgets

Advisor recommendations

Billing

Invoices

Partner information

Settings

Programmatic deployment

Resource groups

Resources

Preview features

Looking for Log Analytics? In Log Analytics you can search for performance, diagnostics, health logs, and more. [Visit Log Analytics](#)

Search

Quick Insights

Management Group : None
















Subscription : Oaas-SubLib-039

Event severity : All

Timespan : Last 6 hours

Add Filter

22 items.

Operation name	Status	Time	Time stamp	Subscription
>  Create role assignment	Succeeded	3 minutes a...	Thu Jan 20 ...	Oaas-SubLib-039
>  Create role assignment	Succeeded	4 minutes a...	Thu Jan 20 ...	Oaas-SubLib-039
>  Write RoleAssignments	Succeeded	6 minutes a...	Thu Jan 20 ...	Oaas-SubLib-039
>  Create or Update an Azure Automation Runbook	Succeeded	17 minutes ...	Thu Jan 20 ...	Oaas-SubLib-039
>  Update resource group	Succeeded	23 minutes ...	Thu Jan 20 ...	Oaas-SubLib-039
>  Validate Deployment	Succeeded	27 minutes ...	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	4 hours ago	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	4 hours ago	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	4 hours ago	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	4 hours ago	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	4 hours ago	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	4 hours ago	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	5 hours ago	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	5 hours ago	Thu Jan 20 ...	Oaas-SubLib-039
>  Delete resource group	Failed	5 hours ago	Thu Jan 20 ...	Oaas-SubLib-039

- c) Set "Timespan" from December 1, 2021, to December 10, 2021, and scan for any anomalous activity. Possible actions include (not an exhaustive list): Resetting of a password on a VM, change access level from "Contributor" to higher privileges, Starting and Stopping of a VM. Such an event will be logged by the Automation Id (Collected in Step 1a) in the column "Event initiated by"
- d) Repeat steps 2a to 2c for every resource discovered in step 1b.