

Chaos Engineering Scenario: Leverage Chaos Studio to validate the impact of an AAD outage on an application dependency

Introduction

You can use a chaos experiment to verify that your application is resilient to global Azure Active Directory (AAD) outages by causing those outages in a controlled environment. By following this guide, you will simulate an AAD outage using a NSG Security Rule fault and Azure Chaos Studio. The purpose of this simulation is to help you defend and prepare against AAD service outages.

Prerequisites

Before proceeding, you should understand:

- Your service's or application's dependency on Azure Active Directory (https://azure.microsoft.com/services/active-directory/?&ef_id=CjwKCAjwquWVBhBrEiwAt1Kmwp7l8eVJ6-27pOtVtEO9xLok6QmaWqGcqOB9oojv9hU3myL562cMMxoCNJ0QAvD_BwE:G:s&OCID=AID2200277_SEM_CjwKCAjwquWVBhBrEiwAt1Kmwp7l8eVJ6-27pOtVtEO9xLok6QmaWqGcqOB9oojv9hU3myL562cMMxoCNJ0QAvD_BwE:G:s&gclid=CjwKCAjwquWVBhBrEiwAt1Kmwp7l8eVJ6-27pOtVtEO9xLok6QmaWqGcqOB9oojv9hU3myL562cMMxoCNJ0QAvD_BwE)
- Network Security Groups (<https://docs.microsoft.com/azure/virtual-network/service-tags-overview>)
- AZ Command-Line Interface (<https://docs.microsoft.com/cli/azure/>)
- The Azure Quality Program (<https://eng.ms/docs/quality/program-overview>)

Note: For the NSG resource targeted in the experiment, make sure that there is not an NSG outbound rule set to a higher priority that would override the rule to be created during the experiment execution.

Tools

This scenario requires you to have:

- An Azure subscription (<https://docs.microsoft.com/azure/guides/developer/azure-developer-guide#understanding-accounts-subscriptions-and-billing>). Create a subscription in AIRS (<https://azuremsregistration.microsoft.com/Default.aspx>) before you begin.
- Access to either Azure CLI or Cloud Shell (<https://portal.azure.com/#cloudshell/>).

Scenario background

AAD provides single sign-on (SSO), multifactor authentication (MFA), and Conditional Access to guard against most cybersecurity attacks. This helps protect access to resources and data using strong authentication and risk-based adaptive access policies without compromising the user experience. AAD is integral to authenticate numerous applications.

In this scenario, you are temporarily adding a NSG rule using the NSG fault which will cut off communication between AAD and any application running behind that NSG, such as your resource dependencies.

Scenario goal

In this scenario, you will:

- Understand how to evaluate the impact of dependency on AAD and the impact of related outages by using Chaos Studio.
 - Identify and use key metrics to formulate an experiment hypothesis.
 - Create an experiment that validates the response of a deployed application in the event of an AAD outage.
 - Interpret experiment results to assess and potentially reformulate your created hypothesis.
-

Establish a hypothesis

Establishing a hypothesis is critical before beginning an experiment. Without a hypothesis, it is difficult to understand what to test or how to interpret any results.

For this scenario, create a hypothesis that addresses both AAD and observability expectations. If there is an AAD outage and it causes a failure to resolve one or more of your application's dependencies, what do you expect to happen, and how do you expect to receive the results?

To create a hypothesis, ask questions relevant to the scenario. For example, what resilience measures are already in place to mitigate the impact of an AAD outage? Do these resilience measures work as expected? By running this experiment, what do you expect to happen given your specific application setup? What does a healthy result look like? What is your failure tolerance? What metrics are you assessing?

A hypothesis for this scenario might look like: "In the event of an AAD outage, **ICM incidents were created, and the appropriate resiliency measures were activated. I expect to find the experiment results by analyzing .**" The hypothesis may differ based on your environment.

Using this example, a potential hypothesis may be: "In the event of an AAD outage, no ICM incidents were created, and the appropriate resiliency measures were activated. I expect to find the experiment results by analyzing my application's availability metrics against my defined SLIs and SLOs."

Create an experiment

1. Set up a fault that Chaos Studio will inject into your application or infrastructure using the JSON file below. Save the **JSON file** included below in the same location you are running the **Azure CLI**.

```
{
  "location": "eastus2euap",
  "identity": {
    "type": "SystemAssigned"
  },
  "properties": {
    "steps": [
      {
        "name": "Step1",
        "branches": [
          {
            "name": "Branch1",
            "actions": [
              {
                "type": "continuous",
                "name": "urn:csci:microsoft:networkSecurityGroup:securityRule/1.1",
                "parameters": [
                  {
                    "key": "Name",
                    "value": "block_aad_fault"
                  },
                  {
                    "key": "Protocol",
                    "value": "Any"
                  },
                  {
                    "key": "SourceAddresses",
                    "value": "[\\\"*\\\"]"
                  },
                  {
                    "key": "DestinationAddresses",
                    "value": "[\\\"AzureActiveDirectory\\\"]"
                  },
                  {
                    "key": "Action",
                    "value": "Deny"
                  },
                  {
                    "key": "DestinationPortRanges",
```

```

        "value": "[\\\"*\\\"]"
      },
      {
        "key": "SourcePortRanges",
        "value": "[\\\"*\\\"]"
      },
      {
        "key": "Priority",
        "value": "400"
      },
      {
        "key": "Direction",
        "value": "Outbound"
      },
      {
        "key": "FlushConnection",
        "value": "true"
      }
    ],
    "duration": "PT5M",
    "selectorid": "Selector1"
  }
]
}
]
}
],
"selectors": [
  {
    "id": "Selector1",
    "type": "List",
    "targets": [
      {
        "type": "ChaosTarget",
        "id": "/subscriptions/472626f1-3dab-48f5-81e2-d6e1733b586a/resourceGroups/hagurbuz-ses-xms-dev/providers/Microsoft.Network/networkSecurityGroups/test-fc-1/providers/Microsoft.Chaos/targets/microsoft-networksecuritygroup"
      }
    ]
  }
]
}

```

```
}  
  }  
]
```

2. Run the following command in your CLI with the **subscription ID**, **resource group**, and **experiment name** replaced to match your experiment.

```
az rest --method put --uri https://management.azure.com/subscriptions/$SUBSCRIPTION_ID/resourceGroups/$RESOURCE_GROUP/providers/Microsoft.Chaos/experiments/$EXPERIMENT_NAME?api-version=2021-09-15-preview --body @experiment.json
```

Assign a role to the Network Contributor

Before triggering the experiment, you must assign a role to the Network Contributor. Otherwise, the fault you just created will not run correctly.

1. In Chaos Studio, select **Home**.

Microsoft Azure (Preview) [Report a bug](#) Search resources, services, and docs (G+/)

Home Chaos Studio >

Create an experiment

Chaos Studio | PREVIEW

Basics **Experiment designer** Review + create

Configure your experiment below. [Learn more](#)

Step 1
1 branch, 0 action, 0 target

Step *

Branch *

Fault	Parameter	Target resources
+ Add action		
Add branch		

[Add step](#)

Provide feedback
Did you find what you needed? Let us know how it went.

Add fault

PREVIEW

NSG Security Rule

Parameters

Parameters allow you to customize the impact of a fault.

Duration (minutes)

direction *

sourceAddresses * ⓘ

sourcePortRanges * ⓘ

destinationAddresses * ⓘ

destinationPortRanges * ⓘ

protocol *

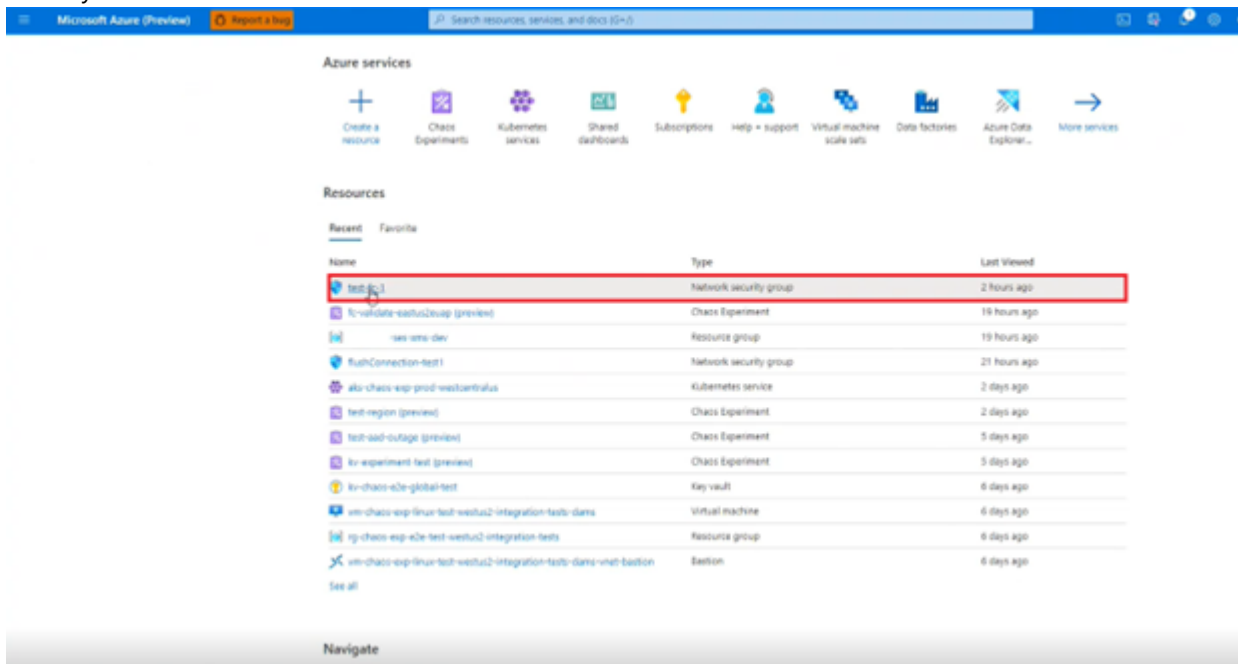
action *

priority

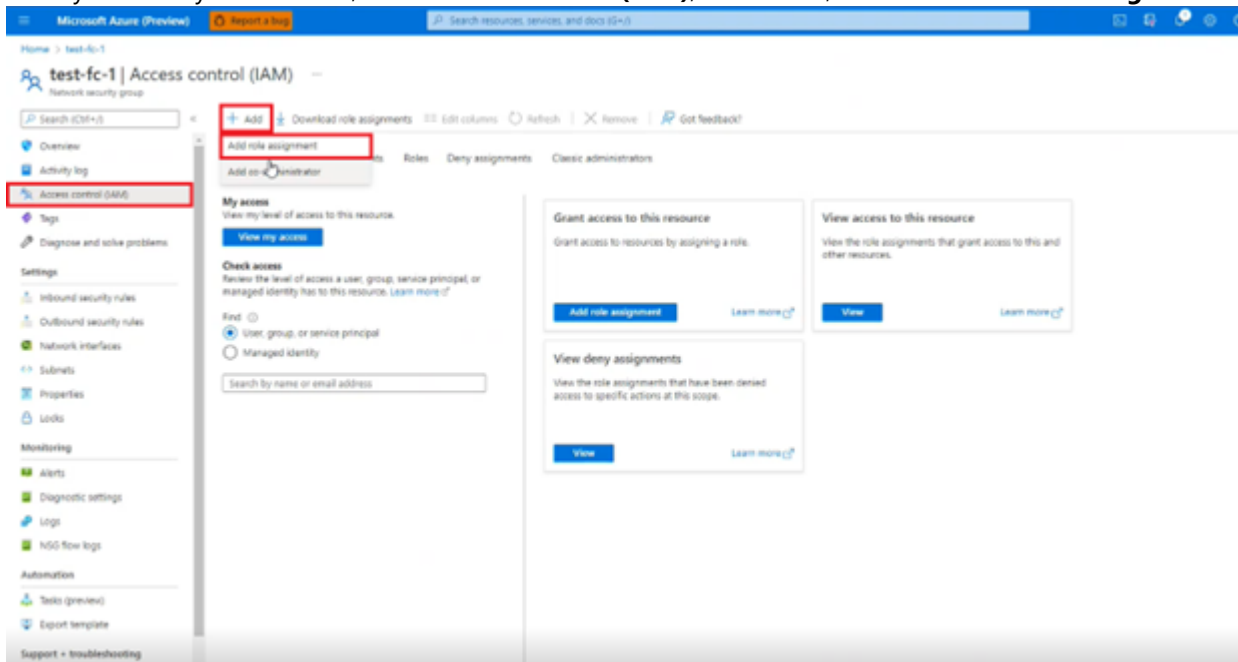
name *

[Add](#) [< Previous](#) [Next: Target resources >](#)

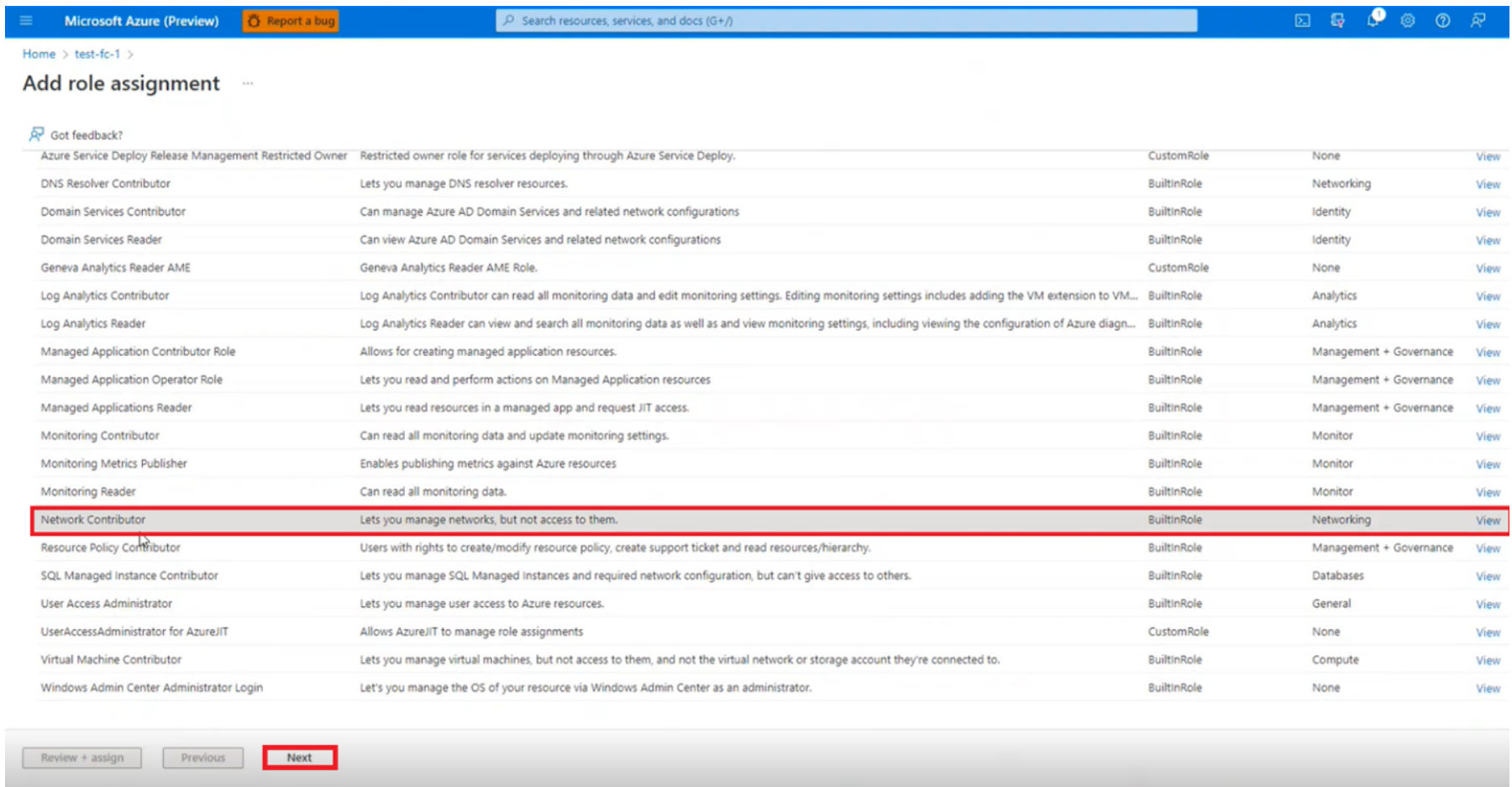
2. Select your resource.



3. Once you select your resource, select **Access control (IAM)**, select **Add**, then select **Add role assignment**.



4. Select **Network Contributor** and then **Next**.



Microsoft Azure (Preview) Report a bug Search resources, services, and docs (G+/I)

Home > test-fc-1 >

Add role assignment

Got feedback?

Azure Service Deploy Release Management Restricted Owner	Restricted owner role for services deploying through Azure Service Deploy.	CustomRole	None	View
DNS Resolver Contributor	Lets you manage DNS resolver resources.	BuiltinRole	Networking	View
Domain Services Contributor	Can manage Azure AD Domain Services and related network configurations	BuiltinRole	Identity	View
Domain Services Reader	Can view Azure AD Domain Services and related network configurations	BuiltinRole	Identity	View
Geneva Analytics Reader AME	Geneva Analytics Reader AME Role.	CustomRole	None	View
Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VM...	BuiltinRole	Analytics	View
Log Analytics Reader	Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the configuration of Azure diagn...	BuiltinRole	Analytics	View
Managed Application Contributor Role	Allows for creating managed application resources.	BuiltinRole	Management + Governance	View
Managed Application Operator Role	Lets you read and perform actions on Managed Application resources	BuiltinRole	Management + Governance	View
Managed Applications Reader	Lets you read resources in a managed app and request JIT access.	BuiltinRole	Management + Governance	View
Monitoring Contributor	Can read all monitoring data and update monitoring settings.	BuiltinRole	Monitor	View
Monitoring Metrics Publisher	Enables publishing metrics against Azure resources	BuiltinRole	Monitor	View
Monitoring Reader	Can read all monitoring data.	BuiltinRole	Monitor	View
Network Contributor	Lets you manage networks, but not access to them.	BuiltinRole	Networking	View
Resource Policy Contributor	Users with rights to create/modify resource policy, create support ticket and read resources/hierarchy.	BuiltinRole	Management + Governance	View
SQL Managed Instance Contributor	Lets you manage SQL Managed Instances and required network configuration, but can't give access to others.	BuiltinRole	Databases	View
User Access Administrator	Lets you manage user access to Azure resources.	BuiltinRole	General	View
UserAccessAdministrator for AzureJIT	Allows AzureJIT to manage role assignments	CustomRole	None	View
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.	BuiltinRole	Compute	View
Windows Admin Center Administrator Login	Let's you manage the OS of your resource via Windows Admin Center as an administrator.	BuiltinRole	None	View

[Review + assign](#) [Previous](#) **[Next](#)**

5. Click on **Select members**. Under **Select members**, search for the experiment name, and select **Select** at the bottom of the page. Then, select **Review + assign**.

Microsoft Azure (Preview)

Report a bug

Search resources, services, and docs (G+)

Home > test-fc-1 >

Add role assignment

Got feedback?

Role

Members

Review + assign

Selected role

Network Contributor

Assign access to

User, group, or service principal

Managed identity

Members

+ Select members

Name	Object ID	Type
No members selected		

Description

Optional

Review + assign

Previous

Next

Select members

Select

aad-demo-2

No users, groups, or service principals found.

Selected members:

aad-demo-2

Remove

Select

Close

6. Select **Review + assign** again.

Microsoft Azure (Preview)

Report a bug

Search resources, services, and docs (Ctrl-Q)

Home > test-fc-1 >

Add role assignment

Got feedback?

Role

Members

Review + assign

Role

Scope

Members

Description

network Contributor

/subscriptions/472628f1-3dab-48f5-81a2-d9e1733b586a/resourceGroups/...-res-vm-deu/providers/Microsoft.network/networkSecurityGroups/test-fc-1

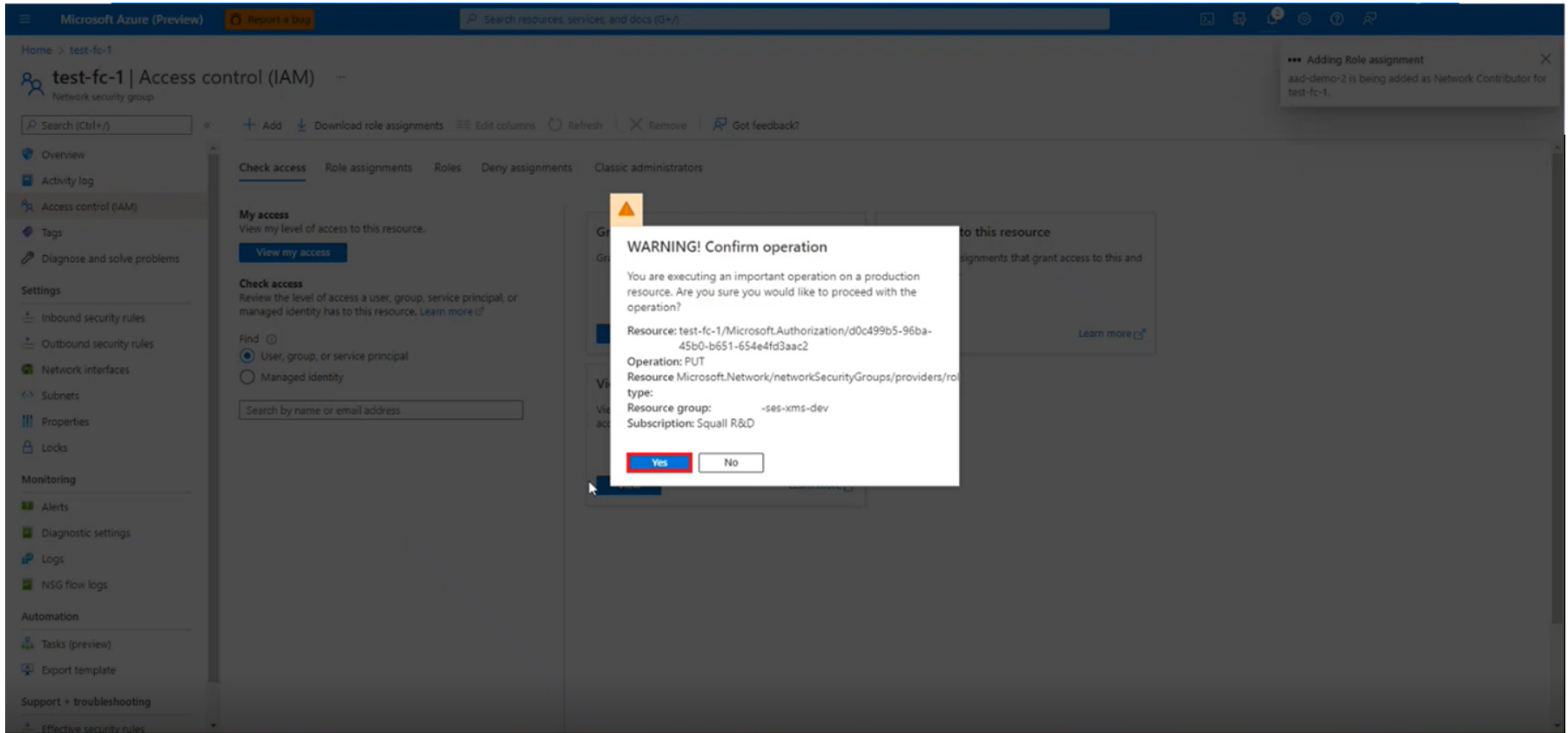
Name	Object ID	Type
aad-demo-2	0ee1a3ca-ebd7-4400-8877-5812a5eac9a8	App

no description

Review + assign

Previous

7. Select **Yes** on the **Warning! Confirm operation** box.



Trigger the experiment

1. Once the **Role assignment** has been successfully added, go back to **Azure Portal** and select your **Resource Group**.

Microsoft Azure (Preview) | Report a bug | Search resources, services, and docs (G+D)

Home > fc-validate-eastus2euap

Search (Ctrl+F)

Start Stop Edit Delete Refresh Feedback

Overview

Essentials

Resource group: **fc-validate-eastus2euap** | [View resource group](#)

Subscription: **fc-validate-eastus2euap** | [View subscription](#)

Location: **eastus2euap** | [View location](#)

Status: **Cancelled**

Last started: 6/22/2022, 11:19:06 AM

Last ended: 6/22/2022, 11:21:11 AM

History

Start time	End time	Status	Identifier
6/22/2022, 11:19:06 AM	6/22/2022, 11:21:11 AM	Cancelled	180CE5CD-A5E3-4653-895C-12885A3208D0
6/22/2022, 11:14:44 AM	6/22/2022, 11:14:44 AM	Cancelled	47D9912A-9E07-4990-8175-28A7818302D0
6/21/2022, 5:54:50 PM	6/21/2022, 6:01:44 PM	Success	8040321E-A589-4886-90CD-6D30A0287A41
6/21/2022, 1:27:42 PM	6/21/2022, 1:33:37 PM	Success	AAAC6A4F-0588-488A-8E7D-62DC58E6A31F
6/21/2022, 11:59:12 AM	6/21/2022, 12:04:48 PM	Success	83854143-783F-4480-873F-04D6108FAC7
6/20/2022, 3:18:25 PM	6/20/2022, 3:19:02 PM	Failed	E734EDC1-5388-4461-986A-421E31152E03
6/20/2022, 2:57:52 PM	6/20/2022, 2:58:10 PM	Failed	C8C3755F-A274-482D-8015-0C76389F017D
6/20/2022, 2:40:55 PM	6/20/2022, 2:41:21 PM	Failed	D88EA880-97FC-4745-AD68-DE10E6AF686A
6/20/2022, 2:39:06 PM	6/20/2022, 2:39:34 PM	Failed	AC83C43F-4A71-4770-8335-932155823D8

2. Select your experiment. If it does not show up, select **Refresh** and search for it again.

Microsoft Azure (Preview) | Report a bug | Search resources, services, and docs (G+D)

Home > ses-xms-dev

Resource group: **ses-xms-dev**

Search (Ctrl+F)

Create Manage view Delete resource group Refresh Export to CSV Open query Assign tags Move Delete Export template Open in mobile

Overview

Essentials

Subscription: **ses-xms-dev** | [View subscription](#)

Subscription ID: 4726247F-3A86-48F5-8162-0E417316086A

Region: **eastus2euap** | [Click here to add tags](#)

Deployments: **13 Failed 180 Succeeded**

Location: **West US 2**

Resources

Recommendations (1)

Filter for any field...

Type equals all Location equals all Add filter

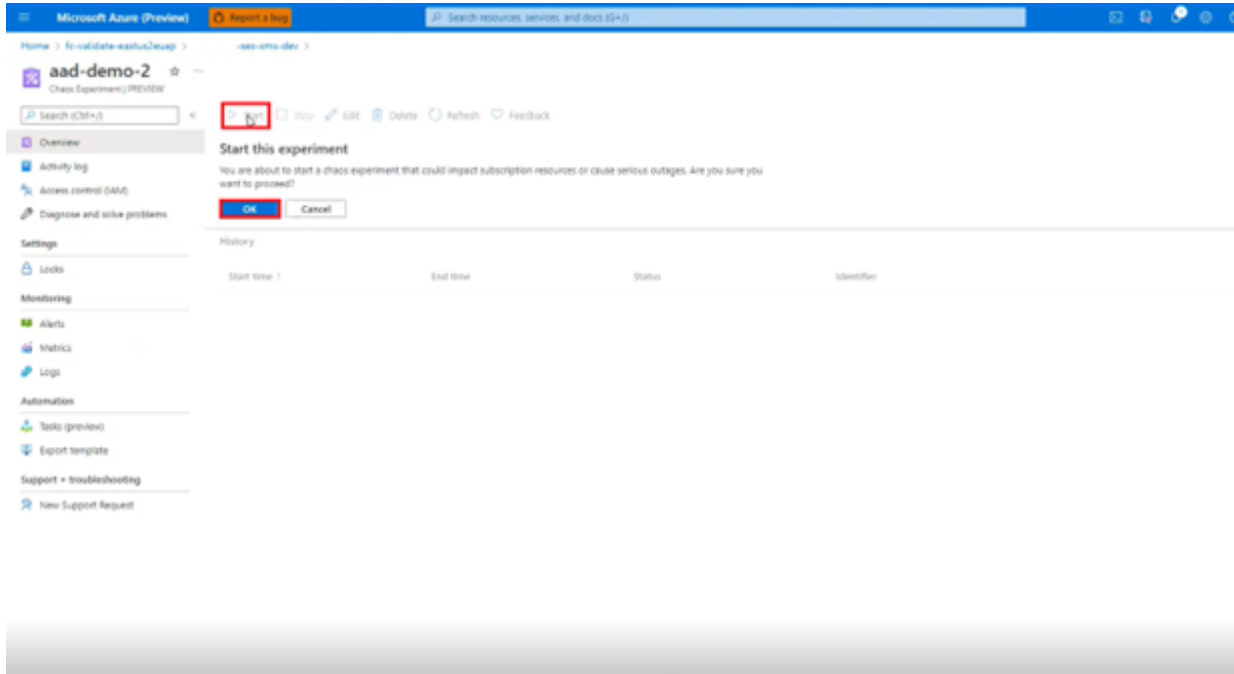
Showing 1 to 41 of 41 records

Show hidden types

Two grouping

Name	Type	Location
aad-demo-2	Chaos Experiment	eastus2euap
arg-test	Application security group	West US 2
experiment	Event Grid Topic	West US 2
fc-validate	Chaos Experiment	West US 2
fc-validate-eastus2euap	Chaos Experiment	eastus2euap
flushConnection-test1	Network security group	East US
-dev-cosmosdb	Azure Cosmos DB account	West US 2
-dev-sbus	Service Bus Namespace	West US 2
-toDenyAccess	Key vault	West US
-toLocal-eastus2	Key vault	West US 2
-test-localtesting	Managed identity	Central US

3. Select **Start** and then select **OK**.



4. The experiment is successfully running once the status updates to **Running**.

The screenshot displays the Microsoft Azure portal interface for a Chaos Experiment named 'aad-demo-2'. The experiment is in the 'Running' state, as indicated by the blue play icon and the text 'Running' in the History table. The interface includes a top navigation bar with the Microsoft Azure (Preview) logo, a search bar, and a 'Report a bug' button. The left sidebar contains a navigation menu with options like Overview, Activity log, Access control (IAM), Diagnose and solve problems, Settings, Locks, Monitoring, Alerts, Metrics, Logs, Automation, Tasks (preview), Export template, Support + troubleshooting, and New Support Request. The main content area shows the experiment details, including the Resource group (-ses-xms-dev), Subscription (Squall R&D), and Location (eastus2euap). The History table lists the experiment's start time (6/22/2022, 1:10:39 PM), end time (-), status (Running), and identifier (98E1071B-0624-4CD5-9703-A5F04CD6EF64).

Microsoft Azure (Preview) Report a bug Search resources, services, and docs (G+)

Home > fc-validate-eastus2euap > -ses-xms-dev >

aad-demo-2 ☆ ...
Chaos Experiment | PREVIEW

Search (Ctrl+/) « Start Stop Edit Delete Refresh Feedback

Overview

- Activity log
- Access control (IAM)
- Diagnose and solve problems

Settings

- Locks

Monitoring

- Alerts
- Metrics
- Logs

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

- New Support Request

Essentials

Resource group (move) : -ses-xms-dev Status : Running

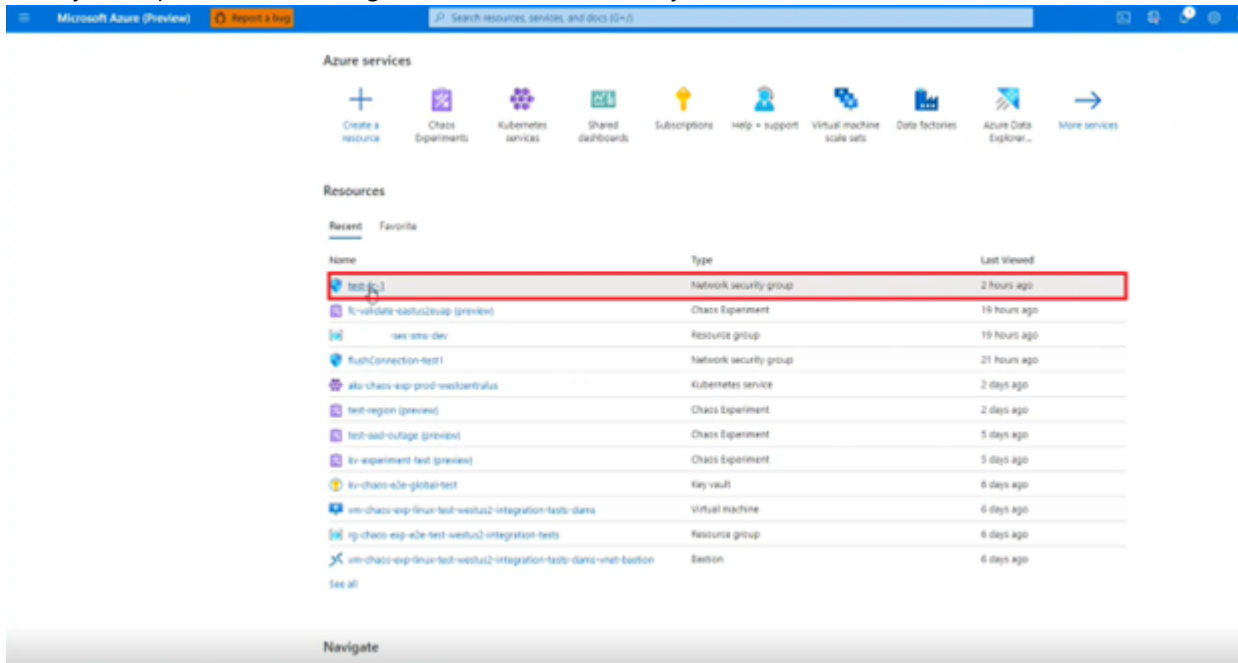
Subscription (move) : Squall R&D Last started : 6/22/2022, 1:10:39 PM

Location (move) : eastus2euap Last ended : -

History

Start time ↑	End time	Status	Identifier
6/22/2022, 1:10:39 PM	-	Running	98E1071B-0624-4CD5-9703-A5F04CD6EF64

5. Once your experiment is running, select **Home** and select your resource.



6. On your resource page, select **Overview** to check for the rule blocking AAD outbound calls. If the rule you inputted says Deny under Action, then it is working correctly and blocking all outbound calls to AAD.

Microsoft Azure (Preview) Report a bug Search resources, services, and docs (G+)

Home > test-fc-1 Network security group

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Monitoring

Alerts

Diagnostics settings

Logs

NSG flow logs

Automation

Tasks (preview)

Export template

Support + troubleshooting

Effective security rules

Subscription ID : 472626f1-3dab-48f5-81e2-d6e1733b586a

Tags (edit) : Click here to add tags

Filter by name

Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
101	NRMS-Rule-101	443	Tcp	VirtualNetwork	Any	Allow
103	NRMS-Rule-103	Any	Any	CorpNetPublic	Any	Allow
104	NRMS-Rule-104	Any	Any	CorpNetSaw	Any	Allow
105	NRMS-Rule-105	1433,1434,3306,4333,5432,6379,70...	Any	Internet	Any	Deny
106	NRMS-Rule-106	22,3389	Tcp	Internet	Any	Deny
107	NRMS-Rule-107	23,135,445,5985,5986	Tcp	Internet	Any	Deny
108	NRMS-Rule-108	13,17,19,53,69,111,123,512,514,593,...	Any	Internet	Any	Deny
109	NRMS-Rule-109	119,137,138,139,161,162,389,636,20...	Any	Internet	Any	Deny
4005	test-rule-4005	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
400	block_aad_fault	Any	Any	Any	AzureActiveDirectory	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Assess the hypothesis

Compare the results of the experiment against your hypothesis. Analyze any relevant metrics. Do the results align with your expectations?

For example, if your hypothesis addresses availability metrics, analyze your health model in Geneva for the duration of the Chaos experiment to see if there was any impact on the failure rate. If there was an impact, analyze the returned logs and metrics from the experiment to understand why there was a failure rate impact. Similarly, if you are testing to validate SLI alerts or to validate feedback on failures, analyze any feedback against the hypothesis to ensure the alerts are properly responding to failures.

If your results were unexpected, consider any reasons why, create a new hypothesis, implement any necessary changes, and repeat the experiment: "In the event of a AAD outage, **ICM incidents were created, and the appropriate resiliency measures were activated because** resilience improvement has been made. I expect to find the experiment results by analyzing ___."

Overview

You have now learned about AAD and observability metrics, how to formulate and evaluate an experiment hypothesis, and how to create an experiment in Azure Chaos Studio that tests the impact of an AAD outage on an application dependency.

Next steps

- Manage your experiment (<https://docs.microsoft.com/azure/chaos-studio/chaos-studio-tutorial-service-direct-portal#:~:text=Manage%20your%20experiment>)

Additional resources

- Troubleshoot issues with Azure Chaos Studio (<https://docs.microsoft.com/azure/chaos-studio/troubleshooting>)
- Chaos Studio fault and action library (<https://docs.microsoft.com/azure/chaos-studio/chaos-studio-fault-library>)