



Power Automate, Key Vault & IPs update

Narisorn Limpaswadpaisarn

Client Technology Lead - Microsoft

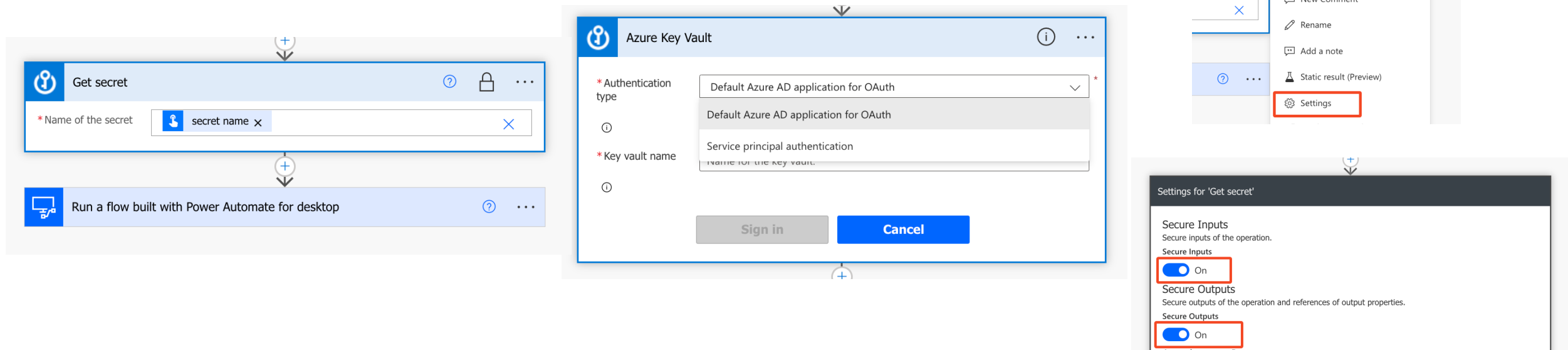
narisornl@microsoft.com

Prerequisites

- Azure Subscription (for Azure Key Vaults)
- Power Automate licenses that has Premium connector

Power Automate – Get Secrets

- Power Automate can get Azure Key Vault secrets
- You can choose between OAuth (Azure AD) or service principals
- You can do secure input and output to hide contents from run flow history



Azure Key Vault

- Create Azure Key Vault and setup secrets based on your need
- Choose Azure role-based access control type

Dashboard > powerautomatetest-champ

powerautomatetest-champ | Secrets ☆ ...

Key vault

Search << + Generate/Import Refresh Restore Backup View sample code Manage deleted secrets

Name	Type	Status
fin1		✓ Enabled
naris		✓ Enabled

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Access policies

Events

Objects

Keys

Secrets

Certificates

Settings

Dashboard > powerautomatetest-champ

powerautomatetest-champ | Access configuration ☆ ...

Key vault

Search << Refresh

Certificates

Settings

Access configuration

Networking

Microsoft Defender for Cloud

Properties

Locks

Monitoring

Alerts

Metrics

D diagnostic settings

Logs

Insights

Workbooks

Automation

Configure your options on access policy for this key vault

To access a key vault in data plane, all callers (users or applications) must have proper authentication operations the caller can execute. [Learn more](#)

Permission model

Grant data plane access by using a [Azure RBAC](#) or [Key Vault access policy](#)

☒ Azure role-based access control (recommended) ⓘ

☐ Vault access policy ⓘ

[Go to access control\(IAM\)](#)

Resource access

Choose among the following options to grant access to specific resource types

☐ Azure Virtual Machines for deployment ⓘ

☐ Azure Resource Manager for template deployment ⓘ

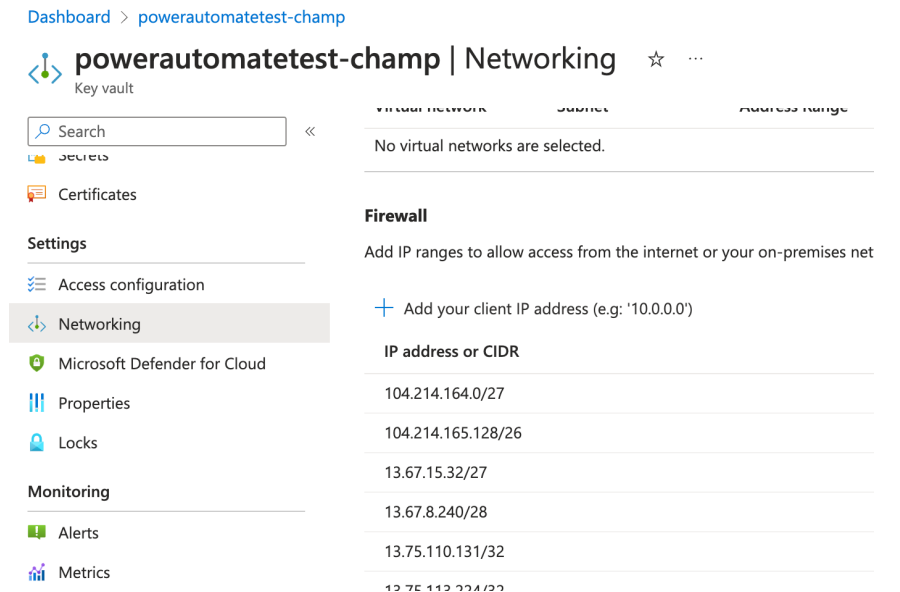
☐ Azure Disk Encryption for volume encryption ⓘ

Azure Service tags and their IPs

- Official download link <https://www.microsoft.com/en-us/download/details.aspx?id=56519> (may update every Monday)
- For get secrets action, the service tags depends on your Dataverse Environment region
- If Environment is in Asia, the services tag are AzureConnector.EastAsia and AzureConnector.SoutheastAsia (for other see <https://learn.microsoft.com/en-us/connectors/common/outbound-ip-addresses#power-platform>)
- These IPs need to add in Azure Key Vault's public access policy (IPv4 only)

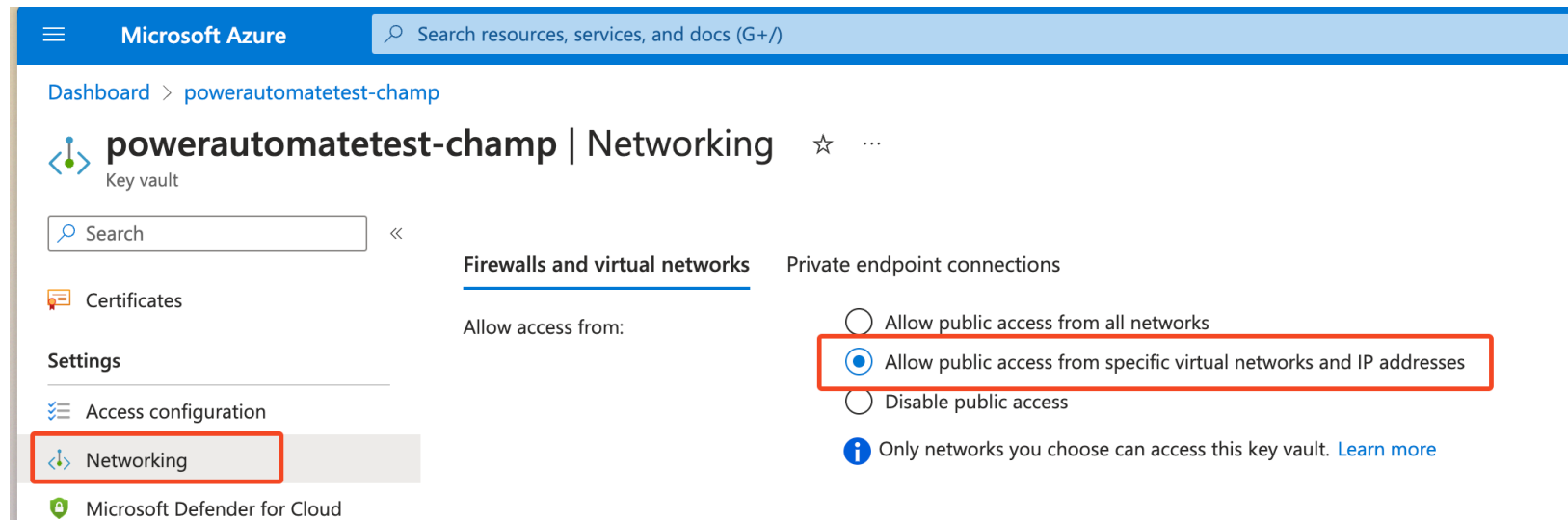
```
{
  "name": "AzureConnectors.EastAsia",
  "id": "AzureConnectors.EastAsia",
  "properties": {
    "changeNumber": 6,
    "region": "eastasia",
    "regionId": 1,
    "platform": "Azure",
    "systemService": "AzureConnectors",
    "addressPrefixes": [
      "13.75.36.64/28",
      "13.75.110.131/32",
      "13.75.113.224/32",
      "20.205.67.48/28",
      "20.205.67.64/27",
      "52.175.23.169/32",
      "104.214.164.0/27",
      "104.214.165.128/26",
      "2603:1040:207:402::180/122"
    ]
  }
},
```

```
{
  "name": "AzureConnectors.SoutheastAsia",
  "id": "AzureConnectors.SoutheastAsia",
  "properties": {
    "changeNumber": 7,
    "region": "southeastasia",
    "regionId": 2,
    "platform": "Azure",
    "systemService": "AzureConnectors",
    "addressPrefixes": [
      "13.67.8.240/28",
      "13.67.15.32/27",
      "20.195.82.240/28",
      "20.195.83.0/27",
      "20.198.148.72/32",
      "20.205.248.224/32",
      "52.187.68.19/32",
      "52.187.147.27/32",
      "2603:1040:5:402::180/122"
    ]
  }
},
```



Azure Key Vault

- After setup Azure Key Vault and Secrets, set the public access to only specific IPs



Create Azure Automation account

- Create Azure Automation Account
- Create PowerShell 5.1 runbook

[Dashboard](#) > [Create a resource](#) >

Marketplace

Get Started

Service Providers

AI-powered search

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

automation

☐ Azure services only

Showing 1 to 20 of 1575 results for 'au



Automation

Microsoft

Azure Service

Automate the management of your cloud and on-premises resources

Create



UpdateIPs | Runbooks

Automation Account

Search

+ Create a runbook

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Process Automation

Runbooks

Jobs

Try the new Azure Automation extension from [Visual Studio](#)

Search runbooks...

Showing 1 to 3 of 3 records

Name

AzureAutomationTut...

AzureAutomationTut...



Create a runbook

Name *

Runbook type *

Runtime version *

Description

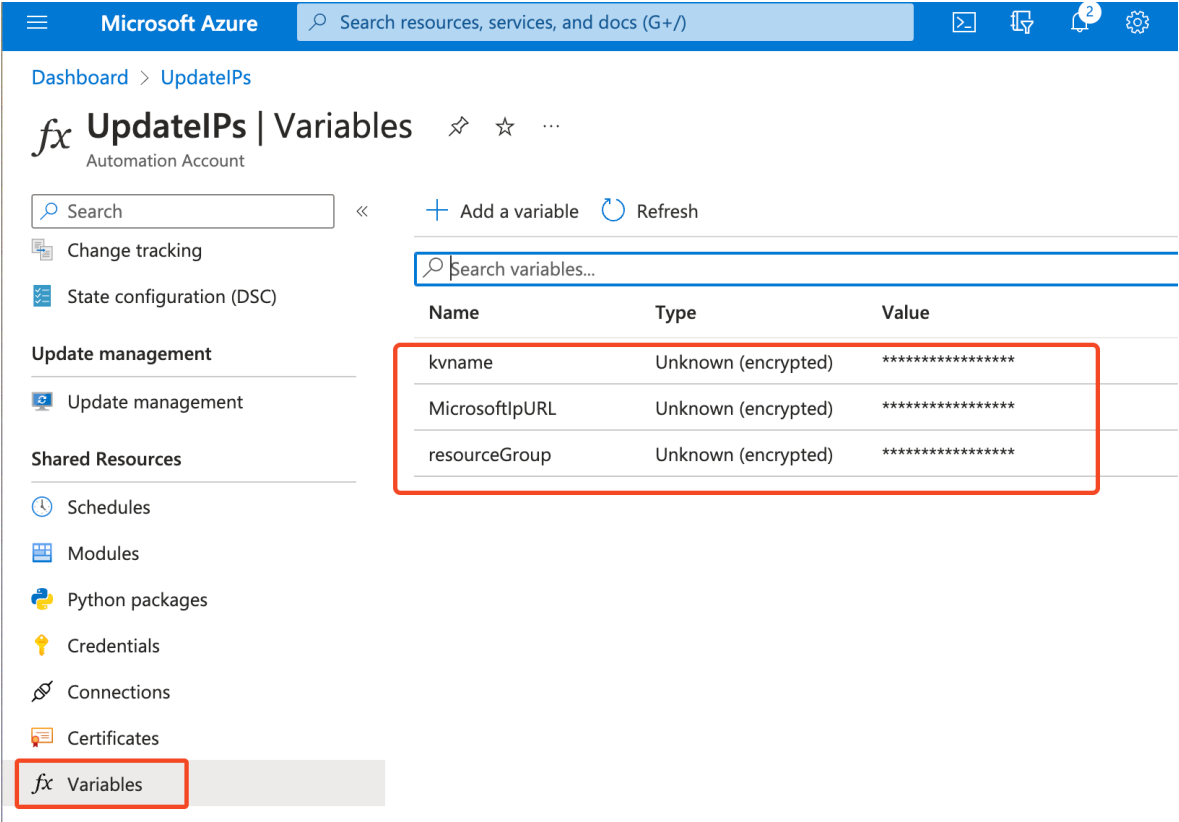
KV-updateIPs

PowerShell

5.1

Assign variables

- Create 3 variables name below



Name	Value
kvname	< < your key vault name > >
MicrosoftIpURL	https://download.microsoft.com/download/7/1/D/71D86715-5596-4529-9B13-DA13A5DE5B63/ServiceTags_Public_
resourceGroup	< < your resource group name > >

Enable Managed Identity

- System assigned managed identity type

Microsoft Azure

Search resources, services, and docs (G+ /)

Dashboard > UpdateIPs

UpdateIPs | Identity ☆ ...
Automation Account

Search

Properties

Networking

Keys

Pricing

Source control

Identity

Run as accounts (retired)

Settings

Locks

Monitoring

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied to the I...
You can grant permissions to the managed identity by using Azure role-based access co...
managed identity is authenticated with Microsoft Entra ID, so you don't have to store an

Save Discard Refresh Got feedback?

Status ⓘ

Off On

Object (principal) ID ⓘ

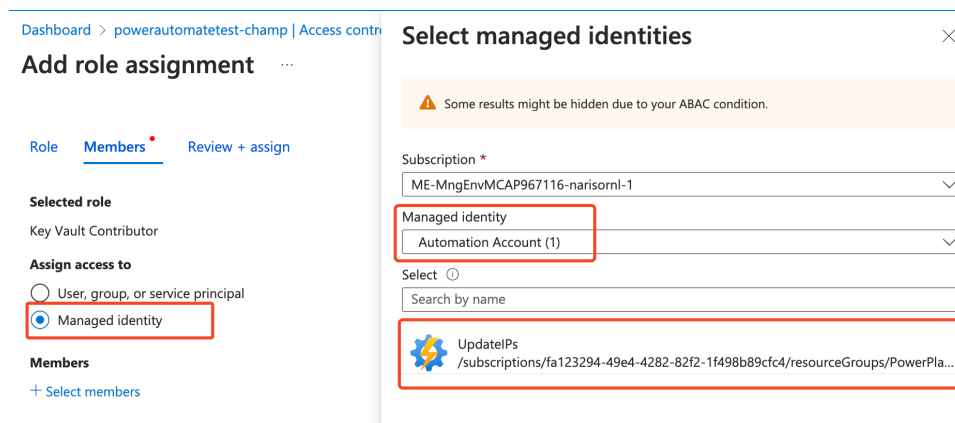
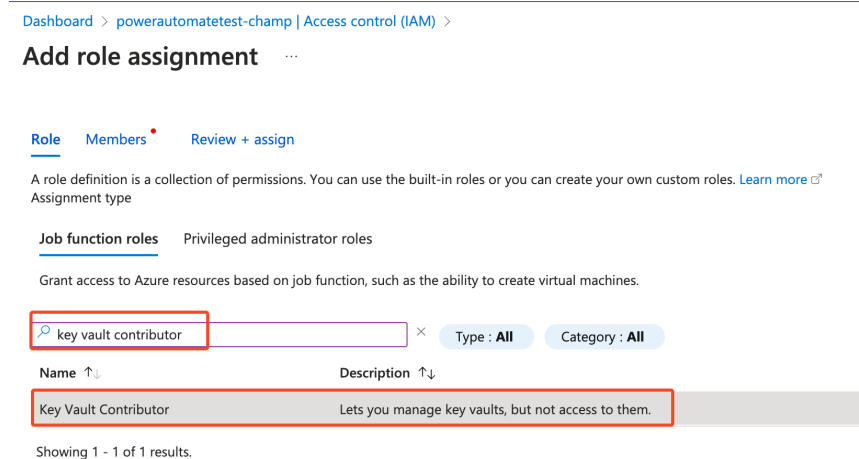
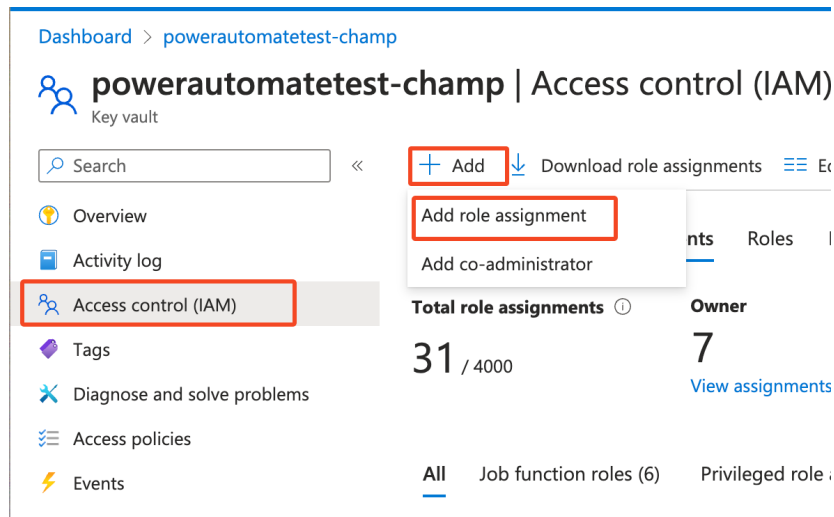
0a792e75-42ac-436a-a817-8c96d6868682

Permissions ⓘ

Azure role assignments

Azure Key Vault

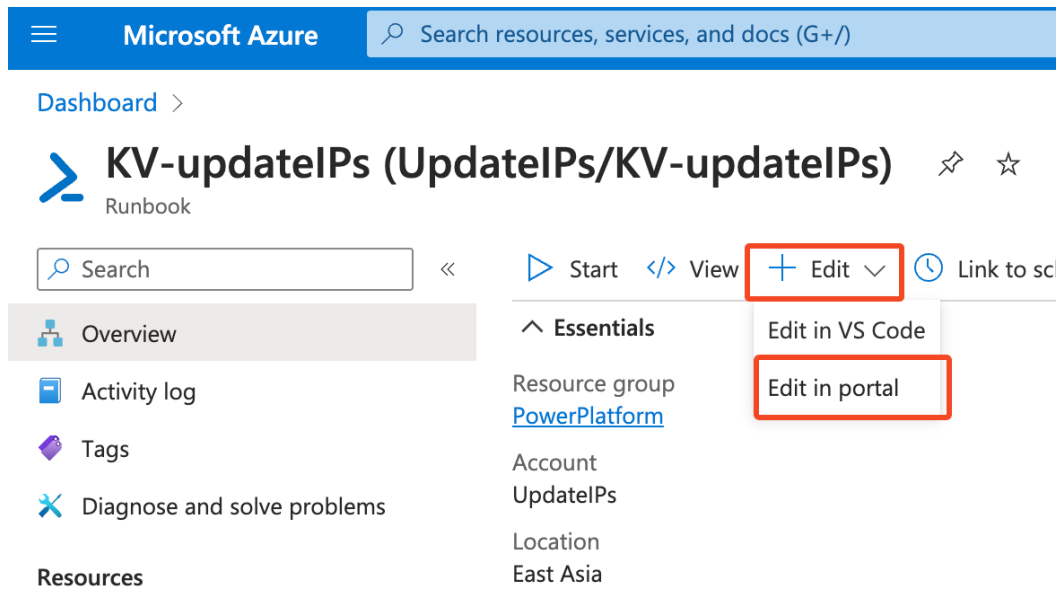
- Back to Key Vault and add access control to managed identity
- Give the role as “Key Vault Contributor”



Add runbook script

- Edit the runbook
- Then add the code from here

[https://github.com/narismadz/PowerAutomateKVIPs/blob/main/akv%20network%20ip%20allowed%20\(Azure%20Automation%20version\).ps1](https://github.com/narismadz/PowerAutomateKVIPs/blob/main/akv%20network%20ip%20allowed%20(Azure%20Automation%20version).ps1)



Microsoft Azure

Search resources, services, and docs (G+)

Dashboard >

KV-updatelPs (UpdateIPs/KV-updatelPs)

Runbook

Search

Start View Edit Link to sc

Overview

Activity log

Tags

Diagnose and solve problems

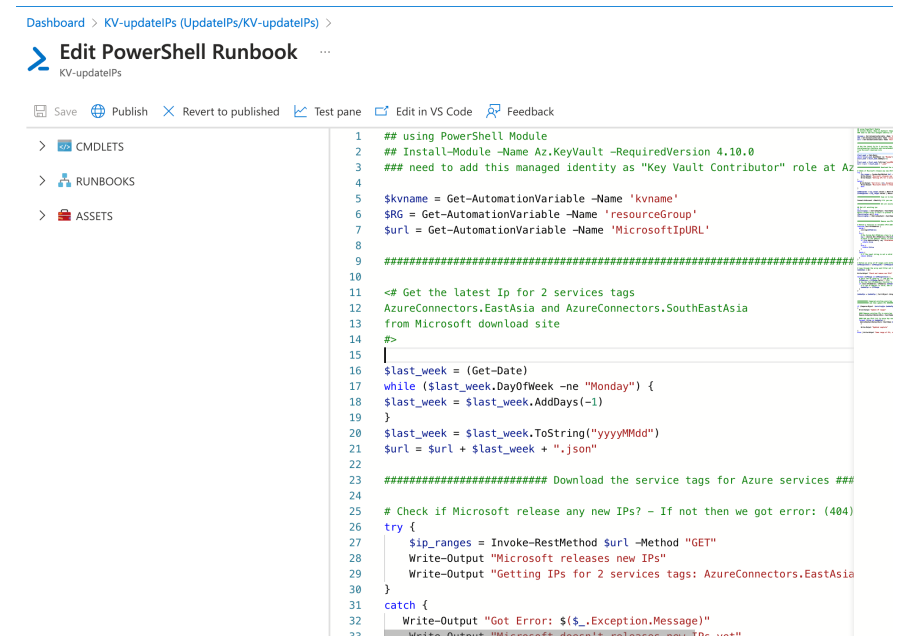
Resources

Essentials

Resource group
[PowerPlatform](#)

Account
UpdateIPs

Location
East Asia



Dashboard > KV-updatelPs (UpdateIPs/KV-updatelPs) >

Edit PowerShell Runbook

KV-updatelPs

Save Publish Revert to published Test pane Edit in VS Code Feedback

CMDLETS

RUNBOOKS

ASSETS

```
1 ## using PowerShell Module
2 ## Install-Module -Name Az.KeyVault -RequiredVersion 4.10.0
3 ## need to add this managed identity as "Key Vault Contributor" role at Az
4
5 $kvname = Get-AutomationVariable -Name 'kvname'
6 $SRG = Get-AutomationVariable -Name 'resourceGroup'
7 $url = Get-AutomationVariable -Name 'MicrosoftIpURL'
8
9 #####
10
11 <# Get the latest Ip for 2 services tags
12 AzureConnectors.EastAsia and AzureConnectors.SouthEastAsia
13 from Microsoft download site
14 #>
15
16 $last_week = (Get-Date)
17 while ($last_week.DayOfWeek -ne "Monday") {
18     $last_week = $last_week.AddDays(-1)
19 }
20 $last_week = $last_week.ToString("yyyyMMdd")
21 $url = $url + $last_week + ".json"
22
23 ##### Download the service tags for Azure services #####
24
25 # Check if Microsoft release any new IPs? - If not then we got error: (404)
26 try {
27     $ip_ranges = Invoke-RestMethod $url -Method "GET"
28     Write-Output "Microsoft releases new IPs"
29     Write-Output "Getting IPs for 2 services tags: AzureConnectors.EastAsia
30 }
31 catch {
32     Write-Output "Got Error: $($_.Exception.Message)"
33     Write-Output "Microsoft doesn't releases new IPs yet"
```

Add runbook script

- This example assumes your dataverse environment is in Asia
- If you are on the different dataverse, need to modified or add more variables to the code
- You can add more line like AzureConnectors.JapanEast based on your region
<https://learn.microsoft.com/en-us/connectors/common/outbound-ip-addresses#power-platform>

Edit/Add this line base on your region

And this line (sum all variables)

```
##### Download the service tags for Azure services #####

# Check if Microsoft release any new IPs? - If not then we got error: (404) Not Found
try {
    $ip_ranges = Invoke-RestMethod $url -Method "GET"
    Write-Output "Microsoft releases new IPs"
    Write-Output "Getting IPs for 2 services tags: AzureConnectors.EastAsia and AzureConnectors.SouthEastAsia"
}
catch {
    Write-Output "Got Error: $($_.Exception.Message)"
    Write-Output "Microsoft doesn't releases new IPs yet"
    exit
}

$IPRangesEa = $ip_ranges.values | Where-Object {$_.name -eq "AzureConnectors.EastAsia"} | Select-Object -ExpandProperty properties
$IPRangesSea = $ip_ranges.values | Where-Object {$_.name -eq "AzureConnectors.SouthEastAsia"} | Select-Object -ExpandProperty properties
```

```
73     # If the input string is not a valid IP address, return $false
74     return $false
75 }
76 }
77
78 # Define an array of IP ranges with different formats
79 $IPRangesCheck = $IPRangesEa + $IPRangesSea
80
```

Add runbook script

- You can test by running script in test pane

Dashboard > KV-updatelPs (UpdatelPs/KV-updatelPs) >

Edit PowerShell Runbook

KV-updatelPs

Save Publish Revert to published **Test pane**

> CMDLETS	1 ##
> RUNBOOKS	2 ##
	3 ##
	4
	5 \$k
	6 \$R
> ASSETS	7 \$u

Dashboard > KV-updatelPs (UpdatelPs/KV-updatelPs) > Edit PowerShell Runbook >

Test

KV-updatelPs

Start Stop Suspend Resume View last test Refresh job streams

Parameters

No input parameters

Run Settings

Run on Azure ⓘ

Using a hybrid runbook worker can increase test performance. [Learn more](#)

Activity-level tracing

This configuration is available only for graphical runbooks.

Trace level

None Basic Detailed

Queued..
Streams will display when the test completes.

Add schedules

- You can add runbook schedule here
- If you already configured since Automation account level then you can link to this runbook also
- Microsoft update IPs on Monday depends on your timezone

Dashboard > KV-updatelPs (UpdatelPs/KV-updatelPs)



KV-updatelPs (UpdatelPs/KV-updatelPs) | Schedules

Runbook

Search

+ Add a schedule

Refresh



Overview



Activity log



Tags



Diagnose and solve problems

Resources



Jobs



Schedules



Webhooks

Name

Next run

No schedules found.

Dashboard > UpdatelPs | Runbooks > KV-updatelPs (UpdatelPs/KV-updatelPs)



Schedule Runbook

KV-updatelPs

Schedule

Link a schedule to your runbook

Parameters and run settings

Modify run settings (Default: Azure)

Microsoft Azure Search resources, services, and docs (G+)

... > UpdatelPs | Runbooks > KV-updatelPs (UpdatelPs/KV-updatelPs) | Schedules

Schedules

UpdatelPs/KV-updatelPs

+ Add a schedule

Name	Next run
No schedules found.	

New Schedule

Name *

EveryMon

Description

Starts *

10/28/2023 4:52 PM

Time zone

Thailand - Indochina Time

Recurrence

Once Recurring

Recur every *

1 Week

On these days *

☒ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

☐ Sunday

Create

Monitor runbook's job

- You can see history log and output

Dashboard >

KV-updatelPs (UpdateIPs/KV-updatelPs)

Runbook

Search

Start View Edit Link to schedule Add webhook Delete Export Feedback

Overview

Activity log

Tags

Diagnose and solve problems

Resources

Jobs

Schedules

Webhooks

Runbook settings

Properties

Description

Logging and tracing

Settings

Locks

Automation

Tasks (preview)

Essentials

Resource group: [PowerPlatform](#)

Account: UpdateIPs

Location: East Asia

Subscription: [ME-MngEnvMCAP967116-narisornl-1](#)

Subscription ID: fa123294-49e4-4282-82f2-1f498b89cfc4

Status: In edit

Runbook type: PowerShell

Runtime version: 5.1

Last modified: 10/28/2023, 3:57 PM

Tags (edit) Add tags

Recent Jobs

Status	Created	Last updated
✓ Completed	10/24/2023, 6:05:55 PM	10/24/2023, 6:06:51 PM
✓ Completed	10/24/2023, 5:06:38 PM	10/24/2023, 5:07:25 PM
✓ Completed	10/24/2023, 5:02:02 PM	10/24/2023, 5:02:56 PM
✓ Completed	10/24/2023, 4:58:02 PM	10/24/2023, 4:59:08 PM

Microsoft Azure

Search resources, services, and docs (G+)

admin@teamsfor...

Dashboard > KV-updatelPs (UpdateIPs/KV-updatelPs) >

KV-updatelPs 10/24/2023, 5:06 PM

Job

Resume Stop Suspend Refresh

Essentials

Id: 09bc6e3d-35d7-4dfe-8e34-75c8ff0f9b5f

Created: 10/24/2023, 5:06:38 PM

Status: Completed

Last Update: 10/24/2023, 5:07:25 PM

Ran on: Azure

Runbook: [KV-updatelPs](#)

Ran As: User

Source snapshot: [View source snapshot](#)

Input Output Errors Warnings All Logs Exception

```
Microsoft releases new IPs

Getting IPs for 2 services tags: AzureConnectors.EastAsia and AzureConnectors.SouthEastAsia

Environments
-----
{[AzureChinaCloud, AzureChinaCloud], [AzureCloud, AzureCloud], [AzureGermanCloud, AzureGermanCloud], [AzureUSGovernme...

Check and remove non IPv4


Update IP ranges

PublicNetworkAccess      : Enabled
VaultUri                  : https://powerautomatetest-champ.vault.azure.net/
TenantId                  : c73d22fa-fef7-4582-8384-f99bd384fb72
TenantName                : c73d22fa-fef7-4582-8384-f99bd384fb72
Sku                       : Standard
EnabledForDeployment       : False
EnabledForTemplateDeployment : False
EnabledForDiskEncryption  : False
```

Results

- The script will check Microsoft's new IPs for these services tag based on yyyyMMdd of the link
- If nothing new, end the flow
- If there's a new IP list, compared to the current settings on the key vault. If they are different then update or end the flow

Dashboard > powerautomatetest-champ

 **powerautomatetest-champ** | Networking ☆ ...

Key vault

Search <<

Secrets

Certificates

Settings

Access configuration

Networking

Microsoft Defender for Cloud

Properties

Locks

Monitoring

Alerts






Metrics

No virtual networks are selected.

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#)

+ Add your client IP address (e.g: '10.0.0.0')

IP address or CIDR	
104.214.164.0/27	
104.214.165.128/26	
13.67.15.32/27	
13.67.8.240/28	
13.75.110.131/32	
13.75.113.224/32	