



Assessment Setup Guide



Introduction

Setting up and configuring On-Demand assessments is a complex process. There are several steps to complete in a specific order to ensure successful assessment setup and execution. This article aims to provide the details required that are applicable across all the On-Demand assessments available on Services Hub.

This article is organized in four major sections which should be followed in order to ensure successful configuration and execution of On-Demand assessments.

Getting Started with On-Demand Assessments

Setting up a data collector machine

Configure Microsoft On-Demand Assessments

Working with assessment results

There are also configuration details applicable to each individual assessment that are referred to in the *Configure Microsoft On-Demand Assessment(s)* section of this article with links to the relevant content.

Ensure that you have reviewed the information in the assessment(s) prerequisites and configuration documentation before continuing the setup in this document. Download the prerequisites for your assessment(s) at [On-Demand Assessments Prerequisites](#) if not already downloaded.

For general information about On-Demand assessments, see the [On-Demand Assessment FAQs](#)

! Important – Migration: Documentation on how to migrate MMA based Assessments to AMA can be found by accessing the following article: [On-Demand Assessments - Migration](#)

This document was last updated on May 30th, 2023. To ensure you have the latest version of this document, check here:
[Assessment Setup Guide](#)

Table of Contents

Introduction	1
Table of Contents	2
Getting Started with On-Demand Assessments	3
Sign up for On-Demand Assessment Initial Setup and Configuration Service	3
Azure Subscription	4
Services Hub Registration.....	5
Linking of the Azure Subscription and Log Analytics workspace	6
Configuration Methods	9
Networking.....	16
Azure VM as data collector machine	17
Offline – Disconnected Environment	18
Add the Assessments in Services Hub.....	21
Providing Access to Azure Log Analytics workspace	23
Configure Microsoft On-Demand Assessment(s)	23
Configuring the required Group Policy Objects	23
Creation of the Assessment Scheduled Task.....	25
Download On-Demand Assessment Prerequisites.....	28
Working with Assessment Results.....	29
Validate Successful Assessment	29
Services Hub Assessment Page	32
Downloading the reports from Services Hub.....	32
Remediation Plan creation in Service Hub	33

Getting Started with On-Demand Assessments

Assessments are available through the Services Hub to help you assess and optimize the availability, security, and performance of your on-premises, hybrid, and cloud Microsoft technology environments. These assessments use Microsoft Azure Log Analytics tables, Azure Workbooks and Azure ARC/Azure VM extensions, which are designed to give you simplified IT and security management across your environment.

Note: *On average, it takes two hours to initially configure your environment to run an On-Demand Assessment. After you run an assessment you can review the recommendations in Azure Workbooks. This will provide you with a prioritized list of recommendations, categorized across six focus areas. This allows you and your team to quickly understand risk levels, the health of your environments, act to decrease risk, and improve your overall IT health.*

Use the following checklist to ensure all steps in this section are completed before moving onto the next section.

- Azure Subscription
- Services Hub Registration
- Link Azure Subscription and Log Analytics Workspace to Services Hub
- Choose your method of configuration (Azure ARC enrollment or Azure VM Extension)
- Add the assessment(s) in your Services Hub workspace
- Provide access to Azure Log Analytics workspace (Required for CSA Delivery only)
- Download your Assessment specific Prerequisite Documentation

Sign up for On-Demand Assessment Initial Setup and Configuration Service

An initial setup and configuration service with a Microsoft engineer is available to simplify the assessment setup process as part of the Microsoft Unified Support base contract offering. We help you link, enable, install, and configure a Services Hub On-Demand Assessment. To learn more, see our [Data Sheet](#). You can get started by clicking 'Sign up' on the top right tile of your Services Hub dashboard under 'Setup & Configuration'. This sends an email to your Microsoft representative to request scheduling of this service.

Whether using the On-Demand Assessment – Setup and Config Service or not, all the steps in this article and the assessment(s) prerequisites documents needs to be completed to ensure successful setup and execution of OnDemand assessments. Complete the steps in this guide, then select an On-Demand Assessment from the table of contents on the left, under Getting Started with On-Demand Assessments, to see details, configuration instructions, and links to download data sheets and detailed prerequisites for selected On-Demand Assessments.

Azure Subscription

On-Demand Assessments ingest their recommendations and supporting details into Azure Log Analytics. The Azure

Log Analytics service requires an Azure subscription owned by the organization. If there is already an Azure subscription, then a customer representative (their registered email address) with the [required](#) Azure Log Analytics access and/or Azure Subscription access will need to be invited to the Services Hub workspace by the CSAM.

If there is no Azure subscription, Microsoft will sponsor one for the customer. The ideal owner for the sponsored subscription is the main point of contact IT professional that will be working with the assessment results. There are a couple of options to have a sponsored Azure subscription provisioned.

The preferred option is to share an organizational email address to be provisioned as owner of a no-cost Azure sponsorship with the organization's CSAM. Once the Azure sponsorship is created, an email with an invitation to activate the subscription will be sent to the provided organizational email address. Activate the Azure subscription through the link provided in the email. This account will be invited to the Services Hub workspace by the CSAM.

An alternative option is to request for one directly by creating a support ticket by [contacting Services Hub Support](#) and providing an organizational email address to be provisioned as owner of a no-cost Azure sponsorship.

Note: Customers can choose to use any Azure Subscription for this purpose as long as the user has the [required](#) Azure Subscription and/or Log Analytics role to perform the required actions. The Azure Subscription can be an EA or PayAsYou-Go or trial azure subscriptions. Azure subscriptions created merely due to presence of Office 365 licenses cannot be used as they don't have active azure credits.

Tip: No-cost sponsored Azure subscriptions by default have a validity of 1 year. These subscriptions can be extended before expiry if needed in case of renewals. You can read more about how to manage these subscriptions in this [Azure Rollover](#) article.

Services Hub Registration

The customer with the required access must be registered with the Services hub. Additionally, if the assessment will include a CSA lead delivery, then the CSA must also be registered with the Services Hub.

CSAM tasks:

1. The CSAM invites customer and CSA (for engineer lead assessment deliveries). Log in to Services Hub using Microsoft Edge and go to **Management > Manage Users**.
2. Add customer's email addresses and CSA with alias@Microsoft.com and ensure the **Health** and **Programs** options are selected to allow the user to see the assessment tab and create a remediation plan.

The screenshot shows the 'Add users' dialog in the Services Hub interface. At the top, there are tabs for 'Users' and 'AAD group access'. Below the tabs, there is a search bar and a '+ Add users' button. The main content area is titled 'Add users' and contains the following sections:

- Single invite:** A text input field with the placeholder 'Enter a valid email address'.
- Language:** A dropdown menu currently set to 'English (United States)'. To its right is a 'Bulk invite' section with a '(Download CSV template)' link and an 'Upload CSV file' button.
- Base support contact:** A toggle switch that is currently turned off.
- Member permissions:** A list of checkboxes for various permissions:
 - Manage users
 - View all support cases
 - Learning Manager
 - Learning
 - Programs
 - Invite users
 - Health
 - Shared files

At the bottom of the dialog, there are 'Cancel' and 'Add users' buttons.

Customer and CSA registration tasks:

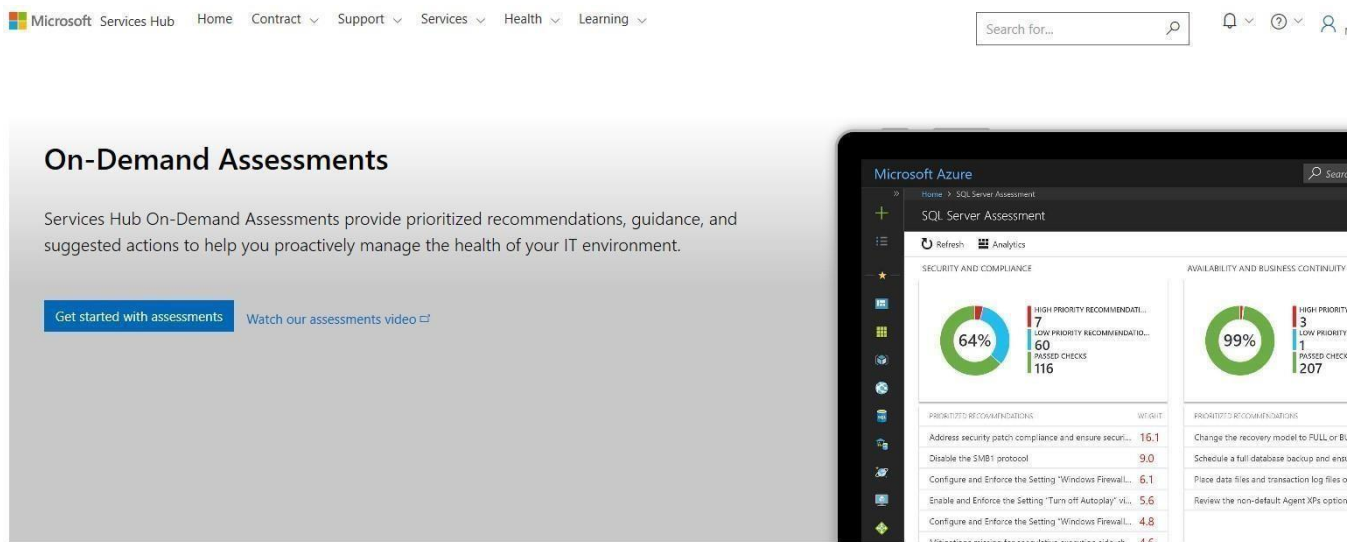
1. Review your email inbox for an email from your CSAM inviting you to register on Services Hub
2. Click the link in the email whose URL begins with <https://serviceshub.microsoft.com/account/register?registrationId=<uniqueID>>

Linking of the Azure Subscription and Log Analytics workspace to Services Hub workspace

1. Log into Services hub with user credentials with the required access. Go to IT Health -> On-Demand Assessments.



2. Click on **Get started with assessments**



On-Demand Assessments

Services Hub On-Demand Assessments provide prioritized recommendations, guidance, and suggested actions to help you proactively manage the health of your IT environment.

[Get started with assessments](#) [Watch our assessments video](#)

Microsoft Azure SQL Server Assessment

Refresh Analytics

SECURITY AND COMPLIANCE

64%

HIGH PRIORITY RECOMMENDATIONS: 7
LOW PRIORITY RECOMMENDATIONS: 60
PASSED CHECKS: 116

AVAILABILITY AND BUSINESS CONTINUITY

99%

HIGH PRIORITY RECOMMENDATIONS: 3
LOW PRIORITY RECOMMENDATIONS: 1
PASSED CHECKS: 207

PRIORITY RECOMMENDATIONS	WEIGHT
Address security patch compliance and ensure secur...	16.1
Disable the SMB 1 protocol	9.0
Configure and Enforce the Setting "Windows Firewall...	6.1
Enable and Enforce the Setting "Turn off Autoplay" vi...	5.6
Configure and Enforce the Setting "Windows Firewall...	4.8
Minimize retention for diagnostic examination data...	4.6

PRIORITY RECOMMENDATIONS
Change the recovery model to FULL or B...
Schedule a full database backup and ens...
Place data files and transaction log files o...
Review the non-default Agent XPs option

Available On-Demand Assessments

-  Active Directory
-  Active Directory Operational Survey
-  Active Directory Security
-  Active Directory Security Survey
-  Azure Active Directory Operational Survey
-  Dynamics 365 Customer Engagement Survey

[Show all assessments](#)

3. Select the desired Azure subscription from the list and choose next.

Enable assessments

Log Analytics is powered by Azure

Link your Azure subscription and Log Analytics workspace to enable assessments

Step 1 of 3: Choose your Azure Subscription

Azure Subscription - My Azure role

Services Hub Demo Open - Other (Microsoft)

To use demo assessments:

Step 1: Join Demo Users Group (this can take 24hrs to resolve).
Step 2: Click on "Use Demo Assessments" button to link.

[Use Demo Assessments >](#)

[Next >](#)

Organizations that have an Azure subscription but lack the required permissions will see:

Enable assessments

Log Analytics is powered by Azure

Link your Azure subscription and Log Analytics workspace to enable assessments

Choose or create an Azure subscription

You are not the owner of your company's Azure subscription and do not have permission to enable your assessments. Please work with your company's Services Admin, TAM or Support Account Coordinator to have the Azure subscription owner enable your assessments.

To use demo assessments:

Step 1: Join Demo Users Group (this can take 24hrs to resolve).
Step 2: Click on "Use Demo Assessments" button to link.

[Use Demo Assessments >](#) [Create a new Azure subscription](#)

Please work with your company's Services Admin, CSAM, or Support Account Coordinator to have the customer representative with the required permissions within Azure register on Services Hub and pre-configure your assessments. Organizations without an Azure subscription refer to [Azure Subscription](#) to get your Microsoft sponsored subscription.

4. Choose the Azure Log Analytics workspace that the assessment(s) you choose will be enabled in. Or use the Create New to create a dedicated workspace for the assessment(s) if desired. Then click next.

Enable assessments

Log Analytics is powered by Azure

Link your Azure subscription and Log Analytics workspace to enable assessments

Step 2 of 3: Choose your Log Analytics workspace

Azure Log Analytics Workspace Name

ServicesHubDemoOpen

[< Back](#) [Next >](#)

5. At the conclusion of the linking process, click "View assessments".

Enable assessments

Log Analytics is powered by Azure

Link your Azure subscription and Log Analytics workspace to enable assessments

Step 3 of 3: Assessment enablement complete

Configure your assessments

Congratulations! You have successfully enabled assessments in your Azure Log Analytics workspace. Now let's get started on configuring your assessments.

[View assessments](#)

Configuration Methods

There are **3 scenarios** available to configure the assessment. Determine which scenario fits best for your organization.

- Azure ARC enrollment
- Azure VM Extension
- Disconnected Environments

Minimum requirements for a successful configuration: Local Administrator on the data collection machine and Azure Contributor role at subscription level

Azure Arc enrollment for on-prem machines

On-premise machines can be easily enrolled to Azure Arc via Azure Portal by following the steps below:

1. Go to the [Azure Portal](#) and look for Azure Arc, under **Getting Started**, go to **Add your infrastructure for free** and click on the **Add button**

Dashboard >

Azure Arc
Microsoft

Search

Get started Infrastructure Services Learn more

Overview

All Azure Arc resources

Management

- Custom locations
- Data controllers
- Resource bridges (preview)
- Service principals
- Private link scopes

Infrastructure

- Azure Arc virtual machines (preview)
- Azure Stack HCI
- Kubernetes clusters
- Servers
- SQL Servers
- VMware vCenters (preview)
- SCVMM management servers

See and manage all your on-prem infrastructure, anywhere. It's free to get started.

With Azure Arc, you can manage your infrastructure in all your environments, including on-premises, other public clouds, and edge devices. There's no charge to start, just add your infrastructure and enjoy the views. [Learn more](#)

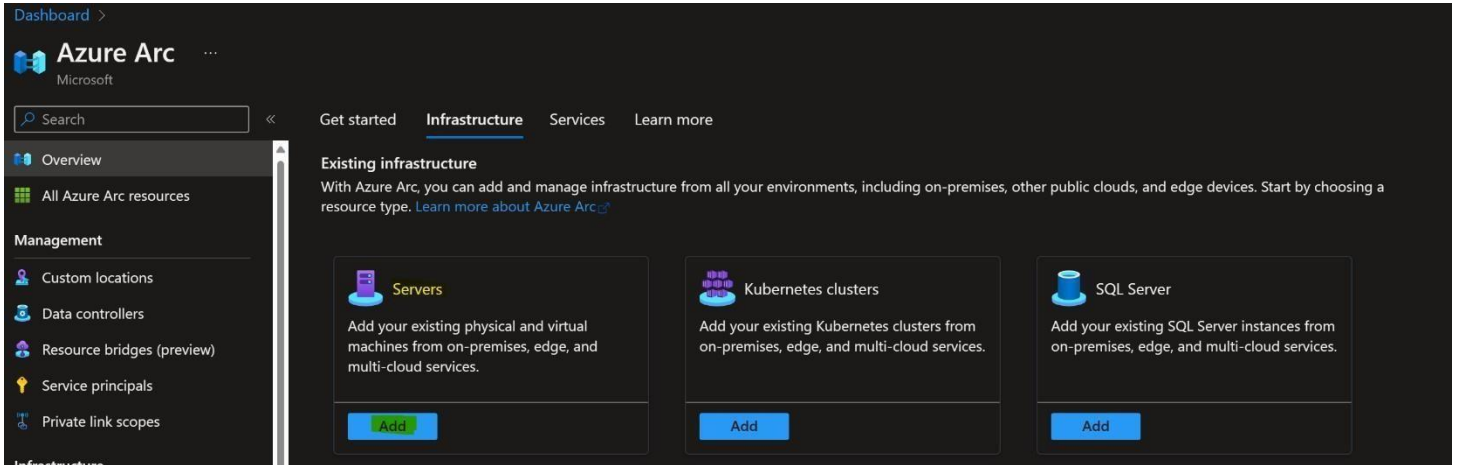
Get hands-on with ArcBox (preview)
Use ArcBox to deploy an Azure Arc sandbox in less than an hour. [Learn more](#)

Add your infrastructure for free
See all your infrastructure in Azure. There's no charge to add and view your existing resources. [Learn more](#)

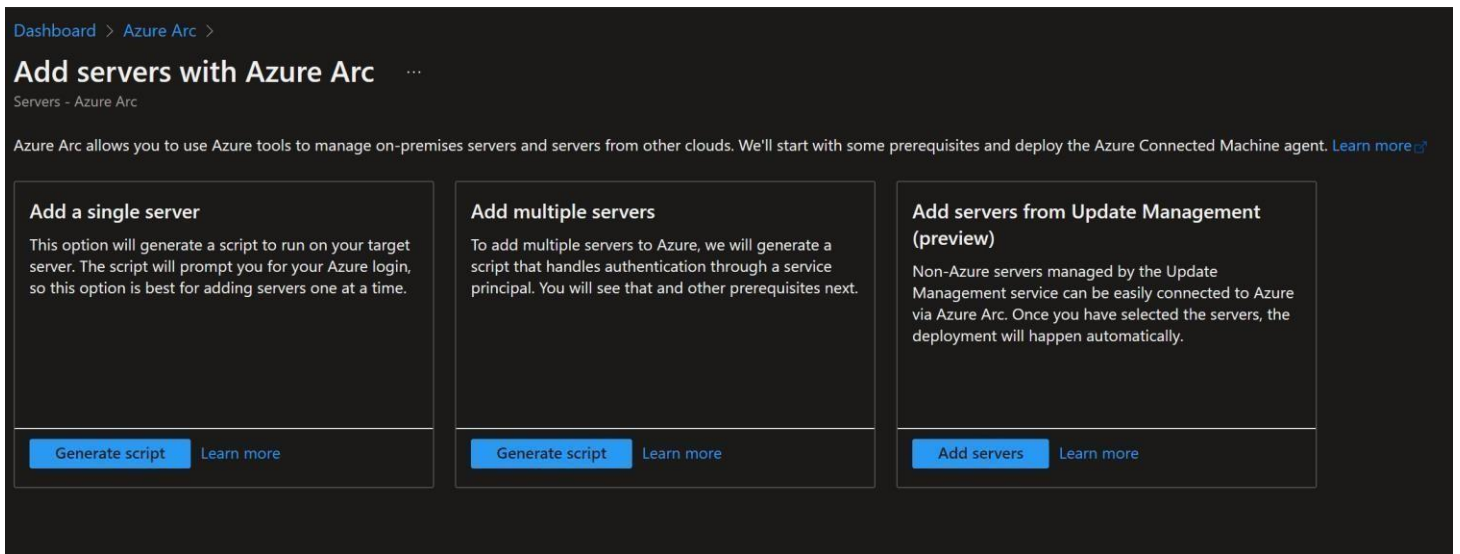
Deploy Azure services
Use Azure Arc to deploy Azure services on your infrastructure. [Learn more](#)

Try ArcBox Add Deploy

2. Go to Servers and click the Add button



3. You can choose between Add a single server or Add multiple servers and click on the **Generate script** matching your selection



- Review the prerequisites for adding a machine and click on **Next**, this will take you to the Resource Details screen where you are required to select the subscription you are planning to use for Azure along with the Resource Group Region, Machine OS and the connectivity method

Dashboard > Azure Arc > Add servers with Azure Arc >

Add a server with Azure Arc

1 Prerequisites 2 Resource details 3 Tags 4 Download and run script

Complete the fields below to connect servers on-premise and in other clouds to be managed and governed in Azure. [Learn more](#)

Project details

Select the subscription and resource group where you want the server to be managed within Azure.

Subscription * ⓘ ASD-PSE

Resource group * ⓘ DeployTest

[Create new](#)

Server details

Select details for the servers that you want to add. An agent package will be generated for the selected server type.

Region * ⓘ (US) West US

Operating system * ⓘ Windows

Connectivity method

Choose how the connected machine agent running in the server should connect to the Internet. This setting only applies to the Arc agent. Proxy settings for extensions are configured separately.

Connectivity method *

- Public endpoint
- Proxy server
- Private endpoint

[Previous](#) [Next](#)

- Final step requires downloading the PowerShell script that was generated based of your selection to the intended collector machine (close the window and go to the on-prem machine)

Note: Before running the script, make sure to set your execution policy to remove signed (set-executionpolicy remotesigned)

[Home](#) > [Azure Arc | Servers](#) > [Add servers with Azure Arc](#) >

Add a server with Azure Arc

- ✓ Prerequisites
- ✓ Resource details
- ✓ Tags
- 4** Download and run script

1. Download or copy the following script

```
1 try {
2     $env:SUBSCRIPTION_ID = " ";
3     $env:RESOURCE_GROUP = "AMATEST2";
4     $env:TENANT_ID = " ";
5     $env:LOCATION = "westeurope";
6     $env:AUTH_TYPE = "token";
7     $env:CORRELATION_ID = " ";
8     $env:CLOUD = "AzureCloud";
9
10
11     [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor 3072;
12
13     # Download the installation package
14     Invoke-WebRequest -UseBasicParsing -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile
"$env:TEMP\install_windows_azcmagent.ps1";
15
16     # Install the hybrid agent
17     & "$env:TEMP\install_windows_azcmagent.ps1";
18     if ($LASTEXITCODE -ne 0) { exit 1; }
19
20     # Run connect command
21     & "$env:ProgramW6432\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group
"$env:RESOURCE_GROUP" --tenant-id "$env:TENANT_ID" --location "$env:LOCATION" --subscription-id
"$env:SUBSCRIPTION_ID" --cloud "$env:CLOUD" --correlation-id "$env:CORRELATION_ID";
22 }
23 catch {
24     $logBody = @{subscriptionId="$env:SUBSCRIPTION_ID";resourceGroup="$env:RESOURCE_GROUP";
tenantId="$env:TENANT_ID";location="$env:LOCATION";correlationId="$env:CORRELATION_ID";
authType="$env:AUTH_TYPE";operation="onboarding";messageType=$_.FullyQualifiedErrorId;message="$_";};
25     Invoke-WebRequest -UseBasicParsing -Uri "https://gbl.his.arc.azure.com/log" -Method "PUT" -Body
($logBody | ConvertTo-Json) | out-null;
```

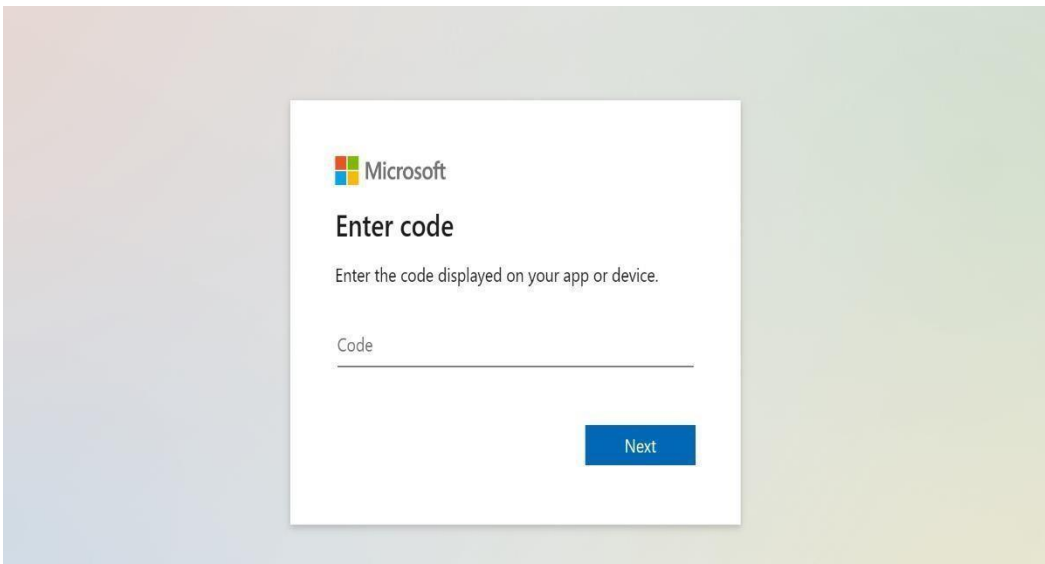
Download



6. Run the downloaded script in PowerShell ISE on the machine, this will trigger a device log in session to complete the enrollment (enter the code provided by the script to complete the process

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X
1 try {
2     $env:SUBSCRIPTION_ID = "Your Azure Subscription ID";
3     $env:RESOURCE_GROUP = "AMATEST2";
4     $env:TENANT_ID = "Your Azure Tenant ID";
5     $env:LOCATION = "westeurope";
6     $env:AUTH_TYPE = "token";
7     $env:CORRELATION_ID = "";
8     $env:CLOUD = "AzureCloud";
9
10
11 [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor 3072;
12 Invoke-WebRequest -useBasicParsing -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile "$env:TEMP\install_windows_azcmagent.ps1";
13 & "$env:TEMP\install_windows_azcmagent.ps1";
14 if ($LASTEXITCODE -ne 0) { exit 1; }
15 & "$env:ProgramW6432\AzureconnectedMachineAgent\azcmagent.exe" connect --resource-group "$env:RESOURCE_GROUP" --tenant-id "$env:TENANT_ID" --location "$env:LOCATION" --subscription-id "$env:SUBSCRIPTION_ID" --
16
17 } catch {
18     $logBody = @{"subscriptionId"="$env:SUBSCRIPTION_ID";resourceGroup="$env:RESOURCE_GROUP";tenantId="$env:TENANT_ID";location="$env:LOCATION";correlationId="$env:CORRELATION_ID";authType="$env:AUTH_TYPE";operation
19     Invoke-WebRequest -useBasicParsing -Uri "https://gbl.his.arc.azure.com/log" -Method "PUT" -Body ($logBody | ConvertTo-Json) | out-null;
20     Write-Host -ForegroundColor red $_.Exception;
21 }
22 }
```

PS C:\windows\system32>

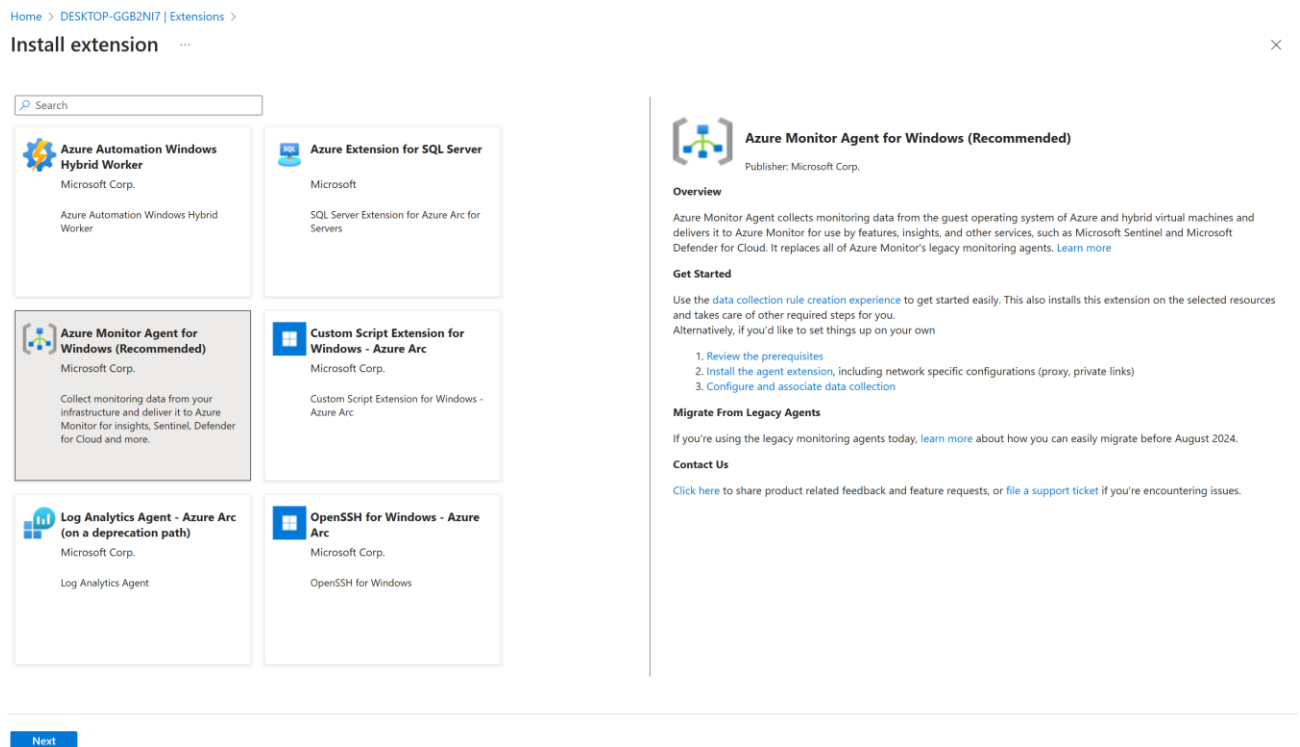


7. Once sign in is complete a confirmation message will be displayed



8. Install Azure Monitoring Agent for Windows

Servers – Azure Arc → Select your server –> Go to **Extensions** and click on **Add**. Search for Azure Monitoring Agent for Windows:



Select **Next** → **Review + Create** → **Create**. After deployment has been completed, the Agent will show up in the list of installed extensions:

Extensions ☆ ...

+ Add Refresh | ↑ Update ✓ Enable automatic upgrade ⏸ Disable automatic upgrade 🗑 Uninstall

i The Log Analytics agents (OMS/MMA) will reach end of support by August 2024. Azure Monitor agent is the recommended replacement. Learn more about migrating to Azure Monitor →

Search to filter items...					
Name	Type	Version	Update available	Status	Automatic upgrade
<input type="checkbox"/> AzureMonitorWindowsAgent	AzureMonitorWindowsAgent	1.15.0.0	No	Succeeded	Enabled

Additional details on the process can be found by accessing the video link below:

[Add Server to Azure Arc | Microsoft Learn](#)

! Note: Currently the recommendation is to ensure all extensions are uninstalled before disconnecting a machine. If an extension request is stuck with deleting or creating status, please reach out to us and we will investigate. From the Azure Arc Server panel -> Select your Machine -> Scroll down to **New Support Request:**

1. Problem description 2. Recommended solution 3. Additional details 4. Review + create

Tell us your issue, and we'll help you resolve it.

Provide information about your billing, subscription, quota management, or technical issue (including requests for technical advice).

Issue type *	<input type="text" value="Technical"/>
Subscription *	<input type="text" value="Your Azure Subscription will be automatically detected"/>
	Can't find your subscription? Show more ⓘ
Service	<input checked="" type="radio"/> My services <input type="radio"/> All services
Service type *	<input type="text" value="Azure Arc enabled servers"/>
Resource *	<input type="text" value="AMATest"/>
Summary *	<input type="text" value="Extensions"/>
Problem type *	<input type="text" value="Extensions"/>
Problem subtype *	<input type="text" value="Extension installation or removal failed"/>

Networking

During installation and runtime, the agent requires connectivity to Azure Arc service endpoints. If outbound connectivity is blocked by the firewall, make sure that the following URLs are not blocked:

Domain Environment	Required Azure Service Endpoints
management.azure.com	Azure Resource Manager
login.windows.net	Azure Active Directory
dc.services.visualstudio.com	Application Insights
agentserviceapi.azure-automation.net	Guest Configuration
*-agentservice-prod-1.azure-automation.net	Guest Configuration
*.his.hybridcompute.azure-automation.net	Hybrid Identity Service

Additional troubleshooting resources can be found here:

[Troubleshoot Azure Arc-enabled servers agent connection issues - Azure Arc | Microsoft Learn](#)

[Connected Machine agent network requirements - Azure Arc | Microsoft Learn](#)

[Use Azure Monitor Troubleshooter - Azure Monitor | Microsoft Learn](#)

Azure VM as data collector machine

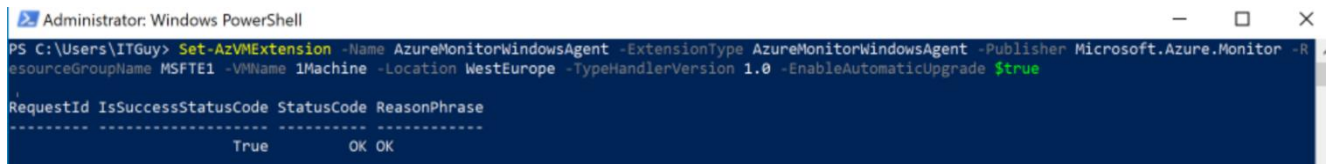
If you are planning to use an Azure VM as a data collector machines for on demand assessments, there is no requirement for the VM to be associated with Azure ARC as the assessment can be activated as a simple extension.

The following article describes how to create a Windows virtual machine in the Azure portal: [Quickstart: Create a Windows virtual machine in the Azure portal](#)

After creating your Azure VM, you'll first need to install the Azure Monitoring Agent for Windows. The following article describes the process: [Manage Azure Monitor Agent - Azure Monitor | Microsoft Learn](#)

Example of AMA installation using PowerShell method:

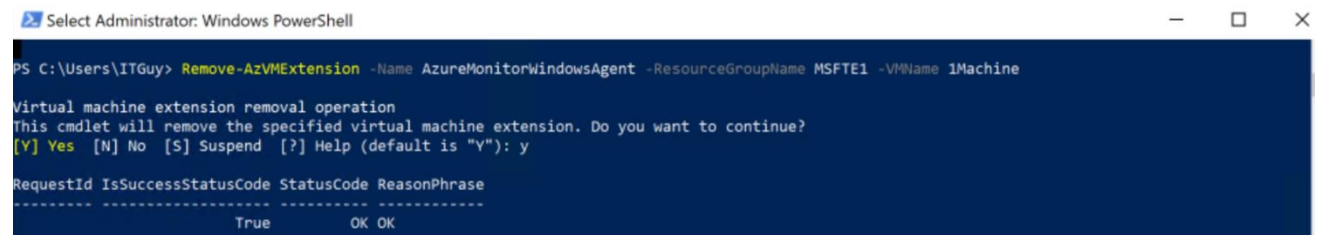
- Connect to the Azure VM and open PowerShell as Administrator
- Run Connect-AzAccount for authentication
- Run the following command in the same PowerShell window:



```
Administrator: Windows PowerShell
PS C:\Users\ITGuy> Set-AzVMExtension -Name AzureMonitorWindowsAgent -ExtensionType AzureMonitorWindowsAgent -Publisher Microsoft.Azure.Monitor -ResourceGroupName MSFTE1 -VMName 1Machine -Location WestEurope -TypeHandlerVersion 1.0 -EnableAutomaticUpgrade $true

RequestId IsSuccessStatusCode StatusCode ReasonPhrase
-----
True      OK OK
```

- To remove the AMA extension from your Azure VM, follow the same procedure as above and run the following PS command:



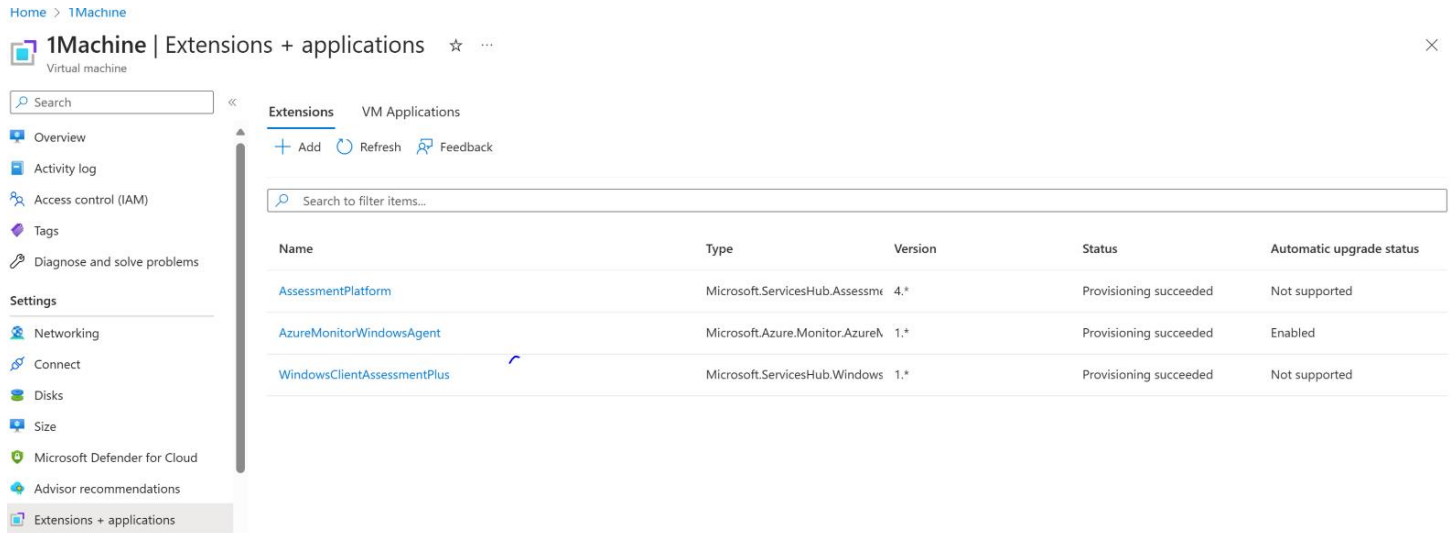
```
Select Administrator: Windows PowerShell
PS C:\Users\ITGuy> Remove-AzVMExtension -Name AzureMonitorWindowsAgent -ResourceGroupName MSFTE1 -VMName 1Machine

Virtual machine extension removal operation
This cmdlet will remove the specified virtual machine extension. Do you want to continue?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

RequestId IsSuccessStatusCode StatusCode ReasonPhrase
-----
True      OK OK
```

In order to ensure data is uploaded, please verify that system managed identity has been turned on for your Azure VM - <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/qs-configure-portal-windows-vm>

Once you have activated your assessments from Services Hub, simply navigate to the Azure portal, select your Azure VM and got to **Extensions + Application** and view all installed extensions:



The screenshot shows the Azure portal interface for a virtual machine named '1Machine'. The 'Extensions + applications' page is active, displaying a table of installed extensions. The table has the following data:

Name	Type	Version	Status	Automatic upgrade status
AssessmentPlatform	Microsoft.ServicesHub.Assessme	4.*	Provisioning succeeded	Not supported
AzureMonitorWindowsAgent	Microsoft.Azure.Monitor.AzureM	1.*	Provisioning succeeded	Enabled
WindowsClientAssessmentPlus	Microsoft.ServicesHub.Windows	1.*	Provisioning succeeded	Not supported

More information about Virtual Machine extensions and features for Windows can be found by accessing the following Article: [Virtual machine extensions and features for Windows](#)

Offline – Disconnected Environment

Decision points at a glance:

- There is zero connection allowed from the assessed environment to the Internet or to any other machine that has Internet access

In this scenario we require two machines

- One is the data collection machine and needs to fulfill prerequisites from the assessment.
- The other is the machine that has Internet access and can upload data to Azure Log Analytics.
 - This machine needs to be enrolled into Azure Arc in order to upload the batch of data from the first machine that did not have an internet connection.

To successfully execute On-Demand assessments via this method, an offline secure file copy process is necessary to transfer files to and from the Internet connected machine and the environment being assessed.

Internet Access Machine

After the enrolled into Azure Arc and setup of the assessment are completed, follow the next steps on the machine that has Internet access.

- Open Task Manager
- Open scheduled tasks and drill down to the assessment task
- Set the scheduled task to start manually, removing the weekly schedule.
- Start the scheduled task, this will download the assessment executable and the assessment package.
 - o Go to the Working Directory that was entered in the assessment setup. <Working Directory>\XXAssessment Where XX is different for each assessment.
 - o A numbered folder will appear. As soon as you see this folder, stop the OMSAssessment.exe process in Task Manager.
- Copy the folder "OMSAssessment" folder that is created in "<working directory>\XXAssessment" to a USB drive or other method of your choice to copy content to the data collection machine
- Go to: C:\ODA\Packages
 1. Search for execpkg
 2. Find the assessment package for the technology you need, open the file location and copy that Execpkg file to the same location as where you stored the "OMSAssessment" folder.

This concludes the actions on the machine with Internet access until we want to upload data.

Data Collection Machine

Create a folder on the local drive that has enough free disk space to store all collected data, up to 10GB.

For instance: C:\MicrosoftAssessment

Create a directory for collection of data. For instance:

- C:\MicrosoftAssessment\Collect

Copy the Execpkg file and OMSAssessment folder to the C:\MicrosoftAssessment folder.

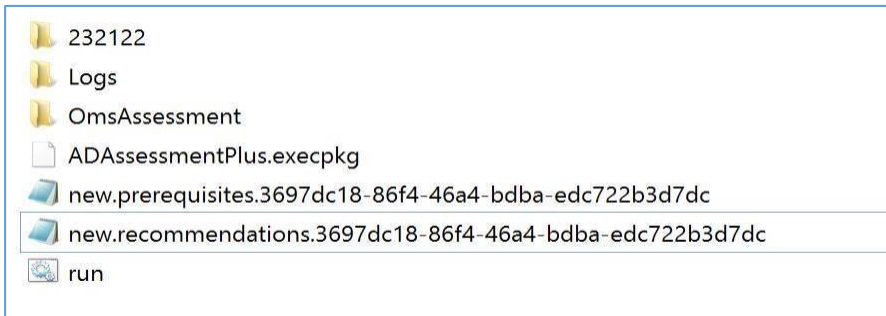
- Open an elevated CMD Prompt, go to C:\MicrosoftAssessment\OMSAssessment and run the following command:
- OmsAssessment.exe -execPackage C:\MicrosoftAssessment\ADAssessmentPlus.execpkg" -w "C:\MicrosoftAssessment\Collect" -trace Off -headers False -assessmentname "ADAssessment" discoverysettings "AD" -computername "<DataCollectionMachine>" -target ToolsMachine -op "<Location for the Recommendation files>" Data collection starts and generate few files named:

new.prerequisite<assessmentguid>.assessmentrecs new.recommendations.<assessment guid>.assessmentrecs

When the assessment is finished, the command prompt is back at the input prompt and you should not see anything running.

Copy the files that are named new.* over to the machine with Internet access

Copy the new.* files in the "<working directory>\XXAssessment"



Our Azure DCR (data collection rules) will detect the new set of recommendations and upload the data to the Workbooks as soon as possible.

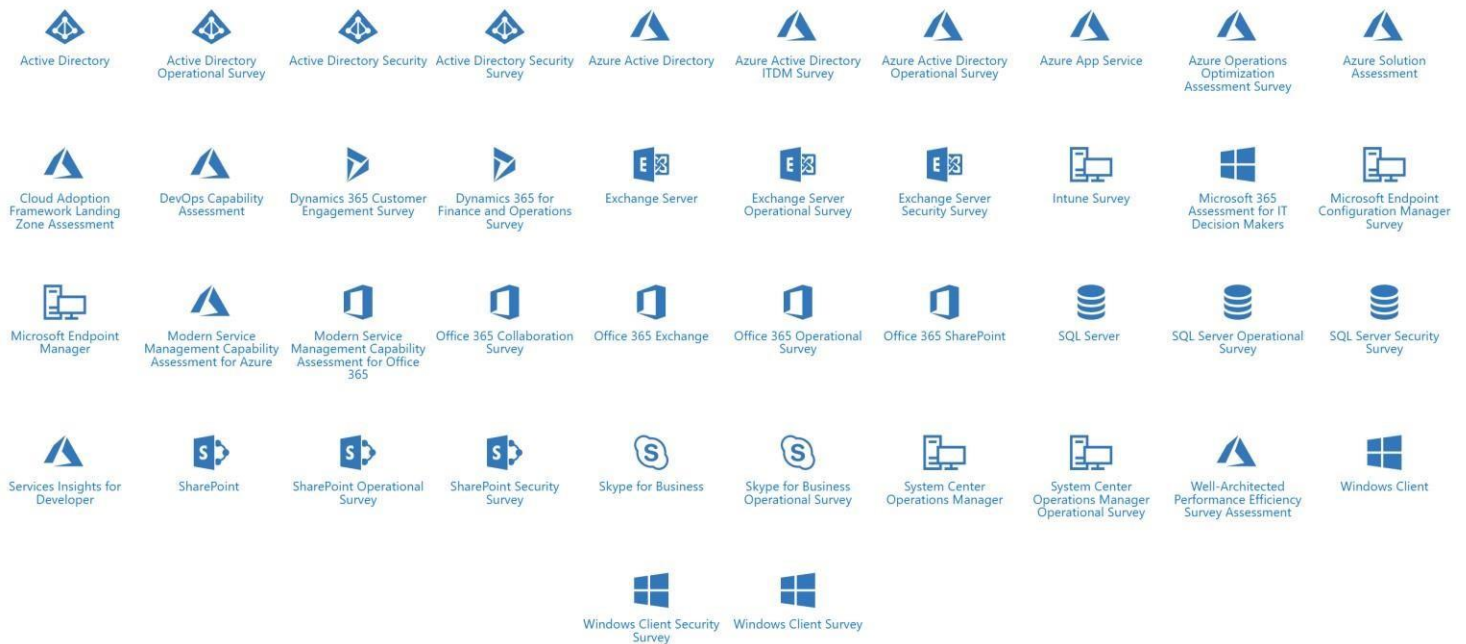
Review data afterwards on the portal, it may take up to one hour after the data is submitted to show up.

Note: More information regarding our data collection configuration (DCR) can be found by accessing the following article: [Data collection rules in Azure Monitor](#)

Add the Assessments in Services Hub

To configure an assessment, go to **Services Hub**, **IT Health**, and **On-Demand Assessments**. Browse through the assessment catalog and choose the **Assessments** that best fit your organization's needs.

Available On-Demand Assessments





Select an assessment of your choice from the list of available assessments and click on the assessment title. For example, Windows Client.

Choose your data collection machine based on your method of configuration (Azure Arc Server or Azure VM) and input the logging path:

Windows Client

The Windows Client Assessment assesses the Client environment in the following areas: Windows Client Baselines and Windows Client Security. The Windows Client Assessment checks the client configuration and operation against Microsoft best practices. We are checking several areas like base configuration, devices, network, group policy, performance, security, reliability, and more.

[Click here to learn how to configure this assessment](#)

Step 1: select the machine *  

DESKTOP-GGB2NI7 

Step 2: logging path * 

C:\Assessments

Please ensure the specified folder exists in the above selected machine.

Close

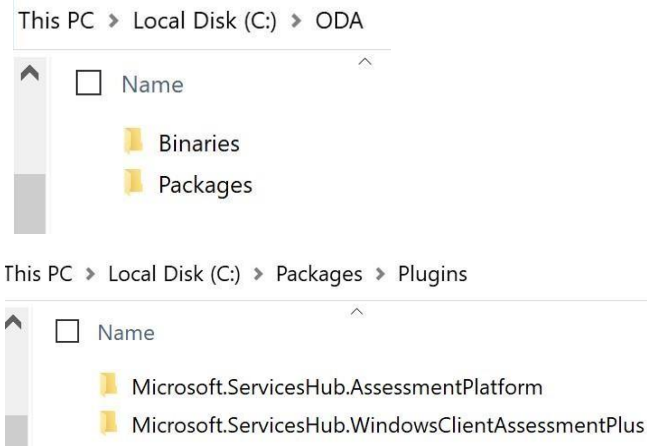
Add Assessment

! Important: Note the logging path (“C:\Assessments” – in our demo), you will be required to use the same path when prompted to declare your Working Directory during the Assessment task creation. This step is described in every Assessment specific prerequisites document.

A installation process will start and can be monitored as shown below:

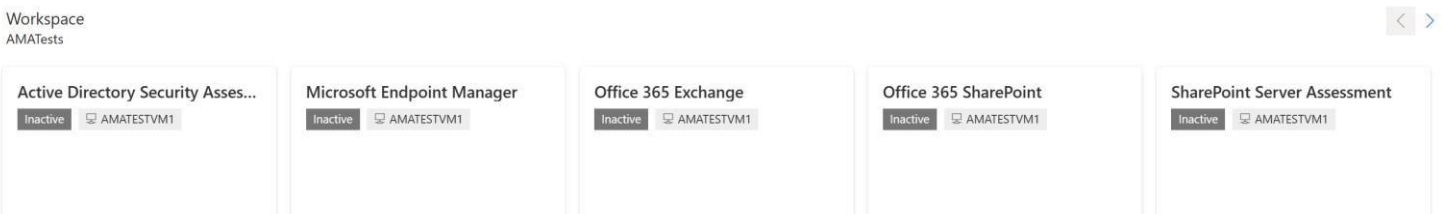


Once the solution has been installed on your data collection machine, you will be able to find the following folders on your Local C:\ drive, these contain the Assessment specific binaries and Solution packages:



Note: All Azure Arc enrolled machines and VM extensions associated with your Azure Subscription, will show up in your Services Hub Workspace(s), even if these are configured in a different Log Analytics Workspace or Resource Group.

Assessments (14)



Providing Access to Azure Log Analytics workspace

Granting access to the Log Analytics workspace to Microsoft personnel is necessary for CSA lead deliveries of OnDemand assessments and must be completed by the Azure subscription owner. We recommended you add users as a Log Analytics Reader to grant @microsoft.com users access to your Azure Log Analytics workspace to view your assessments. They will not have access to your Azure subscription.

Note: This step is not required for self-consumption of assessments without CSA lead delivery.

Provide access to the Log Analytics workspace by adding an account and granting access as mentioned in the following guide: [Add Users to Azure Log Analytics through the Azure portal](#)

- a. Engineer should be given Log Analytics Reader
- b. CSAM optionally should be given Log Analytics Reader

Configure Microsoft On-Demand Assessment(s)

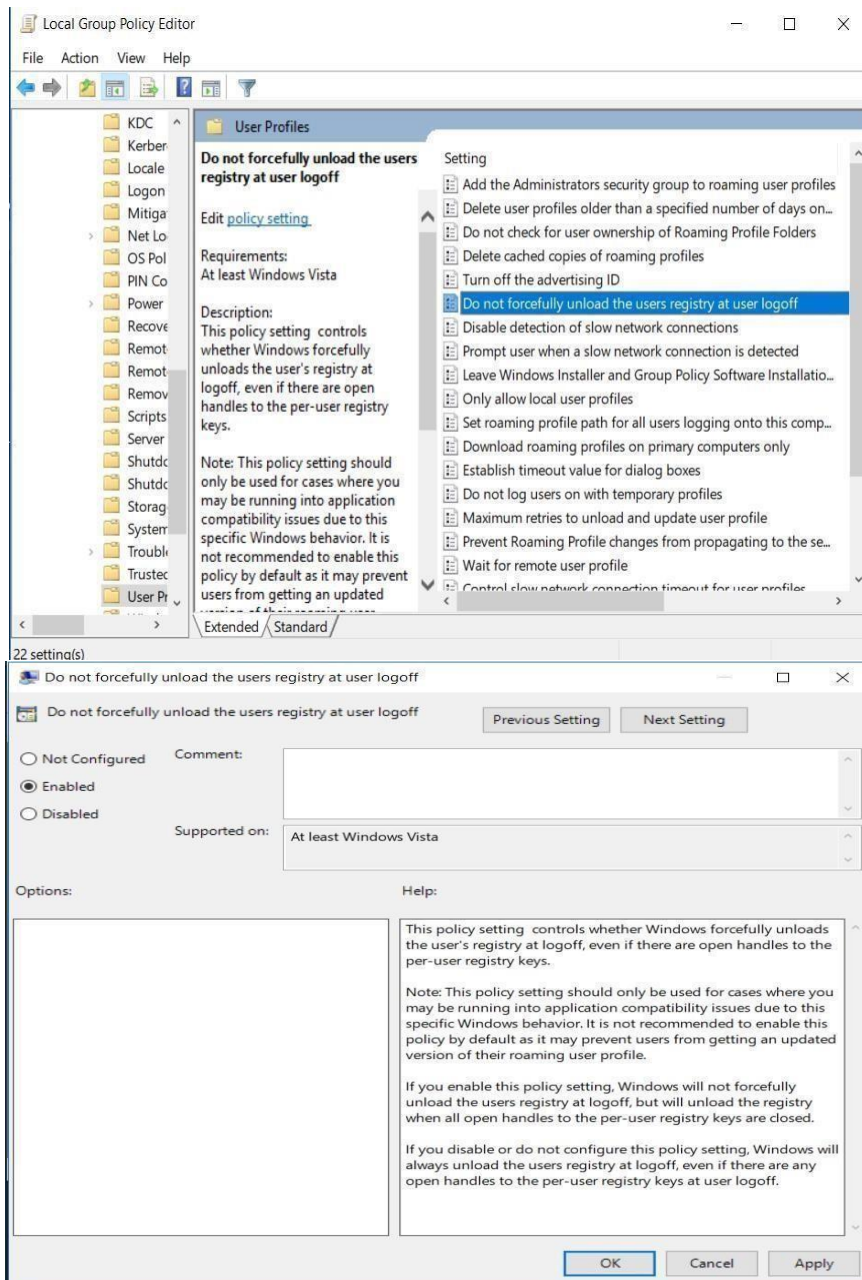
Use the following checklist to ensure all steps in this section are complete.

- Configure required group policy settings
- Verify solution is downloaded on the data collection machine
- Verify environment to be assessment the account running the assessment
- Create assessment scheduled task

Configuring the required Group Policy Objects

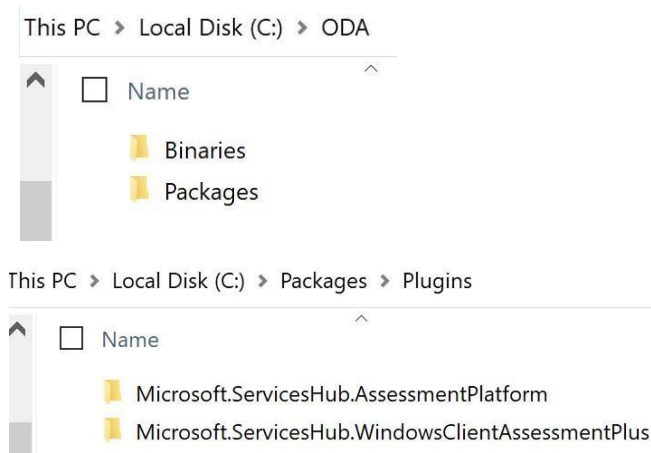
Successful execution of assessment scheduled tasks requires some policy configuration on the data collection machine to mitigate issues/risks known to degrade the successful collection of assessment data from your environment. The following configurations are applicable to all assessments.

Note: there may be policy configuration unique to specific assessments documented in the respective assessment prerequisite documentation. Start -> Run -> gpedit.msc-> Computer Configuration -> Administrative Template -> system -> user profile ->Do not forcefully unload the users registry at user logoff -> Click Enable



Verify the solution is downloaded on the data collection machine

Once the solution has been installed on your data collection machine, you will be able to find the following folders on your Local C:\ drive, these contain the Assessment specific binaries and Solution packages:



Creation of the Assessment Scheduled Task

This step of the assessment setup and configuration is unique per assessment. At a high level, this phase has 2 steps.

1. Validate and configure the environment being assessed and the account and access required for successful collection per prerequisite documents for the respective assessments.
2. Create the assessment scheduled task for the assessments being configured.

The following table illustrates the high-level assessment account permissions required for successful assessment execution:

Assessment	Local Administrator on Data Collection Machine	Enterprise Administrator	Domain Administrator	Local Administrator on targets	SQL SysAdmin	Assessment specific permissions
Active Directory	✓	✓				https://docs.microsoft.com/en-us/serviceshub/health/gettingstartedad#prerequisites
Active Directory Security	✓	✓				https://docs.microsoft.com/en-us/serviceshub/health/gettingstartedadsecurity#prerequisites
SCCM	✓			✓	✓	https://docs.microsoft.com/en-us/serviceshub/health/gettingstartedscm#prerequisites
Exchange	✓		✓ (Optional)	✓		https://docs.microsoft.com/en-us/serviceshub/health/gettingstartedexchange#prerequisites
SQL	✓			✓	✓	https://docs.microsoft.com/en-us/serviceshub/health/gettingstartedsql#prerequisites
Windows Server	✓			✓		https://docs.microsoft.com/en-us/serviceshub/health/getting-started-windowsserver#prerequisites
Windows Client	✓			✓		https://docs.microsoft.com/en-us/serviceshub/health/getting-started-windowsclient#prerequisites
SharePoint	✓			✓	✓	https://docs.microsoft.com/en-us/serviceshub/health/gettingstartedsharepoint#prerequisites

Skype for Business		✓		✓ (Optional)	✓ (Optional)	https://docs.microsoft.com/en-us/services-hub/health/gettingstarted-skypeforbusiness#prerequisites
SCOM		✓			✓	https://docs.microsoft.com/en-us/serviceshub/health/gettingstartedscm#prerequisites
Exchange Online		✓				Global Administrator for Office365 with MFA disabled
SharePoint Online		✓				Global Administrator for Office365 with MFA disabled
Skype for Business Online/ Teams		✓				Global Administrator for Office365 with MFA disabled

Complete the assessment setup by following the "Getting Started" documentation for the assessments being configured, then return to this documentation for post setup details below.

[On-Demand Assessment - Active Directory](#)

[On-Demand Assessment - Active Directory Security](#)

[On-Demand Assessment – Exchange](#)

[On-Demand Assessment - Office 365 Exchange](#)

[On-Demand Assessment - Azure Active Directory](#)

[On-Demand Assessment - Microsoft Endpoint Manager](#)

[On-Demand Assessment - System Center Operations Manager](#)

[On-Demand Assessment – SharePoint](#)

[On-Demand Assessment - Office 365 SharePoint](#)

[On-Demand Assessment – Skype for Business](#)

[On-Demand Assessment – SQL Server](#)

[On-Demand Assessment – Windows Client](#)

Download On-Demand Assessment Prerequisites

This page contains prerequisites documents for the various Assessment solutions running on Azure Log Analytics and Microsoft Services Hub. These documents will help you prepare your environment to setup and configure the Assessment solution.

[Active Directory](#)

[Active Directory Security](#)

[Microsoft Azure](#)

[Microsoft Endpoint Manager](#)

[Exchange Server](#)

[SQL Server](#)

[Windows Client](#)

[Office 365 Exchange Online](#)

[Office 365 SharePoint Online](#)

[System Center Operations Manager](#)

[Skype for Business](#)

[SharePoint Server](#)

Working with Assessment Results

Assessment recommendations may be reviewed once an assessment scheduled task has run and its recommendations and supporting details ingested into Azure Log Analytics – Workbooks.

Complete the steps in this section to navigate and work with assessment recommendations

- Validate successful ingestion of recommendations into Azure Log Analytics
- Review assessment results in Azure Log Analytics Workbooks
- Review assessment results on Services Hub assessment dashboard
- Download assessment reports from Services Hub assessment dashboard
- Create remediation plan for assessment results from Services Hub

Validate Successful Assessment

Go to data collection machine On-Demand assessment working directory (e.g. c:\ActiveDirectory for the configured assessment(s) and click on the assessment folder (example: ADAssessment).

After the conclusion of the assessment execution, several files should be observed. For example:

new.prerequisites.37508ed7ad62-485f-9f22-d5d6fae783fd.assessmentadrecs *new.processingmodel.37508ed7-ad62485f-9f22d5d6fae783fd.ad.assessmenttpm* *new.rawdata.37508ed7-ad62-485f-9f22-d5d6fae783fd.assessmentadrawdata*
new.recommendations.37508ed7-ad62-485f-9f22-d5d6fae783fd.assessmentadrecs *new.trace.37508ed7-ad62-485f-9f22d5d6fae783fd.adassessment.assessmenttrace*

After several minutes, the Azure DCR will begin ingesting these files into Azure Log Analytics.

After 3 to 4 hours, check if you can view the results from the Azure portal.

AMATests | Workbooks | Gallery 🔗 ☆ ...
 Log Analytics workspace

Search « + New 🔄 Refresh 😊 Feedback ? Help 👤 Community Git repo 📁 Browse across galleries

Classic

- Legacy agents management
- Legacy activity log connector
- Legacy storage account logs
- Legacy computer groups
- Legacy solutions
- System center
- Workspace summary (deprecated)
- Service map (deprecated)
- Virtual machines (deprecated)

All | Workbooks | Public Templates | My Templates

Filter by name or category Subscription : **AssessmentSupport** Resource Group : **All** [Reset filters](#)

Quick start

- Default Template**
A report with text and query sections.
- Empty**
A completely empty workbook.

Recently modified workbooks (6)

- demo (Adtest)
- DemoWorkbook (adtest)
- sfb (adtest)
- Windows Client Assessment (Adtest)
- Microsoft Endpoint Mana... (Adtest)
- Sample workbook (adtest)

Click on the Assessment title to navigate to the recommendation section:

📄 Workbooks ✎ Edit 💾 Save 🔄 Refresh 🔔 Alerts 📌 Pins 😊 Feedback ? Help 🕒 Auto refresh: Off

Time Range **Subscription** **Language**

Assessment Quality

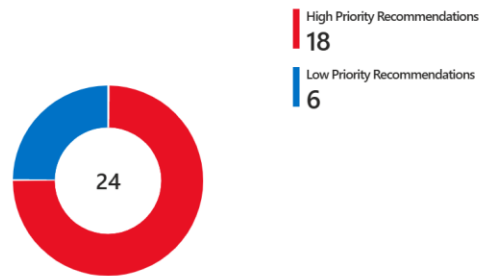
Collection Machines in Critical State	Discovery Failures	Other Prerequisite Failures	Assessment Quality Index
0	0	1	33%

Prioritized Recommendations

Search

Recommendation	FocusArea
Review summary information of Operating System versio...	Operations
Ensure that all the Active Domain Controllers in the forest...	Operations
Ensure that groups with few (two or less) members are se...	Security and
Move the DHCP Server role off the domain controllers, an...	Upgrade, M
Review summary information of Operating System versio...	Operations
Ensure that all the Active Domain Controllers in the forest...	Operations
Ensure that groups with few (two or less) members are se...	Security and
Move the DHCP Server role off the domain controllers&c...	Upgrade&c
Statistics	InternalAss
Remove Group Policy Objects that are not in use	Operations
Configure domain controllers to point to more than one ...	Availability

Security and Compliance



Recommendation

Groups with low numbers of members may be an indication of inefficient Active Directory design and could reduce security, as those groups may have unknown permissions.

Suggested Actions

Review the returned AD_Groups in the collected data to discover groups with low membership count. Identify if these groups are of use and whether they should be removed.

Context

Identify groups you have created that may not be in use anymore and might be a candidate to be cleaned up.

Note that the list can include any Builtin and Administrative group when they have less than two members. Do not remove any Builtin or Administrative groups.

Always ensure to have a valid backup before making changes to Active Directory.

Prioritization Guidance

Impact	Effort	Probability
Moderate Impact	Moderate Effort	Low To Moderate

Learn More

For more information, see The Admin's First Steps: Empty Groups, at <https://devblogs.microsoft.com/scripting/the-admins-first-steps-empty-groups/>.

AffectedObjects	↑↓
rom366.com	
rom366.com	

More information regarding Workbooks and features can be found here: [Azure Workbooks](#)

Services Hub Assessment Page

Once you've linked your Services Hub to an Azure Log Analytics workspace and configured an assessment you can access and view your assessment information from the Services Hub. To view your personalized assessment page, select IT Health from the primary navigation, and then click On-Demand Assessments. Here you'll find all your configured assessments with top-level data pulled from Azure Log Analytics.

Note: Only users that have access to Azure Log Analytics will be able to see the assessment data as we are following the security rules in place for Azure Log Analytics. For access, please contact the Azure owner in your organization.

Downloading the reports from Services Hub

Download the reports from portal. [Serviceshub.microsoft.com](https://serviceshub.microsoft.com)->IT Health->On-Demand Assessments

The screenshot displays the Services Hub assessment interface. At the top, there is a grid of five assessment cards:

- Exchange Server Assessment:** Active, AMATESTVM1, Updated April 12, 2023, 3 high priority recommendations.
- Active Directory Assessment:** Active, LAPTOP-RVGLSSHM, Updated April 12, 2023, 13 high priority recommendations.
- Microsoft Endpoint Manager:** Active, AMATESTVM1, Updated April 11, 2023, 7 high priority recommendations.
- Azure Active Directory:** Active, AMATESTVM1, Updated April 11, 2023, 9 high priority recommendations.
- Azure Active Directory:** Active, LAPTOP-RVGLSSHM, Updated April 11, 2023, 9 high priority recommendations.

Below the grid, the detailed view for the **Exchange Server Assessment** is shown. It includes a donut chart with the number **2** in the center, labeled "Data Collection Servers". To the right of the chart is a summary of recommendations:

- 3 High priority recommendations
- 26 Low priority recommendations
- 0 Resolved Recommendations
- 467 Passed checks

On the right side of the detailed view, there are several action buttons:

- [View all Recommendations](#)
- [Remove Assessment](#)
- [Download Executive Summary](#) (highlighted with a red box)
- [Download All Recommendations](#) (highlighted with a red box)
- [Create a Remediation Plan](#)

At the top right of the detailed view, there are links for [Edit Log Analytics Workspace](#), [Services Hub Connector](#), and [Troubleshooting documentation](#).

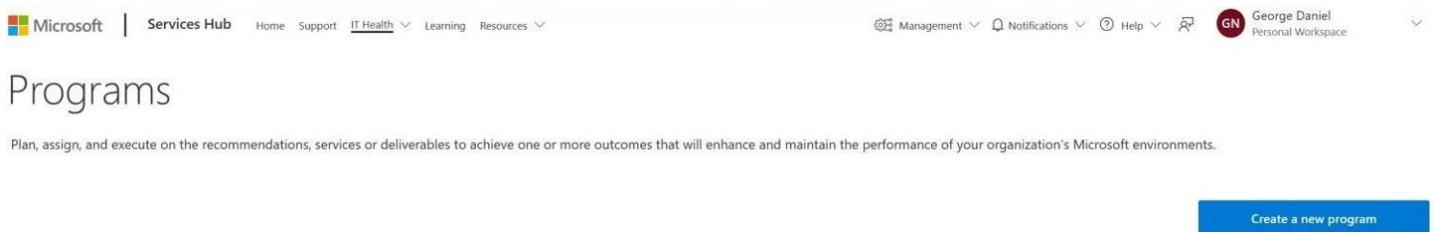
Remediation Plan creation in Service Hub

For creating a remediation plan Please follow the below process:

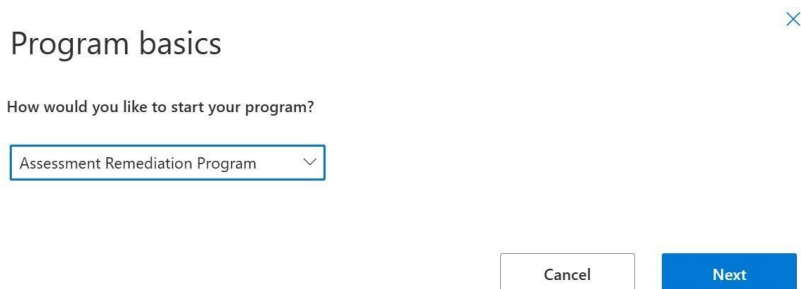
1. Log into the <https://serviceshub.microsoft.com/databoard> IT Health > Programs



2. Click on the Create a new program



3. Select the type of Program you wish to create and click Next
4. Choose the following for the below attributes:
 - a. Plan Template: Select the respective technology
 - b. Owner: Your email ID
 - c. Add a description and outcome (optional)
 - d. Target Date: Select a future Date by which you want to finish the remediation execution and click Save



Your program

Create a new program to track important activities. You can return anytime to update your program.

Template (Required)

Active Directory ▼

Environments

1 of 1 environments selected ▼

Description

AD Assessment Remediation Plan

30 of 2000 (character limit)

Outcome

Improve environment performance and security.

45 of 2000 (character limit)

[+ Add another Outcome](#)

Owner

George Daniel Nicolicioiu (@microsoft.com) ▼



Start date

4/19/2023 

End date

5/19/2023 

Active Directory

 Edit  Remove

Program basics ▲ Hide basics

Description

AD Remediation Plan

Outcome

Improve environment performance and security.

Owner: George Daniel Nicolicioiu

Log Analytics Workspace: ABrinzea

Start Date: April 19, 2023

Target Date: May 19, 2023

Progress: No tasks defined

Status: Pending

[Tasks](#) [Documents](#) [Members](#)

Tasks

Enter text to select a service from the catalog or create a custom task

 Show filters

Applied filters: Assigned To: Any Type: Any Recently Added: Any Deleted Tasks: Off Reset all filters

Notes

Type your note here...

0 of 1024 (character limit)

5. Click Add Recommendations and select from the list of Actions

Tasks Documents Members

Tasks (0 of 43 tasks completed)

 Synchronize Recommendations

Enter text to select a service from the catalog or create a custom task

Add task

 Show filters

Applied filters:

Assigned To: Any

Type: Any

Recently Added: Any

Deleted Tasks: Off

Reset all filters

Actions 

- > Availability and Business Continuity
- > Operations and Monitoring
- > Performance and Scalability
- > Security and Compliance
- > Upgrade&comm& Migration and Deployment

6. Once the recommendations are added, these will have all the issues from Azure portal with respect to the Focus areas.
7. Synchronize Recommendations is an important feature that allows you to sync the latest set of data collection. This will highlight all resolved issues and any new issues found on your environment.
8. The Members section allows you to add people to your Program
9. Now you have a few options that you can use when browsing a specific task. A common practice for complex tasks is to clone it, edit the owner and assign two different stakeholders to complete it.

Configure Multi-homed DNS servers to listen only for DNS resolution queries on the client-accessible interface

Status: Pending Type: Assessment Annotated: No Owner:

0.2

By default, a DNS Server service that is running on a multi-homed computer is configured to listen for DNS queries using all of its IP addresses. It is recommended to not have the DNS server listen on interfaces that are unreachable, i.e. on private networks.

Suggested Actions

To restrict a DNS server to listen only on selected addresses using the Windows interface, carry out the following steps:

1. Click **Start**, point to **Administrative Tools**, and then click **DNS** to open DNS Manager.
2. In the console tree, click the applicable DNS server.
3. On the **Action** menu, click **Properties**.
4. On the **Interfaces** tab, click **Only the following IP addresses**.
5. In **IP address**, type an IP address to be enabled for this DNS server, and then click **Add**.
6. Repeat the previous step as necessary to specify other server IP addresses to be enabled for this DNS server. To remove an IP address from the list, click it, and then click **Remove**.

Additional considerations

- Server IP addresses that are added here must be managed statically. If you later change or remove the addresses specified here from the TCP/IP configurations that are maintained at this server, update this list accordingly.
- After you update or revise the list of restricted interfaces, you must stop and restart the DNS server to apply the new list.
- Restricting the DNS Server service to only listen on specific IP addresses is an effective security measure because only hosts on the same network subnet, or hosts with a router that connects them to that same segment, have access to the server.

To restrict a DNS server to listen only on selected addresses using a command line

1. Open an elevated command prompt.
2. Type the following command, and then press ENTER: `dnscmd <ServerName> /ResetListenAddresses [<ListenAddress> ...]`

Prioritization Guidance

Impact: Low

Probability: Very Low

Effort: Low





Context

Consider an Active Directory integrated DNS infrastructure, where Domain Controllers are DNS servers. The DNS server has two NICs, one for the public network (for users & applications) and the other for private/network backup purposes. Both IP addresses (public and private/backup) are registered in DNS.

When a user or application queries for a name, they can get the private and the public IP address for the same server. However, the private/backup interface cannot be reached from the public network. This configuration can cause for connection issues when the server is contacted through an interface that is unreachable.

Learn More

For more information on how to restrict a DNS server to listen only on selected addresses, go to [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc755068\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc755068(v=ws.11)).

 Annotate task  Remove task  Complete task  Clone task  Edit owner  Edit due date

10. You can use the Remediation plan for tracking the issues progress, assigning the issues to the respective stakeholder.