Azure Assessment: Prerequisites and Configuration

This document explains the required steps to configure the Azure Assessment included with your Microsoft Azure Log Analytics Workspace and entitled Microsoft On-Demand assessment.

There are configuration and setup tasks to be completed prior to executing the assessment setup tasks in this document. For all pre-work, follow the Getting Started with On-Demand Assessments in the Services Hub Resource Center.

Table of Contents

System Requirements and Configuration at Glance

According to the scenario you want to use, review the following details to ensure that you meet the necessary requirements.

Supported Environments
- Azure AD tenant (AzureCloud, AzureChinaCloud, AzureGermanCloud, AzureUSGovernment)

Environment Permissions
- **Assessment account rights:**
  - An assessment scheduled task account with the following rights:
    - Administrative access to the data collection machine
    - Log on as a batch job privileges on the data collection machine
  - An Azure AD account for the setup of the Azure AD Registered Application with the following properties
    - Global Administrator
    - Non-Federated
  - An Azure AD account for assessment execution (can be separate account than above)
    - Global Reader
    - Non-Federated
    - MFA Disabled

Data Collection Machine
- A **data collection machine** running the Azure Assessment requires computers running Windows Server 2016 or Windows Server 2019 or Windows 10.
- The **data collection machine** may be Azure AD joined, Active Directory joined, or Workgroup joined.
- The **data collection machine** must be able to connect to the Internet using HTTPS to successfully perform all steps detailed in this document. This connection can be direct, or via a proxy.
- **Data collection machine hardware:** Minimum 8 gigabytes (GB) of RAM, 2 gigahertz (GHz dual-core processor, minimum 10 GB of free disk space.
- Microsoft .NET Framework 4.6.2 or newer installed
  - Download from: https://dotnet.microsoft.com/download/dotnet-framework-runtime/net462
- The CLR version on the data collection machine should be using .NET 4.0 or greater. This can be verified by running $PSVersionTable.CLRVersion in the PowerShell prompt
- Azure AD Preview Module for PowerShell needs to be installed (this will be installed automatically)
- MSOnline Powershell module. Install MSOnline PowerShell module:

  1. Open a PowerShell session with Administrator privileges
  2. On Start Menu type: PowerShell
  3. Right Click on the Icon and choose Run as Administrator
 4. On the shell type the following command: *Install-Module MSOnline -Verbose -AllowClobber -Force*

Getting started with Microsoft Azure Assessment

Be sure to complete the steps in the following link before proceeding to assessment setup:

https://docs.microsoft.com/en-us/services-hub/health/getting-started-azure

## Setup the Azure AD Application for Graph API authentication.

1. Open a PowerShell session on the data collection machine with Administrator privileges.
2. Ensure the running of scripts is permitted on the machine: *Set-ExecutionPolicy RemoteSigned*.
3. Run the following cmdlet: *New-MicrosoftAssessmentsApplication*.
4. This will prompt for Azure AD tenant Global administrator credentials:
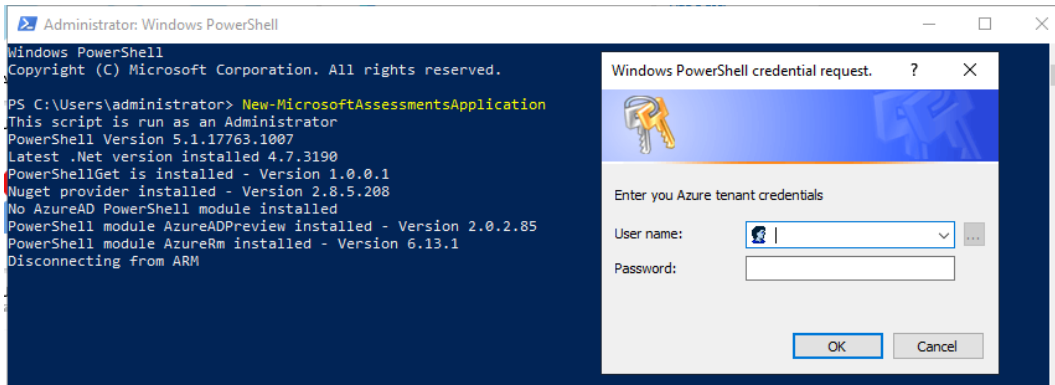
5. Enter the credentials for the Azure AD Tenant Global Administrator to be used to create the Azure application.
6. Once the credentials are entered the application will be created, the AzureAD Preview PowerShell module installed as well as other prerequisites verified.
7. Select the Azure subscription that is in scope for the assessment:
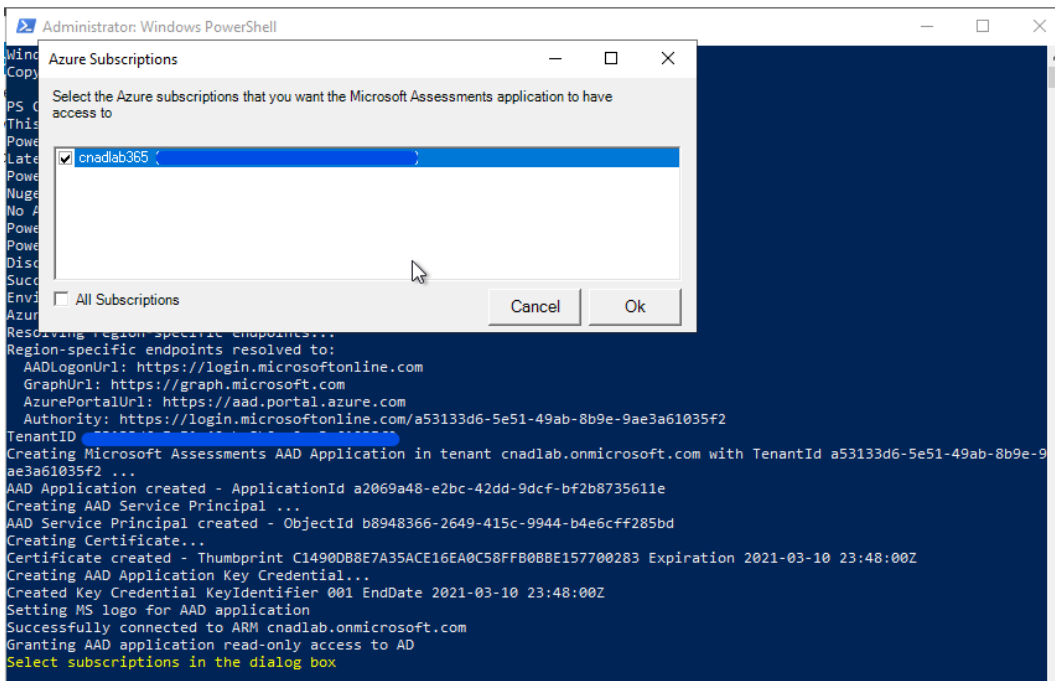
8. An internet browser prompt will appear for Azure portal login with Global Administrator credentials:
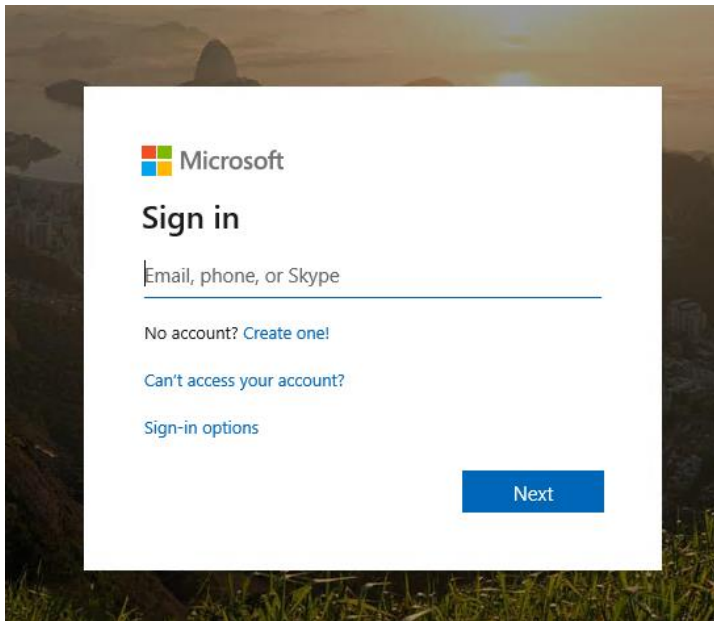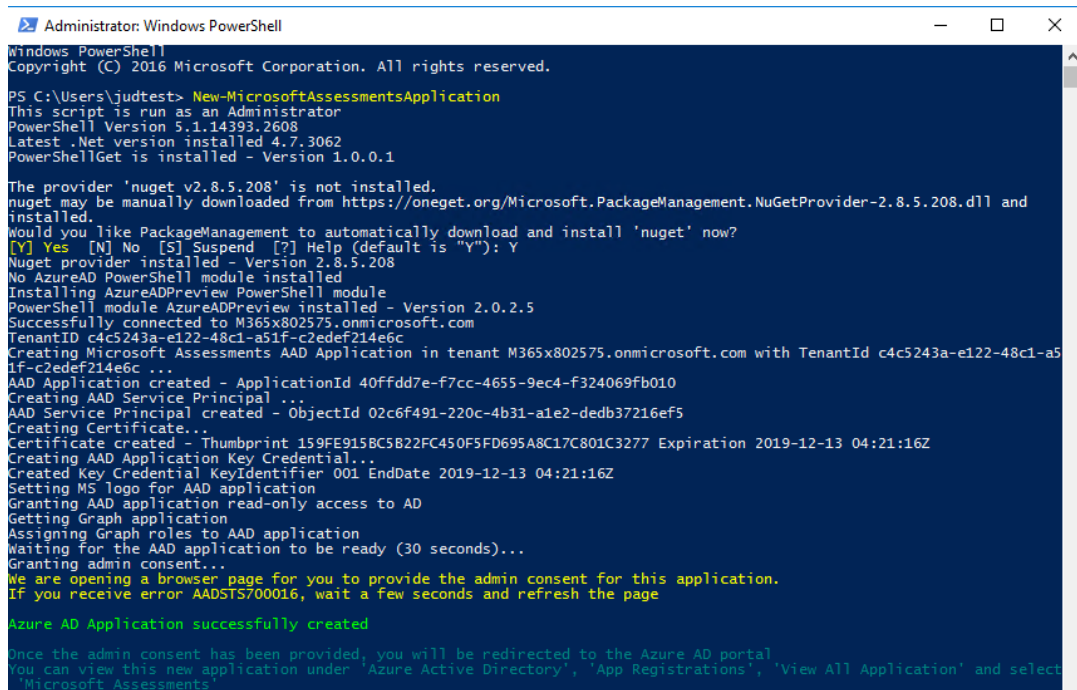

9. The required application consent **read** permissions will be displayed:
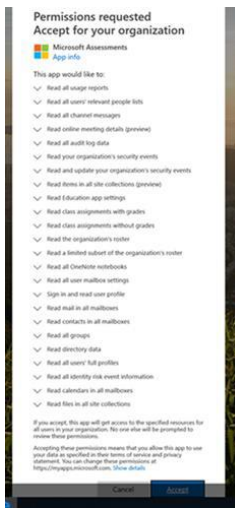
Select accept to complete the application registration.

Note: Please refer to [Permissions for Microsoft Azure AD Assessment Application](#) for consent details.

10. Once everything is complete, the application registration can be viewed in the Azure AD portal and the PowerShell output will state that the Azure AD Application has been successfully created:

11. If you encounter issues with setting up the Assessment Application, for example if you do not receive an authentication prompt please refer to the troubleshooting section in the appendix.

Setup the Azure Assessment

When you have finished the installation of the Microsoft Management Agent/OMS Gateway, you are ready to setup the Azure Assessment. There are two approaches to setting up the assessment scheduled task depending on whether the scheduled task account will be a managed service account or a user account.

Configure with User Account

On the designated data collection machine, complete the following:
1. Open the Windows PowerShell command prompt as an Administrator
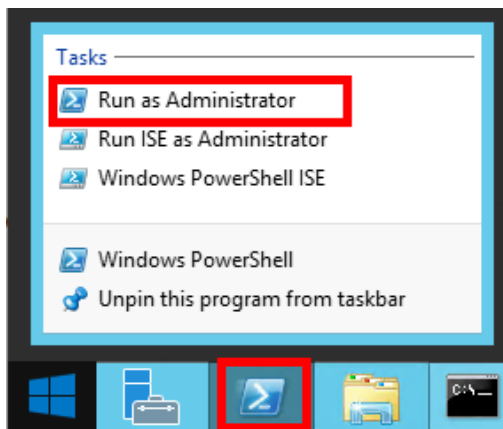
2. Define the credentials for the assessment to use:
   o **$AzureGlobalReader = Get-Credential**

3. Run the **Add-AzureAssessmentTask** command using the parameters below, replacing and **<Directory>** and **<AccountName>** with an assessment working directory and assessment scheduled task account name:
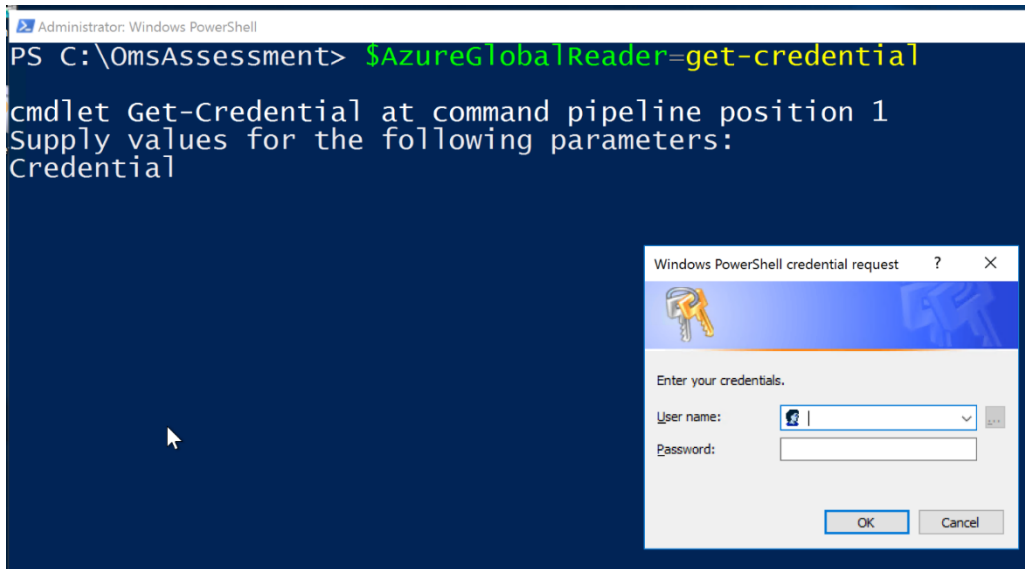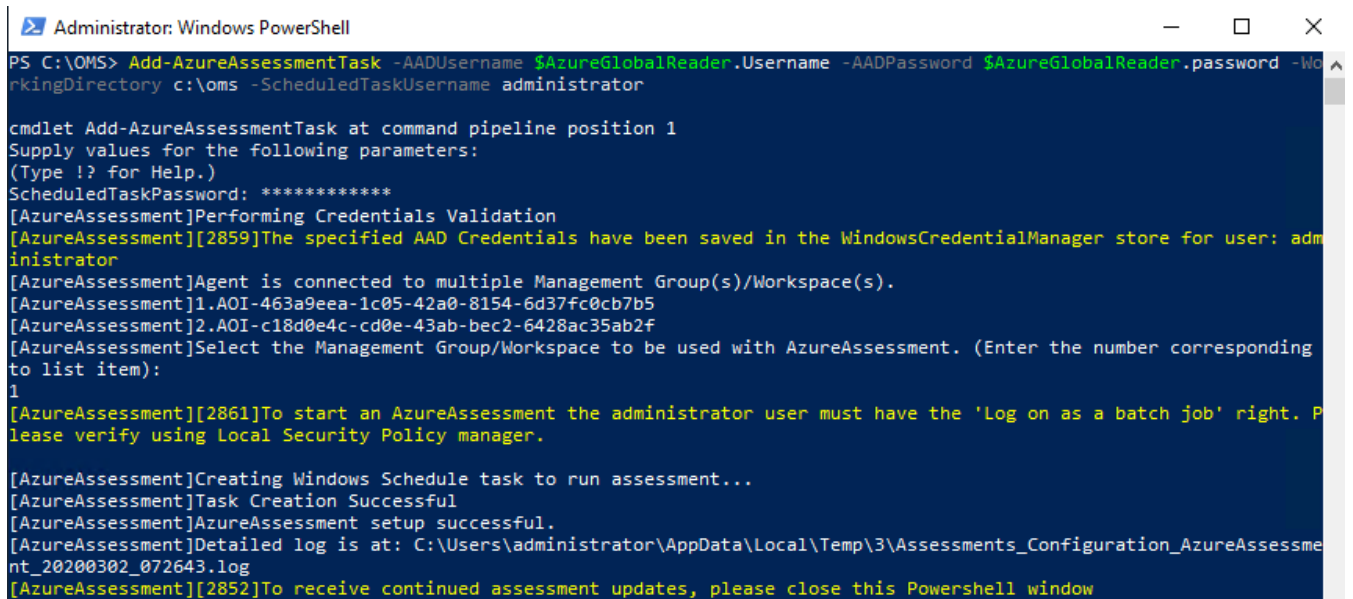   *PS C:\OmsAssessment> Add-AzureAssessmentTask -AADUsername $AzureGlobalReader.Username -AADPassword $AzureGlobalReader.password -WorkingDirectory <Directory> -ScheduledTaskUsername <accountname>*
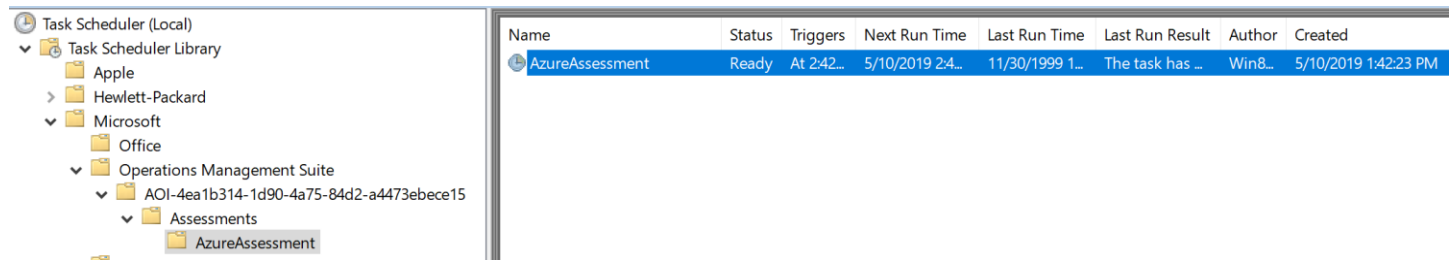
   Note. If the command **Add-AzureAssessmentTask** is not available, the module is not yet found. It can take some time after installing the agent before it to show up.

4. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.

Scheduled Task Details

Data collection is triggered by the **scheduled task** named **AzureAssessment** within an hour of running the previous script and then every 7 days. The task can be modified to run on a different date/time or even forced to run immediately.

For guidance and details on working with assessment results, visit [Working with Assessment Results](#) in the Services Hub Resource Center.

Appendix

Data Collection Methods

The **Azure Assessment** uses a couple data collection methods to collect information from your Azure AD tenant. This section describes the methods used to collect data from your environment. No Microsoft Visual Basic (VB) scripts are used to collect data.

1. Windows PowerShell
2. Graph API

4. Windows PowerShell

PowerShell is used extensively in the Azure Assessment to gather configuration data. This includes scripts that directly call Graph API endpoints as well as cmdlets from MSOnline and AzureADPreview modules.

5. Graph API

Graph API is used to collect configuration and assessment data from Secure Score.

Troubleshooting Azure Assessment Setup

General Troubleshooting OnDemand Assessment Guide
https://docs.microsoft.com/en-us/services-hub/health/assessments-troubleshooting

Azure datacenter IP address ranges
Azure Assessment requires connectivity to the Internet from the data collection machine or proxy server. The endpoints listed in the following articles should be reachable from the data collection machine for successful assessment setup and execution. These are in addition to those required by Azure Log Analytics and the Microsoft Management Agent.

- Public: https://www.microsoft.com/en-us/download/details.aspx?id=56519
- US Gov (including DoD): http://www.microsoft.com/en-us/download/details.aspx?id=57063
- Germany: http://www.microsoft.com/en-us/download/details.aspx?id=57064
- China: http://www.microsoft.com/en-us/download/details.aspx?id=57062
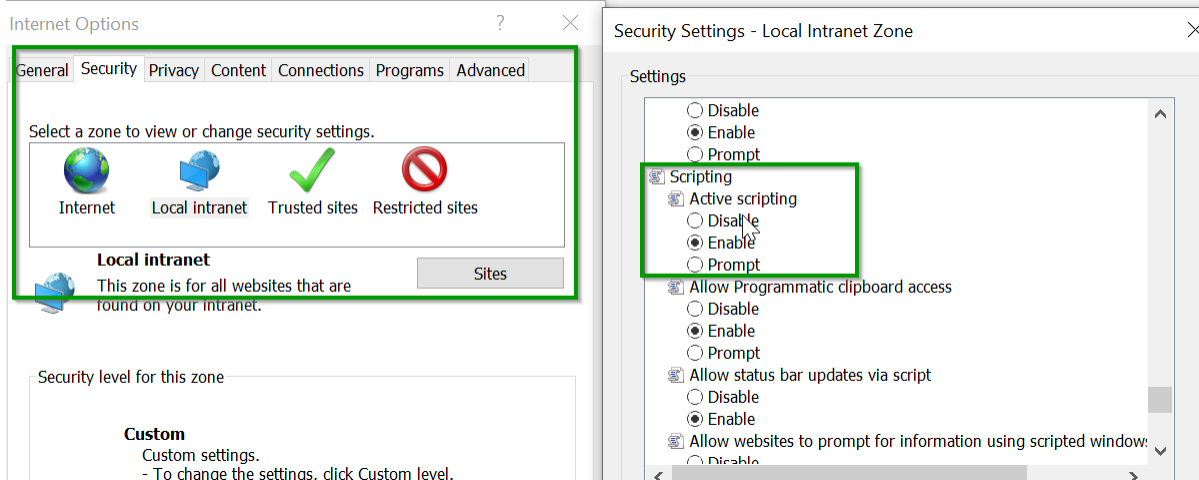
New-MicrosoftAssessmentApplication
If there are URL restrictions in place in order to correctly setup the Assessment Application, you will need to ensure you whitelist the following URLs:

URLs
aadcdn.msauth.net:443
az818661.vo.msecnd.net:443
c.urs.microsoft.com:443
go.microsoft.com:443
iecvlist.microsoft.com:443

ieonline.microsoft.com:443
login.microsoftonline.com:443
oneget.org:443
psg-prod-eastus.azureedge.net:443
www.powershellgallery.com:443

Along with above URLs, ensure the following settings are enabled in Internet Explorer as JavaScript needs to run on the page.

Internet Options ⬚ Security Settings

While executing the New-MicrosoftAssessmentsApplication command, you may be prompted to add additional links to trusted sites to allow the authentication screen to display. These can be added by clicking the "Add" button shown on the popup.

Prerequisites Error

If you encounter any prerequisites errors, please check for any errors in Event Viewer as shown below: