Using Azure AD Report API

An Azure AD How-To Guide

# Desired Outcome

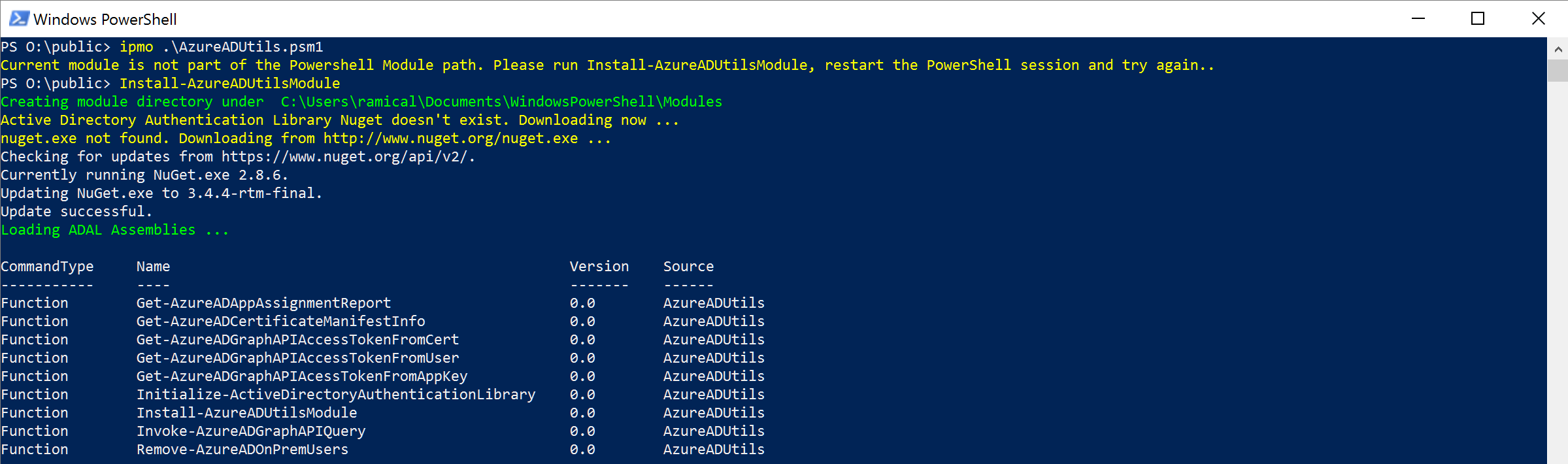
Fetch reports from Azure AD reporting API on a regular basis for compliance, reporting, or auditing purposes.

# Pre-requisites

1. Global admin to create service account
2. On premises server to run powershell commands from

# Steps to implement

1. Create a “service account” with permissions to call the graph api per the article : <https://azure.microsoft.com/en-us/documentation/articles/active-directory-reporting-api-getting-started/>
2. Download the copy from AzureADUtils.psm1 module from github
3. Create a directory to save the powershell module (let’s say it’s called c:\azureAD)
4. Copy the AzureADUtils.psm1 file to the folder you created in step #2 above
5. Open a Powershell session, and go to the directory created in step 2 and import the module. Then, install it in the Powershell module path, using the Install-AzureADUtilsModule cmdlet. The session should look like the picture below



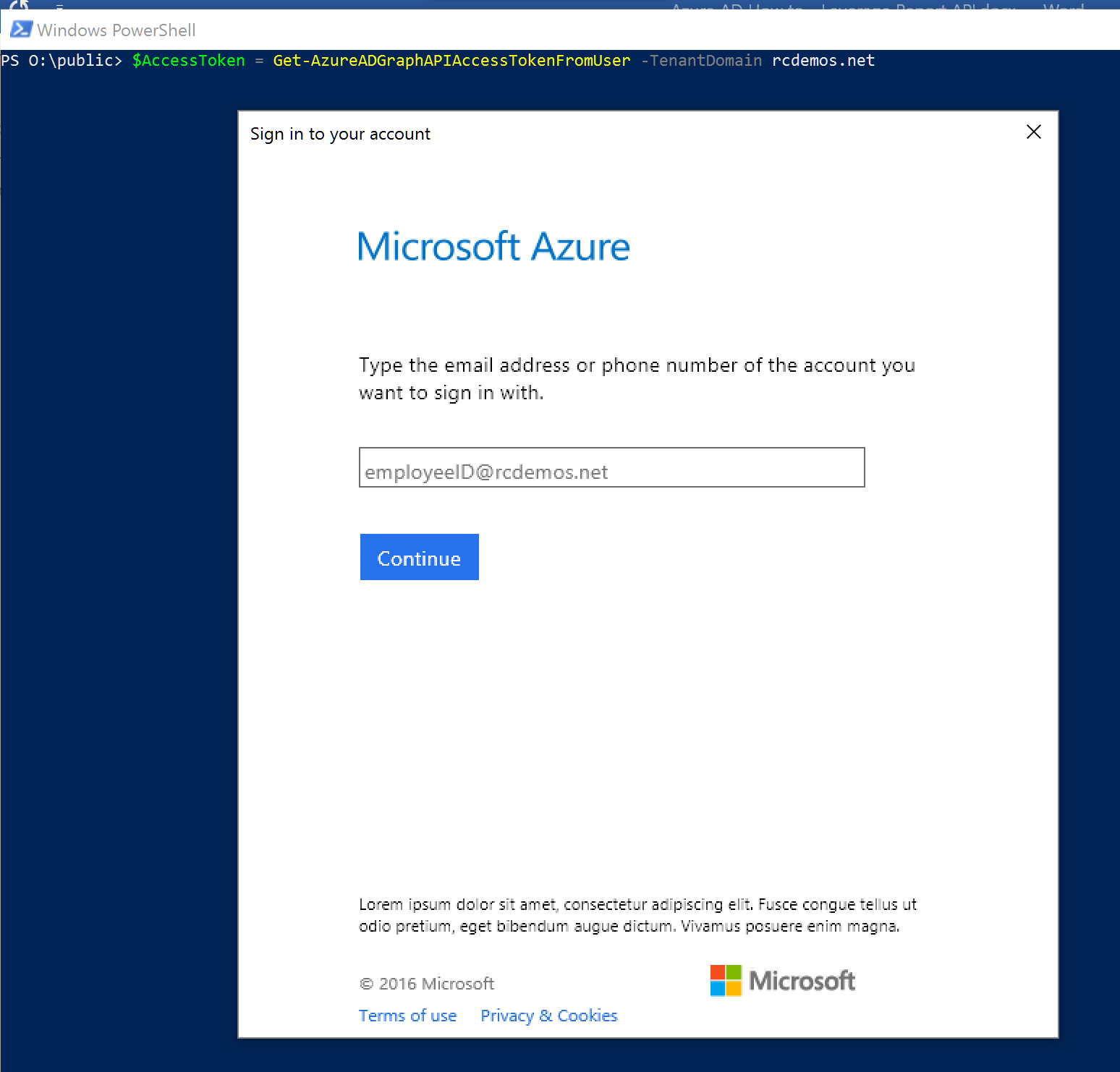
1. Close and reopen the powershell session, and reimport the module
2. Obtain an access token using one of the three cmdlets:

* **Get-AzureADGraphAPIAccessTokenFromAppKey:** You will get an access token from an application key which is effectively a username/password you configure in Azure AD (learn more: [Prerequisites to access the Azure AD reporting API – Create an application](https://azure.microsoft.com/en-us/documentation/articles/active-directory-reporting-api-prerequisites/#create-an-azure-ad-application)). Capture the username and password in a powershell pscredential for the client application created in step 1 as follows

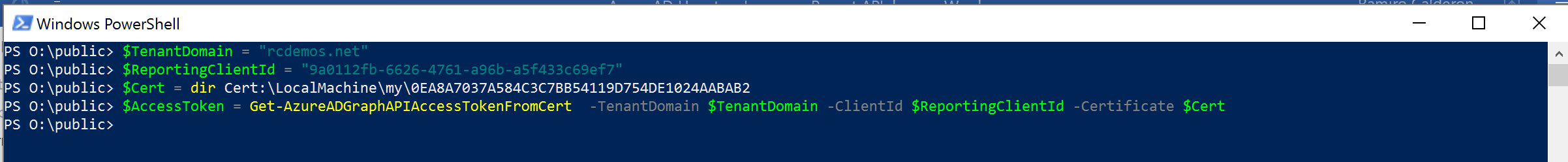
$Cred = Get-Credential

$accessToken = Get-AzureADAcessTokenFromConfidentialClient -TenantDomain rcdemos.net -ClientCredential $Cred

* **Get-AzureADGraphAPIAccessTokenFromUser:** You wil get an access token from a user interactive login. This will pop up a window that will take the user through a web authentication. If the account is federated, and your identity provider on premises supports windows integrated authentication, you can use the “WindowsAuthentication”.



* **Get-AzureADGraphAPIAccessTokenFromCert:** You will get an access token from a certificate credential.This is the recommended approach for automated retrieval of reports. Learn how to create a certificate credential here: [Authenticating to Azure AD in daemon apps with certificates](https://azure.microsoft.com/en-us/documentation/samples/active-directory-dotnet-daemon-certificate-credential/)



1. Invoke any graph query you need. Some example:
   1. Logins

Invoke-AzureADGraphAPIQuery -TenantDomain rcdemos.net -AccessToken $accessToken -GraphQuery "/activities/signinEvents?api-version=beta"

$report | ft

id timeStamp signinDateTime timeStampInMillis signinDateTimeInMillis userName userDisplayName upn

-- --------- -------------- ----------------- ---------------------- -------- --------------- ---

0cc544f4-3c8f-42bf-9930-c7cf5e3504a3\_20c52d09-b679-428b-b4da-2f3766784aaa\_201606061946\_12.130.117.176\_1 2016-06-06T19:46:05.2837701Z 2016-06-06T19:46:05.2837701Z 1465242365283 1465242365283

0cc544f4-3c8f-42bf-9930-c7cf5e3504a3\_0000000c-0000-0000-c000-000000000000\_201606062022\_12.130.117.176\_0 2016-06-06T20:22:46.6097604Z 2016-06-06T20:22:46.6097604Z 1465244566609 1465244566609

0cc544f4-3c8f-42bf-9930-c7cf5e3504a3\_0000000c-0000-0000-c000-000000000000\_201606061932\_12.130.117.176\_0 2016-06-06T19:32:09.0203874Z 2016-06-06T19:32:09.0203874Z 1465241529020 1465241529020 Test User 002 Test User 002 TestUsr002@rcdemos.net

1b10fa10-4f7b-433f-819b-a2313471ac3e\_cd3ed3de-93ee-400b-8b19-b61ef44a0f29\_201606070013\_12.70.137.75\_0 2016-06-07T00:13:59.0025833Z 2016-06-07T00:13:59.0025833Z 1465258439002 1465258439002 Test User 001 Test User 001 TestUsr001@rcdemos.net

1b10fa10-4f7b-433f-819b-a2313471ac3e\_0000000c-0000-0000-c000-000000000000\_201606070013\_12.70.137.75\_0 2016-06-07T00:13:09.1360126Z 2016-06-07T00:13:09.1360126Z 1465258389136 1465258389136

1b10fa10-4f7b-433f-819b-a2313471ac3e\_cf6d7e68-f018-4e0a-a7b3-126e053fb88d\_201606070004\_12.70.137.75\_1 2016-06-07T00:04:42.5869587Z 2016-06-07T00:04:42.5869587Z 1465257882586 1465257882586

6e0a7ff1-ea04-4207-9838-4f5cdb03cd59\_00000013-0000-0000-c000-000000000000\_201606071834\_134.163.253.244\_1 2016-06-07T18:34:03.4085383Z 2016-06-07T18:34:03.4085383Z 1465324443408 1465324443408

0cc544f4-3c8f-42bf-9930-c7cf5e3504a3\_0000000c-0000-0000-c000-000000000000\_201606070313\_12.70.137.75\_1 2016-06-07T03:13:39.88318Z 2016-06-07T03:13:39.88318Z 1465269219883 1465269219883 Test User 002 Test User 002 TestUsr002@rcdemos.net

6e0a7ff1-ea04-4207-9838-4f5cdb03cd59\_00000013-0000-0000-c000-000000000000\_201606070319\_12.70.137.75\_0 2016-06-07T03:19:40.4644015Z 2016-06-07T03:19:40.4644015Z 1465269580464 1465269580464 CloudAdmin CloudAdmin cloudadmin@rcdemosnet.onmicrosoft...

* 1. Audit events

$7daysago = "{0:s}" -f (get-date).AddDays(-7) + "Z"

Invoke-AzureADGraphAPIQuery -TenantDomain rcdemos.net -AccessToken $accessToken -GraphQuery "/reports/auditEvents?api-version=beta&`$filter=eventTime gt $7daysago"

id : SN2GR1RDS128.GRN001.msoprd.msft.net\_8953804

eventTime : 2016-07-06T01:18:05.2171448Z

actor : Microsoft.Azure.SyncFabric

action : Update service principal.

target : Salesforce

actorDetail : Name=Microsoft.Azure.SyncFabric; SPN=00000014-0000-0000-c000-000000000000; Other=ServicePrincipal\_8d04eb4e-840f-490a-a37f-26641c27eb48

targetDetail : Other=ServicePrincipal\_71062b62-d6a9-41d5-a06b-9dc900b934d1; Name=Salesforce; SPN=cd3ed3de-93ee-400b-8b19-b61ef44a0f29;

.ServicePrincipalNames=http://adapplicationregistry.onmicrosoft.com/salesforce.com/primary;https://\*.my.salesforce.com;cd3ed3de-93ee-400b-8b19-b61ef44a0f29

updatedProperties :

correlationId : e1a186e7-c4b3-45f0-a4a7-f1aeea37a43e

roleDetail :

1. Note that you can mix and match to generate whatever format. If you want CSV then pipe the output of any of the commands on step 7 above to Export-CSV commandlet

# Considerations

1. If you want to set it to run on a regular basis, consider creating a scheduled task. Learn more: <https://msdn.microsoft.com/en-us/library/windows/desktop/aa383614(v=vs.85).aspx>
2. For safe management of client credentials, consider using credential manager. See an example at: <https://gallery.technet.microsoft.com/scriptcenter/PowerShell-Credentials-d44c3cde>

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2016 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.