

Azure 評価：前提条件および構成

このドキュメントでは、Microsoft Azure Log Analytics ワークスペースと資格が与えられている Microsoft オンデマンド評価に含まれている Azure 評価の構成に必要な手順を説明します。

このドキュメントには、評価のセットアップ タスクを実行する前に完了させる構成とセットアップのタスクがあります。すべての事前作業については、Services Hub リソース センターの[オンデマンド評価の概要](#)に従ってください。

目次

システム要件および構成の概要	2
サポートされる環境	2
環境関連の許可	2
データ収集マシン	2
Microsoft Azure 評価の概要	3
Graph API 認証用に Azure AD アプリケーションをセットアップしてください。	3
Azure 評価のセットアップ	5
ユーザー アカウントで構成する	5
スケジュールされたタスクの詳細	7
付録	8
データ収集メソッド	8
Azure 評価のセットアップのトラブルシューティング	8
オンデマンド評価のトラブルシューティング全般に関するガイド	8
Azure データセンターの IP アドレス範囲	8
New-MicrosoftAssessmentApplication	8
前提条件のエラー	9

システム要件および構成の概要

使用するシナリオに従って、次の詳細を確認し、必要な要件を満たしていることを確かめてください。

サポートされる環境

- Azure AD テナント (AzureCloud、AzureChinaCloud、AzureGermanCloud、AzureUSGovernment)

環境関連の許可

- 評価アカウントの権利:
 - 次の権利を持つ、評価のスケジュールされたタスクのアカウント:
 - データ収集マシンへの管理アクセス
 - データ収集マシンにバッチ ジョブ特権としてログオンする
 - 次のプロパティを持つ、Azure AD の登録されたアプリケーションのセットアップ用の Azure AD アカウント
 - Global Administrator
 - 非フェデレーション
 - 評価の実行用の Azure AD アカウント (上記とは別のアカウントの場合もあります)
 - グローバルな閲覧者
 - 非フェデレーション
 - MFA が無効

データ収集マシン

- Azure 評価を実行しているデータ収集マシンは、Windows Server 2016、Windows Server 2019、または Windows 10 を実行するコンピューターを必要とします。
- データ収集マシンは、Azure AD、Active Directory、またはワークグループに参加している場合があります。
- このドキュメントに記載されているすべての手順を正常に実行するために、データ収集マシンは、HTTPS を使用してインターネットに接続できる必要があります。この接続は直接の場合、またはプロキシ経由の場合があります。
- データ収集マシンのハードウェア: 最小 8 ギガバイト (GB) の RAM、2 ギガヘルツ (GHz デュアル コア プロセッサ、最小 10 GB の空きディスク領域。
- Microsoft .NET Framework 4.6.2 以降をインストール済み
 - 次からダウンロードしてください: <http://dotnet.microsoft.com/download/dotnet-framework/runtime/net462>
- データ収集マシンの CLR バージョンでは、.NET 4.0 以上を使用する必要があります。PowerShell プロンプトで \$PSVersionTable.CLRVersion を実行すると、これを確認できます。
- PowerShell の Azure AD Preview モジュールがインストールされている必要があります (これは自動的にインストールされます)
- MSOnline Powershell モジュール。MSOnline PowerShell モジュールのインストール:
 1. 管理者特権で PowerShell セッションを開く
 2. [スタート] メニューで次を入力: PowerShell
 3. アイコンを右クリックし、[管理者として実行] を選択します
 4. シェルで次のコマンドを入力: `Install-Module MSOnline -Verbose -AllowClobber -Force`

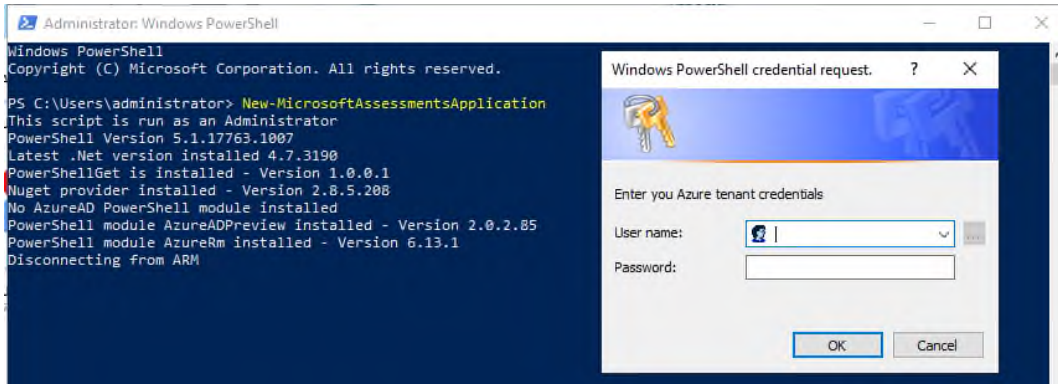
Microsoft Azure 評価の概要

評価のセットアップに進む前に、次のリンクの手順を必ず実行してください：

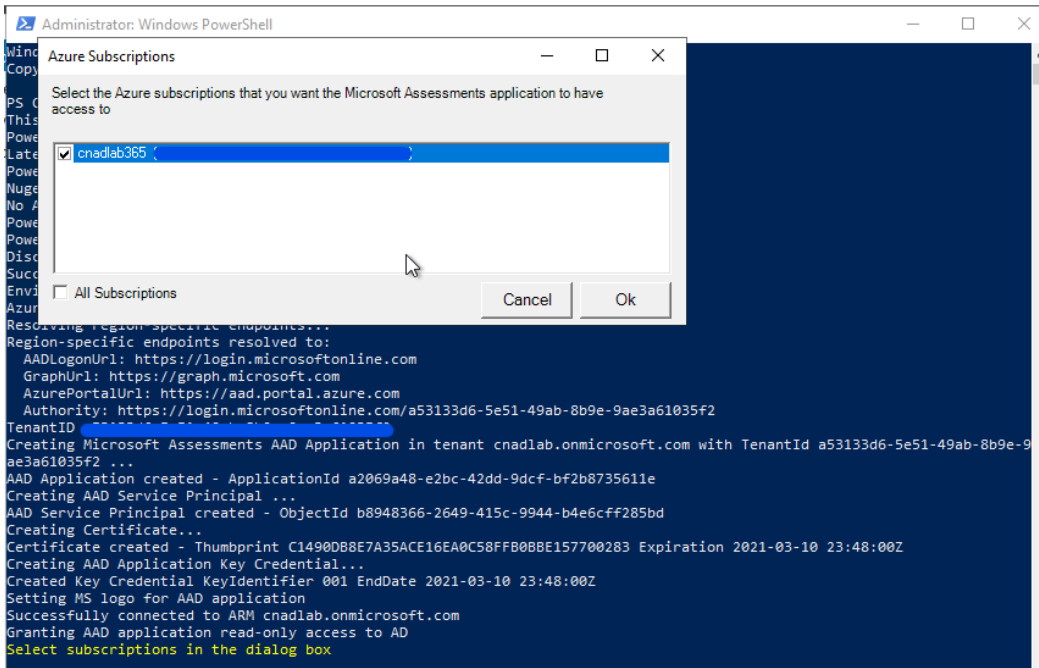
<https://docs.microsoft.com/en-us/services-hub/health/getting-started-azure>

Graph API 認証用に Azure AD アプリケーションをセットアップしてください。

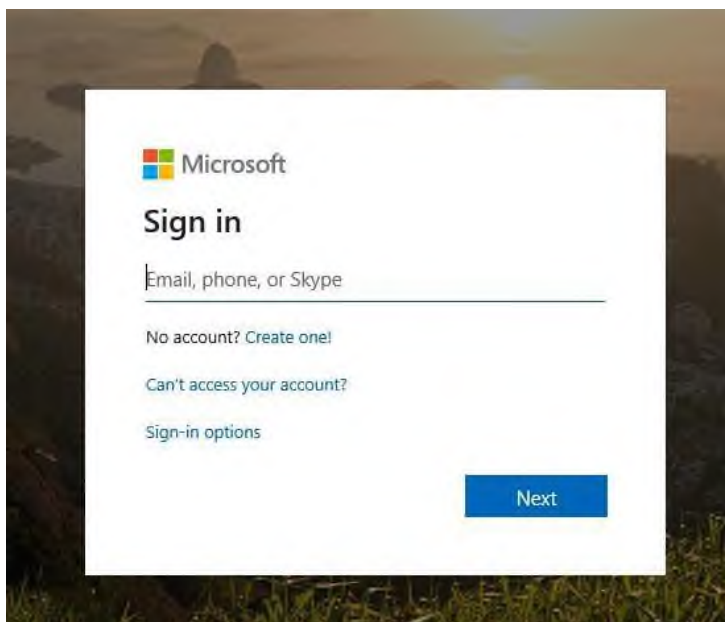
1. 管理者特権を使用し、データ収集マシンで PowerShell セッションを開きます。
2. マシンでスクリプトの実行が許可されていることを確認します：Set-ExecutionPolicy RemoteSigned。
3. 次のコマンドレットを実行します：New-MicrosoftAssessmentsApplication。
4. これにより、Azure AD テナントの Global Administrator の資格情報の入力が必要です：



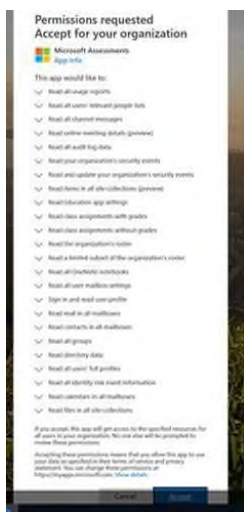
5. Azure アプリケーションの作成に使用する Azure AD テナントの Global Administrator の資格情報を入力してください。
6. 資格情報が入力されると、アプリケーションが作成され、AzureAD Preview PowerShell モジュールがインストールされるとともに、他の前提条件が検証されます。
7. 評価のスコープ内にある Azure サブスクリプションを選択します：



8. Global Administrator の資格情報でログインする Azure ポータル用のインターネット ブラウザー プロンプトが表示されます：



9. 必要なアプリケーションの同意の読み取りアクセス許可が表示されます：



「同意」を選択し、アプリケーションの登録を完了します。

注意：同意の詳細については、[Microsoft Azure AD 評価アプリケーションのアクセス許可](#) を参照してください。

10. すべてを完了すると、アプリケーションの登録を Azure AD ポータルで表示できるようになり、PowerShell の出力により、Azure AD アプリケーションが正常に作成されたことが示されます：

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\judtest> New-MicrosoftAssessmentsApplication
This script is run as an Administrator
PowerShell Version 5.1.14393.2608
Latest .Net version installed 4.7.3062
PowerShellGet is installed - Version 1.0.0.1

The provider 'nuget v2.8.5.208' is not installed.
nuget may be manually downloaded from https://oneget.org/Microsoft.PackageManagement.NuGetProvider-2.8.5.208.dll and
installed.
Would you like PackageManagement to automatically download and install 'nuget' now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
Nuget provider installed - Version 2.8.5.208
No AzureAD PowerShell module installed
Installing AzureADPreview PowerShell module
PowerShell module AzureADPreview installed - Version 2.0.2.5
Successfully connected to M365x802575.onmicrosoft.com
TenantID c4c5243a-e122-48c1-a51f-c2edef214e6c
Creating Microsoft Assessments AAD Application in tenant M365x802575.onmicrosoft.com with TenantId c4c5243a-e122-48c1-a51f-c2edef214e6c ...
AAD Application created - ApplicationId 40ffdd7e-f7cc-4655-9ec4-f324069fb010
Creating AAD Service Principal ...
AAD Service Principal created - ObjectID 02c6f491-220c-4b31-a1e2-dedb37216ef5
Creating Certificate...
Certificate created - Thumbprint 159FE9158C5B22FC450F5FD695A8C17C801C3277 Expiration 2019-12-13 04:21:16Z
Creating AAD Application Key Credential...
Created Key Credential KeyIdentifier 001 EndDate 2019-12-13 04:21:16Z
Setting MS logo for AAD application
Granting AAD application read-only access to AD
Getting Graph application
Assigning Graph roles to AAD application
Waiting for the AAD application to be ready (30 seconds)...
Granting admin consent...
We are opening a browser page for you to provide the admin consent for this application.
If you receive error AADSTS700016, wait a few seconds and refresh the page

Azure AD Application successfully created

Once the admin consent has been provided, you will be redirected to the Azure AD portal.
You can view this new application under 'Azure Active Directory', 'App Registrations', 'View All Application' and select
'Microsoft Assessments'.
```

11. 認証プロンプトを受信していないなど、評価アプリケーションの設定に関する問題が発生した場合は、付録のトラブルシューティングのセクションを参照してください。

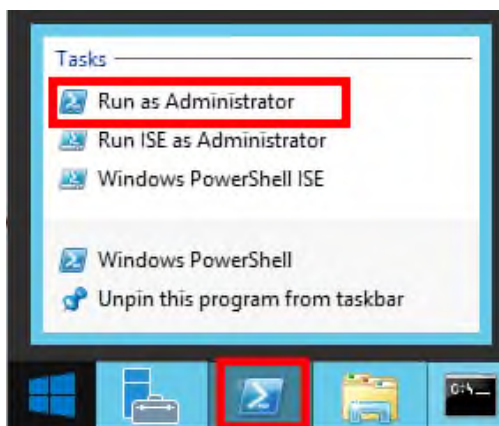
Azure 評価のセットアップ

Microsoft Management Agent/OMS Gateway のインストールを完了したら、Azure 評価をセットアップする準備が整っています。スケジュールされたタスクのアカウントが管理されたサービス アカウントかユーザー アカウントかに応じて、スケジュールされたタスクを評価する方法が 2 つあります。

ユーザー アカウントで構成する

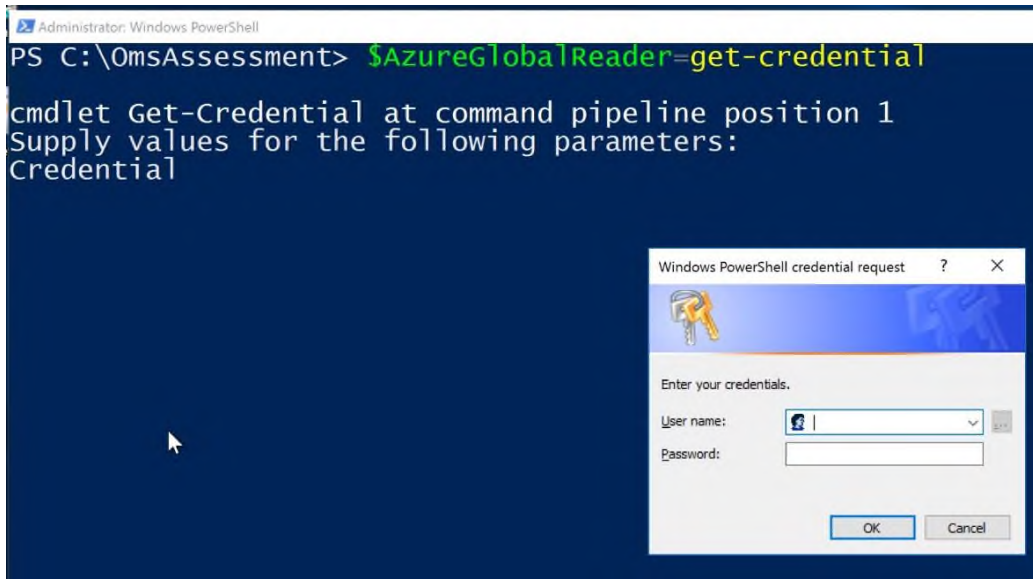
指定されたデータ収集マシンで次の手順を実行します：

1. Windows PowerShell コマンド プロンプトを管理者として開きます



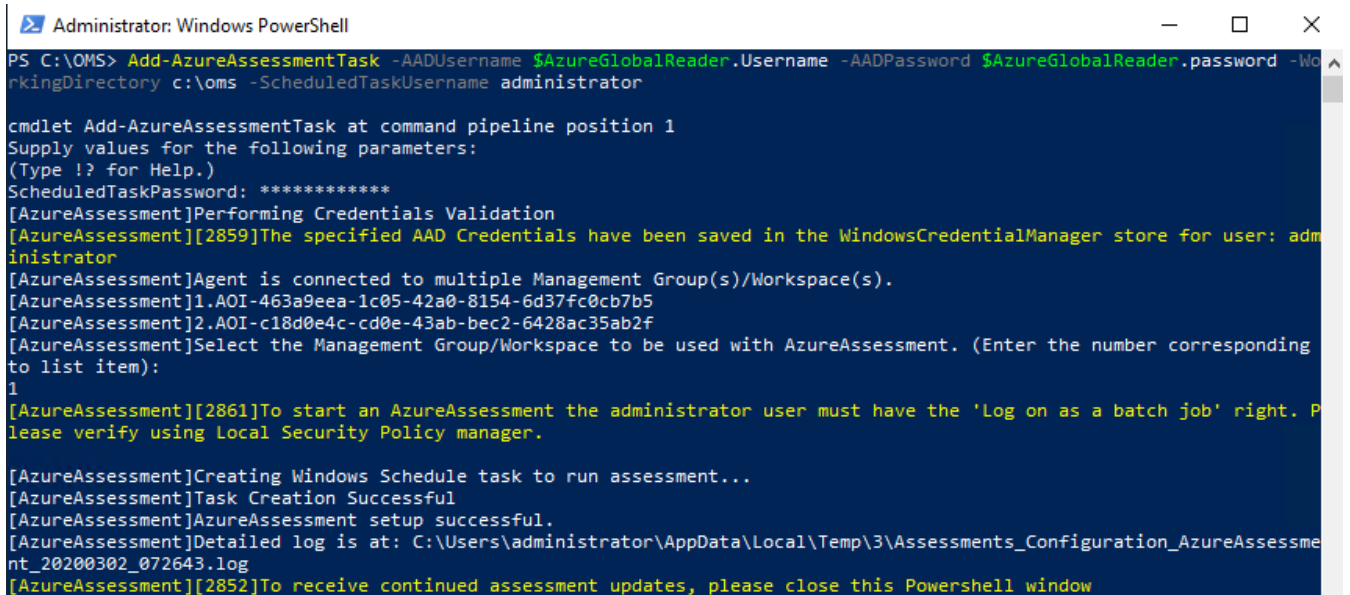
2. 次を使用して、評価の資格情報を定義します：

○ **\$AzureGlobalReader = Get-Credential**



3. 下のパラメーターを使用して、〈ディレクトリ〉と〈AccountName〉を評価の作業ディレクトリとスケジュールされたタスクのアカウント名に置き換えて、**Add-AzureAssessmentTask** を実行します：
PS C:\OmsAssessment> Add-AzureAssessmentTask -AADUsername \$AzureGlobalReader.Username -AADPassword \$AzureGlobalReader.password -WorkingDirectory <Directory> -ScheduledTaskUsername <accountname>

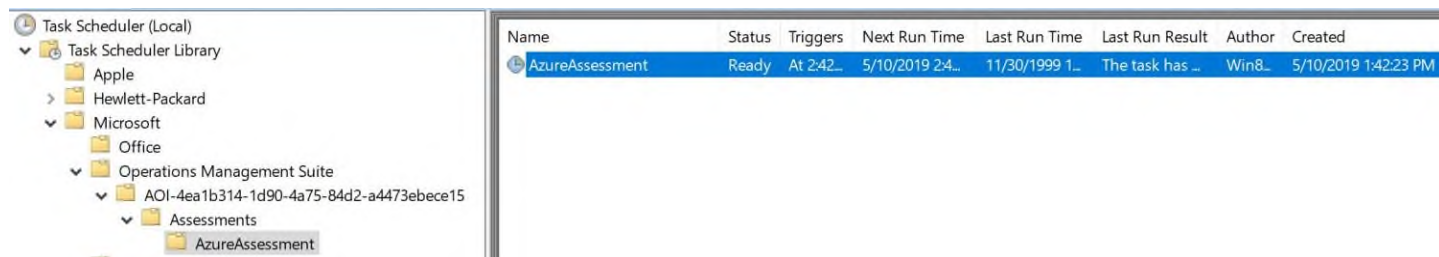
注意：Add-AzureAssessmentTask コマンドを利用できない場合は、モジュールがまだ見つかっていません。エージェントのインストール後、表示されるまでに時間がかかることがあります。



4. 必要な構成に基づいてスクリプトが続行されます。データ収集をトリガーするスケジュールされたタスクが作成されます。

スケジュールされたタスクの詳細

データ収集は、名前 **AzureAssessment** のスケジュールされたタスクにより、前のスクリプトの実行後 1 時間以内、それから 7 日ごとにトリガーされます。タスクは、別の日時に実行するように変更できます。また強制的に即実行することもできます。



The screenshot shows the Windows Task Scheduler interface. On the left, the task hierarchy is expanded to 'Task Scheduler Library > Microsoft > Operations Management Suite > AOI-4ea1b314-1d90-4a75-84d2-a4473ebee15 > Assessments > AzureAssessment'. On the right, a table lists the task details.

Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result	Author	Created
AzureAssessment	Ready	At 2:42...	5/10/2019 2:4...	11/30/1999 1...	The task has ...	Win8...	5/10/2019 1:42:23 PM

評価結果の使用に関するガイダンスおよび詳細については、Services Hub リソース センターの[評価結果での作業](#)を参照してください。

付録

データ収集メソッド

Azure 評価では、数個のデータ収集メソッドを使用して、Azure AD テナントから情報を収集します。このセクションでは、環境からデータを収集するために使用されるメソッドについて説明します。データ収集に Microsoft Visual Basic (VB) のスクリプトは使用していません。

1. Windows PowerShell
2. Graph API

4. Windows PowerShell

PowerShell は、構成データを収集するために、Azure 評価で広く使用されます。これには、MSOnline と AzureADPreview のモジュールのコマンドレット、および Graph API エンドポイントを直接呼び出せるスクリプトが含まれます。

5. Graph API

Graph API は、セキュア スコアから構成および評価データを収集するために使用されます。

Azure 評価のセットアップのトラブルシューティング

オンデマンド評価のトラブルシューティング全般に関するガイド

<https://docs.microsoft.com/en-us/services-hub/health/assessments-troubleshooting>

Azure データセンターの IP アドレス範囲

Azure 評価では、データ収集マシンまたはプロキシ サーバーからインターネットへの接続を必要とします。正常に評価を設定して実行するには、以下の記事に一覧表示されているエンドポイントにデータ収集マシンから到達できる必要があります。これらは、Azure Log Analytics と Microsoft Management Agent で求められるものに追加されています。

- パブリック: <https://www.microsoft.com/en-us/download/details.aspx?id=56519>
- US Gov (DoD を含む): <http://www.microsoft.com/en-us/download/details.aspx?id=57063>
- ドイツ: <http://www.microsoft.com/en-us/download/details.aspx?id=57064>
- 中国: <http://www.microsoft.com/en-us/download/details.aspx?id=57062>

New-MicrosoftAssessmentApplication

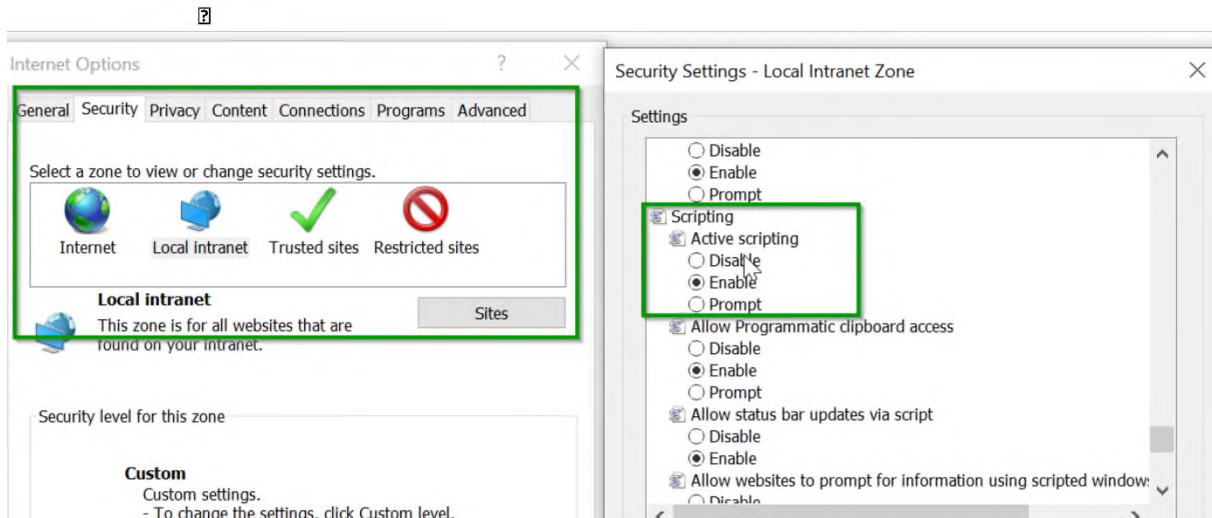
評価アプリケーションを正しくセットアップするために、所定の場所に URL 制限がある場合は、次の URL をホワイトリストに登録していることを確かめる必要があります:

URL
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.pow ershellgallery.com: 443

上記の URL と共に、以下の設定が、ページ上で実行するために必要な JavaScript として Internet Explorer で有効になっていることを確認してください。

インターネット オプション セキュリティの設定



New-MicrosoftAssessmentsApplication コマンドの実行中に、認証画面を表示できるように信頼済みのサイトに追加のリンクを追加するようメッセージが表示されることがあります。これは、ポップアップに表示される [追加] ボタンをクリックして、追加することができます。

前提条件のエラー

前提条件のエラーが発生した場合は、以下に示すように、イベント ビューアーでエラーを確認してください：

