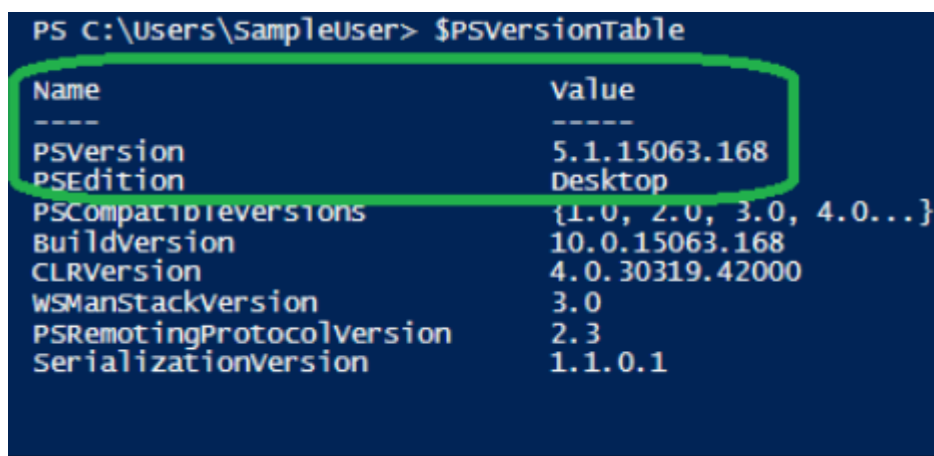


Instructions for Remediation

The following instructions will help remediate the resources for which controls are failing.

1. Validate prerequisites on machine

- i. Supported OS Versions:
 - a. Windows 10
 - b. Windows Server 2019
- ii. PowerShell version should be higher than 5.0. It can be checked by typing `$PSVersionTable` in the PowerShell ISE console window (Refer below image). If the PSVersion is older than 5.0, update it.



```
PS C:\Users\SampleUser> $PSVersionTable
```

Name	value
PSVersion	5.1.15063.168
PSEdition	Desktop
PSCompatibleVersions	{1.0, 2.0, 3.0, 4.0...}
BuildVersion	10.0.15063.168
CLRVersion	4.0.30319.42000
WSManStackVersion	3.0
PSRemotingProtocolVersion	2.3
SerializationVersion	1.1.0.1

2. Installing Az Modules

Az modules contains cmdlet to connect to Azure account. Install Az PowerShell Modules using below command. For more details of Az Modules [refer link](#).

Install-Module -Name Az.Accounts -AllowClobber -Scope CurrentUser -repository PSGallery

3. Extract Downloaded folder and open the folder

Extract the downloaded zip folder and using file explorer go to that folder. Right click on RemediationWrapper.ps1 and click on edit option, this will open Windows Powershell ISE.

4. Elevate the PIM role access using Azure Portal

Elevate the PIM role access using Azure Portal for all the subscriptions whose failing resources have been selected for remediation.

Home > Privileged Identity Management > My roles

My roles | Azure resources ☆ ...

Privileged Identity Management | My roles

« Refresh Got feedback?

Activate

- Azure AD roles
- Privileged access groups (Preview)
- Azure resources**
- Troubleshooting + Support
- Troubleshoot
- New support request

Eligible assignments Active assignments Expired assignments

Search by role or resource

Role	Resource	Resource type	Membership	Condition	End time	Action
Contributor		Resource group	Direct	None		Activate Extend
Cost Management Reader		Subscription	Group	None		Activate Extend
Contributor		Resource group	Direct	None		Activate Extend

5. Unblock the downloaded remediation scripts

Run the below commands in the AzTS remediation package directory to unblock the files required for remediation.

Get-ChildItem -Path "RemediationScripts" -Recurse | Unblock-File

Unblock-File "AutoRemediation.ps1"

6. Connect to your Azure Account

Run the below command to connect to your Azure account to be able to access your Azure resources

Connect-AzAccount

7. Execute the Auto Remediation File

Run the below command in your PowerShell ISE console to start the process of remediation.

.\AutoRemediation.ps1

8. Scan the subscription using AzTS UI

Scan the subscriptions after running Auto Remediation script using AzTS UI to see the updated scan results in the [AzTS UI](#).

DST: Azure Tenant Security (AzTS) - UI

Scan your subscriptions Take a tour

Use this tool to submit requests to scan Azure resources in your subscription(s).

Did you know? See all
Compliance visibility is based on your access ("Owner", "Contributor", "ServiceAdministrator", "CloudAdministrator", "AccountAdministrator", "Security Reader", "Security Admin") at subscription or resource group(s) level.

Exception Mode: Off Refresh Action 1 selected

Submit for Scan 1 selected
Export to CSV
Add/Renew Exceptions
Clear Exceptions

Control Name	Status	Resource	Resource Group	Status Reason
<p>Last Job ID: 20200224 Last Scanned (UTC): 02/04/2022 12:14:21 Last Scan Duration: 82 Seconds</p> <p>Scan requests today: 3 Visibility: Entire Subscription Total Controls: 288 (Passed: 251 Failed: 35)</p> <p>Compliance: 87.16 %</p>				

Unselect