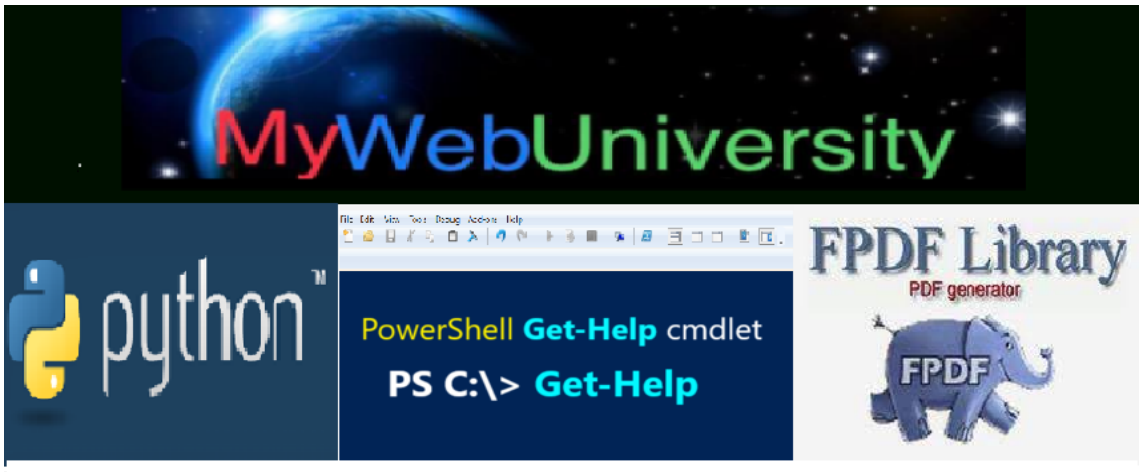

Full credit is given to all the above companies including the Operating System that this PDF file was generated!

Windows PowerShell Get-Help on Cmdlet 'Convert-AzSynapseSqlPoolVulnerabilityAssessmentScan'

PS:\>Get-HELP Convert-AzSynapseSqlPoolVulnerabilityAssessmentScan -Full

NAME

Convert-AzSynapseSqlPoolVulnerabilityAssessmentScan

SYNOPSIS

Converts a vulnerability assessment scan results to Excel format.

SYNTAX

Convert-AzSynapseSqlPoolVulnerabilityAssessmentScan [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-InputObject <Microsoft.Azure.Commands.Synapse.VulnerabilityAssessment.Model.PSVulnerabilityAssessmentScanRecordModel>] [-Confirm] [-WhatIf] [<CommonParameters>]

Convert-AzSynapseSqlPoolVulnerabilityAssessmentScan [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Name <System.String> [-ResourceGroupName <System.String>] -ScanId <System.String> -WorkspaceName <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Convert-AzSynapseSqlPoolVulnerabilityAssessmentScan cmdlet converts a scan results, that resides in the customer storage, identified by the ScanId parameter to an

Excel format placed in the storage Note that you need to run Enable-AzSynapseSqlAdvancedThreatProtection and Update-AzSynapseSqlPoolVulnerabilityAssessmentSetting

cmdlet as a prerequisite for using this cmdlets.

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <Microsoft.Azure.Commands.Synapse.VulnerabilityAssessment.Model.PSVulnerabilityAssessmentScanRecordModel>

The scan record object to use in order to convert a Vulnerability Assessment scan.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Name <System.String>

Name of Synapse SQL pool.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceGroupName <System.String>

The name of the resource group.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ScanId <System.String>

Specifies the scan ID.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-WorkspaceName <System.String>

Name of Synapse workspace.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf <System.Management.Automation.SwitchParameter>

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

System.String

Microsoft.Azure.Commands.Synapse.Models.PSVulnerabilityAssessmentScanRecordModel

OUTPUTS

Microsoft.Azure.Commands.Synapse.Models.PSVulnerabilityAssessmentScanExportModel

NOTES

Example 1: Converts vulnerability assessment scan results and saves them to local disk

```
Start-AzSynapseSqlPoolVulnerabilityAssessmentScan `
        -ResourceGroupName "ResourceGroup01" `
        -WorkspaceName "WorkspaceName01" `
        -Name "Name01" `
        -ScanId "myScan"

$convert_scan_results = Convert-AzSynapseSqlPoolVulnerabilityAssessmentScan `
    -ResourceGroupName "ResourceGroup01" `
    -WorkspaceName "WorkspaceName01" `
    -Name "Name01" `
    -ScanId "myScan"

ResourceGroupName  : "ResourceGroup01"
WorkspaceName      : "WorkspaceName01"
Name               : "Name01"
ScanId             : "myScan"
ExportedReportLocation :
"https://myaccount.blob.core.windows.net/vulnerabilityAssessment/WorkspaceName01/Name01/scan_myScan.xlsx"
```

Example 2: Converts a vulnerability assessment scan results from a scan record

```
Get-AzSynapseSqlPoolVulnerabilityAssessmentScanRecord `
        -ResourceGroupName "ResourceGroup01" `
        -WorkspaceName "WorkspaceName01" `
        -Name "Name01" `
        -ScanId "myScan" `
        | Convert-AzSynapseSqlPoolVulnerabilityAssessmentScan

ResourceGroupName  : "ResourceGroup01"
WorkspaceName      : "WorkspaceName01"
Name               : "Name01"
ScanId             : "myScan"
ExportedReportLocation :
"https://myaccount.blob.core.windows.net/vulnerabilityAssessment/WorkspaceName01/Name01
        /scan_myScan.xlsx"
```

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/az.synapse/convert-azsynapsesqlpoolvulnerabilityassessmentscan