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

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

NAME

Start-AzSynapseSqlPoolVulnerabilityAssessmentScan

SYNOPSIS

Starts a vulnerability assessment scan.

SYNTAX

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

Start-AzSynapseSqlPoolVulnerabilityAssessmentScan [-AsJob] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-SqlPoolObject <Microsoft.Azure.Commands.Synapse.Models.PSSynapseSqlPool>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Start-AzSynapseSqlPoolVulnerabilityAssessmentScan cmdlet triggers a scan with ScanId identifier. Scan results will be saved under the storage defined by the

Update-AzSynapseSqlPoolVulnerabilityAssessmentSetting cmdlet, under scans/{WorkspaceName}/{Name}/scan_{ScanId}.json You can monitor the progress of the scan by using

the Get-AzSynapseSqlPoolVulnerabilityAssessmentScanRecord cmdlet with the scanId parameter and look at the State returned parameter. Note that you need to run

Enable-AzSynapseSqlAdvancedThreatProtection and Update-AzSynapseSqlPoolVulnerabilityAssessmentSetting cmdlet as a prerequisite for using this cmdlets.

PARAMETERS

-AsJob <System.Management.Automation.SwitchParameter>

Run cmdlet in the background

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-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

-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? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-SqlPoolObject <Microsoft.Azure.Commands.Synapse.Models.PSSynapseSqlPool>

The sql pool object to get Vulnerability Assessment scan record for

Required? false

Position? named

Default value None

Accept pipeline input? True (ByValue)

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

Microsoft.Azure.Commands.Synapse.Models.PSSynapseSqlPool

System.String

OUTPUTS

Microsoft.Azure.Commands.Synapse.Models.PSSynapseSqlPool.PSVulnerabilityAssessmentScanRecordModel

NOTES

------ Example 1: Starts a vulnerability assessment scan ------

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

```
ResourceGroupName           : ResourceGroup01
WorkspaceName               : WorkspaceName01
Name                        : Name01
ScanId                      : myScan
TriggerType                 : OnDemand
State                       : Fail
StartTime                   : 6/11/2018 1:57:27 PM
EndTime                     : 6/11/2018 1:57:31 PM
```

```
Error                       : {}
ScanResultsLocationPath     : https://myaccount.blob.core.windows.net/vulnerability-assessment
                              scans/WorkspaceName01/Name01/scan_myScan.json
NumberOfFailedSecurityChecks : 9
```

Example 2: Starts a vulnerability assessment scan without a specific scan ID

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

ResourceGroupName           : ResourceGroup01
WorkspaceName               : WorkspaceName01
Name                        : Name01
ScanId                      : 20180611_135726
TriggerType                 : OnDemand
State                       : Fail
StartTime                   : 6/11/2018 1:57:27 PM
EndTime                     : 6/11/2018 1:57:31 PM
Errors                      : {}
ScanResultsLocationPath     : https://myaccount.blob.core.windows.net/vulnerability-assessment
                              scans/WorkspaceName01/Name01/scan_myScan.json
NumberOfFailedSecurityChecks : 9
```

This command generates a scan ID in the format of "yyyyMMdd_HHmmss" from the UTC date time.

Example 3: Starts a vulnerability assessment scan in the background

```
$scanJob = Start-AzSynapseSqlPoolVulnerabilityAssessmentScan `
        -ResourceGroupName "ResourceGroup01" `
        -WorkspaceName "WorkspaceName01" `
        -Name "Name01" `
        -ScanId "myScan" `
        -AsJob
$scanJob | Wait-Job
$scanJob | Receive-Job

ResourceGroupName           : ResourceGroup01
WorkspaceName               : WorkspaceName01
Name                        : Name01
ScanId                      : myScan
TriggerType                 : OnDemand
State                       : Fail
StartTime                   : 6/11/2018 1:57:27 PM
EndTime                     : 6/11/2018 1:57:31 PM
Errors                      : {}
ScanResultsLocationPath     : https://myaccount.blob.core.windows.net/vulnerability-assessment
                              scans/WorkspaceName01/Name01/scan_myScan.json
NumberOfFailedSecurityChecks : 9
```

Example 4: Starts a vulnerability assessment scan with a managed sql pool object

```
Get-AzSynapseSqlPool `
        -ResourceGroupName "ResourceGroup01" `
        -WorkspaceName "WorkspaceName01" `
        -Name "Name01" `
        | Start-AzSynapseSqlPoolVulnerabilityAssessmentScan
```

```
ResourceGroupName          : ResourceGroup01
WorkspaceName              : WorkspaceName01
Name                       : Name01
ScanId                     : 20180611_135726
TriggerType                : OnDemand
State                      : Fail
StartTime                  : 6/11/2018 1:57:27 PM
EndTime                    : 6/11/2018 1:57:31 PM
Errors                     : {}
ScanResultsLocationPath    : https://myaccount.blob.core.windows.net/vulnerability-assessment
                             scans/WorkspaceName01/Name01/scan_myScan.json
NumberOfFailedSecurityChecks : 9
```

Example 5: Starts a vulnerability assessment scan on all the databases under a managed instance

```
Get-AzSynapseSqlPool `
        -ResourceGroupName "ResourceGroup01" `
        -WorkspaceName "WorkspaceName01" `
        | Where-Object {$_.Name -ne "master"}  `
        | Start-AzSynapseSqlPoolVulnerabilityAssessmentScan

ResourceGroupName          : ResourceGroup01
WorkspaceName              : WorkspaceName01
Name                       : Name01
ScanId                     : 20180611_135726
TriggerType                : OnDemand
State                      : Fail
StartTime                  : 6/11/2018 1:57:27 PM
EndTime                    : 6/11/2018 1:57:31 PM
Errors                     : {}
```

```
ScanResultsLocationPath      : https://myaccount.blob.core.windows.net/vulnerability-assessment
                               scans/WorkspaceName01/Name01/scan_myScan.json
NumberOfFailedSecurityChecks : 9



ResourceGroupName            : ResourceGroup01
WorkspaceName                : WorkspaceName01
Name                         : Name02
ScanId                       : 20180611_135726
TriggerType                  : OnDemand
State                        : Fail
StartTime                    : 6/11/2018 1:57:27 PM
EndTime                      : 6/11/2018 1:57:31 PM
Errors                       : {}
ScanResultsLocationPath      : https://myaccount.blob.core.windows.net/vulnerability-assessment
                               scans/WorkspaceName01/Name02/scan_myScan.json
NumberOfFailedSecurityChecks : 9
```

RELATED LINKS

Online Version:

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