



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

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

NAME

Start-AzSqlInstanceDatabaseVulnerabilityAssessmentScan

SYNOPSIS

Starts a vulnerability assessment scan.

SYNTAX

```
Start-AzSqlInstanceDatabaseVulnerabilityAssessmentScan [-ResourceGroupName] <System.String> [-InstanceName]
<System.String> [-DatabaseName] <System.String> [-AsJob]
[-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]
[-ScanId <System.String>] [-Confirm] [-WhatIf]
[<CommonParameters>]
```

```
Start-AzSqlInstanceDatabaseVulnerabilityAssessmentScan [-ResourceGroupName] <System.String> [-AsJob]
[-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -InputObject
<Microsoft.Azure.Commands.Sql.ManagedDatabase.Model.AzureSqlManagedDatabaseModel> [-ScanId
<System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

DESCRIPTION

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

`Update-AzSqlInstanceVulnerabilityAssessmentSetting` cmdlet, under `scans/{ManagedInstanceName}/{ManagedDatabaseName}/scan_{ScanId}.json`. You can monitor the progress of

the scan by using the `Get-AzSqlInstanceDatabaseVulnerabilityAssessmentScanRecord` cmdlet with the `scanId` parameter and look at the `State` returned parameter. Note that

you need to run `Enable-AzSqlInstanceAdvancedDataSecurity` and `Update-AzSqlInstanceVulnerabilityAssessmentSetting` 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

`-DatabaseName <System.String>`

SQL Managed Database name.

Required? true

Position? 2

Default value None

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

-InputObject <Microsoft.Azure.Commands.Sql.ManagedDatabase.Model.AzureSqlManagedDatabaseModel>

The managed database object to get Vulnerability Assessment settings for

Required? true
Position? named
Default value None
Accept pipeline input? True (ByValue)
Accept wildcard characters? false

-InstanceName <System.String>

SQL Managed Instance name.

Required? true
Position? 1
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-ResourceGroupName <System.String>

The name of the resource group.

Required? true
Position? 0
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

-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.Sql.ManagedDatabase.Model.AzureSqlManagedDatabaseModel

System.String

OUTPUTS

Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.ManagedDatabaseVulnerabilityAssessmentScanRecordModel

NOTES

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

Start-AzSqlInstanceDatabaseVulnerabilityAssessmentScan `

-ResourceGroupName "ResourceGroup01" `

-InstanceName "ManagedInstance01" `

-DatabaseName "Database01" `

-ScanId "myScan"

ResourceGroupName : ResourceGroup01

InstanceName : ManagedInstance01

DatabaseName : Database01

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/ManagedInstance01/Database01/scan_myScan.json
NumberOfFailedSecurityChecks : 9

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

```
Start-AzSqlInstanceDatabaseVulnerabilityAssessmentScan `  
-ResourceGroupName "ResourceGroup01" `  
-InstanceName "ManagedInstance01" `  
-DatabaseName "Database01"
```

ResourceGroupName : ResourceGroup01
InstanceName : ManagedInstance01
DatabaseName : Database01
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/ManagedInstance01/Database01/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-AzSqlInstanceDatabaseVulnerabilityAssessmentScan `
    -ResourceGroupName "ResourceGroup01" `
    -InstanceName "ManagedInstance01" `
    -DatabaseName "Database01" `
    -ScanId "myScan" `
    -AsJob
$scanJob | Wait-Job
$scanJob | Receive-Job
```

```
ResourceGroupName      : ResourceGroup01
InstanceName           : ManagedInstance01
DatabaseName           : Database01
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/ManagedInstance01/Database01/scan_myScan.json
NumberOfFailedSecurityChecks : 9
```

Example 4: Starts a vulnerability assessment scan with a managed database object

```
Get-AzSqlInstanceDatabase `
    -ResourceGroupName "ResourceGroup01" `
```

```
-InstanceName "ManagedInstance01" `
-Name "Database01" `
| Start-AzSqlInstanceDatabaseVulnerabilityAssessmentScan
```

```
ResourceGroupName      : ResourceGroup01
InstanceName           : ManagedInstance01
DatabaseName            : Database01
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/ManagedInstance01/Database01/scan_myScan.json
NumberOfFailedSecurityChecks : 9
```

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

```
Get-AzSqlInstanceDatabase `
-ResourceGroupName "ResourceGroup01" `
-InstanceName "ManagedInstance01" `
| Where-Object {$_.Name -ne "master"} `
| Start-AzSqlInstanceDatabaseVulnerabilityAssessmentScan
```

```
ResourceGroupName      : ResourceGroup01
InstanceName           : ManagedInstance01
DatabaseName            : Database01
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/ManagedInstance01/Database01/scan_myScan.json
NumberOfFailedSecurityChecks : 9

ResourceGroupName : ResourceGroup01
InstanceName : ManagedInstance01
DatabaseName : Database02
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/ManagedInstance01/Database02/scan_myScan.json
NumberOfFailedSecurityChecks : 9

RELATED LINKS

Online

Version:

<https://learn.microsoft.com/powershell/module/az.sql/start-azsqlinstancedatabasevulnerabilityassessmentscan>