Windows PowerShell Get-Help on Cmdlet 'Get-AzSecuritySqlVulnerabilityAssessmentScanRecord'

PS:\>Get-HELP Get-AzSecuritySqlVulnerabilityAssessmentScanRecord -Full

NAME

Get-AzSecuritySqlVulnerabilityAssessmentScanRecord

SYNOPSIS

Gets SQL vulnerability assessment scan summary.

SYNTAX

Get-AzSecuritySqlVulnerabilityAssessmentScanRecord -AgentId <System.String> -ComputerName <System.String> -Database <System.String> [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-ScanId <System.String>] -Server <System.String> -VmUuid <System.String>
-WorkspaceId <System.String> -WorkspaceResourceId <System.String> [<CommonParameters>]

Get-AzSecuritySqlVulnerabilityAssessmentScanRecord -Database <System.String> [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -ResourceId <System.String> [-ScanId <System.String>] -Server
<System.String> -WorkspaceId <System.String> [<CommonParameters>]

DESCRIPTION

Gets SQL vulnerability assessment scan summary.

PARAMETERS

-AgentId <System.String>

Agent ID - on premise parameter

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ComputerName <System.String>

Computer full name - on premise parameter

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Database <System.String>

Database name

Required? true

Position? named

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

-ResourceId <System.String>

ID of the security resource that you want to invoke the command on. Supported resources are:

- ARC: /subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/Microsoft.HybridCompute/machines/{machineName}

- VM: /subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/Microsoft.Compute/virtualMachines/{machineName}

- On-Premise: /subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/microsoft.operationalinsights/workspaces/{workspaceName}/onPremiseMachines/{machineName}

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ScanId <System.String>

Vulnerability assessment scan ID - use scanId = 'latest' to get latest results

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Server <System.String>

Server name

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-VmUuid <System.String>

Virtual machine universal unique identifier - on premise parameter

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-WorkspaceId <System.String>

Workspace ID.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-WorkspaceResourceId <System.String>

Workspace resource ID - on premise parameter

Required? true

Position? named

Default value None

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

None

OUTPUTS

Microsoft.Azure.Commands.SecurityCenter.Models.SqlVulnerabilityAssessment.PSSqlVulnerabilityAssessmentScanRecord

NOTES

Example 1: get scan summary for latest scan for SQL Database.

Get-AzSecuritySqlVulnerabilityAssessmentScanRecord -WorkspaceResourceId

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/ahabas-workspace -ComputerName ahabas-dev01.middleeast.corp.microsoft.com -AgentId 49640166-652f-4ee6-b48b-cfb840b8afe2 -VmUuid 4c4c4544-0030-4b10-8039-b8c04f4a3332 -WorkspaceId ba7c9d0e-a6e3-4997-b575-cf7a18a98a49 -Server AHABASDEV01SRV -Database master -ScanId "latest"

TriggerType : Recurring
State : Failed
Server : AHABASDEV01SRV
Database : master
SqlVersion : 14.0.1000.169
StartTime : 3/17/2021 1:11:10 AM
EndTime : 12/31/9999 9:59:59 PM
HighSeverityFailedRulesCount : 9
MediumSeverityFailedRulesCount : 2
LowSeverityFailedRulesCount : 5
TotalPassedRulesCount : 43
TotalFailedRulesCount : 16
TotalRulesCount : 59
IsBaselineApplied : True
Id : /subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/ahabas-workspace/onpremisemachines/ahabas-dev01.middleeast.corp.microsoft.com_49640166-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b8c04f4a3332/sqlServers/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/bdbdf860-5d58-464b-ad9a-0125af63c162
Name : bdbdf860-5d58-464b-ad9a-0125af63c162

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans

Example for using scan id = "latest".

------ Example 2: Get all scan summaries on SQL Database. ------

Get-AzSecuritySqlVulnerabilityAssessmentScanRecord -WorkspaceResourceId

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/ahabas-workspace -ComputerName ahabas-dev01.middleeast.corp.microsoft.com -AgentId 49640166-652f-4ee6-b48b-cfb840b8afe2 -VmUuid 4c4c4544-0030-4b10-8039-b8c04f4a3332 -WorkspaceId ba7c9d0e-a6e3-4997-b575-cf7a18a98a49 -Server AHABASDEV01SRV -Database master

TriggerType : Recurring
State : Failed
Server : AHABASDEV01SRV
Database : master
SqlVersion : 14.0.1000.169
StartTime : 3/17/2021 1:11:10 AM
EndTime : 12/31/9999 9:59:59 PM
HighSeverityFailedRulesCount : 9
MediumSeverityFailedRulesCount : 2
LowSeverityFailedRulesCount : 5
TotalPassedRulesCount : 43
TotalFailedRulesCount : 16
TotalRulesCount : 59
IsBaselineApplied : True
Id : /subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/aha

bas-workspace/onpremisemachines/ahabas-dev01.middleeast.corp.microsoft.com_49640166-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b8c04f4a3332/

sqlServers/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/bdbdf860-5d58-464b-ad9a-0125af63c162

Name : bdbdf860-5d58-464b-ad9a-0125af63c162

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans

TriggerType : Recurring

State : Failed

Server : AHABASDEV01SRV

Database : master

SqlVersion : 14.0.1000.169

StartTime : 3/17/2021 12:41:14 AM

EndTime : 3/17/2021 1:11:10 AM

HighSeverityFailedRulesCount : 2

MediumSeverityFailedRulesCount : 0

LowSeverityFailedRulesCount : 0

TotalPassedRulesCount : 57

TotalFailedRulesCount : 2

TotalRulesCount : 59

IsBaselineApplied : True

Id :

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/aha

bas-workspace/onpremisemachines/ahabas-dev01.middleeast.corp.microsoft.com_49640166-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b8c04f4a3332/

sqlServers/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/8b2383c3-7c7e-4b6c-9b34-512ce99fd68a

Name : 8b2383c3-7c7e-4b6c-9b34-512ce99fd68a

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans

TriggerType : Recurring

State : Passed

Server : AHABASDEV01SRV

Database : master

SqlVersion : 14.0.1000.169

StartTime : 2/14/2021 4:27:44 PM

EndTime : 3/17/2021 12:41:14 AM

HighSeverityFailedRulesCount : 0

MediumSeverityFailedRulesCount : 0

LowSeverityFailedRulesCount : 0

TotalPassedRulesCount : 59

TotalFailedRulesCount : 0

TotalRulesCount : 59

IsBaselineApplied : True

Id :

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/ahabas-workspace/onpremisemachines/ahabas-dev01.middleeast.corp.microsoft.com_49640166-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b8c04f4a3332/sqlServers/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/6845790d-6463-4f45-96e8-76286edf0267

Name : 6845790d-6463-4f45-96e8-76286edf0267

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans

TriggerType : Recurring

State : Failed

Server : AHABASDEV01SRV

Database : master

SqlVersion : 14.0.1000.169

StartTime : 2/14/2021 3:57:44 PM

EndTime : 2/14/2021 4:27:44 PM

HighSeverityFailedRulesCount : 2

MediumSeverityFailedRulesCount : 0

LowSeverityFailedRulesCount : 0

TotalPassedRulesCount : 57

TotalFailedRulesCount : 2

TotalRulesCount : 59

IsBaselineApplied : True

Id :

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/aha

bas-workspace/onpremisemachines/ahabas-dev01.middleeast.corp.microsoft.com_49640166-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b8c04f4a3332/

sqlServers/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/2058a46e-cb5a-4a49-b28a-6576a540dd9d

Name : 2058a46e-cb5a-4a49-b28a-6576a540dd9d

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans

Example for Listing all scan records when a scan id is not specified.

-- Example 3: Get scan summary using resource id parameters. --

Get-AzSecuritySqlVulnerabilityAssessmentScanRecord -ResourceId

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/ahabas-workspace/onPremiseMachines/ahabas-dev01.middleeast.corp.microsoft.com_49640166

6-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b

8c04f4a3332 -WorkspaceId ba7c9d0e-a6e3-4997-b575-cf7a18a98a49 -Server AHABASDEV01SRV -Database master -ScanId 169a5f78-acff-4e05-b597-6252af7e6677

```
TriggerType                 : Recurring
State                       : Failed
Server                      : AHABASDEV01SRV
Database                    : master
SqlVersion                  : 14.0.1000.169
StartTime                   : 11/18/2020 1:10:34 AM
EndTime                     : 11/18/2020 1:40:20 AM
HighSeverityFailedRulesCount   : 9
MediumSeverityFailedRulesCount : 2
LowSeverityFailedRulesCount    : 5
TotalPassedRulesCount          : 43
TotalFailedRulesCount          : 16
TotalRulesCount                : 59
IsBaselineApplied              : True
Id                          : /subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/ahabas-workspace/onpremisemachines/ahabas-dev01.middleeast.corp.microsoft.com_49640166-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b8c04f4a3332/sqlServers/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/169a5f78-acff-4e05-b597-6252af7e6677
Name                        : 169a5f78-acff-4e05-b597-6252af7e6677
Type                        : Microsoft.Security/sqlVulnerabilityAssessments/scans
```

Example for using azure resource id parameters. Supported resources are:

- ARC: /subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/Microsoft.HybridCompute/machines/{machineName}

- VM:

/subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/Microsoft.Compute/virtualMachines/{machineName}

- On-Premise:

/subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/microsoft.operationalinsights/workspaces/{workspaceName}/onPremiseMachines/{machineName}

--- Example 4: Get scan summary using on premise parameters. ---

Get-AzSecuritySqlVulnerabilityAssessmentScanRecord -WorkspaceResourceId

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/ahabas-workspace -ComputerName ahabas-dev01.middleeast.corp.microsoft.com -AgentId 49640166-652f-4ee6-b48b-cfb840b8afe2 -VmUuid 4c4c4544-0030-4b10-8039-b8c04f4a3332 -WorkspaceId ba7c9d0e-a6e3-4997-b575-cf7a18a98a49 -Server AHABASDEV01SRV -Database master -ScanId bdbdf860-5d58-464b-ad9a-0125af63c162

```
TriggerType                 : Recurring
State                       : Failed
Server                      : AHABASDEV01SRV
Database                    : master
SqlVersion                  : 14.0.1000.169
StartTime                   : 3/17/2021 1:11:10 AM
EndTime                     : 12/31/9999 9:59:59 PM
HighSeverityFailedRulesCount   : 9
MediumSeverityFailedRulesCount : 2
LowSeverityFailedRulesCount    : 5
TotalPassedRulesCount          : 43
TotalFailedRulesCount          : 16
```

TotalRulesCount : 59

IsBaselineApplied : True

Id :

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsights/workspaces/aha

bas-workspace/onpremisemachines/ahabas-dev01.middleeast.corp.microsoft.com_49640166-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b8c04f4a3332/

sqlServers/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/bdbdf860-5d58-464b-ad9a-0125af63c162

Name : bdbdf860-5d58-464b-ad9a-0125af63c162

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans

Example for using on premise parameters.

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/az.security/get-azsecuritysqlvulnerabilityassessmentscanrecord