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

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

NAME

Get-AzSecuritySqlVulnerabilityAssessmentScanResult

SYNOPSIS

Gets SQL vulnerability assessment scan results.

SYNTAX

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

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

DESCRIPTION

Gets SQL vulnerability assessment scan results.

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

-RuleId <System.String>

Vulnerability assessment rule ID

Required? false

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.PSSqlVulnerabilityAssessmentScanResult

NOTES

Example 1: Get all results from latest scan on a SQL Database

Get-AzSecuritySqlVulnerabilityAssessmentScanResult -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

RuleId : VA1017
Status : NonFinding
IsTrimmed : False
QueryResults : {}
Remediation : {
Revoke EXECUTE permission on xp_cmdshell to all users (except dbo)
IsAutomated: False
Portal Link:
Script:
{}
}
BaselineAdjustedResult : {}
RuleMetadata : {

Rule id: VA1017

Severity: High

Category: AuthenticationAndAuthorization

Rule type: NegativeList

Title: Execute?permissions?on?xp_cmdshell?from?all?users?(except?dbo)?should?be?revoked.

Description:

The?xp_cmdshell?extended?stored?procedure?spawns?a?Windows?command?shell,?passing?in?a?string?for?execution.?This?rule?checks?th

at?no?users?(except?users?with?the?CONTROL?SERVER?permission?like?members?of?the?sysadmin?server?role)?have?permission?to?execute?the?xp_cmdshell?ext

ended?stored?procedure.

Rationale:

The?xp_cmdshell?extended?stored?procedure?is?a?very?powerful?tool,?but?because?of?that,?it?is?crucial?that?access?to?xp_cmdshell?be?tightly?controlled. By default,

only users with the CONTROL SERVER permission like members of the sysadmin server role can execute this extended stored procedure.

When?first?enabled,?xp_cmdshell?has?the?same?security?context?as?the?SQL?Server?service?account.?The?SQL?Server?service?acco

unt?is?often?more?privileged?than?necessary?for?the?work?being?performed?by?the?process?created?by?xp_cmdshell.?As?such,?malicious?users?can?attempt?

to?elevate?their?privileges?by?using?xp_cmdshell.

See?https://learn.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql?for?more?information?on?xp_cmdshell.

Query check:

{

Query:

SELECT dpr.name AS [Principal] FROM sys.database_permissions AS dp JOIN sys.database_principals AS dpr ON dp.grantee_principal_id =

dpr.principal_id WHERE major_id = OBJECT_ID('xp_cmdshell') AND dp.[type] = 'EX' AND [state] IN (C

,'W')

Column Names:

Expected Results:

{}}

Benchmark References:

{

Benchmark: FedRAMP

Reference:

}

}

Id :

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

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

rs/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/bdbdf860-5d58-464b-ad9a-0125af63c162/scanResults/VA1017

Name : VA1017

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans/scanResults

RuleId : VA1018

Status : Finding

IsTrimmed : False

QueryResults : {True}

Remediation : {

Install the latest SQL Server CU corresponding to your version of SQL Server. Go to https://technet.microsoft.com/en-us/sqlserver/ff803383.aspx to find and download the required CU.

IsAutomated: True

Portal Link:

Script:

{}

}

BaselineAdjustedResult : {}

RuleMetadata : {

Rule id: VA1018

Severity: High

Category: InstallationUpdatesAndPatches

Rule type: Binary

Title: Latest updates should be installed

Description: Microsoft periodically releases Cumulative Updates (CUs) for each version of SQL Server. This rule checks whether the latest CU

has been installed for the particular version of SQL Server being used.

Rationale: Running with the latest Cumulative Updates (CU) for any particular version of SQL Server is important as these CU are a

collection of all available patches up-to-date, including all known security fixes. Microsoft officially recommends ongoing, proactive installation of SQL

Server CUs as they become available.

Query check:

{

Query:

SELECT CASE WHEN Serverproperty('ProductVersion') >= '14.0.3356.20' THEN 0 ELSE 1 END AS [Violation]

Column Names:

Violation

Expected Results:

{False}}

Benchmark References:

{

Benchmark: CIS

Reference: v1.0.0-08-11-2017:1.1

}, {

Benchmark: FedRAMP

Reference:

}

}

...

In this example when the rule id is not specified all scan results all returned for the scan id in use.

-- Example 2: Get all results with scan id on a SQL Database --

Get-AzSecuritySqlVulnerabilityAssessmentScanResult -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 7db278d4-4629-4f75-ae0b-9c0e3d3b0816

RuleId : VA1017

Status : NonFinding

IsTrimmed : False

QueryResults : {}

Remediation : {

Revoke EXECUTE permission on xp_cmdshell to all users (except dbo)

IsAutomated: False

Portal Link:

Script:

{}

}

BaselineAdjustedResult : {}

RuleMetadata : {

Rule id: VA1017

Severity: High

Category: AuthenticationAndAuthorization

Rule type: NegativeList

Title:

Execute?permissions?on?xp_cmdshell?from?all?users?(except?dbo)?should?be?revoked.

Description:

The?xp_cmdshell?extended?stored?procedure?spawns?a?Windows?command?shell,?passin

g?in?a?string?for?execution.?This?rule?checks?that?no?users?(except?users?with?the?CONTROL?SER

VER?permission?like?members?of?the?sysadmin?server?role)?have?permission?to?execute?the?xp_cmd

shell?extended?stored?procedure.

Rationale: The?xp_cmdshell?extended?stored?procedure?is?a?very?powerful?tool,?but?because?o

f?that,?it?is?crucial?that?access?to?xp_cmdshell?be?tightly?controlled. By default, only

users with the CONTROL SERVER permission like members of the sysadmin server role can execute

this extended stored procedure. When?first?enabled,?xp_cmdshell?has?the?same?security?context?

as?the?SQL?Server?service?account.?The?SQL?Server?service?account?is?often?more?privileged?tha

n?necessary?for?the?work?being?performed?by?the?process?created?by?xp_cmdshell.?As?such,?malic

ious?users?can?attempt?to?elevate?their?privileges?by?using?xp_cmdshell. See?https://docs.micr

osoft.com/en-us/sql/relational-databases/system-stored-procedures/xp-cmdshell-transact-sql?for

?more?information?on?xp_cmdshell.

Query check:

{

Query:

```
SELECT dpr.name AS [Principal] FROM sys.database_permissions AS dp JOIN
sys.database_principals AS dpr     ON dp.grantee_principal_id = dpr.principal_id WHERE
major_id = OBJECT_ID('xp_cmdshell')     AND dp.[type] = 'EX'     AND [state] IN (         'G'
      ,'W'         )
```

Column Names:

Expected Results:

{}}

Benchmark References:

{

Benchmark: FedRAMP

Reference:

}

}

Id : /subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/micr

osoft.operationalinsights/workspaces/ahabas-workspace/onpremisemachines/ahabas-dev01.middleeas

t.corp.microsoft.com_49640166-652f-4ee6-b48b-cfb840b8afe2_4c4c4544-0030-4b10-8039-b8c04f4a3332

/sqlServers/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAsses

sments/default/scans/7db278d4-4629-4f75-ae0b-9c0e3d3b0816/scanResults/VA1017

Name : VA1017

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans/scanResults

...

Example 3: Get result on a specific rule from latest scan on SQL Database

Get-AzSecuritySqlVulnerabilityAssessmentScanResult -WorkspaceResourceId

/subscriptions/f26d1f13-67d5-4ad6-9012-67ca12d2436f/resourcegroups/ahmadtesting/providers/microsoft.operationalinsigh

ts/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 -RuleId "VA2108"

RuleId : VA2108

Status : Finding

IsTrimmed : False

QueryResults : {dbo db_owner SQL_USER}

Remediation : {

Remove members who should not have access to the database role

IsAutomated: True

Portal Link:

Script:

ALTER ROLE [db_owner] DROP MEMBER [dbo]

}

BaselineAdjustedResult : {

Status: Finding

Results not in baseline:

{dbo, db_owner, SQL_USER}

Results only in baseline:

{dbo, db_owner1, SQL_USER}

Baseline:

{

Update Time: 3/24/2021 3:59:39 PM

Expected Results:

{dbo, db_owner1, SQL_USER}}

}

RuleMetadata : {

Rule id: VA2108

Severity: High

Category: AuthenticationAndAuthorization

Rule type: BaselineExpected

Title: Minimal set of principals should be members of fixed high impact database roles

Description: SQL Server provides roles to help manage the permissions. Roles are security principals that group other principals.

Database-level roles are database-wide in their permission scope. This rule checks that a minimal set of principals are members of the fixed database roles.

Rationale: Fixed database roles may have administrative permissions on the system. Following the principle of least privilege, it is

important to minimize membership in fixed database roles and keep a baseline of these memberships. See

https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles for additional information on

database roles.

Query check:

{

Query:

SELECT user_name(sr.member_principal_id) as [Principal] ,user_name(sr.role_principal_id) as [Role] ,type_desc as [Principal Type]

FROM sys.database_role_members AS sr INNER JOIN sys.database_principals sp ON sp.principal_id = sr.member_principal_id WHERE sr.role_principal_id IN

(user_id('bulkadmin'), user_id('db_accessadmin'), user_id('db_securityadmin'),

user_id('db_ddladmin'), user_id('db_backupoperator'),

user_id('db_owner'))

Column Names:

Principal, Role, Principal Type

Expected Results:

{}}

Benchmark References:

{

Benchmark: FedRAMP

Reference:

}

}

Id :

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

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

rs/AHABASDEV01SRV/databases/master/providers/Microsoft.Security/sqlVulnerabilityAssessments/default/scans/bdbdf860-5d58-464b-ad9a-0125af63c162/scanResults/VA2108

Name : VA2108

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans/scanResults

Example for using on premise parameters. scan id is not specified so it gets results for latest.

Example 4: Get result on a specific rule using scan id parameter on SQL Database

Get-AzSecuritySqlVulnerabilityAssessmentScanResult -ResourceId /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 -WorkspaceId ba7c9d0e-a6e3-4997-b575-cf7a18a98a49 -Server AHABASDEV01SRV -Database master -ScanId 5cded390-68c4-4f5b-9ce6-b8a7a12b288b -RuleId "VA2108"

RuleId : VA2108

Status : Finding

IsTrimmed : False

QueryResults : {dbo db_owner SQL_USER}

Remediation : {

Remove members who should not have access to the database role

IsAutomated: True

Portal Link:

Script:

ALTER ROLE [db_owner] DROP MEMBER [dbo]

}

BaselineAdjustedResult : {

Status: NonFinding

Results not in baseline:{}

Results only in baseline:{}

Baseline:

{

Update Time: 12/20/2020 3:33:31 PM

Expected Results:

{dbo, db_owner, SQL_USER}

}

}

RuleMetadata : {

Rule id: VA2108

Severity: High

Category: AuthenticationAndAuthorization

Rule type: BaselineExpected

Title: Minimal set of principals should be members of fixed high impact database roles

Description: SQL Server provides roles to help manage the permissions. Roles are security principals that group other principals. Database-level roles are database-wide in their permission scope. This rule checks that a minimal set of principals are members of the fixed database roles.

Rationale: Fixed database roles may have administrative permissions on the system. Following the principle of least privilege, it is important to minimize membership in fixed database roles and keep a baseline of these memberships. See https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles for additional information on database roles.

Query check:

{

Query:

SELECT user_name(sr.member_principal_id) as [Principal] ,user_name(sr.role_principal_id) as [Role] ,type_desc as [Principal Type] FROM sys.database_role_members AS sr INNER JOIN sys.database_principals sp ON sp.principal_id = sr.member_principal_id WHERE sr.role_principal_id IN (user_id('bulkadmin'),

user_id('db_accessadmin'), user_id('db_securityadmin'),

user_id('db_ddladmin'),

user_id('db_backupoperator'), user_id('db_owner'))

Column Names:

Principal, Role, Principal Type

Expected Results:

{}

}

Benchmark References:

{

Benchmark: FedRAMP

Reference:

}

}

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/5cded390-68c4-4f5b-9ce6-b8a7a12b288b/scanResults/VA2108

Name : VA2108

Type : Microsoft.Security/sqlVulnerabilityAssessments/scans/scanResults

Example of using resource id parameter set. 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}

RELATED LINKS

Online Version:

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