Windows PowerShell Get-Help on Cmdlet 'Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline'

PS:\>Get-HELP Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline -Full

NAME

Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline

SYNOPSIS

Sets the vulnerability assessment rule baseline.

SYNTAX

Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline [-ResourceGroupName] <System.String> [-WorkspaceName] <System.String> [-Name] <System.String> [-AsJob] -BaselineResult <System.String[][]> [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-InputObject <Microsoft.Azure.Commands.Synapse.Models.VulnerabilityAssessment.VulnerabilityAssessmentRuleBaselineModel>] [-RuleAppliesToMaster] -RuleId <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline cmdlet sets the vulnerability assessment rule baseline. As you review your assessment results, you can

mark specific results as being an acceptable Baseline in your environment. The baseline is essentially a customization of how the results are reported. Results that

match the baseline are considered as passing in subsequent scans. Once you have established your baseline security state, vulnerability assessment only reports on

deviations from the baseline, and you can focus your attention on the relevant issues. Note that you need to run Enable-AzSynapseSqlAdvancedDataSecurity and

Update-AzSynapseSqlVulnerabilityAssessmentSetting cmdlet as a prerequisite for using this cmdlet.

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

-BaselineResult <System.String[][]>

The results to set as baseline for the rule in all future scans

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

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.Synapse.Models.VulnerabilityAssessment.VulnerabilityAssessmentRuleBaselineModel>

The Vulnerability Assessment rule baseline object to set

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? 2

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceGroupName <System.String>

Resource group name.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-RuleAppliesToMaster <System.Management.Automation.SwitchParameter>

Specifies whether the baseline results should apply on a workspace level rule identified by the RuleId

Required? false

Position? named

Default value False

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-RuleId <System.String>

The rule ID which identifies the rule to set the baseline results to.

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? 1

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.VulnerabilityAssessment.VulnerabilityAssessmentRuleBaselineModel

System.String[][]

System.Management.Automation.SwitchParameter

OUTPUTS

Microsoft.Azure.Commands.Synapse.Models.VulnerabilityAssessment.SqlPoolVulnerabilityAssessmentRuleBaselineModel

NOTES

--- Example 1: Set a vulnerability assessment rule baseline ---

```
Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline  `
  -ResourceGroupName "ContosoResourceGroup" `
  -WorkspaceName "ContosoWorkspace"  `
  -SqlPoolName "ContosoSqlPool"  `
  -RuleId "VA2108" `
  -RuleAppliesToMaster `
   -BaselineResult @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None')  , @( 'Principal2', 'db_ddladmin', 'SQL_USER', 'None')

ResourceGroupName  : ContosoResourceGroup
WorkspaceName      : ContosoWorkspace
SqlPoolName        : ContosoSqlPool
RuleId             : VA2108
RuleAppliesToMaster     : True
BaselineResult     : @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None')  , @( 'Principal2', 'db_ddladmin', 'SQL_USER', 'None')
```

BaselineResult value is a composition of several sub arrays that described the T-SQL results that will be added to the baseline.

You may find the Scan results under the storage defined by the Update-AzSynapseSqlVulnerabilityAssessmentSetting cmdlet, under

scans/{WorkspaceName}/{SqlPoolName}/scan_{ScanId}.json

Example 2: Set a vulnerability assessment rule baseline from a baseline object

```
Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline `
        -ResourceGroupName "ContosoResourceGroup" `
        -WorkspaceName "ContosoWorkspace" `
        -SqlPoolName "ContosoSqlPool" `
        -RuleId "VA2108" `
                -BaselineResult @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin', 'SQL_USER', 'None')

Get-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline `
        -ResourceGroupName "ContosoResourceGroup" `
        -WorkspaceName "ContosoWorkspace" `
        -SqlPoolName "ContosoSqlPool" `
        -RuleId "VA2108" `
        | Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline `
           -ResourceGroupName "ResourceGroup02" `
           -WorkspaceName "Server02" `
           -SqlPoolName "ContosoSqlPool02"

ResourceGroupName  : ResourceGroup02
WorkspaceName      : Server02
SqlPoolName        : ContosoSqlPool02
RuleId             : VA2108
RuleAppliesToMaster : False
BaselineResult     : @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin', 'SQL_USER', 'None')
```

Example 3: Set a vulnerability assessment rule baseline on all the SQL pools under a workspace

```
Get-AzSynapseSqlPool -ResourceGroupName "ContosoResourceGroup" `
        -WorkspaceName "ContosoWorkspace" `
        | Where-Object {$_.Name -ne "master"} `
        | Set-AzSynapseSqlPoolVulnerabilityAssessmentRuleBaseline `
            -RuleId "VA2108" `
                -BaselineResult @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin',
'SQL_USER', 'None')

ResourceGroupName : ContosoResourceGroup
WorkspaceName : ContosoWorkspace
SqlPoolName : ContosoSqlPool
RuleId : VA2108
RuleAppliesToMaster : False
BaselineResult : @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin', 'SQL_USER',
'None')

ResourceGroupName : ContosoResourceGroup
WorkspaceName : ContosoWorkspace
SqlPoolName : ContosoSqlPool02
RuleId : VA2108
RuleAppliesToMaster : False
BaselineResult : @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin', 'SQL_USER',
'None')
```

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/az.synapse/set-azsynapsesqlpoolvulnerabilityassessmentrulebaseline