



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

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

NAME

Set-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline

SYNOPSIS

Sets the vulnerability assessment rule baseline.

SYNTAX

```
Set-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline [-ResourceGroupName] <System.String>
[-InstanceName] <System.String> [-DatabaseName] <System.String>
-BaselineResult <System.String[][]> [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-RuleAppliesToMaster]
-RuleId <System.String> [-Confirm] [-WhatIf] [<CommonParameters>]
```

```
Set-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline [-ResourceGroupName] <System.String>
-BaselineResult <System.String[][]> [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-InputObject
<Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.VulnerabilityAssessmentRuleBaselineModel>]
[-RuleAppliesToMaster] -RuleId <System.String> [-Confirm]
[-WhatIf] [<CommonParameters>]
```

DESCRIPTION

The `Set-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline` 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-AzSqlInstanceAdvancedDataSecurity` and `Update-AzSqlInstanceVulnerabilityAssessmentSetting` cmdlet as a prerequisite for using this cmdlets.

PARAMETERS

`-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

`-DatabaseName <System.String>`

SQL Managed Database name.

Required? true

Position? 2

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.Sql.VulnerabilityAssessment.Model.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

-InstanceName <System.String>

SQL Managed Instance name.

Required? true

Position? 1

Default value None

Accept pipeline input? True (ByPropertyName)

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

-RuleAppliesToMaster <System.Management.Automation.SwitchParameter>

Specifies whether the baseline results should apply on a server 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

-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.Sql.VulnerabilityAssessment.Model.VulnerabilityAssessmentRuleBaselineModel

System.String[]

System.Management.Automation.SwitchParameter

OUTPUTS

Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.ManagedDatabaseVulnerabilityAssessmentRuleBaselineModel

NOTES

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

```
Set-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline `
```

```
-ResourceGroupName "ResourceGroup01" `
```

```
-InstanceName "ManagedInstance01" `
```

```
-DatabaseName "Database01" `
```

```
-RuleId "VA2108" `
```

```
-RuleAppliesToMaster `
```

```
-BaselineResult @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin', 'SQL_USER',  
'None')
```

ResourceGroupName : ResourceGroup01

InstanceName : ManagedInstance01

DatabaseName : Database01

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-AzSqlInstanceVulnerabilityAssessmentSetting cmdlet, under

scans/{ManagedInstanceName}/{ManagedDatabaseName}/scan_{ScanId}.json

```

Set-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline `
    -ResourceGroupName "ResourceGroup01" `
    -InstanceName "ManagedInstance01" `
    -DatabaseName "Database01" `
    -RuleId "VA2108" `
    -BaselineResult @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin',
'SQL_USER', 'None')

```

```

Get-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline `
    -ResourceGroupName "ResourceGroup01" `
    -InstanceName "ManagedInstance01" `
    -DatabaseName "Database01" `
    -RuleId "VA2108" `
| Set-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline `
    -ResourceGroupName "ResourceGroup02" `
    -InstanceName "ManagedInstance02" `
    -DatabaseName "Database02"

```

```

ResourceGroupName : ResourceGroup02
InstanceName      : ManagedInstance02
DatabaseName      : Database02
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 databases under a managed instance

```

Get-AzSqlInstanceDatabase -ResourceGroupName "ResourceGroup01" `

```

```
-InstanceName "ManagedInstance01" `
| Where-Object {$_.Name -ne "master"} `
| Set-AzSqlInstanceDatabaseVulnerabilityAssessmentRuleBaseline `
    -RuleId "VA2108" `
    -BaselineResult @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin',
'SQL_USER', 'None')
```

```
ResourceGroupName : ResourceGroup01
InstanceName      : ManagedInstance01
DatabaseName      : Database01
RuleId            : VA2108
RuleAppliesToMaster : False
BaselineResult    : @( 'Principal1', 'db_ddladmin', 'SQL_USER', 'None') , @( 'Principal2', 'db_ddladmin', 'SQL_USER',
'None')
```

```
ResourceGroupName : ResourceGroup01
InstanceName      : ManagedInstance01
DatabaseName      : Database02
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.sql/set-azsqlinstancedatabasevulnerabilityassessmentrulebaseline>