Windows PowerShell Get-Help on Cmdlet 'Convert-AzSqlDatabaseVulnerabilityAssessmentScan'

PS:\>Get-HELP Convert-AzSqlDatabaseVulnerabilityAssessmentScan -Full

NAME

Convert-AzSqlDatabaseVulnerabilityAssessmentScan

SYNOPSIS

Converts a vulnerability assessment scan results to Excel format.

SYNTAX

Convert-AzSqlDatabaseVulnerabilityAssessmentScan [-ResourceGroupName] <System.String> [-ServerName] <System.String> [-DatabaseName] <System.String> [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-InputObject <Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.VulnerabilityAssessmentScanRecordModel>] [-ScanId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Convert-AzSqlDatabaseVulnerabilityAssessmentScan cmdlet converts a scan results, that resides in the customer storage, identified by the ScanId parameter to an Excel format placed in the storage defined by the Set-AzSqlServerVulnerabilityAssessmentSettings cmdlet. Note that you

need to run

Enable-AzSqlServerAdvancedDataSecurity and Update-AzSqlServerVulnerabilityAssessmentSetting cmdlet as a prerequisite for using this cmdlets.

PARAMETERS

-DatabaseName <System.String>

SQL 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.VulnerabilityAssessmentScanRecordModel>

The scan record object to use in order to convert a Vulnerability Assessment scan

Required? false

Position? named

Default value None

Accept pipeline input? True (ByValue)

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

-ServerName <System.String>

SQL Database server name.

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.Sql.VulnerabilityAssessment.Model.VulnerabilityAssessmentScanRecordModel

OUTPUTS

Microsoft.Azure.Commands.Sql.VulnerabilityAssessment.Model.DatabaseVulnerabilityAssessmentScanExportModel

NOTES

Example 1: Converts vulnerability assessment scan results and saves them to local disk

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
        -ResourceGroupName "ResourceGroup01" `
        -ServerName "Server01" `
        -StorageAccountName "mystorage"

Start-AzSqlDatabaseVulnerabilityAssessmentScan `
        -ResourceGroupName "ResourceGroup01" `
        -ServerName "Server01" `
        -DatabaseName "Database01" `
        -ScanId "myScan"

$convert_scan_results = Convert-AzSqlDatabaseVulnerabilityAssessmentScan `
        -ResourceGroupName "ResourceGroup01" `
        -ServerName "Server01" `
        -DatabaseName "Database01" `
        -ScanId "myScan"
ResourceGroupName  : "ResourceGroup01"
ServerName         : "Server01"
DatabaseName       : "Database01"
ScanId             : "myScan"
                                                                    ExportedReportLocation :
"https://myaccount.blob.core.windows.net/vulnerabilityAssessment/Server01/Database01/scan_myScan.xlsx"

$connection_string_to_storage_account = "DefaultEndpointsProtocol=https;AccountName=myaccount...."
$converted_scan_results_download_local_folder = "C:\Downloads\"
$storage_account_context = New-AzStorageContext -ConnectionString $connection_string_to_storage_account
$convert_scan_result_splitted = $convert_scan_results.ExportedReportLocation -split "/"
```

```
$container_name = $convert_scan_result_splitted[3]
Get-AzStorageBlobContent -Blob ($a -split $container_name + '/')[1] `
    -Container $container_name `
    -Destination $converted_scan_results_download_local_folder `
    -Context $storage_account_context
```

Example 2: Converts a vulnerability assessment scan results from a scan record

```
Get-AzSqlDatabaseVulnerabilityAssessmentScanRecord `
            -ResourceGroupName "ResourceGroup01" `
            -ServerName "Server01" `
            -DatabaseName "Database01" `
            -ScanId "myScan" `
            | Convert-AzSqlDatabaseVulnerabilityAssessmentScan

ResourceGroupName  : "ResourceGroup01"
ServerName         : "Server01"
DatabaseName       : "Database01"
ScanId             : "myScan"
ExportedReportLocation : "https://myaccount.blob.core.windows.net/vulnerabilityAssessment/Server01/Database01
                         /scan_myScan.xlsx"
```

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.sql/convert-azsqldatabasevulnerabilityassessmentscan