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

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

NAME

Set-AzSynapseSqlAuditSetting

SYNOPSIS

Changes the auditing settings of an Azure Synapse Analytics Workspace.

SYNTAX

Set-AzSynapseSqlAuditSetting [[-ResourceGroupName] <System.String>] [-WorkspaceName] <System.String> [-AsJob] [-AuditActionGroup {BATCH_STARTED_GROUP | BATCH_COMPLETED_GROUP | APPLICATION_ROLE_CHANGE_PASSWORD_GROUP | BACKUP_RESTORE_GROUP | DATABASE_LOGOUT_GROUP | DATABASE_OBJECT_CHANGE_GROUP | DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP | DATABASE_OBJECT_PERMISSION_CHANGE_GROUP | DATABASE_OPERATION_GROUP | DATABASE_PERMISSION_CHANGE_GROUP | DATABASE_PRINCIPAL_CHANGE_GROUP | DATABASE_PRINCIPAL_IMPERSONATION_GROUP | DATABASE_ROLE_MEMBER_CHANGE_GROUP | FAILED_DATABASE_AUTHENTICATION_GROUP | SCHEMA_OBJECT_ACCESS_GROUP | SCHEMA_OBJECT_CHANGE_GROUP | SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP | SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP | SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP | USER_CHANGE_PASSWORD_GROUP}] [-BlobStorageTargetState {Enabled | Disabled}] [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-EventHubAuthorizationRuleResourceId <System.String>] [-EventHubName <System.String>] [-EventHubTargetState {Enabled | Disabled}] [-LogAnalyticsTargetState {Enabled | Disabled}] [-PassThru] [-PredicateExpression <System.String>] [-RetentionInDays <System.Nullable`1[System.UInt32]>] [-StorageAccountResourceId <System.String>] [-StorageKeyType {Primary | Secondary}] [-WorkspaceResourceId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Set-AzSynapseSqlAuditSetting [-AsJob] [-AuditActionGroup {BATCH_STARTED_GROUP | BATCH_COMPLETED_GROUP | APPLICATION_ROLE_CHANGE_PASSWORD_GROUP | BACKUP_RESTORE_GROUP | DATABASE_LOGOUT_GROUP | DATABASE_OBJECT_CHANGE_GROUP | DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP | DATABASE_OBJECT_PERMISSION_CHANGE_GROUP | DATABASE_OPERATION_GROUP | DATABASE_PERMISSION_CHANGE_GROUP | DATABASE_PRINCIPAL_CHANGE_GROUP | DATABASE_PRINCIPAL_IMPERSONATION_GROUP | DATABASE_ROLE_MEMBER_CHANGE_GROUP | FAILED_DATABASE_AUTHENTICATION_GROUP | SCHEMA_OBJECT_ACCESS_GROUP | SCHEMA_OBJECT_CHANGE_GROUP | SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP | SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP | SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP | USER_CHANGE_PASSWORD_GROUP}] [-BlobStorageTargetState {Enabled | Disabled}] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-EventHubAuthorizationRuleResourceId <System.String>] [-EventHubName <System.String>] [-EventHubTargetState {Enabled | Disabled}] [-LogAnalyticsTargetState {Enabled | Disabled}] [-PassThru] [-PredicateExpression <System.String>] -ResourceId <System.String> [-RetentionInDays <System.Nullable`1[System.UInt32]>] [-StorageAccountResourceId <System.String>] [-StorageKeyType {Primary | Secondary}] [-WorkspaceResourceId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

Set-AzSynapseSqlAuditSetting [-AsJob] [-AuditActionGroup {BATCH_STARTED_GROUP | BATCH_COMPLETED_GROUP | APPLICATION_ROLE_CHANGE_PASSWORD_GROUP | BACKUP_RESTORE_GROUP | DATABASE_LOGOUT_GROUP | DATABASE_OBJECT_CHANGE_GROUP | DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP | DATABASE_OBJECT_PERMISSION_CHANGE_GROUP |

DATABASE_OPERATION_GROUP |

DATABASE_PERMISSION_CHANGE_GROUP | DATABASE_PRINCIPAL_CHANGE_GROUP | DATABASE_PRINCIPAL_IMPERSONATION_GROUP | DATABASE_ROLE_MEMBER_CHANGE_GROUP |

FAILED_DATABASE_AUTHENTICATION_GROUP | SCHEMA_OBJECT_ACCESS_GROUP | SCHEMA_OBJECT_CHANGE_GROUP | SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP |

SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP | SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP | USER_CHANGE_PASSWORD_GROUP}] [-BlobStorageTargetState {Enabled | Disabled}]

[-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-EventHubAuthorizationRuleResourceId <System.String>]

[-EventHubName <System.String>] [-EventHubTargetState {Enabled | Disabled}] [-LogAnalyticsTargetState {Enabled | Disabled}] [-PassThru] [-PredicateExpression

<System.String>] [-RetentionInDays <System.Nullable`1[System.UInt32]>] [-StorageAccountResourceId <System.String>] [-StorageKeyType {Primary | Secondary}]

-WorkspaceObject <Microsoft.Azure.Commands.Synapse.Models.PSSynapseWorkspace> [-WorkspaceResourceId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-AzSynapseSqlAuditSetting cmdlet changes the auditing settings of an Azure Synapse Analytics Workspace. When blob storage is a destination for audit logs,

specify the StorageAccountResourceId parameter to determine the storage account for the audit logs and the StorageKeyType parameter to define the storage keys. You

can also define retention for the audit logs by setting the value of the RetentionInDays parameter to define the period for the audit logs.

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

-AuditActionGroup <Microsoft.Azure.Commands.Synapse.Models.Auditing.AuditActionGroups[]>

The recommended set of action groups to use is the following combination - this will audit all the queries and stored procedures executed against the database, as

well as successful and failed logins:

"BATCH_COMPLETED_GROUP",

"SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP",

"FAILED_DATABASE_AUTHENTICATION_GROUP"

This above combination is also the set that is configured by default. These groups cover all SQL statements and stored procedures executed against the database,

and should not be used in combination with other groups as this will result in duplicate audit logs.

For more information, see

https://learn.microsoft.com/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions#database-level-audit-action-groups.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-BlobStorageTargetState <System.String>

Indicates whether blob storage is a destination for audit records.

Required? false

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

-EventHubAuthorizationRuleResourceId <System.String>

The resource Id for the event hub authorization rule

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EventHubName <System.String>

The name of the event hub. If none is specified when providing EventHubAuthorizationRuleResourceId, the default event hub will be selected.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EventHubTargetState <System.String>

Indicates whether event hub is a destination for audit records.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-LogAnalyticsTargetState <System.String>

Indicates whether log analytics is a destination for audit records.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PassThru <System.Management.Automation.SwitchParameter>

This Cmdlet does not return an object by default. If this switch is specified, it returns true if successful.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-PredicateExpression <System.String>

The T-SQL predicate (WHERE clause) used to filter audit logs.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

Resource group name.

Required? false

Position? 0

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceId <System.String>

Resource identifier of Synapse workspace.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RetentionInDays <System.Nullable`1[System.UInt32]>

The number of retention days for the audit logs.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-StorageAccountResourceId <System.String>

The storage account resource id

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-StorageKeyType <System.String>

Specifies which of the storage access keys to use.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-WorkspaceName <System.String>

Name of Synapse workspace.

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-WorkspaceObject <Microsoft.Azure.Commands.Synapse.Models.PSSynapseWorkspace>

workspace input object, usually passed through the pipeline.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-WorkspaceResourceId <System.String>

The workspace ID (resource ID of a Log Analytics workspace) for a Log Analytics workspace to which you would like to send Audit Logs. Example:

/subscriptions/4b9e8510-67ab-4e9a-95a9-e2f1e570ea9c/resourceGroups/insights-integration/providers/Microsoft.OperationalInsights/workspaces/viruela2

Required? false

Position? named

Default value None

Accept pipeline input? False

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

Microsoft.Azure.Commands.Synapse.Models.PSSynapseWorkspace

OUTPUTS

Microsoft.Azure.Commands.Synapse.Models.WorkspaceAuditModel

NOTES

---------- Example 1 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -BlobStorageTargetState Enabled -StorageAccountResourceId

"/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/resourcegroup01/providers/Microsoft.Storage/storageAccounts/mystorage" -StorageKeyType Primary

Enable the blob storage auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace.

---------- Example 2 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -BlobStorageTargetState Disabled

Disable the blob storage auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace.

---------- Example 3 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -BlobStorageTargetState Enabled -StorageAccountResourceId

"/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/resourcegroup01/providers/Microsoft.Storage/storageAccounts/mystorage" -StorageKeyType Primary

-PredicateExpression "statement <> 'select 1'"

Enable the blob storage auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace with advanced filtering using a T-SQL predicate.

---------- Example 4 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -PredicateExpression ""

Remove the advanced filtering setting from the auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace.

---------- Example 5 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -EventHubTargetState Enabled -EventHubName "EventHubName" -EventHubAuthorizationRuleResourceId

"EventHubAuthorizationRuleResourceId"

Enable the event hub auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace.

---------- Example 6 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -EventHubTargetState Disabled

Disable the event hub auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace.

---------- Example 7 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -LogAnalyticsTargetState Enabled -WorkspaceResourceId

"/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/insights-integration/providers/Microsoft.OperationalInsights/workspaces/myworkspace"

Enable the log analytics auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace.

---------- Example 8 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -LogAnalyticsTargetState Disabled

Disable the log analytics auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace.

---------- Example 9 ----------

Get-AzSynapseWorkspace -Name ContosoWorkspace | Set-AzSynapseSqlAuditSetting -BlobStorageTargetState Disabled

Disable the blob storage auditing policy of an Azure Synapse Analytics Workspace named ContosoWorkspace through pipeline.

---------- Example 10 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -LogAnalyticsTargetState Enabled -WorkspaceResourceId

"/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/insights-integration/providers/Microsoft.OperationalInsights/workspaces/myworkspace"
-BlobStorageTargetState Disabled

Disable sending audit records of an Azure Synapse Analytics Workspace to blob storage, and enable sending them to log analytics.

---------- Example 11 ----------

Set-AzSynapseSqlAuditSetting -WorkspaceName ContosoWorkspace -BlobStorageTargetState Enabled -StorageAccountResourceId

"/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/resourcegroup01/providers/Microsoft.Storage/storageAccounts/mystorage" -EventHubTargetState
Enabled -EventHubName "EventHubName" -EventHubAuthorizationRuleResourceId "EventHubAuthorizationRuleResourceId" -LogAnalyticsTargetState Enabled -WorkspaceResourceId

"/subscriptions/4b9e8510-67ab-4e9a-95a9-e2f1e570ea9c/resourceGroups/insights-integration/providers/Microsoft.OperationalInsights/workspaces/viruela2"

Enable sending audit records of an Azure Synapse Analytics Workspace to blob storage, event hub and log analytics.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.synapse/set-azsynapsesqlauditsetting