Windows PowerShell Get-Help on Cmdlet 'New-AzSecurityDefenderCspmAwsOfferingObject'

PS:\>Get-HELP New-AzSecurityDefenderCspmAwsOfferingObject -Full

NAME

New-AzSecurityDefenderCspmAwsOfferingObject

SYNOPSIS

Create an in-memory object for DefenderCspmAwsOffering.

SYNTAX

New-AzSecurityDefenderCspmAwsOfferingObject [-CiemDiscoveryCloudRoleArn <String>] [-CiemOidcAzureActiveDirectoryAppName <String>] [-CiemOidcCloudRoleArn <String>] [-ConfigurationCloudRoleArn <String>] [-ConfigurationExclusionTag <IDefenderCspmAwsOfferingVMScannersConfigurationExclusionTags>] [-ConfigurationScanningMode <String>] [-DataSensitivityDiscoveryCloudRoleArn <String>] [-DataSensitivityDiscoveryEnabled <Boolean>] [-DatabaseDspmCloudRoleArn <String>] [-DatabaseDspmEnabled <Boolean>] [-MdcContainerAgentlessDiscoveryK8SCloudRoleArn <String>] [-MdcContainerAgentlessDiscoveryK8SEnabled <Boolean>] [-MdcContainerImageAssessmentCloudRoleArn <String>] [-MdcContainerImageAssessmentEnabled <Boolean>] [-VMScannerEnabled <Boolean>] [<CommonParameters>]

DESCRIPTION

Create an in-memory object for DefenderCspmAwsOffering.

PARAMETERS

-CiemDiscoveryCloudRoleArn <String>

The cloud role ARN in AWS for CIEM discovery.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-CiemOidcAzureActiveDirectoryAppName <String>

the azure active directory app name used of authenticating against AWS.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-CiemOidcCloudRoleArn <String>

The cloud role ARN in AWS for CIEM oidc connection.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ConfigurationCloudRoleArn <String>

The cloud role ARN in AWS for this feature.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ConfigurationExclusionTag <IDefenderCspmAwsOfferingVMScannersConfigurationExclusionTags>

VM tags that indicates that VM should not be scanned.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ConfigurationScanningMode <String>

The scanning mode for the VM scan.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSensitivityDiscoveryCloudRoleArn <String>

The cloud role ARN in AWS for this feature.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSensitivityDiscoveryEnabled <Boolean>

Is Microsoft Defender Data Sensitivity discovery enabled.

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-DatabaseDspmCloudRoleArn <String>

The cloud role ARN in AWS for this feature.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DatabaseDspmEnabled <Boolean>

Is databases DSPM protection enabled.

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-MdcContainerAgentlessDiscoveryK8SCloudRoleArn <String>

The cloud role ARN in AWS for this feature.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-MdcContainerAgentlessDiscoveryK8SEnabled <Boolean>

Is Microsoft Defender container agentless discovery K8s enabled.

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-MdcContainerImageAssessmentCloudRoleArn <String>

The cloud role ARN in AWS for this feature.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-MdcContainerImageAssessmentEnabled <Boolean>

Is Microsoft Defender container image assessment enabled.

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-VMScannerEnabled <Boolean>

Is Microsoft Defender for Server VM scanning enabled.

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

OUTPUTS

Microsoft.Azure.PowerShell.Cmdlets.Security.Models.DefenderCspmAwsOffering

NOTES

COMPLEX PARAMETER PROPERTIES

To create the parameters described below, construct a hash table containing the appropriate properties. For information on hash tables, run Get-Help

about_Hash_Tables.

CONFIGURATIONEXCLUSIONTAG <IDefenderCspmAwsOfferingVMScannersConfigurationExclusionTags>: VM tags that indicates that VM should not be scanned.

[(Any) <String>]: This indicates any property can be added to this object.

---------- EXAMPLE 1 ----------

PS C:\>$arnPrefix = "arn:aws:iam::123456789012:role"

New-AzSecurityDefenderCspmAwsOfferingObject `

-VMScannerEnabled $true -ConfigurationScanningMode Default -ConfigurationCloudRoleArn "$arnPrefix/DefenderForCloud-AgentlessScanner" -ConfigurationExclusionTag

@{key="value"} `

-DataSensitivityDiscoveryEnabled $true -DataSensitivityDiscoveryCloudRoleArn "$arnPrefix/SensitiveDataDiscovery" `

-DatabaseDspmEnabled $true -DatabaseDspmCloudRoleArn "$arnPrefix/DefenderForCloud-DataSecurityPostureDB" `

-CiemDiscoveryCloudRoleArn "$arnPrefix/DefenderForCloud-Ciem" -CiemOidcAzureActiveDirectoryAppName "mciem-aws-oidc-connector" -CiemOidcCloudRoleArn

"$arnPrefix/DefenderForCloud-OidcCiem" `

-MdcContainerImageAssessmentEnabled $true -MdcContainerImageAssessmentCloudRoleArn "$arnPrefix/MDCContainersImageAssessmentRole" `

-MdcContainerAgentlessDiscoveryK8SEnabled $true -MdcContainerAgentlessDiscoveryK8SCloudRoleArn "$arnPrefix/MDCContainersAgentlessDiscoveryK8sRole"

RELATED LINKS

https://learn.microsoft.com/powershell/module/Az.Security/new-azsecuritydefendercspmawsofferingobject