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

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

NAME

New-AzKeyVaultManagedHsm

SYNOPSIS

Creates a managed HSM.

SYNTAX

New-AzKeyVaultManagedHsm [-Name] <System.String> [-ResourceGroupName] <System.String> [-Location] <System.String> [-Administrator] <System.String[]> [-AsJob]

[-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-EnablePurgeProtection] [-PublicNetworkAccess

<System.String>] [-Sku <System.String>] -SoftDeleteRetentionInDays <System.Int32> [-SubscriptionId <System.String>] [-Tag <System.Collections.Hashtable>]

[-UserAssignedIdentity <System.String[]>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzKeyVaultManagedHsm cmdlet creates a managed HSM in the specified resource group. To add, remove, or list keys in the managed HSM, user should: 1. grant

permissions by adding user ID to Administrator; 2. add role assignment for user like "Managed HSM Crypto User" and so on; 3. back up security domain data of a managed

HSM using `Export-AzKeyVaultSecurityDomain`.

PARAMETERS

-Administrator <System.String[]>

Initial administrator object id for this managed HSM pool.

Required? true

Position? 3

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-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

-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

-EnablePurgeProtection <System.Management.Automation.SwitchParameter>

specifying whether protection against purge is enabled for this managed HSM pool. The setting is effective only if soft delete is also enabled. Enabling this

functionality is irreversible.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Location <System.String>

Specifies the Azure region in which to create the key vault. Use the command Get-AzResourceProvider with the ProviderNamespace parameter to see your choices.

Required? true

Position? 2

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Name <System.String>

Specifies a name of the managed HSM to create. The name can be any combination of letters, digits, or hyphens. The name must start and end with a letter or digit.

The name must be universally unique.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-PublicNetworkAccess <System.String>

Controls permission for data plane traffic coming from public networks while private endpoint is enabled.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-ResourceGroupName <System.String>

Specifies the name of an existing resource group in which to create the key vault.

Required? true
Position? 1
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-Sku <System.String>

Specifies the SKU of the managed HSM instance.

Required? false
Position? named
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-SoftDeleteRetentionInDays <System.Int32>

Specifies how long the deleted managed hsm pool is retained, and how long until the managed hsm pool in the deleted state can be purged.

Required? true
Position? named
Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SubscriptionId <System.String>

The ID of the subscription. By default, cmdlets are executed in the subscription that is set in the current context. If the user specifies another subscription,

the current cmdlet is executed in the subscription specified by the user. Overriding subscriptions only take effect during the lifecycle of the current cmdlet. It

does not change the subscription in the context, and does not affect subsequent cmdlets.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Tag <System.Collections.Hashtable>

A hash table which represents resource tags.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-UserAssignedIdentity <System.String[]>

The set of user assigned identities associated with the managed HSM. Its value will be ARM resource ids in the form:

'/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.ManagedIdentity/userAssignedIdentities/{identityName}'.

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

System.String

System.String[]

System.Collections.Hashtable

OUTPUTS

Microsoft.Azure.Commands.KeyVault.Models.PSManagedHsm

NOTES

---------- Example 1: Create a StandardB1 managed HSM ----------

New-AzKeyVaultManagedHsm -Name 'myhsm' -ResourceGroupName 'myrg1' -Location 'eastus2euap' -Administrator "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
-SoftDeleteRetentionInDays 70

Name Resource Group Name Location SKU
---- ------------------- -------- ---
myhsm myrg1 eastus2euap StandardB1

This command creates a managed HSM named myhsm in the location eastus2euap. The command adds the managed HSM to the resource group named myrg1. Because the command
does not specify a value for the SKU parameter, it creates a Standard_B1 managed HSM.

---------- Example 2: Create a CustomB32 managed HSM ----------

New-AzKeyVaultManagedHsm -Name 'myhsm' -ResourceGroupName 'myrg1' -Location 'eastus2euap' -Administrator "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" -Sku 'CustomB32'

-SoftDeleteRetentionInDays 70

Name Resource Group Name Location SKU

---- ------------------- -------- ---

myhsm myrg1 eastus2euap CustomB32

This command creates a managed HSM, just like the previous example. However, it specifies a value of CustomB32 for the SKU parameter to create a CustomB32 managed HSM.

Example 3: Create a managed HSM with an user assigned identity

New-AzKeyVaultManagedHsm -Name 'myhsm' -ResourceGroupName 'myrg1' -Location 'eastus2euap' -Administrator "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"-SoftDeleteRetentionInDays 70 -UserAssignedIdentity /subscriptions/xxxx/resourceGroups/xxxx/providers/Microsoft.ManagedIdentity/userAssignedIdentities/identityName | Format-List

Managed HSM Name : myhsm

Resource Group Name : myrg1

Location : eastus2euap

Resource ID : /subscriptions/0b1f6471-1bf0-4dda-aec3-cb9272f09590/resourceGroups/bez-rg/providers/Microsoft.KeyVault/managedHSMs/bezmhsm

HSM Pool URI :

Tenant ID : 54826b22-38d6-4fb2-bad9-b7b93a3e9c5a

Initial Admin Object Ids : {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}

SKU : StandardB1

Soft Delete Enabled? : True

Enabled Purge Protection? : False

Soft Delete Retention Period (days) : 70

Public Network Access : Enabled

IdentityType : UserAssigned

UserAssignedIdentities :

/subscriptions/xxxx/resourceGroups/xxxx/providers/Microsoft.ManagedIdentity/userAssignedIdentities/identityName

Provisioning State : Succeeded

Status Message : The Managed HSM is provisioned and ready to use.

Security Domain ActivationStatus : Active

Security Domain ActivationStatusMessage : Your HSM has been activated and can be used for cryptographic operations.

Regions :

Tags

This command creates a managed HSM with an user assigned identity.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.keyvault/new-azkeyvaultmanagedhsm

Get-AzKeyVaultManagedHsm

Remove-AzKeyVaultManagedHsm

Update-AzKeyVaultManagedHsm

Undo-AzKeyVaultManagedHsmRemoval