Full credit is given to all the above companies including the Operating System that this PDF file was generated!

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

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

NAME

New-AzRoleAssignment

SYNOPSIS

Assigns the specified RBAC role to the specified principal, at the specified scope.

The cmdlet may call below Microsoft Graph API according to input parameters:

- GET /users/{id}

- GET /servicePrincipals/{id}

- GET /groups/{id}

- GET /directoryObjects/{id}

Please notice that this cmdlet will mark `ObjectType` as `Unknown` in output if the object of role assignment is not found or current account has insufficient

privileges to get object type.

SYNTAX

New-AzRoleAssignment [-AllowDelegation] -ApplicationId <System.String> [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-ObjectType <System.String>] -ResourceGroupName <System.String> -RoleDefinitionName <System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] -ApplicationId <System.String> [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-ObjectType <System.String>] [-ParentResource <System.String>] -ResourceGroupName <System.String> -ResourceName <System.String> -ResourceType <System.String> -RoleDefinitionName <System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] -ApplicationId <System.String> [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-ObjectType <System.String>] -RoleDefinitionName <System.String> [-Scope <System.String>] [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] -ObjectId <System.String> [-ObjectType <System.String>] -RoleDefinitionName <System.String> [-Scope <System.String>] [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] -ObjectId <System.String> [-ObjectType
<System.String>] -ResourceGroupName <System.String> -RoleDefinitionName <System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] -ObjectId <System.String> [-ObjectType
<System.String>] [-ParentResource <System.String>] -ResourceGroupName <System.String> -ResourceName <System.String> -ResourceType <System.String> -RoleDefinitionName
<System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] -ObjectId <System.String> [-ObjectType
<System.String>] -RoleDefinitionId <System.Guid> -Scope <System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-ObjectType <System.String>]
-ResourceGroupName <System.String> -RoleDefinitionName <System.String> -SignInName <System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>] [-ObjectType <System.String>]

[-ParentResource <System.String>] -ResourceGroupName <System.String> -ResourceName <System.String> -ResourceType <System.String> -RoleDefinitionName <System.String>

-SignInName <System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] [-Condition <System.String>] [-ConditionVersion <System.String>] [-DefaultProfile

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

-RoleDefinitionName <System.String> [-Scope <System.String>] -SignInName <System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

New-AzRoleAssignment [-AllowDelegation] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -InputFile

<System.String> [-SkipClientSideScopeValidation] [<CommonParameters>]

DESCRIPTION

Use the New-AzRoleAssignment command to grant access. Access is granted by assigning the appropriate RBAC role to them at the right scope. To grant access to the

entire subscription, assign a role at the subscription scope. To grant access to a specific resource group within a subscription, assign a role at the resource group

scope. The subject of the assignment must be specified. To specify a user, use SignInName or Microsoft Entra ObjectId parameters. To specify a security group, use

Microsoft Entra ObjectId parameter. And to specify a Microsoft Entra application, use ApplicationId or ObjectId parameters. The role that is being assigned must be

specified using the RoleDefinitionName parameter. The scope at which access is being granted may be specified. It defaults to the selected subscription. The scope of

the assignment can be specified using one of the following parameter combinations a. Scope - This is the fully qualified scope starting with

/subscriptions/<subscriptionId> b. ResourceGroupName - to grant access to the specified resource group. c. ResourceName, ResourceType,

ResourceGroupName and (optionally) ParentResource - to specify a particular resource within a resource group to grant access to.

PARAMETERS

-AllowDelegation <System.Management.Automation.SwitchParameter>

The delegation flag while creating a Role assignment.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ApplicationId <System.String>

The Application ID of the ServicePrincipal

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Condition <System.String>

Condition to be applied to the RoleAssignment.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ConditionVersion <System.String>

Version of the condition.

Required? false

Position? named

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

-Description <System.String>

Brief description of the role assignment.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-InputFile <System.String>

Path to role assignment json

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ObjectId <System.String>

Microsoft Entra Objectid of the user, group or service principal.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ObjectType <System.String>

To be used with ObjectId. Specifies the type of the asignee object

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ParentResource <System.String>

The parent resource in the hierarchy(of the resource specified using ResourceName parameter). Should only be used in conjunction with ResourceGroupName,

ResourceType and ResourceName parameters to construct a hierarchical scope in the form of a relative URI that identifies a resource.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceGroupName <System.String>

The resource group name. Creates an assignment that is effective at the specified resource group. When used in conjunction with ResourceName, ResourceType and

(optionally)ParentResource parameters, the command constructs a hierarchical scope in the form of a relative URI that identifies a resource.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceName <System.String>

The resource name. For e.g. storageaccountprod. Should only be used in conjunction with ResourceGroupName, ResourceType and (optionally)ParentResource parameters

to construct a hierarchical scope in the form of a relative URI that identifies a resource.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceType <System.String>

The resource type. For e.g. Microsoft.Network/virtualNetworks. Should only be used in conjunction with ResourceGroupName, ResourceName and

(optionally)ParentResource parameters to construct a hierarchical scope in the form of a relative URI that identifies a resource.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-RoleDefinitionId <System.Guid>

Id of the RBAC role that needs to be assigned to the principal.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-RoleDefinitionName <System.String>

Name of the RBAC role that needs to be assigned to the principal i.e. Reader, Contributor, Virtual Network Administrator, etc.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Scope <System.String>

The Scope of the role assignment. In the format of relative URI. For e.g. "/subscriptions/9004a9fd-d58e-48dc-aeb2-4a4aec58606f/resourceGroups/TestRG". If not

specified, will create the role assignment at subscription level. If specified, it should start with "/subscriptions/{id}".

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-SignInName <System.String>

The email address or the user principal name of the user.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-SkipClientSideScopeValidation <System.Management.Automation.SwitchParameter>

If specified, skip client side scope validation.

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.Guid

OUTPUTS

Microsoft.Azure.Commands.Resources.Models.Authorization.PSRoleAssignment

NOTES

Keywords: azure, azurerm, arm, resource, management, manager, resource, group, template, deployment

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

New-AzRoleAssignment -ResourceGroupName rg1 -SignInName allen.young@live.com -RoleDefinitionName Reader -AllowDelegation

Grant Reader role access to a user at a resource group scope with the Role Assignment being available for delegation

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

Get-AzADGroup -SearchString "Christine Koch Team"

DisplayName Type Id

Christine Koch Team 2f9d4375-cbf1-48e8-83c9-2a0be4cb33fb

New-AzRoleAssignment -ObjectId 2f9d4375-cbf1-48e8-83c9-2a0be4cb33fb -RoleDefinitionName Contributor -ResourceGroupName rg1

Grant access to a security group

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

New-AzRoleAssignment -SignInName john.doe@contoso.com -RoleDefinitionName Owner -Scope "/subscriptions/86f81fc3-b00f-48cd-8218-3879f51ff362/resourcegroups/rg1/providers/Microsoft.Web/sites/site1"

Grant access to a user at a resource (website)

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

New-AzRoleAssignment -ObjectId 5ac84765-1c8c-4994-94b2-629461bd191b -RoleDefinitionName "Virtual Machine Contributor" -ResourceName Devices-Engineering-ProjectRND
-ResourceType Microsoft.Network/virtualNetworks/subnets -ParentResource virtualNetworks/VNET-EASTUS-01 -ResourceGroupName Network

Grant access to a group at a nested resource (subnet)

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

```
$servicePrincipal = New-AzADServicePrincipal -DisplayName "testServiceprincipal"
New-AzRoleAssignment -RoleDefinitionName "Reader" -ApplicationId $servicePrincipal.ApplicationId
```

Grant reader access to a service principal

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.resources/new-azroleassignment

Get-AzRoleAssignment

Remove-AzRoleAssignment

Get-AzRoleDefinition