



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

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

NAME

New-AzPostgreSqlFirewallRule

SYNOPSIS

Creates a new firewall rule or updates an existing firewall rule.

SYNTAX

```
New-AzPostgreSqlFirewallRule -ResourceGroupName <String> -ServerName <String> [-Name <String>] [-SubscriptionId
<String>] -EndIpAddress <String> -StartIpAddress
<String> [-DefaultProfile <PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend
<SendAsyncStep[]>] [-NoWait] [-Proxy <Uri>]
[-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzPostgreSqlFirewallRule -ResourceGroupName <String> -ServerName <String> [-Name <String>] [-SubscriptionId
<String>] -ClientIpAddress <String> [-DefaultProfile
<PSObject>] [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>]
[-NoWait] [-Proxy <Uri>] [-ProxyCredential
<PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]
```

New-AzPostgreSqlFirewallRule -ResourceGroupName <String> -ServerName <String> [-Name <String>] [-SubscriptionId <String>] -AllowAll [-DefaultProfile <PSObject>]
 [-AsJob] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-NoWait]
 [-Proxy <Uri>] [-ProxyCredential <PSCredential>]
 [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

Creates a new firewall rule or updates an existing firewall rule.

PARAMETERS

-ResourceGroupName <String>

The name of the resource group.

The name is case insensitive.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ServerName <String>

The name of the server.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Name <String>

The name of the server firewall rule.

Required? false
Position? named
Default value
Accept pipeline input? false
Accept wildcard characters? false

-SubscriptionId <String>

The ID of the target subscription.

Required? false
Position? named
Default value
Accept pipeline input? false
Accept wildcard characters? false

-EndIPAddress <String>

The end IP address of the server firewall rule.
Must be IPv4 format.

Required? true
Position? named
Default value
Accept pipeline input? false
Accept wildcard characters? false

-StartIPAddress <String>

The start IP address of the server firewall rule.
Must be IPv4 format.

Required? true
Position? named
Default value

Accept pipeline input? false

Accept wildcard characters? false

-ClientIPAddress <String>

Client specified single IP of the server firewall rule.

Must be IPv4 format.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-AllowAll [<SwitchParameter>]

Present to allow all range IPs, from 0.0.0.0 to 255.255.255.255.

Required? true

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-DefaultProfile <PSObject>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-AsJob [<SwitchParameter>]

Run the command as a job

Required? false
Position? named
Default value False
Accept pipeline input? false
Accept wildcard characters? false

-Break [<SwitchParameter>]

Wait for .NET debugger to attach

Required? false
Position? named
Default value False
Accept pipeline input? false
Accept wildcard characters? false

-HttpPipelineAppend <SendAsyncStep[]>

SendAsync Pipeline Steps to be appended to the front of the pipeline

Required? false
Position? named
Default value
Accept pipeline input? false
Accept wildcard characters? false

-HttpPipelinePrepend <SendAsyncStep[]>

SendAsync Pipeline Steps to be prepended to the front of the pipeline

Required? false
Position? named
Default value
Accept pipeline input? false
Accept wildcard characters? false

-NoWait [<SwitchParameter>]

Run the command asynchronously

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Proxy <Uri>

The URI for the proxy server to use

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyCredential <PSCredential>

Credentials for a proxy server to use for the remote call

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyUseDefaultCredentials [<SwitchParameter>]

Use the default credentials for the proxy

Required? false

Position? named

Default value False
Accept pipeline input? false
Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Required? false
Position? named
Default value
Accept pipeline input? false
Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Required? false
Position? named
Default value
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.PostgreSql.Models.Api20171201.IFirewallRule

```
PS C:\>New-AzPostgreSqlFirewallRule -Name rule -ResourceGroupName PostgreSqlTestRG -ServerName PostgreSqlTestServer -EndIpAddress 0.0.0.1 -StartIpAddress 0.0.0.0
```

----- EXAMPLE 2 -----

```
PS C:\>New-AzPostgreSqlFirewallRule -ResourceGroupName PostgreSqlTestRG -ServerName PostgreSqlTestServer -ClientIpAddress 0.0.0.1
```

----- EXAMPLE 3 -----

```
PS C:\>New-AzPostgreSqlFirewallRule -ResourceGroupName PostgreSqlTestRG -ServerName PostgreSqlTestServer -AllowAll
```

RELATED LINKS

<https://learn.microsoft.com/powershell/module/az.postgresql/new-azpostgresqlfirewallrule>

