


CREATING AND DELETING A FOLDER



my_folder

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> cd C:/Users/Admin/OneDrive/Desktop
PS C:\Users\Admin\OneDrive\Desktop> mkdir my_folder

Directory: C:\Users\Admin\OneDrive\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----          5/25/2021   9:00 PM              my_folder

PS C:\Users\Admin\OneDrive\Desktop>
```

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> cd C:/Users/Admin/Documents
PS C:\Users\Admin\Documents> mkdir new_folder

Directory: C:\Users\Admin\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          5/25/2021   9:17 PM              new_folder

PS C:\Users\Admin\Documents> ls

Directory: C:\Users\Admin\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          5/25/2021   9:17 PM              new_folder
-a----          10/14/2020   9:09 AM        595782 muk.pdf

PS C:\Users\Admin\Documents> rm new_folder
PS C:\Users\Admin\Documents> ls

Directory: C:\Users\Admin\Documents

Mode                LastWriteTime         Length Name
----                -
-a----          10/14/2020   9:09 AM        595782 muk.pdf

PS C:\Users\Admin\Documents>
```

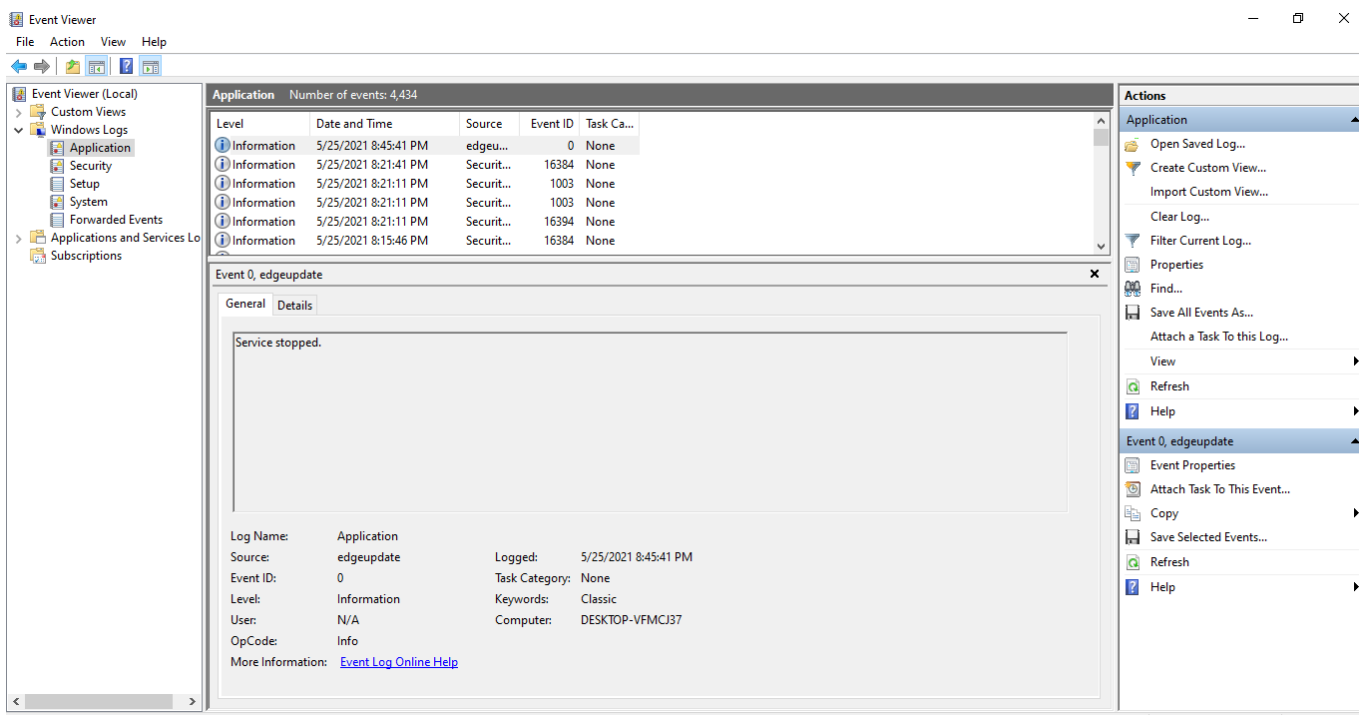
TERMINATING MULTIPLE PROCESSES

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-Process -Name "*cal*"

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
557 28 24132 60740 0.94 880 1 Calculator
1017 42 25940 74872 1.22 5584 1 HxCalendarAppImm

PS C:\WINDOWS\system32> taskkill /F /PID 880
SUCCESS: The process with PID 880 has been terminated.
PS C:\WINDOWS\system32> taskkill /F /PID 5584
SUCCESS: The process with PID 5584 has been terminated.
PS C:\WINDOWS\system32> Get-Process -Name "*cal*"
PS C:\WINDOWS\system32>
```

LOGS IN WINDOWS EVENT VIEWER



VIEWING, GRANTING AND REMOVING PERMISSIONS

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> cd C:/Users/Admin/OneDrive/Desktop
PS C:\Users\Admin\OneDrive\Desktop> icacls random.txt
random.txt NT AUTHORITY\SYSTEM:(I)(F)
          BUILTIN\Administrators:(I)(F)
          DESKTOP-VFMCJ37\Admin:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\Admin\OneDrive\Desktop> icacls random.txt /grant "Admin:(w)"
processed file: random.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\Admin\OneDrive\Desktop> icacls random.txt /grant "Everyone:(x)"
processed file: random.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\Admin\OneDrive\Desktop> icacls random.txt
random.txt Everyone:(X)
          DESKTOP-VFMCJ37\Admin:(W)
          NT AUTHORITY\SYSTEM:(I)(F)
          BUILTIN\Administrators:(I)(F)
          DESKTOP-VFMCJ37\Admin:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\Admin\OneDrive\Desktop> icacls random.txt /remove "Everyone"
processed file: random.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\Admin\OneDrive\Desktop> icacls random.txt
random.txt DESKTOP-VFMCJ37\Admin:(W)
          NT AUTHORITY\SYSTEM:(I)(F)
          BUILTIN\Administrators:(I)(F)
          DESKTOP-VFMCJ37\Admin:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\Admin\OneDrive\Desktop>
```

TERMINATING A SPECIFIC PROCESS

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

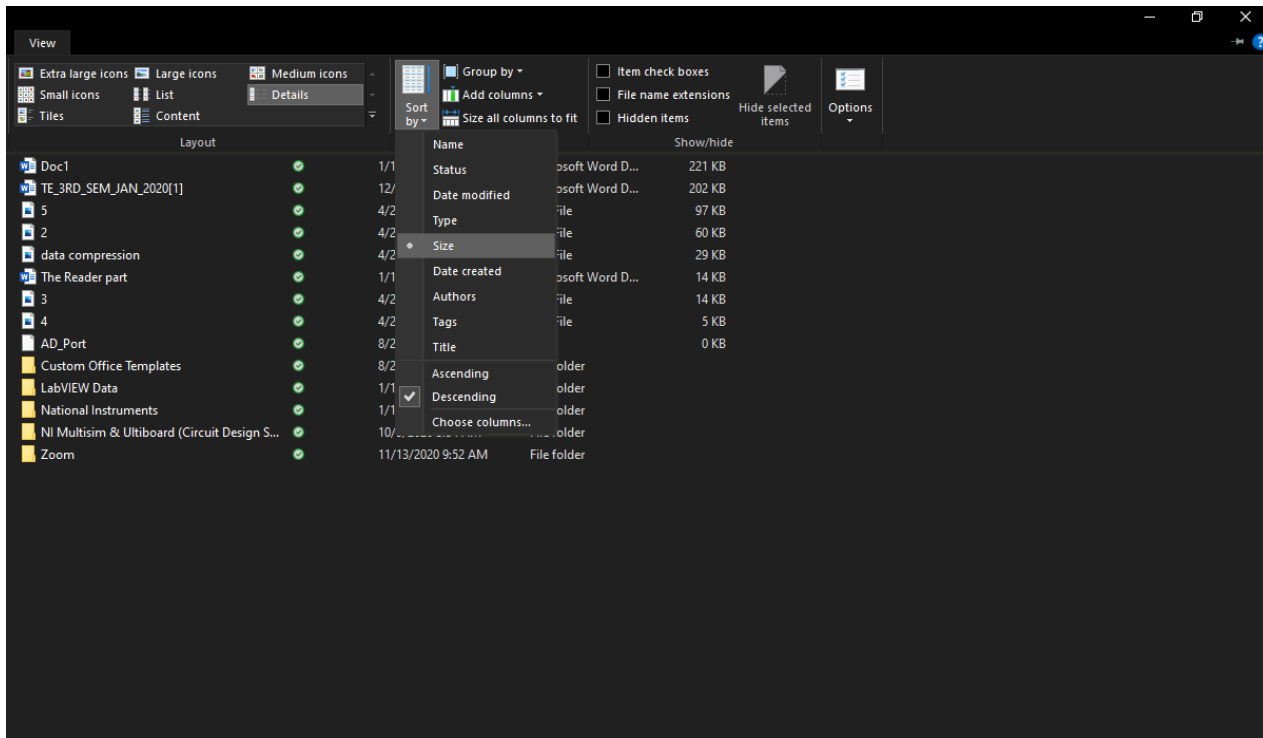
PS C:\WINDOWS\system32> Get-Process -Name "notepad"

Handles  NPM(K)  PM(K)  WS(K)  CPU(s)  Id  SI ProcessName
-----  -
238      13      3040   14104   0.17    9704  1 notepad

PS C:\WINDOWS\system32> taskkill /F /PID 9704
SUCCESS: The process with PID 9704 has been terminated.
PS C:\WINDOWS\system32> Get-Process -Name "notepad"
Get-Process : Cannot find a process with the name "notepad". Verify the process name and call the cmdlet again.
At line:1 char:1
+ Get-Process -Name "notepad"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (notepad:String) [Get-Process], ProcessCommandException
+ FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand

PS C:\WINDOWS\system32>
```

SORTING BASED ON SIZE



FILTERING ERROR LOGS

Event Viewer (Local)

File Action View Help

Custom Views

Administrative Events

muktha

Windows Logs

Application

Security

Setup

System

Forwarded Events

Applications and Services Logs

Subscriptions

muktha Number of events: 438

Number of events: 438

Level	Date and Time	Source	Event ID	Task Category
Error	5/25/2021 8:13:52 PM	niZeroconfService	100	None
Error	5/25/2021 8:13:52 PM	niZeroconfService	100	None
Error	5/25/2021 8:13:52 PM	niZeroconfService	100	None
Error	5/25/2021 8:13:51 PM	niZeroconfService	100	None
Error	5/25/2021 8:13:51 PM	niZeroconfService	100	None

Event 100, niZeroconfService

General Details

The description for Event ID 100 from source niZeroconfService cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

Local Hostname DESKTOP-VFMCJ37.local already in use; will try DESKTOP-VFMCJ37-2.local instead

The specified resource type cannot be found in the image file

Log Name: Application

Source: niZeroconfService

Logged: 5/25/2021 8:13:52 PM

Event ID: 100

Task Category: None

Level: Error

Keywords: Classic

User: N/A

Computer: DESKTOP-VFMCJ37

OpCode: Info

More Information: [Event Log Online Help](#)

Actions

muktha

Open Saved Log...

Create Custom View...

Import Custom View...

Filter Current Custom View...

Properties

Find...

Save All Events in Custom View As...

Export Custom View...

Copy Custom View...

Attach Task To This Custom View...

View

Delete

Rename

Refresh

Help

Event 100, niZeroconfService

Event Properties

Attach Task To This Event...

Copy

Save Selected Events...

Refresh

Help

Create Custom View

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose ☒ Error ☐ Information

By log Event logs:

By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel