Lab - Reset a Lost Administrator password in Windows Server

Overview

In this lab, you will learn how to reset a lost administrator password for a Windows Server 2012, 2016 or 2019 standalone server or domain controller. Anyone who works with Microsoft operating systems long enough will be called upon to either reset or attempt to recover a lost or forgotten administrative password. Administrator's quit or get terminated, and some will reset the administrator password on the way out the door. Office managers forget their server administrator password or the machine has become infected with malware.

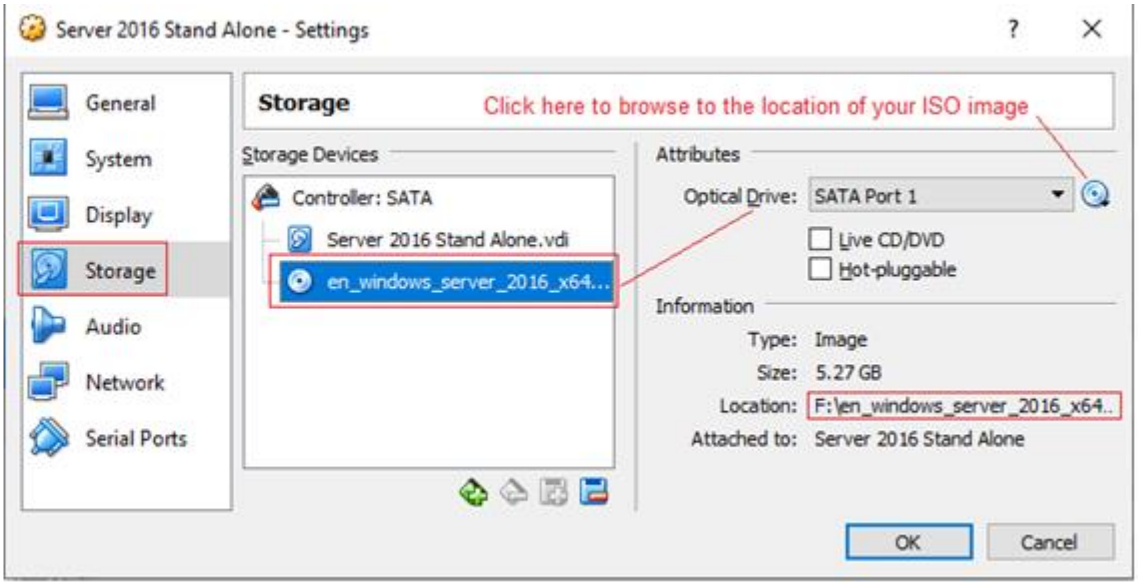
Hardware Requirements

- One virtual or physical install of Server 2012, 2016 or 2019 running as a standalone server or as a domain controller.
- ISO image or the physical media (DVD) for either Server 2012, 2016, or 2019.

Begin the lab!

For this demonstration, we will be using a virtual install of Server 2016 running inside of VirtualBox. The same procedure would apply using Hyper-V or VMWare or a physical machine. The machine first needs to be configured to boot from either the ISO image or the DVD media. If you are using a virtual machine, you can set the VM to boot from the ISO image accessing the Settings for the VM, selecting Storage and selecting the optical drive as the first boot device.

For VirtualBox



Server 2016 Stand Alone - Settings

Storage

Click here to browse to the location of your ISO image

Storage Devices

Controller: SATA

Server 2016 Stand Alone.vdi

en_windows_server_2016_x64...

Attributes

Optical Drive: SATA Port 1

□ Live CD/DVD

□ Hot-pluggable

Information

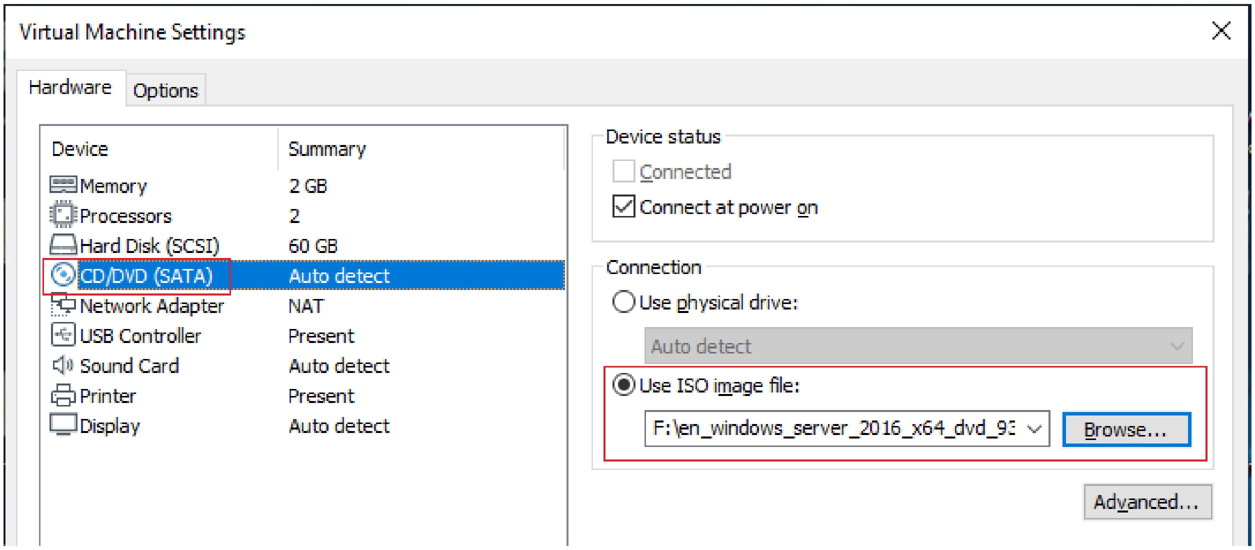
Type: Image

Size: 5.27 GB

Location: F:\en_windows_server_2016_x64..

Attached to: Server 2016 Stand Alone

For VMWare



Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☐ Connected

☑ Connect at power on

Connection

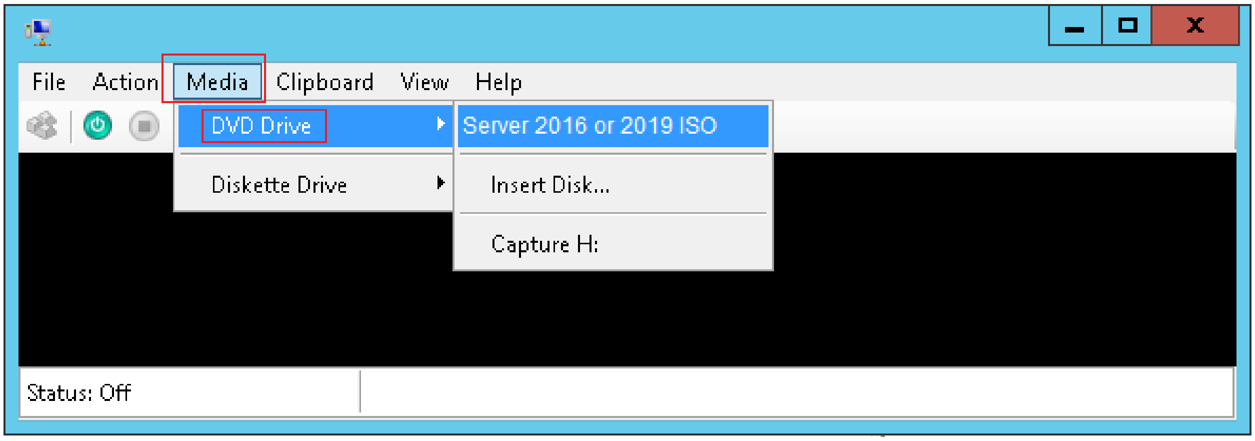
○ Use physical drive:

Auto detect

● Use ISO image file:

F:\en_windows_server_2016_x64_dvd_93

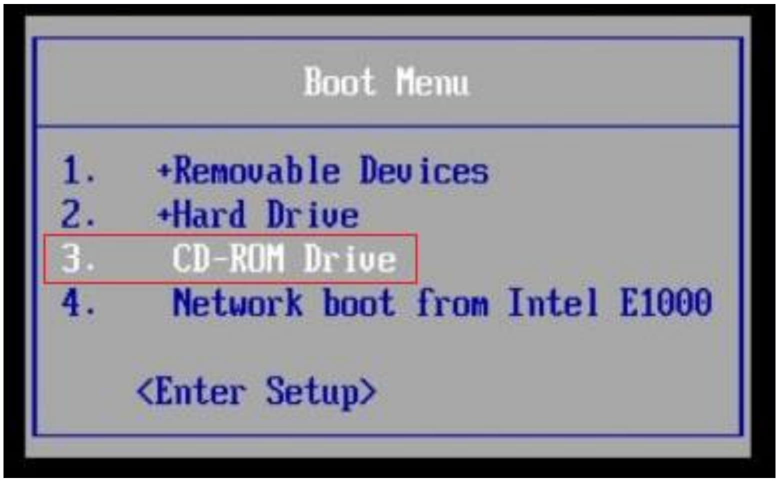
For Hyper-V



Status: Off

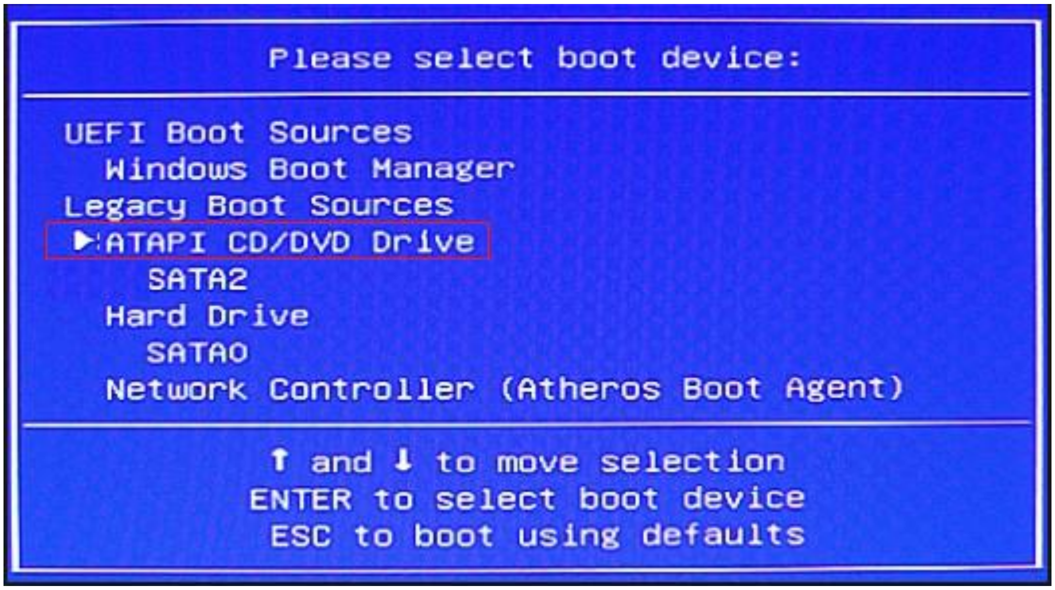
For a physical install of the server, you would need to boot into the system BIOS or insert the DVD and during the boot process, press the F12 key and select the optical/DVD drive as the first boot device.

Using F12



```
Boot Menu

1.   +Removable Devices
2.   +Hard Drive
3.    CD-ROM Drive
4.    Network boot from Intel E1000

    <Enter Setup>
```

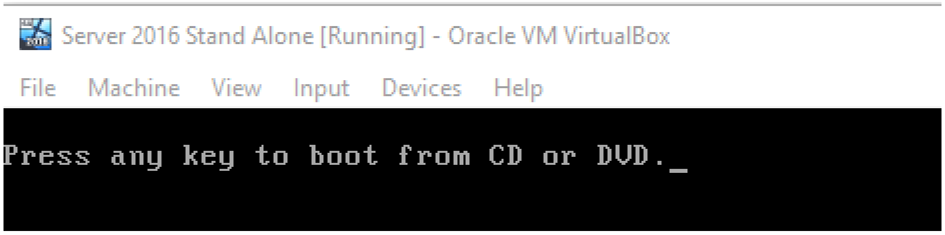
Setting the boot device using the BIOS



```
            Please select boot device:

  UEFI Boot Sources
    Windows Boot Manager
  Legacy Boot Sources
   ▶ATAPI CD/DVD Drive
      SATA2
    Hard Drive
      SATA0
    Network Controller (Atheros Boot Agent)

             ↑ and ↓ to move selection
            ENTER to select boot device
             ESC to boot using defaults
```

You'll want to go back into your setting once the password has been reset and restore your settings to boot from your hard drive or virtual disk.

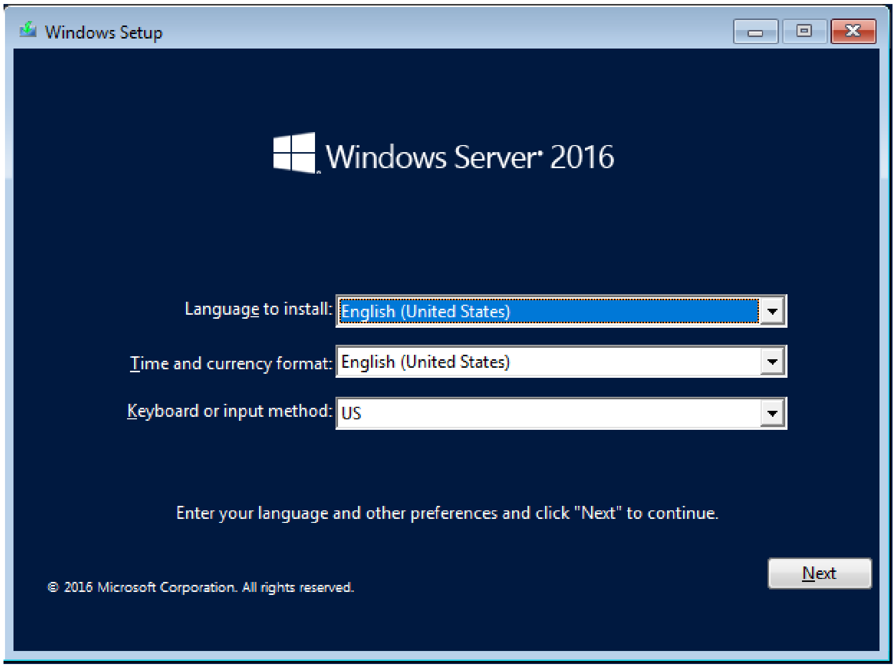
With the ISO or physical media selected as the boot device, toy will see the following message. Hit Enter when you see the message. This will begin the installation process.



Server 2016 Stand Alone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

```
Press any key to boot from CD or DVD._
```

On the first screen of the windows setup, press enter.



Windows Setup

Windows Server 2016

Language to install: English (United States)

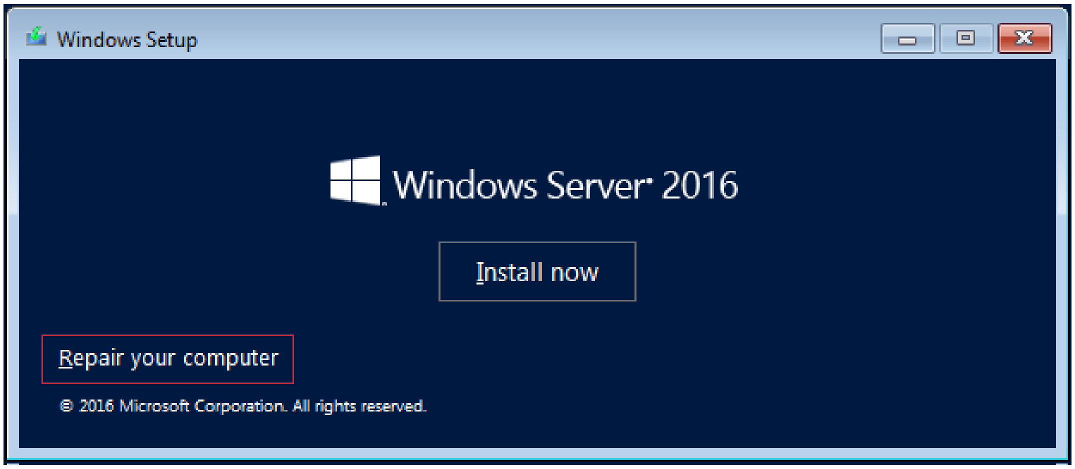
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

© 2016 Microsoft Corporation. All rights reserved.

On the next screen, select the repair your computer option.

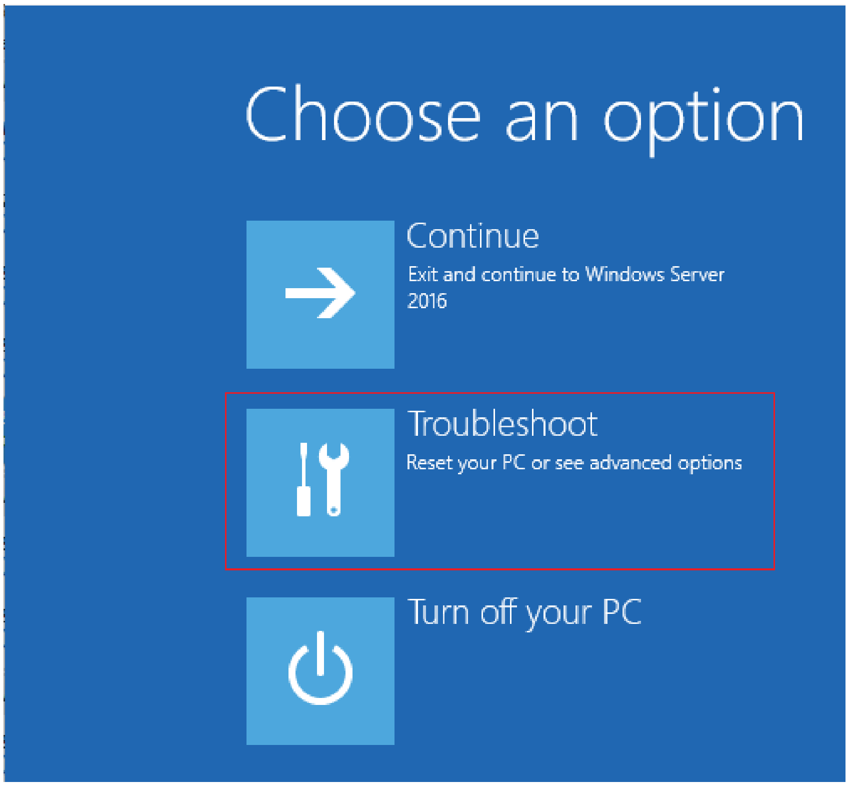


Windows Setup

Windows Server 2016

© 2016 Microsoft Corporation. All rights reserved.

On the next screen, troubleshoot option.



Choose an option

Continue

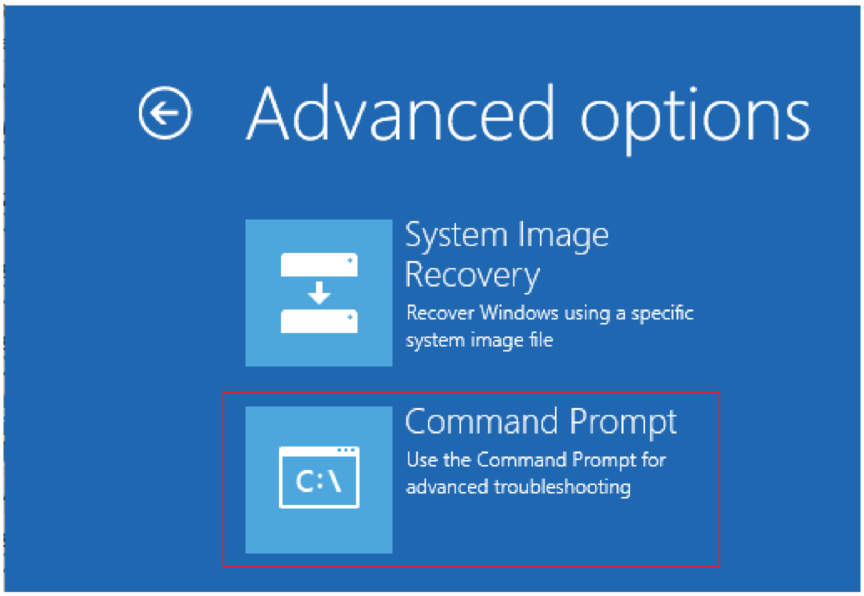
Exit and continue to Windows Server 2016

Troubleshoot

Reset your PC or see advanced options

Turn off your PC

On the next screen, select the option for the Command Prompt.



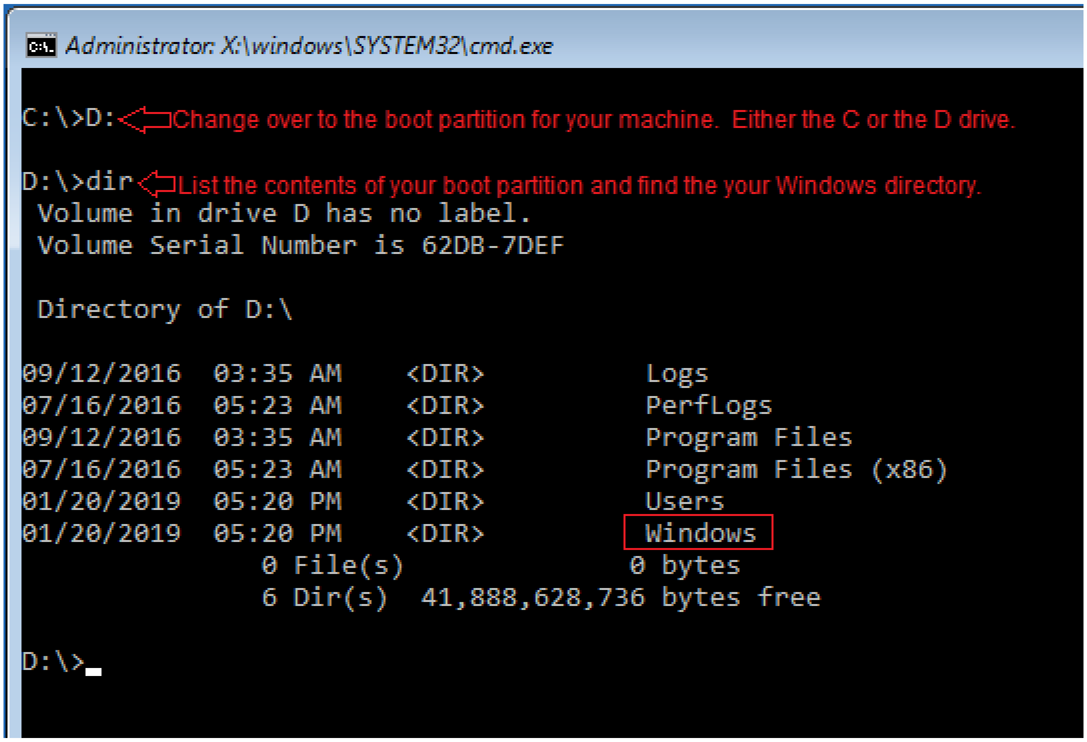
Advanced options

System Image Recovery

Recover Windows using a specific system image file

Command Prompt

Use the Command Prompt for advanced troubleshooting

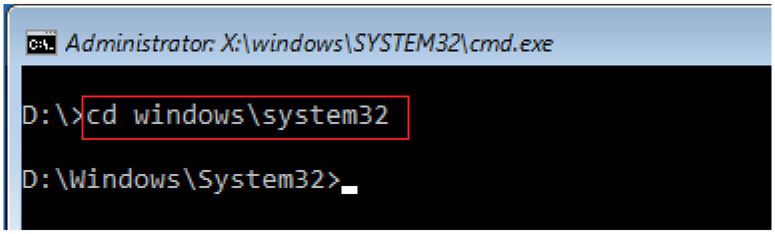


Administrator: X:\windows\SYSTEM32\cmd.exe

```
C:\>D:<=Change over to the boot partition for your machine.  Either the C or the D drive.

D:\>dir<=List the contents of your boot partition and find the your Windows directory.
 Volume in drive D has no label.
 Volume Serial Number is 62DB-7DEF

 Directory of D:\

09/12/2016  03:35 AM    <DIR>          Logs
07/16/2016  05:23 AM    <DIR>          PerfLogs
09/12/2016  03:35 AM    <DIR>          Program Files
07/16/2016  05:23 AM    <DIR>          Program Files (x86)
01/20/2019  05:20 PM    <DIR>          Users
01/20/2019  05:20 PM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  41,888,628,736 bytes free

D:\>_
```

Change over to the windows\system32 directory

```
cd windows\system32
```



Administrator: X:\windows\SYSTEM32\cmd.exe

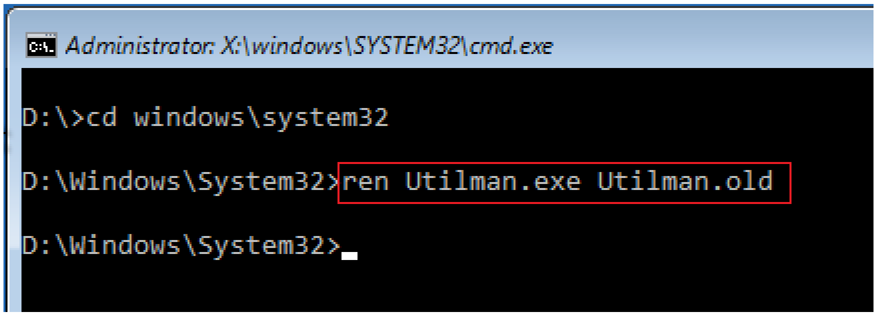
```
D:\>cd windows\system32

D:\Windows\System32>_
```

We now need to rename the Utilman.exe to Utilman.old

Utilman.exe is a built-in Windows application that is designed to allow the user to configure Accessibility options such as the Magnifier, High Contrast Theme, Narrator and On-Screen Keyboard before they log onto the system.

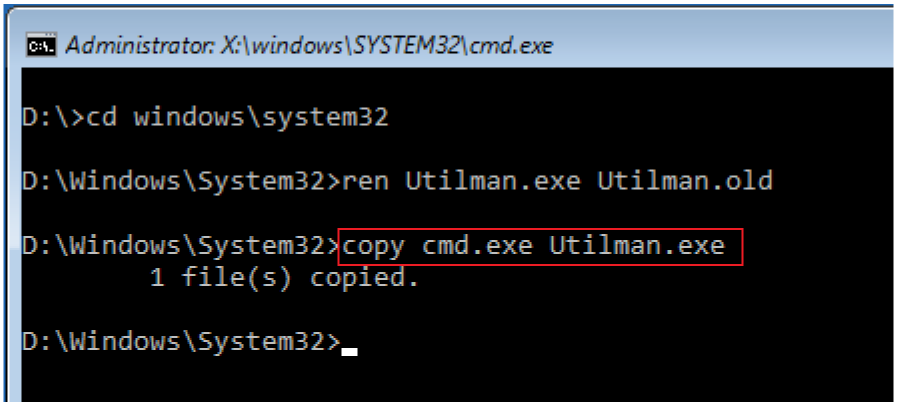
We can use to bypass the Windows login screen.

```
ren Utilman.exe Utilman.exe.old
```



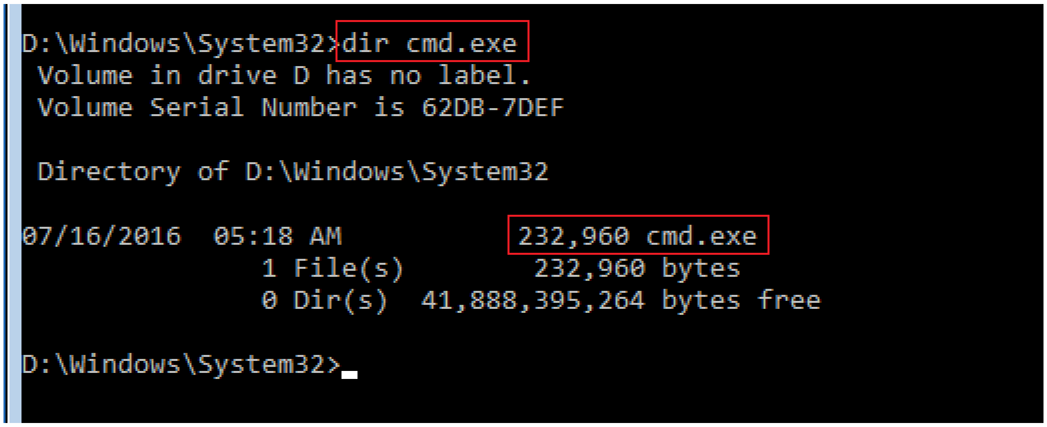
```
D:\>cd windows\system32

D:\Windows\System32>ren Utilman.exe Utilman.old

D:\Windows\System32>_
```

We next need to be able to launch the Utilman.exe at login and have access to the command prompt. To do this, we make a new Utilman.exe by making a copy of the command prompt and naming the copy Utilman.exe. (remember, we renamed the original to Utilman.old)

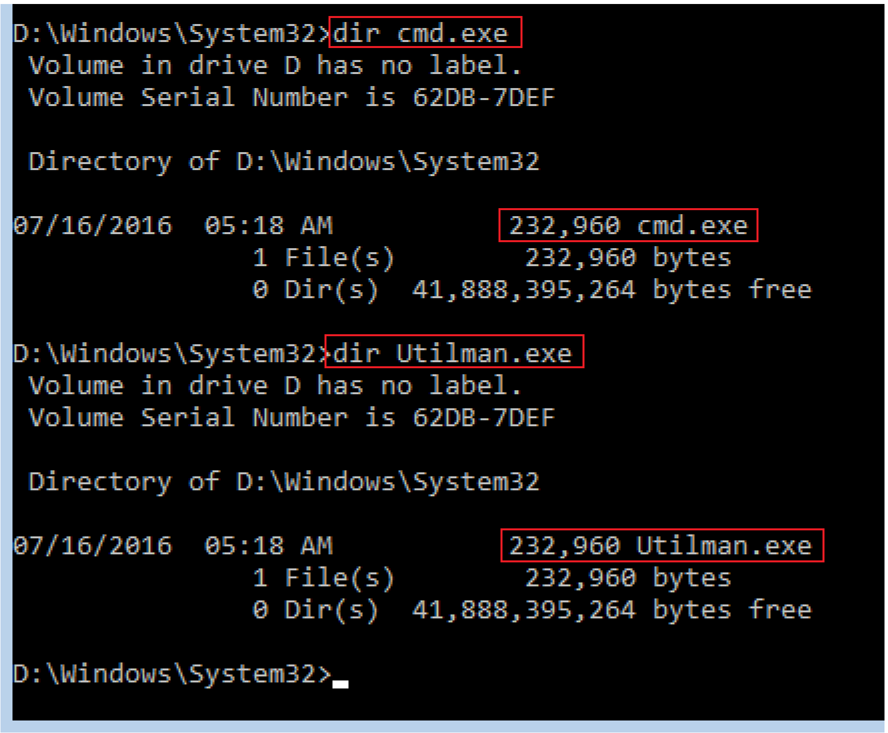


```
D:\>cd windows\system32

D:\Windows\System32>ren Utilman.exe Utilman.old

D:\Windows\System32>copy cmd.exe Utilman.exe
        1 file(s) copied.

D:\Windows\System32>_
```

You can compare the two files to see if the size of each matches using the dir command.

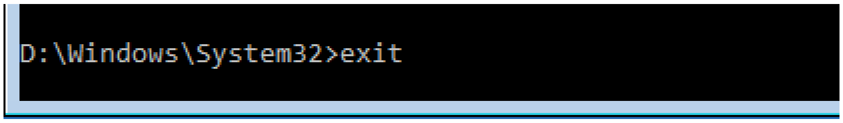


```
D:\Windows\System32>dir cmd.exe
 Volume in drive D has no label.
 Volume Serial Number is 62DB-7DEF

 Directory of D:\Windows\System32

07/16/2016  05:18 AM           232,960 cmd.exe
               1 File(s)        232,960 bytes
               0 Dir(s)  41,888,395,264 bytes free

D:\Windows\System32>_
```



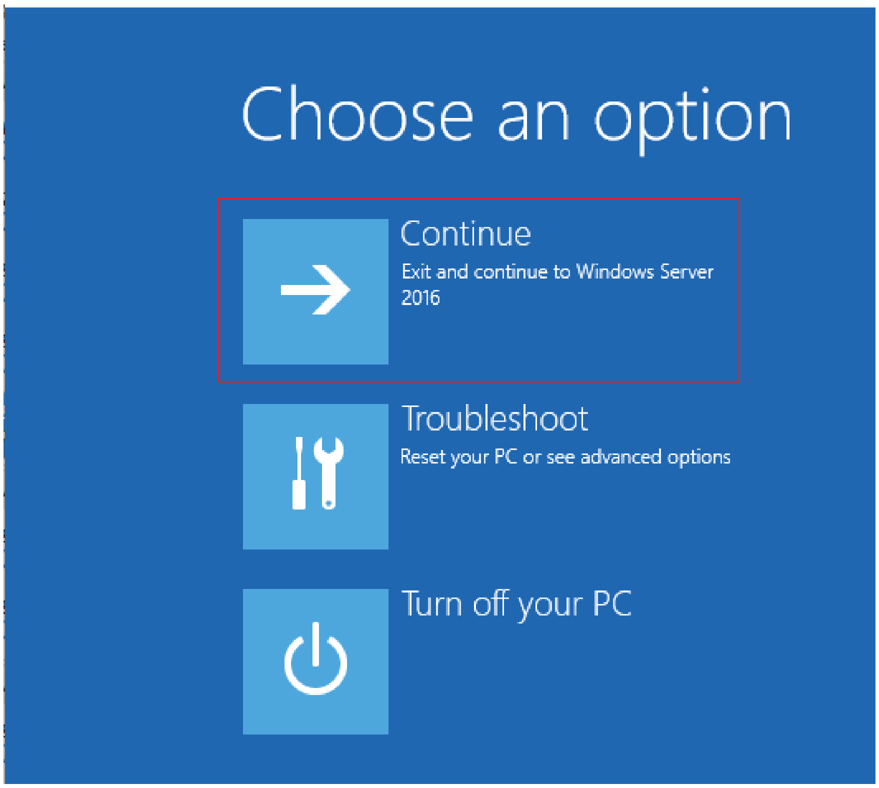
```
D:\Windows\System32>dir cmd.exe
 Volume in drive D has no label.
 Volume Serial Number is 62DB-7DEF

 Directory of D:\Windows\System32

07/16/2016  05:18 AM           232,960 cmd.exe
               1 File(s)        232,960 bytes
               0 Dir(s)  41,888,395,264 bytes free

D:\Windows\System32>dir Utilman.exe
 Volume in drive D has no label.
 Volume Serial Number is 62DB-7DEF

 Directory of D:\Windows\System32

07/16/2016  05:18 AM           232,960 Utilman.exe
               1 File(s)        232,960 bytes
               0 Dir(s)  41,888,395,264 bytes free

D:\Windows\System32>_
```

At the command prompt type, exit to return to the options screen.



```
D:\Windows\System32>exit
```

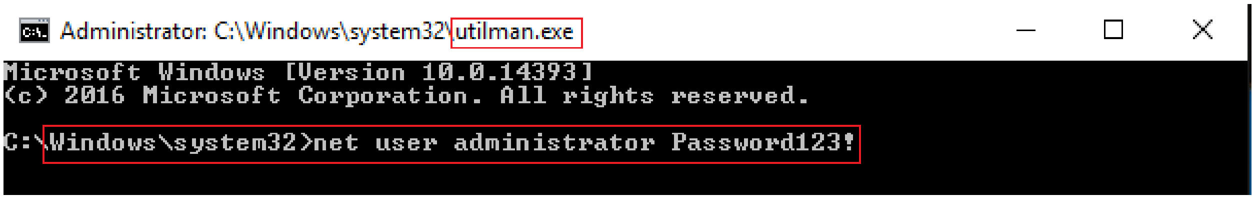
At the options screen, select continue to continue logging on to Windows.


Choose an option
Continue
Exit and continue to Windows Server 2016
Troubleshoot
Reset your PC or see advanced options
Turn off your PC

When the computer restarts, you will want to remove your physical media for your DVD drive, so the machine will start to boot normally.

At the logon screen, press the **Windows+ U** key, the command prompt will pop up. At the command prompt, we can now change our admittatur password using the following command

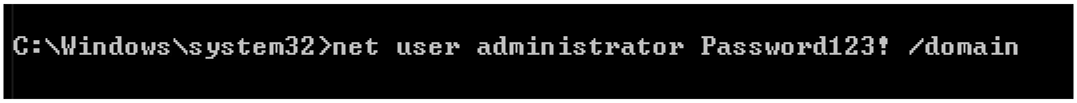
net user administrator Password123!



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user administrator Password123!
```

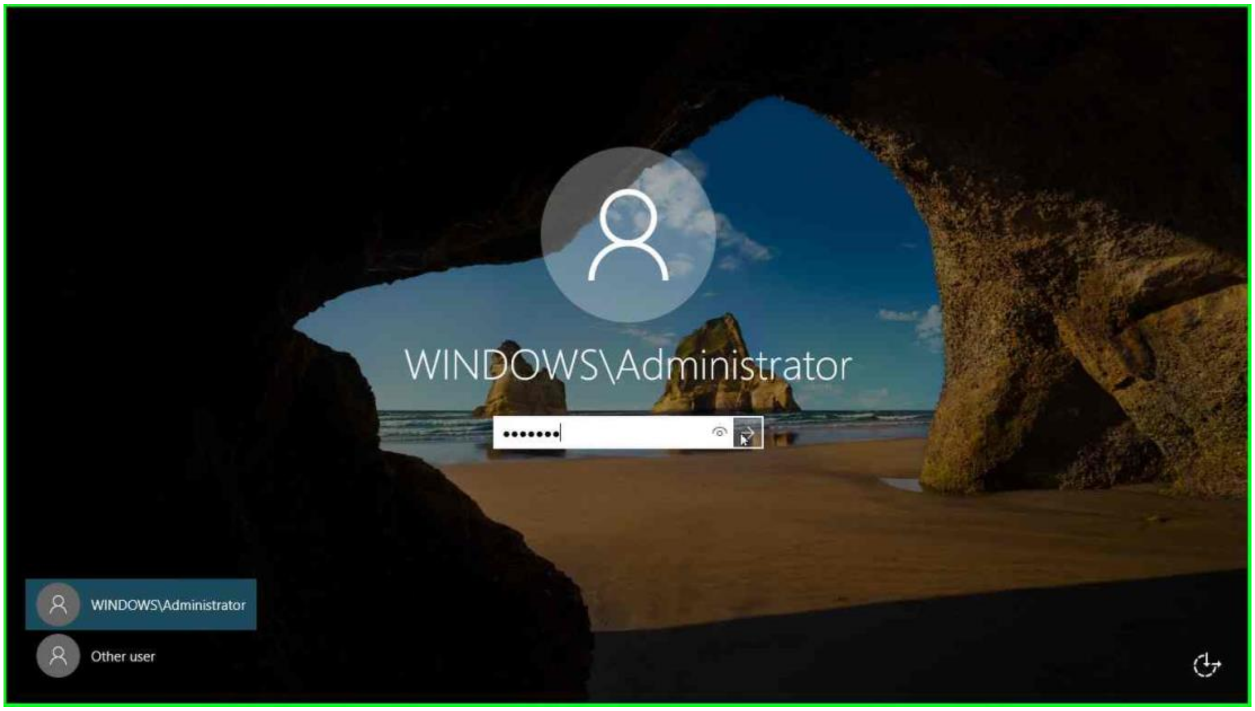
If this were a domain controller we would type:

net user administrator Password123! /domain



```
C:\Windows\system32>net user administrator Password123! /domain
```

Close the command prompt and logon to your server using the new password.



At this point, you can repeat the repair process and restore the original Utilman.exe back using the following commands.

```
cd windows\system32
ren utilman.exe utilman.exe.123
copy utilman.exe.old utilman.exe
```