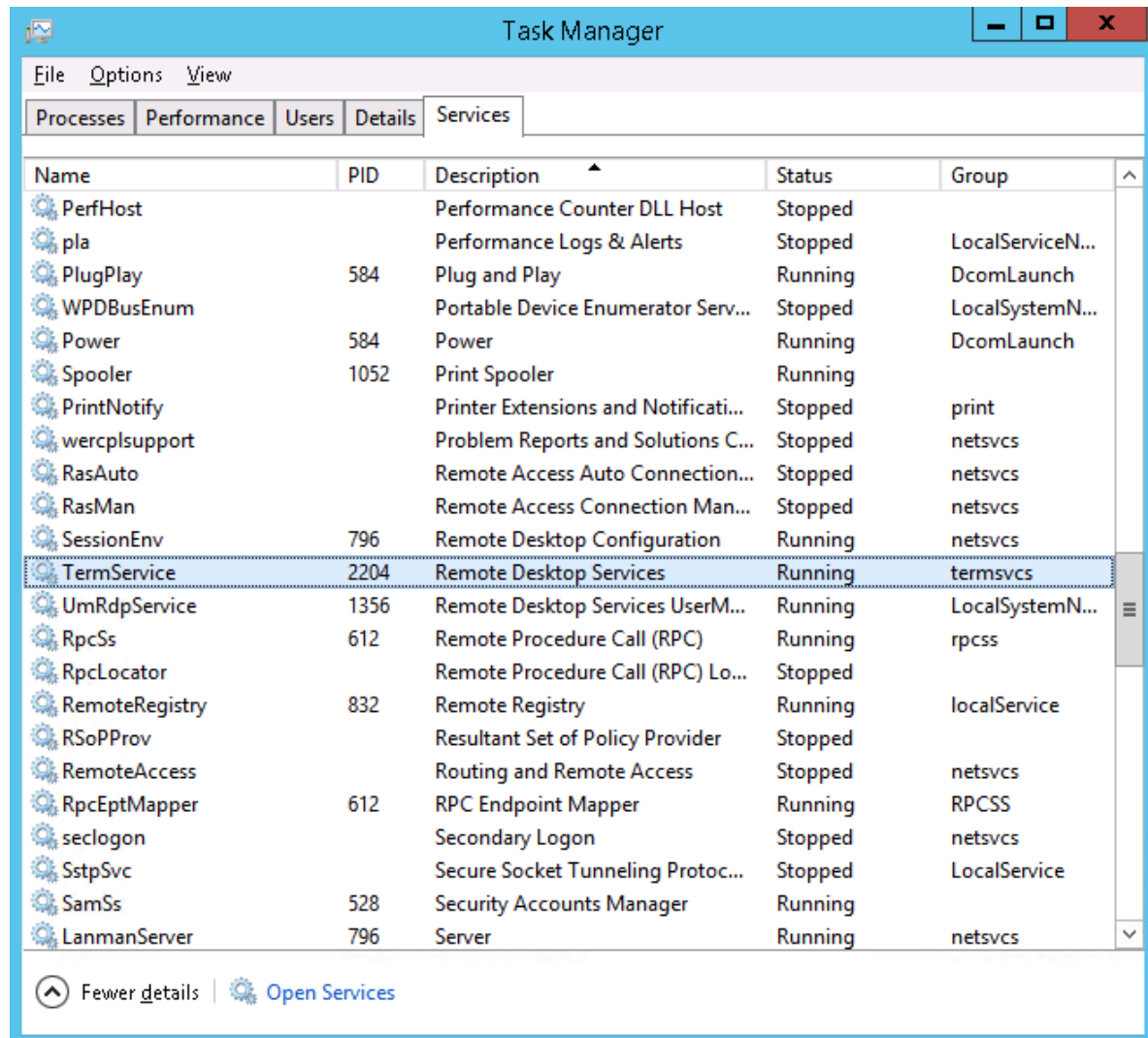


# Lab 10

Authors: Daniel Gisolfi, James Ekstract

## Section 1

screen capture showing all the processes associated with Remote Desktop Services

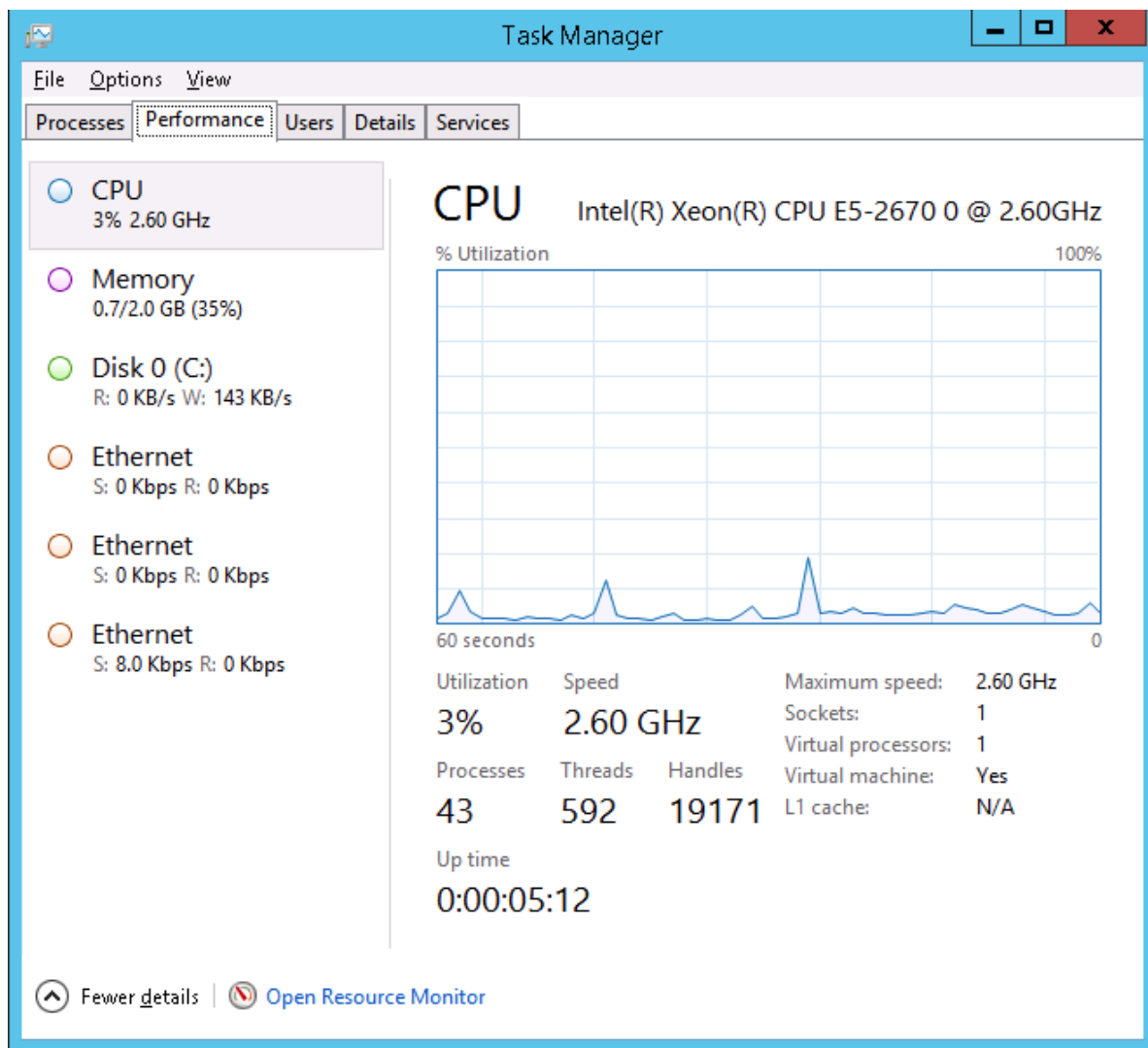


The screenshot shows the Windows Task Manager application with the 'Services' tab selected. The window title is 'Task Manager'. The menu bar includes 'File', 'Options', and 'View'. The 'Services' tab is active, showing a list of system services. The list has columns for Name, PID, Description, Status, and Group. The 'TermService' (Remote Desktop Services) is highlighted. Other services like 'PerfHost', 'pla', 'PlugPlay', 'WPDBusEnum', 'Power', 'Spooler', 'PrintNotify', 'werpcplsupport', 'RasAuto', 'RasMan', 'SessionEnv', 'UmRdpService', 'RpcSs', 'RpcLocator', 'RemoteRegistry', 'RSoPProv', 'RemoteAccess', 'RpcEptMapper', 'seclogon', 'SstpSvc', 'SamSs', and 'LanmanServer' are also visible.

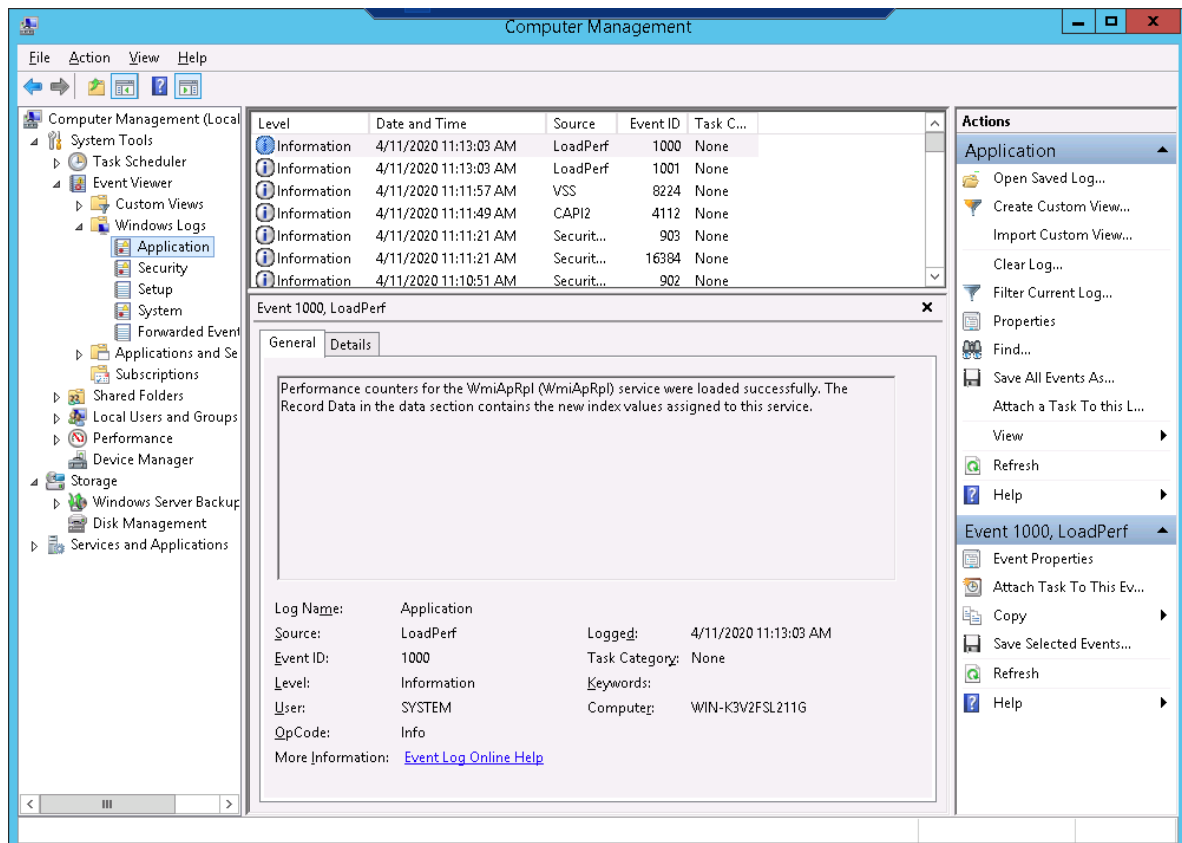
Name	PID	Description	Status	Group
PerfHost		Performance Counter DLL Host	Stopped	
pla		Performance Logs & Alerts	Stopped	LocalServiceN...
PlugPlay	584	Plug and Play	Running	DcomLaunch
WPDBusEnum		Portable Device Enumerator Serv...	Stopped	LocalSystemN...
Power	584	Power	Running	DcomLaunch
Spooler	1052	Print Spooler	Running	
PrintNotify		Printer Extensions and Notificati...	Stopped	print
werpcplsupport		Problem Reports and Solutions C...	Stopped	netsvcs
RasAuto		Remote Access Auto Connection...	Stopped	netsvcs
RasMan		Remote Access Connection Man...	Stopped	netsvcs
SessionEnv	796	Remote Desktop Configuration	Running	netsvcs
<b>TermService</b>	<b>2204</b>	<b>Remote Desktop Services</b>	<b>Running</b>	<b>termsvcs</b>
UmRdpService	1356	Remote Desktop Services UserM...	Running	LocalSystemN...
RpcSs	612	Remote Procedure Call (RPC)	Running	rpcss
RpcLocator		Remote Procedure Call (RPC) Lo...	Stopped	
RemoteRegistry	832	Remote Registry	Running	localService
RSoPProv		Resultant Set of Policy Provider	Stopped	
RemoteAccess		Routing and Remote Access	Stopped	netsvcs
RpcEptMapper	612	RPC Endpoint Mapper	Running	RPCSS
seclogon		Secondary Logon	Stopped	netsvcs
SstpSvc		Secure Socket Tunneling Protoc...	Stopped	LocalService
SamSs	528	Security Accounts Manager	Running	
LanmanServer	796	Server	Running	netsvcs

At the bottom of the window, there are links for 'Fewer details' and 'Open Services'.

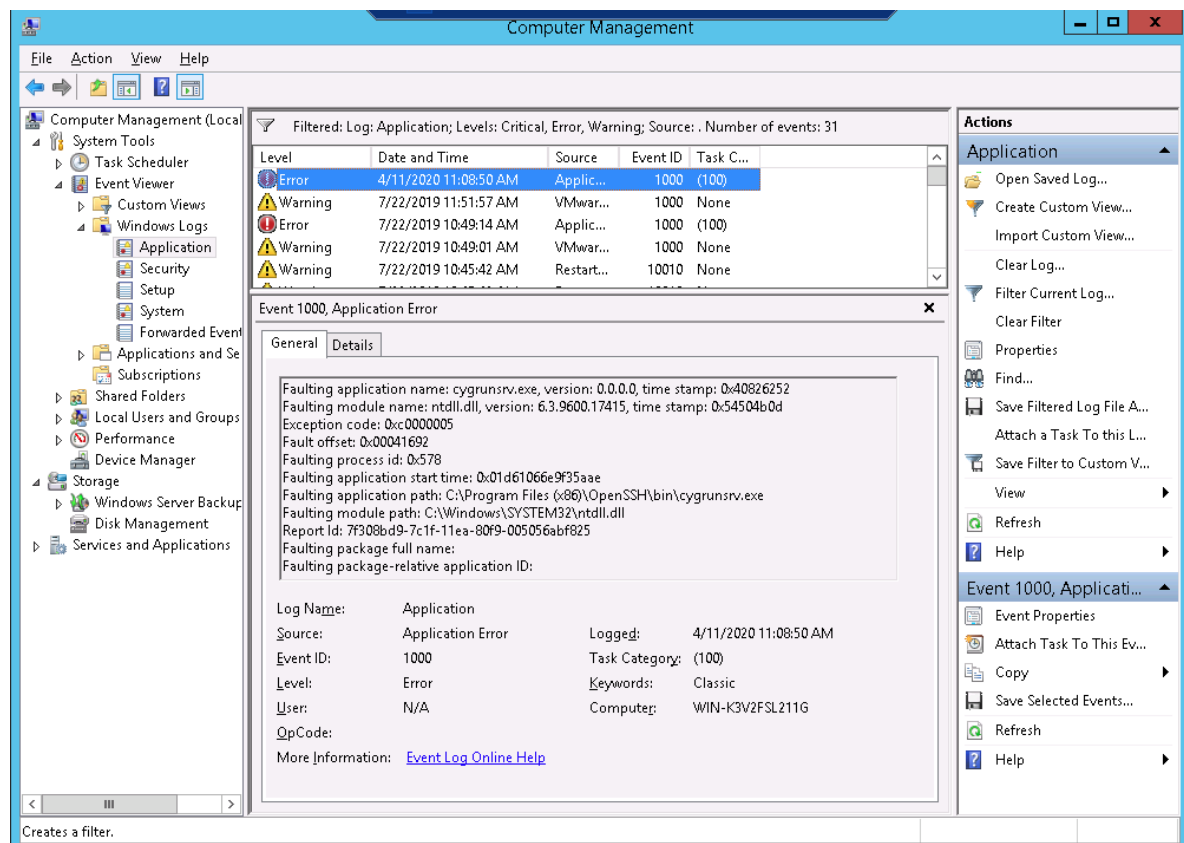
screen capture showing the current system performance



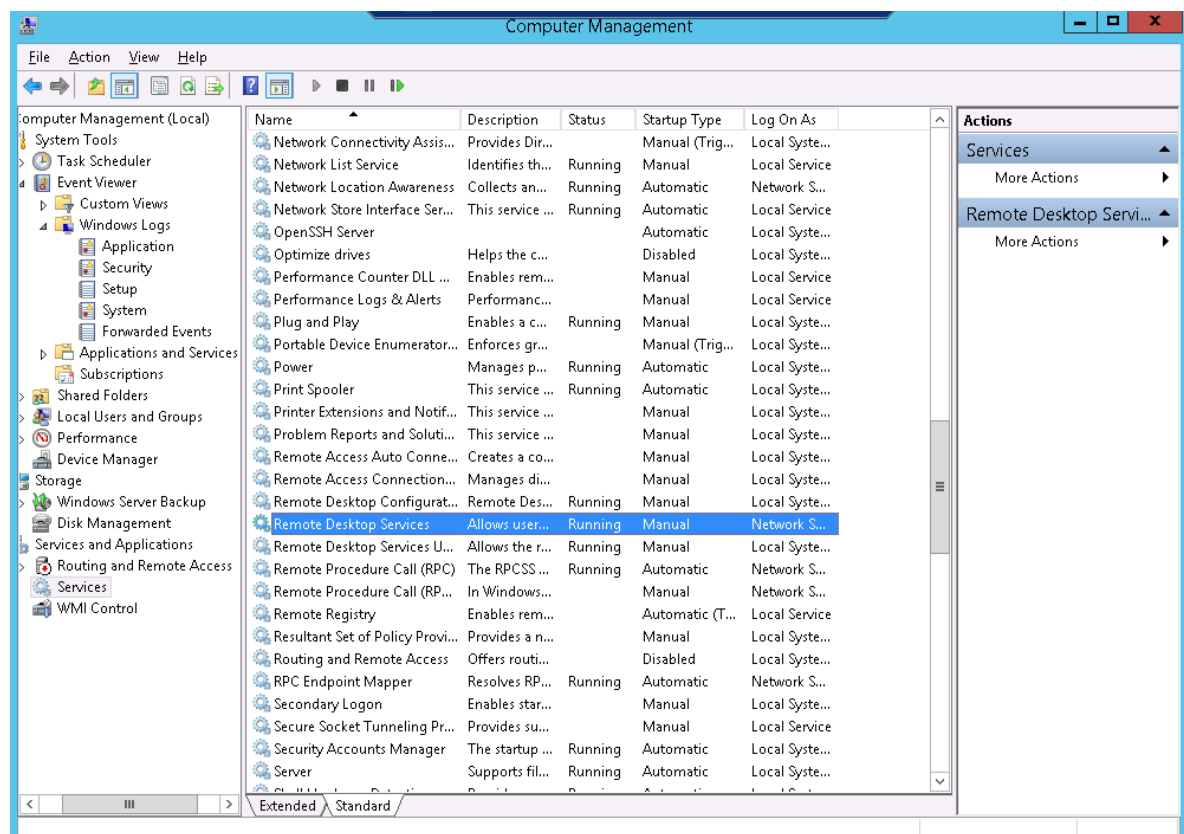
## screen capture showing the Windows Application Log



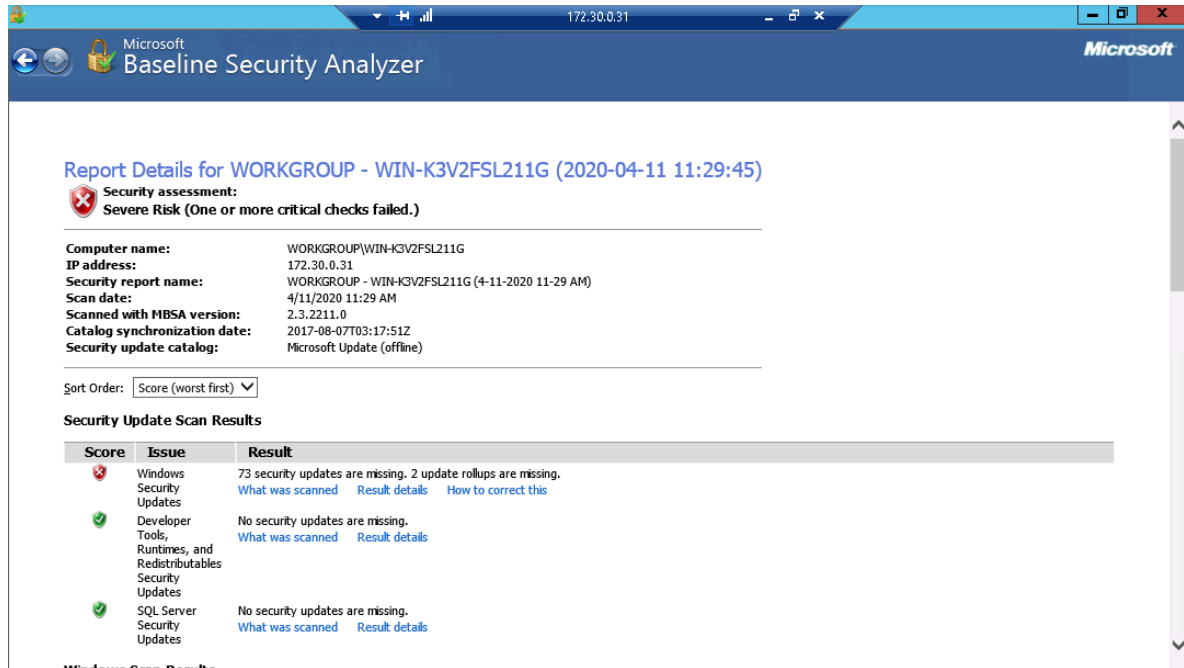
## screen capture showing the entire event entry for the error



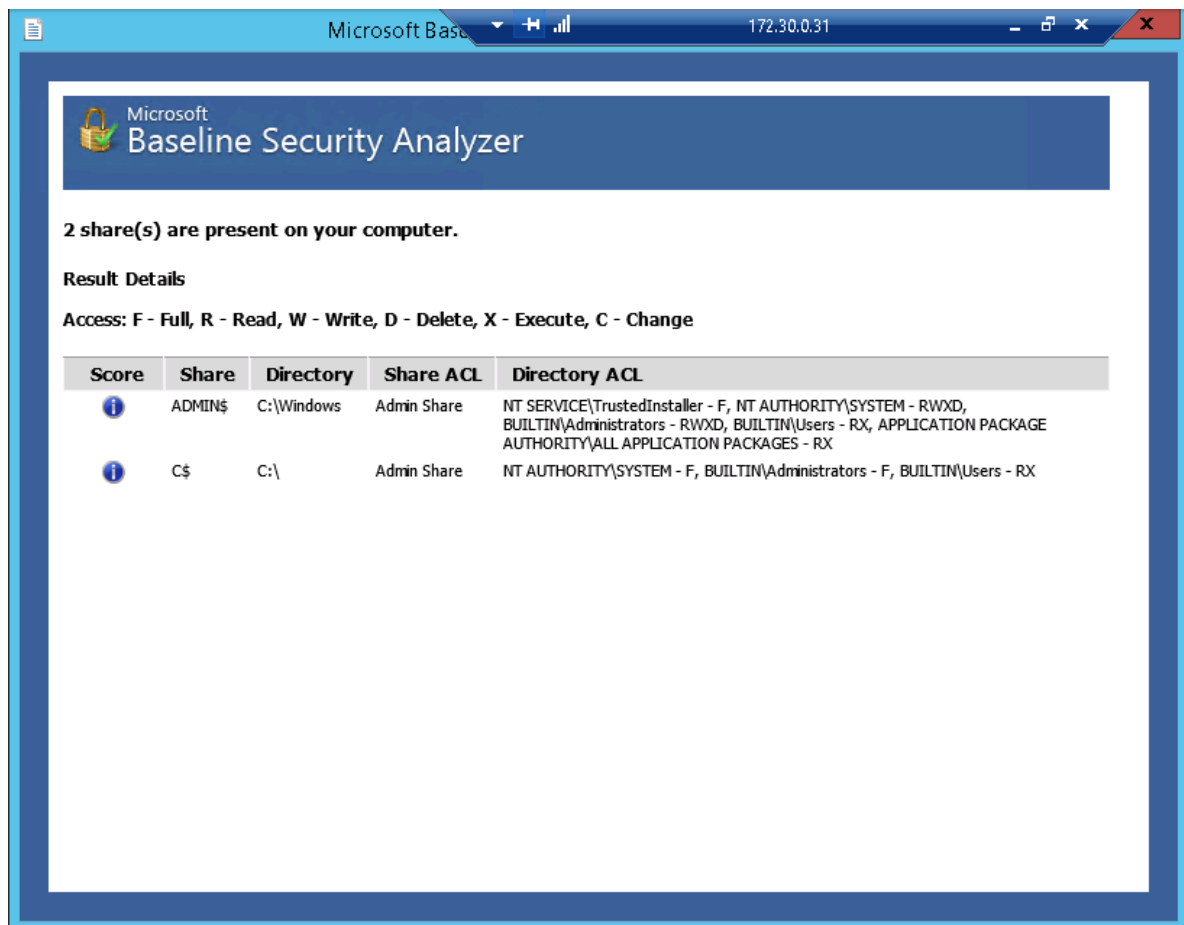
## screen capture showing the Status and Startup Type columns for the Windows services that manage Remote Desktop Services



screen capture showing the first page of the report, including the header








screen capture showing the result details for the Shares issue



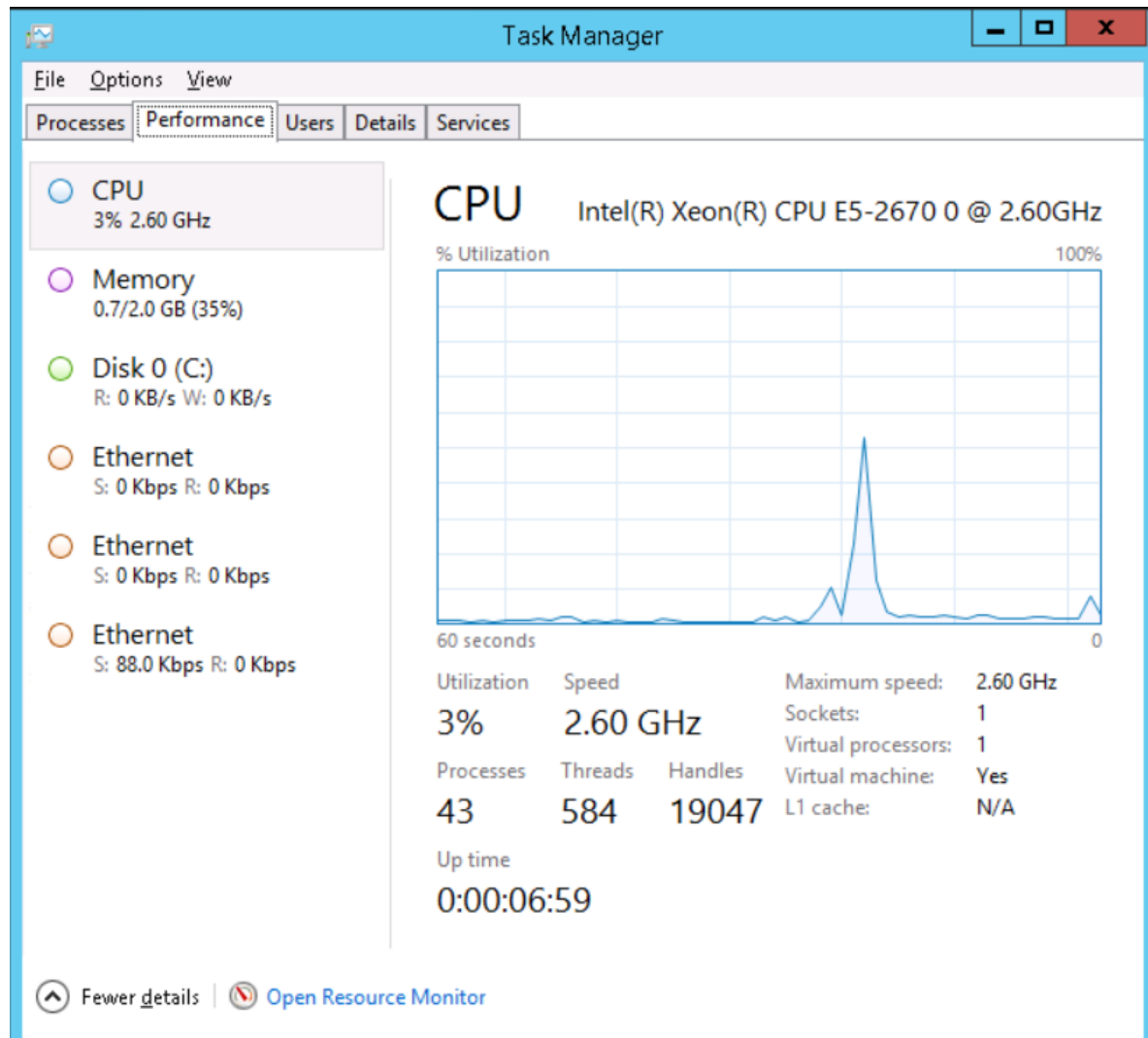
## Section 2

## Part 1

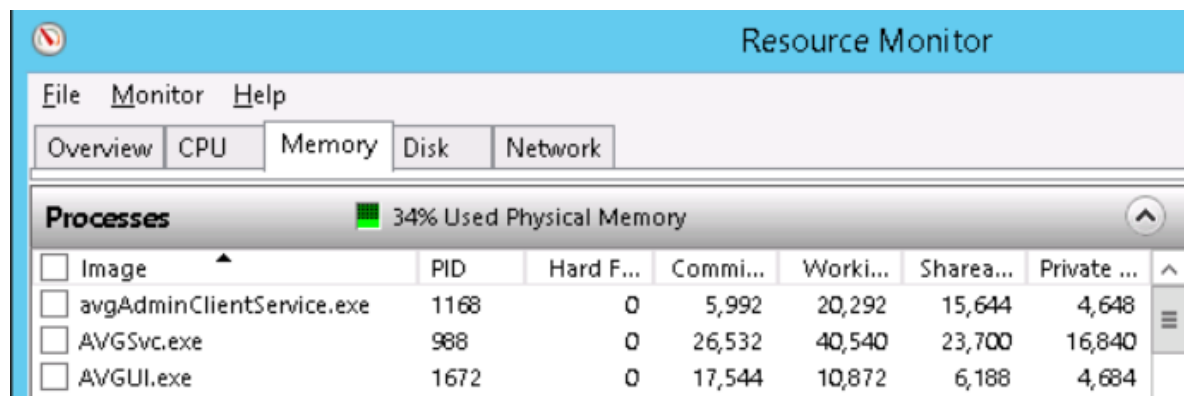
### The services associated with Remote Desktop Services

	RasAuto		Remote Access Auto Connection...	Stopped	netsvcs
	RasMan		Remote Access Connection Man...	Stopped	netsvcs
	SessionEnv	772	Remote Desktop Configuration	Running	netsvcs
	TermService	2152	Remote Desktop Services	Running	termsvcs
	UmRdpService	1352	Remote Desktop Services UserM...	Running	LocalSystemN...

### The current system performance



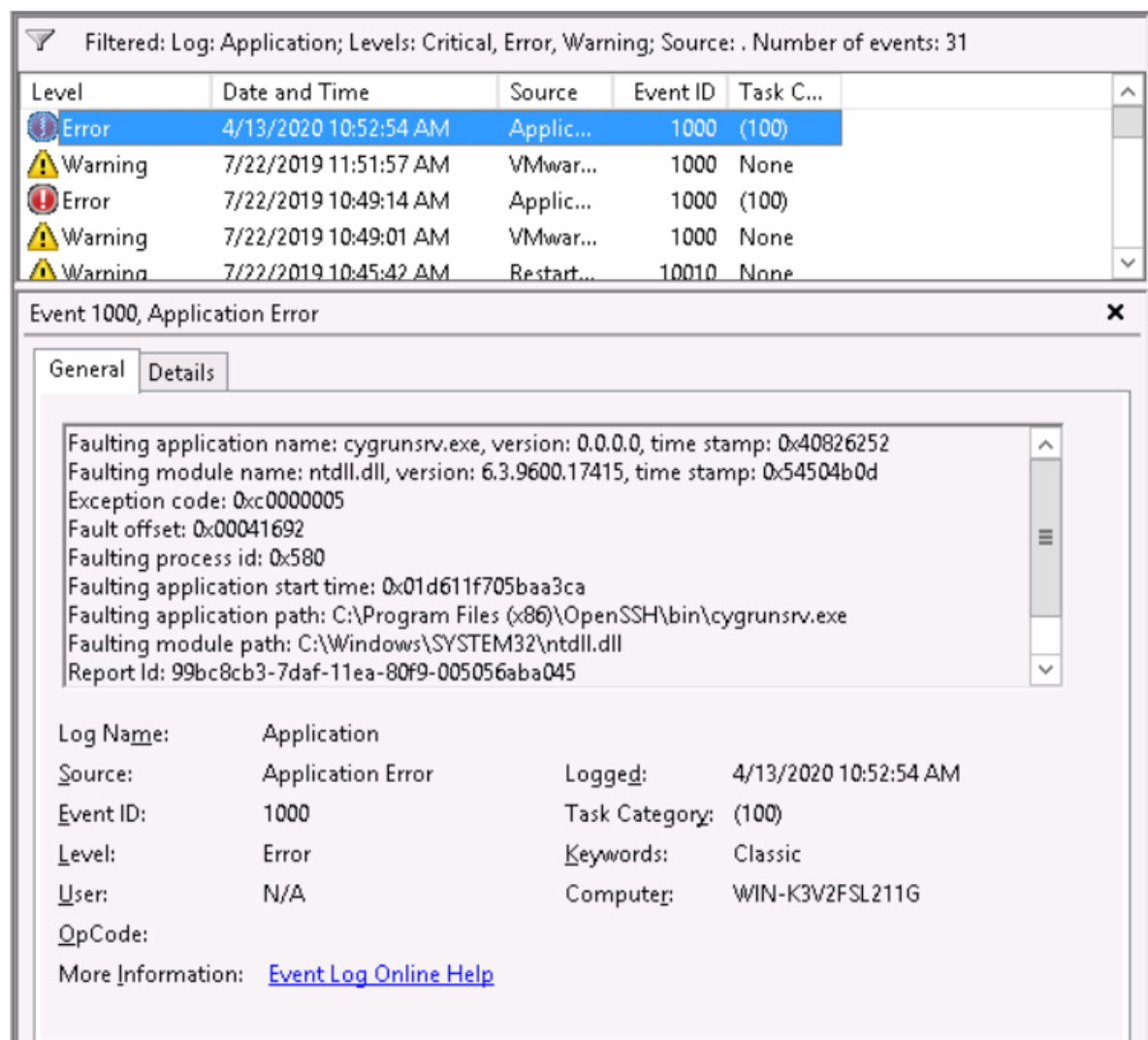
### The AVG processes displayed on the Memory tab of the Resource Monitor



## The AVG update URL displayed in the Resource Monitor

AVGUI.exe	1672	r-23-44-62-5.ff.avast.com	34
-----------	------	---------------------------	----

## The entire entry for the first Application error in the Application logs



## The entire entry for the first Application error in the System logs

Filtered: Log: System; Levels: Critical, Error, Warning; Source: . Number of events: 63

Level	Date and Time	Source
Error	4/13/2020 5:52:46 PM	Service Con
Warning	4/13/2020 5:52:45 PM	AFD
Warning	7/22/2019 11:51:58 AM	Windows R
Error	7/22/2019 10:49:11 AM	Service Con

Event 7000, Service Control Manager

General Details

The UAC File Virtualization service failed to start due to the following error:  
This driver has been blocked from loading

Log Name: System  
Source: Service Control Manager  
Event ID: 7000  
Level: Error  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 4/13/2020 5:52:46 PM  
Task Category: None  
Keywords: Classic  
Computer: WIN-K3V2FSL211G

The entire entry for the first Security issue in the Windows Security logs

Keywords	Date and Time	Source	Event ID	Task Category
Audit Succ...	4/13/2020 10:56:09 AM	Microsoft Wi...	4672	Special Logon
Audit Succ...	4/13/2020 10:56:09 AM	Microsoft Wi...	4624	Logon
Audit Succ...	4/13/2020 10:56:09 AM	Microsoft Wi...	4648	Logon
Audit Succ...	4/13/2020 10:56:09 AM	Microsoft Wi...	4776	Credential Vali...
Audit Succ...	4/13/2020 10:56:09 AM	Microsoft Wi...	4672	Special Logon
Audit Succ...	4/13/2020 10:56:09 AM	Microsoft Wi...	4624	Logon

Event 4672, Microsoft Windows security auditing.

General

Details

Special privileges assigned to new logon.

Subject:

Security ID: WIN-K3V2FSL211G\Administrator  
Account Name: Administrator  
Account Domain: WIN-K3V2FSL211G  
Logon ID: 0x659DA

Privileges: SeSecurityPrivilege

Log Name: Security  
Source: Microsoft Windows security  
Event ID: 4672  
Level: Information  
User: N/A  
OpCode: Info  
More Information: [Event Log Online Help](#)

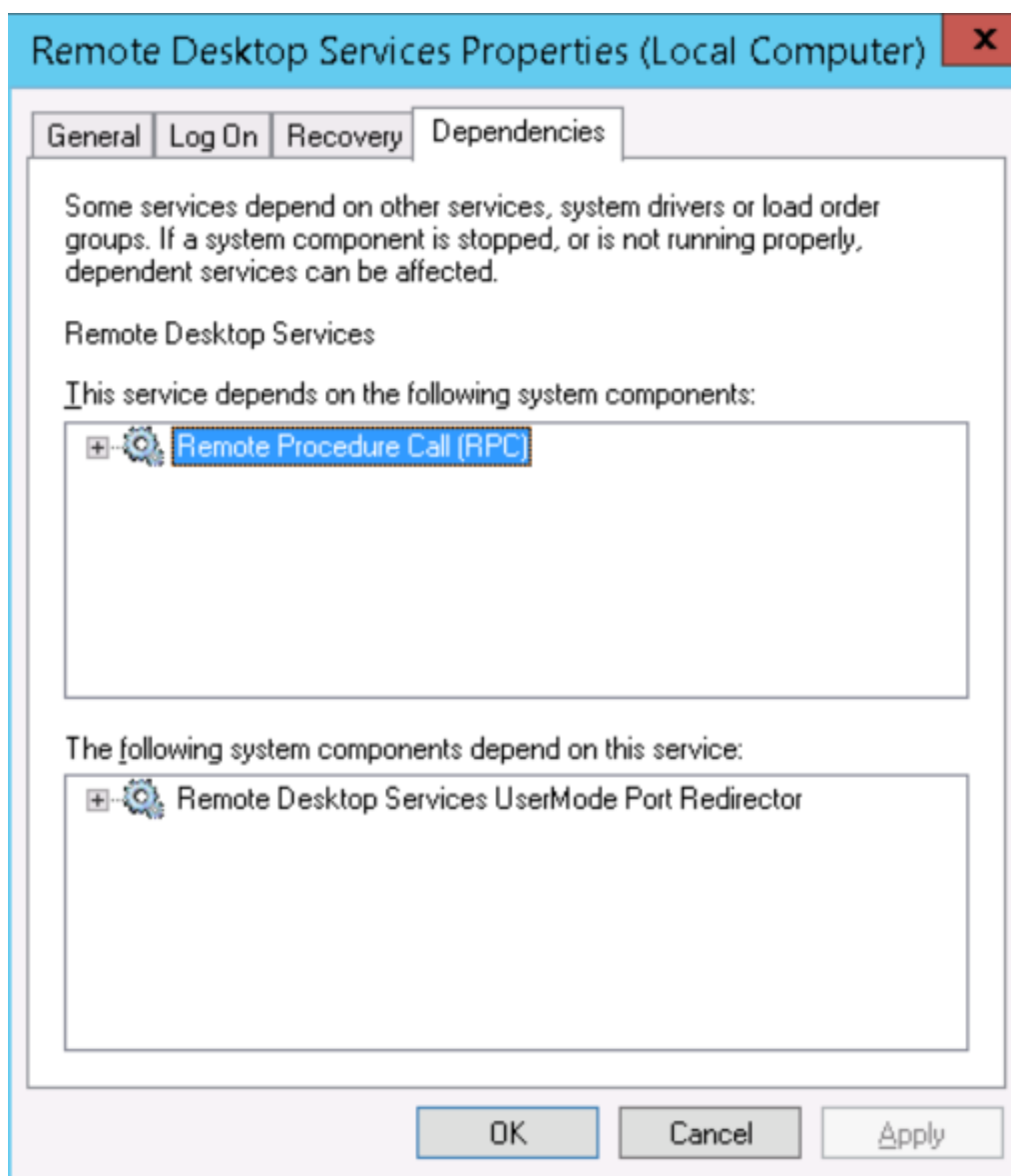
Logged: 4/13/2020 10:56:09 AM  
Task Category: Special Logon  
Keywords: Audit Success  
Computer: WIN-K3V2FSL211G

## The Windows services that manage Remote Desktop Services

Name	Description	Status	Startup Type	Log On As
Remote Desktop Services	Allows user...	Running	Manual	Network S...
Remote Desktop Services U...	Allows the r...	Running	Manual	Local Syste...

## The Dependencies of the Remote Desktop Services service





## Part 2

### The MBSA report results

## Report Details for WORKGROUP - WIN-K3V2FSL211G (2020-04-13 11:15:22)



### Security assessment:

Severe Risk (One or more critical checks failed.)

**Computer name:** WORKGROUP\WIN-K3V2FSL211G  
**IP address:** 172.30.0.31  
**Security report name:** WORKGROUP - WIN-K3V2FSL211G (4-13-2020 11-15 AM)  
**Scan date:** 4/13/2020 11:15 AM  
**Scanned with MBSA version:** 2.3.2211.0  
**Catalog synchronization date:** 2017-08-07T03:17:51Z  
**Security update catalog:** Microsoft Update (offline)

Sort Order:

### Security Update Scan Results

Score	Issue	Result
	Windows Security Updates	73 security updates are missing. 2 service packs or update rollups are missing. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. <a href="#">What was scanned</a> <a href="#">Result details</a>

## The first page of critical updates

### Security Updates

Items marked with are confirmed missing. Items marked with are confirmed missing and are not approved by your system administrator.

Score	ID	Description	Maximum Severity
	MS14-068	<a href="#">Security Update for Windows Server 2012 R2 (KB3011780)</a>	Critical
	MS14-057	<a href="#">Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2978041)</a>	Critical
	MS16-087	<a href="#">Security Update for Windows Server 2012 R2 (KB3170455)</a>	Critical
	4034672	<a href="#">2017-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4034672)</a>	Critical
	MS16-144	<a href="#">December, 2016 Security Only Quality Update for Windows Server 2012 R2 (KB3205400)</a>	Critical
	4019213	<a href="#">2017-05 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4019213)</a>	Critical
	4015547	<a href="#">April, 2017 Security Only Quality Update for Windows Server 2012 R2 (KB4015547)</a>	Critical
	MS17-008	<a href="#">March, 2017 Security Only Quality Update for Windows Server 2012 R2 (KB4012213)</a>	Critical
	MS16-057	<a href="#">Security Update for Windows Server 2012 R2 (KB3156059)</a>	Critical
	4025333	<a href="#">2017-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4025333)</a>	Critical
	MS16-142	<a href="#">November, 2016 Security Only Quality Update for Windows Server 2012 R2 (KB3197873)</a>	Critical
	4034681	<a href="#">2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)</a>	Critical
	MS16-120	<a href="#">October, 2016 Security Only Quality Update for Windows Server 2012 R2 (KB3192392)</a>	Critical
	4022717	<a href="#">2017-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4022717)</a>	Critical
	MS16-076	<a href="#">Security Update for Windows Server 2012 R2 (KB3162343)</a>	Important
	MS16-092	<a href="#">Security Update for Windows Server 2012 R2 (KB3169704)</a>	Important
	MS15-060	<a href="#">Security Update for Windows Server 2012 R2 (KB3059317)</a>	Important

## The scan results that no longer include the update that was installed

72 security updates are missing. 2 service packs or update rollups are missing.

### Result Details for Windows

### Security Updates

Items marked with are confirmed missing. Items marked with are confirmed missing and are not approved by your system administrator.

Score	ID	Description	Maximum Severity
	MS14-057	<a href="#">Security Update for Microsoft .NET Framework 4.5.1 and 4.5.2 on Windows 8.1 and Windows Server 2012 R2 x64-based Systems (KB2978041)</a>	Critical
	MS16-087	<a href="#">Security Update for Windows Server 2012 R2 (KB3170455)</a>	Critical
	4034672	<a href="#">2017-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4034672)</a>	Critical
	MS16-144	<a href="#">December, 2016 Security Only Quality Update for Windows Server 2012 R2 (KB3205400)</a>	Critical
	4019213	<a href="#">2017-05 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4019213)</a>	Critical
	4015547	<a href="#">April, 2017 Security Only Quality Update for Windows Server 2012 R2 (KB4015547)</a>	Critical
	MS17-008	<a href="#">March, 2017 Security Only Quality Update for Windows Server 2012 R2 (KB4012213)</a>	Critical
	MS16-057	<a href="#">Security Update for Windows Server 2012 R2 (KB3156059)</a>	Critical
	4025333	<a href="#">2017-07 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4025333)</a>	Critical
	MS16-142	<a href="#">November, 2016 Security Only Quality Update for Windows Server 2012 R2 (KB3197873)</a>	Critical
	4034681	<a href="#">2017-08 Security Monthly Quality Rollup for Windows Server 2012 R2 for x64-based Systems (KB4034681)</a>	Critical
	MS16-120	<a href="#">October, 2016 Security Only Quality Update for Windows Server 2012 R2 (KB3192392)</a>	Critical
	4022717	<a href="#">2017-06 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4022717)</a>	Critical
	MS16-076	<a href="#">Security Update for Windows Server 2012 R2 (KB3162343)</a>	Important
	MS16-092	<a href="#">Security Update for Windows Server 2012 R2 (KB3169704)</a>	Important
	MS15-060	<a href="#">Security Update for Windows Server 2012 R2 (KB3059317)</a>	Important
	MS16-014	<a href="#">Security Update for Windows Server 2012 R2 (KB3126041)</a>	Important

**KB number of installed update:**

KB3011780