Windows Server®

SERVER MAINTENANCE

TOP 10 BEST PRACTICES

Windows Server Maintenance is essential to maximize uptime and minimize disruption due to neglected maintenance. This guide lists the Top Ten Best Practices all Server administrators should follow.

TOP 10 BEST PRACTICES

#10. IMPLEMENT A REGULAR MAINTENANCE SCHEDULE

#9. AUTOMATE EVERYTHING + MANAGE BY EXCEPTION

#8. RUN WEEKLY WINDOWS UPDATES + INSTALL ALL SECURITY PATCHES

#7. REBOOT

#6. DOMINO HOUSEKEEPING

#5. DISKSPACE, DEFRAG AND MEMORY

#4. RUNNING SOFTWARE INVENTORY

#3. STAGGER UPDATES

#2. RUN DURING WEEKDAYS

#1. REPORT RESULTS

TAKE GOOD CARE OF YOUR SERVERS

AND YOUR SERVERS WILL TAKE GOOD CARE OF YOU *

***AND YOUR USERS**

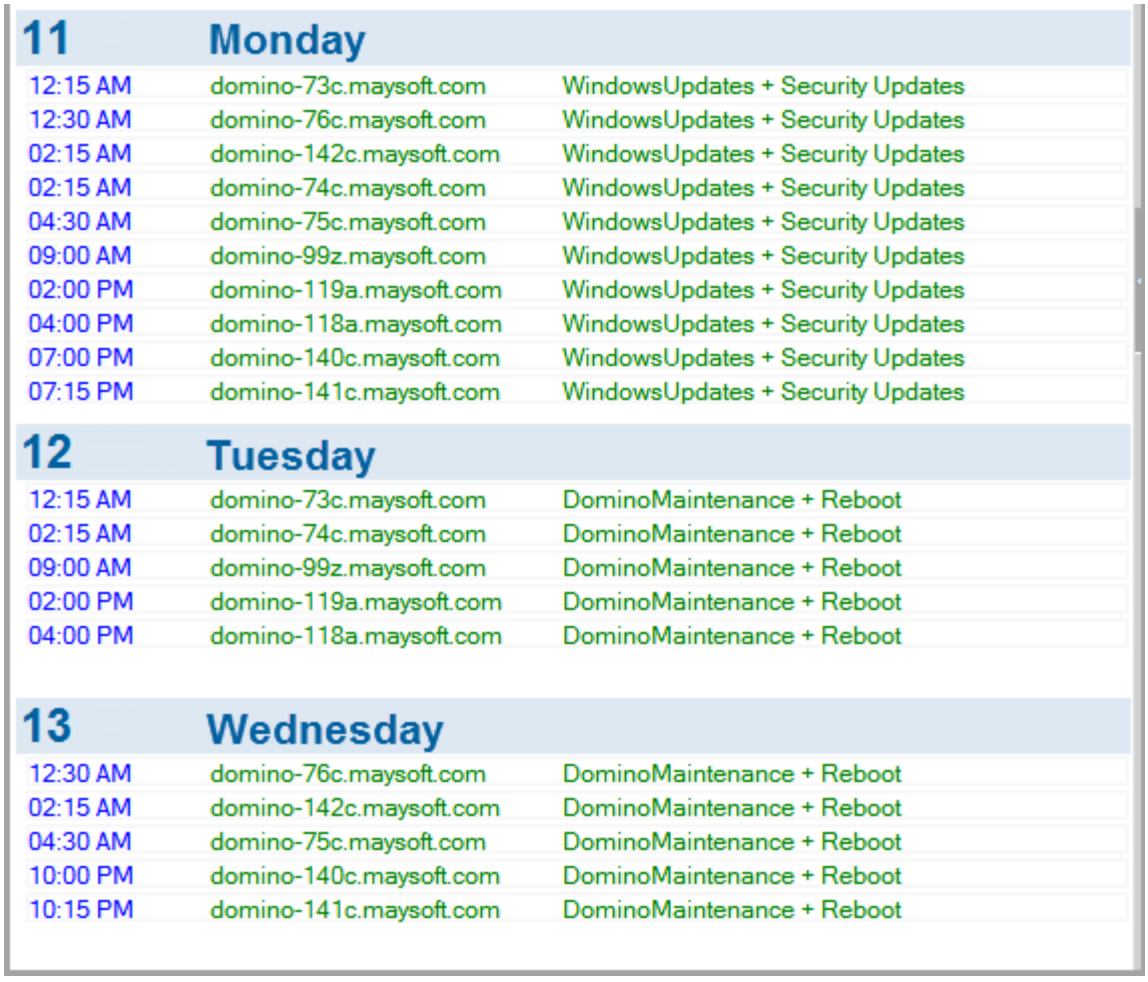
#10. IMPLEMENT A REGULAR MAINTENANCE SCHEDULE

This is the first and most important step. Put all of your servers on a weekly schedule which **includes a server reboot**.

Once you have a schedule, you can look at it, present it to management or your Change Control Group so everyone will know when your servers will be unavailable due to maintenance. You can also check for conflicts with critical business processes and move the maintenance window to a more convenient time.

Also, any server downtime alerts that you have in place can be disabled or ignored during your maintenance window.

But most importantly, you know that all of your servers are being maintained weekly and therefore you maximize availability for your servers to work for you.



11	Monday	
12:15 AM	domino-73c.maysoft.com	WindowsUpdates + Security Updates
12:30 AM	domino-76c.maysoft.com	WindowsUpdates + Security Updates
02:15 AM	domino-142c.maysoft.com	WindowsUpdates + Security Updates
02:15 AM	domino-74c.maysoft.com	WindowsUpdates + Security Updates
04:30 AM	domino-75c.maysoft.com	WindowsUpdates + Security Updates
09:00 AM	domino-99z.maysoft.com	WindowsUpdates + Security Updates
02:00 PM	domino-119a.maysoft.com	WindowsUpdates + Security Updates
04:00 PM	domino-118a.maysoft.com	WindowsUpdates + Security Updates
07:00 PM	domino-140c.maysoft.com	WindowsUpdates + Security Updates
07:15 PM	domino-141c.maysoft.com	WindowsUpdates + Security Updates
12	**Tuesday**	
12:15 AM	domino-73c.maysoft.com	DominoMaintenance + Reboot
02:15 AM	domino-74c.maysoft.com	DominoMaintenance + Reboot
09:00 AM	domino-99z.maysoft.com	DominoMaintenance + Reboot
02:00 PM	domino-119a.maysoft.com	DominoMaintenance + Reboot
04:00 PM	domino-118a.maysoft.com	DominoMaintenance + Reboot
13	**Wednesday**	
12:30 AM	domino-76c.maysoft.com	DominoMaintenance + Reboot
02:15 AM	domino-142c.maysoft.com	DominoMaintenance + Reboot
04:30 AM	domino-75c.maysoft.com	DominoMaintenance + Reboot
10:00 PM	domino-140c.maysoft.com	DominoMaintenance + Reboot
10:15 PM	domino-141c.maysoft.com	DominoMaintenance + Reboot

#9. AUTOMATE EVERYTHING + MANAGE BY EXCEPTION

Almost any task that you run at the server console can be automated and scheduled. If you do any maintenance regularly, or at least four times per year, we recommend automating it.

There are two main reasons:

1. Once automated, it is much less prone to human errors. Our experience is that human errors or oversights are a big reason why maintenance is not performed, or performed incorrectly.

2. Automated tasks have much better Run Tracking Logs for history and troubleshooting.

Once all of these maintenance tasks are automated, you can then **Manage by Exception** and only work on failed server upgrades when, for example, the server does not return to service after a reboot.

#8. RUN WEEKLY WINDOWS UPDATES + INSTALL ALL SECURITY PATCHES

Run Windows updates weekly. DISABLE the automatic updates. Automatic updates blindly reboot your server and can interrupt other important processes (like server backups).

Windows updates does not know anything about Domino, so it exits and oftentimes Domino does not stop gracefully, leaving open databases. When Domino restarts, consistency checks are required, slowing down the restart while the corruption in the databases, caused by the surprise reboot, is fixed.

Viruses and hackers look for **unpatched servers**, and use the Microsoft patch list as a "what-to-hack" guide. With Cryptolocker approaching a $ 500 million business, you can be sure that your server is being probed for vulnerabilities. Once you are on a weekly automated schedule, you are much less prone to these exploits. **Don't let it be your server that is compromised.**

#7. REBOOT

Windows servers like to be rebooted weekly. We know some server administrators like to brag how long a server has been running without a reboot, as if that means the server is “beefy”. However, many Windows 3rd party applications “leak” memory and eventually crash, or start running sluggishly. Server performance degradation is the result.

Automatically monitor servers that are rebooting to ensure they start properly and complete the cycle. This should be part of **#9. AUTOMATE EVERYTHING** where every maintenance task is “closed” as “completed” only after the server “wakes up” and “checks in”.

Server performance is always improved with server reboots.

#6. DOMINO HOUSEKEEPING

Domino likes to have certain housekeeping done, like compacting mail databases **(mail.box, mail1.box, mail2.box etc).**

Many Domino databases (.NSF files) cannot be compacted with Domino running because they are locked by the server. Log.nsf is one of those databases. This is a very common error on the Domino console:
“Cannot write to log file: Database is corrupt -- Cannot allocate space.".

Deleting the log.nsf (with an archive copy) weekly prevents this problem situation and can only be done with Domino stopped.

Cleaning up other databases like names.nsf with an fixup and updall is also recommended weekly.

User Mail files should be compacted using the option while the Domino server is running, and is not recommended to be run while Domino is stopped as some of these files can take hours to compact, causing too much server downtime.

Regular stopping of Domino will result in clean shutdowns. Servers with extended Domino uptime, greater than one month, oftentimes do not stop cleanly, and results in having to execute a -**kill** command, which is not recommended. In addition, weekly **rebooting** also improves overall server response time and helps keep the server from crashes that occur due to long uptime.

#5. DISKSPACE, DEFRAG AND MEMORY

Running low on disk space is a problem that is unrecoverable in Windows. Monitoring percent utilization and flagging it in the Run Report is critical to staying ahead of this problem.

Likewise, a highly fragmented disk can adversely affect server performance and it will appear “slow” to users.

Low Free Memory also is a problem that will cause disk thrashing and significantly reduce server performance.

Reporting on any 3 of these conditions is useful. Unfortunately only disk defragmentation can be automated. Disk space and memory need to be addressed by an administrator who knows what files can be deleted or can add more disk storage.

#4. RUNNING SOFTWARE INVENTORY

Looking what software is actually loaded tells a lot about server performance issues. Many times software is running that is expired or no longer needed, and perhaps interferes with other software (like backup software).

Uninstalling expired or unneeded software can provide more Free Memory. It can also warn you of any other processes, like data backup processes, that are running and could be connected to Domino and not allow a server shutdown.

#3. STAGGER UPDATES

If you have server clusters for failover, it is important that these updates be staggered at least one day apart. That way, if, for example, a Windows driver update causes problems, these can be resolved before the cluster-mate is updated.

If you have two SMTP servers, you should never stop them both at the same time. A popular schedule staggering is every other week (one server every two weeks). This is good for humans, so they can remember one server every Saturday. However, with automation, we prefer a **weekly** schedule like this:

SMTP1: Monday

SMTP2: Wednesday

#2. RUN DURING WEEKDAYS

We strongly recommend running these updates Monday through Thursday nights.

Let us explain why.

Everyone does updates on weekends. No one asks why. The answer is that it is when server utilization is low (users generally are not using the servers) AND the server administrators have the time to run the updates. But running updates on weekends means that the server administrator has to give up one weekend per month to run updates. This causes 2 problems:

1. The Servers only are updated monthly
2. The Server Administrator does not like giving up a weekend and may rush or skip steps that are deemed “non-critical”

But if the updates are automated, then they can be run at another time when even fewer people are using the machines: around midnight. Automated software does not mind working late at night (but administrators do). If there is any problem, your full staff is available to resolve it (and our full staff is available, too).

Ending weekend work is a win for everyone.

#1. REPORT RESULTS

A report that shows what happened is essential to managing server health and uptime. It highlights any issues or tells you **"Success" don't worry!**

[SUCCESS] (Belle/Maysoft) Windows Update Domino Cleanup + Reboot
ServerSentinel to: Frank Paolino

Server	Belle/Maysoft
Task	Windows Update Domino Cleanup + Reboot
Company	Maysoft
Result	Success
Elapsed Time	12:02 AM - 12:41 AM

12:02:55 AM Starting Maintenance
12:03:11 AM: Begin Domino Shutdown
12:03:29 AM Telling SMTP to quit.
12:03:35 AM Telling HTTP to quit.
12:03:41 AM Telling replica to quit.
12:03:59 AM Telling Update to quit.
12:04:05 AM Telling AMGR to quit.
12:04:11 AM Telling Indexer to quit.
12:04:17 AM Telling LDAP to quit.
12:04:23 AM Telling AdminP to quit.
12:04:29 AM Telling ProcMon to quit.
12:05:53 AM Telling Router to quit.
12:05:59 AM Telling Domino to quit.
12:06:05 AM End Domino Shutdown
Time for Domino Shutdown = 3.4 minutes.

12:06:20 AM Starting Windows Updates.
12:06:21 AM Starting Windows Update service
12:06:29 AM Running Windows Update.

2 Accepted KB3126587 29 MB Security Update for Windows Server 2008 R2 x64 Edition (KB3126587)
2 Accepted KB890830 5 MB Windows Malicious Software Removal Tool x64 - February 2016 (KB890830)
2 Accepted KB3126593 30 MB Security Update for Windows Server 2008 R2 x64 Edition (KB3126593)
2 Accepted KB3127220 424 KB Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64 (KB3127220)
2 Accepted KB3127229 1 MB Security Update for Microsoft .NET Framework 4.5.2 on Windows 7, Vista, Windows Server 2008, Windows Server 2008 R2 for x64 (KB3127229)
2 Accepted KB3134814 85 MB Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems (KB3134814)
2 Accepted KB3135445 3 MB Update for Windows Server 2008 R2 x64 Edition (KB3135445)

3 Downloaded KB3126587 29 MB Security Update for Windows Server 2008 R2 x64 Edition (KB3126587)
3 Downloaded KB890830 5 MB Windows Malicious Software Removal Tool x64 - February 2016 (KB890830)
3 Downloaded KB3126593 30 MB Security Update for Windows Server 2008 R2 x64 Edition (KB3126593)

3 Downloaded KB3127220 424 KB Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64 (KB3127220)
3 Downloaded KB3127229 1 MB Security Update for Microsoft .NET Framework 4.5.2 on Windows 7, Vista, Windows Server 2008, Windows Server 2008 R2 for x64 (KB3127229)
3 Downloaded KB3134814 85 MB Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems (KB3134814)
3 Downloaded KB3135445 3 MB Update for Windows Server 2008 R2 x64 Edition (KB3135445)

4 Installed KB3126587 29 MB Security Update for Windows Server 2008 R2 x64 Edition (KB3126587)
4 Installed KB890830 5 MB Windows Malicious Software Removal Tool x64 - February 2016 (KB890830)
4 Installed KB3126593 30 MB Security Update for Windows Server 2008 R2 x64 Edition (KB3126593)
4 Installed KB3127220 424 KB Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64 (KB3127220)
4 Installed KB3127229 1 MB Security Update for Microsoft .NET Framework 4.5.2 on Windows 7, Vista, Windows Server 2008, Windows Server 2008 R2 for x64 (KB3127229)
4 Installed KB3134814 85 MB Cumulative Security Update for Internet Explorer 11 for Windows Server 2008 R2 for x64-based Systems (KB3134814)
4 Installed KB3135445 3 MB Update for Windows Server 2008 R2 x64 Edition (KB3135445)

12:20:54 AM Windows Update complete
12:20:54 AM Windows requires Server reboot.

Starting Domino Maintenance.

12:20:54 AM Log.nsf size is 6,318.25MB
12:20:54 AM Log file renamed to D:\Lotus\Domino\data\log.nsf.2016-02-27--12-20-54
12:20:54 AM Log file moved to D:\archive
12:23:35 AM Names.nsf starting size is 1,002MB
12:23:35 AM Names.nsf ending size is 505MB
12:30:03 AM Names.nsf index update complete
12:30:26 AM DDM.nsf starting size is 63.75MB
12:30:26 AM DDM.nsf ending size is 57.25MB
12:30:37 AM DDM.nsf index update complete
12:32:05 AM MTStore starting size is 1,075MB
12:32:05 AM MTStore ending size is 155MB
12:39:06 AM Admin4.nsf starting size is 2,310.75MB
12:39:06 AM Admin4.nsf ending size is ,090.5MB
12:39:43 AM Admin4.nsf index update complete
12:40:05 AM StatRep.nsf starting size is 113MB
12:40:05 AM StatRep.nsf ending size is 8MB
12:40:13 AM StatRep.nsf index update complete
12:40:34 AM Events4.nsf starting size is 56.75MB
12:40:34 AM Events4.nsf ending size is 44.25MB
12:40:46 AM Events4.nsf index update complete
12:40:58 AM mail1.box starting size is 540MB
12:40:58 AM mail1.box ending size is 5MB
12:41:09 AM mail2.box starting size is 353MB
12:41:09 AM mail2.box ending size is 27MB
12:41:11 AM Domino Maintenance Complete.

Time for Entire Server Maintenance = 38.4 minutes.
12:41:16 AM Finished. Start server reboot
12:41:16 AM Maintenance complete.

