

Re: Auto-Updates for production servers

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2007-10/msg01417.html>

- *From:* "SBS Rocker" <noreply@xxxxxxxxxxxxx>
 - *Date:* Tue, 30 Oct 2007 09:18:57 -0700
-

I think your misunderstanding Brian's problem here. Apparently he has no issues with servers being updated. His issues are with servers being updated during business hours where it affects production time and work if I understand correctly. Brian I find it hard to believe that management would not work with you on this especially if it affects yours and others work. Why not propose they schedule their auto updates say like every evening at midnight?

"Anthony" <anthony.spam@xxxxxxxxxxxxx> wrote in message news:%23KOHyzsGIHA.3548@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

OK, so you have a specific problem with the update options. I would take a look at the Group Policies for Windows Updates and suggest to them which ones would make your life easier.

<http://technet2.microsoft.com/windowsserver/en/library/51c8a814-6665-4d50-a0d8-2ae27e69ca7c1033.msp>

It sounds as though the one that is affecting you is "No auto-restart for scheduled Automatic Updates installation". That reboot prompt would only happen if:

- the production server was switched off at the scheduled time, and so the installation happens when it restarts, or
- a user is logged in either at the scheduled time (but it's supposed to be out-of-hours).

So I would talk to them about the specific update options: when is the scheduled time, and what options are they using?

Hope that helps,

Anthony, <http://www.airdesk.co.uk>

"Brian Kitt" <BrianKitt@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:1548528A-3E6A-460E-AF22-5FD215FBC738@xxxxxxxxxxxxxxxxxxxx

Sorry Anthony, you misunderstand the problem. I totally agree with keeping the servers up to date. Every Friday night, or whatever, is perfect.

HOWEVER, that is not what I am asking about.

Re: Auto-Updates for production servers

They have the actual Windows Auto-Update on which applies all updates on an 'as released basis' from Microsoft. In other words, updates go on production servers, and nobody, not even them, have any idea which updates went on or when. Since auto-updates are on, the 'you need to reboot your server now' function keeps trying to reboot servers. For example, every time we log on to terminal services, we are prompted to reboot because of auto-updates. However, we don't have authority to reboot, so the box is grayed out. We just have to cancel the prompt. This prompt comes up every 10 or 15 minutes. There are days when I will work for 10 hours through terminal services, for every day of the week, so there are times, that for 40 or 50 hour work week, I am canceling that dang prompt every 10 minutes. It is not unusual that I may have to tunnel through 2 or 3 levels of terminal services, so take the every 10 or 15 minutes times 2 or 3.

To me, this is down and out wreckless to just apply updates to production without any knowledge whatsoever of what is being applied.

"Anthony" wrote:

Hi Brian,
I hope you won't mind advice that contradicts your presumed views.
When Microsoft or any software vendor discovers a flaw that can be exploited, they need to fix it.
If you don't apply the fix, you are vulnerable from that time on because everyone knows what the flaw is.
You can test the fix to see if it breaks anything, but you still need to apply it even if it does.
So really it could be a responsibility of the developers to be aware of fixes, maintain a testing environment and identify what to do if a fix breaks their software. They would then need to deploy their own patch within a week or two. If they object to having to test, it demonstrates that it

Re: Auto-Updates for production servers

is
really an argument about who should do the work rather than
whether it
should be done.

The only way to avoid patching, or to postpone it till the
developers
are
ready, is to maintain a sealed environment. You can do this
as follows:

- run the application on terminal services
- allow no other applications to run: no IE, no Word, no
iTunes etc,
just
the application.
- run a firewall between the LAN and the terminal servers
and allow no
other
connections to the terminal servers.

Apart from that, you just have to live with patching. What
problems
exactly
does it cause? Rebooting should be addressed either by
patching
out-of-hours, or by a resilient service (e.g more than one
application
server). What are the miscellaneous problems? You should
probably
identify
what they are and try to resolve them rather than prevent
patching.

Hope that helps,
Anthony, <http://www.airdesk.co.uk>

"Brian Kitt" <BrianKitt@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
news:FB252A39-79A5-4522-9113-71C1A1303DBB@xxxxxxxxxxxxxxxxxxxx

Hello.
I am a developer, and have been having an
ongoing battle with our
Network
Admins, and would like advice here.

They have Microsoft Windows
Auto-Updates turned on for all production
servers. This has caused numerous problems,
because patches get
applied,
then cause servers to reboot, or other

Re: Auto-Updates for production servers

miscellaneous problems.

I keep trying to tell them it is not a 'best practice' to have auto-updates on for production servers, but rather they should push them out with admin tools on a regular scheduled basis. They assure me they 'know what they are doing', and auto updates 'are required to prevent viruses and hackers'. They have assured me that Microsoft strongly recommends auto updates for all production servers.

The amount of problems alone this has causes ought to be proof enough this is a bad idea, but can anyone point me to 'official' statements from Microsoft as to 'auto-updates' for production servers? I am having trouble finding an official statement from Microsoft either way.