



RUNAS RADIO



<http://www.runasradio.com>



Richard
Campbell

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Greg
Hughes

Text Transcript of Show #135
(Transcription services provided by [PWOP Productions](#))



**Susan Bradley Patches Our Machines with Windows Server Update
Services!
November 18, 2009**



[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #135, with guest Susan Bradley, recorded Sunday, November 1, 2009. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com. You can follow the boys on Twitter at twitter.com/runasradio.

Richard Campbell: Thank you, Brandon. This is RunAs Radio. I'm your host Richard Campbell. With me as always, my co-host Greg Hughes.

Greg Hughes: Hey everyone. What's up, Richard?

Richard Campbell: Not too much, man. We're all dealing with the challenges of life changes and making shows

Greg Hughes: Right. This new recording "studio," which consists of course of a large and well clothed walk-in closet which makes actually for great recording level system, kind of had to move though because the 15-year-old is taking a shower on the other side of the wall and that got noisy.

Richard Campbell: Nice. So now you're in the bedroom?

Greg Hughes: TMI I'm sure, but yeah.

Richard Campbell: Well we've tried to make the best out of a show as we can so let's keep going. I'm dealing with the chaos in my house too. God, I'm only home for 24 hours these days but you know. Let's dive right into the show. We're talking to Susan Bradley. Susan has been passionate about Patch Management since she used to patch her SBS 2000 for Code Red and Nimda. Oh man.

Greg Hughes: Yo, sir.

Richard Campbell: She writes on the topic for Brian Livingstone's Windows Secrets that is an equal opportunity patcher as she has maintained patches for five Windows PCs at home, two Macs, and umpteenth Windows Exchange, SQL Server machines at the Office. She considers visiting the Microsoft Knowledge-based site of KB 894199 as perfectly normal and we're certain you will too after she tells you why you need to bookmark it. The patch that she loves to hate and hates to love our .NET, SQL, and XML, and you can read her topics at the PATCH WATCH column on windowssecrets.com and on her blog at www.sbsdiva.com. Welcome, Susan.

Greg Hughes: Hey, Susan.

Susan Bradley: Thank you.

Greg Hughes: Good to talk to you again.

Richard Campbell: And for the folks who haven't taken the hint, we're going to talk about Update Services today and I didn't realize this when we talk to you also long ago about SBS that obviously Windows Update is a favorite of yours.

Susan Bradley: It's one of the, you know, you love to hate it and you hate to love it. It is on the box and as I said earlier, as you said in the start of the show, I've been patching boxes since Code Red and Ninja days where I slam my Mountain Dew can down on the desk and go running to the server where everybody can stay because I'm about to reboot the server on that day.

Richard Campbell: Right.

Susan Bradley: So it has gotten better since then. That was back in the days when Microsoft would release Patches at any point in time, any day of the week and it was like, "Oh gee, what is that? Oh, my gosh, everybody get off and save."

Greg Hughes: We were patching when patching wasn't cool.

Susan Bradley: We had no patching tools and that's actually why I've been a long time customer of Shavlik, which is a third party patch tool, because I had no patch tool, and then first came trust, and by the way I should say that we should put in a plus for some better marketing people to write better codenames for these patch tools that they have at Microsoft because they're not the greatest in the world as far as calling these patching tools. It was first called SUS, Software Update Services. It's now called WSUS.

Richard Campbell: WSUS.

Susan Bradley: But some people call it WUS or WUSUS. I have no idea exactly what the official wording is. It's just Windows Software Update Services and it's basically a free download. You can augment it with third party products and programs out there that takes it to a higher level of meaning that you can put in your own patches and you can roll up your own third party stuff.

Greg Hughes: Yeah.

Susan Bradley: I can just buy a standalone third party tool called Shavlik that patches for everything else, but basically WSUS patches the core products that we know. Obviously it does Windows Operating System itself, and then on top of that it does Exchange with the exception of Service Packs,



like for example it does not do Exchange 2007 Service Pack 2.0. 2000 Service Pack needs some prerequisites and a little bit of reading of a KB, things that we don't normally do as geeks. You know, we kind of try to not do that.

Richard Campbell: What is this reading thing you're talking about?

Susan Bradley: Yeah, I don't know. We rarely read 140 characters at a time these days I think, no.

Richard Campbell: Nice.

Susan Bradley: So Exchange 2007 Service Pack 2 is not in WSUS so that's why that KB article 894199, you can also get -- my cheaper way of getting intuitive if you Google on WSUS-based SUS content. That's WSUS-based SUS-based content. Google hits first hit all the time. So that KB article is your bible of what WSUS handles and its success. If it's not listed there, it's not going to come down on your machine. So what you do is you install this platform on a server, it needs IIS to be reading on that server.

Richard Campbell: Right.

Susan Bradley: All of the workstations then are set up through a group policy. There's actually a couple of ways that you can do this. It's easier on the domain. In a domain, we've got group policies. You can go up to the group policies setting and say go talk to this WSUS server. It pushes that group policy. They all talk in and they all grab their patches from that server so you don't have like a hundred different workstations all grabbing some Microsoft that does it all the same time.

Greg Hughes: Right.

Susan Bradley: And if you pay, like if you're overseeing, and you pay by the bits for the downloads, that can be pretty expensive if you got 150 machines all getting the same patch pulling it in. WSUS pulls it in one time, your workstation then quit your WSUS server, they then pull it down from your central location, you host the patches if you will.

Greg Hughes: You also get to exercise control there, right?

Susan Bradley: Exactly. If you're a control freak, it's the ultimate nirvana because you are controlling the patches of the network. You say who's going to get them, you say what they're going to get, you can approve, you disapprove like for example there are still 400 million Vista language updates that are sitting on Microsoft unapproved because, I'm sorry, I don't need more and more language on my Vista workstation so I'm not going to approve it. The same way with the Windows 7.0 and you have to

have a new Windows with WSUS 3.0 Service Pack 2.0 on your network in order to support the Windows 7.0 if you do the same thing for the Win 7.0. If you don't want them to have 400 trillion different language patches on there, you don't approve it up on the server.

Greg Hughes: Right.

Susan Bradley: You can also do, if you're in a work group where you don't have it in name, you can actually push out of registry key to off the domain workstation so that they then -- what you do is you set up your WSUS to publish externally, you open up some ports out there and you have it pushing out externally, and then you have your workstations out there pointing at your one master server and again you can control them that way.

Greg Hughes: Cool.

Susan Bradley: I won't get into the legalities of the licensing, if you're a smaller firm you have to look into what's called small licenses because this is when they tell people to take your aspirin, drink a beer, go call a licensing expert because it gets down that nasty road of, oh gosh, let's call those licensing people. But it can be done if you need to host and push out patches for other people too.

Greg Hughes: Got you.

Richard Campbell: But most people get the services through their Volume Licensing Agreement.

Susan Bradley: You don't even have to have a Volume Licensing Agreement because that's actually a free download. As long as you've got a server that can handle this, you start it, you can go to Microsoft and I believe it's Microsoft that should have put that up in time. I believe it's Microsoft/WSUS and just download it for free. So as long as you've got a Server 2008 license, Server 2000 doesn't support WSUS 3.0.

Richard Campbell: Right.

Susan Bradley: Also too for those people that are still running SUS or WSUS 2.0, those are unsupported at this time because you're running this older platform so you just get up to WSUS 3.0. But basically as long as you've got a server license, you're good to go.

Richard Campbell: Right.

Susan Bradley: And you don't even need Volume License, retail OEM, you name it. You can download the WSUS product and put it on your server. Now, the caveat I will say we're getting pretty good at patching Windows stuff. The bad guys know this. The bad guys are starting to go after other stuff



like Java, like Flash, like QuickTime, and WSUS natively does not patch that so what always WSUS does is it uses the Microsoft platform and the Microsoft stack. So that's why if you really want to secure it with the patches, you need to either look at a third party product that plugs in and allows you to add them, or you need to get a lot more intense into WSUS scripting than I am, or you need to do what I've done where I've chicken out and I've bought a third party product that natively does support for patching for iTunes and QuickTime and all those other third party stuff. So I always look at it from this standpoint. You know, it takes some time to learn how to code and learn how to process these third party patches. I don't have the time so I pay other people to have that time so that I'm freed up and do other things.

Greg Hughes: Right.

Susan Bradley: So it just depends on what your priorities are and what your budget is. You can do this yourself. People can push out patches via scripting and things like that, but if you're not that kind of person and you don't have the time, there are vendors and companies out there that code up these things so that you don't have to do that.

Greg Hughes: What are the primary differences between versions 1, 2, and 3? If I'm running one of the past versions, toss a couple of characters out there and dangle them in front of me, why should I be making the move?

Susan Bradley: The main thing is that right now you want to make sure that you're with WSUS 3.0 Service Pack 2.0 in Windows 7.0, and who isn't excited about Windows 7.0 right now? And if you've got a network where you already have an existing patching system like either SUS or WSUS, you aren't going to see those seven patches come and being offered up to you. So my main tier for getting WSUS, anybody on SUS 3.0 Service Pack 2.0 is being able to support and protect those Windows 7.0 machine. The first one SUS, CRUD app isn't supported at all anymore. So if you've any issues at all and you call into Microsoft or you go into a forum at Microsoft, they're going to say, "Dude, that is way old. You need to get yourself up on a supported version." The same way with WSUS 2.0, the trial version, that as in April 2009, you're going to see where -- you're not going to see some patches coming out because it's not getting the detection updates that it needs. So just from the flat out, you aren't going to get the patches you need because you're not on the supported platform anymore. At that point, you need to get up to WSUS 3.0 Service Pack 2. The other thing that I like from it is it has built-in tools now. With SUS 2.0, you always have to Google up this WSUS Wiki entry called Mowing the Grass. Let me explain what that whole concept is. When you have a WSUS server and you've got a pretty active network and a mixture of different operating systems and different platforms,

you start to build up a database of patches up on that with SUS database. It's a SQL database that keeps track of the stuff, and after a while you kind of go, "That's pretty big out there," and now that these workstations have those patches, you don't need them anymore. So you need to mow the grass.

Richard Campbell: Right.

Susan Bradley: So in the past there was this Wicky entry that you have to go through and give these commands and all these kinds of stuff, and now with WSUS 3.0 there are actually buttons right inside the interface that is a clean-up tool that is really great for keeping your WSUS kind of trimmed down and not too fat. You go in there and usually if you've never done it before, you go into that tool console interface, you go into the clean-up tools and you want just like about five or six different clean-up steps, and the very first time you've done it, if you've never, ever done it before and you want to do each one one at a time especially in a small business network, if you do them all at once it will just cry that server to a halt. It is trying to do too much all at the same time. So you want to make sure that you do just one at a time. So you run one and make sure that's complete, to the next one and make sure that's complete. The other thing that we always recommend that you do is you hand-check drivers. The golden rule of thumb in patching in general is to kind of use that update window when it says, oh, you need a driver for such and such, oh, you need a driver for this. It kind of look at that as just a suggestion. Don't look at that as, oh, you must install this because it's getting better but for the longest time if you must install the driver up at Microsoft, let's say there was a really good chance that you'd be banging your head against the wall going why did I do that because I just blue-screened or did this or something isn't working and now I have to pull back, so I always look at the driver window as a suggestion. I don't look at it as mandatory and especially the way they currently publish out drivers, there are notoriously have been evenings when you will get like 4,000 drivers of a different manufacturer in one night and we're going like, "oh, my word." So we uncheck the driver category in the WSUS section in the classification. Because I don't want drivers to be pushing down through with us, so I uncheck it. It puts a lot of storage on the server that I don't need. So that's one of my kernel rules, it's when you go into the WSUS console there are two settings. One is products, the other side is classification. We always leave products as fully checked all products even if we don't have all products inside of our network. Like for example, I don't have BizTalk inside my network. I barely even know what BizTalk is, but I check the box of products because I want to make sure that as I bring new system into my network, that WSUS will automatically detect it and say, oh, you need a patch for this. So if I suddenly decide tomorrow, gee, I really need BizTalk for some unknown reason, and no, I don't mean to *dis* all of BizTalk consultants and



users in the marketplace that I just love to take on that particular product, but if I suddenly bring that product into the network, if I don't have all products selected I might forget that I don't have that box checked and I might not get the patches for that particular product if I don't have all products selected. So some people usually go through like, oh gee, I don't have that. So I'm going to uncheck your products and I'm just going to check the server that's going to work the things I have, which is fine as long as you remember that if you bring anybody new in, you make sure you go back and revisit that train because if you forget to go check that box, let's say you bring in a brand new Windows 7.0 and let's say you're already on WSUS 3.0 Service Pack 2, you're going to find that that 7.0 is not being detected because you haven't checked that box up on that console. So on all the products side now, which leaves that box checked because it's checking not pushing, the other side of the column is classification and the one that I always leave unchecked like I said the drivers because they can be kind of fat and take up a lot of room if you unchecked that. I do leave the rest. I also have the network setup so it does not automatically approve. I approve. Again, control freak, you can just go to town on this. You set it up so that nothing automatically gets installed. The reason why you're installing WSUS in the first place is because you want control. So you would convince that, okay, and especially on servers, you may make the decision that it's okay on workstations or categories of workstations, you get automatic updates, but in general I like to have absolute control over the servers so I detect I do not have it approving so I go in and approve. The other big issue that some people have with WSUS, it is not a push now patching platform. It is a detection. The clients in the servers go up to WSUS and they pull down the patches so when you go in there and you say, okay, detect patches, and when you give that approval it maybe up to 24 hours before that patch actually gets on the system. So it's not an immediate go out there push now, and you can set up some scripts and things in some ways to say okay, at this time at 3:00 in the morning, make sure you go out to check and if there's anything out there at this time, go install, regroup the box and go on. We also tend to -- again you have to kind of set up your network accordingly. If you're like me, I leave my computers on at the office 24/7 including the workstations. That's not the greatest and greenest in the world. I'm trying to work on that, but it also allows me to have detection windows throw WSUS in the middle of the night so then I'm not patching 8:00 to 5:00. All of my patching stuff is done between the hours of like about 2:00 and 4:00. It's in the middle of the night so that it doesn't interfere with our workday. Again, I'm kind of struggling a little bit with the green scenario because obviously that's not the greenest echo friendly and I'm not saving energy so I'm trying to release that and kind of work around that a little bit but sometimes you have to kind of balance the, okay, how can I protect

as well as how can I be efficient at the same time. So it's something I'm struggling with the personally.

Greg Hughes: Hey, your points about the ability to exercise that control, if your working environment, for example, where maybe you run custom applications or non-Microsoft application for business critical purposes, yeah, it doesn't happen often. Well, in a happy world it doesn't happen often but you start pushing out patches without testing against your applications on the server and on the workstations sometimes too, you could end up in an I can't do business type of situation.

Susan Bradley: I get this question a lot of times. How can you do this even in a small network? How can you have like a test lab?

Greg Hughes: Yeah.

Susan Bradley: The big firms have test labs. Well, how can you do this in a little firm? And I do a process that I call the Canary Test. If you remember the old story of canaries in a coalmine, they would take canaries down in the coalmine and as the air down there got bad, if the canaries, if a little tweety bird died, everybody knew that the air down here is getting a little dead, we need to vacate immediately.

Greg Hughes: Yeah.

Susan Bradley: So we have two workstations in the office, myself and another gentleman, we actually manually go to Microsoft, let's say we manually get the patches in our workstation. We, what I call bake, for about a day to making sure that everything is okay with our line of business apps. If both of us say yeah, it looks good, thumbs up, then I approve them on the server. As far as server patches are concern, I have a -- and it's easier, it's way easier now. Back in the good old days, the part where you have to buy additional hardware in order to have some kind of a test network, these days you can send a virtual box.

Greg Hughes: Right.

Susan Bradley: So VMware, Hyper-V, Virtual PC, you name it, just throw more RAM into workstations, build a box that has lots of RAM, stand up a Hyper-V, stand up a VMware and build yourself up a little network of the same kind and buy TechNet Plus latest thing just by a spread because that is to be used for testing, and you mimic your network at the office. You know, obviously you don't have to build an exact replica but you can get it close and these days too you can take a systems' state restore and actually detect the DC information, the Active Directory information. So you can get as identical as you want to spend the time, money, energy, effort, you name it, and test those patches in a lab situation first before you then go out and do it on your real. The other way you can do it is you can wait for somebody else to be



stupid and do it first. There's a list served at www.patchmanagement.org. If you go to that page, there's a list archive and a list sign-up. There are always consultants and users and big firms that say, hey, I install this, get this to my machine, are you seeing this too? A recent one had occurred that nailed a lot of us was in the October patches, the month of October which was the largest patch month that Microsoft ever had and also jokingly we call it the longest patch today because it was the patch that never died, that kept coming back and being released over and over again, initially when that came out there was a crypto patch, and I can't remember the name but it's on the top of my head, but it absolutely nailed the Office communication servers. The minute you put it on any Live communication or Office communication server, the minute you reboot the box you have no Instant Messenger inside of your Office.

Richard Campbell: Ugh.

Greg Hughes: Not good.

Susan Bradley: Just totally dies, and the word got out pretty quickly that on that list, that that was the ascending patch, take it back off, and reboot your box and you'll be fine. Also via that list, I got word that, oh, the 6.0 got released. I did not hear about that from Microsoft security bulletins, I didn't see it on their blog, I didn't see it on any other place. That community word of mouth was number one, what got us to the problem, and number two, what got us to the information that, oh gee, there's a fix out there. I would not have known about one without community resources. So absolutely, if you can empower your firms and your bosses, and I know this is hard sometimes, some larger firms have issues with sharing information. Totally understandable. But if you can also empower your boss to see the power of sharing information like what hurts in patching, and if they can empower you to sign up with an alias like a Gmail account and lurk on that list and when you, in your firm, have an issue and especially when it's a line of business application, if you can say, hey, we're seeing this, just a heads up FYI, it helps us all. I mean, the bad guy share information. The good guys should share information too and especially when we can find out very quickly after Patch 2.0 that oops, this one is hurting, oops, let's get and call Microsoft and figure out what's going on, why is it doing this. Because the last thing that you want to do is roll back a patch because obviously the bad guys now have that patch, they can start reconstructing, they can start reverse engineering it and figuring out how to attack you so you try to keep the patches on as much as you can, but sometimes when they hurt there's no other choice, you have to roll them off. So then you try to look too, okay, what mitigations can I have, now that this is off how bad is this? Because this is where that sharing of information is key because if we know, oh, that hurts, okay, somebody call in at Microsoft, let

them know how big this is and let's get this fixed as soon as we can.

Richard Campbell: And where is this site that everyone that's using WSUS is focused?

Susan Bradley: www.patchmanagement.org.

There are actually two WSUS. One is on patches in general, the other one is specifically on with SUS. So if you have administrative issues with WSUS, if you have questions about deployment, about setting up, there's this two WSUS on that site, www.patchmanagement.org, like I said one is specifically on patch is use, and the other one is more targeted right on with SUS installing, deploying, setting an app, you name it. Like I said, there's a whole bunch of this that stuff that we, you know -- and also it's really, really helpful sometimes when you've got a unique line of business application and you've installed something and you go, "Okay, I'm seeing this. Is anybody else?" And if somebody comes and actually say "No, we've got the same basic set-up but we don't have that line of business application and we're not seeing it," you kind of go "Okay, hmm." It allows you to kind of focus more into what trigger it.

Richard Campbell: Yeah.

Susan Bradley: Because sometimes, you know, okay, it's not just a patch. It's the interaction of that patch with my thing.

Richard Campbell: Right and that's what you know you're sitting on a unique piece of knowledge now. If everybody is broken, then fine. But if it's just you, now what's unique about you? Or even better, it's now two or three people who come back and say "Yes, I am having that problem but a bunch of other people aren't," and now you can start comparing, hey, what's similar about us is different about them.

Susan Bradley: Exactly.

Greg Hughes: I like to go back just to reflect on your point about using a virtualized environment to be able to do a test lab. Back in the day, in trying to deal with patch management in the first version of SUS and then the first updates that came out, I've spent a lot of time, and some of the people that I was working with spend a lot of time learning a lot about patching but also about virtualization because it was a neutral relatively speaking that was available for people that have not touched Software Updates Services or WSUS and who have not yet played with virtualization. This is sort of a perfect, low risk, easy to do, won't take too much time type of environment to set up using the tools that are available like you said through TechNet Plus in order to really learn about all of the above. Isn't it?

Susan Bradley: Absolutely. I mean, I don't know how I would keep up with patches these days



out of virtual environment because it allows me -- the other thing is that it allows me to have a baseline. I have two servers in my Hyper-V environment. One is my more like my real box at the office, the other one is my clean, pristine nesting extra third party added to it all and so sometimes you need this, okay, what's the baseline, what's the normal setting is on the box, what's the normal stuff. There's nothing third party on that and I use that as my sanity check of going okay, hmm, that install is just fine. Nothing occurs so, hmm, it's working just fine on a clean, pristine environment. It must be something unique to me over here.

Richard Campbell: Yeah.

Greg Hughes: And having used physical or virtual tools in the past, sometimes you really have to actually replicate a service or a machine in your test environment, but there are lots of tools to make that relatively easy to do.

Susan Bradley: Absolutely. There's that recent one that Russinovich came out with, that is a free PBV easy tool, the only issue that I've heard on that is it does not trip up the HAL, so therefore, again using that lovely TechNet Plus subscription, and I'm going to massacre the name because I can never remember all that, I think it's SCVMM, I think. They have a lovely alphabet soup up there. There's a virtual machine manager. If you go out to the virtual machine blog, and I can get some link on that...

Richard Campbell: I remember what you're talking about there. Yeah.

Greg Hughes: Systems Center Virtual Machine Manager.

Susan Bradley: Yeah.

Richard Campbell: And this is a tool for updating virtual machines with patches without actually sort of starting them.

Susan Bradley: But it also gives you a way in their R2 version that you can PBV and it goes through VSF.

Greg Hughes: Right and with the HAL Abstraction, right.

Susan Bradley: Exactly. It pulls up the HAL so you can take let's say you want to have an exact duplicate of your physical machine at the office and you want to pull the HAL out so you can install it up to a Hyper-V box and set up a test network, you can use the SCVMM and I think it's the R2 version that does this, that pulls out the HAL Layer so we can virtualized and it won't blue screen a desk on you when you go in a places that it didn't work.

Greg Hughes: Is the result then -- so what I pull out, they're called the Hardware Abstraction Layer? Is that what it should be called?

Susan Bradley: Yes, that's it.

Greg Hughes: It's the AL.

Susan Bradley: It's not the "I'm sorry, HAL, you can't do that." There's nothing robust that tells you you can't do that. Yeah. It's basically pulling out the specific information so that when you move it from environment to environment, when the system boot back up again it doesn't go "I don't know what this hardware is, I'm going to blue screen on you." So if you take that out and it moves in virtualization, then the happy can't hurt now.

Greg Hughes: What's one more thing that people should know about WSUS that they probably don't know today?

Susan Bradley: One more thing that they should know. I think one more thing that they should know is that if they don't have it, they need it. I always look at it. There are times that I use it as a sanity check against my third party tool and vice versa. There's a rule in security, trust their play. If you only have one patching mechanism, sometimes it's wrong.

Richard Campbell: Right.

Susan Bradley: Sometimes WSUS is wrong. Sometimes the third party tools are wrong. It is always wise to have some other thing to go and say, hmm, you say I'm patched but when I use this other tool over here I'm not patched, why is that? And it's always in the figuring out who's right and who's wrong that you go, okay, hmm, I wasn't as locked in as I thought I was. I was missing a stack. So my thing that I tell people is even if you think you don't need it because you've got something else, give it a try. You might be surprise that there are patches that WSUS detects that nobody else offers up and vice versa. Sometimes WSUS, if you're using WSUS, when they would take a workstation, go out to secunia.com, and there's an online skin or tool that you can run on the desktop and make sure what you think you're being patched is what you're being patched because sometimes Secunia will come back and say you're missing this and this and this. So I say trust and verify.

Richard Campbell: Susan, it's great talking to you about Windows Update Services. It's one of those things that I think a lot of folks are using without really understanding, and the other half don't even know it's there.

Susan Bradley: And it's free.



Susan Bradley Patches Our Machines with Windows Server Update Services!

November 18, 2009

Richard Campbell: And it's free so go get it.

Greg Hughes: Free is free. Thanks Susan.

Susan Bradley: Thank you.

Richard Campbell: And we'll talk to you next time on RunAs Radio.