



RUNAS RADIO



<http://www.runasradio.com>



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.



*Text Transcript of Show #120*  
(Transcription services provided by [PWOP Productions](#))



**Phil Peery Keeps Active Directory Working!**  
**August 5, 2009**





[Music]

**Brandon Wenn:** From [runasradio.com](http://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 #120, with guest Phil Peery, recorded Monday, July 13, 2009. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at [pwop.com](http://pwop.com). You can follow the boys on Twitter at [twitter.com/runasradio](http://twitter.com/runasradio).

**Richard Campbell:** Thank you Brandon. This is Richard Campbell. You're listening to RunAs Radio. With me, as always, my co-host Greg Hughes.

**Greg Hughes:** That's me. Hey Richard.

**Richard Campbell:** Hi Sir, how are you?

**Greg Hughes:** I'm doing -- actually life is hectic but I'm doing okay.

**Richard Campbell:** Yeah well, better than not being busy.

**Greg Hughes:** I'm getting married and I've never done that before and...

**Richard Campbell:** Congratulations man, that's good news.

**Greg Hughes:** Yeah, thanks. It's interesting, it's exciting but it's tough.

**Richard Campbell:** Yeah, you only want to do it once.

**Greg Hughes:** Best part is that last night we're at somebody else's wedding, an outdoor wedding which ours is planned to be an outdoor wedding in the fall and it rained?

**Richard Campbell:** Yeah.

**Greg Hughes:** And so she was like, "Maybe we should get married in your church." I already put a thousand dollars down on the outdoor wedding place, no, we can have the reception there.

**Richard Campbell:** All right Greg, well let's introduce Phil Peery again. He was on the show just a couple of weeks ago, so if you want to hear his whole bio, you can listen to that show.

**Greg Hughes:** Yeah, we don't need to read it again, he's a good guy.

**Richard Campbell:** I know when we talked about 64-bit computing, there was a whole bunch of other

topics we wanted to get into and I just wanted to get straight to that, welcome back Phil.

**Phil Peery:** Hi guys, how are you doing?

**Richard Campbell:** Things are good, yeah.

**Greg Hughes:** Doing well.

**Richard Campbell:** No rest for the wicked, that's for sure. When we talked a few weeks back, we talked about 64 bit computing and we talked a little bit about Active Directory and I thought we come back and sort of drill into AD and this is part of the work that you do as in PFE?

**Phil Peery:** Oh yes, yeah, absolutely. Active directory is a big part of, well it's one of the areas of specialty for me, so every customer I guide to is part of the work.

**Richard Campbell:** Is AD that much pain these days, I thought it just worked?

**Phil Peery:** Yeah, a lot of the stuff that I do for customers now is going in and talking about the new features of Windows 2008 Active Directory and the upcoming 2008 R2 release, right?

**Greg Hughes:** Sure.

**Phil Peery:** So most of our customers are running 2003 Active Directory and running it fairly, fairly well, fairly stable, right? Some people have some work they need to do on improving the performance, replication performance from a site topology perspective and things like that but by and large, that's true, Active Directory does just one, it runs very well.

**Richard Campbell:** Is it a size thing when you start having these replication problems like where does the size of AD become a problem?

**Phil Peery:** Actually there's really not a theoretical limit to the size of the Active Directory database, it's only, really limited by any more, especially with 64-bit domain controllers, it's really only limited anymore to the size of the physical disc you can provide for the database, right? So in some cases we have customers that have active directory databases that are just gigs and gigs and gigs in size and holding millions and if not billions of objects. Now, most customers of course aren't, don't get directories that big, it's only the great, big, huge companies that do that but from that perspective, nobody's really kind of hit those limits yet.

**Richard Campbell:** Yeah. When you say it's just limited to disc space, I think 1 ½ terabyte drive.



**Phil Peery:** Okay.

**Richard Campbell:** Let me just...

**Phil Peery:** You could get an Active Directory database to fill that drive, you could create enough objects in an Active Directory database to fill that size. It would take some time, granted, right, but it would absolutely work, right?

**Richard Campbell:** And you really wouldn't want to replicate it, though.

**Phil Peery:** Well, one of the things about Active Directory replication is you're not replicating the entire database, it's not like you're replicating the NTDS.DIT file, which is the Active Directory database. You're not actually, physically copying that file from domain controller to domain controller, you're only replicating the objects and attributes that change within that directory, right?

**Greg Hughes:** Right, just deltas, right.

**Phil Peery:** So it's not like a 1.5 terabyte chunk of replication right?

**Richard Campbell:** Right.

**Phil Peery:** Unless, of course, you've got that Active Directory database is that big and you promote a new domain controller, then of course you've got to replicate that entire database for that first time to the new DC but anything after that it's just changes, it's just the deltas to the database gets replicated. So from that perspective it's a very efficient operation. Now, to replicate that 1.5 terabyte Active Directory database the first time, if you do it over the network, that can be fairly slow right? So we have a feature called "*Install for Media*" where you can actually take a snapshot of your current Active Directory database and instead of doing the initial replication over the wire, you can actually use that back up of your Active Directory, copy it, burn it to a CD or to a tape or what have you and move it locally to that new domain controller and promote it from that source instead of replicating it over the wire. Actually *Install for Media*, one of the reasons why it was created was specifically for that purpose. So once that database is up and live on that new machine, it then just starts talking to the other DCs in the environment and again we're just replicating the deltas, the changes to the directory at that point and as I said it is most Active Directory objects are fairly small attributes or fairly small in size and replicate very quickly.

**Greg Hughes:** So if I have a new domain controller saying a new data center that I want to

bring up for the first time, I can burn that to a CD or DVD, ship it over there, load it up, probably has a serial number, date, timestamp type thing on there and it will just start replicating the deltas since it was created?

**Phil Peery:** Yeah. So what happens is during the DC promo process right, instead of and this is something you can do with 2003 but it's much enhanced and improved in 2008, when you do that DC promo process instead of saying replicate from DC3 or DC4, replicate from this *Install for Media* set, right?

**Greg Hughes:** Gotcha, gotcha.

**Richard Campbell:** That I have local on the machine right and then we do that initial database build from that source. Once that's complete, we establish a connection to our domain controllers through the Active Directory site topology and then we begin our normal object and attribute replication from there. It's actually a very efficient way of bringing up a new database, a new domain controller...

**Greg Hughes:** Sure.

**Phil Peery:** With a really big database.

**Greg Hughes:** Maybe kind of a random or tangent of a question here but, hinging off our last week's show, do you run across because you're going into a lot of different customers and sites that are running, that are running Active Directory for a long time, do you still run across Active Directories that are in 2000 mode or haven't even gone to 2003 native mode, do you still run across that?

**Phil Peery:** Actually just recently, pretty funny, yeah. Funny thing you asked that question, actually just recently I went to a customer who had a root domain and a couple of child domains and one of the child domains was still 2000, it was only two domain controllers but it was 2000 DC's...

**Greg Hughes:** Yeah.

**Phil Peery:** And of course that was a big red flag because Windows 2000 is no longer supported...

**Greg Hughes:** Sure

**Phil Peery:** So we had to work with them to get that those OS's upgraded and those domain controllers running on a new Active Directory but yeah, I bump into more member servers running Windows 2000 than I do domain controllers. You get the customer that's running a customized application,



that refuses to run on anything new so they kind of keeping it limping along on the old box and until they can get the app upgraded. That's a little more frequent than actually domain controllers but it does happen on occasion.

**Richard Campbell:** Yeah. Every so often you'll find an NT4 box stashed at the back too, right?

**Phil Peery:** Yeah and occasionally Windows 95 machines, isn't that scary yeah.

**Greg Hughes:** The story of the old NT4 domain controller that got dry walled in when they took one room that was "data center" and made it into two offices in the dry wall there was some machine running that had to be chopped back out.

**Phil Peery:** Yes.

**Richard Campbell:** And if it's still alive now, it's never going to die, so...

**Greg Hughes:** Yeah.

**Phil Peery:** Yes and you know a lot of those machines are like that, NT4 ...

**Greg Hughes:** Oh yeah.

**Richard Campbell:** Especially was extremely stable and very reliable. From an up time perspective, it would just run and run and run. So yeah, you run into that on occasion.

**Greg Hughes:** Well, a company that I worked at, as a start up, had an NT4 domain controller, the downstairs domain controller, so to speak and it was in a closet and it got covered up by marketing crud basically boxes and boxes of stuff that got stacked around it, nobody knew that machine was there and it sat for a year and a half or two years under all those boxes, just doing it's job sitting there just fine until somebody finally tried to go and say, "Hey, wait there's a domain controller there. Where is that thing?" It took a while to find it but they found it, it was hot but it was sitting under there running.

**Richard Campbell:** Do you see many folks using Core to run AD?

**Phil Peery:** Actually, it's one of the things that I kind of push, I've only had one customer that actually had to port it but I think it's an excellent solution, right? So the idea is, with Windows Core is we reduce the footprint and the memory utilization by removing all the GUI components from the operating system, okay? You get a machine that will typically run faster with less amount of memory, it's easier to manage because there's fewer binaries on it and all

that jazz and as a result, you put a service on like Active Directory, directory services and it just runs great, it's just runs like a champ especially again on a 64-bit machine.

**Greg Hughes:** Yeah.

**Phil Peery:** Again one of the things that I like to strongly suggest to all the customers that I go to, one of the things that I do a lot of lately, as I mentioned, is I go and I do these shoptalks on Windows 2008 and Windows 2008 R2 and this is actually one of the things that I actually do, a virtual demo of, is I sit down and we do a DC promo of a Core box that we run perfmon on it and see how the memory is utilized and all that and it's actually a lot of people get interested by it when they actually see it first hand like that. Actually two of the DC's that I run in my home lab, two of the three DC's that I run in my home lab are running on Windows 2008 Core, runs great.

**Richard Campbell:** Do you just generally look, before you run it as a virtual machine, I haven't seen any bare metal core machines.

**Phil Peery:** You can, of course one of the other advantages of, if you run a Hyper-V machine and then you do your guest OS's as Core, that's one way to do it but right now my two physical domain controllers are, they're physical rather than are running core in their physical boxes, so you can do it either way, right?

**Greg Hughes:** Now I'd like to point out what Phil just said, two domain controllers in his home lab.

**Richard Campbell:** Nice.

**Greg Hughes:** So, yeah this is...

**Phil Peery:** Well, I have two core and one Windows, yes, I actually have three DC's in my home lab.

**Greg Hughes:** Three DC's in his home lab so we're, this is, yeah, we're hitting ultimate geek here, that's what we're doing.

**Phil Peery:** Yeah, I get accused of that.

**Greg Hughes:** What else do you run in your home lab Phil, tell us.

**Phil Peery:** Okay, so I have my three domain controllers, I have a Hyper-V box that is running a two node cluster, file and print services and running a SQL server so I can play with it and kick the tires.



**Greg Hughes:** Uh huh.

**Phil Peery:** And I have about one, two, three, well my work laptop is connected to the network I have five Windows 7 machines, desktop OS's, between my son's, my wife's and my personal desktop. So, yeah, I've got a pretty good load of boxes, the electric company loves me.

**Richard Campbell:** Yes but have you ever been rated as a grow-op because of this?

**Greg Hughes:** Richard just built a new house.

**Richard Campbell:** Because of the data center the racks are based here, we consume too much power at night and we actually had the police show up thinking we were a marijuana grow operation.

**Phil Peery:** Wow.

**Richard Campbell:** Yeah.

**Phil Peery:** Well, that's never happened to me. My basement office is the warmest room in the house during the winter, though.

**Richard Campbell:** Yeah, I could see that. Again we're back to this whole thing of isn't Active Directory just plumbing? I find the UI for Active Directory is a problem like it's hard to do certain things in a detailed configuration and I'm sort of battling with it, is this actually an active directory problem, or is this just a classic permissions group type problem.

**Phil Peery:** So give me an example, I'm curious because well one of the things that we've done with 2008 is one of the big complaints prior to 2008 is along those lines. Yeah, it's hard to, you have to run this MMC, you've got to run that, there's no unified tool right? So within 2008 we've implemented Server Manager which unifies all of those tools under one console and has provided some enhancements to the existing tools and has really improved the management experience considerably. So specifically, what kind of issues are you're referring to?

**Richard Campbell:** So I'll tap Mark Minasi's complaint in the previous show which was if you want to have multiple password policies. So you have a group of power users and they have to change their password more frequently than the sort of typical user, you're right down to the bare metal ADSI edit to make that happen.

**Phil Peery:** Yeah. What you're talking about is fine-grained password policy.

**Richard Campbell:** Right.

**Greg Hughes:** Yeah.

**Phil Peery:** And it's a new feature in 2008 and 2008 R2 and he's absolutely correct, the initial release of fine-grained password policy is a little tough to implement and to manage. One of the things that I'm kind of hoping, we're going to see with R2 is we're going to see a GUI tool or maybe a PowerShell applet or something like that that will take care of that. Not really sure 100% where that's at but you are correct, fine-grained password policies can be tough.

**Greg Hughes:** So is this one of those things where Microsoft, somebody decided, "Hey, this feature is important enough, we need to get it out even though we don't have the matching fancy UI, even though you do have to get low level to make these changes, it's worth that."

**Phil Peery:** Yeah, something along those lines and also the new enhancements to audit policy are also similarly limited from the GUI, it's a command line only, type of interface. So, yeah, there a couple of things that do need to get a better interface and I believe will in the near future. I think we'll, when 2008 R2 comes out, we'll start to see some enhancements there and plus the PowerShell guys just generate great PowerShell applets to do that kind of thing anyway...

**Greg Hughes:** Right.

**Phil Peery:** So we'll probably see something from them as well.

**Greg Hughes:** You mentioned audit policy, why don't you talk about what's new in audit policy in 2008 R2, it's kind of interesting.

**Phil Peery:** So right now, audit policy in 2003 is fairly limited right. You can get access to the directory, you can get log on, log off, that kind of stuff, the big enhancement to the audit policy in 2008 is the ability to audit changes to the directory. We have a whole slew, a whole range of event ID's for auditing changes, adds, deletes, modifies to any object in Active Directory which is something that's been needed for a long time, that's really the big thing there.

**Greg Hughes:** It's a big deal for people that have compliance efforts, regulatory efforts that they have to show evidence...

**Phil Peery:** Exactly

**Greg Hughes:** Of compliance, the changes that have been made are, do make the amount of



information that's available to the auditor or to the reviewer a lot more useful.

**Phil Peery:** Yes, exactly, exactly. Well, one of the limitations, like I said, is something gets changed in an OU or an attribute gets changed that affects an application, that kind of thing and earlier versions of Active Directory, it was really hard to audit and trace back where that change was made.

**Greg Hughes:** Yeah.

**Phil Peery:** And that's where the new policy changes to auditing fill that gap completely, right? As I said, I'm looking for the event ID ranges for you really briefly but any change, any move of an object or an attribute, any deletion, creation, of course, are fully audited now right down to the user ID and IP address of the workstation where the change was made from, so really great stuff there. Any auditor, anybody that has to interface with an auditor is going to really going to love these new features.

**Richard Campbell:** But even beyond that, just recovery from that up until now in Active Directory, if you accidentally deleted an organizational unit, you're screwed like restoring that is a nightmare.

**Phil Peery:** Yes, oh yeah because first of all if the person who didn't actually delete it doesn't fess up right away and say, "Oops, I accidentally deleted this..."

**Greg Hughes:** Uh huh.

**Phil Peery:** If it's a Friday afternoon, how are you going to know right away? Until maybe people start logging in against that OU and can't, so yeah this provides you with not only an audit trace source but also as a potential source to monitor changes to your directory.

**Greg Hughes:** Sure.

**Phil Peery:** Which is a really good thing.

**Richard Campbell:** I'm going to presume the best intentions of the guy, he didn't realize he deleted it, right?

**Phil Peery:** Yeah, yeah exactly.

**Richard Campbell:** But the guys who are already logged in, they keep functioning, it's not until Monday when they come and try to log back in again and then they submit it as a bug, it takes a long time for you to finally trace all the way back to the fact that you lost that OU.

**Phil Peery:** Yes.

**Richard Campbell:** Step me through the process of how you get it back, I know in R2 we get undelete...

**Phil Peery:** Yes.

**Richard Campbell:** But before that, here I am in a happy 2003 R2 environment, how do I get that OU back?

**Phil Peery:** Well, actually you're talking about relying on your system-state back ups right at that point right? So hopefully everybody out there is doing system-state back ups, right? So basically what you have to do is you have to, first of all, identify the OU that's been deleted and you have to go to your most recent system-state back up and do a, reboot a domain controller in directory services restore mode and recover that guy that way using NT back ups and that's the 2003 methodology.

**Richard Campbell:** You have to restore the whole system-state to do that, you can't just get this OU.

**Greg Hughes:** The one OU.

**Phil Peery:** Well you can if you use third party tools you can go get the one OU and using a non-authoritative restore you can recover an OU.

**Greg Hughes:** Oh, is that right?

**Phil Peery:** Yes.

**Greg Hughes:** Otherwise, you're going back to yesterday's back-up or the day before's back up or whatever it is and any changes that you've made since then, you lose those.

**Phil Peery:** Yes. Well you're going to have, if the OU is deleted, you're going to have to do that anyway.

**Greg Hughes:** Sure.

**Phil Peery:** Now, one of the cool things in 2008 is you can, of course, mark those OU's as undeletable, you can go in and check them inside.

**Greg Hughes:** Right.

**Phil Peery:** Protect from delete which is also one of those cool little features that have been asked for, for a long time

**Greg Hughes:** Right but they do have to be marked as, they have to be marked specifically as undeletable in order to be able to do that...

**Phil Peery:** Yes.



**Greg Hughes:** So you have to do that ahead of time, right?

**Richard Campbell:** Well it gets back to when is an OU designated to be deletable right, like what?

**Phil Peery:** Usually the OU structure put in place of course for the administrators to manage the environment. Once you get your layout kind of your OU layout canned and the way you like it, yeah you should never really have to delete that unless of course there's a corporate change or kind of structural change within the organization but yeah, that's absolutely correct once they are in place, we very rarely see the need to delete or move an OU. Also one of the reasons why we implemented that check box that says, protect from delete.

**Richard Campbell:** Do you find that active directory running with Exchange is quite a bit a different piece from Active Directory without?

**Phil Peery:** Oh no, not really, not really because Exchange is really a consumer of all that services right?

**Richard Campbell:** Right.

**Phil Peery:** Of course it does its own thing with email but, and actually in, from my experience it's actually one of the biggest consumers of Active Directory, all that services from an application perspective. So I personally find it doesn't really change the way AD runs at all. Now you certainly have to plan your AD infrastructure accordingly if you're going to be deploying Exchange but especially the newer versions of exchange because we rely more on site topology than we used to for Exchange now but it's definitely Active Directory is still Active Directory underneath it and you do of course, you have to do some schema expansions to support Exchange as well which is a lot of customers all nervous about but it's really a fairly straightforward process.

**Richard Campbell:** I just find it once you've got Exchange in the loop, your AD is much bigger.

**Phil Peery:** Oh yeah, well it will of course grow, absolutely, because we're adding a whole bunch of objects and attributes to the directory so it does certainly grow.

**Richard Campbell:** Yeah, it uses AD in a way that I don't think any other application uses AD the way that Exchange does.

**Phil Peery:** Absolutely.

**Richard Campbell:** Yeah.

**Phil Peery:** Yeah. I do believe that Exchange is the biggest like I said, the biggest consumer of LDAP services that we see. There's some other consumers of LDAP, the PeopleSoft type of applications and Cisco Unity can use Active Directory but certainly Exchange is the biggest one.

**Richard Campbell:** So Phil, any favorite stories of Active Directory scares that we could share with the listeners?

**Phil Peery:** Favorite stories of Active Directory scares, you guys all know that we utilize Kerberos as our authentication engine for Active Directory, correct?

**Richard Campbell:** Right.

**Greg Hughes:** Right.

**Phil Peery:** As such, Windows Time is a fairly important component of Active Directory.

**Greg Hughes:** Sure.

**Phil Peery:** In Active Directory we have a limit for the amount of time skew that can exist between two domain controllers. In other words, if domain controller A has a time of 10:00 and domain controller B, his time is greater than, in either direction, plus or minus 5 minutes difference on that domain controller where the time is plus or minus 5 minutes difference Kerberos will stop authenticating users on that DC because Kerberos, after that time skew, can't verify whether or not the Kerberos Ticket Granting Ticket has been spoofed or stolen or what have you and that's actually part of the MIT standard for Kerberos. So one of the things that I've run into is I had a customer who had a domain controller, a number of domain controllers in the East Coast of the US and a couple of domain controllers in the UK and one of the domain controllers in the UK had become compromised and the customer believed it was from an internal source and one of the things that happened was the time of the domain controller was set back two years, right? This was way 2007 when the time was set back at 2005, right?

**Richard Campbell:** Wow.

**Phil Peery:** And of course as soon as that happens, that domain controller stops authenticating users...

**Greg Hughes:** Sure.



**Phil Peery:** But Active Directory continues to run and over a period of time it caused enough issues within replication, within time stamps on records and things like that when they corrected the time of the domain controller, when they found it and corrected the time on the domain controller and brought it back in sync with the rest of the environment, the fact that it had a whole bunch of time stamps to Active Directory caused Active Directory replication to fail environment-wide across about 45 domain controllers.

**Richard Campbell:** Ouch.

**Greg Hughes:** Oh boy.

**Phil Peery:** Within about two hours, replication had completely ground to a halt and it took us about 18 hours to get the replication back up and running again. So I was on site, Father's Day no less that year with this customer trying to get their environment back up and working which we were able to do without any loss of data. So that's one of my big war stories, actually.

**Greg Hughes:** At a high level, what's the process of fixing that look like?

**Phil Peery:** From a higher level what we essentially had to do was we had to, first of all, verify that time, environment-wide was stable and then to correct the Active Directory replication issue, we basically had to go in and recreate basically all the replication connection objects and in a couple of cases we actually had to rebuild site links because with this old replication, with this old time, date stamp being set, some of the site links were completely corrupted.

**Greg Hughes:** Sure.

**Phil Peery:** On top of that because it was a two-year interval, we also had to do some scanning of the directory for lingering objects as well.

**Greg Hughes:** That's right.

**Phil Peery:** So we actually have to do some lingering object clean up as well. So it was a tough one and it took a lot of time to correct.

**Greg Hughes:** Just thinking about time across an organization for people that are running large Active Directories or even decent-sized active directories, do you generally recommend that they have an internal atomic clock sync time server, do you find that generally helps or are there other ways to do it? I know that if I've had, for example, not to bash but if I have to rely on [time.windows.com](http://time.windows.com), I've got nothing to rely on.

**Phil Peery:** Yeah. I have a couple of favorites that I like ticandtoc.usno is a good one, one of the military ones. I used to really like the atomic clock in Boulder, Colorado as a highly reliable time source but I don't think they allow free public NTP access anymore, I think you actually have to pay for that service. One of the other options is they make these NTP services, it's a little device and you run an area aerial up through your roof...

**Greg Hughes:** Right.

**Phil Peery:** And it gets time from GPS satellites, that's also a really good solution and it's fairly inexpensive, I think they're under \$1,000 bucks.

**Greg Hughes:** Yup.

**Phil Peery:** And also if you have a highly reliable router on your internal network, that's also another option as well.

**Greg Hughes:** Oh yeah, good thing.

**Phil Peery:** But the thing in regard to Windows is important, in regard to Active Directory that's important is that the Forest Root PDC Emulator in the root domain if you have a parent-child domain structure, he's the only guy that has a time type of NTP and he's the guy that's configured to point to that reliable time source right? Every other domain controller, member, server and workstation should have a time type of NT5DS and that basically says for that particular device, "Get my time from the Active Directory hierarchy right? Get my time from the domain controller where I established my secure channel connection to, right?"

**Greg Hughes:** Sure.

**Phil Peery:** That way, we have one authoritative time source at the top of the pyramid and it filters down to everybody else. That's from a Windows perspective, that's what we like to see from a best practice perspective.

**Richard Campbell:** Well, that's good to know. I know several times I can think of, where I've seen creeping time on the domain controller servers where that time creep over time has resulted in replication issues and pretty substantial problems, yeah.

**Phil Peery:** Oh yeah.

**Greg Hughes:** Yeah.

**Phil Peery:** And it's a tough one to track down if you're not thinking Windows Time, Windows Time, right?



**Greg Hughes:** Right. It's one of the very basic things you have to think of.

**Richard Campbell:** Yeah. There's actually a really good white paper on setting up Windows Time available from [microsoft.com](http://microsoft.com) search on win32 time service best practices and you'll find it.

**Greg Hughes:** Cool.

**Richard Campbell:** But isn't the important part here to keep all the machines in sync? You don't actually have to have the right time, it's just that all the machines have to have the same time?

**Greg Hughes:** Consistent time.

**Phil Peery:** Exactly and that's the thing right? So if your connection, if you're pointing to an external time source and your internet connection goes out, as long as everybody is using NT5DS and it's using the Active Directory hierarchy, if the time drifts on that NTP server that Forest Root PDC Emulator, it's not too big of a deal because everybody's going to shift with him, right?

**Richard Campbell:** Right.

**Phil Peery:** As long as everybody stays together, it's kind of like the school of fish theory right, if everybody stays together, maybe nobody will get eaten by a shark, that kind of thing. So yeah, shifting, a time drift as a group is not an issue, it's when you have a domain controller who starts to wander off on his own maybe because the system clock on that domain controller's hardware is failing that's where we start to have issues or if it's of course maliciously changed for evil purposes.

**Richard Campbell:** Right. Phil I think we're just about out of time, any final words?

**Phil Peery:** Yeah, actually I'd like to encourage everybody to look at Windows 2008 R2 when it becomes released and available later this year, hopefully later of this year. Some great features, new features in R2, one of the ones we touched on very briefly. The recycle bin for Active Directory...

**Richard Campbell:** Right.

**Phil Peery:** Is great, that's a great feature and as we also talked about 64-bit domain controllers are a wonderful thing and also think about Core for your domain controllers, right?

**Richard Campbell:** Phil Peery thanks so much for coming back on the show.

**Phil Peery:** Pleasure.

**Greg Hughes:** Thanks Phil.

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