



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 #119
(Transcription services provided by [PWOP Productions](#))



Mark Minasi Digs on Windows 2008 R2!
July 29, 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 #119, with guest Mark Minasi, recorded Monday, July 17, 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 very much. This is Richard Campbell. You're listening to RunAs Radio. With me, as always, my host Greg Hughes.

Greg Hughes: Hey, how are you doing?

Richard Campbell: I am well sir and I have an email. Actually we have a bunch of emails stacked up but I thought I'd drag it out today and read a few of them and unfortunately, we don't have RunAs mugs, you know, 120 shows later we still don't have -- I got to do something about that. I think my summer project is going to be get a RunAs mug and start sending to folks who send us emails. Anyway, let me read you this one. "Hi Greg and Richard," I love that he listed your name first. "I just completed a single sign-on unified password manager project for a customer. The project included 600+ users and 15 different major company wide systems and roughly the same number of department-level specific applications. It was a challenge but the unified log-in and password management system is a dream compared to the nightmare that it was before."

Greg Hughes: Oh, yeah.

Richard Campbell: "As Greg is a security geek, he should have some interesting thoughts around my question or ideas for a show or perhaps he's already got a silver bullet solution. My thought goes around the next step past unified password manager which is unified rights management. How can this be done? Are there products out there that let you retrofit third party applications with unified rights management across the company or is this the last Holy Grail of the IT department? Today, in many larger IT departments, it's nearly impossible to know exactly who has access to what, especially fun when you get to the task of creating a user just like an existing user without missing something. Regards, Mattias Carlsson." It looks like he's from Sweden. Thanks for your email Mattias. Greg, you're on the spot, man.

Greg Hughes: Sorry there is no such thing as a silver bullet, it just doesn't happen.

Richard Campbell: Right.

Greg Hughes: Rights management in third party applications, no, there is no one answer to all that at least not that I know of and would that be a holy grail? Well, it wouldn't be the Holy Grail but it would certainly be, it would be a holy grail. That's a tough one, like you said, it's hard enough just doing unified identity right? There have been a lot of products that have come out recently to do unified identity but rights management, it really has to be supported inside the application. So, as more and more applications as we've seen support things like authorization, not just authentication identity but authorization rights and tie that in to some of the common identity stores, the unified identity stores then more and more of that becomes available.

Richard Campbell: I'll throw my developer hat on this problem and say, "The dumber my code is, the better off we are from a rights management perspective." If I just try and get to the file, then you get to use Ackles to decide who has rights to that and you can set up your own groups to set those rules up and so forth but then I have to write my code to deal with the fact that sometimes when I go to get that file, I'm going to get denied and I shouldn't crash my app.

Greg Hughes: Sure. Yeah, I think about things like Geneva, I think it's called...

Richard Campbell: Yes.

Greg Hughes: Microsoft's sort of open-standards, you can say based, sort of, approach to doing identity and I know people that are doing workaround, there's Geneva Server and then there's the Geneva Framework and I know there are some people leveraging Geneva Framework and what they're doing is they're building in multi-tenancy capabilities, so if you have multiple sets of customers or sets of internal customers or using multiple applications, that's pretty cool but also they're building around so you have identity access and authorization and tokens to handle that and way to assert claims and way to move that information back and forth across an enterprise of applications but the applications have to support it. You still, you have to have, if you have an API where you can pass that type of information back and forth, your applications have to consume and have to know how to speak that language.

Richard Campbell: Absolutely and I also think that the other key issue here is this whole, actually having a good tool for managing rights just figuring out why can't this user access X or how do I make another user that has the same privileges as this guy?

Greg Hughes: Yeah.



Richard Campbell: What are the details of all the privileges he has? I still don't see good tooling around that.

Greg Hughes: Well, there are better tools out there that do rights management but they tend to do it in certain slices of the pie that don't cover the entire pie, right? You have rights management stuff that Microsoft has had out for a while and it's improved over time, over Office and things like that. So if you get into certain, certain areas, some of the document management type of systems that are out there that work really well but the question really went to, well, how could, is this something that I can just sort of magically make work in all applications? What's a silver bullet or this isn't really a silver bullet, this would be more like pixie dust, right now.

Richard Campbell: Right.

Greg Hughes: And it just doesn't exist.

Richard Campbell: So the answer Mattias is, get it right it's hard and it's not going to get easier any time soon.

Greg Hughes: Well, the answer is it's not going to get easier anytime soon. It's hard but you know Mattias, go make it happen man because he's right, this is something that we need, right?

Richard Campbell: Yeah.

Greg Hughes: So I'm sure there are smart people working on this, the questions is, who's going to come up with that creative idea that really makes it happen?

Richard Campbell: That makes the difference. All right, let's talk to our guest. When Mark Minasi attended this first lecture about computers in 1973, he learned two things, first, computers are neat and second, many technical people are very nice folks but they can put you to sleep in an instant while explaining technical things. Mark transformed those two insights into a career, making computers easier and more fun to understand. He's done that by writing over a thousand popular computer columns, several dozen best-selling technical books and explaining operating systems and networking to crowds from two to two thousand. Awarded "Favorite Technical Author" by CertCities four times out of four, Mark is best known for his "Mastering Windows Server" and "Complete PC Upgrade and Maintenance" books, both of which have seen more than 12 editions and sold over a million copies. An audience member at a recent talk remarked that he believed that Mark Minasi could "do a talk on watching paint dry that would be so good that people would be motivated to go home and paint a wall just

to experience the joy of watching paint dry." While this has led to several tempting offers from Sherwin-Williams, he's decided to stay with his first and best love... technology. Welcome, sir.

Mark Minasi: Welcome, it's an awful long bio I've got to get it down to like two sentences.

Richard Campbell: Yeah, I could've just said it's Mark Minasi and we'd be done, right?

Mark Minasi: Ah, no, no, no I actually liked that famous one, that was really when I started writing books, I always thought writing books would make me famous, you know?

Richard Campbell: Right.

Mark Minasi: And so my first book, Inside OS2 1.0, let's be clear, it swept the market, both users bought it...

Richard Campbell: Yes.

Mark Minasi: But it didn't make my name a household word that I hoped for. So I set my sights a little lower and I thought if I could just be micro-famous, if you took like a million geeks off the street, one of them knew my name, that would be me being micro famous. I've since soared to milli-fame, I figured 100,000 geeks know my name and I'm creeping towards centi-fame so, it might just be like, it just take me that long until "it just don't get any better."

Richard Campbell: Yup, by bit by bit and the interesting challenge of actually presenting technical content in a way that works for people.

Mark Minasi: Something that you're no stranger to doing, Richard.

Richard Campbell: Huh?

Mark Minasi: I don't know if the listeners know this, but I was at TechEd last July, when was it, May?

Richard Campbell: It was May, yeah.

Mark Minasi: And I was going to be in his room and I thought, "Well, I'd get in early because you know how you have to change some speakers off the Podium and who is there but our host Richard Campbell doing a gosh, darn technical talk about how to fix broken web servers and stuff. I mean who knew? I thought he was just a pretty face but now we know better.



Richard Campbell: Oh, it was of my Death Of A Web-Server talk, it all came from that whole, I've got these mini servers that I can bring with me and setup on the stage and then I just bury the web server under load and I show how we fix the failure and yeah it was about an hour of iterating through load tests and debugging and finding caching problems and all that good stuff, it was a lot of fun.

Mark Minasi: Very chewy, very nitty-gritty stuff quite delightful.

Richard Campbell: Yeah, the audience had a good time. Yeah, I forgot, you were sitting on the back corner there and came up afterwards because I was getting off the stage because the next guy was pushing me off this thing.

Mark Minasi: You really have to do that, people start like collecting cards and that sort of thing, "Take it outside, take it outside, my stage now."

Richard Campbell: Move along, it's my turn.

Mark Minasi: And that turned out to be a successful talk, it was the third most popular out of 454 talks.

Richard Campbell: Which talk was that?

Mark Minasi: Believe it or not, I actually got that wrong, I had the second most popular and the fourth most popular talk among my other talks and they were both about UAC. I consider that a personal, if you can get three out of the top 10 at TechEd, that's good, but if two of them were about user account control, if you can make people like user account control, I feel that's something, few have done...

Richard Campbell: That beats out paint drying as a topic...

Mark Minasi: You're downright cruel Richard. UAC has just got a bad name, it's like Vista, that's sort of what I've been doing for the last, I realized that for the last three years I've been adopting homeless software, Vista, I'm the only one that likes Vista, UAC.

Richard Campbell: Yup.

Mark Minasi: So what about you know, speaking of Vista, it's pretty clear that Microsoft has thrown Vista under the bus and to make room for Windows 7, so are you hacking around with Windows 7 just yet?

Richard Campbell: Oh, absolutely. The RC is lovely and as we're recording this, I think the RTM is imminent, it's any day now.

Mark Minasi: Yeah, we're speaking, what, on July 13th.

Richard Campbell: Right.

Mark Minasi: And there was a rumor that it may come out today, I've been on the boards and I haven't seen it yet. There was a rumor, that I just read on some site that there's some Russian Microsoft site that said that partners will get it on the 24th of July, so I can't wait. I went out and spent a few grand for a new server because I was going to move my web servers from Server 2003 to Server 2008 but then I looked at R2 I mean R2 is just, isn't it astounding, I don't know if you agree about this but when you look from 2003 to 2008, they had 5 years to do stuff.

Richard Campbell: Right.

Mark Minasi: And sure there are definite improvements in 08 versus 03 but you know, there's almost nothing to make me say, "Ooh, got to have that." Which is funny because I expected Server Core and RODC's would be really big and so I spent a lot of time studying that and picking it apart and figuring out what I could figure out that others hadn't figured out yet and they both have been real downers because people tell me they like the idea of Server Core but the lack of a GUI has upset a lot of people because with servers, sometimes you get these strange quad ethernet cards and that kind of thing.

Richard Campbell: Yeah.

Mark Minasi: And in order to control those things, you the GUI tool that comes from the vendor, the HP's, the Dell's or whomever and those guys don't run on Server Core which means your only other option is to get the WMI provider for it and sit down and write your own scripts to configure it, which is about as much fun as you can have with your clothes on and so people have been skipping Server Core for that reason and RODC's turned out to be a big loser as well because you tell people what they do and they say, "Oh, that sounds good." And you say, "Well, an RODC can be a global catalogue server but, oh, it's not a good enough catalogue server to serve exchange and that's when people change the subject. So it's interesting, I see people rolling out 08 but I don't see them really stampeding to do it and what's interesting is that, what do we got, like a year and a quarter, year and a quarter, year and a half later, then Server 2008 R2 comes out and I think it's the better value proposition. It seems to me like the 03, 08 was fewer was fewer goodies that 08 to 08 R2.

Richard Campbell: Well, aren't we getting to the standard sort of scenario that Microsoft does where



they do this, the heavy lifting that 5-year run of changing a lot of the underlying infrastructure, new network stack, new video stack, like really core stuff and then when they finally ship it, it's got no paint on it, it's just, it's kind of ugly but the next version that comes along is the pretty one.

Mark Minasi: So like Windows 3 versus 3.1 and AD has got some cools stuff, I actually want to get, but before we move to Windows 7 I have to, I'm sorry I can't resist doing this. I like Vista for the very reason that you just quoted about Server 2008, "I'm not an Aero Glass guy, I don't even understand what the idea of Aero Glass was, I don't use a Mac, my guess is that some ideas that they ripped off from the Mac.

Richard Campbell: Right.

Mark Minasi: And I just look at it and I say, "Hmm, all it does is it runs my graphical processing unit at about 200°."

Richard Campbell: Yeah, heat problems.

Mark Minasi: I don't see the value with it but there's a ton of under the hood things, changes to the services architecture, for example. I mean the Vista services, Vista and later, services architecture is just so much better. People say to me, "What would going to Vista or Windows 7 do under the hood and one of them is. When they built XP, virtually, every workstation had one core, one processor, there was hyperthreading but that was only expensive processors. Nowadays, I don't think you can buy a computer without two cores at least and because Windows 7 and Vista and XP for that matter can, theoretically support up to eight cores, that's as far as they'll go, try it on an XP box and you're going to see that one or two cores are doing all the work and almost nothing else is being done.

Richard Campbell: Yeah.

Mark Minasi: Do that with Windows 7 or Vista though and wow. So I'm wondering, once we start seeing the quad core laptops will that end up being the, I guess the killer app that makes people go out and buy something other than XP. But it's funny, I've been saying that I liked Vista for a few years, again because of the under the hood stuff and I guess the other thing important about it is when Microsoft built XP, if you think about it, they're building this thing in what, '99, 2000 around there and sure there were threats but the average malware threat in the late 90's was sort of what, it was just people trying to build a reputation, just jerks sitting in their parents basement and popping their pimples wishing they had a girlfriend, writing some piece of malware that would infect several million machines so that they can

impress their other friends that live in their parent's basements and popped pimples and wished they had girlfriends but as you know and as everyone listening to this knows, the game has changed, I mean now it's about money, uh oh, what greater motivator is there...

Richard Campbell: Yeah.

Mark Minasi: In the human world and I think that the bad guys have gotten a lot better at being bad guys in the 2000's and Vista really was the first of a bunch of operating systems, that had a kernel built from the get go to understand that the internet is a very, very, very scary place and if you don't believe me, think about when Blaster came out in 2003. If you recall, there was this period of time when Blaster was just running around the internet, it was like about a year and a half before it mostly died but if you recall, did you ever try to install XP on a new machine that you had accidentally left plugged into the internet? It was like you are being infected before you even got the operating system installed...

Richard Campbell: Yeah, yeah. You couldn't patch it fast enough, the time it took to download the service pack was longer than your infection rate.

Mark Minasi: Right and there is, when I tell that story, the reason that I'm doing that to put up the things that are different, I wonder how many people are shaking their heads and saying, "Well, what idiot would install an operating system when a computer's connected to the internet?" Well, I mean right now, it's common sense that it's foolish to do that.

Richard Campbell: Yes.

Mark Minasi: But it was in 2003, that's how much worse things are. So that was the fist of the spate of operating systems that I think understand that the world is a big, scary place but as you know, Vista got some minorly negative press.

Richard Campbell: Minorly?

Mark Minasi: Minorly and what I find interesting about this is the very same people that hated Vista are loving Windows 7, and Windows, I mean I like it, I hate to torpedo it but Windows 7 is just basically Vista version 1.2.

Richard Campbell: Yes. It really is, it's just a retuned version of Windows but they did the right tunings.

Mark Minasi: You're not going to tell me Windows 7 is faster on the same box as Vista? Because I keep hearing that and then I have to look people in the eye and say, "Do you have a real benchmark on that? Well, it feels like, uh."



Greg Hughes: Gotcha.

Mark Minasi: It's all marketing.

Richard Campbell: Well I think it's part of it but I also think that they've done a better job of using multiple cores and of keeping the foreground worker processors responsive except for Outlook, you can't save Outlook. I've got a whole core dedicated to just Outlook and it's still making me wait.

Mark Minasi: And you know what's astounding, I'm running what, Outlook 2007 and it's amazing to me that it is 2007, it's Microsoft writing this and it's still single-threaded. I have three different email accounts, so when I fire up Outlook, you know how that works, you've got to click one, click one folder, click another folder, whatever, it goes out and synchronizes the data and it just sits there and does nothing for a while. I mean the words that I most often see after Outlook is not responding.

Richard Campbell: Yeah.

Mark Minasi: And you'd think someone at the Office team maybe we could send them an email that says, "Have you guys heard of multi-threading?" If you could have it sync up different folders at the same time or don't make me wait for the calendar, I just want to see the calendar, anyway that's the end of my rant there.

Richard Campbell: Yeah. I want to point out that when I pull up Task Manager, Outlook has about 60 threads going.

Mark Minasi: Yes, yes, absolutely. If you pull up like post explorer or something like that but it certainly behaves in a single-threaded manner, if you know what I'm saying.

Richard Campbell: Yes.

Mark Minasi: Certainly it is possible to have many threads but if the input is all spinning on a particular one, then you're essentially single-threaded as far as us carbon-based life forms are concerned.

Richard Campbell: It's definitely effectively single-threaded.

Mark Minasi: Right, right. So Windows 7 that's cool, let's talk about some R2 stuff. In 2008, the big thing was going to be RODCs but that went nowhere.

Richard Campbell: Right.

Mark Minasi: And so the question for 2008 is, 2008 R2 is what's going to be the RODC of 2008

R2? I think it's going to be active directory undelete because possibly, the coolest feature on Server 2008 R2 is the ability when you've accidentally deleted a user, yeah, accidentally...

Greg Hughes: Right.

Mark Minasi: And you ordered OU or something like that, an organizational unit, full of users then now just run this command line tool and you can undelete all of those users in twinkling and that's pretty cool sounding stuff but I think the reason that it's going to be end up being the RODC of 2008 R2 is because for some reason, Microsoft has, I think they regret this now but they made us all fear touching the schema, the structure of the active directory.

Greg Hughes: Oh, yeah back in the day, for sure.

Mark Minasi: And every time you go to a new forest functional level or something along those lines or a domain function level...

Greg Hughes: Yup.

Mark Minasi: Or when you start incorporating domain controllers from different versions of Server and you've got to go mess with the schema, I have never seen anybody, ever, mung their schema. I mean the way I make a lot of my money is like consult an active directory for organizations large and small and I've never seen anybody screw up their schema and yet we have this fear of going to, of getting, making changes to the schema and making changes to the domain structure and so on. So I think it's going to be people, say Ross Buscemi, well you help people out? Have you seen anyone go to 2008 domain function level yet?

Richard Campbell: No. Everybody's still got at least one 2003 Server in their life.

Mark Minasi: Okay, let's take a step further. What percentage of your clients are still at 2004's function level?

Richard Campbell: I don't think I have very many that actually have a 2004, they've operated everything at that point, it's mostly...

Mark Minasi: No, no, no, no, no. No argument there. I know a fair number of people, they don't have any 2000 domain controllers.

Richard Campbell: Right.



Mark Minasi: They've only got 2003 and up but they haven't gone to 2003 domain functional level...

Richard Campbell: Oh, I see.

Mark Minasi: Because the boss says it might break something and it's not reversible.

Greg Hughes: Right. So for the people that don't understand, why don't you explain real quick the difference between 2000 and 2003 functional levels?

Mark Minasi: Oh, that's right. So the idea is that active directory first came out in Windows 2000 which eponymously arrived in year 2000 and I've been looking all day for the chance to use the word eponymous, by the way and so when you, there were NT 4 domains before that and of course an NT 4 domain was radically different than a 2000-based active directory and so you could start up kind of being half and half where you'd have some of your domain controllers are running NT 4 and some of them are running Windows 2000.

Richard Campbell: Yeah.

Mark Minasi: You wouldn't get all of Windows 2000's chocolaty goodness if you had any NT 4 domain controllers...

Richard Campbell: Right.

Mark Minasi: Some of us like to do this slowly and so the notion was that when you finally shot that last NT 4 domain controller in the back of the head, you could then have a little party and pop the champagne and say to your system, system, there's no more NT 4, let's get rid of that NT 4 badness and let's just bring out the wonderful creamy goodness of active directory on Windows 2000 and that was called going from mixed mode to native mode, and I'm thinking to myself, what is the next word?

Greg Hughes: Native mode...

Mark Minasi: Real mode? No, native mode. When 2003 came out, 2003 offered probably about a dozen large and small improvements to active directory.

Greg Hughes: Right.

Mark Minasi: About 2/3 of them, you wouldn't get until you went to 2003 entirely. Obviously if it's going to be function that only a 2003 based domain controller can do, you have to have all of your domain controllers at 2003.

Richard Campbell: Right.

Mark Minasi: And then once you've done that, you flip a switch that says, "My domain is now in 2003 domain functional level, yeah, yeah, yeah." I like mixed and native myself but Microsoft decided that that was too clear and so now they're called domain functional levels. I really like the idea of mixed mode, native mode and Whistler super native mode, that was sort of like the internal name for that.

Richard Campbell: Whistler Super Native...

Mark Minasi: So anyway, so what's happening is that people have these 2003 domain controllers and they have nothing but 2003 domain controllers, maybe some 2008s and there's no reason why they can't say to their domain, "Domain, I don't know if you've noticed but there are no 2000 boxes anymore, it doesn't happen automatically." People get twitchy about it because it's a general feeling that, "Oh, it might break something, we just don't know." And another thing about it is like many things in active directory. I like AD but one of the things I don't like about AD is that sometimes it seems like everything in active directory should have a sound effect, where you push a button and you should hear the sound of a heavy door slamming shut and a bolt sliding in place and there's just, I think that's what scares people but it's a shame, it is a shame because I would be willing to bet that if we surveyed a thousand active directories from different sized companies, I think at least a quarter of them would still be on 2000 domain functional level even though they could easily go to 2003 domain functional level or 2008 because we went from NT that was mixed, to native which is 2000, to domain functional level 2003, that was the super Whistler native mode and...

Greg Hughes: Yeah.

Mark Minasi: There's another, yet super super Whistler native mode that would come with all 2008 and yet another one if we go to all 2008 R2, I'm just breathless thinking about it.

Greg Hughes: So what's the really, really cool chocolaty goodness that you get in native mode 2008 R2 that people should actually care about?

Mark Minasi: The single biggest one has to be active directory undelete. If all of your domain controllers gets shot up to 2008 R2, then that's only step 1 by the way, then you can turn on undelete, you have to turn on undelete, otherwise you don't get the benefits of it, which is odd.

Greg Hughes: Uh huh.

Mark Minasi: Even if all your systems are 2008 R2 and even if you set yourself to 2008 R2



domain functional level, you don't get the undelete until you turn it on and you can't turn on the undelete until you are at 2008 R2 functional level.

Greg Hughes: Gotcha.

Mark Minasi: And once you do that, that if you delete, let's say, an organizational unit full of people, then you can undelete it. It's not the smartest thing in the world in the sense that you first have to undelete the organizational unit, that's one step, then you can go back and say, "Oh now that I have undeleted the organizational unit, I have to go on and say by the way let's do one big loop, that's a one-liner you can do, I will say grab all the things you find in that OU that are deleted and undelete them." So, a little bit of annoying part is if you want to do something really dumb like delete an OU, organizational unit that has organizational unit inside of it...

Greg Hughes: Right.

Mark Minasi: And you want to undelete all that, it's a multi-step process because you've got to go down to the bottom level and start undeleting things by hand.

Greg Hughes: So delete a container and then you can get whatever objects are in that container or even if those objects are other containers, right?

Mark Minasi: Exactly, exactly.

Greg Hughes: Okay.

Mark Minasi: And the other thing that's interesting about it is Microsoft seems to love, they have this new thing where they like to hide their light under bushel and what I mean is in 2008, 2008 not 2008 R2, in 2008 arguably, maybe the coolest thing about a 2008 domain functional level active directory wouldn't be RODCs, it would probably be flexible password policies. This is where I could say, "I've got 200 people in my domain, I want those 5 guys who have a lot of power to change their passwords every three weeks but everybody else we've locked down so they can do it every 6 months," and that was a kind of cool feature. However, as anyone knows who's tried to use it, it's like you have to put the mining helmet on and get your rope and go down to the cave in order to figure out how to use it. You have to use ADSI Edit which for those who don't know, it's kind of like ADSI Edit is to active directory as debug is to like your computer. It's the fastest way to destroy your computer in just one second.

Greg Hughes: Pretty low level operation type stuff there.

Mark Minasi: Yes, extremely low level and ADSI Edit is the only way to make use of domain functional level.

Richard Campbell: I've always compared ADSI Edit to regedit and I can't remember who came up with this quote but it was, I think it was Bill Vaughn he said, "Regedit is like doing brain surgery on yourself with a mirror."

Mark Minasi: I think of it as the fastest way to ruin your computer.

Richard Campbell: Yeah, if you make a mistake, you are well and truly screwed like, the thing that scares me about ADSI edit is it's not just you're ruining the machine you're on, you go around modifying domain level directory entries, you're ruining your whole domain.

Greg Hughes: Replicates, yup, instant replication.

Mark Minasi: So here's like the best feature in the world for 2008 and you have to be spelunker or a cave diver in order to make this thing work, so what is arguably the best thing in 2008 R2? Well, that would be the undelete but in order to do it, you can only do it from the command line with PowerShell. Now, I will speak no ill of PowerShell but it is kind of scary to the normal human and even to most IT administrators. So, why didn't they put a GUI on this thing is beyond me and why they didn't make it recursive which is the geeky word for "Don't make me put things back together container by container, I just don't know."

Greg Hughes: Right.

Mark Minasi: I just don't know. So maybe that's a new Microsoft thing that you have to really, really, really want the new features in order to get them. And the other thing that's kind of cool is managed service accounts. Some of our listeners who have big organizations will sometimes, will know that sometimes when you're running certain services, certain network-based programs, then of course those things are services in the Windows sense of programs that run whether you're logged in or not, they kind of run in the background, they don't run this to you, they run as someone else...

Greg Hughes: Right.

Mark Minasi: And they typically run is system which is just the name for the local authority, the machine that they're running on. There are times though that you have to run one of them, one of these services not based on a local account but instead



based on the domain account, you do this for security reasons or a number of other kinds of things.

Greg Hughes: Sure, it happens a lot. I know I've run an IT organization where we had lots and lots of service accounts especially when you had things like a lot of test automation, a lot of development environments going on. It was pretty much, it was a necessity to be able to do things that way. This stuff couldn't run a service because if you ran it as a service, it wasn't operating properly.

Mark Minasi: Right.

Greg Hughes: You weren't testing it in a valid way.

Mark Minasi: Right. So one of these services was the notion that we've got some service running under an account, that's a domain account, the other possibilities that if you have a complex website where you have lots of different application pools...

Greg Hughes: Right.

Mark Minasi: Application pools are just ways of breaking up your website so that if this part of your website dies, it won't necessarily affect the rest of the website or sometimes you want to put barriers between them for big organizational reasons or whatever. Anyway, you can run these different application pools under different service accounts again and service accounts. In this case, until R2, has just meant you go to active directory, you create a user but you're never going to actually log on as and you let the service log on as that, so far so good. What's the problem with it? The answer I usually get is, now because those are regular accounts, they have to be treated like regular accounts, so you've got to change the password every 42 days...

Greg Hughes: Right.

Mark Minasi: Or whatever you set your password policy to and so the frustrating part is that means that someone's got to remember, by the 42nd day, to log on as a domain administrator, change that account password and then go over to the server that's got a service running under that account and change that password inside the services snap in and if you don't do it right, that's when bad things happen because if all of a sudden the database server doesn't work or the website doesn't work and it doesn't come out and say, "Hey dummy, you forgot to change the password," it's something cryptic and bizarre and obscure. So what a lot of people do, none of our listeners would do something this dumb but what a lot of people do is that they just go check the box that says, "This password never has to change."

Richard Campbell: Right.

Mark Minasi: Of course a very bad idea. So it's troublesome one way or the other, what Microsoft has done is they've created inactive directory, this is new kind of account called an MSA, Manage Service Account, kind of like a machine account actually. It's almost like your computer if it's a member of active directory, has a machine account, making it a member of a domain, this is an account very much like that except you don't use it for that, you use it to run services under. So you create this manage service account, you hook it up to this particular service running on this particular server and just set it and forget it. The passwords get updated automatically and it's just, it's seamless. Even better if you've ever hacked around with this stuff, if you've ever had to troubleshoot one of these things and I'm sure you have Richard because you're a big web server guy...

Richard Campbell: Yeah.

Mark Minasi: That if you go change any of those accounts, what have you got to do? You've got to get this tool called setSPN which allows you to change, I'm simplifying, the Kerberos name for the service, it's a black art. What's nice about 2008 R2, in R2domain functional level is that if any of that happens, these Managed Service Accounts will manage the changes in the SPN, Service Principle Names automatically. So it's quite interesting that, when I started talking about active directory, the AD undelete is always the big crowd pleaser but then when I mention the MSA's, Manage Service Accounts, most people have not heard them but when they do, the first thought is, "Oh service accounts, boring, boring, boring," then you see the little light coming over the head...

Greg Hughes: The light bulb comes on, yeah.

Mark Minasi: Oh, where can I get that? Can I have that now?

Richard Campbell: Well and it feels...

Greg Hughes: from an administrator standpoint, it's a pain.

Mark Minasi: Yeah.

Richard Campbell: But it feels like these are the features that will drive you to get to that 2008 R2 standard for your whole AD just to get that chocolate goodness.

Mark Minasi: Again, who knows? I mean to paraphrase a line from Wayne's World, "We are IT



people, we fear change." And I can't wait for it, I just absolutely cannot wait for it because as I was saying, I was about to move my '03 web servers up to '08 and of course that's my excuse to go to 64 bit at the time but then I look R2 is coming and there's just so much good stuff, there are things that I really like, this is more of a small operation wonderful but it's still wonderful, is you guys run an operation not terribly large, perhaps, you have a dozen or so servers, how do you back them up? Unless you want to spend a tremendous amount of money for a third party back up solution that ends up costing more than the whole operating system did in the first place.

Richard Campbell: Yeah.

Mark Minasi: What have you got? I mean if you go to the NT backup route, where you're basically just backing up files. Did you ever try to rebuild a 2003 server with a handful of tapes?

Richard Campbell: Yeah, you're in hell.

Mark Minasi: It's a fate worse than death; yeah. But when Vista first came out and I'm going to keep saying good things about Vista because I was right, damn it, it's a good operating system and eventually the world would come around and there would be apologies, oh yes, oh yes but anyway, seriously it's got a completely different back up solution called the complete PC back up solution. Now let's be clear, this is not an idea, when I say this, a lot of our listeners, they're going to say, "Oh, such and such has been doing this for a long time." For example, a Acronis has this great tool called True Image Workstation and Acronis True Image Server. The Acronis tool for the desktop is about \$90 or something like that and it will let you take complete back ups, they can do bare metal restores, it's wonderful, I will say nothing bad of it except for the fact that it cost money.

Greg Hughes: Yeah, it's cool software.

Mark Minasi: What's that?

Greg Hughes: It's definitely cool software.

Mark Minasi: It's definitely cool software, I can't figure out though why the product is almost identical between Server and Workstation. The workstation version cost like \$90 bucks and Server version is \$1200.

Richard Campbell: Right.

Mark Minasi: I wonder what happened there?

Greg Hughes: The reason for that is because people will pay that extra money, so why not?

Mark Minasi: So yeah, think about this, I mean that means when I build a 2000 Server the first thing I do is that I bite down hard and I buy a copy of True Image Server because that way I know I've got back ups and I can do a bare metal restore. If meteors fly in the window and smash my server to bits, if the power supply goes crazy and the thing gets set on fire, it doesn't matter.

Greg Hughes: Yeah.

Mark Minasi: I'll just go to this back up and inside about 40 minutes, 40 minutes to an hour, I can have the server up and running as if it were never down, now that's great.

Greg Hughes: Sure.

Mark Minasi: Are there better ways? Sure, but I don't have the money to build a monster VM ware infrastructure and stuff like that. So we have this complete PC back up which is basically that tool and now it's built into the server operating system. So you think about it, you buy a copy of a standard server which is \$1,000, you're essentially saving \$200, you don't have to spend the \$1200 on the True Image Server.

Richard Campbell: Yeah. Well I feel for companies like Acronis that have really broken ground on this because as Microsoft commoditizes that sort of stuff, this market is going to go away.

Mark Minasi: That's an interesting question, that's a really, really good question and because some of the guys that write those things are my friends and their good people and I, but if you've been doing computers as long as you have Richard, think about what deserves to be in the operating system? I mean I remember when I worked on IBM main frames that there wasn't even anything, I'm simplifying, but there wasn't even anything in the operating system that would let you copy a file.

Richard Campbell: Yeah.

Mark Minasi: You needed to go buy a third-party product...

Greg Hughes: Right.

Mark Minasi: For which you were paying licensing fees every single year to just copy a file. So I mean, what is fair game in an operating system? I think that effective back up and store is a given.

Richard Campbell: Yeah.



Mark Minasi: I think that effective modern back up and store.

Richard Campbell: The same as networking itself, I mean you remember we used to buy Windows without networking and you went and bought...

Greg Hughes: Yup, yup.

Richard Campbell: Your, go buy Banyan VINES or Novell or whatever I'm going to network with.

Mark Minasi: Yeah, people used to buy, I mean remember the days of dealing with 15 different winsock.dll's because you had this IP stack or that IP stack that...

Richard Campbell: Yeah.

Mark Minasi: Microsoft incorporated it. I guess I'm just going duck out of this one and say I don't know what the answer is but I do know that well if they had the TCP stack vendors were damaged when Windows For Workgroups 3.11 came with the wolverine TCP stack, I think that the world is a better place because it's in the operating system.

Richard Campbell: Yeah.

Mark Minasi: You know, or whether you're talking about disk compression routines remember, if you recall the big thing it was tool called Stacker.

Richard Campbell: Stacker.

Greg Hughes: Ah yes, Stacker.

Mark Minasi: Microsoft incorporated it, I forgot what they called it, Double Space?

Richard Campbell: It's something like that, yeah.

Greg Hughes: Yup.

Mark Minasi: Anyway...

Greg Hughes: Maybe the ultimate measure of success for third party software is that eventually it's no longer native because it becomes part of the operating system, that sort of...

Mark Minasi: You know what they say, plagiarism is the sincerest form of flattery.

Greg Hughes: Exactly, yeah.

Richard Campbell: All right guys, I think we're running down on time here, Mr. Minasi any final words?

Mark Minasi: No I just can't wait to get my hands on the new stuff.

Richard Campbell: Well in 2008 R2 to be clear here, should be RTMing with Windows 7 right because they're essentially the same core stack.

Mark Minasi: Yes. So the guess is that we're going to see, the RTM sometime in July and then what happens is that, that is the final stuff it's the same thing that will appear in the shelves but it doesn't appear in the shelves until the 22nd of October and the reason is, it takes time to print all those DVD's and which leads to by the way, it's an important tip you see, those of you listening to RunAs Radio, here's an example of why you want to listen to Run As Radio because you hear things that you will not hear from anyone else and this is the tip, the tip is my projection is, in the past when Microsoft has come out with a new operating system, when Windows 95 came out, they actually cornered the market for 3½' floppies, you couldn't buy one for whatever money for several months.

Greg Hughes: Yup.

Mark Minasi: When, I believe it's Windows 2000, came out, they actually cornered the market on CD's, so my guess is that of you're thinking you want some blank DVD's in the next month or so, go buy them right now because the price is about to go through the roof and you heard it here first.

Richard Campbell: Mark, thank you so much coming on the show.

Greg Hughes: Thanks Mark.

Mark Minasi: Always a pleasure, thanks guys.

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