



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 #142
(Transcription services provided by [PWOP Productions](#))



Laura Hunter Upgrades Active Directory with Server 2008 R2!
January 6, 2010



[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 #142, with guest Laura Hunter, recorded Monday, December 21, 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 Richard Campbell. You're listening to RunAs Radio. With me as always, my co-host, Greg Hughes.

Greg Hughes: Hi Richard, hi everyone. Hey, what's going on?

Richard Campbell: Well, you know, end of the year.

Greg Hughes: Yes it is.

Richard Campbell: By the time this show is published, it's now 2010 so all the wonder is among us.

Greg Hughes: I guess it's one of those dates that just kind of make us stop and think "what?"

Richard Campbell: We're already living in the science fiction novel, man. I was chatting with a friend of mine who is in Stockholm while I'm in Vancouver on Instant Messenger and we're arguing about a particular book and I picked up my Kindle and download the book so that I can reference the quote he's talking about. The whole thing takes place in 30 seconds, and then you have that moment where you're like "wow, that is kind of cool actually."

Greg Hughes: You know, there are a couple of things that I'm still waiting for and one of them is like on the enterprise they had that little thing they'd walk up to in the corner of the room and they would like wave their hand or push the buttons and like scramble their eggs that magically appear.

Richard Campbell: Yeah.

Greg Hughes: Or bake the goose or whatever it is they wanted so I'm kind of waiting for that.

Richard Campbell: Yeah. You want that one. A few haven't come along just yet. Well, there you go. Let's actually do a show. What the heck.

Greg Hughes: Yeah.

Richard Campbell: Let me introduce our guest. Laura Hunter is a Directory Services MVP and an

Architect working in the areas of Active Directory, Federated Identity and Identity Management. She's the Principal Consultant for LHA Consulting, Incorporated, blogs at www.shutuplaura.com, and twitters at lhaconsulting. Welcome back, Laura.

Greg Hughes: Hi, Laura.

Laura Hunter: Hi. Thanks so much for having me.

Richard Campbell: Well, we've been having some adventures in the Active Directory land as I understand.

Laura Hunter: Oh, very much so. With the recent Wave 10 release as they call it with Server 2008 R2 and Win 7.0 shipping, we've got a kind of a whole slew of new features in Active Directory that people like me have to go out and start deploying to our clients, and for folks who are still running in Win 2000 and Win 2003, now that 2008 is out people can now look back and say, okay, I guess 2008 is safe now.

Richard Campbell: Right, right.

Laura Hunter: So it's good news all around.

Richard Campbell: Although as I understand it, the big deal here especially when you're talking from a group policy perspective is the client operating system, getting Win 7.0 on the desktops gives you way more control over group policy.

Laura Hunter: Oh, absolutely. I mean, Win 7.0 on the client is just going to be an amazing thing to see because for good, bad, or indifferent, a lot of our organizations never made change to the stuff.

Richard Campbell: Right.

Laura Hunter: And so you've got a lot of good companies out there that are still running XP, Windows XP Service Pack 2, Windows XP Service Pack 3 which is -- how old is that operating system now? It's approaching nine years old now.

Greg Hughes: The operating system.

Richard Campbell: Yeah, 2001 was the original edition. I would argue that XP 2.0 was actually a new OS, but even that was 2005.

Greg Hughes: Right.

Laura Hunter: Absolutely. So you've got all these organizations out there who are running a very stable but very long in the true the operating system and they're just now starting to see what really interesting things they can start doing in terms of controlling their clients and what's the Microsoft speak



optimizing their user experience, and I think the move to Win 7.0 is going to really make a lot of organizations very happy because in a lot of ways Win 7.0 is the things that we wanted Vista to be but it wasn't.

Richard Campbell: Right.

Laura Hunter: It's got all the pretty and all the shiny and the stable all at the same time.

Richard Campbell: Yeah. It's got a Windows 2000 workstationship and it was for a final consolidation through NT and the 9 set and it just felt so good like it really was a sturdy, robust version. Of course you know then XP came along and it was Windows 2000 with the Fisher-Price interface.

Greg Hughes: Right.

Richard Campbell: But 2000 was the one that made me smile and I feel like that about Win 7.0 too. It's just there, it works, it's not a big deal like let's move on.

Laura Hunter: I just really like how intuitive the Win 7.0 interface is. I was sitting in a client site the other day and CEO had just put Windows 7.0 on the laptop for the first time and he asked me a question. He said "What happened to the screen where you would set file associations?" You know, maybe you wanted a .text file opening with PrimalScript instead of notepad or something.

Greg Hughes: Right.

Laura Hunter: Where did that screen go? I can't find it. I sat back and I was like I don't actually know where that is now. So I click the start and I go to the little run line, little search line and I type change file association and I hit enter, and the control panel window pops up and it was that simple.

Greg Hughes: It just figured out what you want and did it for you.

Laura Hunter: And it figured out I want I wanted and it gave me exactly what I wanted, and of course the CEO because he's a geek and he's a thinker, he said "Well, what training control panel was that?" And I said "I don't know. I asked the search line for it, they gave it to me." And from that point I don't care.

Richard Campbell: I don't need to know. It just works.

Greg Hughes: That's really cool. You know, can I do a jump back question real quick? This conversation, I've heard this conversation a few times and if you have Active Directory you're on the line and let's just ask this one. This is a very basic question

but people will often confuse, at least in conversational terms, and I think it's largely people who don't have a lot of experience with Active Directory, but they'll think that a domain and Active Directory are the same thing.

Laura Hunter: They'll think that a domain and Active Directory are the same thing, and that's...

Greg Hughes: Well, some people think that it's all tied together as one big thing. How would you explain to somebody, maybe that's used to working with workgroup computers and stuff, what is a domain and what is Active Directory?

Laura Hunter: Sure, absolutely and that's a very common conception to have because something like 80% or 90% of all Active Directory deployments in corporate environments are going to be a single domain Active Directory.

Richard Campbell: Right.

Laura Hunter: So it's very easy to just look at that and say there's my domain, there's my Active Directory. But when Active Directory was being designed, was being developed by the product group back in the late 90s I suppose, it was this idea of being able to create a very scalable directory service and a lot more scalable than what we'd had with the NT 3.5.1 and Windows NT 4.0. For anyone who can date themselves back that far, one of the major weaknesses of Windows NT was its scalability. You had that database files which couldn't exceed 14 Megs in size.

Greg Hughes: Right.

Laura Hunter: There were facets of NT 4.0 replication where essentially you just couldn't have a single NT 4.0 domain going across WAN boundaries. The performance just got impossible for you, and so what the project did with Active Directory was they design this directory service. They based it also with all that. This directory service deck could scale to literally millions and millions of objects so I think the theoretical maximum number of objects in any Active Directory environment is 2 to the 31st minus 255 which if you punch in your calculator is a pretty big number.

Richard Campbell: Yeah and it's almost enough for Exchange.

Laura Hunter: I know. I checked that out and so when you think about Active Directory versus a domain, you can think of a domain as the primary organizational piece of Active Directory. It's the when you install Active Directory for the first time, you are installing a new domain and that domain is -- and it commensurate a boundary that contains a one or hopefully you have more than one domain controller



which is going to house the user account and the computer account you're using in your passwords and your groups and all the stuff that you think of when you think of Active Directory. Now as I said, for a lot of organizations a single domain is going to get you there and it's going to be all that you're ever going to see. But there are going to be certain situations, because of organizational requirements, because of bandwidth requirements, because of geographical requirements where you might have multiple domains configured within a single Active Directory. You might think of, for example, if you're running Active Directory on a bunch of oil rigs. You know, these things are largely physically disconnected from the rest of the world -- maybe they've got a satellite link that hooks them up once an hour or four times a day or something, you're not going to want to have that single Active Directory domain trying to replicate and trying to pass information from this oil rig to that oil rig back to the corporate headquarters all the time in a very chucky sort of manner and so you might segregate all these different locations into separate domains to create an administrative boundary, to create also a replication boundary so that these kinds of isolated places can manage themselves and can operate in almost, not really a standalone fashion because they're all going to talk to each other to a certain extent, but it does allow to create administrative boundaries within a single Active Directory.

Richard Campbell: And that was the big trick here. Of course it advanced a lot now because it was in 2008 when we finally get the read only domain controller so it's becoming easier and easier to have branch offices still run well in the AD environment.

Laura Hunter: Absolutely and if you look at the guide that has come out from Microsoft back in the 2000, 2003 era, you would see a recommendation of creating an Active Directory that had what they called an empty forest root domain which contain effectively just a couple of administrative accounts and then child domain, so a separate domain for each of your geographical entities, each of your organizational entities. Because of things like read only domain controllers, because of improvements that they've made in the algorithms that are used for replicating information back and forth, and also because of security implications of having multiple domains within a single forest, those practiced recommendations have now mature, have now changed to the point of the de facto place that you're going to begin from when you're designing an Active Directory. If you're in like a Greenfield deployment, if you're sending a brand new, or if you're migrating to a new environment, you start from a single domain, you know start from a single domain forest, start from a single domain Active Directory and then only branch out into multiple child domains if you've got a really compelling need to do so.

Greg Hughes: Got you. So what's the great stuff that's now available in wave 10? What are we getting that we didn't have before?

Laura Hunter: So the Active Directory goodness in wave 10, the biggest and the most visible update in 2008 R2 is the Active Directory recycle bin which is exactly what it sounds like. It creates a very easy, very simple way to recover deleted objects within an Active Directory domain. You know, someone deletes the user object text that way, someone deletes even an entire OU or an entire container accidentally, prior to 2008 R2 the restore scenario was you had to reboot your domain controller into the special single user mode, you have to go find a back-up tape, pray your back-up tape work, roll back all the changes and then mark those changes as what we call mark those changes to be authoritative. In 2008 R2, with the introduction of the recycle bin, it's not quite the client desktop recycle bin experience where you just double click on a folder and go right click restore. It's actually done through PowerShell. It's done through PowerShell commandlets, but it becomes a lot simpler to restore either a single object or an entire container's worth of object using a very simple PowerShell syntax that brings back the object, brings back all of their attributes, brings back any of their links to other attributes when kind of seeking point in Active Directory restore scenario. It was, okay, I brought back the user but this user is a member of a bunch of other groups and now how do I restore the links to those other groups that you used to be a member of.

Greg Hughes: Right.

Laura Hunter: And that gets even worse. It's up to you to build the user and the groups, or the groups and not the user and you can see where the permutations can get sort of complex from there. So that's kind of a big one and in describing that I mentioned probably the feature that has a similar buildings to that which is the Active Directory PowerShell module that's been released for 2008 R2 which is an actual fully pledged get – 80 users, set – 80 groups module of a number of commandlets that are only adhering to that verb – noun PowerShell syntax and these are built directly into the operating system. We've had the ability to do PowerShell management in Active Directory prior to R2 but it's either been a matter of downloading like a free ware PowerShell commandlets from quest and from some folks in the community like Dare Morelia who did a bunch of PowerShell commandlets for group policy but these are now built directly into the operating system.

Richard Campbell: Most folks that I talked to who are working with PowerShell of course reference Active Directory because that's where you get all the users and so forth but it was mostly to act on something else.



Laura Hunter: Uh-hmm.

Richard Campbell: You didn't see a lot of how do I make mass modifications to PowerShell or to Active Directory data itself using PowerShell.

Laura Hunter: Yup, yup and now with the commandlets that are built with the R2 you have now the ability to do any number of the normal, I'd say probably 90% or even more of the normal everyday administrative task that you'd expect someone to do in a GUI. There's now PowerShell equivalent for that. You can create a user and then believe the user can create a group, add a user to a group, remove a user from a group. You know, you can manage, you can add your domain controllers, you can manage or you just talk about ODBC 16:05. There's an entire bunch of commandlets talking about them, talking about managing ODBC's and behavior that's specific to ODBC's. As I said the partial commandlets are built into 2008 R2 so any R2 domain controller is going to have these commandlets build right into them. There are also an out-of-band download that's up on the TechNet download site so that you can download these commandlets. Effectively they're going to be hosted via a web service and so that will make those commandlets also available for 2008 and 2003 domain controllers. Just to be very clear, when I say web service, because I know that from the IT Pro perspective, this is the first thing that I was afraid of when I heard this, the fact that the PowerShell commandlets are running via a web service does not mean that we're installing IIS on our domain controllers.

Richard Campbell: Right.

Laura Hunter: Because, well, that's a bad thing and we try not to do that. This is a very specific, very purpose built web service to run server one very specific course the number of which is of course completely eluding me right now, but it is neither 80 nor 43.

Richard Campbell: Okay, and yeah, these are just commandlets that we can add into the older versions of server. We don't have to have R2 to get these things.

Laura Hunter: Correct, correct. You don't have to have R2 to run these commandlets. You do have a permit to have at least one domain controller that will support these commandlets and that means either you got a 2008 R2 domain controller or you get 2003 or 2008 DC that's running this web service that's put up on the download site.

Richard Campbell: Okay.

Greg Hughes: Cool.

Richard Campbell: I meant to say put that in and off we go. I'm just looking at the list of commandlets here, the get QAD user, set QAD user. These are all the real core kind of things you want to do for managing AD directly. Do you do this mostly in PowerShell these days, Laura, when you do a lot of management to this or is it better to use the GUI, like what do you like?

Laura Hunter: It really depends on my audience. If I'm working with kind of a smaller organizations who are very comfortable with and who are very familiar with working on the GUI, then I'm going to keep them at their comfort level and I'm going to keep folks working with things that are comfortable with them, however, I do have this theory that as soon as you need to do something twice you should find a way to automate it. So if you're dealing with -- either if you're dealing with a larger organization or an organization that has a lot of users in their database, you're creating a lot of users, if you're deleting a lot of users, or you're just making a lot of changes to your database, then you're absolutely going to find some efficiencies in moving away from always using the GUI to do this path and moving towards using really any kind of command line script, any sort of command line scripting pollution. I mean, I know there are folks that are crazy about PowerShell, there are folks that can take only PowerShell, but PowerShell is not the only way to get there. There are many other number of command line tools that you can use to automate your Active Directory management, and again I think if you're going to be doing any sort of tasks more than once in a week, more than once in a day, whatever your productivity comfort level is there, then I think there's definitely value in learning how to do things from a command line, from a scripted perspective not only because it makes you more efficient but it also makes you less error prone. You know, how many different ways can you spell the name Kennebunkport for example.

Richard Campbell: Right, yeah. So you're just having all that, a parent when you go along. I like the way that PowerShell tends to just naturally journal all the steps you took.

Laura Hunter: Uh-hmm.

Richard Campbell: It's a lot simpler than trying to Camtasia about your GUI.

Laura Hunter: Certainly and the PowerShell's commandlets for Active Directory are just like any of the other ones in that they are extremely discoverable. If I wanted to create a user, then I would type new dash, and then start hitting tab until I see the clan that I think makes a lot of sense for me, and if I don't have all the right parameters in place, if I hit enter and my parameters are incomplete, it's going to start prompting me for, "Oh, you forgot this



parameter. Give me a certain account name for the user. Give me the distinguish name for the user." It's going to start prompting me for any of the parameters that I forgot rather than just spewing back error messages and saying "Nope, you got it wrong. Start over again."

Richard Campbell: Right.

Greg Hughes: That's cool.

Richard Campbell: It's easier to follow along with that. I'm a little frustrated with the whole naming strategy of server 2008 R2 because I'm finding that R2 is not a minor version of 2008. It was not a small upgrade. There was more to it than that.

Laura Hunter: There are certainly a lot of goodness to be found there and even if we get away from the Active Directory piece for example you can look at something like direct access only on the networking...

Richard Campbell: Oh yeah.

Greg Hughes: Yeah, that's pretty cool.

Laura Hunter: Direct access is just kind of change your world. That's just kind of completely rock your world, but it does make non-trivial assumptions of your infrastructure.

Richard Campbell: Yeah.

Laura Hunter: I think you're absolutely right, that bringing direct access into the environment is going to be a major change but with change comes added goodness and I think things like direct access and things like in a way key features this is going to open all kinds of new world for people.

Richard Campbell: I'm looking at managed server's account. This is really powerful stuff too but not that simply just drop into play.

Laura Hunter: Oh, sure, sure and that's another one of the new features that we get with Active Directory, it's this idea of creating a specialized type of user object that has a password that you as the administrator never actually needs to manage.

Richard Campbell: Yeah.

Greg Hughes: Right.

Laura Hunter: Not like you look at how you create applications now. You create a username on your application. Hopefully you set it with a nice long complex password and then you set it to never expire because frankly it's not even that you're lazy, it's that we always do that.

Richard Campbell: Yeah. You'll never look at it again.

Laura Hunter: Yeah because you don't want your app failing at 3:00 in the morning, the nanosecond that password expires, so you set the password to never expire and you're saying to yourself that you're going to log in and change that password every three months or every six months and then at that point you get lazy and you never do it, and manage service account really gets you away from that because it creates a specialized type of user account where Active Directory will, on your behalf, every 30 days in the background go in and change the passwords to something like 240 character complex, monstrosity of a password...

Richard Campbell: Ouch.

Laura Hunter: And change password on your behalf, it will go into your services NSC and will change the password on the account and restart the service for you so that you never even notice that it happened. Maybe you get a little flat second blip every start of the service.

Greg Hughes: So the service that's running on Windows, the Windows service knows what the new password is but that account can't be leverage by a malicious third party program that's not directly controlled by the system that's doing the password change.

Laura Hunter: Well, you know, it's still the user object and it still has that password so it's the password that's out there, it certainly can be cracked but it's a 240 character complex password. Good luck cracking that with any kind of modern computing and even more than that your administrators never know it, and so your administrators never know it, your developers never know it, your end-users never know it, and that's really the danger of service accounts, the danger of service accounts is the fact that you have the service accounts that maybe once upon a time it had a nice complex password but it has now had that password for the last five years and every single member of the DBA team, and every member of the IT admin team, and every developer now knows the password. That's really the danger there.

Greg Hughes: Right and when we make service accounts in the lazy model that we've been discussing, quite often what people do is I'll go out and I'll just create a regular Windows user account and not restrict the account. You still have to log on local privileges and what have you, but this is a completely different class of user account.

Laura Hunter: Absolutely. Strangely enough, it's actually a type of computer account and computer accounts with an Active Directory actually have their own passwords and have that sort of 240-character



password that is again managed by Active Directory. But because computer objects inherit from user objects in the whole developer framework scheme of things, managed server accounts will also inherit all of the attributes, all of the behavior of a user account so that they can go out and run applications just like any kind of server account that you might manually create as an admin.

Greg Hughes: Got you.

Richard Campbell: Well, and just making them not have the password so they can't abuse the account plus it totally breaks wrench cryptography. That whole problem goes away.

Laura Hunter: Uh-hmm, yup and the problem goes away of trying to log on to a machine one day and trying to log on to one of your production servers and seeing that someone has logged on as a service account.

Richard Campbell: Right.

Laura Hunter: Well, guess what? You just lost accountability, you just lost the accountability. Anyone who can log on at that service account, there's no repetition there.

Richard Campbell: Yeah.

Laura Hunter: That person can log on locally to a server as this account which likely has some rather some extensive privileges and they could do anything they want and claim that they didn't do it because how are you going to prove it.

Richard Campbell: Yeah, I know. That was a runaway application misbehaving.

Laura Hunter: Uh-hmm.

Richard Campbell: Just keeping those things completely separated. Active Directory Management Gateway Services, I'm just starting to play with this now. Maybe you fill us in. It's one of the other big new features.

Laura Hunter: So with the other management gateway service, that is going to be that web service that we just talked about for the PowerShell module. So that is the web service. It runs natively on 2008 R2 domain controller because it's not just PowerShell that's going to be accessing and it's going to be accessing and administering Active Directory through the web service. It's also going to be the new Active Directory administrative center which is kind of the new and improve A doc. It's the new and improved AD used in computers.

Richard Campbell: Yeah.

Laura Hunter: And that's also going to be leveraging this management service and again its going to be an out-of-band download that you can install on your 2008, your 2003 domain controller so that those down level domain controllers kind of leverage this new management features. The goal as I understand it moving forward is that any of the new Power Shell modules, any of the administrative tools, rather than hammering directly at the Active Directory database, are going to be leveraging this management service to do their work.

Greg Hughes: So is this a service that has public APIs that people can write their own Power Shell or other application interfaces into, or is it really just for the Power Shell commandlets and the new interface for Microsoft.

Laura Hunter: I haven't seen an API for it but it would very much surprise me if there wasn't one out there. This is very much something that they want the community to be able to plug into and to be able to write their own management module, their own extensibility so I'm sure people grant an MSDN part of. You're going to find the documentation on that somewhere.

Greg Hughes: What about identity management as a big picture topic. I know that you deal with this. I'm sort of deep into the big identity management project which just happens to be right now. I'm curious where do you see the identity management story going with the new things that have just come out and that might be in the horizon for Microsoft and from others.

Laura Hunter: The thing that they're saying in a big sort of, much that I hate to use this phrase, paradigm shift, I owe somebody a quarter for having used that phrase now, but I think the major change that's coming both from Microsoft as well as from third party vendors is this idea that the Cloud is real and the Cloud is big and the Cloud is coming and we need to find a way of managing both our identities. The way that we've been managing things up until now, we've always made assumptions, we've always made assumptions that our applications are residing on premises and are joined to an Active Directory domain. Our users are sitting in an Active Directory domain or they're using certificates or we're making all these implementation assumptions about our users and about our applications that when we seed that out to the cloud model, they really don't apply anymore. My users could be in an onsite Active Directory. They could be sitting up in the Cloud. They could be sitting up in Windows Live. They could be sitting at an open IDE somewhere

Greg Hughes: It could be any of the above.

Laura Hunter: My applications could be sitting on premises. My applications could be hosted up in



Azure. They could be any combination of the above, and the way that authentication and authorization are going to need to evolve to deal with that is going to be an interesting thing to watch. Certainly the direction that Microsoft and a lot of other folks are going in is pursuing this idea of a clean-face model. You may have heard of them. Active Directory Federated Services was initially released with 2003 R2 back in 2005. The new release of it which was codenamed Geneva actually just shipped the release candidate, just shipped on Friday.

Richard Campbell: Wow.

Laura Hunter: I know the Federated Identity team was working very hard on that and are now taking the rest of the year to recover. I think that's going to be a huge thing.

Greg Hughes: So Geneva, this is the security token server, so the idea of being able to assert claims and do identity across boundaries in that way.

Laura Hunter: Exactly. That's exactly what you're looking at. You're looking at the security token service. You're looking at the security token service that will authenticate a user to wherever that user needs to be authenticated, maybe it's in Active Directory, maybe in Windows Live and then once that user is authenticated we then take that user's information and generate claims which are in effect big old bunch of XML tokens and then we send those tokens over to an application and that application can then consume those claims and the application doesn't really care where those claims came from. It doesn't care if you use real authenticated IDE. It doesn't care if it's authenticated by an open IDE. It doesn't much care for the implementation of how that user is authenticated. All the application knows is I'm getting a bunch of claims. I trust these claims because of whatever security relationship I have with this at TS, maybe we're joined in Active Directory domain, maybe we've traded PKI certificates, but however we got there I'm getting a bunch of claims and these claims tell me that this user is a member of some marketing role and so I'm going to dish out content diffuser that's relevant to that role.

Greg Hughes: So this is going directly to the concept of Federated Identity then. I trust that other authentication mechanism and I just explicitly trust that it is doing its job well and therefore whatever it sends me I'm just going to take it face value and leverage.

Laura Hunter: Yup, absolutely and up until now has been a very common motto in kind of business-to-business scenarios where someone from, you know, A. Datum got the user account, eight items has got the SharePoint and so users can access the SharePoint, sorry, the A. Datum SharePoint without needing to really authenticate, without having to have,

you know, the administrators need datum, creates separate accounts, create shadow accounts, another set of passwords you've got to manage, blah, blah, blah. We don't have to do that anymore. It's simply create this federated relationship where until an A. Datum organizationally trust one another and so at that point the A. Datum SharePoint is then able to accept those incoming claims from those partner users and just make their authorizations accordingly.

Greg Hughes: Got you.

Richard Campbell: Well, guys, I think we're just about out of time. Laura, places we should be looking for more info around ADFS v2 and AD in general.

Laura Hunter: Good Active Directory resources are microsoft.com/activedirectory. It's a very good place to start, and for the upcoming ADFSv2 launch microsoft.com/adfsv2. Also the Geneva team's blog which is on the MSDN blog site and the name of the blog is Card, actually C-A-R-D because of the Windows CardSpace which is component of ADFS v2, and all kinds of good information to start with from there and it's all over the Twitter space, and it's all over the blog and it's just a good thing. Go all you forth and federate.

Richard Campbell: Nice. Laura Hunter, thanks so much for coming on the show again.

Greg Hughes: Thanks, Laura.

Laura Hunter: Thank you very much.

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