



<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 #124
(Transcription services provided by [PWOP Productions](#))



Sahil Malik Manages Sharepoint 2007!
September 2, 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 #124, with guest Sahil Malik, recorded Saturday, August 22, 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. With me, as always, my co-host Greg Hughes.

Greg Hughes: Hey everybody. Richard, how are you?

Richard Campbell: I'm well sir and coming into the fall now so I've got a crazy conference season.

Greg Hughes: Yeah. Your fall is, you know what, it's not just the fall. I mean let's be real; you travel all the time, right?

Richard Campbell: I do but the summer is, I only do about four shows this summer, I'm doing like 10 in two and a half months.

Greg Hughes: See, for you, 10 in two and a half months, see that's crazy for you but for most people four shows in the summer is completely insane as well.

Richard Campbell: Oh well, I guess.

Greg Hughes: So really what it means is that you're baseline is completely insane.

Richard Campbell: Yeah, so when it finally gets to panic levels for me, it must be completely irrational okay, I'm okay with that.

Greg Hughes: Yeah but you know, I mean first of all you love that stuff.

Richard Campbell: Yeah.

Greg Hughes: And you're good at it so...

Richard Campbell: Thank you.

Greg Hughes: Yeah, okay.

Richard Campbell: We all have our hobbies.

Greg Hughes: Yeah. I fly airplanes and you do trade shows.

Richard Campbell: There you go. Hey, we're talking SharePoint today let me jump in with our guest here. Sahil Malik is the founder and principal of WinSmarts and he's been a Microsoft MVP and an IT speaker from the past many years. Author of many books and numerous articles, consultant and trainer, he delivers training and talks in conferences internationally and a good friend of mine, we've spoken together on, I guess three or four continents. Hey Sahil, how are you doing?

Sahil Malik: Hey Richard, hey Greg, how are you guys?

Greg Hughes: Good, how are you?

Sahil Malik: Quite good, it's Saturday.

Richard Campbell: Yeah, it's unusual for us to be recording on a Saturday but I'm enjoying it, it's kind of peaceful around my place and here we are.

Sahil Malik: That's nice.

Richard Campbell: We did a show a little while ago with you on .NET Rocks! about SharePoint and I really wanted to get you back to talk about the IT side of SharePoint with SharePoint 2007. So how is it to run the infrastructure for SharePoint these days?

Sahil Malik: Well, you know that's great because one of the things that I mentioned on the .NET Rocks! show is that there's a higher overlap between the IT Pro and developer roles in the case of Share Point as compared to a .NET project.

Richard Campbell: Right.

Greg Hughes: Yeah.

Sahil Malik: But still, the IT Pro side of things is a very well-defined role in SharePoint and today it really, I mean honestly I want to talk about the challenges people have faced when running a SharePoint 2007 farm and trying to manage it from an IT Pro side. So I mean let's just pick topic by topic, how is performance to begin with?

Richard Campbell: Right and I think performance is always great right up until people start really using it then you get bitten.

Greg Hughes: Yeah, I know, I had a conversation with somebody recently in a work context where they're talking about using SharePoint, the platform SharePoint as like a foundational platform for building great, big applications on like high scale applications. So how does it perform and how does it scale?



Sahil Malik: Hmm. So we are going to do another follow up show to this and also talk about what SharePoint 2010 brings to the picture and especially since we're so close to the release of SharePoint 2010. It would probably be, we wouldn't get the whole picture unless we did consider the next version as well.

Richard Campbell: Sure.

Greg Hughes: Sure.

Sahil Malik: But we're in August right now and the show is going to release in September so we can't really talk about 2010 so I guess probably what we'll do is go over a few topics in this show and talk of how to apply to 2007 and then possibly do a follow up show on how 2010 makes these things better, I guess.

Greg Hughes: No, absolutely, we'll look forward to doing that.

Sahil Malik: Lovely. Okay, so let's talk about performance. Now let me take the example of Excel services, right? In SharePoint2007, you have a concept of something called a Shared Service Provider right, and the Shared Service provider is typically another website or something that can be segregated out to another server where the Shared Service Provider takes responsibility of doing a lot of heavy duty tasks behind the scenes, right? Things that the Shared Service Provider is responsible for doing is, let's say user profile import, so that you may designate the active directory or some other source as the source of your user profiles. So first let me talk a little bit about what user profiles are, let's say I log into my account every morning onto the network using domain-smalik but my identity's a little bit more than domain-smalik, I have a first name, last name, I have certain qualifications, I am a manager, my locations. So all that other metadata about the user is the user profile and typically you would have this user profile information stored in the AD, that's one of the very typical sources but then you would also have parts of the user profiles stored in other stores like a database somewhere for instance sort of SAP database or an HR system or something like that. So the Shared Service Provider has the responsibility of keeping SharePoint in sync with the rest of the user profile stores in the organization and you have to configure the same port yourself. We were talking of our performance, so let's go back to Excel services, Excel services is relatively demanding for the server, now one of the limitations that the Shared Service Provider model has is that in a farm, on a Share Point farm, you can have multiple SSPs, one SSP can manage multiple web applications but one web application can be managed by a maximum of one SSP at a time.

Richard Campbell: Okay.

Sahil Malik: So let's imagine that you have a particular web application that has a lot of demands on it from a performance side of point of view and the reason I picked Excel service is that Excel services can get demanding on the server resources because typically, you're delegating, it's a very common scenario that you're delegating the sheet processing to a powerful machine such as a server because people's laptops are not capable of doing it, the sheets are just too big. Of course you want to share the sheets and that's another big reason to use Excel services but what happens is that since you have a single SSP devoted to a website and if this website is very, very Excel services-centric, you run into performance issues, you cannot scale, you can't tell SharePoint that, "You know what, this one website is really, really overloaded so I'd like it's Excel services responsibilities to be delegated to three or four SSP's." You can't do that because or you cannot even segregate the Excel services calculations from say, user profile import or business data catalogue or you can't, it gives you, it puts you under certain limits when it comes to scaling it out.

Greg Hughes: Right.

Last edit 8:45

Sahil Malik: Now there are products, there's the Microsoft Compute Cluster that will allow you to scale Excel services but then those products can get expensive or can become really challenging on hardware. I mean scalability is different than performance, scalability is the trick of segregating your work into equal and similar pieces and distributing them across a farm of servers and any server can pick up at anytime right?

Richard Campbell: Right.

Sahil Malik: So it's cheaper to scale amongst a number of cheaper servers rather than to build this one humongous server that is so darn powerful.

Greg Hughes: Oh, makes sense.

Sahil Malik: And gives us so much hardware that we can keep DC warm without the politicians, right?

Richard Campbell: But also you get more reliability when you have redundant hardware like that.

Sahil Malik: Absolutely, you have better up time. So if the SSP goes down and so one of the things that the SSP is responsible for is search and



when search goes down, if you have a small farm, it's not an issue because you simply re-index but one of the challenges of backing up search, is that you have to back up the database and the index files at exactly the same time.

Richard Campbell: Right.

Sahil Malik: And let's say you've got a terabyte size of a farm, it's going to take a day for SharePoint to re-index the content and if you bring the farm up, say in a high availability scenario and if search is going to be inaccurate or unavailable for the next 24 hours that's sort of unacceptable. So you back up search and you restore search but that's difficult because you want to back up both the index files and the database at exactly the same time and again I mean it's sort of hard to do that for 2007. There are third party products that may help you but at least, out of the box, it's a little hard to do it.

Richard Campbell: Yeah, that's what I was thinking, there's third party tools for that but they're not free either.

Sahil Malik: Oh, absolutely not and one of the challenges would, I wouldn't say challenges but one of the worries that I always have when I purchase a third party tool is that that how is this tool going to work when I'm ready to upgrade to the next order.

Richard Campbell: Right, yeah.

Greg Hughes: Exactly, yeah.

Sahil Malik: So it means the more tools you introduce, potentially more things there are for you to check when you are upgrading then you just introduce more and more interdependencies and some vendors are better than others in ensuring that the product will upgrade smoothly.

Richard Campbell: Yeah but it's definitely a vulnerability and we've all been burned by this before that suddenly you're trapped, unable to move to the latest Microsoft product because the third party vendors you're using don't support it yet.

Greg Hughes: Right or you find out that you make an investment in a third party provider and then that becomes something that becomes requested so much in the core product that it just becomes part of the core product, that's happened before too.

Sahil Malik: Exactly. So again, talking further about performance another thing that is, I want to say it's a little bit of a myth or a rumor about SharePoint is that SharePoint lists are capped at 2,000 items and you can't put more than 2,000 items in a SharePoint list.

Greg Hughes: Okay.

Sahil Malik: That is a myth. When SharePoint 2007 was new, Microsoft released some guidances and they were very safe and conservative on what you can do with the list and one of the things it said was if you go beyond 2,000 items in a particular view, any container rather, then you may see performance degradation beyond 2,000 items.

Greg Hughes: Got it.

Sahil Malik: And while that is true, there are still many other ways to go beyond 2,000 items, there are ways to go beyond millions of items. What they really meant over there was that in all particular containers, so in a view or as in a folder, if you show 2,000 items and if you extract 2,000 items at the same time or more, then it's going to take a while for SharePoint to return all those items and that's fair but if you use, say a CAML query behind the scenes, then you can easily query millions of items in a matter of milliseconds, right?

Richard Campbell: Right.

Sahil Malik: Yeah. So that sounds pretty good. Also there are facilities such as logical indexes, even in 2007, where you can create logical indexes on a certain column and then the 2,000 limit can go up to, say 20,000, and you can continue to increase it. So, but again the challenge that that poses, both on the developer and the IT Pro guy, is that you sort of have to guess and estimate and rather predict the usage of a particular SharePoint list and you have to block the scenarios yourself where some user might query 10,000 items in one go right, and you have to sort of write the UI in a certain way or the IT Pro guy has to monitor the list themselves and manage them and sort of the IT Pro guy has to go and look around for these problems or problems waiting to happen and take necessary steps in advance and this sort of creates more extra work for the IT Pro guy to sort of manage and monitor all these lists that have the potential of growing large.

Richard Campbell: Right.

Sahil Malik: And again, the IT Pro guy technically should not be worried about the functionality, the role is more about keeping the servers running and availability and those kinds of things. So they can have the IT Pro guy to guess which list is going to get big. That's really the application developer or the business application owners would know that better. So that's another challenge that people, they rely on extra work and they rely on better communication and we know we have plenty of that in most projects we work in.



Greg Hughes: Oh, absolutely.

Richard Campbell: Very easy.

Sahil Malik: Another interesting thing that is sort of a segue from the SSP limitation that I mentioned earlier where you have in one SSP that can manage multiple websites but one website can be managed by a single SSP at any given time right, and that creates a whole set of challenges in itself. So one problem I mentioned was scalability but it also results in some functionality related issues. So one of the things I mentioned earlier was user profiles, now this is another challenge, let's say you have multiple farms in your organization and you'd say why would you have multiple farms? Well it's quite typical to have multiple farms, if an organization commits to SharePoint and let's say that they have an intranet based on SharePoint and they have an extranet based on SharePoint, chances are that these intranet and extranet are probably going to be in a complete set of different servers and also maybe segregated because of security reasons if nothing else, right?

Greg Hughes: Sure, right, right.

Richard Campbell: Once you get to a large scale application like that, shouldn't you have dedicated hardware? Shouldn't that farm just do that one thing?

Sahil Malik: A farm is a way for you to scale out. Now you could argue that why not just add more web front-ends into the same farm?

Greg Hughes: Yeah.

Sahil Malik: And not have separate farms and that is a way of scaling it out absolutely but for various other reasons you may end up with multiple farms.

Richard Campbell: Right.

Sahil Malik: Like user profile, oh I'm sorry, security is a very big reason why you may want separate farms.

Greg Hughes: Right.

Sahil Malik: Your outside-facing websites may not be allowed to talk to your intranet because if a hacker breaks into your outside-facing sites...

Greg Hughes: Yup.

Sahil Malik: You don't want them coming into the inside network.

Richard Campbell: Sure.

Sahil Malik: So there are multiple reasons why you'd have to have multiple farms but again the challenge that that produces is that's a user profile information, your extranet users and your inside user as well, extranet and inside users plus external users. So shouldn't the identity of the inside users or the user profile information on the extranet and the intranet farms be same or at least shared into some extent?

Greg Hughes: Uh huh, right.

Sahil Malik: But if you have an SSP that is limited to, I want to use one farm, it is limited to one website or rather the one website can be managed by one SSP at a given time, then it becomes very difficult to share user profile information between multiple farms.

Richard Campbell: Right. Do you have to build a bridge for that specifically? Some kind of DMZ?

Sahil Malik: You'd have to write code to do that and I did write some code for that very purpose, it's at codeplex.com/mossprofileimport, but this is open source shareware and we know how much IT Pro's like deal with other people's code because a lot of IT Pro people are not developers.

Richard Campbell: Yeah, no kidding.

Sahil Malik: So the IT Pro guy has to go and ask the developer on, "Hey, I have this tool, can you use this to move profile information from one farm to another?" And then somebody has to write those manually scripted jobs to do it like the tool that I mentioned MOSS Profile Import, it has the ability to export out profile information as an XML file and they move over the XML file and then you import the profile information into the other server.

Richard Campbell: Right.

Sahil Malik: And then you may have profile properties as well because SharePoint allows you to embellish the user profile information with properties that did not ship out of the box but they maybe useful to use. So you can add more properties to the user profile and again, if you add a property and each property can have multiple characteristics like it's a string with so much LANS and so on and so forth and you have to accurately make sure that those properties are reflected and are exactly the same on the other side, on the other farm. So keeping profile information in sync across multiple farms almost always becomes a challenge.

Richard Campbell: Okay.



Sahil Malik: It's a challenge but it's a small work for the people managing the system. It's not a challenge that can't be solved but it's just more work and it's just more headaches that we have to deal with. So that's another example where the whole SSP model that we have in SharePoint 2007 results in a few challenges that are extra work that we have to deal with. So that's probably one of the scenarios, now one of the things we mentioned earlier was why should we have multiple farms? Frequently, when we deploy custom code to SharePoint some of the changes go in the database but frequently a lot of those changes go on to the file system.

Richard Campbell: Okay, yeah.

Sahil Malik: Like when you deploy a solution you may edit a certain web.config or you may add certain files and SharePoint will also let you overwrite, out of the box, Microsoft files but as a best practice, you should not do that. So when you watch a movie and they say, no animals were hurt in filming this movie?

Richard Campbell: Right.

Sahil Malik: The SharePoint solution will say no Microsoft files were hurt in building this solution. It's just the best practice so people may not follow those rules, right? Now ASP.NET is one of the things, is the other Microsoft technology we use to create web based applications and one of the things that ASP.NET is very good at is its ability to work in a hosted scenario, right?

Richard Campbell: Yes.

Sahil Malik: So let's say I'm a person who has a very low budget and I want to have an internet facing site, I'll just contact someone, I mean one of these hosting providers like Orchestra or what not and they would give me a space on a server with very well-defined limitations and then that gives the hosting provider the confidence that I cannot potentially do anything that is going to affect other applications on the same server, right?

Richard Campbell: Okay, yeah, that's the way we do it at ASP.NET. Can you do that with SharePoint?

Sahil Malik: Well, you see, it's challenging, what you have to do, when I'm deploying custom code I have the ability to write to the file system and then the file system now has, is shared amongst everybody on the same server.

Richard Campbell: Right.

Sahil Malik: In fact we are sharing literally the same file and what that causes is, it just creates a management nightmare...

Richard Campbell: Sure.

Sahil Malik: For the hosting provider, so typically what hosting providers will do is that they will just say, "Well you know we're just going to limit you, you can't add custom solutions and it's difficult for them to be able to provide a single server where multiple tenants can live.

Richard Campbell: Yeah.

Sahil Malik: Again, take the example of the user profile import service, can you have such a shared service or a resource made available to multiple people without them having stepping on each other.

Richard Campbell: Yeah, you'll import somebody else's data.

Sahil Malik: Yeah. How do you prevent that from happening and can you have a scenario where you can say, "Well person A, you're willing to pay more, so you can have five of my services but person two who doesn't need my five services, I can give you only two, the ones that you really need and I'll charge you lesser." Can you do that with 2007? Not really. Another thing is that you have a concept of site collections in SharePoint.

Richard Campbell: Right.

Sahil Malik: So what a lot of hosting providers will do is that they'll say that we will restrict you, if you want to have a completely hands off management of a SharePoint hosted server, right? This is sort of what you have to do in 2007, is that you'll say we'll going to give you a site collection or let's say website which you can create your own site collections but you have to go ask us to create a site collection, ask us and the hosting provider...

Richard Campbell: Right.

Sahil Malik: Because to create a site collection you have to go through central administration, you don't want to give access to central administration to end users.

Richard Campbell: These sound like the same problems we used to have with hosted SQL server where there really was no concept of isolating tenants.



Sahil Malik: Oh, wow! Yeah, I would think SQL server would have a lot of similar problems but how do you do that now in SQL server?

Richard Campbell: Now that clients have gotten more sophisticated where I can individually identify what users can see, what databases and so on so that I can fire up the master client but only see my database is in a shared environment.

Sahil Malik: Oh yeah. I remember I used to be able to see the list of every single database on a server.

Richard Campbell: Right.

Sahil Malik: That's right.

Richard Campbell: And then it would go, "Oh no, you can't access that."

Sahil Malik: Yeah.

Richard Campbell: Isn't the answer here from the SharePoint perspective today to use virtual machines for isolation?

Sahil Malik: You can but then when you run a virtual machine then you're sort of handing over a full machine to the end user even though it's virtual...

Richard Campbell: Yes.

Sahil Malik: And then you have a limit on how many VM's can you run on a particular piece of hardware so it then becomes expensive and I'm sure that a lot of hosting providers probably do that, they'll say, "We'll give you SharePoint hosting" but really what they're giving you is that they're just giving you Windows hosting and they'll say, "Here's your Windows box and you have access to every portion on this particular system. We're running this Windows box in our data center even, virtual or physical doesn't matter but you own this entire box and you know what, if you break it, you fix it."

Richard Campbell: Yeah, your problem. All we can do is roll it back.

Sahil Malik: Right and Snapshots have a great way of doing that but let's consider this, a typical SharePoint farm has got a domain controller and multiple machines. Just because you rolled the Snapshots on one machine doesn't mean that your entire farm got snap shotted so snap shooters make you safe but they don't make you immune to the management issues that that may cause.

Richard Campbell: Yeah. I've always thought that snap shots are one of those great ways in making you

feel like you're backed up right up until you try and restore it.

Sahil Malik: Yeah, that's about right and you know that Active Directory works in strange ways.

Richard Campbell: Yeah.

Sahil Malik: When you rename an account, the SID changes and the SID is something that doesn't really show on the screen very well, you have command line utilities to find that out but if the SID changes and the problem doesn't surface easily to the IT Pro manager, you're going to run into a problem later that's going to be very hard to diagnose.

Richard Campbell: Definitely, yeah.

Sahil Malik: I mean those kinds of scenarios and the thing is one of the ways that a lot of people solved the hosting challenges are, they would give users a site collection and they would say, "This is your site collection and do whatever you want out of the box but we don't let you deploy custom code and we don't let you deploy custom solutions." And then you just use your farm out of the box and then it still good but it's not, I mean you just miss out on so much, there's so much more that you can do with SharePoint when you customize it.

Richard Campbell: Right.

Sahil Malik: And there are things that come out of the box at SharePoint, like the Wiki, for instance, it's okay but it's not the best Wiki around or the discussion board and you frequently want to enhance it further but if it's a site collection you got, that's all you've got. So that's another sort of challenge that running SharePoint in a shared hosting scenario is difficult both for the end user and also for the IT Pro manager and if you start giving people collections and other than establishing quotas, it is sort of difficult to guesstimate say, how much CPU resources is a particular site collection using, for instance.

Richard Campbell: Right.

Sahil Malik: So you can check disk usage but CPU usage, how much of the server does somebody really using becomes a little difficult to check? So here's another challenge that people run into when they're running a SharePoint farm, typically let's say, in an extranet scenario, let's say that you're an organization who's bought into SharePoint and now you've created an intranet that is based on SharePoint and now you want to create an extranet that is based on SharePoint.

Greg Hughes: Yup.



Sahil Malik: Now, by definition an extranet is something that's both internal and external users will use and by definition internal users will want to use that extranet using their active directory identities...

Richard Campbell: Right.

Sahil Malik: Because it seamlessly logs them in, you've got great things such as Client integration and so on so forth. Now there is this user who accesses the extranet both from inside and outside.

Greg Hughes: Yeah, exactly, right.

Sahil Malik: And then what happens is that in SharePoint when you implement an extranet, what you have to do is that by definition you have multiple authentication mechanisms on the same content.

Greg Hughes: Right.

Sahil Malik: So one is let's say farm space or RSA and the other is active directory. So in SharePoint 2007 what you have to do is that you have to take the same website and you'd have to extend it onto another port or another host center, basically onto another website.

Richard Campbell: Right.

Sahil Malik: And then you can have multiple authentications on the same content but you can have only one kind of authentication on one website.

Greg Hughes: Right.

Sahil Malik: So to support multiple authentications, you have to extend the website and the extended website can farm space now, for instance.

Greg Hughes: So you're creating a new IIS virtual server, if you will, or an instance of IIS?

Sahil Malik: IIS website.

Greg Hughes: Yes, a new IIS website and you're pointing that at the same content and using a different authentication mechanism.

Sahil Malik: Absolutely.

Richard Campbell: Don't you get into the complex with the actual ACLs that are on the files then?

Sahil Malik: When working with SharePoint you'd almost never set ACLs on to individual files.

Richard Campbell: Okay.

Sahil Malik: If you look at the details of how ACLs are implemented out of the box in SharePoint what it does, it will create a group called the wss_wpg...

Richard Campbell: Right.

Greg Hughes: Yeah.

Sahil Malik: And the files in the AP directory which is the Inetpub and in the 12 hive are given read access, read and execute access to wss_wpg and as long as you've given those rights you're set, that's all you need to do. So you don't end up giving ACLs to individual files but you do give ACLs to or individual permissions to items such as list items or list of sites...

Greg Hughes: Right.

Sahil Malik: But those go into the database and the database is shared amongst multiple websites...

Richard Campbell: Right.

Sahil Malik: So that's not such a problem.

Richard Campbell: Yup.

Greg Hughes: So that access then is managed outside of, it's application managed access, SharePoint is managing that security?

Sahil Malik: Exactly, exactly, absolutely and I mean it sounds like an engineer solution that you have two websites or two kinds of authentication but this introduces some challenges. One challenge it introduces is that the way it allows you to use farm space authentication is that it uses the membership provider API that comes with ASP.NET and farm space authentication that comes out of ASP.NET. Now let's say that I have, from the same farm, I have three different websites using three different kinds of forms of authentication talking to three different databases. Now for central administration to understand which website uses, to understand farm space authentication and to understand their user stores, central administration needs to be able to connect to those databases as well, the user-store databases, the user name password wherever that is, so all those three websites. Now if .NET doesn't support the concept of having multiple websites in the membership provider database, it supports multiple applications but the application in this case is always at root because it's a website so it doesn't support the segregation of multiple websites and therefore as a result of that, central administration will not prevent



you from marking a user from website A as a site collection administrator to website B.

Greg Hughes: Ah, okay.

Richard Campbell: In fact it doesn't even prevent you, it's a different thing, it doesn't tell you you're doing that. There is no way for you to execute a people picker search that restricts you to only a single database of users because ASP.NET doesn't support that concept and SharePoint builds on that so it becomes a management hassle for IT Pro's, that's one issue. Another issue it creates for you is that you have a system that you extranet that you created that can be accessed both by internal users and external users. Now there is this guy who's an internal user who accesses the system over AD when he's inside, when he goes home he accesses the system over an external user, using a farm space authentication mechanism but as far as SharePoint is concerned, this user is a completely different guy when he's outside the network right, because he's coming from a different user store and there is no way for SharePoint to know that this user name password that came across the farm space authentication is really the same guy that matched to this active directory identity went on the inside, you can't do it.

Richard Campbell: Right. Yeah, there's no way to connect those together?

Sahil Malik: Right. I mean this sounds trivial but it creates a lot of challenges because let's say this particular user is Richard and Richard needs to be able to edit this particular file and Greg goes in and gives Richard access to this file but he forgot to give access to farm space Richard but he did give access to AD-based Richard...

Richard Campbell: Right.

Greg Hughes: Right, right.

Sahil Malik: So now when Richard goes home, Richard has to call Greg and say, "Can you give these rights to me" and then this is one file, you multiply that with multiple files or lists or whatever that Richard could get access to and multiply it with all the users that you have and you pretty soon begin to see that this becomes a challenge.

Greg Hughes: Well that happened just the other day and I thought that Richard was just drunk dialing me on me but it turns out he was just confusing me because I can't decide which user he was talking about.

Richard Campbell: Sahil isn't it a mistake here using form-based security? Couldn't they maybe

doing some digest authentication or something that's still actually use the AD identity?

Sahil Malik: Well, yes and no. I mean, then what you have to do is that you have to expose your internal AD to the outside network and we don't want to do that for security reasons and the second thing is that if you use SharePoint 2007 Active Directory based identities directly exposed over the internet that what happens is that the browser will prompt you for a username password and you're supposed to enter it in the form of domain/username and then password...

Richard Campbell: Right.

Sahil Malik: I mean how many business users do you know who'll remember to type in the domain and how many business users do you know who will type in the right slash over there, so then it creates a helpdesk nightmare.

Richard Campbell: Yeah.

Sahil Malik: And then it's very hard to be in the phone and tell them that, "What kind of slash do you have?" You make sure you type in the domain. Now let's add more complexity to that a lot of security conscious organizations will also have policies and places that if you enter the username password incorrectly three times, it will lock your account out.

Richard Campbell: Right.

Sahil Malik: So then the guy enters his password and enters it correctly and bingo, next morning your account is locked out and he can't do anything, so it just creates a support hassle.

Greg Hughes: Yeah, exactly. There's got to be a better way to do all these things right? We've certainly identified an awful lot of opportunity.

Sahil Malik: Right and for the authentication side of things specifically, I can talk a little bit about this because this is already out is claim space authentication that will be available in the next version of SharePoint...

Richard Campbell: Oh.

Sahil Malik: In fact it is, claim space authentication is applicable to more than just SharePoint, I'm not talking about SP2010, I'm talking more about claim space authentication and that will solve a lot of problems. In fact, even enabling scenarios such as delegation over the internet, the my identity flows to another system over the internet or the ability for multiple organizations to talk to each other and be able to log in, let's say I want to log in to runasradio/something but a server that is hosted by



you Richard but I want to use an identity that is familiar to me so I want to use winsmart/smalik but I'm logging in to server that you host.

Richard Campbell: Right.

Sahil Malik: So currently, you do that using ADFS but let's say you have 10 search organizations and ADFS pretty soon becomes very, very, very complex to manage across 10 organizations.

Richard Campbell: Yeah.

Sahil Malik: And then not to mention ADFS is not the simplest thing to set up either and then things that says client integration with office client apps starts to break.

Greg Hughes: Right.

Sahil Malik: And claim space authentication does end up fixing a lot of that as well and we'll talk more about in detail I guess in the second episode of this podcast.

Greg Hughes: So that sounds very Geneva like, so are we talking about trusting identity providers and that type of mechanism, is that what you are talking about?

Sahil Malik: I maybe confusing the code names because I think the code names have changed but I think we're talking about Geneva...

Greg Hughes: Yeah.

Sahil Malik: But then at some point the code name used to be Zerman, I'm guessing that they changed it but I think the name now is claim space authentication but when you say Geneva we very may well be talking about the same thing.

Greg Hughes: Sure, sure. Well good, well that will be interesting to talk about when the time is right.

Sahil Malik: Perfect. Now how much time do we have left?

Richard Campbell: We're good to go man, let's wrap it up.

Sahil Malik: Okay. So I'll wrap it up by saying this one other thing that high availability and back ups and restores has been another massive challenge in the case SharePoint projects.

Greg Hughes: Oh yeah, for sure.

Sahil Malik: And again it can be done but it is a hassle to do it, it takes a lot of work to implement a good back up and high availability story in SharePoint 2007 and hopefully we could talk more about that in the next podcast.

Richard Campbell: You bet, Sahil thanks so much for coming on the show.

Greg Hughes: Thanks Sahil.

Sahil Malik: Thanks guys.

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