

**Video title:** [Partner Spotlight: Do your directories play nicely?](#)

**Date:** 3/29/06

**Description:** Directory specialist Jackson Shaw from Quest Software joins Sam Ramji from the Open Source Software Lab at Microsoft, to talk Active Directory and interoperability.

**Sam Ramji:** Hi, I'm Sam Ramji, I'm the director of the Linux Center Open Source Interoperability Lab here at Microsoft. Today in the studio I have the opportunity to interview Jackson Shaw. Jackson's a Senior Director of Product Management at Qwest Software. He came to Qwest through their Vintella acquisition. Qwest is one of our management partners at Microsoft and Vintella is one of the leading innovators in the field of UNIX and Windows interoperability. Jackson, thanks for coming in today.

**Jackson Shaw:** Thanks, my pleasure. Great to be here.

**Sam:** So you focus a lot of your time these days on Active Directory interoperability. Can you tell me a little bit about that?

**Jackson:** Sure. Well, basically what we're trying to do is help customers who've made a strategic investment in Active Directory, to be able to take that investment and extend it to the UNIX and Linux platforms that they've also got in their organization.

**Sam:** So those tend to be your typical, I've got lots of everything CIO, very heterogeneous organizations.

**Jackson:** Right.

**Sam:** What about the primarily Linux or UNIX organizations or do you not see many of those in the market? What's your experience there?

**Jackson:** Well, if it's primarily UNIX and Linux and they don't have any Active Directory, there's not really much of a play for us obviously. If they've got Active Directory to some degree, typically they're using it for their employee authentication already. You know, someone comes in in the morning, logs in on their Windows desktop and they might also happen to have a Linux or UNIX box there and they want to get that integrated authentication set up between those systems. So that's a perfect environment. If it's

strictly 100% UNIX Linux, highly doubtful that they'd be bringing in Active Directory to sort of help there.

**Sam:** OK. So you typically see what? These are the Global 2000 types of organizations?

**Jackson:** Right. Right. Yeah, I mean, you know, we've seen smaller organizations but it's organizations, as you said before, which have this mixed environment. They have perhaps, you know, half UNIX Linux or less than that but they've got a significant enough mixture of these different systems that they're seeing those cracks begin around things like security and integration between the platforms and people having multiple user IDs and multiple passwords, sort of the whole identify management compliance problem.

**Sam:** Sure, well identity integration is really hard.

**Jackson:** Exactly.

**Sam:** And it's pretty complex. As a matter of fact, recently we had Jason Zions in here, Jason is a— wrote Open NT originally and SUA so now he's an architect in the core interoperability solutions group working on those issues so I have about this much understanding about how hard it is actually to get it together technically at that level. What do you see as the big challenges in doing Active Directory interoperability? And let me start out with, if you can lay the groundwork around identity integration into big buckets and then start looking at Active Directory and specific.

**Jackson:** Sure, I mean I think one of the most interesting problems, and one of the analogies that I use with customers, is UNIX and Linux boxes themselves as they sit in a network are very much akin to when we had the whole NT domain situation, pre AD. So they're each sort of sitting there on their own, they might be networked together, but they pretty much each have their own administrator. And if you need help on machine A, you have to go to the administrator for machine A; if you need help on machine B, you have to go to the administrator for machine B.

**Sam:** So no shared trust.

**Jackson:** So there's really no shared trust. And what a lot of customers are trying to do is figure out how they can manage the identities on these different UNIX and Linux machines. A typical answer to that would be use a meta directory or some kind of a directory synchronization solution. Problem with that is you've got to go out there and use

that product and connect to every one of those different UNIX machines. So, company with 10 or 15 machines maybe not a big deal. A company with 1500 or even 500 or maybe even 100, pretty big deal because...

**Sam:** Because it ends up like the enterprise application integration problem in a way, you've got all these adapters, they're brittle, snap, you have to repair them.

**Jackson:** Yes, exactly and you've got to maintain each one separately. So the whole premise behind a lot of the work that we've done is — you know, Active Directory, you know, was born back in 2000, it's received a lot of adoption, tons of companies are using it now, it's well entrenched, there isn't that fear anymore that, you know, we don't need AD, pretty much everybody's got it now, they like using it. And one of the big premises about it is that Active Directory is that one place to go to manage all your Windows users. You don't have to manage a particular domain controller; you just manage everything as a whole. And if you could bring the UNIX and Linux machines in, and the UNIX and Linux users into Active Directory in that same fashion, I mean still keep them as UNIX Linux machines, mix users, but bring them in so they can be managed from one place. You get a fairly significant benefit from that because you don't have to have management of each individual UNIX or Linux machine anymore.

**Sam:** We used to call that the ideal where you've got decentralized operation but you've got the impression of centralized management even if that's through federation or integration.

**Jackson:** Exactly. And the beauty of this is it's not the appearance of actual centralized management, it's true centralized management in the way that a Microsoft Windows administrator would see it today with a Windows desktop. So those UNIX and Linux machines actually are domain joined so they look to Active Directory just as if they were another Windows machine. But if you go and look at the OS tablet, it doesn't show Windows, it shows something else. So the AD administrator sees this cohesive total of all these different machines out there and all these different users, and the UNIX and Linux people really don't see any difference on their end because they still have a user ID and a credential but they're now benefiting from the fact that it is domain joined, they're using their AD credential instead of a UNIX credential. Everything can be managed from that one place and it's that one sort of security principle that they can all utilize.

**Sam:** Sure, so it's really a bi-directional integration?

**Jackson:** That's right. And it's really — one of the key things about it is its actual true single sign on which has been a holy grail that many companies have been trying to get.

**Sam:** Well, I'd also say it was real interesting from a lot of perspectives. I remember we were working on a government project a few years ago where the one single point of failure for the whole project was their SSO system. They'd have 400,000 users come in and they had to first authenticate through that and half the time that would be down and nobody could access any of the work. So, does this help, does integrating these things help with those kind of scale issues or is that really more just a cluster?

**Jackson:** Yes. Well, this is—no, this is the ideal thing about Active Directory, is Active Directory is already used in some of the biggest companies in the world. I mean, 400,000 users is not unusual. You know, there are situations that I know of where there are telecom providers that have 25 million users in Active Directory. There's a local bank here that's got 17 million users in Active Directory. So the scalability, the reliability, the sort of overall guaranteed uptime that you could get with Active Directory is already there. We just leverage it with our product. So it's a great side benefit that you get from this. So, being able to handle all those extra people logging in, not a big deal.

**Sam:** So tell me a little bit about some of the customer scenarios that you see where people are using it. You know, the counter example is if it's mostly a Linux and UNIX shop you're not seeing people going and buying Active Directory to do this. You know, you'd think they'd be using Open LDAP or eDirectory or some other solution. But you also end up with some of those shops in the G2000s because you've got mergers and acquisitions that have pulled these things together. So, tell me about some of the more complex customer scenarios that you see this being a challenge.

**Jackson:** So I mean one of them right off the bat is the sort of more Microsoft focused customer that has pretty much a, you know, Window-centric view of life. They've got perhaps different versions of Windows and different versions of the OS on the server and then they go off and acquire a company or they merge with a company that might have a significant amount of UNIX or Linux machines or maybe even a lot of Mac machines. And that forces the integration because, you know, once you've worked in an all Microsoft environment and you see what the sort of UNIX and Linux people have with respect to multiple authentications and, you know, having a login in different places, different times, you want to try to be able to provide that benefit to your whole user population. So, one area that we see this happening is with those types of mergers and acquisitions. Another area is just quite frankly, you know, what we've been talking about which is the company that has grown up for whatever reason in a mixed environment. I mean some of those reasons are things like they've deployed a large ERP system and for whatever reason it

was deployed on a UNIX box and they either don't have the money or don't really see the impetus to move it to a Windows infrastructure. So, they do want to benefit from how— from that integration with Windows and Active Directory so, you know, that's one of the sort of other scenarios that we see that's happening.

**Sam:** Fix what's broken but don't break what's working.

**Jackson:** Right, exactly. Exactly. Or make it better just, you know, don't break it or—you know, I've been a big believer for a long, long time that, you know, in the whole directory services area we'll never get to one directory, right? I mean I started back many, many years ago was like oh it's all going to be a big X500 directory in the sky. Never happened. Then it was going to be the big LDAP directory in the sky. That never happened.

**Sam:** And then it was going to be one metadirectory.

**Jackson:** One metadirectory.

**Sam:** One virtual directory.

**Jackson:** And none of those have happened and there's not one Active Directory in the sky or even at a company that can do it all. So, what we typically see is that there quite frankly are going to be mixed environments where someone's going to have probably a fairly big contingent of Active Directory and they probably might have an open LDAT or an eDirectory.

**Sam:** Or several.

**Jackson:** Or several right. Or tens.

**Sam:** But then you've also got, if I'm interpreting you correctly, a lot of this is really about OS level support and it's where I usually think about identity integration fitting in, maybe some Web apps but primarily, you know, can I get to the network resources that I need and all that. But I think you're starting to get identity stores for applications whether or not those are integrated with their local OS, whether those are federated with other trust stores. Can you talk through some customer scenarios that you've seen around that and, again, drivers for why people are seeking to integrate Active Directory with UNIX and Linux?

**Jackson:** Right. Well, again, I think if you look at what some of the key drivers are and we can go into some of the use scenarios, it's things like, you know, they're already very reliant on Active Directory. They've maybe had three, four years of using Active Directory and now they're authenticating 10,000 or 20,000 or 50,000 people. It's been working really well. And someone just sits there and goes well how can we extend that further? How can I get some more value out of this investment and obviously if we can integrate UNIX and Linux systems with it let's do that.

**Sam:** So it's partly an IT portfolio management thrust saying we don't want to get more systems.

**Jackson:** Right, so it's partially simplification but quite frankly there are a lot of other drivers these days like compliance.

**Sam:** Okay, talk about that.

**Jackson:** Well, you know, I want to make sure that the—that Jackson is a—you know, when I want to go do a report on what he's done, if I just have to go to the Windows directory, if I just have to go to Active Directory and run one report and see what he's done across UNIX, Linux and Windows, that's a heck of a lot easier than me having to go to a UNIX System and run a report and it might be even a different user ID over there and then that Linux system or the 200 or 300 that we talked about run those reports.

**Sam:** So you're dealing with a lot of the things that would otherwise be data normalization and data cleansing issues.

**Jackson:** Right.

**Sam:** Which is rough because otherwise you've got spreadsheets in a room when you're crossing out in the Amazon.

**Jackson:** Right, and I mean if we look at for example security, I don't mean security from the Microsoft perspective, let's just talk about security of that password. AD gives you a really good capability to do things like have password rollover, password length, password complexity, password reuse; all these great rules around it. You don't have a lot of those capabilities on UNIX and Linux. They're very difficult to have those kind of policies standardized across all the different systems.

**Sam:** What are the challenges that you see there? What are the challenges that customers bring to you when they're saying we need to do better policy management across all our systems, we're having issues with our policy support on our Linux UNIX.

**Jackson:** Well, the problem they typically have is, you know, how do you maintain that across all those different systems right. How do I set up—you know, what software can I buy that's going to help me manage all of those different systems. And then even if you have that software, the credential that the person has on that side of the house is still going to be different than the AD credential. So then they're challenged with well do we synchronize those credentials together so it's one password or is there something else we can do? So I mean basically what we talk to clients about is how they can integrate those systems and basically take that AD credential that they've already wrapped a lot of these policies around and just simply extend it to UNIX and Linux.

**Sam:** So if someone were going to build this in-house, if someone were going to do this integration by themselves on a main force, what would be the thorniest technical problems that they would run into?

**Jackson:** Right. Well, you know, I want to step back and say that one of the really interesting ways that we've done this is we've basically enabled the—these capabilities within our products through the use of the standards that Microsoft has built into the product, like LDAP and Kerberos and some of the other standards that they've supported in the industry.

**Sam:** So these are strong industry standards.

**Jackson:** Exactly, exactly. So for us it was very easy to do that. The problem I would say for, you know, let's say anybody else out there to do it is that to set up all the right things and the intricacies around Kerberos authentication and LDAP authentication it's really, really difficult. I mean I've seen prescriptive guidance over 300 pages on how to do it. So you could imagine when, you know, you're sort of faced with a book that's this thick on how to do this integration manually that it's really, really difficult. And, of course, if you think of all the variants of UNIX and Linux that are out there and having to have each LDAP version, each Kerberos version on all these different systems all tuned the right way, we take away all that complexity, we vastly simplify it.

**Sam:** You end up with the N squared adaptor which is really difficult. What we found in the EII industry a few years ago is that you've got multiple versions of every adaptor and they're all handwritten. So that's a challenge.

**Jackson:** Right, and for us this isn't even a situation of going from N-squared to N, it's a situation of us going from N-squared to 1—that 1 being Active Directory.

**Sam:** Yes, that's a huge flattening. Do you find that people have usually struggled with this already? They have a number of patches or scripts or home grown code in place?

**Jackson:** Yes.

**Sam:** And what do those solutions usually look like and where are they breaking down that people say, "Help there's got to be another approach!"

**Jackson:** It's—I've seen it at some really great companies. I've talked to a lot of companies in the past and some really, really smart people. I've walked into rooms where they've said, "Gees, we've had these five guys off in closets for the last 18 months trying to, you know, hand wire all this stuff work together and we just haven't been able to get it to work." And some of the reasons are simply because of the fact that there are so many different UNIX and Linux variants that they have to, you know, sort of jiggle and juggle all these different components together to get them to work and they just have difficulty doing that.

**Sam:** So it's a heterogeneity issue on this?

**Jackson:** It's really a heterogeneity issue. In some cases they're working with Open Source solutions and it's not that the Open Source solutions don't do the job, in fact in a lot of cases if you've got one UNIX variant and you've got a small operation, you can use an Open Source solution.

**Sam:** Because that starts to look like homogeneity.

**Jackson:** Exactly.

**Sam:** Which is probably one of the advantages you have on the Windows side except the platform looks more homogeneous than you have on the flip side. Heterogeneity is always the name of the game.

**Jackson:** And as soon as you start mixing and building out the number of platforms, start getting into some of the scalability we talked about, I mean Active Directory handling

400,000 authentications or people logging in during the day, not a big concern. I don't know about the enterprise strength of some of the other solutions that are out there that you're throwing at it. So again, in the lab, in the small environment, the small business, probably something that's not as hard to do. Try to scale it out, more variants of UNIX and Linux, the problems become more N-squared like you said. And I've just seen a lot of people fail and it's not that they're not smart people it's just a very, very complex problem.

**Sam:** If you can give us a look inside this, a few years ago a very large IT company, services and software company, put out an ad that had a big black box on a big blue table and it said, Universal Integrator. It said there is no such thing. So they said be wary of N-squared to 1 reduction in complexity. Clearly they had a certain angle that they were selling services and customization but...

**Jackson:** It was a box that came with two greyhound buses full of engineers.

**Sam:** Exactly. But let's look at inside the black box if we can. What is it that you're doing that makes you able to bring this down from N-squared to 1? Without infringing on trade secrets just give us a sense for why is this possible.

**Jackson:** Sure. Well I don't think it's infringing on trade secrets at all. I mean there's two really key things. One is we've made a bet. Our company has made a bet on the adoption—the strategic adoption of Windows and Active Directory companies. Okay, and that is the platform that we're staking all of our software on. So in other words, the black box guy has to deal with, you know, all the platforms we've talked about, the e-directories and the open LDAPs and everything else that's out there. I mean that's not just N-squared, it's, you know, N-Squared to whatever.

**Sam:** Okay, so then you're federating forests that are based on heterogeneous directories?

**Jackson:** Well it's—you know, you can imagine that they've got to solve all the problems across all these things and all the different UNIXes and potentially all the different directors that are out there.

**Sam:** Now you integrate with the different directories as well?

**Jackson:** No, no, we're totally Active Directory focused. So we've kind of sliced this to the—we believe that the customers of adopted Active Directory, have adopted it in a

strategic fashion and that a lot of these customers are basically looking at how they could get better value out of Active Directory. That's all we care about. In fact, first question to the customer is, are you using Active Directory? If the answer is no, we move on.

**Sam:** What if the answer is yes and...?

**Jackson:** If the answer is yes and, then we want to drill down into what the—how they think about Active Directory, what is their thought process around Active Directory? Is it a strategic investment? Nine out of ten companies, the answer's going to be yes.

**Sam:** So let's say it is, and we've got a whole bunch of user rights and credentials and authentication stored in open LDAP. What do you do at that point?

**Jackson:** Well, there are a number of things that we'd obviously want to talk to the customer about. If they're already doing their authentication that way, there are ways for us to help them rationalize that with Active Directory or just simply turn on Active Directory. In some cases the customer—you know, they've got an investment in another directory and they may be using it for multiple things, they really do want to have Active Directory fit that challenge.

**Sam:** And how would you go about that cutover because that's fairly interesting for the main topic?

**Jackson:** Well, it's relatively easy because most everybody that walks in the door of the company to log on at your desk is going to know what they're, you know, Active Directory credential is. Right?

**Sam:** Right, because they think that is their Windows password.

**Jackson:** Exactly. So basically you install the software and you tell everybody okay, tomorrow when you come in, at that user prompt put your AD name in and at the password put your AD password in, over and done. It's really that simple.

**Sam:** And do you end up exporting a lot of the credentials that are in Open LDAP and adding those in? Because I may have a bunch of application and resource specific credentials only stored there and maybe as a user I'm used to logging into those resources, you know, manually, I get a network credential prompt every time.

**Jackson:** Right, so there may very well be a situation where the company wants to keep the application off—the application authentication in eDirectory, okay, but the non-application indication—integration or the—authentication, I should say, or the apps that we can support through these standards like Kerberos and LDAP have those all centered around Active Directory. I mean that's the key thing with apps is if it's a Web app that we can use federation with or if it's just a regular application like SAP or Oracle that integrates with these standards like the Kerberos and LDAP standards that we've talked about then we can integrate those guys into Active Directory and give them that sort of bigger single sign on real estate.

**Sam:** So you can kind of go in and snarf the rights and suck them into the same users Active Directory store. I imagine there's a lot of planning that has to go into any project like that where you're literally manually matching up users and making sure that you've got name parity or maybe there's name mismatches and who's who.

**Jackson:** Well, in some cases we're basically just going to cut them over, right? You know, one day you're logging on with your Open LDAP password, the next day you're going to log in with your AD password. In some companies they actually want to have some kind of separation of church and state. They may say for all the employee authentication we'll use AD, but we may have 100,000 business partners or customers out there, we're going to leave that in open LDAP for something else. We've seen that happen too. And that's just because from a security perspective they feel that they want to keep things separate or from just a general technical perspective they want to keep AD as being the sort of internal directory and just have something totally separate. Sometimes it is even AD separate outside for...

**Sam:** Right, the architecture is you're trying to build some separation and have fiefdom A and fiefdom B.

**Jackson:** Right. And then those are valid reasons.

**Sam:** Yes, those seem like pretty reasonable.

**Jackson:** Yes, so it depends on what the customer exactly wants and how we go about achieving that. But generally speaking it's more of a cutover than it is a migration.

**Sam:** Okay. Interesting. So effectively you have built a product that is based in terms of its core business logic, one to use as a repository and all the primary management mechanisms is AD but you've built adaptors to must be hundreds of different variants of

Linux and UNIX and different applications and all those adaptors are something that you provide basically out of the box.

**Jackson:** Right. It's—you know, the great thing about it is it's not just standards-based on the Windows side, but on the UNIX side we use PAM, which is the pluggable authentication modules. So we just plug into that which is a standard that most UNIX or Linux people understand. So yes you're right, we definitely have, you know, compiled versions of that and the code for, you know, Linux this and UNIX that on all the different variants. And then as we move from the operating system sort of up the stack to the applications then we provide the—either the prescriptive guidance or the code that helps them integrate with IBM DB2 databases, for example, or SAP or Oracle or any of the other products that we've worked with.

**Sam:** Sure. Let me ask you one last question which is, what's the wildest interoperability problem you've ever seen or heard a customer coming across. This can be before they're integrated, during the integration process, whatever. You name it, what's the craziest thing you've seen?

**Jackson:** What's the craziest thing I've seen? You know, I've seen one customer who basically wanted to—they were a telecom customer and they wanted to integrate, you know, every cable modem in the country with Active Directory. It was 7 million devices. So, that was really interesting because it was a sort of edge scenario that we'd never seen where, you know, most cases that this is dealing with, you know, you and I as IT pros sitting in their office, you know, logging in and taking care of things that way, this company was really interested in integrating all these things with an Active Directory so that they could manage them through group policy and then use some of our other management tools to, you know, both manage and monitor the devices. So that was pretty crazy because you're dealing with, you know, broadband networks and devices that are on all the time. You know, very strange. I'd put it on par with some of the other companies we've dealt with that have—you know, we're all again—most of us are all used to this, you know, you've got some big broadband pipe at home or your office, everything works, you know, kind of instantly for you but we still see customers who've got the typical 64K ISDN link from some place in, I don't know, Africa to another place where they're using a satellite connection where there's a lot of, you know, delay or they've got machines that are disconnected quite frequently. So all of those sort of add into the mixture of, you know, wild and crazy situations with customers.

**Sam:** That is pretty cool yes. Well Jackson, it's been a pleasure having you on.

**Jackson:** My pleasure.

**Sam:** Thanks for taking the time today.

**Jackson:** Great, perfect. Good to talk to you.

**Sam:** And yes, thank you.

**Jackson:** You're welcome.

**Sam:** And to those of you watching on the Web I invite you to give us feedback, let us know what are the partners—what are the topics you'd like us to cover, anything in the realm of interoperability, Linux, Open Source, it's all fair game, it's all interesting to us. So thanks a lot. Jackson, look forward to talking with you and your team again.

**Jackson:** Yes, great. Thank you.

**Sam:** Take care.

**Jackson:** Thanks everybody.

#### End of Interview ####