



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 #061
(Transcription services provided by [PWOP Productions](#))



SQL Server 2008 Compliance Features at Tech Ed US!
June 11, 2008



[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 #61, with guests Dan Jones, Sung Hsueh, and Il-Sung Lee, recorded live at TechEd, Tuesday, June 10, 2008. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com.

Richard Campbell: Hi. This is Richard Campbell coming to you for a very special edition of RunAs Radio from the floor at TechEd and with me as always, my fine friend and co-host, Greg Hughes.

Greg Hughes: That's me. Hello Richard.

Richard Campbell: How are you doing, man?

Greg Hughes: Good. It's been a pretty fun day.

Richard Campbell: Oh, it's crazy, crazy, crazy. I love recording shows right in the venue. Everything is going on around us. You can hear all the noise. You'll certainly hear it on this show coming up as well. It's a busy, noisy, frenetic time, but it's a lot of fun.

Greg Hughes: Yeah, we have the opportunity to talk to a lot of people here and everybody is very busy and so we worked really hard to try to get a few of those busy people in to record shows with us and in this particular case, you hosted a panel, you moderated a panel.

Richard Campbell: Yeah, it was a panel from a bunch of SQL Server guys, three of them to be exact.

Greg Hughes: Right.

Richard Campbell: Specifically about compliance and you were out in the audience. I know you got a couple of bits here and there.

Greg Hughes: Yeah, I was kind of carrying the mic around and trying to help keep things moving around.

Richard Campbell: All right. Well, have a listen to this. It's not too long, but it's definitely very focused on the compliance aspect of SQL Server 2008.

Hi. This is Richard Campbell from RunAs Radio coming to you from the floor at TechEd Online US for the IT week. We're at the TechEd Online stage with the fine folks from the SQL Server team. We're going to talk compliance with SQL Server 2008. So, why

SQL Server 2008 Compliance Features at Tech Ed US!

June 11, 2008

don't you guys introduce yourselves? I'll start from the far end.

Dan Jones: Great. My name is Dan Jones. I'm a Group Program Manager of the Manageability Team of SQL Server.

Richard Campbell: Excellent.

Sung Hsueh: My name is Sung Hsueh. I am on SQL Server Security Development Test team and I am a tester on the team.

Richard Campbell: And you must be working in encryption?

Sung Hsueh: Yes. My feature area that I work on is core database encryption and I've worked on both the top down level encryption features and the transparent data encryption features.

Richard Campbell: Fantastic. Finally?

Il-Sung Lee: And I'm Il-Sung Lee and I'm the Program Manager for the SQL Server Security. My responsibilities for the component are areas that include authentication authorization, encryption, things like that, all things security.

Richard Campbell: I think we got a great mix of a panel here because we've got the overall security issue. I think encryption is a huge part of when we talk about why this is going on and then Dan, you're here representing manageability.

Dan Jones: Yes.

Richard Campbell: The biggest challenge I have when we deal with the clients is just trying to understand what we need to do and then trying to figure out a reasonable way to do it. It's hard. It's not an easy problem.

Dan Jones: It's not easy. Prior to SQL Server 2008, it was even harder for customers. They really were left with creating a custom solution for monitoring a system for compliance with their policies, so pretty much every larger IT shop has a set of policies written down in a Word document, in an Excel sheet or an a SharePoint site. How does the IT guy know their system is in compliance with those IT policies?

Richard Campbell: Well, I've seen these compliance documents. I thought the tech folks wrote funny documents, but those things are terrible to read.

Dan Jones: The joke I like to make is policies or compliance documents are written by lawyers for lawyers...



Richard Campbell: Right.

Dan Jones: Not for IT people.

Richard Campbell: And it's not like that we get a sign that pops out of our machine and says we're not compliant. What's the actual process with -- I guess when we talk about the clients, are we really talking about Sarbanes-Oxley here or are there major compliance sets we care about?

Dan Jones: Well, there are government regulations such as Sarbanes-Oxley. There are industry regulations like PCI.

Richard Campbell: Right.

Dan Jones: Then IT shops themselves will create compliance policies...

Richard Campbell: Sure.

Dan Jones: Based on their internal needs.

Richard Campbell: Yeah. Whether we have regulation or not, it is not in our best interest to allow our data to escape our company.

Dan Jones: Correct. That's one policy.

Richard Campbell: Yeah, it's a pretty good policy, but vague. Now what? I've given this vague policy of protect our data, now what do you do to do that?

Dan Jones: There really has to be a manual translation process. What does that mean to the IT environment? If it's credit card data, you want to encrypt that data. Well, how do I encrypt the data? In 2005, we had some encryption technologies, but they required changes to the applications that were accessing the data.

Richard Campbell: Sure.

Dan Jones: In 2008, with transparent data encryption, you can turn on encryption without any changes to the application and now you're safe and secure. Your data on disk is encrypted, but what happens when a junior DBA comes along and turns off that encryption? How do you know when you're out of compliance with encryption policy?

Richard Campbell: Right and when it's turned off. Let me jump over to you Sung because we're speaking encryption and that's your schtick. So, are we now talking literally just a modification to a stored procedure and the data gets written encrypted?

Sung Hsueh: It's actually even easier than that.

Richard Campbell: Oh.

Sung Hsueh: It's actually just the database option. So if you're familiar with alter-database calls, you know, alter database set encryption on, this is literally just alter database set encryption on and then you're ready to go. I mean there's a few more things that you have to do to set it up, of course, but it almost literally is that easy.

Richard Campbell: Are we encrypting the whole database, the table, the column? What's the granularity like?

Sung Hsueh: The whole shebang. The entire database gets encrypted. This gives you a lot of great benefits like previously when you use encryption, any query optimizations that you had doesn't work anymore. We didn't get to encrypt the data, but now that we can encrypt the whole database, you get everything. All your indexes work, all your keys work. You have all the credit performance that you had before, so you have a lot of speed benefits and you have a lot of security benefits because you don't have to worry about that corner case like is this really encrypted if I encrypt this column? Well, yeah, it is encrypted because we encrypted the whole database.

Richard Campbell: So, the advantage of encrypting the whole database is that it just works uniformly I don't have the code for it.

Sung Hsueh: Exactly, exactly. There are no changes to any stored procedures. There are no changes to any views. You just use the data as it is.

Richard Campbell: So, how much of a performance penalty am I paying for that overall encryption?

Sung Hsueh: That's a great question. It really depends on your overall workload. If you see a high number of IO usage, then your workload will be IO-bounded anyway. So, you won't see a significant drag on performance, but if your workload is CPU-bounded, you will see some pit because encryption is all CPU.

Richard Campbell: Yeah, it's all about the CPU.

Sung Hsueh: Right.

Richard Campbell: Is this an opportunity there to justify a couple more cores on my server?

Sung Hsueh: Absolutely.



Il-Sung Lee: One thing I'd like to add about the transparent data encryption is that it's really meant for solution to taking data at rest and so a lot of compliance regulations such as PCI require you to have data while at rest. Now, the thing is we're not guaranteeing that this is going to make the test compliant. It really, really depends on your other -- it depends on interpretation. That's one of the issues with compliance is we can't come out of SQL as a product group and say that this is going to make you compliant or not you compliant. It's really up to the interpretation of the auditor of that compliance regulation.

Richard Campbell: Well, if I encrypted data on my disk and yet left it wide open with no password for you to pull that data, I'm still not in compliance just because data is encrypted. I mean there are a couple of different angles here and I want to go over these things about the auditing process is one thing, but also this -- if we're talking about true compliance and PCI, all right, we've got a great feature now to protect the data while at rest. What are we doing to protect the data in transit? I guess that's really not your problem as SQL Server folks. Am I able to pull that data in encrypted form so that I could pass it on already encrypted?

Dan Jones: Not with transparent data encryption, but with the COM level encryption or the cell level encryption that we used to offer in 2005 and we're still offering in SQL Server 2008, you can actually just pull the data in encrypted format. I mean it's not usable per se, but it will still be encrypted so you can pull it as a direct var binary data and then have your application try to deal with it. That's one possibility.

Richard Campbell: So, you do have to code to support this.

Dan Jones: You do have to code to support that.

Richard Campbell: But we do both, right?

Dan Jones: You can, exactly, yeah. You can absolutely use both and you can actually even use the cell level encryption with transparent data encryption.

Richard Campbell: Sure.

Dan Jones: So, if there's some piece of data that you really, really paranoid about, you could actually enable cell level encryption on top of the transparent database encryption and then still have that kind in-transit encryption. I mean it's not truly where we want to be with in-transit encryption, but I

mean it's definitely an option that developers can take advantage of.

Richard Campbell: Ultimately, there's more code to be done to do that even better if you want.

Dan Jones: Yes.

Richard Campbell: I don't think it's SQL Server's responsibility ultimately to take care of all that.

Il-Sung Lee: Well, if you're really concerned about data in-transit, SQL Server has supported full encryption since SQL Server 2000. So, if you're just worried about the wired communications, then that could be protected.

Richard Campbell: Right, but it's sort of beyond that people tend to move data around and so forth. So, I've been through the compliance process and you brought this up Il-Sung that in the end it's in the interpretation of the auditor that we're compliant or not and that really comes down to the auditor's comfort in our ability to show him the state of affairs and I think we've sort of been hinting at this, the logging of changes of rules. Dan brought up this issue of, yeah, we turned on overall encryption, but a junior guy shut it off. Do we know when that happened, do we know how that happened, how does that get then captured?

Il-Sung Lee: With 2008, one of the great new features I think that we introduced is SQL Server Audit feature and the SQL Server Audit feature includes a lot of benefits that, for example, SQL Trace in 2005 didn't provide.

Richard Campbell: Right.

Il-Sung Lee: One of the things that it actually does provide is that it tells you anytime that someone changes the state of the audit, so if someone tries to turn off the audit, that automatically gets capture in the audit file.

Richard Campbell: Right.

Il-Sung Lee: And now you can send it to a file, but you can also craft it in such a way that it's very difficult for even a system administrator to be able to change or modify the file and so it can be very difficult for the administrator to make any changes to the audit without it being captured in some form.

Richard Campbell: Without clearly leaving a trace.

Il-Sung Lee: Correct.

Richard Campbell: It's pretty hard for us to stop and shut off the log at all, but it's almost impossible to not leave a trail that they did that.



Il-Sung Lee: Correct.

Richard Campbell: All right. I guess that's fair. I mean we'd love to have it perfect and never could be changed, but it's better to have good tracking around it. There are legitimate reasons to turn this stuff off at times.

Il-Sung Lee: There are and, you know, in that case, you'll see in the log that they turned it off and you'll be able to tell that this person was going to turn off this, maybe asked for permission ahead of time.

Richard Campbell: Right.

Il-Sung Lee: And it kind of correlates with what they planned, but if it's unplanned, then it comes out as a glaring error. You can take these files and you can actually import into a database. You can do all sorts of queries against the log entries and maybe you just want to select for every time the audit has been changed. The other thing with the audit is actually you can do fine grain auditing where you could target specific activity within a database and you can have one log file that specifically keeps track of whenever the audit file gets turned off or on. You can have another file that keeps track of access to sensitive database or data or you can have one log that, for example, keeps track of every time someone logs in or logs out or fails to log in even. So, all this information can be captured through audit and it's very, very rich in terms of functionality and the scope of things that can be captured.

Richard Campbell: I know from my experience of dealing with this that the auditors were very interested in anytime structures were modified in the database. Alt DML was a big deal to everyone to see where the tables have been dropped or alterations have been made, and who might've done that. I also find it interesting to log when administrators modify data, when they do update stuff because that normally should never happen so that to them was really sort of a key thing. I wonder if we're granular enough that we can say, "Hey, this classic account issuing these kinds of statements needs to be logged separately."

Dan Jones: The answer is yes. For your first part, we can check and we can audit anytime that an object is manipulated or changed.

Richard Campbell: Right.

Dan Jones: So, that's something that's available in SQL Trace as well, but, you know, everything you can do in SQL Trace is also available in SQL Audit. The other thing is the granular auditing and so we now have the capability of saying that I

want to know when this particular principle, can be a user, a role, a group, is accessing a particular data and doing a specific action.

Richard Campbell: Right.

Dan Jones: For example, if I want to know when, say, a user Bob is accessing table HR and doing selects, then I can target my audit just to report that information. So, what that does is it gives you very targeted information in your log so you don't have a lot of noise. You have to post filter through, but it also enhances performance because now you have a situation where you're only collecting information that you want instead of collecting all these information and having to do post filtering.

Richard Campbell: Yeah. I guess the challenge is actually those logs get enormous and trying to find something relevant could be very time consuming.

Dan Jones: It can be and so, again, we provide functions that let you import these log files into a database, into a table and through that you can actually selected queries on the whole...

Richard Campbell: We happen to have a handy good quality query engine right nearby.

Dan Jones: We do. We do. One of the main "asks" I get is actually to have the audit log use the database as a target.

Richard Campbell: Right.

Dan Jones: Unfortunately, we didn't provide that in SQL Server 2008.

Richard Campbell: So, we're still writing the log files, we just snap to import.

Dan Jones: We write log files and I just want to add also that log files are not the only target that we have in 2008. We also allow you to send information to the Windows application log and the Windows Security Log.

Richard Campbell: Right.

Dan Jones: The Windows Security Log is actually a fairly big deal because it's the so-called tamper proof log that Windows provides.

Richard Campbell: Yes.

Dan Jones: Some people are using that and leveraging systems operation manager to actually collect the security logs from different machines, generate reports, things like that. So, that's one option that we have now.



Richard Campbell: Where does PowerShell fit into this whole equation in terms of the compliance issues?

Il-Sung Lee: I don't really view PowerShell as part of the compliance solution, but really higher up in the stack in terms of the overall manageability solution.

Richard Campbell: Okay.

Il-Sung Lee: With SQL Server 2000, DBAs constructed a lot of VBScripts over DMO, Data Management Object. DMO was a COM-based API for managing SQL Server. On 2005, we also read DMO to work against 2005, but we introduced SMO, SQL Server Management Object, which was the managed API, but there was no scripting support for SMO.

Richard Campbell: Right.

Il-Sung Lee: You had to create a VB.NET or C# application to interact with SMO. The introduction of PowerShell by the Windows team, we now have scripting support over our managed APIs. So, anything I can drive through the GUI or through T-SQL, I can also drive through the managed API and I can script that with PowerShell.

Richard Campbell: My initial thought, the reason I brought that up was that PowerShell would be a tool that you would tend to use with the auditor sitting over your shoulder, but since we basically import the logs into SQL Server anyway, you're just going to be inside the management studio doing the queries for them that way.

Il-Sung Lee: Exactly.

Richard Campbell: So, really, it's not that necessary. I find PowerShell might be an interesting tool for the routine self-audit just to see if there's surprises showing up.

Il-Sung Lee: Right and we have a new commandlet for PowerShell called `invoke-policy` evaluation. So, if you have a set of policies that you need to run against 2008, 2005 and 2000, you can now script support for that in PowerShell. Run those policies against your set of servers, import the results into a table and then query over that result.

Richard Campbell: See what you get and what do these policies look like?

Il-Sung Lee: Outside of the database, the policies are simply an XML file.

Richard Campbell: Right.

Il-Sung Lee: We can also store the policy inside an instance of SQL Server and then it's just stored as well in a bunch of tables.

Richard Campbell: And how granular a policy; we're just talking about logging is on, that sort of thing?

Dan Jones: Any what we call physical property of a table or a database or the instance itself, we can construct policy over. So, if we need to monitor whether database encryption is turned on for a particular database, we can offer a policy that says `encryption=true`. Now, we can monitor that database for compliance of that policy. If the database comes out of compliance for whatever reason, then we can use auditing to figure out exactly what was the set of events that led up to and after encryption being turned off.

Richard Campbell: This sounds like a new feature for my weekly maintenance stack alongside DBCC and so forth.

Dan Jones: Absolutely. I think there have been several blog postings and articles written for sqlservercentral.com around what is your morning ritual as a DBA or your weekly ritual as a DBA and they really constructed a bunch of "here's scripts you need to do" or "you need to go check this setting in the server." Well, if anybody is like me, the minute I walk in, in the morning and open up email, my day is shot.

Richard Campbell: Right.

Dan Jones: So, I may not remember to follow my daily ritual. With policy-based management, I can capture all of that intent in a set of policies, either have those policies monitoring the system real time and so I can get alerts when the system comes out of compliance or I can set those policies up to run on a schedule on a daily or weekly or monthly basis and then I can review the results of the policy evaluation.

Richard Campbell: Sometimes you'll find legitimate policy violations. You'll just need to go hunt those things down in order to check for them.

Dan Jones: Well, you don't have to know to check for them. That's the great thing.

Richard Campbell: Right.

Dan Jones: There's notification. You can receive an email to do the integration with DBMail. If you're using a monitoring tool like System Center,



policy violations are written to the event log and you can monitor the event log. Also, when you log in to Management Studio, we give you an indication if your server is violating any policies so you can do the analysis there.

Richard Campbell: So, a startup of the Studio, you do a run through of the policies that are existing?

Dan Jones: Well we're not evaluating the policies at that time, but we're looking for previous evaluations that show failures.

Richard Campbell: Show out of compliance, yes.

Dan Jones: And we've got those up in the GUI.

Richard Campbell: That's very cool. All right. Where should we go? What are we missing on compliance?

Dan Jones: Well, here's the big picture I think is compliance is really a number of different facets and elements. One is what is the intent of compliance policy and that, as an IT person, you really need help from your auditing team doing that interpretation to turn it into something that's meaningful to the system. You have to turn on data encryption. You have to turn on auditing and exactly what level you have to audit. Second, it's a set of technologies within SQL Server. So prior to 2008, you could achieve much of this, but you have to do a homegrown solution and all of your intent and your knowledge was locked away in your triggers and your custom scripts. With 2008, it's now captured as an auditing object.

Richard Campbell: Right.

Dan Jones: It's captured as transparent data encryption and it's captured as a policy. These features really work in concert with one another to provide that auditing or that compliance solution.

Richard Campbell: I can see very compelling and auditing event where I can show this collection of compliance feature essentially for that database and show how we're currently compliant and pass violations and how well the information is logged.

Dan Jones: Precisely.

Greg Hughes: What about people who are responsible for specific types of compliance? Maybe I have a PCI requirement. Is there anything that you're doing in SQL Server 2008 to kind of help me get up to speed faster than if I have to figure it all out by hand?

Il-Sung Lee: Currently, right now, the problem is and we've mentioned this a couple of times already is that I've actually dealt with several customers who have been under the PCI gun and it's actually quite surprising how different that their auditors interpret things.

Greg Hughes: Absolutely.

Il-Sung Lee: So, the first thing that we have to make sure is that we have to find out what requirements are from the auditor point of view. I can use TDE as an example, the transparent data encryption. For most people, this solves their data rest problem because data really is encrypted at rest. Some auditors may feel that that's not sufficient, that they interpret data at rest as maybe data that's not being accessed, so even if it's in memory, it may be data at rest in which case TDE doesn't really solve their problems. It depends on that, so once you get a list of these requirements from your auditor as to what they interpret the regulation to be, then it's something that we can provide in terms of, like if you have a problem with your cryptography, then someone like Sung would be able to provide some pointers on that. I mean he's already published a whitepaper on TDE that is out there right now that you can look at. Every compliance regulation has auditing requirements and so I think that depending what the auditing requirements are, there's information out there about how to set the audit to do exactly what you want and I think that's not a problem. So, I think right now the thing that's really missing is that there's a layer between what the compliance regulation mean and what does it mean to SQL Server and it's a bit gray right now because it depends on interpretation and then once interpretation is done, then I think that there's a lot of guidance out there right now. For example, for SOX compliance there's a whitepaper out there that I think one of the banks in Switzerland actually adopted to SQL Server and so it's available.

Sung Hsueh: I'll tiptoe out on the edge a little bit. We're working on a couple of customers on we call it internal compliance SDK.

Richard Campbell: Sure.

Sung Hsueh: It's a CDK, compliance development kit, which will via theories of best practices, whitepapers and a set of policies and configuration objects for customers to be jumpstarted in their environment for implementing compliance.

Richard Campbell: Well, it sounds almost like you could have a compliance role in the database now, someone who's able to go test policy and validate auditing rules, but probably not do a lot of the other things that DBAs might do inside the database. It's an interesting angle on some things and I was listening



to these thoughts around depending on whether an auditor would react well to the data at rest encryption level. Of course, the problem is you've almost made it too seamless now. If someone could get into Studio, they just see the data naturally. It's not like the encryption is an obstacle. If you haven't put good procedures in front of your login rules and so forth, SA still has no password, you're going to be able to circumvent encryption pretty easily.

Dan Jones: I think that's absolutely true, but the thing is though we have a really robust permission model as well and that's what we have to encourage people to learn more about.

Richard Campbell: They have to use that permission.

Dan Jones: Exactly. Yeah, I mean like -- we say upfront that TDE, transparent data, encryption is not meant to be a replacement for good authorization model, so we absolutely still encourage people to learn about roles, to learn about permissions and, you know, to make the most use out of them because that's actually what's going to really protect your data and online server.

Richard Campbell: But ultimately, TDE is going to be great in the case where I have a detached database, I just can't read it, and then back up the same way?

Dan Jones: Exactly. Yes.

Richard Campbell: So, as soon as I get away from the parent machine and I can't control that parent machine, TDE is covering it.

Dan Jones: Absolutely. I think that's one of the key benefits that TDE also provides.

Richard Campbell: Absolutely.

Dan Jones: I mean there's been a huge request for backup encryption and transparent data encryption won't give you that. When you're backing your database by default, you will have an encrypted backup and you absolutely need to have the correct key in order to use that in the future.

Richard Campbell: And that key is how scary?

Dan Jones: Actually, that's an excellent point. That's something that can be kind of frightening to people who are not that familiar with encryption at all because if you lose your key, you lose your data and there is no recovery for that. I mean we can't provide you a back door because if there's a back door, that means somebody else could get to that back door.

Richard Campbell: Absolutely.

Dan Jones: Absolutely.

Dan Jones: So, there is no way to actually recover that key if you lose it. We can only advise you to try to back it up as often as possible.

Richard Campbell: And also secure it as well so that you don't break your whole protection system.

Dan Jones: Exactly, yeah.

Richard Campbell: In the event that key gets into the wild.

Dan Jones: That's absolutely true.

Richard Campbell: Is this a private key or a public key?

Dan Jones: Yes.

Richard Campbell: Identify the encryption you're using.

Dan Jones: There are actually several layers of it.

Richard Campbell: Okay.

Dan Jones: Yeah, this is a good point. There are several layers of encryption. So, at the topmost layer, you kind of have this certificate object, which is, you know, as you mentioned, a public key and private key pair and that's meant so that there's some really easy tech support to take around with you. There's X.509-based exported format. So, we just use industry standards for the certificate and that in turn protects a symmetric key which actually protects the data and the symmetric key can be of the AS, that's encryption standard algorithm, or we even support Triple DES...

Richard Campbell: Right.

Dan Jones: For, you know, just crypto agility. So, yeah, that's the key structure that we use.

Richard Campbell: So, these keys could be good and long as well. I mean the nice thing about symmetrical keys is you're minimizing the performance impact.

Dan Jones: Exactly.

Richard Campbell: It's a strong encryption methodology but it runs well on the machine.



Dan Jones: Exactly, absolutely. That's why we use the symmetric key to protect the data, then we use the certificate to protect the symmetric key.

Richard Campbell: Right. That makes sense to me.

Dan Jones: Yup.

Richard Campbell: Any other questions?

Greg Hughes: So, what I'm taking away from this, let me see if I'm hearing you right is you're providing us with tools it takes to be compliant, but compliance is probably important to understand that that's a case by case basis as to what "compliant action" means. It's exciting to hear there are a lot of new tools that are coming out as part of the product in order to better enable that.

Il-Sung Lee: That's essentially correct. I mean compliance is such a large and varied field right now and it's really, really hard for us to provide any kind of, you know, one rule to say that this is going to solve your problems.

Greg Hughes: Yeah, there probably isn't that one rule.

Il-Sung Lee: Right and so what we're working towards is we're working towards trying to give you the tools necessary to make it easy for you to solve the task that you have that's identified as needed for your compliance needs and as we roll on further, I mean this is something that we're really, really focused on and we will focus on in future versions.

Greg Hughes: That was really my next question was what do you hope to do next? What does the future look like? I mean with limited amount you probably can share, but what...

Richard Campbell: 2008 I guess are we getting a beta or an RC0 this week?

Il-Sung Lee: Yes, yes. It's actually out. You can pick up the discs at our kiosk.

Richard Campbell: Yeah, so the SQL Server space over at the community area. We got RC0 out, so, you know, soon we're going to have 2008. Is it time to start talking about the next version of SQL Server?

Il-Sung Lee: After my vacation, then we can start talking.

Richard Campbell: But I've got to think there's a set of features that you managed to get in here

because you're probably much feature lockdown now if you're an RC0. There's got to be some stuff that can be carried forward for v.next so to speak.

Dan Jones: That's correct and there's very limited amount of things we can say about the next version...

Richard Campbell: Sure.

Dan Jones: Because we're still planning it right now.

Richard Campbell: Yes, still working it out, but I mean the obvious one, you brought this up, was can I log directly to a table rather than logging on log files then importing.

Dan Jones: That's definitely one of the things we're considering and I think that we're going wherever the customers is demonstrating the most need. Compliance is definitely up there in terms of the questions that we get and "asks" that we get.

Richard Campbell: Sure. Well, then it's certainly merit to let's get 2008 out, let's see how our customers use it, and then find out what we need to do for them to make it easier.

Dan Jones: Right.

Richard Campbell: All right, guys. I think we got a great discussion here. I really appreciate you coming on the show talking to us about compliance.

Il-Sung Lee: Thanks a lot.

Dan Jones: Thank you.

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