



<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 #082*  
(Transcription services provided by [PWOP Productions](#))



**Clint Huffman Does Performance Analysis of Logs!**  
**November 5, 2008**



## Clint Huffman Does Performance Analysis of Logs!

November 5, 2008

[Music]

**Brandon Wenn:** From [runasradio.com](http://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 #82, with guest Clint Huffman, recorded Thursday, October 23, 2008. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at [pwop.com](http://pwop.com).

**Richard Campbell:** You're listening to RunAs Radio. I'm your host, Richard Campbell; with me as always my co-host, Greg Hughes.

**Greg Hughes:** Hi everyone. How are you, Richard?

**Richard Campbell:** I'm well, sir. I'm in Barcelona if all has gone well. Don't you love the time shift to Radio?

**Greg Hughes:** That's cool. It's quite a coincidence, I think. I'm in Barcelona too.

**Richard Campbell:** Yeah, funny how that works actually.

**Greg Hughes:** Yeah.

**Richard Campbell:** It being Wednesday; we should be in the middle of doing Speaker Idol and have partied for several nights in a row. We should be wrecks actually.

**Greg Hughes:** Yeah, it should be. This is about the time that we should be completely exhausted.

**Richard Campbell:** And two more days to go.

**Greg Hughes:** A couple more days to go, right, exactly.

**Richard Campbell:** TechEd is a marathon, no two ways about it. Pace yourselves.

**Greg Hughes:** Looking forward to it though, it's going to be quite a good show.

**Richard Campbell:** Absolutely and if you have any questions, comments, want to ask for a particular show, I know we've been on a PerfMon-bent lately but it's a good thing, we're learning lots of stuff, send us an email, [info@runasradio.com](mailto:info@runasradio.com). All right, Greg, let's introduce our guest. Clint Huffman joined Microsoft in 1999 supporting web technologies, Microsoft load testing tools, and later worked as a Testing Consultant helping people with load testing at the Microsoft Services Labs. There he found a passion for

solving Windows performance issues. In 2006, he joined Microsoft Premier Field Engineering to take on BizTalk performance issues only to find that most issues could be diagnosed by analyzing operating system resources. Some may say that performance analysis of Windows is more of an art than a science. Well, Clint strives to make it as much of a science as possible and to bring it to the masses. Clint is probably best known for his Performance Analysis of Logs, PAL tool, which simplifies the analysis of performance monitoring logs. He is the author of many of the recent BizTalk performance guides on MSDN and recently spoke at Tech Ed 2008 on BizTalk performance analysis. Welcome Clint.

**Greg Hughes:** Hi, Clint.

**Clint Huffman:** Hey, glad to be here.

**Richard Campbell:** So you are a part of a cluster of folks we have just been talking to recently. I blame Steven Choy actually.

**Clint Huffman:** Yeah, that kind of spawned it all.

**Richard Campbell:** He really did. As soon as we tipped in to PFE, there is suddenly this realization of wow. I always thought there's a lot to Performance Monitor, I think most people don't understand it. It's got to be better ways and when we started talking to Steven about it, he tipped us to PAL which led to you and also Shane Creamer stuff around the boot camp for Performance Monitor. I'm really excited because I'm learning a ton.

**Greg Hughes:** It turns out there's this secret world of Performance Monitoring and Performance Metrics that nobody knew about that we're just trying to bring to light.

**Richard Campbell:** Yeah.

**Clint Huffman:** Well, we're in the field all the time and so we run into a lot of pressure to solve these issues very quickly so we've got the developer and tools and we're now on techniques to really solve these things, real world stuff, that's why we got this stuff now.

**Richard Campbell:** In PerfMon, everything is there. It's like your own little internet. Everything you want to find is in there. You just don't know where it is.

**Clint Huffman:** I heard you say that many times and that's very true. I mean, that's what has frustrated me all these years that we have all this fantastic information and there are people out there that know what those counters mean and what they do.



## Clint Huffman Does Performance Analysis of Logs!

November 5, 2008

**Richard Campbell:** Yeah.

**Clint Huffman:** It's just a matter of getting that kind of mentality. They get their brain basically in the way they analyze things, and then finally get it on to some kind of formula then actually be able to analyze that in a scientific manner. So like I said, most people, like I was saying earlier like, you know, most people would say Performance Analysis is more of an art than a science. Well, that's true but there usually are reasons for that. Usually they said that because, well, there are a lot of factors involved that they maybe considering and to show me different factors that they had considered like, well, you know, it's got to be an art because it has some of the variables in this whole equation.

**Richard Campbell:** Sure.

**Clint Huffman:** But as you look down the equation, you might have something to go by at least for some guidance.

**Richard Campbell:** Well, it is certainly math. I think the art part of this is the knack of diagnostics of being able to look at all those values and get a sense of what's actually happening in the machine.

**Clint Huffman:** True.

**Richard Campbell:** And I do find there are people who do that very easily, that they have that diagnostic knack that they can put themselves in the context of the machine saying with this much memory consumed -- you know the great battle is I do this with load testing all the time for websites where suddenly we double up the load demand onto the website but the website load increase only goes up about 20% and so folks go, "Wow, we hit saturation point. Even though we double the number of connections, it hasn't gone up that much." And I've got that instinct that goes, "Nah, I think the test machines are saturated." And you go look and you go, "Yeah." Actually things during the load can't generate anymore load. Just because you told it to double it up doesn't mean it delivered.

**Clint Huffman:** Right, exactly and your response times probably went up as well.

**Richard Campbell:** Sure and it's interesting, you know those kinds of graphs where you see, yes, I increase load, increase load, increase load, the times increased will then eventually hit saturation and they sort of decrease again before the whole thing fails.

**Clint Huffman:** Right, diminishing returns, yes.

**Richard Campbell:** Yeah, it's funny and there is where I think there's really an art element to it, that sometimes the stuff is not intuitive. It's counter-intuitive to what you think would happen and you got to really find out what's the narrowest point in the pipe now where are we actually strangled.

**Clint Huffman:** We have some good indicators of that and that's what Shane Creamer's Vital Sign is all about as far as this workshop in key core OS performance counters and their thresholds but in order to understand those, of course you have to know a little bit of Windows Architecture and of course not everybody wants to learn that.

**Richard Campbell:** Yeah and I think that's the key part to this. I mean there are two things. One is what to measure and what does that mean, but then you get into this whole threshold element of what's a good number, when is something too busy and that is not always obvious. I guess this is where PAL comes into play, right?

**Clint Huffman:** Right. When I started teaching in the Vital Signs, for example, with Shane which was teaching Performance Analysis and Performance counters, people would leave that workshop and say, "You know what, that was the best workshop I ever had," but I just realized there is like about a hundred counters I need to be looking at to really understand the Performance Monitor log against that machine to understand why it's slow.

**Greg Hughes:** Right.

**Clint Huffman:** You know I got a day job. I'm managing hundreds of servers; I can't do that on a regular basis. So everyone is, "You know what, there's got to be some kind of automation here, some kind of way to make it a little easier." Furthermore, customers would give -- I was getting known for doing Performance Analysis and customers start sending me about 10 Performance Monitor logs and say, "Hey, can you analyze those by this afternoon?" I go, "You've got to be kidding me." You realize how much work is involved in that, you know, looking at all these things properly. So then I started teaching the VBScript workshop which is also another great workshop we deliver and I thought, you know what, I'm teaching VBScripting, I'm teaching Performance Analysis at logs so why don't I put the two things together, and that's when PAL started to come out.

**Richard Campbell:** What did you write it in? Just out of curiosity.

**Clint Huffman:** Well, I wrote it in VBScript.

**Richard Campbell:** Nice.



## Clint Huffman Does Performance Analysis of Logs!

November 5, 2008

**Clint Huffman:** The power is actually about a 6,000-line VBScript. It's pretty big. It's a language I know best and so I wrote it in that.

**Greg Hughes:** I can relate to that. A company that I worked at, we put together a security software that did bad behavior fraud analysis on web server logs and it's about a 15,000-line pro-program. It's compiled but it started out as a perl-script.

**Clint Huffman:** Wow, yeah, they get pretty big.

**Greg Hughes:** Yeah.

**Richard Campbell:** I'm horrified, sorry.

**Clint Huffman:** Horrified.

**Greg Hughes:** Sometimes you use the tools that do the job well.

**Clint Huffman:** Yeah.

**Richard Campbell:** I guess yeah, the proofs in the pudding; the thing works. It's just VBScript and --well, Clint, work us through. How does this thing work?

**Clint Huffman:** Okay. So right now it has evolved so now has a full user interface but it's actually VB.NET user interface, but really the user interface is just a glorified batch file creator for the Script underneath.

**Richard Campbell:** Beautiful.

**Clint Huffman:** So anyway, you download the tools from [codeplex.com/pal](http://codeplex.com/pal), PAL, and you go there and download. It's free, and open source. That was one of my other criteria too because Microsoft we produce some great tools and I've seen these tools and I'm like, "Great, this is awesome. What can I use it with in front of the customer?" Like, oh, "It's actually for our internal use only for now." I'm like "Oh, man, you got to be kidding me." So that's why I started writing something open source and free. But anyway, download it from there and then you got to install the MSI Installer and stuff and then you'll be presented with kind of the user interface here. Unfortunately, I can't show it to you guys in front of this but...

**Richard Campbell:** Yeah, radio.

**Clint Huffman:** Yeah, its kind of radio, yeah. So I just kind of talk about it I guess. So you're presented with basically a wizard. It is the best kind of format I figured that would be fit for this because all the arguments going to the Script get pretty big and I wanted to make it very easy. The whole idea here is that you basically give it a Performance Monitor log,

the path to the log file, then you specify what kind of machine was it, was it Active Directory, was it BizTalk, Exchange, IIS, SQL, take your pick at what kind of a machine it is. Then once you've established that, then you have to decide which questions, the answer on that particular item. So the idea about other performance tools that I've encountered in the past, something like the Server Performance Advisor tool, which is a great tool by the way, but a lot of these tools didn't take into consideration information about the server that they couldn't get anywhere else. For example is the system 64-bit or 32-bit, how much physical memory does it have, are you using the 3GB switch? All those have an effect on the system as a whole as far as performance, and so by having these questions being asked and then later using those questions that you're asked as variables in the thresholds is really what gives us a lot of power.

**Richard Campbell:** Right. It's really that combination of knowing the infrastructure of the machine or the configuration of the machine combined with these variables or the load levels that really gives you the insight.

**Clint Huffman:** Right and what's even better about this now, yes, I could have gotten some of this information from the machine itself by using WMI and various other things but the stuff like RAID type that I might not be able to get from the machine...

**Richard Campbell:** Right.

**Clint Huffman:** Only the standard administrator maybe will tell me that and we're actually considering writing a performance storage, storage performance threshold where we actually define the RAID types and the LUNs and then with that information, and using the performance counter standardized the counters in a better light because looking at the counter straight up but not of that knowledge is not going to be helpful, but having that ahead of time really helps.

**Greg Hughes:** Now maybe a bit of a stretch, am I able to take, say change the array type or flip some of those variable switches to do some estimation of what if I did change this thing. Is that a useful way to use PAL to figure out what might happen if I do change the configuration? Or is that not a valid way to use it?

**Clint Huffman:** Oh, like a "what if" type of thing? No, it wasn't originally design for that per se. It really was kind of designed to tell you when you're breaking a threshold based on your current configuration.

**Greg Hughes:** Got you.



## Clint Huffman Does Performance Analysis of Logs!

November 5, 2008

**Clint Huffman:** But that's certainly something to consider and I've also been approached about doing green computing with PAL, which is a new concept for me, basically telling people where they had excess and resources, the inverse.

**Greg Hughes:** Interesting.

**Clint Huffman:** Yeah, that is interesting.

**Richard Campbell:** Yeah, in the green computing side of things, I like this idea of starting to break down to watts per transaction.

**Clint Huffman:** Oh my gosh.

**Richard Campbell:** I think one set of instrumentation that we don't have right now is how much power the machine currently consuming. It could be a PerfMon metric but we don't have it yet but I think once you have that, you can get into that kind of detail because people are getting really serious about -- I think, there are two forces going on in that whole greening datacenter thing. One is we've now got a processor density per use so high we almost can't feed enough power in cooling to the rack. It's killing us; and then you also get into this how do we be more efficient like if I could actually go back to developers and say like you could work on your -- I want you to help develop code that consumes fewer watts per transaction, it's an interesting angle on that...

**Greg Hughes:** You could do just some correlation, I mean even if it accepts that information about power consumed overtime, you know, and did some baselines for different machines that you have, I guess you could at least correlate the information and do some of that. Its pretty interesting stuff.

**Clint Huffman:** Yeah.

**Greg Hughes:** There's no way to get wattage and stuff like that into PerfMon right now, right.

**Clint Huffman:** No, there's nothing in there yet.

**Greg Hughes:** If you know what a 100% CPU or 90% CPU uses in terms of wattage, I guess you can infer that, maybe you can do some calculations though.

**Richard Campbell:** Yeah but there are so many other factors when you get into the spinning drives and the cooling fans and I'd really like to...

**Greg Hughes:** Sure.

**Richard Campbell:** The only common point here is actually instrumenting the power supply but I think

we're a little off track. I'd love to instrument power supply but I think that I'm the only one.

**Clint Huffman:** Well, that is a serious topic of course and they were definitely looking into that so that's definitely something and that's another reason why we've got a lot of people going into virtualization which if there is one thing I want to talk about, its virtualization and analyzing performance in Hyper-V, before we're done with this talk, assuming we come back around to that.

**Greg Hughes:** Sure.

**Richard Campbell:** Sure.

**Clint Huffman:** So I've mentioned the whole idea was to make this really simple with the analysis so I want to basically ask you for the PerfMon log which is easy enough to do when you give me the path to it and then answer a few questions about the server, how many processors, does it have a 3 GB switch turned on and things of that nature. So answer those questions for me so that I can do a better analysis on the log. The other things are pretty much optional at that point. The analysis answerable is do you want to break this thing down and what kind of time slices, and this isn't the data gathering time slices because you can gather a log in a certain rate. This is how you want to break up the log. So if I default it to set auto which is to break up the log in 30 separate chunks, 30 different time slices and then we analyze each individual time slice ahead of time. The reason we did it this way is because some of these logs can be humongous and we really can't analyze every single data point in that case. It would just take too long first to process all that. So breaking it down into these time slices, we can actually analyze it much faster and still be relatively accurate because we're still looking at minimum values, average values, and maximum values, and even trend values in each of these time slices.

**Greg Hughes:** So you're going to see what's your minimum and your maximum for any given counter for like a one hour if your time slices is one hour or two hours, as opposed to maybe 24 hours. Is that right?

**Clint Huffman:** It could be a variable depending on how long the log was taken for and yeah, if there was like a spike in disk usage where you went to up to like one second IO response time per second, you know, we'll catch that because the maximum value hit that.

**Greg Hughes:** Right.

**Richard Campbell:** Yeah and of course the maximum value is the one that matters, that's the



## Clint Huffman Does Performance Analysis of Logs! November 5, 2008

point at which the machine was likely the most in trouble or the minimum value right out of the memory or totally burying the processor.

**Clint Huffman:** Correct, correct and so what it is is that power has different weights that it has for those particular metrics. So for example you've got CPU spike, you know height would not be considered very -- it will be like more of a warning than a critical, but an average CPU for the entire time slice would be considered critical just because it's the average value versus the maximum.

**Richard Campbell:** That makes sense to me. I find processors banging against 100% all the time, that's not a big deal. It's just when they're pinned there for an hour that it's bad.

**Clint Huffman:** Exactly. So it depends on the scenario and certainly you can adjust that.

**Richard Campbell:** You can adjust the weights?

**Clint Huffman:** Yes, yeah, that's the other thing. So in the PAL tool, the other thing I was a little frustrated with (well, not frustrated but) what I really wanted to have in a performance analysis tool is that the thresholds in many of the products that we have really were not cutting the mustard when it came down to analyzing performance. They really had like, okay, if this counter value was greater than 5,000, then it alert and that doesn't cut it. What it is, is at PAL, actually every one of the thresholds are actually code so that's the kind of the beauty of it. The reason why I want VBScript in the first place was because there's a cool command in VBScript called .execute which allows you to bring in text, like a string of texts, and execute that as code during runtime.

**Richard Campbell:** So you're essentially able to store an expression of how you would evaluate that combination of counters or that metric and just execute it in line.

**Clint Huffman:** Right. So what it is is PAL is actually writing the code for threshold or at least finishing it up and then executing it and say, okay, did we have a Boolean value I guess, or no, in breaking a threshold.

**Richard Campbell:** That's cool. It's clever.

**Clint Huffman:** Yeah, this makes it extremely flexible because now, like for example calculating like a non-page pull-to-pull page by itself kernel memory, that's very difficult if you've ever taken the course because you have to look up how much physical memory is on the box. If you're using 32-bit or 64-bit, 3GB, PAE, all that stuff changes maximum values of those pool sizes...

**Richard Campbell:** Right.

**Clint Huffman:** So I can put that in a one big little VB or another like put it in a threshold code which is actually quite long and then executing that and then it's done, it does it for me.

**Richard Campbell:** That's cool and that really does take it up a notch because that's hard to do by hand to sort of bring all those factors in and you end up writing it on a piece of paper so you're scratching, okay, that's a bad number, that's a good number.

**Clint Huffman:** Oh yeah, this has saved me so much of my own time because you know, first you got to calculate on what it is and then you got to see if its within 60% of that value or more than 80% of that value.

**Richard Campbell:** Right.

**Greg Hughes:** Right. The real value of tools like this is instead of spending all that time doing the heavy lifting and kind of the grunt work, you can do that for you, now you're well paid or well trained technicians and the people don't have to solve problems and actually instead of spending time figuring out what the problems are, they can actually spend their time solving it. Right?

**Clint Huffman:** Exactly. That's the whole idea. This is again is not a replacement for traditional performance analysis and I keep telling everybody that. Other people still use it without any knowledge which is a little scary sometimes but it is strictly a timesaver to have you quickly go into it, and then the whole idea is that once you've identified, oh, there might be a problem with the disk, you know, or disk response times on PAL showing here, then you go into the PerfMon log itself to see, okay, is this really true or not. That's what you're supposed to do at least.

**Richard Campbell:** Right.

**Greg Hughes:** Got you.

**Clint Huffman:** Most people now are just saying, hey, give me a power port.

[Laughter]

**Richard Campbell:** Yeah. The interesting angle on this is diagnosed, this is only step one. What you do about it is another thing entirely and then hopefully after you've done whatever efforts you've done, you reanalyze it to see did I actually make a difference.



## Clint Huffman Does Performance Analysis of Logs!

November 5, 2008

**Clint Huffman:** Oh, absolutely and I'm glad you brought that up because that's another feature of PAL. So I've written tons of performance analysis documentation up on MSDN, TechNet, and blogs and what I found is that, I'll give this information to my customers saying read this information and this will solve your problem and I found out they don't read it.

**Greg Hughes:** Exactly.

[Laughter]

**Clint Huffman:** I got to thinking about it, it's like taking your car to a mechanic and saying, "You know what, my car is broke. Can you fix it?" The mechanic looked at you and says, "Well, here's a huge manual and you can fix it yourself by reading the manual."

**Richard Campbell:** Yeah, knock yourself out.

**Clint Huffman:** Yeah, yeah.

**Greg Hughes:** Not really what they're asking for, right?

**Clint Huffman:** Exactly, exactly. So when I wrote the PAL tool, all the analysis that it does, I wanted them run in a knowledge-based form look and feel to say here's what we're looking at, here's why we're analyzing this particular counter and if you run into this threshold, here is remedies and how to fix this, or next steps on how to accomplish this. So say context full of information, you know, its like I tell you, oh yeah, your carburetor needs to be changed and here's how to do it or I can do it for you.

**Richard Campbell:** Yeah and that's the reality here, is you know, how much do people want to learn and how much do they need to know and what is taken actually, but in most part, people just want these problems to go away. They are not that all interested in exactly how to solve them. If there was a big red button that says this problem goes away, they'd push the button and be happy.

**Clint Huffman:** Exactly.

**Greg Hughes:** The easy button. Right, exactly. The expense of time spent on trying to figure out how to figure out a problem is probably what people are trying to avoid. Just save me some time here so I can spend it there.

**Clint Huffman:** Yeah. Sometimes we have like a huge number of people onsite trying to solve this huge political performance issue and it ends up really something small and they spend all this money trying to figure out why is that.

**Richard Campbell:** I also find people find big chunks of equipment, nothing worse than swapping out a bunch of servers, the old servers are just buried and it performs no better on the new one.

**Greg Hughes:** Right.

**Clint Huffman:** Yup.

**Richard Campbell:** I recently had to diagnose a case where it was exactly the opposite. They were convinced that the database was killing them, that it was painfully slow that they bought a new fancy database server, set the whole thing up, switched over to it and everything was slower.

**Greg Hughes:** Wow.

**Richard Campbell:** Yeah. You know, actually having a clear picture of what the real problem is far harder than we think.

**Greg Hughes:** Right.

**Clint Huffman:** Right and that's why having these reports are so much nicer because now we're basing things on evidence, obviously an educated guess at least versus intuition.

**Richard Campbell:** And also I love the third partiness of this. A lot of these thresholds have been set by experts so I like the fact that PAL will give me a sense of confidence that my servers are running within reasonable thresholds right now or the one that I think is in trouble, the degrees is also in trouble.

**Clint Huffman:** Right. There's one thing I want to make a point as well and I'm glad you brought that up too, its that many of the threshold files like Microsoft Active directory, for example, was written by colleagues on my team like Kip Gumenberg, Matt Reynolds was involved with that and, oh. the Exchange ones are extremely popular, and Mike Lagase and Microsoft support is a big owner of these contents. So I've actually got people who own the contents of each of these different threshold files.

**Richard Campbell:** Right.

**Clint Huffman:** They are the masters of their field. I can't be master of all, right. It's impossible. So I eventually employed these guys and/or gals depending on who's involved with it. They own it and now their names are online and they put some great stuff together...

**Greg Hughes:** That's really cool.



## Clint Huffman Does Performance Analysis of Logs!

November 5, 2008

**Richard Campbell:** Yeah and that's brilliant. I've read Michael Lagase's blog. He is the Exchange Performance god.

**Clint Huffman:** He'll be happy to hear that. David Plus just took over the SQL server stuff. Originally it was written by Kartik Tamhane but David Ploss just took it over and he was awesome at SQL Performance Analysis.

**Richard Campbell:** Great. Where does PowerShell fit into all of these?

**Clint Huffman:** Oh yeah. So I was up in Montreal about two weeks ago and they gave an introductory course on PowerShell. Something cool, I've been wanting to learn about this and the guy they had teaching us was Bruce Payette...

**Richard Campbell:** Oh yeah.

**Clint Huffman:** Who I later found was deadily at PowerShell and like how did they actually get this guy out here.

**Richard Campbell:** That's cool.

**Clint Huffman:** I came to find out that he's from Montreal so I think he has a vested interest in being there of course but it was great, I mean I learned in that one hour than I ever did in probably any other class, other than Vital Signs. Now, I'm like hardcore PowerShell all the way. I've done analysis into it and played with it a little bit. I can do everything made of PowerShell now because right now PAL requires Microsoft LogParser which is a fantastic tool by the way...

**Greg Hughes:** Right.

**Clint Huffman:** Microsoft LogParser is just bringing everything like that. It also requires Office Web Components 11, which is Office 2003 Web Components.

**Richard Campbell:** Right.

**Clint Huffman:** Now, the vendors are free and they create charge for me free, they're quite old so now I'm doing everything in PowerShell this time around.

**Richard Campbell:** So we will see a new version at some point here, all PowerShell.

**Clint Huffman:** Yes, yes. Version 2.0 which I will try to get out probably, I don't know, maybe March of next year or so. I want to do it in pure PowerShell. I've already written some .NET classes that do charting for me so I've got the charting part covered

**Greg Hughes:** Very cool.

**Clint Huffman:** And I've already got some proof of concept stuff working all right.

**Richard Campbell:** Excellent. It sort of reduces the dependencies for PAL to actually be all in PowerShell and use in more .NET resources.

**Clint Huffman:** Correct, correct.

**Greg Hughes:** So what about Hyper-V?

**Clint Huffman:** Oh yeah, yeah. So all of the dependencies of PAL are free by the way so the work on log part is free, it's just a pain to install all of those.

**Richard Campbell:** You've got to get all those bits in, you got to get it to configure it right and its just more moving parts to make the whole thing work.

**Clint Huffman:** Right. So yeah; Hyper-V. One of the things I wanted to mention on this call is that one thing that many people don't know about it is in Hyper-V, the processor analysis was quite tricky. I was actually with the BizTalk product team for a month and we did a whole bunch of analysis. So to make the long story short, we loaded up a whole bunch of BizTalk virtual machines on a physical box and we've drove them up to 100% CPU so we had four virtual processors at 100% CPU. So there I looked at the -- I bring up Task Manager up on the physical host of these machine's operating system, bring up Task Manager, everything is running around one to two percent CPU.

**Richard Campbell:** Wow, that's wacky.

**Clint Huffman:** Yeah, yeah, and so I got thinking to myself, okay, either Hyper-V is the most efficient thing in the world for CPU consumption or I'm doing something wrong. So I talked to Tony Voellm who is the dev performance lead in Hyper-V. He kind of laughs and chats with us and he is like, well, the physical machine is not a physical machine anymore. As far as the host, it's actually called the roof partition and it's just another virtual machine.

**Richard Campbell:** Right.

**Clint Huffman:** And I'm like, "What?" And he's like, "Yeah. It's just another virtual machine." I'm like, "Okay. So then I'll bring RAM from the operating system." He's like, "No, no, no, no. Hyper-V is in the kernel and all these machines including the host are running as virtual computer off of that."



## Clint Huffman Does Performance Analysis of Logs!

November 5, 2008

**Richard Campbell:** So that one particular scene was that actually the CPU being consumed by the host partition or the root partition.

**Clint Huffman:** Correct. Only that machine, exactly; not all the machines as a whole so you're not actually looking at the physical processors when you bring up Task Manager.

**Richard Campbell:** Once you're writing Hyper-V because it goes into that whether they call it ring -1 mode where Hyper-V is above any of the visible processes.

**Clint Huffman:** Yes.

**Richard Campbell:** So then you just have everything in partition.

**Clint Huffman:** And so in order to see the physical processors, you actually have to look Hypervisor counters.

**Richard Campbell:** Ah, because, yeah, that was Hypervisor everywhere.

**Clint Huffman:** Yeah, so if you go on the host machine, you bring up the Hypervisor counters. There's one called the Percent Total Runtime and that's the one that you want to look at.

**Richard Campbell:** Now would you look at that in the context of the host partition, the root partition?

**Clint Huffman:** Yes, yes so you bring up Performance Monitor on the host machine, the root partition machine, bring it up there and then there'll be Hypervisor, Hyper-V processor, I think its Hyper-V logical processor...

**Richard Campbell:** I'm looking at your blog actually, yes, Hypervisor logical processor percentage total runtime.

**Clint Huffman:** Yes, you want to look at that.

**Richard Campbell:** And that's the number that would actually show you how the processors consumed overall.

**Clint Huffman:** Yes, that's the physical processors and their consumption, yes.

**Richard Campbell:** Even though it says logical processors, I love that.

**Clint Huffman:** Yeah, that's the whole thing. You have logical processors, virtual processors, and some other method processors that -- it's really

confusing as to what are you talking about, you know, so then you have sockets and it gets very confusing.

**Richard Campbell:** This is the issue that we run into with PerfMon in general, it's again all the facts are there, we just have to sort them out knowing what each one of these counters actually means in a given configuration. I mean the only time that percentage processor time on a machine means nothing is when you have Hyper-V running so unless you account for Hyper-V, you don't know what that counter actually means.

**Clint Huffman:** Yeah. By the way, PAL now has a Hyper-V threshold file in it in the latest builds.

**Richard Campbell:** Excellent, so now we can actually instrumenting Hyper-V in a rational way but I got to think that all your other counter sets would want to -- or all of your other files would now want to say, hey, am I running Hyper-V because some of these measurements will be different.

**Clint Huffman:** Right. Well, I kind of assume you are -- if you pick the Hyper-V threshold file that I assume you have Hyper-V enabled...

**Richard Campbell:** Yes. I'm thinking if I'm using the Exchange file, the measurements for Exchange will be different if it's running in Hyper-V or not.

**Clint Huffman:** Oh, that's true, yeah.

**Richard Campbell:** This just sounds like we have to add more -- it's just an update to the algorithms because this is where your algorithm approach is so compelling, it's now that I can add these issues that says, hey, are we running in Hyper-V, okay, measure the numbers this way versus measuring it that way.

**Clint Huffman:** Right. Actually, there's a actually another thing I've been trying to really encourage Michael Lagase to do is, you know, because you want to measure some of the disk performance definitely where the data stores that in Exchange, then you wouldn't like other drives and so one of the questions I was trying to have him do was question the variable and say what drive letter is the data store on, or what drive letters, and then later on you can use that in your threshold to make it more strict on performance analysis of that drive.

**Richard Campbell:** Right. I think the whole storage subsystem is another issue because of the visibility into it or lack of visibility into it.

**Clint Huffman:** Another thing I want to talk to you guys about too is XPerf. Have you guys heard of it yet?



**Clint Huffman Does Performance Analysis of Logs!**  
**November 5, 2008**

**Richard Campbell:** No.

**Greg Hughes:** Nope.

**Clint Huffman:** Okay. XPerf enhanced is the next generation performance analysis tool. It's been done by the Windows product group. It's been rendered development for about 10 years now and this now have a rather usable version of it now. This thing kicks butt; it's awesome. We can get detailed information about a context switch now.

**Richard Campbell:** Wow.

**Greg Hughes:** Wow.

**Richard Campbell:** That's amazing.

**Clint Huffman:** Yeah. So this thing is part of the Windows 2008 Server Performance Toolkit.

**Greg Hughes:** Okay.

**Clint Huffman:** Maybe just do a search for Windows 2008 Server Performance Toolkit on the internet, you'll find it up on Microsoft -- free download. The problem is it only works on Vista and Windows Server 2008.

**Richard Campbell:** Right.

**Clint Huffman:** But if you're running this tool and have it gather data for any, or you're driving a problem, you run it for gathering time, the driving problem, then have it then produce a report, you won't get a really easy to understand report, you still have to know Windows Architecture so it's kind of like back to PerfMon again.

**Richard Campbell:** Yeah.

**Clint Huffman:** We've got all these great counters, we don't know exactly what we're looking at but it's great information so the next thing I'm going to try for automating is XPerf and this tracing data that's using...

**Richard Campbell:** I'm just poking through the Windows Performance toolkit here; it looks like a very low level tracing ability into the machine.

**Clint Huffman:** Oh, extremely and then you have to try using it internally now for Vista and Windows server 2008. It's just an incredible amount of information.

**Richard Campbell:** Awesome. Well, Clint, I think we're about out of time.

**Clint Huffman:** Well, that was quick.

**Richard Campbell:** Half hour flies by when we're digging into something this cool. Thanks so much for coming onto the show.

**Greg Hughes:** Thanks Clint.

**Clint Huffman:** Oh thanks.

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