IBM Podcast

[MUSIC]

WEN: Welcome to this IBM podcast, the IBM WebSphere SOA appliances for optimizing your SOA. In this podcast, we speak again with Steve Craggs from Lustratus Research on how SOA appliances help optimize security in your SOA project. I'm Ben Wen from IBM. Hello, Steve, welcome back to this podcast, and thank you all for joining us.

CRAGGS: Hello, Ben, and it's good to be back.

WEN: Great. One of the things that we talked about in our first podcast of the series is about the Craggs SOA adoption paradox. Maybe if you could take us through for a few minutes here about that SOA paradox, a set of paradoxes. This will provide a little bit more a frame here, then we can dive into the thing that I'm personally very interested in about, which is security challenges.

CRAGGS: Yes, sure, Ben. So just to recap on the three SOA paradoxes that Lustratus has come up with. This is based upon interaction with a lot of different companies who have gone down the SOA route over the last five or 10 years.

And essentially, there are these three areas which I supposed you might call them tradeoffs, but we quite like to call them paradoxes, where customers need to think hard about what they're going to do when they hit these inhibitors to getting the value that they want to get.

And the first is scale. The problem here is that SOA, to get its real value, it needs to scale. And if it starts repaying back when you've got a lot of SOA use, not just within a department, but also between departments and across the value chain into departments and all over the place.

So that's what SOA wants, but on the other hand, SOA hates scale. It hates it because as soon as you start moving SOA adoption into different departments and perhaps into different companies, then you have to look at, do we have the skills there that we need? Have we got the infrastructure there to make sure that we can deliver that successfully?

And, how do we actually manage fixing problems if something comes up when an application may be running across a whole set of different departments. I mean, there's a whole set of challenges there that really mean that SOA doesn't like scale.

The second paradox is security. And I know we're going to go into that one in more detail, but just at a summary level, SOA needs freedom for it to blossom. And to get that penetration across the enterprise and beyond, you need departments to have the freedom, you need the multiple development teams to have the freedom to use the SOA services, to access and learn to operate with each other's business services.

But SOA security doesn't like at that freedom because that causes issues in terms of, if I'm making a service available, I no longer really know who is using it. It could be being used by a different department, it could be being used in a partner's company.

So that throws all sorts of issues up about the security domain and how comfortable I am with that, and could even open up, if you're not careful, the possibility of somebody getting in and doing things that could actually not only be not what you want, but may actually cause damage. So, you know, be that's the security paradox.

And then the third is cost. A lot of people do SOA because they want to reduce their IT costs. And SOA is very good for that, but you have to be careful, because we certainly found that if you're not careful, you could find SOA increasing costs.

As you deal with the issues of scale and performance and security and management and all those sorts of things, that those can all have an adverse effect on IT costs. So those are what we call the three SOA adoption paradoxes.

WEN: Great. Well, thank you for that overview again. And around security in particular, I know that you've had a chance to talk with clients and customers and practicers around the world.

What are some of the things that you see folks doing, and what do you recommend to mitigate some of the these very important security concerns around SOA, integration and working across not only departments but across partners and across different governance boundaries?

CRAGGS: Well, you know, I think a lot of people...it's not new, security. Everybody knows that security had got to be an issue. But the point with SOA is it often starts in a single department. So it often starts in a very safe environment where everybody knows that it's only Joe down the corridor who is using this I've just built.

And you know, you can make sure that he knows what the security characteristics are with that particular service, and how sensitive it is. And you know, that's all pretty manageable, just the business as usual sort of thing.

But the issue comes when you start spreading out SOA into other departments and into other companies and other locations. And that's where you really have to make sure that you think about your security strategies, that you think about the policies that you want to use, you think about, which services are going to be available to who, and what about the document flows?

If you were, for instance, interoperating with other businesses, you've got to be sure that the documents that you're flowing through your SOA are protected when they go outside the firewall, for example. So these are all issues which have to be managed carefully.

And I think one of the things that we've certainly seen is that there's a great approach of having a single gateway to each, whether it's a department, whether it's a company, the idea of having a gateway where all the SOA traffic flows through.

Now obviously it needs to be robust, and it needs to have enough redundancy to make sure it's no a single point of failure. But the idea of having such a gateway means that there's a place that you can actually do that policing of the flows.

You can do that policing that says, what's coming through here? Who sent this? Do I need to actually make sure whether there's anything dangerous in this package of information that's just come in? Are these people authorized to get at that service? And all those sorts of things. Having a single point of control really does help here.

Now, the normal argument against that is to say, oh, yes, gosh, you don't want that to become a performance bottleneck, do you? But in fact, this is one the places where the idea of having a dedicated appliance has a lot of value. I think people are well aware that we've probably all used firewalls, firewall appliances to protect e-mail and that sort of thing.

And it's the same principle. The idea is if you have an appliance which is a dedicated appliance, it will have the capacity to actually examine traffic, keep an eye on traffic, police traffic, make sure that everything fits in with the corporate security strategy. So I think probably that is one of the key things that people have done, and other than, of course, actually bothering to think about this up front.

My advice to people on the security front would be, think about your security policies when you create new services that are going to be used across the SOA and consider the idea of having some sort of gateway between the different areas of security sensibility, whether that be between individual departments or between the enterprise and partners or whatever, to allow you to do the policing and the checking that you need to do to maintain the right level of security.

WEN: Great. So it sounds like there's two key components to utilizing some of these security architectures. You talked about authentication, "who is." You talked about authorization, "do they have the right to." You talked about protecting the data; usually that implies some type of encryption.

I think you also mentioned validating the data, could be validation through either, like you said before, authorization, authentication, digital signature is another component I think you're employing in there, as well as making sure that the data is actually what you're looking for, that you've cleaned the data or validated the data.

And then taking all of those policies which can be fairly complex, and I think you're also saying here, too, if I can reflect back, there are some performance concerns about having all of these different checks put together in a single control point.

So being able to mitigate that while still having the performance that your users expect implies taking advantage of dedicated hardware appliances to do that. Is that a good characterization of what I think I heard you say?

CRAGGS: Yes, I mean, that is a good characterization, Ben, and I guess I might add the fact that the idea of using an appliance has another implication on the security front, which is, it's quite hard to tamper with an appliance.

You know, you could argue this is all down to internal discipline and making sure that you've got the right people in your organization, but there is no doubt that if you have just a server handling the linkage out to other departments or out to other enterprises, and programmers can quite possibly get at that server, maybe maliciously, maybe accidentally.

And maybe it's human error or maybe it's deliberate. But it is definitely, if you've got software running in a server, almost by definition, that is more..you can tamper with that more easily than you can with a dedicated hardware appliance that may not even give you an environment in which you can tamper. So there's this aspect that says, well, this hardened sort of security gives you an extra level of protection.

But the other thing that I'd add and stress which you did mention but I didn't think necessarily got [INAUDIBLE] stress was this business of the performance aspect. And some of the things you mentioned like encryption and checking the traffic that's going through and examining the data streams, these can be incredibly intense operations. It can put a great strain on a processor or a combination of processors.

And the idea of offloading those into an appliance which might have a more attractive price performance point, for instance, that makes a lot of sense because you're not in danger of slowing down your key business applications because of all this work that happened to be done on the SOA traffic flows.

WEN: Good clarifications. Good points. Definitely, definitely appreciate that in terms of having that hardened profile that a hardware appliance can have as well as a better cost profile which I think also implies sort of the discussion that we'll have in our next of the series here on podcast series with Steve.

So if I could summarize, security is an area of importance where if you aren't careful about implementing your SOA architecture, it can come back to bite you. So think early about security, authentication and authorization, the protection of the data, the validation of the data, making sure that the control point you have is redundant and has the robustness that you need in an overall architecture.

But also, thinking about the level of threat protection, not only from a data and network connectivity standpoint but also from the actual implementation and hardware component, as well as the overall performance as the security policies get implemented and need to be rolled out with partners...

...both within an enterprise and outside the walls of the enterprise, that appliances is provide a component that is very attractive from all of these characteristics as well as the overall TCO and cost perspective. Does that sound about right?

CRAGGS: That sounds fine. Good summary.

WEN: Good. Well, also want to say thanks to everybody for listening in. We'll have Steve back for another round here to talk about the third component of the Craggs SOA paradoxes, cost and TCO, to make sure that you can implement your SOA or continue to implement your SOA projects with the best technologies, the best adoption characteristics. So, thank you again, Steve, for joining us. Thank you for listening. We'll look forward to hearing from you all.

CRAGGS: Thanks, Ben.

IBM Podcast

[MUSIC] [END OF SEGMENT]