Minnesota and Private Cloud. There Goes Today’s Blog

Don MacVittie, 2010-27-09

I had a blog partially written for today when @GeorgeVHulme tweeted this: "WAHOO! Minnesota goes Private Cloud! ". And that changed my thoughts and direction completely. Here's the article George linked to State of Minnesota Signs Historic Cloud Computing Agreement With Microsoft. The fact that it was private cloud and with Microsoft got me to read the article. And it's actually a pretty impressive story for both the state and for Microsoft.

In essence, this takes "private cloud" to a different place than I would have envisioned. They're outsourcing. Yes, there's a line in the sand, beyond which the state has complete control, but they have essentially given Microsoft their infrastructure (the collaboration and email piece of it anyway) and are holding Microsoft accountable for security and software maintenance. That's a pretty solid plan if the admins at the state can manage the applications as they need/desire. There are gray areas that would need to be covered, like what types of threats are user/application threats that Microsoft isn't responsible for, what's the escalation path, etc. But those are no doubt covered in the contract, which we don't have access to.

Microsoft is giving over dedicated space (notice that the article does not say dedicated hardware anywhere in it), and even has committed a datacenter that the cloud will run out of. The price tag must have been pretty high, but Microsoft Exchange admin, IM (ala Microsoft Communicator) admin, and Microsoft Sharepoint admin – the hardware and software maintenance, routing, upgrades, etc part – is expensive too. The state knows what that portion of its budget will cost and can focus on running the apps that the state and its citizens require to get the job done.

I admit to being a bit intrigued. Not just by the concept, but by the actual architectural implementation. Assuming that the access is via some form of SSL VPN, is it to be expected then that when another portion of the state is signed out to a cloud vendor, another VPN connection will be required? That would seem to be… Awkward. But they do reference a dedicated line, so it is possible that there is no "gateway" to the services, but that would seem irresponsible from a security perspective on both parts, so I doubt it. Though lock-down by IP might be possible, that's spoofable, so again, I doubt it.

Microsoft This arrangement has half of the issues that traditional outsourcing does, but I would argue the worst of the issues are taken care of. In a traditional outsourcing arrangement, the fact that your contract decreases in value as time goes on (assuming your vendor is successful anyway) means that your staffing levels are slowly watered down by other duties, and by the end of the contract you are likely frustrated. This is compounded by the fact that your IT needs grow in the two to five year period of an outsourcing contract.

But in this case, the labor intensive part of the agreement resides with state employees. Upgrading hardware and software is labor intensive but "bursty" to put it in IT terms. You do it, and then it's done until next time you need it. On the other hand, maintenance of users, modifying software configurations to meet your needs, and managing that software is a constant job that will likely increase over time.

This may be the answer outsourcing has been looking for. To me, having Microsoft employees apply their own security patches sounds like right-sizing. Of course there will be speed bumps, but even that has a pressure release valve. If a server drops for no explainable reason, state IT staff will point to Microsoft, but be quietly glad that they have someone to point at.

Depending upon the agreed-upon price, states with much larger budget woes than Minnesota should probably be considering such an arrangement. Instead of a hazy partial budget that is padded in case Exchange use grows at a faster-than-expected pace, they can have a number that is required to keep the lights on for critical state systems. It cleans up budgeting and allows the state to make critical choices in hard times without as much guesswork. Capital expenditures drop, ostensibly staffing needs will go down, but that greatly depends upon the number of servers this system replaces and what their server:admin ratio is.

And I'm really intrigued by the implication that Microsoft, just by virtue of taking over this function, increases the security of Minnesota's data. I know that Microsoft has been getting better over the last decade at security, but that is still an intriguing concept to me. Hope my boss (who lives in Minnesota) doesn't notice it…

By way of disclosure, we are a Microsoft Partner, not that being one had anything to do with this blog, just making sure you know.


F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com