

How to integrate cloud services management into your IT operations
David Strom, david@strom.com
December 2011 (this is the basis for a webinar given on MSPtv.net)

Getting started with a cloud-based service is relatively easy, and a number of webcasts and white papers from Zenith already describe that process in detail. But what is more difficult is how you can better use these cloud services and make them a part of your overall IT operations. In this paper and the accompanying webcast, we look at ways that you can better govern your cloud deployments and make use of the best practices of IT that you use for your own servers. We'll look at three specific areas: how to secure your virtual machines, how to keep track of costs of your virtual infrastructure, and how to automate various actions. We'll also introduce you to what Zenith has in the cloud computing space as well.

Securing your virtual machines

If you would ask most IT professionals on whether they have practices and procedures for securing their physical servers, you would probably get solid affirmative answers. Over the years, the collection of firewalls, intrusion prevention appliances, authentication servers, and other network equipment has been perfected and tuned to make this kind of security plentiful and powerful. But the same isn't true when it comes to securing servers in the cloud, where for many it is still the wild west.

While few attacks have been observed on virtual machines (VMs) directly, it is still good security practice to protect them and a growing concern particularly as more servers move to VMs. However, the protective vendors have been slow to provide these features in the virtual world. As the number of VMs increase in the data center, it becomes harder to account for, manage and protect them. Physical firewalls aren't designed to inspect and filter the vast amount of traffic originating from a hypervisor running ten virtualized servers, for example. And because VMs can start, stop, and move from hypervisor to hypervisor at the click of a button, protective features have to be able to handle these movements and activities with ease.

Part of the problem is that we assume the cloud provider handles security of our collection of VMs that live inside their data centers. Nothing could be further from the truth.

Just as in the physical world, security is a multi-pronged approach in the virtual world as well. You need basic **anti-virus/anti-malware protection** just like any desktop or server receives across your enterprise; **access controls** so that a random employee can't bring down your entire virtual infrastructure; **firewalls and intrusion prevention** products to keep network-based attackers out; and **auditing and compliance** tools to make sure your security is up to snuff. That is a lot of gear to handle, and all of it has to come cloud-aware otherwise it won't be much use.

Another part of the problem is that the current products available only protect different parts of your virtual infrastructure, so they are not directly comparable. You will have to buy multiple security technologies from multiple vendors as your cloud footprint increases and as you virtualize more of your IT infrastructure.

Let's look at some typical products that are available for securing your cloud resources.

Reflex' Virtual Management Center is the most comprehensive security solution, with modules in three broad areas (auditing/compliance, firewall/intrusion detection, and access controls). The product is actually four separate protective modules that are knit together with separate reporting and management consoles:

- **vTrust** for virtual firewall protection,
- **vCapacity** for capacity management,
- **vWatch** which handles performance and resource monitoring and
- **vProfile** for configuration management

Trend Micro purchased Third Brigade last year and has incorporated its features into its **Deep Security** product. The product has a variety of protective modules, including agent or agentless firewall/IDS, anti-malware, and web application protection. As you might suspect from a consumer software company, its Web management interface is very attractive and the dashboard has a lot going on. At a glance you can see your entire VM collection, whether any protective measures have been installed, and what alerts have been reported. You have to use the maps generated by VMware to see a visual picture of your network of VMs and their hosts.

Finally, there is **Dome9.com**, which is trying to make the cloud more secure by providing an automated service to centralize and consolidate security management across both private and public clouds and in and outside of your data center, including VMs residing on Rackspace, Amazon's EC2 and GoGrid. They will manage all of your Window and Linux servers' existing built-in firewalls. The product uses either agents or talks directly to VMware and other cloud provider APIs to automate secure access. For example, you can open and close RDP ports on a timed schedule to make sure that someone didn't inadvertently leave them open when they were done with a remote connection. They can also close ports without locking out legitimate server admins who need to get in on an as-needed basis without having to bother the overall security administrator to temporarily grant this access. You can see their central console below:

Welcome to Dome9 Security Management Service

We are happy to welcome you to Dome9 security management service! You're now ready to start securing your servers. Installing and using Dome9 is easy and fast. Select from the options below which security service you'd like to start with:



Manage Server Security & Firewall

Start managing your servers' security policies the right way! Quickly installs on any cloud, VPS or dedicated server.

[Install Dome9 Agent](#)

Supported OS
 Windows Server - 2008 R2, 2008, 2003 & Windows 7
 Linux - CentOS | RHEL
 Linux - Ubuntu | Debian - **Just arrived!**



Manage AWS EC2 Security Groups

Start managing EC2 Security Groups the right way! No Agent installation necessary. All security policy management actions are preformed through the AWS EC2 API interface.

[Add AWS Account](#)

Dome9 AWS integration doesn't require installing Dome9 Agents on your EC2 instances. We utilize the built-in EC2 Security Groups to manage and automate your security policy.

[How do we secure your API key?](#)

All rights reserved, Dome9 Security © 2011 | [Support forum](#)

Automating common procedures

Now let's turn to another aspect of cloud services. While VMs are so easy to start and stop, the hard part is having a series of automated procedures that allow you to control them and match the cloud resources with your particular demands. There are numerous "orchestration" tools that do this and let's look at how several of these operate.

You can think of **ScaleXtreme** as offering middleware for cloud management. They have developed a robust offering, complete with its own app store with several dozen add-ons< such as apps to install everything from a Java JDK to a full LAMP stack on a cloud-based Linux server.

The service can handle complex provisioning such as dynamic machine groupings, and works with OpenStack, VMware's vCloud Director, AWS and Rackspace. You can browse individual VM file systems, copy files among VMs, monitor each VM, and more. Everything can be run across multiple private and public clouds, and all of this functionality is cloud-based with no software to install other than your browser and some agents to manage your servers.

Next is **CumuLogic** which is a Java Platform-as-a-Service (PaaS) software provider, This helps enterprises, cloud providers and ISVs to build and manage Java PaaS in public, private and hybrid cloud environments. The product is based on a cloud application management platform, and includes cloud services automation,

autoscaling, monitoring, policy-based workload deployment resource management and user management. The idea is to mix and match different cloud-based applications, no matter where they reside.

The service will include a cloud services catalog of various infrastructure elements that are available as part of the management framework. Initially, it will support Amazon Web Services, Cloud.com, Eucalyptus Systems, Openstack and on-premises VMware vSphere installations.

The product also includes features such as policy-based workload deployment and the ability to mix-and-match infrastructure software which enables the deployment of modern applications, as well as consolidation of legacy Java applications to a single platform, substantially lowering the cost of managing various infrastructure assets.

Cloud provider **Skytap** has two interesting twists on their offerings. First is a cloud orchestration interface to stage which particular VMs are started and in a particular sequence. As our clouds become full of virtual servers, we need these tools so that your database server starts after your directory server, for example. There are rules for both startup and shutdown sequences, along with scheduling operations of particular VMs. While there are very expensive cloud orchestration tools from IBM, Novell, CA and the like, this is a great idea for Skytap and a way to differentiate their service from the dozens of competitors.

The second piece is being able to connect different virtual networks to each other within your particular account. Again, this is accomplished with just a few simple keystrokes. Other hosting providers make these connections difficult or impossible, although you can create a single network that connects a group of machines together in most services. So one could have an entire testing network and connect it with a different server to see if the test falls over or continues to run. The screenshot below shows you how easy this is to accomplish – just with a few mouse clicks. You don't need to stop any of your running VMs and reconfigure their network settings, everything happens on the fly and is instantly active.

HotLink SuperVisor provides system management of heterogeneous virtual computing and supports all major hypervisors including VMware vSphere, Microsoft Hyper-V, Citrix XenServer and Red Hat Enterprise Linux. What this means is that you can choose your management console, such as vCenter, and have it manage multiple hypervisors (other than VMware) using the glue that Hotlink provides to connect the two. Your VMs are still running on the original hypervisors, but you can manage everything from one console. You can also migrate your VMs to other hypervisors too if you so desire.

Nimbula Director provides for managing multiple kinds of cloud environments and hypervisors and on and off premises. It offers secure multitenancy, cloud orchestration and metering and monitoring. They are able to support a

geographically distributed cloud and presenting a single login and a single view of the entire virtual infrastructure.

CA's Service Operations Insight can visualize and analyze an entire infrastructure, including both cloud and physical applications and transactions together, in the context of the business services they support. It correlates and analyzes information from infrastructure, application performance and other IT management tools in real time. This information is used to map and display IT assets that deliver specific business services, calculate service quality, and identify which IT assets impact service quality and put it at risk. The idea is to model an end-to-end and real-time view of services across the enterprise. It can automate actions that re-allocate data center and cloud resources to quickly fix service problems. "Impact analysis from CA Service Operations Insight allows for quick problem identification, notification and automated help desk ticketing, so service quality problems can be quickly resolved and other risks to business services can be mitigated," says Dan Colleli, a monitoring technician with Raymond James and a CA Insight customer. All this insight doesn't come cheap: a site license for CA Service Operations Insight starts at \$175,000 for up to five data sources.

Finally, there is **Tier 3's Environment Engine** that can help the automation of various Microsoft and Linux server deployments. Each deployment can be configured to be private, shared publically or limited sharing to specific individuals. You can add multiple VMs so that an entire Web app can be brought up with a single command, even though it is deployed across multiple Web, database, and app servers on different VMs. You can script out an entire installation, adding monitoring, backups, firewall rule sets – in short, you can replicate in the cloud your entire computing environment.

Blueprint Designer

The screenshot displays the 'Blueprint Designer' interface. On the left, a dark sidebar contains a navigation menu with four items: '1 Blueprint Info', '2 Servers' (highlighted with a '3' in a grey box), '3 Scripts & Execution', and '4 Review'. Above the menu, a black box shows 'estimated cost as configured' as '\$1,321.92 per month'. A blue button labeled 'Submit For Publishing' is positioned below the cost information.

The main content area is titled 'Servers' and includes the instruction 'Add and configure each server for the blueprint.' Below this, there is a '+ add server' button. Three server configurations are shown in a grid:

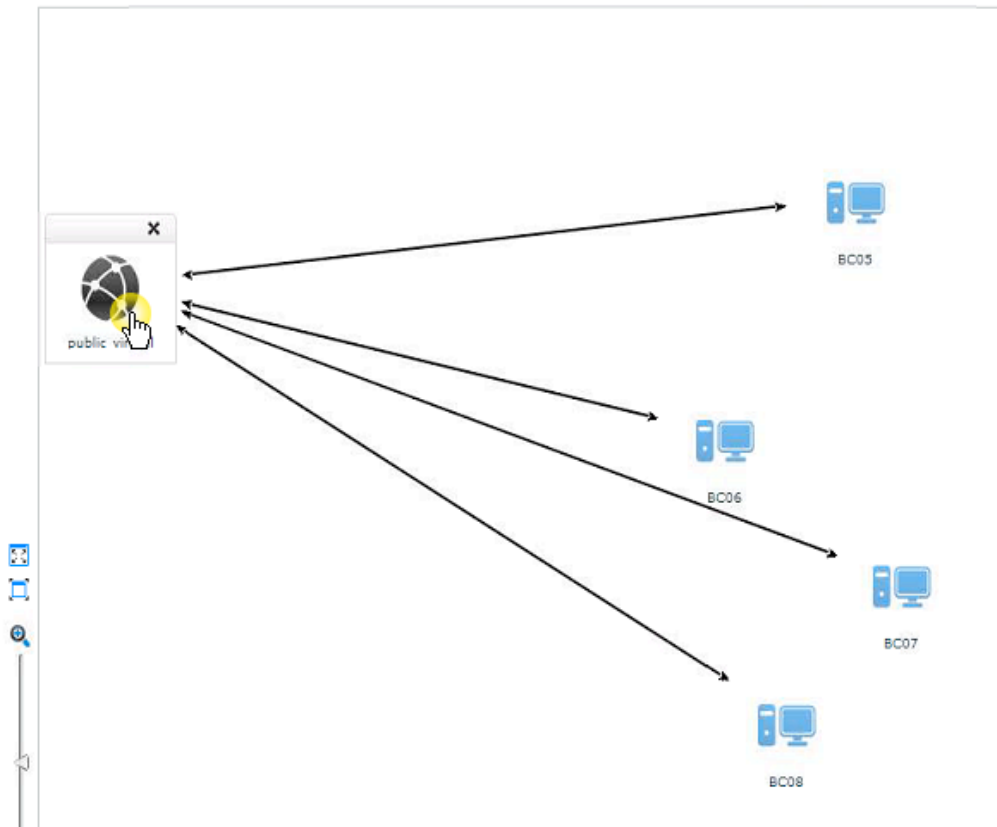
- ...AD**: 1 processor, 2GB memory, 0GB storage. Includes icons for a gear (x1), a folder (x0), and a document (x1).
- ...SQL**: 2 processors, 4GB memory, 0GB storage. Includes icons for a gear (x1), a folder (x1), and a document (x1).
- ...WEB**: 2 processors, 4GB memory, 0GB storage. Includes icons for a gear (x1), a folder (x0), and a document (x2). A red 'x' icon is in the top right corner of this card.

Below the grid is a dashed box with a '+ Add Server' button. At the bottom of the main area is a blue button labeled 'Next: Scripts and Execution' with a right-pointing arrow.

Zenith SmartStyle offerings

Zenith has its own cloud-computing offering called SmartStyle that is based on Oracle's Virtual Box.

You can set up a variety of subnets and connect different VMs to each one, as well as create logical groups of VMs to assemble complete virtual datacenters, in much the same way that Skytap offers. You can also set up a series of commands for particular collections of VMs so you don't have to start up each VM individually, for example. And you can see a map of which VMs are connected together as you can see below.



You can add both virtual desktops and servers, and easily clone existing VM configurations too. There are separate production and maintenance environments so you can set up and experiment with test machines before rolling out into production. You can also optionally register the entire domain so that the Zenith network operations center can monitor all the VMs in the domain for you or your customers.

Keeping track of costs

Yes, we all know that cloud computing can be cheaper than paying for setting up and running your own server. But the dirty little secret is that comparison shopping can be a bear, akin to trying to get that "final number" from your local car dealer. The reason is because almost everything in the cloud is priced a la carte. Some cloud providers don't have pricing available until you sign up for their service.

And therein lies the challenge for an IT manager who wants to try to find the best-priced cloud: you have to read the fine print, and make sure you understand what is billable and when the meter starts – and stops – running.

Every one of the major public cloud providers has pricing so complex that they have devoted an entire Web page to calculating what those costs are. Here is the Amazon calculator for example:

<http://calculator.s3.amazonaws.com/calc5.html>

Here is Rackspace's calculator:

http://www.rackspace.com/cloud/cloud_hosting_products/servers/pricing/

GoGrid offers a slightly different pricing scheme, called "RAM-hours" meaning the amount of RAM per server you have deployed multiplied by the number of hours that it is running. Each of its pricing plans includes a fixed number of RAM-hours, if you go over that amount, you get charged for the overage. They have their own calculator here to estimate your bill here:

<http://www.gogrid.com/cloud-hosting/cloud-hosting-pricing-calculator.php>

The second challenge for cloud pricing comparisons: things change, and they change quite often and without much notice. So just because you went to a particular Web site and got one quote today doesn't mean that the vendor won't adjust things tomorrow and render all your research obsolete. Amazon is fond of actually reducing its prices quite frequently as it buys new and cheaper equipment, for example.

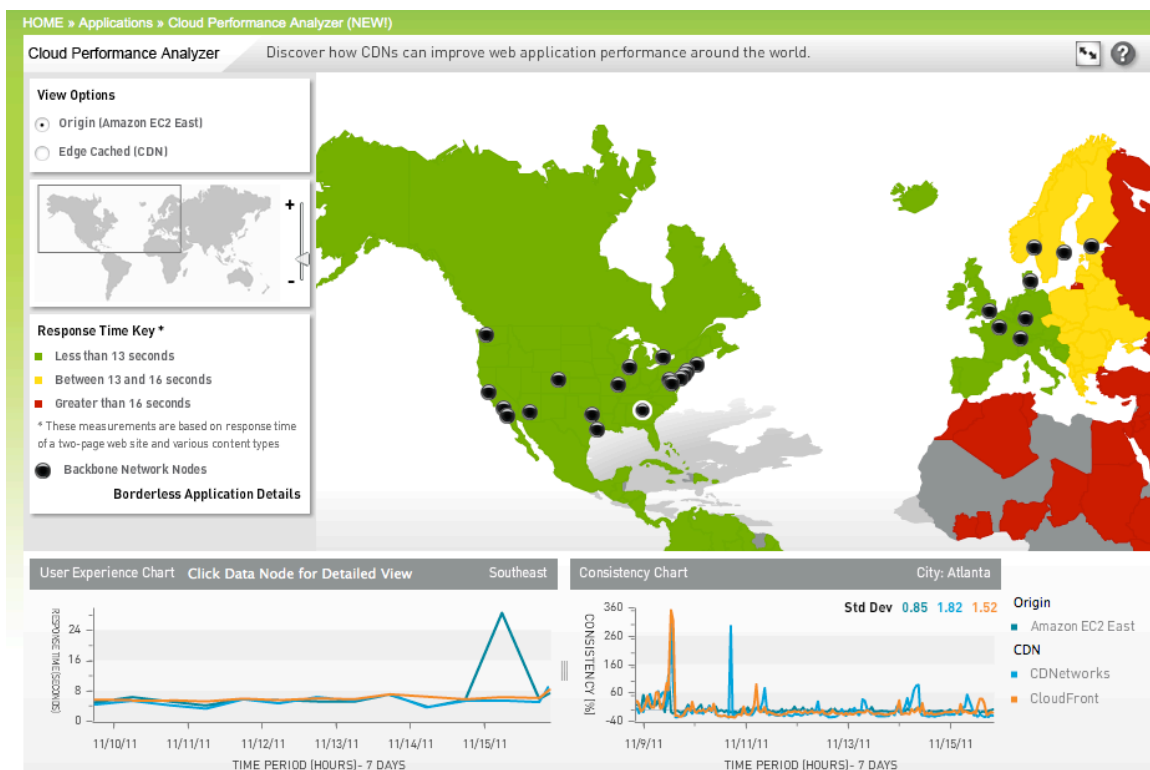
The third issue is make sure you understand whether you are being billed for VMs that are only up and running, or all the time. Verizon's Computing as a Service SMB offering charges for all of its VMs whether or not they are actually turned on and running. If you just want to set up a test VM environment and try out a few things, and then turn it off, you would be better to use Amazon or someone else that doesn't continue charging you.

Fourth, what is the surcharge for particular OS instances? Each cloud vendor has a different way to handle passing the cost of its licenses on to you – the best deal is Cloudshare, which doesn't have any surcharge. There are many other factors to consider, including 24x7 live support and the various remote access plans offered by each vendor.

This complexity has brought with it a new class of products that attempt to predict your consumption of cloud resources and there are various tools that are now around that help you compare these costs. Here is a selection of products.

- **Zenoss** offers a variety of cloud monitoring and costing products.
- Uptime Software has its **Uptime Cloud** that will show you the current costs of all your running instances, as well as make recommendations for how to save money by changing your cloud configuration. Right now it just works with Amazon but more services are planned.

- **Cloud Cruiser** is another tool that is available for both private and public cloud environments.
- **Cloudability** has a variety of tools available that including costing and monitoring and you can set up a free trial account to try them all out.
- vKernel provides a free capacity planning tool called **Capacity View**. The tool is Windows-only and connects to your vCenter or ESX server and quickly gives you a lay of your virtual landscape. While much of this information is available through various VMware consoles and displays, it is nice to have everything consolidated into a single dashboard.
- **CloudHarmony** is yet another site that you can benchmark particular performance metrics for dozens of different cloud providers. You can actually run your own real-time tests too.
- **Cloudsizer.com** is another tool that has more than a dozen different cloud providers that can you track costs.
- **Cloudsleuth.net** is a great service that can keep track of uptime at various public cloud providers. Here is a sample map showing you this status:



Summary

As you can see, the number of individual products and services that are available to handle cloud computing is a huge space, and only growing as the importance of the cloud picks up for many IT managers. As a MSP, it is your responsibility to try out some of these services and provide solid recommendations for your customers, and to educate them on the various features that are available.

While we have tried to show what each of these tools is about with some illustrated screen captures, you might want to tune in to the associated webcast where we will explore each tool in more depth.