TOP 10 TIPS FOR VMWARE NSX SUCCESS IN A PRIVATE CLOUD

Reporting from the trenches

As a Senior Technical Account Specialist (TAS) specializing in VMware NSX, over the years I've seen a lot of NSX-based private cloud implementations. With that experience in mind, I'd like to share some tips for making your NSX implementations as effective as possible. I have three main categories of recommendations:

- Start with People
- Plan for Deployment
- Tidy Up your Operations.

Start with People

Tip #1: Establish a dedicated cloud team

Your cloud team should include individuals with strengths distributed across virtualization/hosting, storage, networking, security, and automation. Borrowing people from each of these functional areas—rather than creating a team of dedicated members—doesn't work. Creating a dedicated, cross-disciplinary cloud team lets you:

- Sustain cloud effectiveness
- Reduce the time to market of new services
- Authoritatively pitch your private cloud to internal customers

A team made up of part-timers creates delays because action items constantly bounce between teams. Plus, your cloud team members' first priority will always be their core team, not the cloud; you will rarely get their full attention.

Tip #2: Build T-shaped expertise

Choose people for your cloud team who have deep expertise in one area (virtualization/hosting, storage, networking, security, or automation). Then, encourage them to acquire build an understanding of their non-specialty areas. A networking team member, for example, doesn't need to also become a vSphere administrator. But without a solid grounding in virtualization, they won't be able to contribute to decisions as constructively.

Tip #3: Embrace different

Private clouds (with their underlying microservices and containers) are a new design, a new way of doing things. Trying to replicate your current environment—from a security, networking, or server perspective – in your new software-defined environment will bake in limitations. Inevitably, you will have to start over. So, don't be afraid of different. Different is the way forward!

Tip #4: Start learning about microservices and containers

Everyone on your cloud team needs to become fluent in the use of microservices and containers. Deploying new apps and converting existing infrastructure using microservices will be a big part of their day. And it can get complicated. On the infrastructure side, for example, there are a number of containers types—Pivotal, Kubernetes, and Docker, to name just a few. And there are multiple tools for using them.

Ben is an experienced NSX and private cloud specialist, having spent over 15 years working with several companies in the data networking industry. As an NSX Technical Account Specialist (TAS) at VMware Ben has collaborated on deploying multiple software-defined data centers at Fortune 100 companies across several industries. Prior to joining VMware, he was a Director of Network Engineering and Security for an enterprise retail organization.

BEN BOWMAN
VCIX-NV
SENIOR TECHNICAL ACCOUNT SPECIALIST (TAS) – NSX

PEOPLE

1. Establish a dedicated cloud team
2. Build T-shaped expertise
3. Embrace different
4. Start learning about microservices and containers

PLAN FOR DEPLOYMENT

5. Start segmentation with one application
6. Build networks per application
7. Check and recheck infrastructure connectivity

TIDY UP YOUR OPERATIONS

8. Make sure someone has access to everything
9. Check firmware and drivers at the host level
10. Get your logs right

Microservices and containers are fundamental to almost everything a cloud team does, and they're a new to most people. Invest in developing these skillsets.

Plan for Deployment (of a Software-defined Network)

Tip #5: Start segmentation with one application

Don't try to boil the ocean. Don't bite off more than you can chew. Don't try to do everything at once. You get the idea. But DO choose a mission-critical app to start with. Otherwise, it's too hard to get the much-needed attention of management and business owners. (And your success will go unnoticed!)

Tip #6: Build networks per application

Moving your existing network infrastructure design—where multiple applications share a network—into a software-defined environment will severely limit private cloud effectiveness. This is especially true for disaster recovery and security, where the traditional networking approach makes it difficult to manage the mobility of applications to and from a public cloud.

In a cloud-based design, you want to failover specific apps, not entire networks. So, create network subnets for each application, for each geographic region, for any unit of measure that you want to be able to failover.

Tip #7: Check and recheck infrastructure connectivity

Make sure all the critical components can talk to each other. Private clouds give you a lot of flexibility regarding where you deploy things. But if relationships change or you didn't notice that this piece can't talk to that piece—it can be a show stopper.

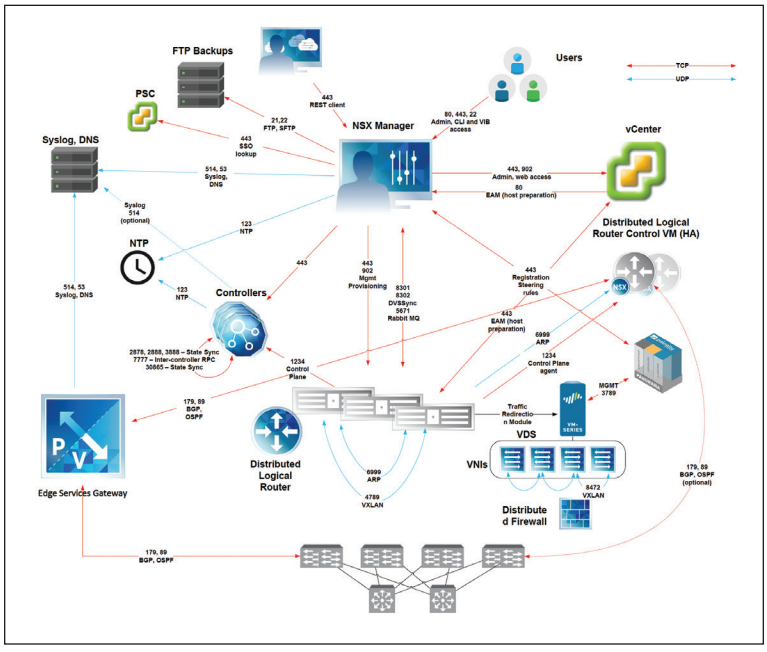

Figure 1. NSX Communications

Tidy Up Your Operations

Tip #8: Make sure someone has access to everything

In traditional environments, networking, storage, hosts, etc. are typically subdivided and no one person needs access to everything. Things are different with a private cloud, where infrastructure elements routinely cross multiple towers. Assign access to NSX Manager, ESXi hosts, syslogs, and the network infrastructure to one or more persons.

Tip #9: Check firmware and drivers at the host level

VMware technology is hardware agnostic. But, it's important that each piece of hardware have the latest firmware and drivers in place. Discrepancies creep when you least expect it. Say you buy five new blades off the shelf, and the first three put into service are all up to date. No need to check the last two, right? Wrong. Therein lies the road to regret. Be thorough. Check everything.

Tip #10: Get your logs right

Distributed firewall (DFW) syslogs come from the ESXi host. NSX health logs come from the NSX Manager. But in production, it's common for the logging servers to be separate from all the hardware firewalls. The NSX and firewall teams both need access to all these logs.

Know where the log messages are going. Grant access or replicate them on accessible servers. They're essential for troubleshooting, so everybody needs to see them. Of course, that's doubly true for your networking and security teams.

The devil's in the details

Success with NSX often comes down to getting the little things right. Train your people, cover your deployment bases, and mind your operational Ps and Qs.

Let us know if you'd like more specifics regarding the VMware NSX TAS service and the long term assistance we can provide, helping you drive more business value from your NSX implementations.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com