Improve Existing Disaster Recovery Solutions with VMware NSX

Kevin Reed
Sr Manager, VMware
Federal Networking & Security Team
kreed@vmware.com
703.307.3253

Don Poorman
Manager – Solutions Enginering
Govplace
dpoorman@govplace.com
301.678.3667

GOVPLACE

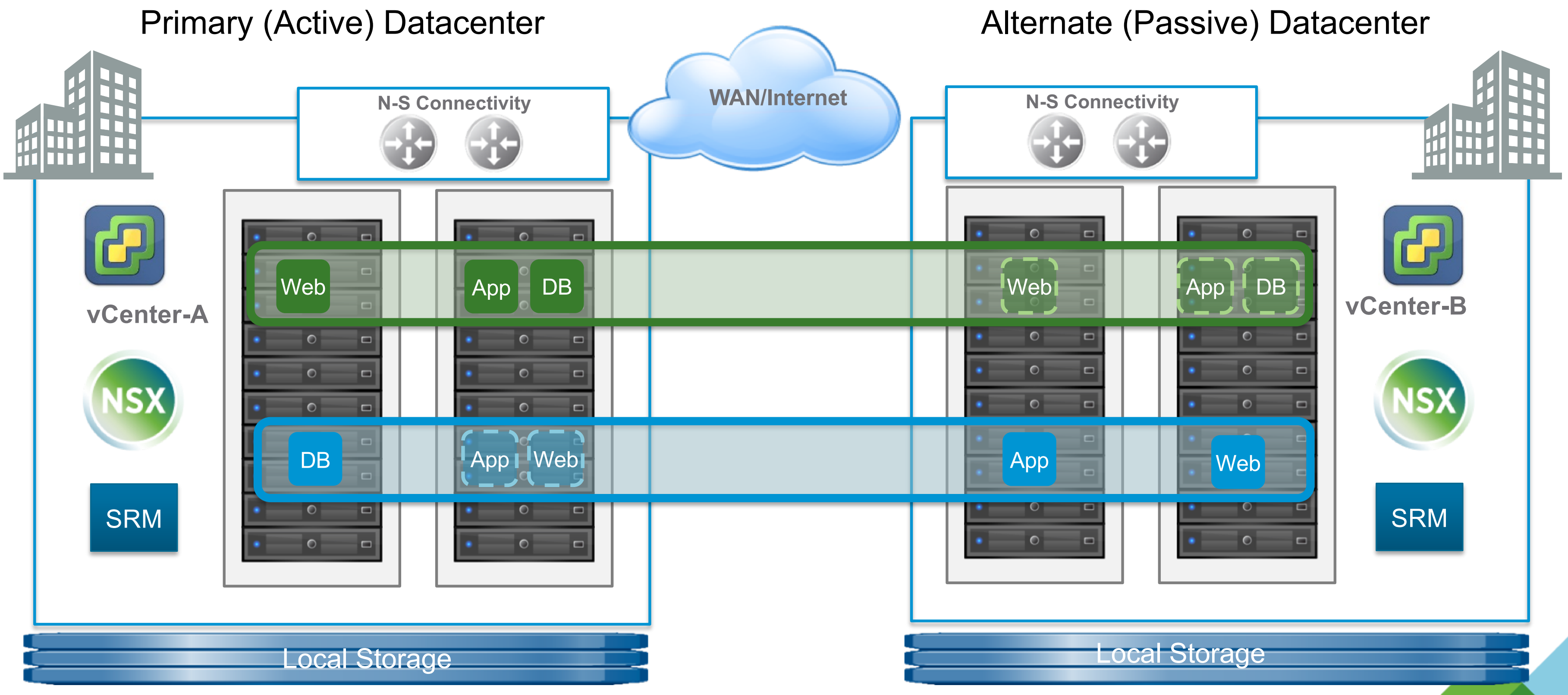
vmware®

Revisiting Disaster Recovery

…everybody’s FAVORITE topic!

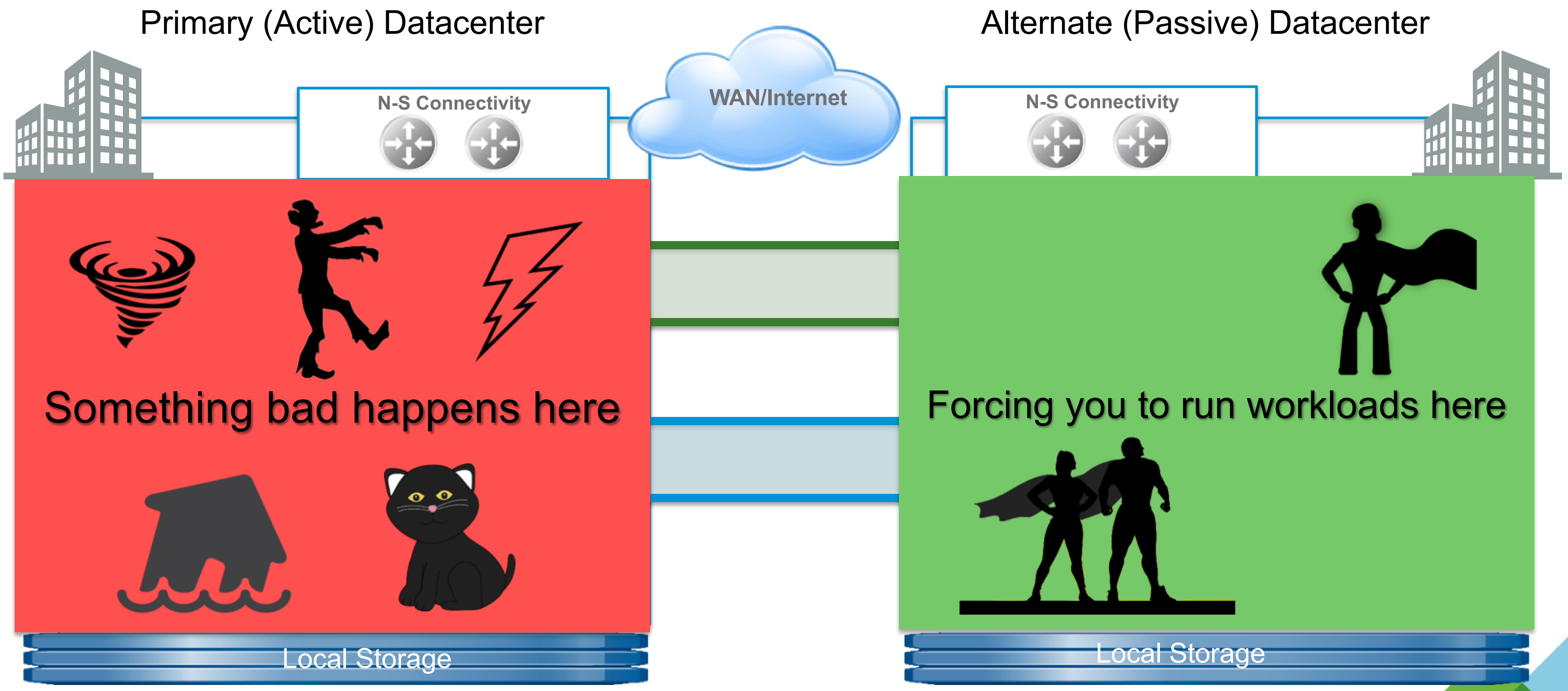
What is Disaster Recovery & Business Continuity?

…at least for the purposes of this webinar?



What is Disaster Recovery & Business Continuity?

…at least for the purposes of this webinar?


Primary (Active) Datacenter
Alternate (Passive) Datacenter
N-S Connectivity
WAN/Internet
N-S Connectivity
Something bad happens here
Forcing you to run workloads here
Local Storage
Local Storage

Traditional Workflow for Virtual Workload Failovers

- Get called at 2:32 AM
- Diagnose outage – begin executing runbook for site failover and reach for lucky horseshoe keychain.
- Get halfway through powering up recovery VMs and realize ALL of their network settings are configured for the PRIMARY datacenter subnets. Grumble and add changing IP addresses to the list of things to do.
- Get halfway through reconfiguring recovery VM IP addresses before realizing your DNS entries are all pointing at the PRIMARY datacenter subnets. Bang head on table and plan to script those changes in future failover tests.
- Finish networking reconfiguration and application consistency checks just as Primary site comes back online.

Always Remember…

It has, and always will be, about workload SLA.

Application Continuity

Traditional Challenges for DR Solutions

- Change application IP addresses
- Re-create/Re-configure physical network for L2-L3 connectivity requirements
- Re-create security policies
- Update other physical device configuration Ex: load balancer
- Additional update/re-configuration (ACLs, DNS, Application IP Dependencies, etc.)

Traditional Solutions::

Ex:

- L2 Over Dark Fiber
- VPLS Over MPLS Back Bone
- Hardware-Based Solution (OTV)

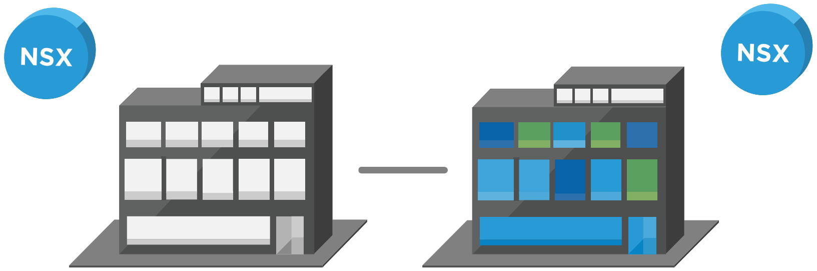
Expensive, hardware-based, complex, operationally challenging, and/or long lead times required

Not holistic solutions – only focused on the network and per-device configuration and lack automation and flexibility

NSX Networking and Security for DR Solutions

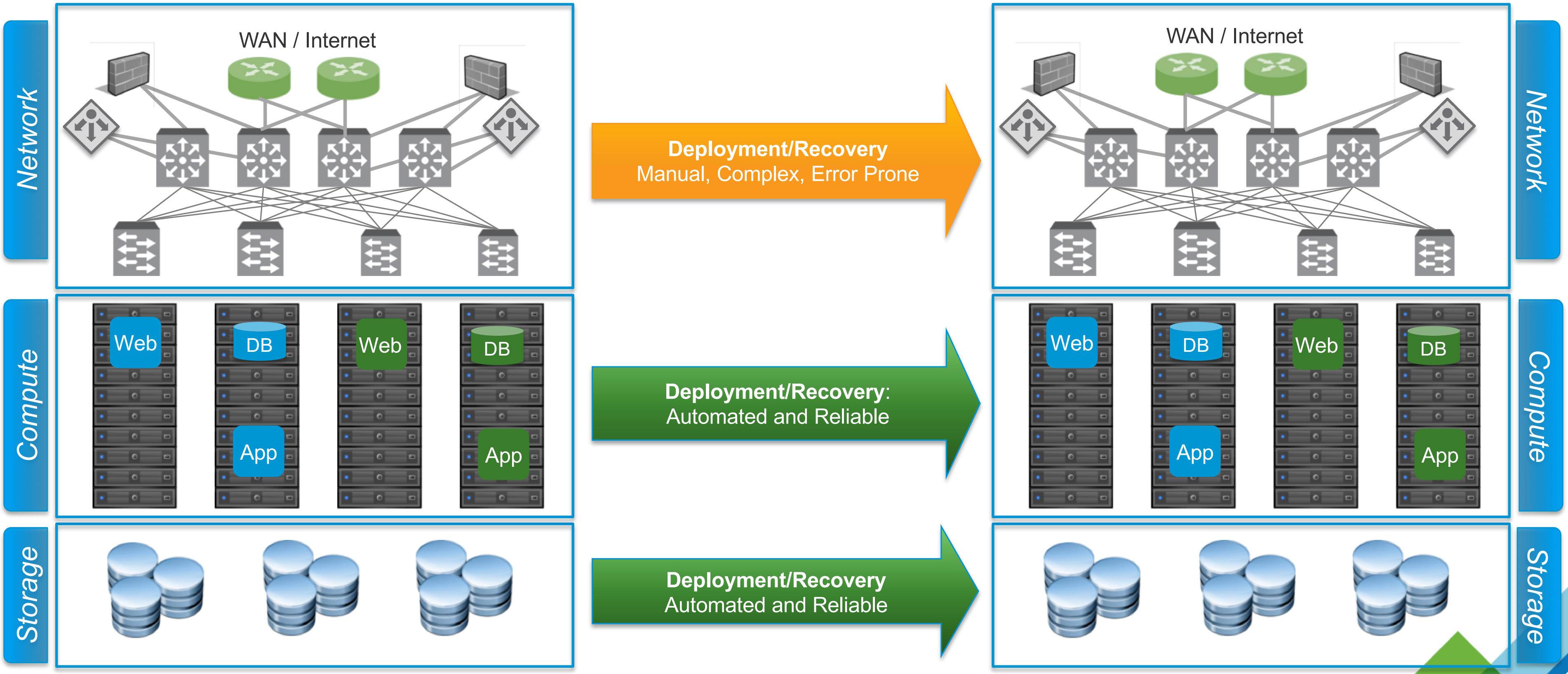
What's needed is a software based approach which can provide:

- Decoupling from physical hardware
- Ease of deployment
- Ease of use
- Better security with micro-segmentation
- Leverage higher-level security constructs
- Flexibility
- High degree of automation
- Rapid deployment/recovery and productivity
- Ease of testing DR Plan
- Extensive partner ecosystem for services
- Integration with other DR & SDDC components (SRM, vSphere hypervisor, vRealize Suite, etc.)



Traditional Disaster Recovery: Manual, Unreliable, Complex

Infrastructure Challenges: Compute, Networking and Storage



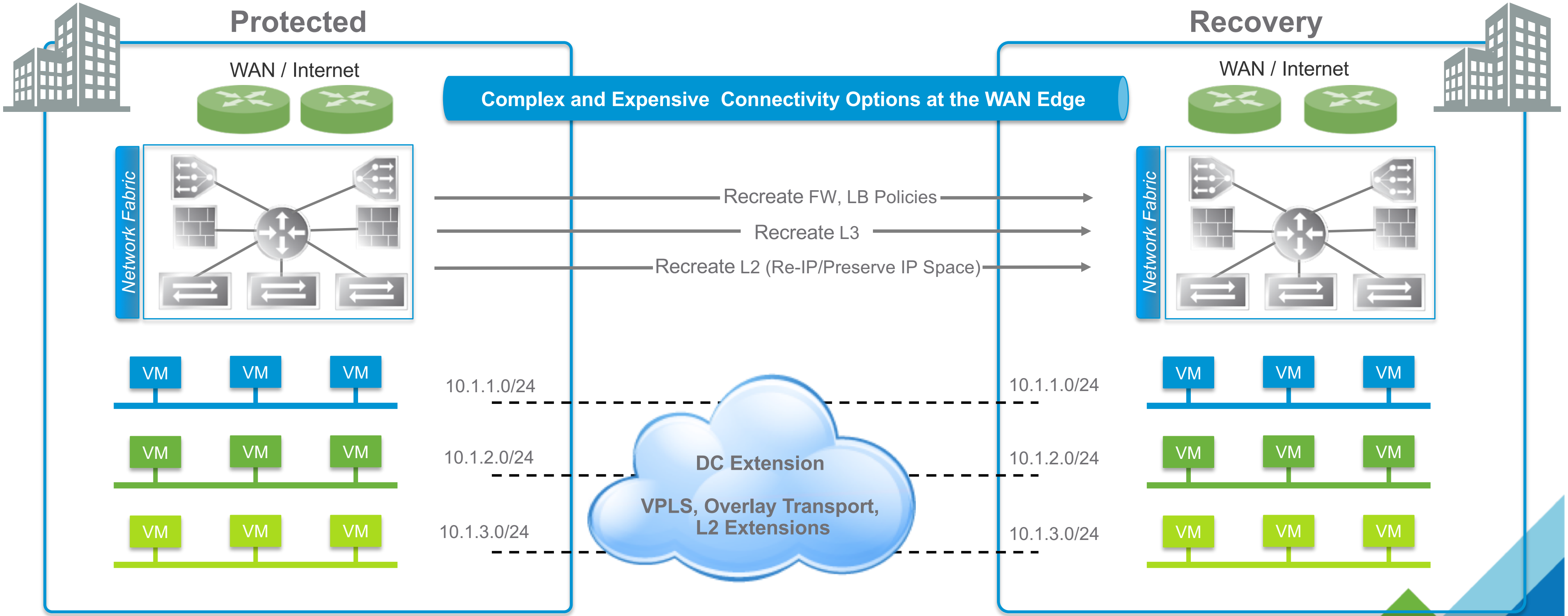
Deployment/Recovery
Manual, Complex, Error Prone

Deployment/Recovery:
Automated and Reliable

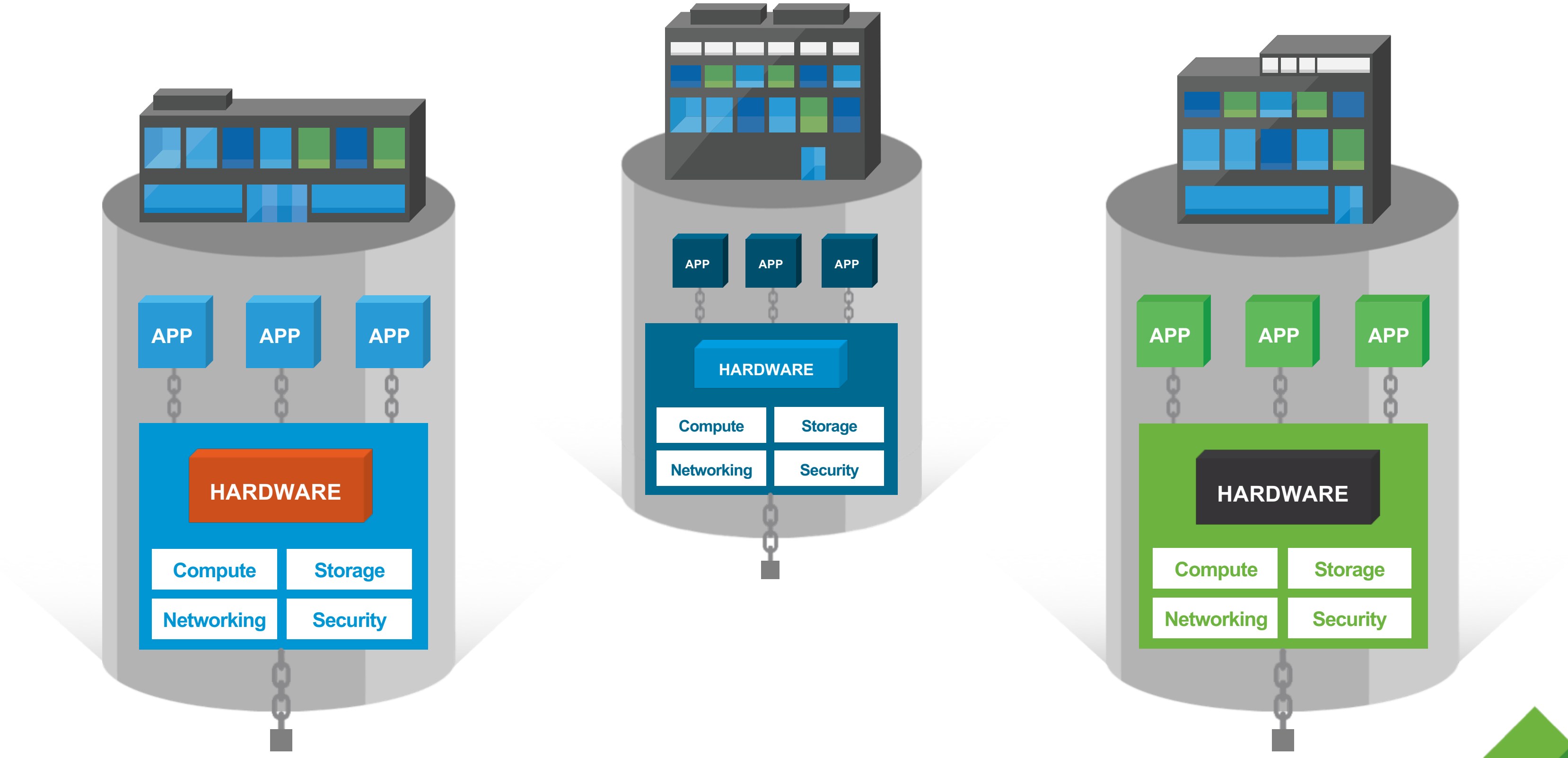
Deployment/Recovery
Automated and Reliable

Traditional Disaster Recovery: Requires L2 Extension

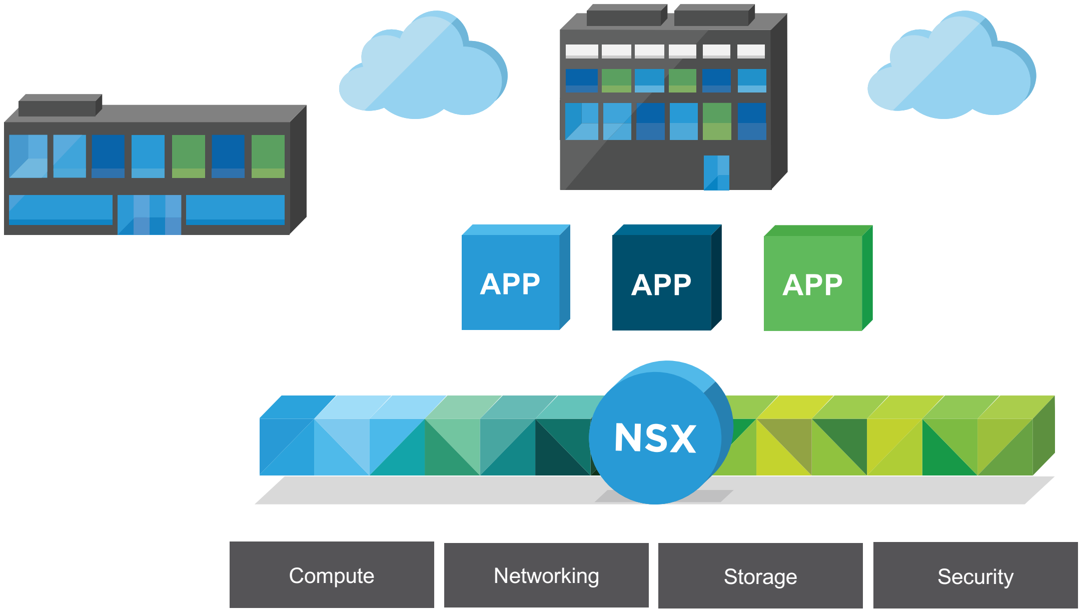
Infrastructure Challenges: Site Connectivity



The Solution: VMware NSX



The Solution: VMware NSX



APP

APP

APP

NSX

Compute

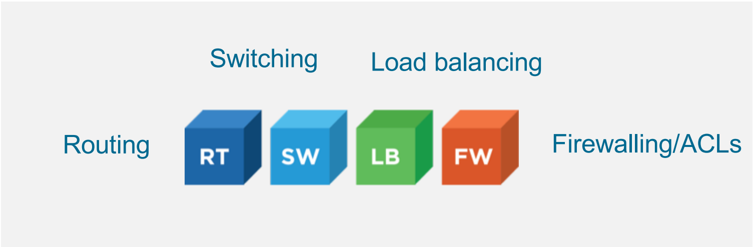
Networking

Storage

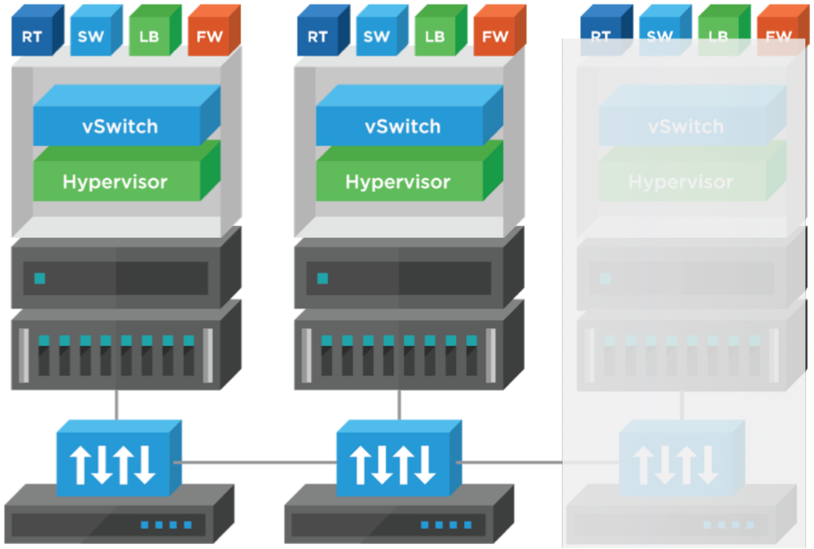
Security

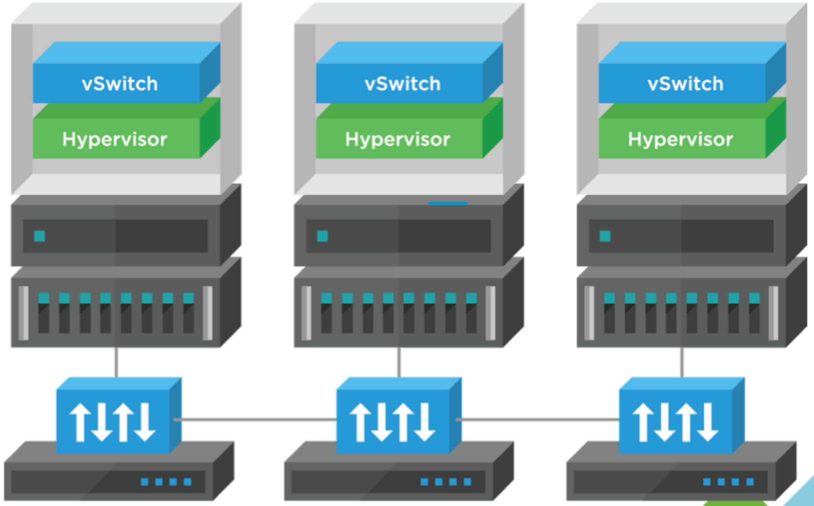
- Reduce hardware complexity and OpEx costs
- Improve application availability and resiliency
- Expedite recovery and decrease downtime

VMware NSX
The Next-Generation Networking Model



Network and security services now in the hypervisor



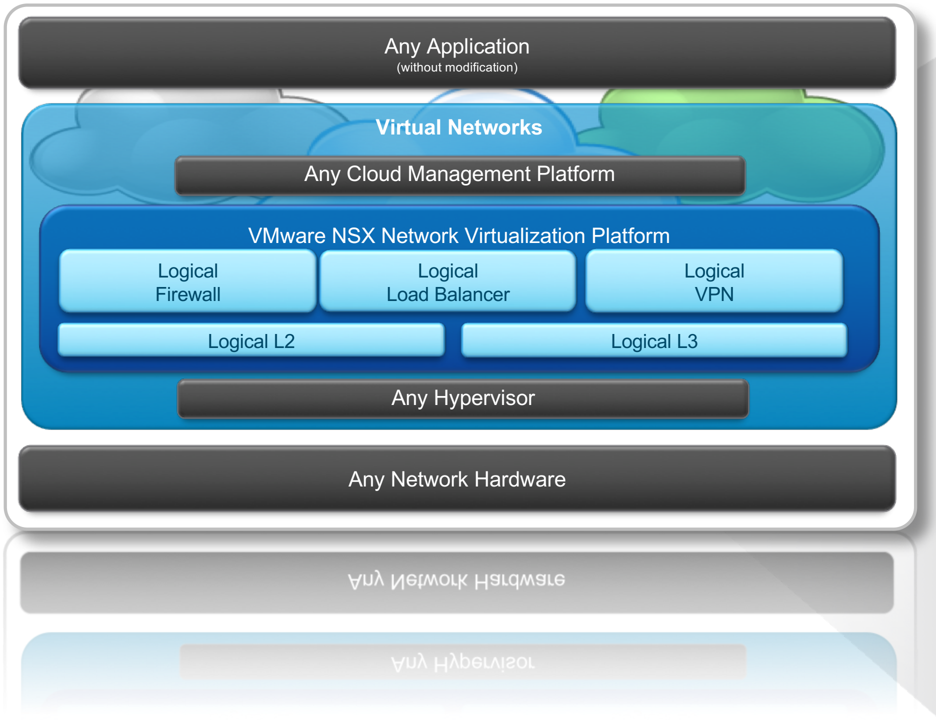


- East-west firewalling
- High throughput rates
- Hardware independent

Applying Network and Security Virtualization to IT Challenges

Theme	**Security: Inherently Secure Infrastructure**	**Automation: IT at the Speed of Business**	**Application Continuity: Datacenter Anywhere**
Lead Use Case	Micro-segmentation ★	IT Automating IT ★	Disaster Recovery ★
Mission Value	Enhanced Mission Security at reduced cost	Time to Mission: Reduce infrastructure provisioning time from weeks to minutes	Mission Resilience and Agility
Other Use Cases	Data Segmentation	Developer Cloud	Data Center Consolidation and Migration
	Secure End User	Multi-tenant Infrastructure	NSX in Public Cloud

VMware NSX – Networking & Security Capabilities



Logical Switching– Layer 2 over Layer 3, decoupled from the physical network

Logical Routing– Routing between virtual networks without exiting the software container

Distributed Firewall (DFW) – Logical Firewall, Kernel Integrated, High Performance

Logical Load Balancer – Application Load Balancing in software

Layer 2 and Layer 3 VPN – Site-to-Site & Remote Access VPN in software

Network Address Translation (NAT) – translate private IPs to public IPs

DHCP - Server and Relay

NSX API – RESTful API for integration into any Cloud Management Platform

Partner Eco-System

NSX Multi-Site Deployment Options

- **Active-Active Data Centers**
  - Logical Network Connectivity (L2-L7) that enables resources in different physical locations to be pooled together as a unified set of compute resources. Also supports workload mobility between sites using Logical Networks and Security
  - **Solution:** Single or Multi VC Logical Networks across Datacenters
- **Disaster Recovery**
  - An active and stand-by application deployed in two different locations that are NOT in the same geographical fault domain
  - Only one instance of application is active and passing traffic at any time
  - **Solution:** SRM Protected Applications
- **L2 Extension**
  - Extending L2 between sites and admin boundaries over L3 with or without encryption
  - **Solution:** NSX L2 VPN

NSX Current Federal Certification Status

- **Army CON (July 2015)**
  - Certification # 201519393 approved on 7/27/2015
- **DISA STIG (July 2016)**
  - Completed and published to IASE.
- **ICSA Certification (January 2017)**
  - Both NSX for vSphere Distributed Firewall and Edge Firewall are certified against ICSA Corporate Firewall criteria.
- **FIPS 140-2 (February 2017)**
  - NSX for vSphere 6.3.0 has a FIPS mode that uses only those cipher suites that comply with FIPS. NSX Manager and NSX Edge have a FIPS Mode that can be enabled via the vSphere Web Client or the NSX REST API.
- **Common Criteria (May 2017)**
  - NSX for vSphere 6.3.0 testing has been completed and is in compliance with the EAL2+ level of assurance.

NSX for Disaster Recovery Resources

Whitepapers / Design Guides

Disaster Recovery with NSX and SRM

NSX-V Multi-site Options and Cross-VC NSX Design Guide

VMware NSX-V: Control Plane Resiliency with CDO Mode

Enterprise Hybrid Cloud

iland

Network Virtualization Blog:

Enhanced Disaster Recovery with Cross-VC NSX and SRM

Cross-VC NSX for Multi-site Solutions

NSX-V: Multi-site Options and Cross-VC NSX Design Guide

Cross-VC NSX: Multi-site Deployments with Ease and Flexibility

Multi-site with Cross-VC NSX: Consistent Security and Micro-segmentation Across Sites

Multi-site with Cross-VC NSX and Palo Alto Networks Security

VMware NSX and SRM: Disaster Recovery Overview and Demo

NSX-V 6.3: Cross-VC NSX Security Enhancements

NSX-V 6.3: Control Plane Resiliency with CDO Mode

Multi-site Active-Active Solutions with NSX-V and F5 BIG-IP DNS

Disaster Recovery with VMware NSX-V and Zerto

Videos (NSX YouTube Channel):

Multi-site with Cross-VC NSX: Workload Mobility and Consistent Security Across Sites

Multi-site with Cross-VC NSX and Palo Alto Networks Security

VMware NSX and SRM - Disaster Recovery Overview and Demo

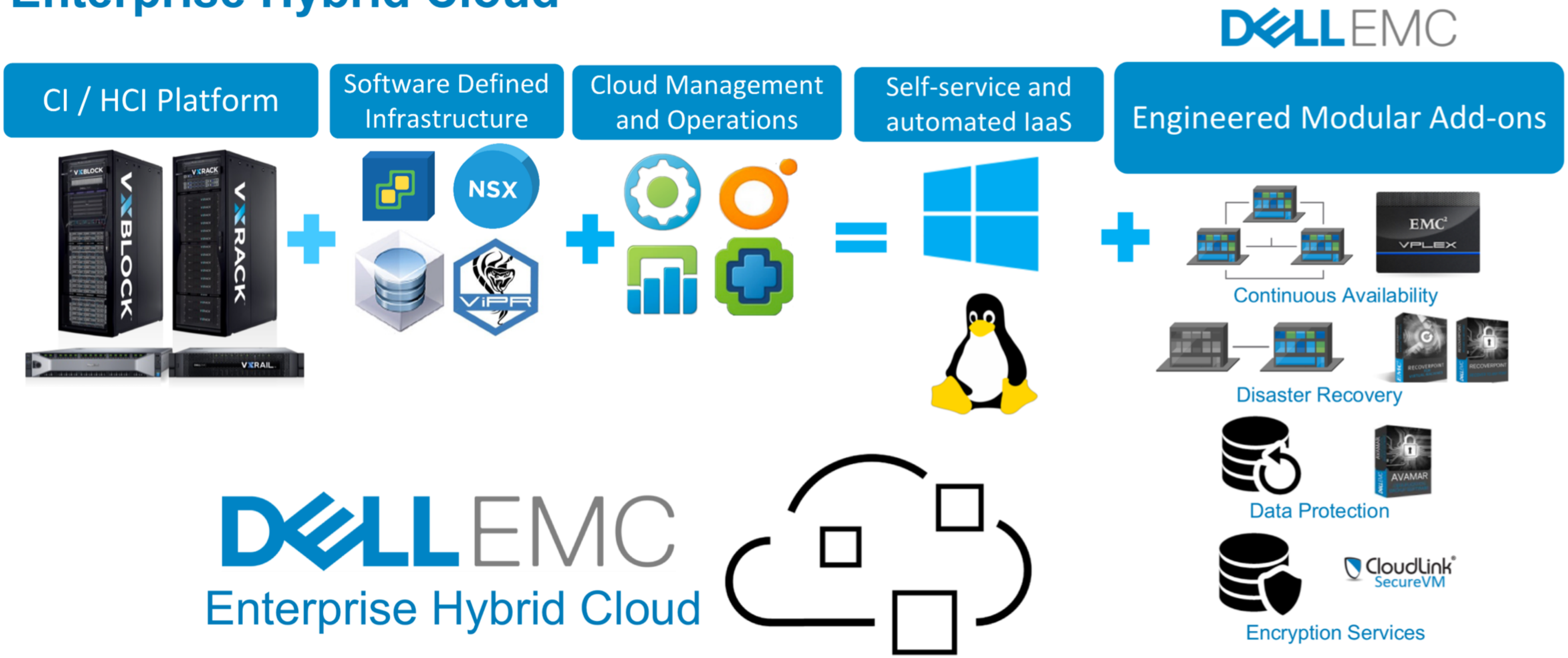
NSX DR In Action

DR Solutions with NSX

Dell EMC Enterprise Hybrid Cloud

DELL EMC
Enterprise Hybrid Cloud

Enterprise Hybrid Cloud



DELL EMC

CI / HCI Platform + Software Defined Infrastructure + Cloud Management and Operations = Self-service and automated IaaS + Engineered Modular Add-ons

Continuous Availability

Disaster Recovery

Data Protection

Encryption Services

DELL EMC
Enterprise Hybrid Cloud

Business value NSX with EHC delivered to our customers

Insight

25% time saved from operational activities

Provisioning time reduced from days to **minutes**

Increased resource utilization

ciic

Reduced provisioning times from **2–3 weeks to minutes**

Decreased total IT spend by **60%**

Reduced time to market for new business services by **65%**

etisalat

4X faster provisioning time

90% reduction in downtime

50% reduction in data center costs

MARKEL®

Consolidated data centers by **71%**

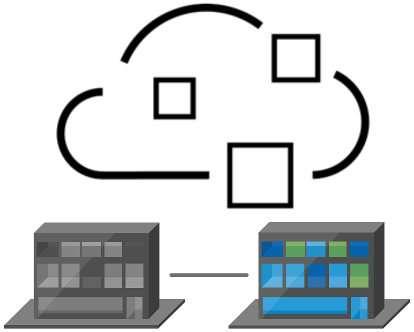
Reduced resource provisioning time from months to **hours**

Unification of entire IT department vs. siloed teams

NSX Simplifies EHC DR add-on

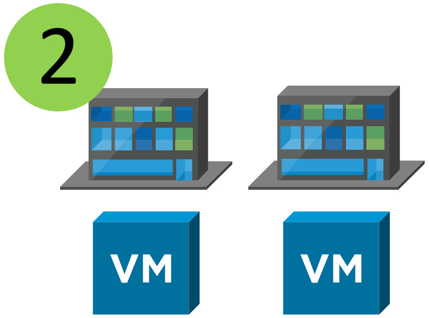
RecoverPoint for Virtual Machines (RP4VM)

- **VM-level disaster recovery granularity**
- **Virtual Appliance Replication**
- **vSphere web client integration**

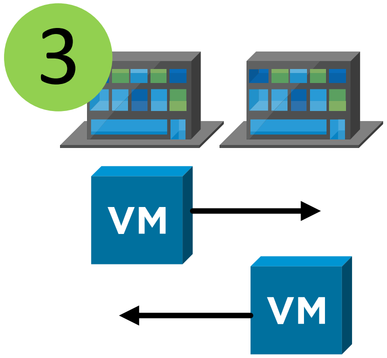


Use Case: Requirements

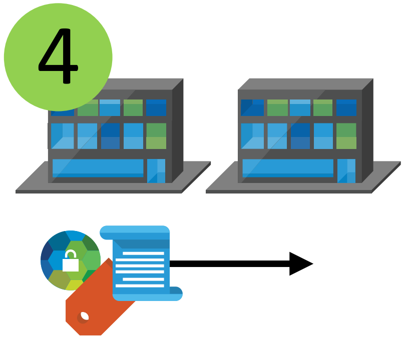
2 Sites, 2 vCenters



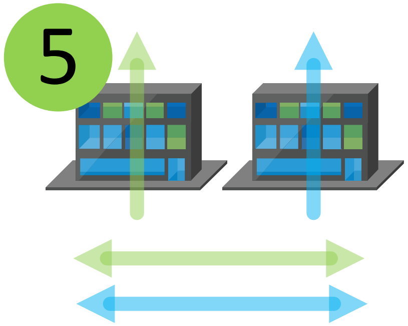
Active workloads



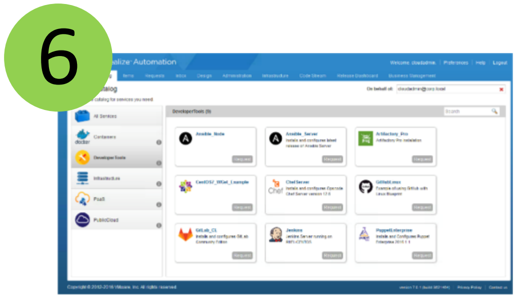
Bi-directional DR



Consistent security



Consistent networks and traffic engineering


6
vRealize Automation
Welcome: cloudadmin. | Preferences | Help | Logout
Catalog | Items | Requests | Inbox | Design | Administration | Infrastructure | Code Stream | Release Dashboard | Business Management
All Services
Containers
DeveloperTools
Infrastructure
PaaS
PublicCloud
Search
Request

Catalog

Search the catalog for services you need.

On behalf of: cloudadmin@corp.local

DeveloperTools (9)

Ansible_Node

Ansible_Server — Installs and configures latest release of Ansible Server

Artifactory_Pro — Artifactory Pro installation

CentOS7_WGet_Example

ChefServer — Installs and configures Opscode Chef Server version 12.6

GitHubLinux — Example of using Github with Linux Blueprint

GitLab_CE — Installs and configures GitLab Community Edition

Jenkins — Jenkins Server running on RHEL/CentOS

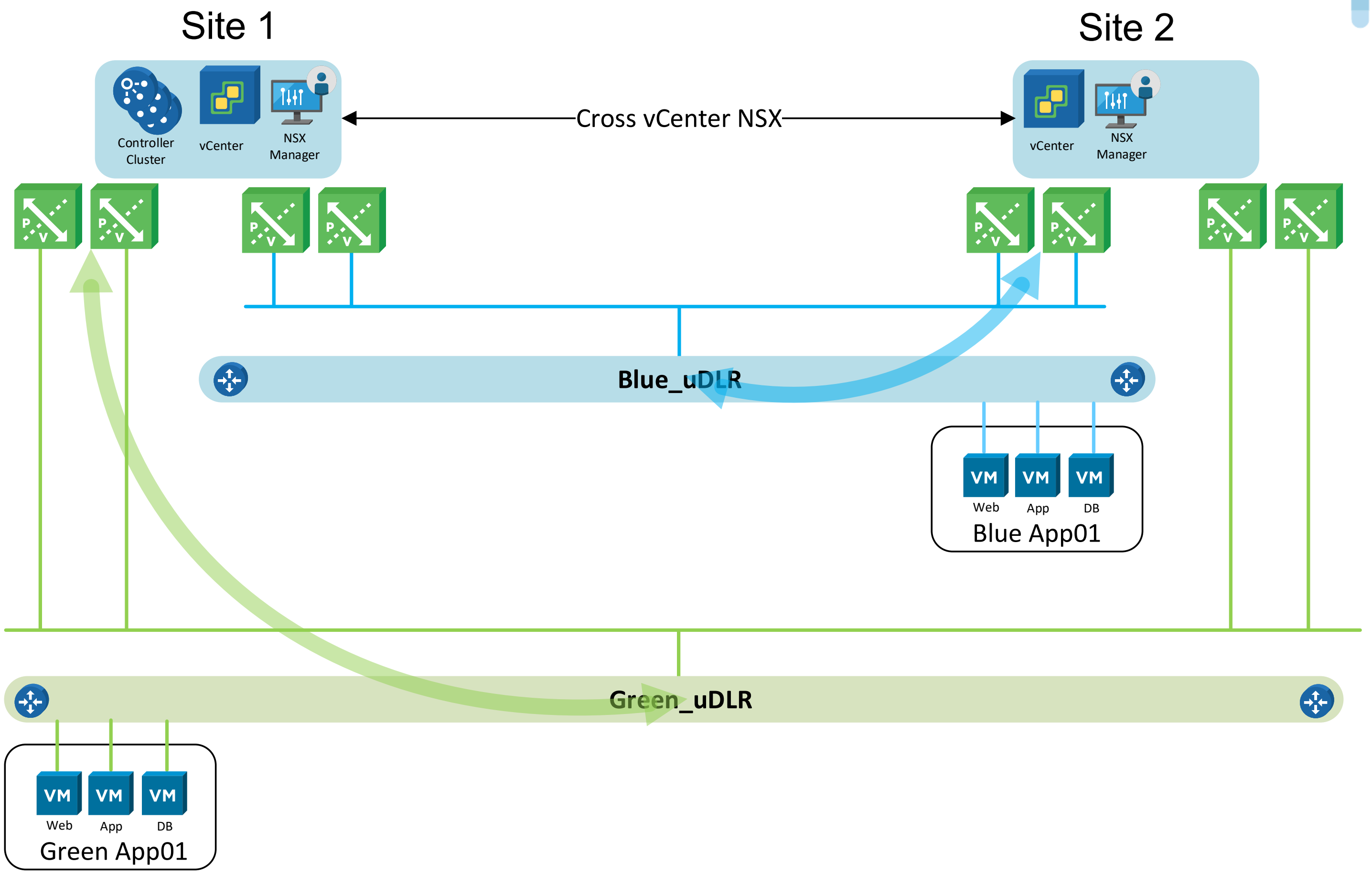
PuppetEnterprise — Installs and Configures Puppet Enterprise 2016.1.1

Copyright © 2012-2016 VMware, Inc. All rights reserved.

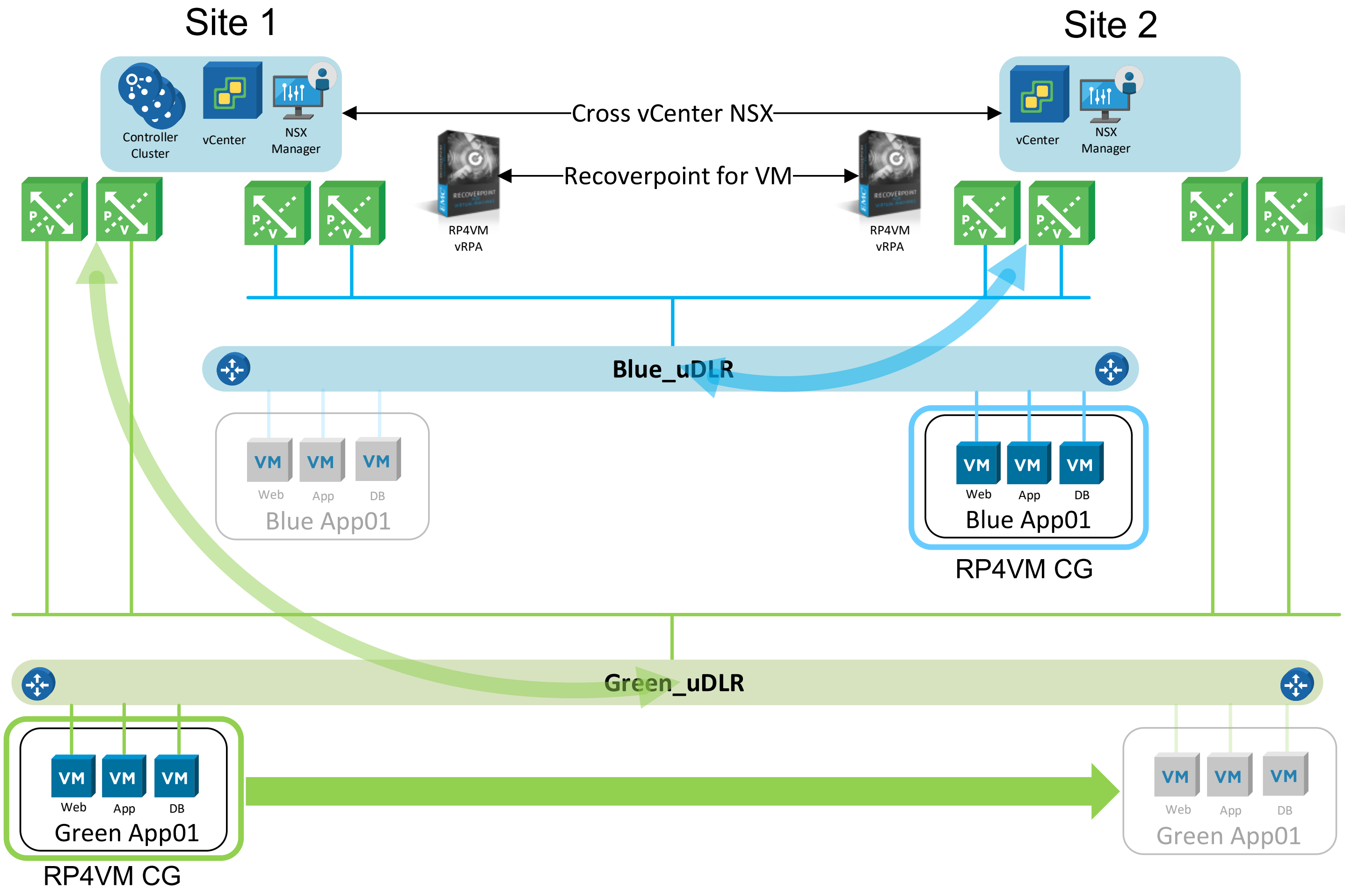
version 7.0.1 (build 3621464) | Privacy Policy | Contact us

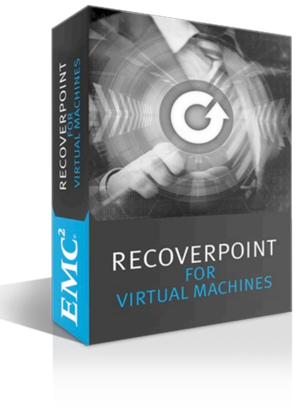
DR Consumption through CMP

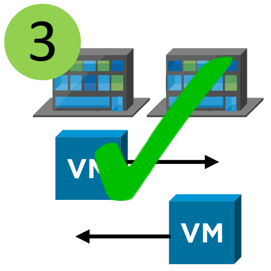
Building the Network



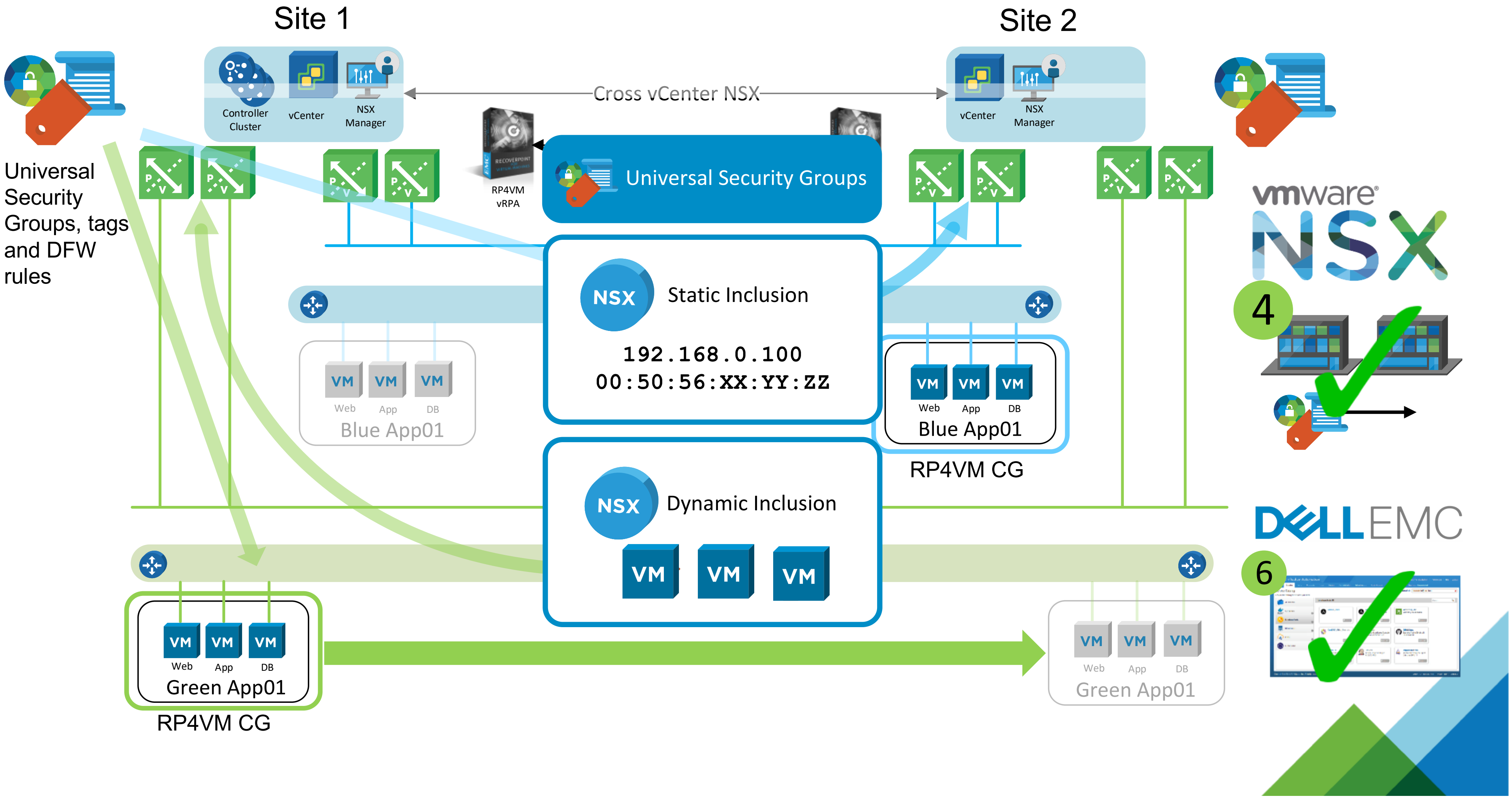
Replicating the VMs







Securing the Applications



Site 1

Site 2

Controller Cluster

vCenter

NSX Manager

Cross vCenter NSX

vCenter

NSX Manager

RP4VM vRPA

Universal Security Groups, tags and DFW rules

Universal Security Groups

NSX Static Inclusion

192.168.0.100
00:50:56:XX:YY:ZZ

NSX Dynamic Inclusion

VM VM VM

VM VM VM
Web App DB
Blue App01

VM VM VM
Web App DB
Blue App01

RP4VM CG

VM VM VM
Web App DB
Green App01

RP4VM CG

VM VM VM
Web App DB
Green App01

vmware NSX

4

DELL EMC

6

Summary

- NSX decouples networking services form the physical infrastructure allowing for a resilient DR solution
- Cross-VC NSX and SRM together provide an enhanced DR solution
- Consistent networking across sites with NSX prevents the need to manually map different networks and change application IP addresses
- NSX also provides consistent security policies across vCenter sites which enables automatic correct security for applications when a DR event occurs
- Cross-VC NSX component and site recovery is fully supported
- Automation can be leveraged in a NSX / SRM environment for additional requirements/needs: vRO, NSX REST API

Thank You

- Kevin Reed
- Sr Manager, VMware
- Federal Networking and Security Team
- kreed@vmware.com
- 703.307.3253

- Don Poorman
- Manager – Solutions Engineering
- dpoorman@govplace.com
- 301.678.3667