# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>vSphere Replication</td>
<td>3</td>
</tr>
<tr>
<td>VMware NSX for vSphere</td>
<td>4</td>
</tr>
<tr>
<td>What is Disaster Recovery-as-a-Service?</td>
<td>5</td>
</tr>
<tr>
<td>Benefits</td>
<td>6</td>
</tr>
<tr>
<td>DRaaS with VMware NSX</td>
<td>7</td>
</tr>
<tr>
<td>Key Benefits for Cloud Providers</td>
<td>7</td>
</tr>
<tr>
<td>NSX Use Cases with DRaaS</td>
<td>8</td>
</tr>
<tr>
<td>References</td>
<td>12</td>
</tr>
</tbody>
</table>
Executive Summary
Small, Mid-Sized and Enterprise businesses alike are looking for disaster recovery solutions that provide more agility, faster implementation, and cost reduction through the elimination of additional sites, servers, storage and/or sole reliance on off-site tape backups. VMware Cloud Provider Partners can seize on this opportunity and increase revenue by adding Disaster Recovery-as-a-Service service offering to their portfolio.

451 Research conducted a survey on VMware cloud Provider Partner based DR. There were 403 respondents in total, they covered North America, across all various verticals (Manufacturing, Financial Services, Healthcare/Pharmaceutical, Public Sector/Education, etc), and a good mix of segment-wise, 40% from SMB, 28% from Commercial segment and 32% from Enterprise and up. Respondent job titles spanned from 31% C-level, 10% VP, 23% Directors, and 25% Managers and Others. 80% of respondents were decision makers and 20% were influencers.

Results are consistent with the top use cases Cloud Provider Partners can use to promote their Disaster Recovery-as-a-Service Offering.

Introduction
Disaster recovery as a service (DRaaS) for VMware Cloud Provider Partners is the replication, hosting and recovery of customers on-premise as well as Cloud-based Virtual Machines into the Cloud Provider’s infrastructure. Disaster Recovery-as-a-Service is built on vSphere replication and VMware NSX for vSphere. DRaaS enables High Availability (HA), typically called “Carrier Class” services that are 5 9’s (99.999 %) available. Cloud provider partners using vCloud Director can also leverage VMware vCloud Availability for vCloud Director.

vSphere Replication
VMware vSphere Replication is a vSphere hypervisor-based, asynchronous replication solution for vSphere virtual machines. It is fully integrated with VMware vCenter Server and the vSphere Web Client. vSphere Replication delivers flexible, reliable and cost-efficient replication to enable data protection and disaster recovery for all virtual machines in your environment.
vSphere Replication is used to define Virtual Machine Recovery Point Objective and Synchronization of Virtual Machine changes into the Cloud Provider’s Infrastructure.

**VMware NSX for vSphere**
VMware NSX® is the network virtualization and security platform for the Software-Defined Data Center, delivering the operational model of a virtual machine for entire networks. With NSX, network functions including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment. This effectively creates a “network hypervisor” that acts as a platform for virtual networking and security services. Similar to the operational model of virtual machines, virtual networks are programmatically provisioned and managed independently of the underlying hardware.

NSX is utilized to provide a secure network for the replication/migration of virtual machines to the Cloud Provider’s infrastructure, enforce multi-tenancy and thus protect and isolate tenant’s workloads, as well as, faithfully reproduce a tenant’s on-premise or Cloud-based application networks and security services in the Cloud Provider’s Data Center.
What is Disaster Recovery-as-a-Service?
Disaster Recovery-as-a-Service is a category of cloud computing used for protecting an application or data from a natural or human disaster or service disruption at one location by enabling a full recovery in the cloud. Disaster Recovery-as-a-Service differs from cloud-based backup services by protecting data and providing standby computing capacity on demand to facilitate more rapid application recovery. Disaster Recovery-as-a-Service capacity is delivered in a cloud-computing model so recovery resources are only paid for when they are used, making it more efficient than a traditional disaster recovery warm site or hot site where the recovery resources must be running at all times.

With disaster recovery as a service for VMware Cloud providers, the time to return applications to production is reduced because data does not need to be restored over the internet. DRaaS can be especially useful for small and medium-sized businesses that lack the necessary expertise to provision, configure and test an effective disaster recovery plan. Using DRaaS also means organizations don’t have to invest in and maintain their own off-site DR environment.

As more organizations look to VMware Cloud providers for as-a-Service solutions, multiple analyst sources show an over 30% growth increase year over year for Disaster Recovery-as-a-Service, with most organizations showing an interest in DRaaS when compared to Storage-as-a-Service or Monitoring as-a-Service. This means an increase of over 30% to Cloud Provider revenues providing DRaaS.
Benefits
For organizations, relying on stored tape backups off-site in case of a disaster, VMware cloud Provider-Based DR is enabling DR capabilities that were not previously affordable.

<table>
<thead>
<tr>
<th>Storage-as-a-Service</th>
<th>43%</th>
<th>29%</th>
<th>28%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring-as-a-Service</td>
<td>28%</td>
<td>26%</td>
<td>46%</td>
</tr>
<tr>
<td>Disaster Recovery-as-a-Service</td>
<td>25%</td>
<td>34%</td>
<td>41%</td>
</tr>
</tbody>
</table>

- **Currently deployed**
- **Not deployed but planning to deploy**
- **Not planning to deploy**

Disaster Recovery-as-a-Service with VMware Cloud providers resolves the current issues around complexity, cost and the absence of a solution for most organizations. It’s also simple to implement, leverages an organization’s existing vSphere assets, ensures compatibility and reliability.
DRaaS with VMware NSX
NSX provides a complete set of logical networking elements and services for VMware Cloud Providers and Enterprises alike, including logical switching, routing, firewalling, load balancing, VPN, quality of service (QoS), and monitoring. These services are provisioned in virtual networks through any cloud management platform leveraging the NSX APIs. Virtual networks are deployed nondisruptively over any existing networking hardware.

Key Benefits for Cloud Providers
NSX enhances Disaster Recovery-as-a-Service for VMware Cloud Providers by ensuring:

- Secure multi-tenancy in a shared infrastructure. Using the distributed firewall providers can divide the data center into distinct security segments logically, down to the level of the individual tenant and workload.
- Workload mobility independent of physical network topology within and across Cloud Provider’s data centers.
- Dramatically improved operational efficiency through automation. Providers can create networks and security policies in software, eliminating bottlenecks, costs, and overall operational overhead associated with hardware-based networks.
- Enhanced security and advanced networking services through an ecosystem of leading third-party vendors. Providers can integrate third-party security solutions ensuring compliance to corporate security policies and governances are met when workloads failover into their infrastructure.

<table>
<thead>
<tr>
<th>Key Benefits for VMWare Cloud Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro-Segmentation</td>
</tr>
<tr>
<td>Workload Mobility</td>
</tr>
<tr>
<td>Network &amp; Security Provisioning automation</td>
</tr>
<tr>
<td>Enhanced Security and networking services</td>
</tr>
</tbody>
</table>
NSX Use Cases with DRaaS

NSX functionality can be consumed to enable provider side or provider managed use cases for a Disaster Recovery-as-a-Service offering. So this enables providers to deliver additional value-added services to cloud consumers.

• Automation to deliver Network and Security in minutes - NSX completely removes hardware-centric barriers to the automation of networking operations. By moving networking and security services into the data center virtualization layer, NSX delivers the same automated operational model of a VM, but for the entire network. Whether through VMware vCloud Director, vRealize Automation, OpenStack, or other tools, NSX is able to automate a number of processes, significantly accelerating service delivery and reducing provision times from months to minutes. Cloud providers, therefore, can automate the faithful reproduction of the Networks and security policies of tenant’s on-premise workloads before they are replicated/migrated to the provider’s data center, ensuring both the tenant workload networks and security policies are in-place and therefore primetime ready for a failover event.

• Data Center and multi-Tenant Network Security - NSX enables a fundamentally more secure the data center by integrating virtualized security and distributed firewallsing directly into the infrastructure. This creates policy enforcement points for every workload. For the first time, it is operationally feasible to provide granular security with policies that travel with the workloads, independent of where workloads are in the network topology. This dramatically reduces risk to the provider's and their tenants by enabling security actions to adapt quickly to changing threats, while significantly simplifying the operational model for security.

Providers can leverage this functionality to isolate and protect workloads between tenants as well as, their individual applications. This allows for the highest level of security (inter & intra tenant) to be programatically enforced in the hypervisor, ensuring zero exposure during and after a failover event.
• Logical Network Extension - At a high level the L2VPN provides an SSL secured L2 extension over any IP network. An NSX Edge in the tenant's location runs as the L2VPN Client, while another NSX Edge runs as an L2VPN server at the provider and terminates connections from the client. This provides the ability to extend any combination of VLAN or VXLAN networks across different environments and enables on-premise to cloud L2 connectivity. Importantly we have unbundled the client from NSX, so the customer footprint is minimal as the solution will work with any ESXi 5.0 or newer environment. With VXLAN and VLAN trunk support, we also support multiple internal networks to be extended per edge.

Providers can use this functionality to support Disaster Recovery plan testing and partial failover tests. In these scenarios, some nodes of a tenant application may run on-premise while others failover to the provider. With the L2VPN the tenant's L2 network is logically stretched allowing zero network configuration change to the application nodes during these events.
Secure Inter-Data Center connections - NSX Edge supports site-to-site IPSec VPN between an NSX Edge instance and remote sites. Certificate authentication, preshared key mode, and IP unicast traffic are supported between the NSX Edge instance and remote VPN routers. Behind each remote VPN router, multiple subnets can be configured to connect to the internal network behind an NSX Edge through IPSec tunnels.

Providers can use this functionality to create a secure network channel through which replication traffic over the internet can be carried.

Note:
Subnets and the internal network behind an NSX Edge must have address ranges that do not overlap.

Platform Service Insertion - NSX is a platform that supports a policy-based approach to services, either natively from NSX like DFW or Guest Introspection, or from our 3rd party ecosystem for functionality like AV, Anti-Malware, Enhanced Firewalling, IDS/IPS etc. So, using NSX Service Composer and security groups providers can deliver additional value-added services from these partners to their tenants.
This functionality ensures the security services required by a tenant in order to meet corporate security policies and/or governance, and network services like an Application Delivery controller are programmatical provisioned and enforced when a failover event occurs.
References