

OVERVIEW

The Nutanix DRaaS Service focuses on collaborating with the customer to enable a new tenant in Nutanix DRaaS, connecting it with existing Nutanix on premises resources, and configuring replication.

- Implement Nutanix DRaaS in a simple configuration to speed initial adoption and enablement
- Mitigate risk and accelerate time to value by leveraging our knowledgeable and experienced consultants
- Gain understanding through rapid knowledge transfer for the most common configuration and operations topics

OUR SERVICE OFFERING

THE NUTANIX DRAAS SERVICE OFFERING WILL INCLUDE THE FOLLOWING OBJECTIVES:

- Conduct a preliminary workshop and validate networking requirements
- Pair an existing Prism Central instance to DRaaS
- Assist with connectivity from on premises locations to DRaaS
 - Changes executed to on-premises VPN devices must be performed by customer's existing network SMEs
- Create a supported third-party VPN VM in DRaaS to act as customer's gateway in the event of a disaster
 - Add VPN VM file to cluster
 - Configure VPN VM with (2) interfaces - Untrust/Trust
 - Configure (1) VPN IPSec tunnel to on-premises firewall
 - Configure base security for VPN VM
 - Note: Configuration of VPN devices beyond listed above is not included
- Configure Prism Central policies to utilize Nutanix DRaaS
 - Create up to five (5) protection policies
 - Create a recovery plan for two non-production Windows VMs to demonstrate 'Power On Sequence' as one capability of failover (disaster recovery) Orchestration
 - Create up to ten (10) categories
 - Affecting up to two (2) clusters in one source availability zone
- Create a virtual Microsoft Active Directory Domain Controller in DRaaS
 - Verify health of existing environment prior to starting
 - Configure sites and services to reflect topology change
 - Configure Active Directory FSMO roles
 - Validate Active Directory and Sysvol replication
 - Note: Remediation of existing Active Directory replication issues is not included
- After allowing for synchronization, perform a test failover and failback with up to two (2) non-production VMs using 100 GB or less aggregate
- Conduct a knowledge transfer session on the solution as built
- Provide documentation of the environment as built

PRE-REQUISITES

- Existing functional AHV or ESXi cluster on current supported AOS code
- Existing Prism Central deployed and functional
- Functional backup system or pre-production cluster already in place
- Network segments available to failover to Nutanix DRaaS
- 3rd party firewall must support external BGP (eBGP)

DELIVERABLES

- Knowledge transfer session
- Project status reports
- VPN as-built documents
- Project close out

OUT OF SCOPE

- Any Citrix components are out of scope as part of Choice Solutions Nutanix DRaaS and would need to be scoped separately

Typically a 3 - 4 day engagement.