Copyright

Copyright 2020 Nutanix, Inc.

Nutanix, Inc.
1740 Technology Drive, Suite 150
San Jose, CA 95110

All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws.

Nutanix is a trademark of Nutanix, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.
# Contents

1. Executive Summary ........................................................................................................... 5

2. Introduction .......................................................................................................................... 6
   2.1. Audience ....................................................................................................................... 6
   2.2. Purpose ......................................................................................................................... 6

3. Nutanix Enterprise Cloud Overview .................................................................................. 7
   3.1. Nutanix Xi Cloud Services .......................................................................................... 8

4. Xi Cloud Services ............................................................................................................... 9
   4.1. Common Terminology ................................................................................................. 9

5. Pairing .................................................................................................................................. 12

6. Xi Connectivity .................................................................................................................. 13
   6.1. Enable VPN .................................................................................................................. 13
   6.2. Direct Connect ............................................................................................................. 17

7. Customer Network Requirements and Considerations .................................................. 18
   7.1. Policy-Based Routing ................................................................................................. 18
   7.2. Security for On-Premises CVMs ............................................................................... 19

8. Failover ............................................................................................................................... 20
   8.1. Normal State ................................................................................................................. 20
   8.2. Xi Complete Failover ................................................................................................... 21
   8.3. Xi Partial Failover ........................................................................................................ 23
   8.4. Xi Partial Subnet Failover ........................................................................................... 23
   8.5. Xi Failover Test .......................................................................................................... 24

9. Conclusion ............................................................................................................................ 26
1. Executive Summary

Traditional cloud services require a separate set of constructs and management tools with distinct operational requirements, complex management, and higher overall costs. Xi Cloud Services offers the following advantages:

- Own your on-premises infrastructure and consume public cloud services at the same time.
- Instantly provision and configure a public cloud environment.
- Seamlessly integrate Xi Cloud Services with your on-premises Nutanix implementation.

Nutanix supports multiple options for linking your on-premises datacenter to Xi: you can use a direct connection or your own third-party firewall or use the Nutanix VPN service to join quickly and keep your communication secure. Once you connect your datacenter to Xi, you can enable the disaster recovery (DR) service to protect your workloads. The Nutanix Prism UI facilitates seamless management to configure the shortest recovery time objectives (RTOs) possible and allow customers to build complex DR workflows at a moment’s notice.

The DR package works in multiple failover scenarios: you can fail over your whole datacenter, fail over a couple subnets, or enable automatic failover testing while you keep production running. The enterprise receives an auditable record of any event—reassurance that their recovery plans are working.

As application requirements change and grow, Nutanix can easily adapt to business needs. Nutanix is uniquely positioned to protect and operate in environments with minimal administrative effort because of its web-scale architecture and commitment to enterprise cloud operations. The same intuitive UI allows you to use your application in a hybrid environment, whether on-premises or in the cloud.
2. Introduction

2.1. Audience
This tech note is part of the Nutanix Solutions Library. We wrote it for Nutanix customers who want to connect their datacenters to Xi Cloud Services. Xi Cloud Services provides a native extension to the Nutanix Enterprise Cloud, delivering an integrated public cloud environment that you can instantly provision and automatically configure. Readers should already be familiar with basic Nutanix administration and networking concepts.

2.2. Purpose
In this document, we cover the following topics:
- Xi networking and datacenter concepts.
- On-premises networking topology for Xi.
- How to connect on-premises Nutanix clusters to Xi for DR.
- How hosted Xi applications talk to on-premises services.
- Impact of failover and subnet topology.

Table 1: Document Version History

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Published</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>October 2018</td>
<td>Original publication.</td>
</tr>
<tr>
<td>1.1</td>
<td>November 2018</td>
<td>Added Xi Connectivity Checklist.</td>
</tr>
<tr>
<td>1.2</td>
<td>April 2019</td>
<td>Updated Nutanix overview and Direct Connect section.</td>
</tr>
<tr>
<td>1.3</td>
<td>August 2019</td>
<td>Updated the Xi Cloud Services and Xi Connectivity sections.</td>
</tr>
<tr>
<td>1.4</td>
<td>March 2020</td>
<td>Updated for new regions.</td>
</tr>
</tbody>
</table>
3. Nutanix Enterprise Cloud Overview

Nutanix delivers a web-scale, hyperconverged infrastructure solution purpose-built for virtualization and both containerized and cloud environments. This solution brings the scale, resilience, and economic benefits of web-scale architecture to the enterprise through the Nutanix enterprise cloud platform, which combines the core HCI product families—the Nutanix Acropolis OS and Nutanix Prism management—along with other software products that automate, secure, and back up cost-optimized infrastructure.

Available attributes of the Nutanix enterprise cloud OS stack include:

• Optimized for storage and compute resources.
• Machine learning to plan for and adapt to changing conditions automatically.
• Self-healing to tolerate and adjust to component failures.
• API-based automation and rich analytics.
• Simplified one-click upgrade.
• Native file services for user and application data.
• Native backup and disaster recovery solutions.
• Powerful and feature-rich virtualization.
• Flexible software-defined networking for visualization, automation, and security.
• Cloud automation and life cycle management.

Nutanix Acropolis provides data services and can be broken down into two main components: the Distributed Storage Fabric (DSF) and AHV. Nutanix Prism furnishes one-click infrastructure management for virtual environments running on Acropolis. Acropolis is hypervisor agnostic, supporting two third-party hypervisors—VMware ESXi and Microsoft Hyper-V—in addition to the native Nutanix hypervisor, AHV.
3.1. Nutanix Xi Cloud Services

Xi Cloud Services offers a native extension to the Nutanix Enterprise Cloud, delivering an integrated public cloud environment that customers can instantly provision and automatically configure. The first service available in Xi Cloud Services, Xi Leap, provides disaster recovery as a service (DRaaS). Leap rapidly and intelligently protects the applications and data in your Nutanix environment without the need to purchase and maintain a separate infrastructure stack.

To learn more about the Nutanix Enterprise Cloud, please visit the Nutanix Bible and Nutanix.com.
4. Xi Cloud Services

Xi Cloud Services is a native cloud extension for the Nutanix Enterprise Cloud. Because it has access to the entire infrastructure stack, Xi Cloud Services uniquely enables IT teams to extend their environments beyond traditional datacenter boundaries. Xi is an integrated cloud environment that you can instantly provision and automatically configure.

To take advantage of Xi Services, use your Nutanix portal account to pair your on-premises Prism Central with Xi. You can link to Xi using the VPN service provided by Nutanix, a direct connection, or your own third-party firewall.

Xi provides a range of public floating IPs that you can use for the source and destination for traffic entering the customer’s virtual private cloud (VPC). The VPC provides a pool of shared computing resources in the Xi environment and isolates the different tenants. Xi uses policy-based routing to deliver advanced networking and security services, providing access control over both on-prem and cloud resources.

4.1. Common Terminology

Here are a few common terms related to Xi Cloud Services and private datacenters to help avoid any misunderstandings:

- **Autonomous system number (ASN)**
  An autonomous system is the unit of router policy, either a single network or a group of networks controlled by a common network administrator. An ASN is a unique number available globally to identify and enable a system to exchange exterior routing information with neighboring autonomous systems.

- **External Border Gateway Protocol (eBGP) password**
  The password for exchanging routing and reachability information among autonomous systems on the Internet.

- **Xi region**
  A geographical area with one or more availability zones. Regions are completely independent of each other, so failures in one region should not affect other regions.

- **Availability zone**
  A high-availability offering that protects your applications and data from datacenter failures. Availability zones are unique physical locations and are implemented such that normal failures (such as a power plant failure) in one zone do not affect others. Natural and manmade
disasters, such as catastrophic earthquakes and nuclear strikes, may disable more than one availability zone in a region.

- **Classless Interdomain Routing (CIDR)**
  A method for dividing a block of IP addresses into networks and the hosts that run on them.

- **Virtual network**
  A representation of the customer’s own isolated network in the Xi Cloud. Each virtual network is logically isolated from other virtual networks in the Xi Cloud and can have its own CIDR block. A user can create one or more subnets in a virtual network. A given virtual network can span multiple availability zones but not multiple regions.

- **Subnet**
  A range of IP addresses in a virtual network. A virtual network can have multiple subnets. A subnet forms a layer 2 broadcast domain, so VMs attached to the same subnet have layer 2 reachability between them.

- **MPLS**
  Multiprotocol Label Switching (MPLS) is a data-carrying technique for high-performance telecommunications networks. MPLS directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence “multiprotocol.”

- **Floating IPs**
  Publicly routable IP addresses you can selectively assign to instances. The term “floating” comes from the fact that you can dynamically (without rebooting the instance) reassign these IPs from one instance to another.

- **Private IPs**
  IP addresses from within the virtual network CIDR block that allow VMs in the virtual network to communicate.

- **VPN gateway**
  Internet Protocol Security (IPSec) gateway that allows private connectivity between a customer’s on-premises network and their Xi virtual network.

- **Virtual private cloud (VPC)**
  An elastic cloud service that can run VMs.

- **Virtual routing and forwarding (VRF)**
IP-based solution that allows network routers to have multiple instances of a routing table working simultaneously. Different tenants don’t have to be concerned about their network ranges overlapping because their traffic is segregated.
5. Pairing

You can pair your on-premises Prism Central with Xi by clicking the **Xi Cloud Services** menu option and entering your Nutanix credentials.

![Xi Cloud Services Logon](image)

*Figure 2: Xi Cloud Services Logon*
6. Xi Connectivity

Once you pair your on-premises Prism Central with Xi, you can configure the connectivity from the Xi portal. By default, you have a production virtual network and a test network. Select the production virtual network, then click Enable VPN or Enable Direct Connect.

6.1. Enable VPN

In this section we discuss the various options available for connecting to Xi using a VPN. VPN solutions involve a VPN gateway appliance deployed as a VM running in Xi. This appliance learns about local routes, establishes an IPSec tunnel with its remote peer, exchanges routes with its peer, and directs network traffic through the tunnel. This appliance is required on the Xi side and is deployed on the tenant’s overlay network.

By default, each tenant has a unique identifier provisioned for their VPN when it is initially created. The configuration is generated in the Xi portal and displayed for the handoff to the customer's network team. The unique identifier is tied to a floating IP to ensure that all destination traffic to the incoming VPN goes to the appropriate tenant VRF.

Enable VPN has two main options: the Nutanix Networking Service or Router and Firewall. The Nutanix Networking Service option creates a new VPN gateway VM that runs on your on-premises cluster and connects to your network. You must deploy the Networking Service VM to the on-prem cluster that has the correct VLAN in order for the configuration to succeed. The Router and Firewall option allows you to connect to your Xi VPC using an existing firewall or router device as the VPN gateway. For this option, Nutanix presents the configuration parameters required to connect. Available VPN endpoints are:

- Checkpoint
- Cisco ASA
- Juniper
- Palo Alto
- Fortinet
- SonicWall

**Note:** We update this list whenever we certify additional devices.

If your firewall or VPN is not included in the previous list, your on-premises firewall must:

1. Support IKE v2.
2. Support tunnel interfaces.
3. Have eBGP enabled.

Figure 3: Xi VPN Setup

Required Xi Gateway Configuration Information

To proceed with either VPN option, you need additional information from your network team:

- **Customer gateway ASN**: If the customer already has a BGP environment on-premises, the customer gateway is the ASN for the organization. If customer does not have a BGP environment on-premises, they can choose any number, typically in the 65000 range.

- **Xi gateway ASN**: The Xi gateway ASN can't be same as the customer gateway ASN. Usually customers set the Xi gateway to be the ASN customer gateway ASN plus or minus one. For instance, if customer gateway ASN is 65314, the Xi gateway ASN could be either 65313 or 65315.

- **eBGP password and IPSec secret**: These passwords can be any string, preferably alphanumeric. During on-premises VPN configuration, the customer must securely persist these passwords. If the customer forgets these passwords, we can't recover them; they must delete the Xi VPN configuration and recreate it.
• On-premises public IP used by the VPN.

The following table lists the basic ports that must be open to establish connectivity between Xi and your on-premises firewall. Depending your specific scenario, you may need to open additional ports.

Table 2: VPN and BGP Ports

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Payload Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKEv2</td>
<td>500</td>
<td>UDP</td>
</tr>
<tr>
<td>IPSec</td>
<td>4500</td>
<td>UDP</td>
</tr>
<tr>
<td>BGP</td>
<td>179</td>
<td>TCP</td>
</tr>
</tbody>
</table>

**Deployment Scenarios**

In the following scenarios, PC subnet refers to the subnet where Prism Central is running. The Xi infrastructure load balancer route is where the traffic for Xi CVMs and PC is located. You receive this information when you begin using Xi.

**On-Premises Behind National Address Translation or Firewall**

In this scenario the IPSec tunnel terminates behind the firewall. For the network address translation (NAT) to work, you need to open UDP ports 500 and 4500 in both directions. Ports 1024 through 1034 are ephemeral ports used by the CVMs. Enable the on-premises VPN gateway to allow the rules in the following table.

Table 3: On-Premises VPN Gateway Rules

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Destination Address</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC subnet</td>
<td>Load balancer route advertised</td>
<td>Any</td>
<td>1024–1034</td>
</tr>
<tr>
<td>Xi infrastructure load balancer route</td>
<td>PC and CVM subnet</td>
<td>Any</td>
<td>2020</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2009</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9440</td>
</tr>
</tbody>
</table>
The open ports you need for this example are the same as in the previous example, but you don’t need to open the ports for NAT (500 and 4500).

**IPSec Terminates on the Firewall**

The open ports you need for this example are the same as in the previous example, but you don’t need to open the ports for NAT (500 and 4500).
6.2. Direct Connect

Customers can also connect directly to Xi using exchange points. Customers looking to replicate traffic over a private connection can go through a variety of partners based on the recovery location they select. A direct connection enables connectivity through the provider’s network and is transparent to Xi. All we see is a subnet exchanged through eBGP.

When you want a more stable and consistent Internet connection, you should use a direct connection. As an additional advantage over the single VM the VPN service deploys, a direct connection also provides load balancing on the Xi infrastructure.

Direct Connect Partners:
- **Megaport**: U.S., U.K.
- **Telecom Italia**: Italy
- **Equinix**: Germany, Japan

Figure 6: Megaport Direct Connection Locations
7. Customer Network Requirements and Considerations

To prepare datacenters for Xi, we must consider two key elements: on-premises and Xi datacenter networking. For on-premises networking, the CVM subnet should not have IPs that overlap with the user subnets. Both on-premises and Xi CVMs need to talk to each other and that communication takes place through a public IP assigned to a load balancer in Xi. Therefore, we recommend:

- A separate infrastructure subnet for CVMs and Prism Central. The on-premises Prism Central needs to talk to the Xi Prism Central.
- Separating additional services required for Xi Cloud Services (like DNS and Active Directory) from the infrastructure subnet or onto a limited subnet.

**Tip:** Try to limit the number of subnets exposed to Xi.

Assign the load balancer in Xi a public-facing IP for each customer. This IP should not conflict with any IP on the customer side, which is why it needs to be a public IP. This IP routes traffic to the customer on-premises side through the VPN tunnel; CVM traffic from customer on-premises also goes to this IP address.

For Xi, each tenant gets two VRF instances. The VMs use one VRF instance for production and one for live failover testing. Only use the second VRF instance for failover testing. All Xi testing uses this second VRF instance to ensure that no subnets overlap with production workloads, so subnets can be active on the Xi Cloud while they’re active on-premises. Each VRF can handle up to 100 subnets, and the CIDR for those subnets in Xi can be anything the customer wants except the public IPs that Xi is using.

You can assign floating IPs in Xi to a jump host or directly to a VM. These IPs come from the Nutanix public IP pool, and the customer doesn’t have direct control over which IPs they get. You can reserve a set of floating IPs for a user account or tenant. If you don’t assign a floating IP or you delete the VM, the floating IP goes back to the reserved pool for that tenant.

### 7.1. Policy-Based Routing

The Xi side routes to the VPN or directly to the subnets advertised by on-premises. All other traffic is sent to the Internet (after floating IP conversion). You can use policy-based routing for more granular control over which on-premises networks can be reached from the cloud. When you use floating IPs, also configure policy-based routing in the Xi Cloud Prism Central to limit network traffic.
7.2. Security for On-Premises CVMs

In addition to user-configurable policies for securing on-premises subnets, Nutanix enforces additional security for on-premises CVMs in the Xi network by default:

- **Xi side**: Security policies on the Xi network are configured to only allow access to specific ports (Stargate, Cerebro, or NGT ports) of on-premises CVMs from specific IPs (Xi-CVMs).
- **On-premises**: All CVM IP traffic from the Xi side to on-premises comes from a specific source IP. Nutanix recommends that users write policies on the on-premises network to allow only the Xi public IP to talk to the on-premises CVMs.
8. Failover

This section covers the most common failover scenarios for Xi. We encourage you to check with your local Nutanix team about any scenarios not listed here.

Some things to keep in mind during failover events:

• Xi doesn’t provide layer 2 extension (stretched layer 2).
• VMs can keep their original IP addresses when failing over to Xi.
• A test network is available in Xi where subnets can be active while they are also active in the on-premises datacenter.
• You shouldn’t need to reconfigure the customer network (router) during failover because of the initial Xi setup of dynamic routing protocols (eBGP).

8.1. Normal State

In normal state, all workloads are running on-premises and only replicate to Xi.

The following CIDRs and subnets, with their associated VLANs, are used on-premises and need to be protected in Xi:

• Subnet 192.168.10/24, VLAN ID 100
• Subnet 192.168.20/24, VLAN ID 200
• Subnet 192.168.30/24, VLAN ID 300
• Subnet 192.168.40/24, VLAN ID 400
8.2. Xi Complete Failover

Complete failover occurs when the on-premises subnets are down. The tenant fails all subnets over to Xi. Once network connectivity is restored, the protection policies start replicating data back to the datacenter.
When a complete subnet failover occurs, the source datacenter may not come back online. If the source site is completely down, getting the VPN connection back up and running is not a big concern because it only affects the reprotection status. The VPN connection reprotects your applications and replicates them back to the source site. Currently, Xi only supports one connected VPN per tenant. If your main site (with the VPN connection) goes down, it reconnects when it comes back online. If the site remains down, you could connect the Xi VPN to an existing site and update the information on the Xi web portal if the public IP changed.

Users connecting to Xi have a couple options:

- Users could connect to their applications using a floating IP for the front end and policy-based rules to lock down access.
- Users could connect to a jump host or terminal services (RDS) and launch their applications residing in Xi.
- Users could set up a third-party VPN in Xi and use policy-based routing to redirect all external traffic to the VPN.
8.3. Xi Partial Failover

Partial failover occurs when some subnets are active on-premises and some subnets are active in Xi on the production network, and the on-premises VMs can connect to the Xi VMs. With this setup, the failed-over VMs retain their IP addresses.

In a partial failover, the VPN connection is probably still established. In these cases when the VPN is active but the workload has failed over, you want to ensure that you have set up preferred routes and cost metrics. Implementation details may vary between switch vendors. Another option is to shut down the on-premises VLAN until you can fail the workload back.

8.4. Xi Partial Subnet Failover

Partial subnet failover occurs when some VMs run on-premises and some run in Xi. This scenario requires changing the IP addresses of the VMs running in Xi. In this example, two VMs (VM-103 and VM-104) from the on-premises subnet 192.168.10/24 now run in the Xi production network on subnet 10.10.100/24. The on-premises VMs can connect to the Xi VMs.
8.5. Xi Failover Test

Customers can perform the Xi failover test when all subnets are active on-premises and in the Xi virtual test network. On-premises VMs cannot connect to Xi VMs because there is no direct connection or VPN connection from the Xi test network to on-premises. The test network does not have any routes to the production network.
Figure 12: Failover to the Xi Test Network
9. Conclusion

Nutanix offers granular data protection based on recovery point objectives across many different deployment models. You can easily connect to Xi by automating a cloud VPN deployment for each tenant, which also provides different ways to connect based on the company’s needs. Allowing full subnets to fail over to Xi drastically reduces complexity. The ability to retain working IP addresses without having to maintain a stretched layer 2 network allows application owners to focus more on the business and less on keeping their workloads running when failure strikes.

Paired with Xi’s disaster recovery features, which are purposeful, fully integrated, and 100 percent software-defined, Nutanix provides the ultimate adaptability solution to your enterprise’s backup and recovery needs.
Appendix

Xi Connectivity Checklist

Xi Cloud Services is a native cloud extension for the Nutanix Enterprise Cloud. Because it has access to the entire infrastructure stack, Xi Cloud Services uniquely enables IT teams to extend their environments beyond traditional datacenter boundaries. Xi is an integrated cloud environment that you can instantly provision and automatically configure.

To take advantage of Xi Services, use your Nutanix portal account to pair your on-premises Prism Central with Xi. You can link to Xi using the VPN service provided by Nutanix, a direct connection, or your own third-party firewall. Following is a quick checklist to prepare you to consume Xi Services:

• Maintain infrastructure (CVMs and hypervisor) on a separate subnet from user VMs.
• If you aren’t using AHV IPAM, install Nutanix Guest Tools on the protected user VMs.
• Use a public IP on-premises for the VPN connection.
• Use an Autonomous System Number (ASN) on the top-of-rack switch where the cluster is connected for Border Gateway Protocol (BGP). A VPN connection requires the BGP to exchange routes.
• Deploy Prism Central on-premises on a subnet that doesn’t fail over (infrastructure subnet is a good choice).
• Five supported VPNs or firewalls:
  # Cisco ASA (minimum version 9.7)
  # Palo Alto (minimum version 8.0)
  # Check Point (minimum version R77.10)
  # Juniper (minimum version 11)
  # SonicWall (minimum version 6.5.4.4)
• Other VPNs or firewalls may work if they support IKEv2, tunnel interfaces, and BGP.

About Nutanix

Nutanix makes infrastructure invisible, elevating IT to focus on the applications and services that power their business. The Nutanix Enterprise Cloud OS leverages web-scale engineering and consumer-grade design to natively converge compute, virtualization, and storage into a resilient,
software-defined solution with rich machine intelligence. The result is predictable performance, cloud-like infrastructure consumption, robust security, and seamless application mobility for a broad range of enterprise applications. Learn more at www.nutanix.com or follow us on Twitter @nutanix.
List of Figures

Figure 1: Nutanix Enterprise Cloud ................................................................. 8
Figure 2: Xi Cloud Services Logon ................................................................. 12
Figure 3: Xi VPN Setup ................................................................................. 14
Figure 4: VPN Gateway Ports ................................................................. 16
Figure 5: IPSec Terminates on the Firewall ................................................. 16
Figure 6: Megaport Direct Connection Locations ........................................ 17
Figure 7: Policy-Based Routing ................................................................. 19
Figure 8: On-Premises Subnets ................................................................. 21
Figure 9: Complete Failover ..................................................................... 22
Figure 10: Partial Failover ......................................................................... 23
Figure 11: Partial Subnet Failover ............................................................. 24
Figure 12: Failover to the Xi Test Network ................................................. 25
List of Tables

Table 1: Document Version History................................................................................... 6
Table 2: VPN and BGP Ports.......................................................................................... 15
Table 3: On-Premises VPN Gateway Rules.................................................................... 15