v3.1 | May 2022 | TN-2124

TECH NOTE

Nutanix DRaaS Security

NUTANIX
YOUR ENTERPRISE CLOUD

Copyright

Contents

1. Executive Summary

Nutanix takes a holistic approach to security, with an inherently secure platform, extensive automation, and a robust partner ecosystem. The Nutanix security development life cycle (SecDL) integrates security into every step of product development, rather than applying it as an afterthought. The SecDL is a foundational part of product design and extends to both on-premises and Nutanix Cloud environments. The pervasive culture and processes built around security harden the Nutanix cloud platform OS and eliminate zero-day vulnerabilities. For example, research and development teams work together to fully understand all the code in the product, whether it's produced in-house or inherited from dependencies. We schedule product updates to handle known Common Vulnerabilities and Exposures (CVEs) for minor release cycles and backport all dependencies to their latest release versions in major release cycles. This approach significantly reduces zero-day risks without slowing down product evolution.

Nutanix puts appropriate security controls in place both physically and when operating the web properties that help run the Nutanix Cloud. We also extend capabilities like web application firewalls and intrusion detection to help secure customer workloads where possible. Along with a defense-in-depth approach, we secure the perimeter and use the very best in software-defined networking to tunnel and encapsulate traffic traveling from on-premises to the Nutanix Cloud and traffic running east-west within Nutanix DRaaS (Disaster Recovery as a Service). Our native key manager and software encryption protect a customer's data at rest for additional security.

The Nutanix Cloud provides a native extension to Nutanix software, delivering an integrated public cloud environment that you can instantly provision and automatically configure. Security of Nutanix DRaaS is the highest priority for the Nutanix Cloud team. As a Nutanix DRaaS customer, you immediately benefit from hardened, military-grade security built across the different layers of the service, ranging from securing datacenter access to protecting against distributed denial of service (DDoS) attacks to fortifying day-to-day operations. Similarly, the Nutanix Cloud enables you to enhance and improve the security posture in your account with the same capabilities you already use with on-premises Nutanix. Additionally, we work with independent and authorized third-party

vendors to assess, validate, and certify our design, architecture, and data handling elements related to security.

2. Introduction

Purpose

In this document, we cover the following topics:

- Security of the Nutanix Cloud.
- Security capabilities in Nutanix DRaaS.
- Trust and assurance: compliance programs.

Document Version History

Version Number	Published	Notes
1.0	April 2019	Original publication.
2.0	October 2019	Updated for current service state.
3.0	May 2021	Updated certifications.
3.1	May 2022	Refreshed content, including updated product names.

3. Nutanix Cloud Services

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

4. Security of Nutanix DRaaS

Datacenter Security

Nutanix maintains Nutanix DRaaS datacenters around the globe. Only select personnel responsible for datacenter equipment operations have physical access to the datacenter. To validate those individuals' access to the datacenter, Nutanix requires two factors of authentication: biometric verification and passcodes. All visits—both successful and failed authentications—are logged and reviewed as a part of our standard access auditing process. In the datacenter, access control determines which team member has access to a specific rack and the equipment in that rack. In addition to supporting stringent access control, all the datacenters have been built for high availability and resiliency to sustain power failures, HVAC issues, water leaks, and natural hazards.

Distributed Denial of Service (DDoS) Protection

Nutanix DRaaS runs industry-leading DDoS protection solutions to safeguard applications running in the Nutanix Cloud. Because DDoS protection is integrated into Nutanix DRaaS, the system can mitigate threats such as SYN floods and reflection attacks and end them in an effective and timely manner. Additionally, all layer 7 traffic passes through a web application firewall, so the Nutanix Cloud can filter out requests that could result in SQL injection or cross-site scripting attacks. The Nutanix Cloud also checks HTTP requests against an IP reputation database and filters and blocks requests from badly reputed IP addresses, requests originating from top-of-rack nodes, or requests from a specific IP or CIDR block.

Data Sovereignty

Our customers are distributed around the world, and they all have stringent requirements for data sovereignty based on their local laws and regulations. With Nutanix DRaaS, customers select their region, and any replicated customer data or metadata is then processed and stored in that same region. Customer data doesn't move out of a given

region unless the customer chooses to move it. As we work to expand Nutanix DRaaS to additional areas, data sovereignty remains a central commitment.

Data Protection and Encryption

Nutanix DRaaS runs on AOS, the same highly available and redundant software used in on-premises Nutanix environments. All generated data has at least two copies distributed between multiple nodes. Data at rest is encrypted using customer-specific keys that Nutanix manages. As a result, customers don't have to worry about managing encryption keys, key management servers, or hardware security modules. Similarly, when data replicates from on-premises to Nutanix DRaaS, Nutanix encrypts it over IPSec tunnels with a requirement for Internet Key Exchange (IKE) version 2 to ensure secure transfer.

Data Deletion

Like data protection and encryption, data deletion is a standard operating procedure for Nutanix DRaaS. Once a customer terminates a Nutanix Cloud account, all customer data and resources are marked for deletion immediately and deleted over the next few hours. The customer can then use the reclaimed raw storage for new resources (such as VMs) and overwrite it with new data. Nutanix holds all metadata about the customer's resources and usage until the end of the billing cycle to ensure that Nutanix Cloud can appropriately prepare and present all billing information for customers at once.

Day-to-Day Operations

Day-to-day work in Nutanix DRaaS involves developer and operations activities related to troubleshooting hardware and software issues, so specific team members in various teams have access to the services they own and manage. Our access control policies implement the minimum privileges that a team member needs to perform their tasks. As an additional layer of security, team members sign on to a specified management host and network that their administrators can use to manage and operate their services. Furthermore, team members must request, obtain, and use short-term credentials that expire within a specified time period (typically two hours), which they can then extend as needed. The Nutanix Cloud monitors all operations-related activity with a fully automated security alerting and paging service.

5. Security Capabilities in Nutanix DRaaS

Two-Factor Authentication to Nutanix Cloud Portal

As an additional layer of security, customers can enable two-factor authentication in the Nutanix Cloud portal. With two factors of authentication, customers are protected when a user's credentials are stolen or lost or when a larger breach occurs. Currently, customers can configure Google Authenticator as the second factor.

On-Premises Integration with Active Directory

Most customers use Active Directory (AD) on-premises for their authentication needs. Customers prefer not to maintain a second set of credentials: not only are multiple usernames and passwords a burden to remember, but they also increase the possibility that the user could lose them. Customers can integrate their on-premises AD with the Nutanix Cloud portal in just a few steps.

Role-Based Access Control

Nutanix provides role-based access control both on-premises with Prism Central and for the Nutanix Cloud portal. You can lock down new Nutanix Cloud network creation and decide who can view data, billing information, and user administration details. Regular IT operations staff members have only the minimum access they need to perform their duties. Regular users can neither create accounts nor create or edit networks in the Nutanix Cloud.

Policy-Based Routing

The Nutanix Cloud routes to the VPN or directly to the subnets advertised by your on-premises environment. All other traffic goes 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, configure policy-based routing in Nutanix DRaaS Prism Central to limit network traffic.

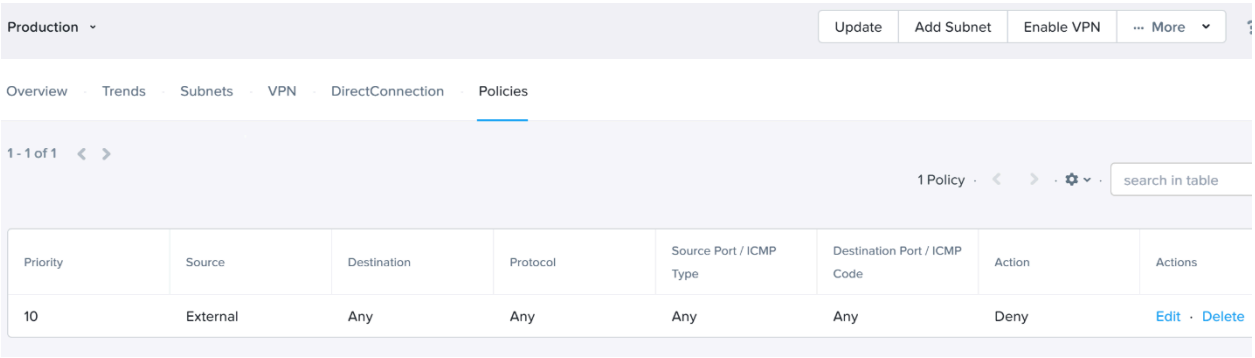

Figure 1: Policy-Based Routing

If you deploy your own third-party firewall in the Nutanix Cloud, you can make sure all traffic reroutes through it for all the subnets you create in the Nutanix Cloud. You can also limit traffic by port number and protocol and block ICMP requests if you use our available public IP address (floating IPs). Policy-based routing gives you the same flexibility as your on-premises firewall.

Network Segmentation

Every tenant consuming Nutanix Cloud services runs on its own overlay network. The overlay is a virtual network built on an underlying network infrastructure and isolated from the physical network and other overlay networks. In their own overlay network, a customer can create any needed IP ranges as long as they don’t overlap with public IP ranges.

When onboarding customers, Nutanix uses an internal service called datacenter management (DCM) to automate and secure the network to reduce the chance of human error. DCM talks to other internal services to coordinate the firewall rules and access lists that limit tenants to replicate only back to their own on-premises environments. Rules also ensure that only on-premises customer Controller VMs (CVMs) can send replication traffic to Nutanix Cloud. No customer has direct access to the network where the CVMs run.

6. Trust and Assurance: Compliance Programs

We are fully committed to continuously validating our security posture through independent and registered third-party vendors. Currently, Nutanix DRaaS is certified for ISO 27001, ISO 27017, ISO 27018, and ISO 27701 and is compliant with GDPR. Nutanix DRaaS also maintains SOC 2 Type 1, SOC 2 Type 2, and SOC 3 certifications. We continue to pursue other geography-, industry-, and vertical-specific certifications, attestations, compliance with regulations and laws, and alignment with industry standards and frameworks. You can verify our latest trust and assurance status on the Nutanix trust webpage. If you need specific certifications or have questions, reach out to your account team; they can connect you with our compliance team.

7. Conclusion

Nutanix provides a secure and easy-to-consume environment that protects and runs workloads in the cloud. Both the software development life cycle and supply chain are secure to prevent rogue access. Physical controls along with the industry's best protection from DDoS attacks limit attack vectors.

Customer data is secure at rest and on the network using strong encryption. Day-to-day Nutanix Cloud operations collect all security best practices, which we regularly review to maintain industry-standard certifications. Nutanix adheres to data sovereignty and ensures that customer data doesn't move outside the geographical region selected for it.

Nutanix customers not only save time when they protect and run workloads in the Nutanix Cloud—they also inherit a great security posture. Security has always been a leading design decision in how Nutanix builds code, and now it's also part of the way we operate datacenters on our customers' behalf.

About Nutanix

Nutanix is a global leader in cloud software and a pioneer in hyperconverged infrastructure solutions, making clouds invisible and freeing customers to focus on their business outcomes. Organizations around the world use Nutanix software to leverage a single platform to manage any app at any location for their hybrid multicloud environments. Learn more at www.nutanix.com or follow us on Twitter @nutanix.

List of Figures