EXAM BLUEPRINT GUIDE

Nutanix Certified Professional Network & Security (NCP-NS) 6.10 Beta Exam

Table of Contents

Author

Jeff Hall, Manager, Technical Certification Development

Contributors

Amin Aflatoonian, Sr. Product Manager

Amit Gupta, Sr. Product Manager

Aniket Daptari, Sr. Director, Product Management

Aritro Basu, Sr. Staff Consulting Architect

Ashish Sharma, Service Provider Solution Architect

Asir Sikdar, Staff Engineer

Danny Reppe, Advisory Solution Architect

Eric Walters, Sr. Technical Marketing Engineer, NCI & Security

Frank Shen, Sr. Product Manager

Harikrishna Reddy Y, Sr. Member of Technical Staff

Jason Burns, Director, NCI TMM

Jeroen Tielen, Nutanix Trainer & Citrix Guru

Komal Bhat, Associate Resident Consultant

Krishna Chakra Karanam, Principal Product Manager

Maroane Boutayeb, Sr. Staff Customer Experience Manager

Pavan Kumar, Member of Technical Staff 4

Rushabh Jain, Consultant

Saloni Vanit Pipariya, Member of Technical Staff 2

Sam Ghardashem, Principal Product Manager

Stephen Martin, Sr. Staff Consultant

Steve Eyler, Sr. Solution Architect

Steve Loh, Advisory Solution Architect

Steven Murray, Systems Engineer

Vimal Dharmavarapu, Principal Product Manager

1. The Exam

1.1 Purpose of Exam

The Nutanix Certified Professional - Network & Security (NCP-NS) 6.10 beta exam will measure a candidate's ability to validate the candidate's ability to deploy, manage, and troubleshoot network virtualization and network security using Nutanix Flow. Successful candidates demonstrate mastery of these skills and abilities.

1.2 Number of Questions

The NCP-NS 6.10 beta exam consists of 106 multiple-choice and multiple-response questions.

1.3 Pricing

There is no cost for the NCP-NS 6.10 beta exam.

1.4 Passing Score

The final score will be determined by examining the results from the beta exam period, determining which exam items performed well, and evaluating each candidate's results, based on only the items that performed well.

This process can take from 4-6 weeks from the time the beta period has ended. Once the evaluation is complete, candidates will receive their scores. Candidates who have passed will not need to take the live exam.

1.5 How Objectives Relate to Questions on the Exam

Objectives summarize what the test is designed to measure. Objectives are developed by Exam Developers and Subject Matter Experts based on identified tasks that relate to the job of deploying, monitoring, administering, troubleshooting, and maintaining end user computing environments utilizing Nutanix technologies.

Once the initial development process is complete, these objectives are verified using an external group of individuals in the actual job role. Finally, a number of questions is determined for each objective, which relates directly to the criticality of the task in the job role.

1.6 Languages

The beta exam is available in English.

1.7 Time Limit

The time limit for the beta exam is 180 minutes.

1.8 Scheduling and Taking the Exam

This exam is delivered via remote proctoring or in-person at select test centers.

If you select remote proctoring, after registering for the exam and providing valid identification, you will receive information on how to take the exam from your location using a web browser. Because the exam is remote proctored, you will be provided with a locked down, monitored, secure exam experience.

If you select in-person testing, you will be able to select a test center near you. On the day of the exam, you will need to arrive at the test center 15 minutes prior to the exam start time with a valid government-issued ID.

1.9 Certification Tracks

The NCP-NS 6.10 exam is a core component of the Nutanix Network & Security track. Passing this exam results in achieving the NCP-NS 6 certification.

The certification requires a passing score on the exam. While it is not required that you attend a course, Nutanix provides training that covers the objectives on the exam. Details on the recommended training course are provided in Section 4.

1.10 Retake Policy

If a candidate fails an exam on the first attempt, he or she is allowed two additional attempts. There is a seven-day waiting period between attempts. Like the first attempt, these are paid for individually and Nutanix recommends that you allow sufficient time between attempts to be properly prepared and to maximize your chances for success.

Please note: After three attempts, you will be unable to take the exam for 60 days, after which you can email university.nutanix.com and request that your attempts are reset. Nutanix recommends you utilize the time to thoroughly review this guide and the related references and/or take the recommended training for this exam.

1.11 Exam Security

Nutanix reserves the right to refuse certifying a candidate who violates exam security policies. This includes copying and redistribution of exam material, using any type of study material during the exam itself, attempting to photograph exam items and taking an exam using a false identity. Your identity is captured as part of the exam registration process and must be validated before you will be allowed to take the exam.

1.12 Recertification

Once you have passed the Nutanix Certified Professional – Network & Security 6.10 exam and achieved the NCP-NS 6 certification, it will remain valid for three years.

To maintain your certification status, you must either renew your existing certification, pass an equivalent NCP-level exam within another certification track, or pass the NCM-MCI exam.

1.13 Benefits of Certification

- Digital badge from Credly that you can share on social media
- Access to the Certification store at http://store.nutanix.com for shirts, mugs, and more
- Opportunity to participate as a SME to develop future exams
- Discount on attending Nutanix .NEXT

2. Intended Audience

A candidate for the NCP-NS 6.10 exam and NCP-NS 6 certification has approximately two years of experience in a Network or Security capacity and at least six months of experience with Nutanix Flow.

Successful candidates are typically Network Engineers, Network Administrators, Network Architects, Security officers, or Security Administrators who have experience in deploying, managing, and troubleshooting network virtualization and network security using Nutanix Flow.

Finally, the successful candidate will most likely have taken training courses, such as the Nutanix Network & Security Administration (NNSA) course.

3. Objectives Covered in the NCP-NS 6.10 Exam

3.1 Introduction

It is recommended that candidates have the knowledge and skills necessary for deploying, managing, and troubleshooting network virtualization and network security using Nutanix Flow before attempting the NCP-EUC 6.10 exam. It is also recommended that the candidate complete the training course described in Section 4 prior to taking the exam.

For the NCP-NS 6 certification, candidates will be tested on the following software versions:

- Flow Virtual Networking: version 6.0
- Flow Network Security: version 5.2
- Prism Central: version 7.3

3.2 Objectives

Prior to taking this exam, candidates should understand each of the following objectives. Each objective is listed below; along with related tools the candidate should have experience with, and related documentation that contains information relevant to the objective. Please note that some documentation requires access via the Support Portal. Information on creating an account for use with the Support Portal can be found here.

All objectives may also be referenced in other product documentation not specifically highlighted below. The candidate should be familiar with all relevant product documentation or have the equivalent skills.

Section 1 – Configure Flow Virtual Networking

Objective 1.1: Create a VPC and Overlay Networks

Knowledge

- Determine whether tenant or a transit VPC is required
- Recognize the purpose or usage of ERP in the VPC
- Identify the VPC Gateway nodes
- Associate routed and private CIDRs

References

- Creating a Virtual Private Cloud
- Network Types
- Virtual Private Cloud Management
- Virtual Private Network Connections

- Flow Virtual Networking Architecture
- Attaching a Subnet to a Virtual Machine
- Creating a Policy
- Essential Concepts

Objective 1.2: Create and Manage VPC External Networks

Knowledge

- Determine when overlapping ERPs is necessary
- Associate Scale-out VPC Gateway nodes to a VPC
- Determine when to set the default route
- Determine routes to be set during VPC creation
- Assign a specific Router IP/ SNAT IP to a VPC
- Change the external network for a VPC
- Create a Overlay External Network
- Associate a VPC to a transit VPC Overlay External Network
- Determine when to connect a VPC to a NAT or a No-NAT network

References

- Externally Routable Prefix and IP Addresses
- Requirements and Limitations of Flow Virtual Networking
- Creating a Virtual Private Cloud
- Network Types
- Virtual Private Clouds Summary View
- Connectivity for Flow Virtual Networking User VMs
- Layer 2 Network Extension
- NAT and No-NAT Gateway Scaleout
- Creating Static Routes
- VM and Network Migration
- Creating a Policy
- Connections Management

Objective 1.3: Configure Connectivity Options

Knowledge

- Create network load balancer with a target group of VMs
- Analyze the status of BGP peering sessions, including advertised & received routes
- Define a Policy Based Routing policy to redirect traffic via a security appliance for inspection
- Assign a floating IP address to a workload for external access when using NAT external connectivity
- Create resiliency within BGP neighbors

References

- Floating IPs
- Connectivity for Flow Virtual Networking User VMs
- Attaching the Overlay External NAT Subnet to User VPC
- Virtual Private Network Connections
- BGP Session Details View
- Policy-Based Routing for Redirection
- Border Gateway Protocol Sessions

Section 2 – Configure Flow Network Security

Objective 2.1: Analyze and Document Application Flows

Knowledge

- Determine when monitoring mode is appropriate for policy creation
- Configure syslog to ship logs to an external source for analysis/enable policy logging
- Define and/or update a policy rule set using the flow visualization/captured traffic
- Recognize the purpose and use case for a shared services policy

References

- Security Policy Enforcement Modes
- Flow Network Security Logs and Audits with Syslog

- Applying an Application Policy
- Flow Network Security Application Policies
- Policy Consumption and Visualization

Objective 2.2: Create and Configure Security Policies

Knowledge

- Determine the appropriate policy type based on business needs
- Configure Isolation policies between two or more entities
- Configure Application Policies with appropriate Secured Entities
- Configure Group ID lookup for Active Directory
- Configure VDI Policies
- Explain the use case for the quarantine function

References

- Creating Security Policy with Flow Network Security
- Security Policy Model
- Creating an Application Policy
- Creating an Application Security Policy
- Shared Service Policy
- Isolation Environment Policy
- Creating an Isolation Environment Policy
- Monitoring an Isolation Environment Policy (Visualizing Network Flows)
- Cloning a Security Policy
- VDI Policy Configuration
- Service Insertion
- vNIC Specific Policy using Subnet Categorization
- Configuring Intra-Tier Traffic Rule
- FNS Next-Gen Support for Multi-Prism Central Disaster Recovery
- Entity Groups

Objective 2.3: Manage Policy Lifecycle and Modes

Knowledge

- Create a policy in Monitor mode and identify discovered traffic
- Enforce a policy currently applied in Monitor mode
- Clone a policy and apply to a different Scope
- Identify the number of entities potentially impacted by enforcing a monitored policy
- Describe the different policy lifecycle modes

References

- Cloning a Security Policy
- Security Policy Model
- Security Policy Enforcement Modes
- Application Policy Configuration
- Types of Policies
- Network Configuration Maximums
- Lifecycle Modes for Dark Sites

Section 3 – Troubleshoot Flow Virtual Networking

Objective 3.1: Troubleshoot Connectivity Issues

Knowledge

- Determine why a VM inside a VPC cannot reach the Internet
- Determine why two VMs within the same VPC cannot communicate with each other
- Determine why a VM within a VPC cannot access the external network
- Determine why the BGP neighbor is not receiving expected routes from the VPC
- Identify and resolve network gateway status issues
- Determine if a Gateway VM (VTEP, VPN, or BGP) is unhealthy
- Verify that the subnet extension is active and in a healthy state

References

- Creating a Traffic Mirroring Session
- Service Insertion
- Extending a Layer 2 Subnet Across Availability Zones over VTEP
- PBR-based Tromboning in L2 Extended Subnet
- Isolation Environment Policy
- Requirements and Limitations of Flow Virtual Networking
- Flow Virtual Networking Ports and Protocols

Objective 3.2: Analyze Alerts and Logs to Address Virtual Networking Issues

Knowledge

- Diagnose BGP state using session logs
- Determine which user made a particular change and when
- Analyze IPFIX exports to identify network connectivity issues
- Interpret alerts and take corrective actions

References

- Application Security Policy Configuration
- Troubleshooting Tips
- Prism Central Alerts and Events Reference Guide

Objective 3.3: Analyze the Health of Infrastructure System Components

Knowledge

- Describe how to check the Network Controller's health
- Recognize which actions can be performed (or not) when a Network Controller is unhealthy
- Interpret network controller and Flow Network Security alerts

References

- Network Controller Health Check Attributes
- Network Controller Health Failure Reasons

- External Routable Prefix and IP Addresses
- Prism Element Alerts/Health Checks

Section 4 – Troubleshoot Flow Network Security

Objective 4.1: Troubleshoot Undesired Network Communication

Knowledge

- Determine if desired traffic is being prevented by a security policy
- Verify VM membership in a policy component
- Assess Security Policy Hitlogs to identify allowed and denied traffic
- Identify policy priority conflicts (including prioritization of intra-tier rules vs. inbound/outbounds)
- Determine the root cause of packet loss when service insertion is in use
- Troubleshoot an issue where routes are present but North/South traffic is broken (MTU)

References

- VM Traffic Considerations with Flow Network Security
- Application Policy Configuration
- Service Insertion
- Flow Network Security Logs and Audits with Syslog
- Security Policy Management

Objective 4.2: Analyze Logs to Address Flow Network Security Issues

Knowledge

- Describe how to pipe FNS Security Hit logs to external syslog server
- Determine the status of the conntrack table through NCC healthchecks
- Interpret FNS audit logs to diagnose an FNS issue

References

- Syslog Modules
- Prism Central Logs
- Failure Handling in a Nutanix Cluster

Objective 4.3: Troubleshoot Identity-Based Policy Failure Related to User Group Mapping

Knowledge

- Verify that AD is properly configured (URL, service account, credentials, etc.)
- Enable ID Based Security and configure/manage referenced AD groups
- Validate dynamic category assignment at login time
- Validate that group memberships have been applied to a policy

References

- Creating a VDI Policy
- Security Management using Prism Central
- Configuring a Role Mapping

Section 5 – Deploy and Upgrade a Flow Environment

Objective 5.1: Prepare a Cluster for Flow Network Security

Knowledge

- Enable FNS from Prism Central
- Create categories and associate to VMs
- Confirm versions are supported and up-to-date before enablement
- Identify the resources needed on nodes and Prism Central

References

- Flow Network Security Product Generation and Release Version
- Flow Virtual Networking Configurations
- How to Install Flow Network Security
- Placing the Firmware and Software LCM Bundles on a Web Server
- Security Policy Model

Objective 5.2: Prepare a Cluster for Flow Virtual Networking

Knowledge

- Confirm that network controller is enabled and is the right version
- Ensure all clusters compatible prior to enabling FVN

- Set MTU on virtual switch
- Confirm that Prism Central has adequate resources for the deployment

References

- Flow Virtual Networking Overview
- Requirements and Limitations of Flow Virtual Networking
- Flow Virtual Networking Configurations
- Extending a Layer 2 Subnet Across Availability Zones Over VTEP
- Prism Central Infrastructure Overview

Objective 5.3: Determine Order of Upgrades and Upgrade Paths

Knowledge

- Identify and take actions on incompatible clusters
- Determine if the Network Controller can be updated and identify dependencies
- Determine if the FNS version can be upgraded and identify dependencies

References

- Upgrading the Network Controller
- Updating a Network Gateway
- Prism Central Upgrade in a Nutanix Environment
- Expanding a Cluster

Objective 5.4: Configure Virtual Switches and MTU

Knowledge

- Modify MTU size to allow subnet extension or other features to be used
- Segregate East-West and North-South Traffic
- Segregate UVM and Management and/or replication traffic

References

- Service Insertion
- Virtual Switch Limitations

- Requirements and Limitations of Flow Virtual Networking
- Prerequisites for VPN Configurations
- Enabling Jumbo MTU on AHV for UVMs

Objective 5.5: Configure and Manage User Roles

Knowledge

- Recognize which User roles can and cannot create a VPC
- Create a custom Role
- Limit Custom-Admin to specific VPCs
- Determine the appropriate System defined FNS RBAC role for a given user
- Create an Authorization policy for FNS
- Create an FNS RBAC custom role with granular permissions
- Determine the pre-configured permissions for system defined FNS RBAC roles

References

- Flow Network Security Roles and Permissions
- Control User Access in Flow Virtual Networking (RBAC)
- Built-in Roles List
- Configuring a Role Mapping
- Custom Role Management

4. NCP-NS 6.10 Training Recommendations

4.1 Course Recommendation

Nutanix offers a course that provides training on the objectives tested for in the exam. More information on this course, including delivery methods and pricing, can be found at nutanix.com/training.

The enterprise threat landscape has evolved into one of constant, high-velocity attack activity. Organizations now face approximately 1,900 cyberattacks per week—a number that underscores how critical skilled networking and security professionals are to modern business resilience With cybercrime projected to cost enterprises $10.5 trillion annually by 2025, industry experts who can design, secure, and optimize resilient network architectures are positioned at the center of one of the fastest-growing domains in IT.

For a networking or security professional, these trends present a career-defining opportunity. As the global average cost of a data breach hits $4.44 million, enterprises increasingly seek architects and engineers capable of implementing segmentation, zero-trust strategies, and advanced network governance.

To stay competitive, professionals must not only understand today's threats—they must master the platforms and technologies that enterprises are adopting to combat them. Two such technologies are Nutanix Flow Virtual Networking and Nutanix Flow Network Security, which reduce network complexity and strengthen security posture in hybrid and multicloud environments.

To help you position yourself for success with Nutanix Flow, this course will equip you with the skills and knowledge needed to:

- Prepare an environment and deploy Nutanix Flow.
- Configure various Flow constructs such as virtual private clouds, border gateway protocol sessions, security policies, and so on.
- Configure and manage role based access control (RBAC).
- Identify and investigate common Flow issues.

This course is available online or instructor-led. More information including schedules and how to register can be found at www.nutanix.com/university.

The material provided in the course covers a majority of the objectives (approximately 80%) that appear on the NCP-NS 6.10 exam and is recommended for individuals who want to gain a good understanding of these objectives. Please note that additional exposure to a Nutanix environment is highly recommended.

5. Resources

5.1 Nutanix Community Edition

The Nutanix Community Edition is a free product that allows you to deploy a Nutanix Cloud Platform. To download the software and build your own environment for exam preparation, click here.

5.2 Test Drive

You can also take a 2-hour Hyperconverged Test Drive, which utilizes the Nutanix Community Edition, by clicking here.

5.3 The Nutanix Community

Connect with cloud builders from around the world, learn from IT Pros in your industry and share experiences on the Nutanix Community. The community maintains an area focused on Nutanix certifications, which is located here.

5.4 Additional Network & Security Resources

Find a wealth of additional Network & Security resources here.