NC2 on AWS - Networking
https://squasta.github.io
Updated: 02 05 2025

- **VPC**
  - CIDR range between /16 and /23
    - Within the private IP ranges
    - Min value
      - Recommended /23
      - MCM Portal /23 (MCM Portal)
      - User created /24 [To be Confirmed]
  - Do not use 192.168.5.0/24 CIDR for the VPC to deploy NC2 on AWS
    - All Nutanix nodes use that CIDR to communicate between the CVM and the installed hypervisor
  - Enable DNS attributes
- **VPC endpoints**
  - S3
    - S3 endpoints (Gateway endpoints)
  - EC2
    - EC2 endpoints (Interface endpoints)
- **Subnets**
  - Public subnet
    - CIDR Range between /16 and /25
      - Defaut CIDR of /28 (MCM Portal)
    - Internet access is essential for NC2 on AWS to communicate with the NC2 portal
      - NAT Gateway + Internet GW
      - OR
      - Network Virtual Appliance
      - Proxy
        - For AOS 6.7.1.6 or higher
  - Private management subnet For cluster (AHV and CVM)
    - CIDR Range between /16 and /25
      - Sizing would depend on the maximum nodes and number of cluster(s) planned
      - Defaut CIDR of /25 (MCM Portal)
        - Enough for a 28 nodes cluster
    - Can be Share across multiple clusters for centralized management
  - Private UVM subnets
    - CIDR Range between /16 and /25
      - Subnet sizing depends on the number of user VMs to deploy
      - You can't use or assign the first four IP addresses or the last IP address in each subnet; they're reserved by AWS
    - Dedicated to individual clusters for hosting user VMs
  - Private Prism Central subnet
    - Dedicated to Prism Central for management and orchestration purposes
      - Because you must deploy Prism Central in a separate subnet
    - CIDR Range between /16 and /28
      - Default CIDR of /28 (MCM Portal)
  - When using Flow Networking
    - Needs Prism Central
    - Private Subnet Flow Networking
      - Dedicated to a single cluster for Flow Virtual Networking
      - This subnet cannot be shared and only one cluster can be deployed per VPC with Flow Virtual Networking
      - CIDR Range between /16 and /24
        - Default CIDR of /24 (MCM Portal)
- **Elastic Network Interfaces (ENIs)**
  - Attached to metal instances
    - 1 for Host (AHV) and CVM
    - 1 to 14 for UVMs
  - The cloud network controller (service in the AHV host) helps with ENI creation
- **MTU**
  - By default
    - Maximum transmission unit (MTU) of 1,500 bytes for all the network interfaces
  - When using Flow Virtual Networking
    - The system advertises the MTU of 1442 bytes to UVMs using DHCP to account for the extra 58 bytes used by Generic Network Virtualization Encapsulation (Geneve)
    - Nutanix recommends setting an MTU of 9000 bytes for all the network interfaces of AHV hosts with NC2 on AWS when using Flow Virtual Networking
- **Proxy**
  - VPC Endpoints
- **Ports and Endpoints Requirements [Outbound traffic]**
  - For Prism Central (automated installlation)
    - TCP 80/443
      - *.cloudfront.net
    - Allow downloading .tar extension
      - PC image is a tar file
      - Firewall blocking features
        - Palo Alto
        - Fortinet
        - Cisco
        - Sophos
        - Juniper
  - For CMSP (for Flow Virtual Networking)
- **Routing**
  - Public Subnet with Public Route Table (Public RT)
    - Optional if your Local Route Table has route to a TransitGW or any NVA that allows Internet Access
  - Private Subnets with Local Route Table (Local RT)
- **AWS Load Balancing**
  - To allow internet access to Prism Central or Prism Element on the CVM
    - Can be deployed automatically using Public Access Policy for Prism
  - To Access workload on User VM
- **AWS Security Groups**
  - Network Security using AWS Security Groups
    - Inbounds & outbounds rules
      - Security group referencing
  - Default AWS security groups (Created for each cluster by NC2 portal)
    - Internal management
      - Controls AHV to CVM communication within a cluster
      - Recommendation : Do not modify manually this SG
    - User management
      - attached to
        - ENIs associated with the Management subnet
      - Controls UVM to CVM communication and external communication (administration, with other clusters)
      - Nutanix Prism Element and additional services like replication and data use this security group to allow or deny access to AHV and the deployed CVMs
      - Recommendation : Try to not modify manually this SG in AWS console
        - Access Policy can be setup during or after NC2 cluster deployment in NC2 portal
          - Prism Element
          - Management Services field (SSH, Move, PC...)
    - UVM
      - attached to
        - ENIs associated with the UVM subnet(s)
          - brOverlay0,NoNAT in case of using Flow Virtual Networking
      - Controls external traffic entering or leaving the UVMs
      - Associated tags
        - tag: key=nutanix:clusters:cluster-uuid, value=cluster UUID
        - Tag: key=nutanix:clusters:networks, value=all-uvms
    - Prism Central (PC) (Only if Flow Networking has been selected in NC2 deployment wizard)
      - attached to
        - ENI associated to FVN Subnet (br0.uvms)
  - AWS Custom security groups (to more granularly control traffic to an NC2 environment)
    - Supported on AOS 6.7 or >
      - Only for AHV Native network integration
    - Apply at
      - VPC-level
      - Network-level
      - Cluster-level
    - You must configure Prism Central VM security group and all the UVM security groups in a way that allows communication between Prism Central VM and UVMs.
      - In a single cluster deployment, the Prism Central VM and UVM communication is open by default
      - if your Prism Central is hosted on a different NC2 cluster, then you must allow communication between the Prism Central VM on the cluster hosting Prism Central and the management subnets of the remaining NC2 clusters
    - The default AWS service quota allows you to create a maximum of 5 custom security groups per ENI
    - Ports and Endpoints requirements