Networking

Decide on the following before creating your Frame account:

1. How will your users reach their workload VMs? From the Internet or from a private network?
2. Do you want Frame Control Plane to provision and manage the network where the workload VMs reside ("Frame-managed Networking") or whether you wish to manage the network yourself ("Customer-managed Networking")?
3. Will the workload VMs run in a public cloud or on-premises on a Nutanix AHV cluster?

This guide outlines the differences and tradeoffs between Frame-managed versus customer-managed networking and summarizes the network requirements based on the above choices for Frame and network administrators.

Management Responsibility

Note

Considerations

1. Frame-managed networking is only available when a Frame account is provisioned on public cloud infrastructure.
2. Customer-managed networking is required for Frame accounts provisioned on Nutanix AHV infrastructure.
3. Customer-managed networking is an option for Frame accounts provisioned on customer-managed public cloud infrastructure.
4. Customer-managed networking is not available when using Frame-provided public cloud infrastructure.

Frame-managed Networking

When Frame-managed networking is selected during Frame account creation in public cloud, Frame will provision all **public cloud** networking elements required for the operation of the

platform:

- VPC/VNET
- Subnets
- Routes
- Security groups/firewall rules
- NAT gateway
- DNS
- DHCP
- Load balancer (if required for SGA high availability).

When a Frame account is terminated, Frame control plane will deprovision all network elements it previously provisioned.

> If you attach network elements to the Frame-managed VNET or VPC after the Frame account is provisioned, Frame Control Plane will return an error and not deprovision the network elements when you terminate the Frame account.

Customer-managed Networking

When customer-managed networking is selected during Frame account creation in public cloud or on AHV clusters, the customer is responsible for provisioning and managing all **public cloud** or **AHV** networking elements required for the operation of Frame:

- VPC/VNET
- Subnets
- Routes
- Security groups/firewall rules
- NAT gateway
- DNS
- DHCP
- Load balancer (if required for SGA high availability).

The Frame account creation process requires the following information, which can be obtained from the console of your infrastructure provider. This information dictates where Frame control plane will provision the workload VMs.

Infrastructure	Configuration Parameters
AWS	VPC name and CIDR Subnet name and CIDR Security Group

Infrastructure	Configuration Parameters
Azure	Resource group name VNET name Subnet name and CIDR
AHV	VLAN name
GCP	VPC name Subnet name

Frame will only provision and deprovision virtual machines, volumes, and snapshots.

Requirements

Frame DaaS requires the Frame workload virtual machines (Sandbox, production, test, and Utility server) to be able to communicate with Frame control plane. It also requires end users to be able to communicate with the Frame control plane and the Frame workload VMs. Additionally, for Frame-managed workloads on Nutanix AHV clusters, the Frame Platform must be able to communicate with Prism Element and Prism Central via one or more Frame Cloud Connector Appliances (CCAs), a Frame-provided appliance you deploy in your AHV cluster(s).

Based on your overall configuration (user access, network responsibility, and infrastructure), choose and implement one of the deployment models in Network Requirements.

> If you choose **customer-managed networking**, you must ensure that your networking (CIDR, routes, security group/firewall rules) meets the [network requirements](/platform/networking/requirements) for the deployment model you wish to use **before** you attempt to create a Frame account.

WARNING

FQDN vs. IP Address

Frame protects its control plane from DDoS and external threats using a global content distribution network (CDN) and web application firewall. The public IP addresses associated with the Frame Fully-Qualified Domain Names (FQDNs) may change without notice and vary globally due to this CDN service.

Customers who deploy Frame into a private network (in public cloud or on-premises with AHV) may need to configure their network security appliances to allow Frame workload VMs (and Frame Streaming Gateway Appliances and Cloud Connector Appliances, if required) in their network to communicate with the Frame control plane. These customers are **strongly recommended** to use the Frame Fully-Qualified Domain Names (FQDNs) instead of public IP addresses. Alternatively, they may use an outbound proxy supporting HTTP/HTTPS and Secure WebSocket (WSS) in conjunction with their firewall.

If a customer chooses to use public IP addresses within their security appliances (instead of the Frame FQDNs), customers will need to monitor these Frame control plane DNS records and update their security appliances with the new Frame public IP addresses, if they change.

Revision #7
Created 1 October 2025 04:47:10
Updated 15 January 2026 05:20:14 by Nikola Savic