v1.1 | February 2022 | TN-2118

TECH NOTE

# Nutanix Frame

NUTANIX
YOUR ENTERPRISE CLOUD

# Copyright

# Contents

# 1. Executive Summary

Nutanix Frame is a cloud-based platform that enables customers to deliver virtualized applications and desktops hosted in public or private clouds to end users. End users only need an HTML5 browser on a connected device. Nutanix operates and maintains the multitenant Frame platform, which provides customers with automated cloud resource orchestration, user session brokering, and environment administration. The result is a cloud- and service-based approach to delivering virtual desktop infrastructure (VDI), commonly referred to as desktop as a service (DaaS).

This document briefly covers Nutanix Frame architecture and discusses the key design decisions and best practices that customers, system integrators, partners, and solution architects should consider to successfully deploy and manage their Frame environments. We included details on deploying end-user workloads running in a customer's own public or private cloud account, although customers can configure accounts that run in Nutanix public cloud accounts as part of an all-inclusive service. There are specific articles with additional details at docs.frame.nutanix.com, the central public documentation site for Frame.

 

# 2. Introduction

## Audience

This tech note is part of the Nutanix Solutions Library. We wrote it for customers, system integrators, partners, and solution architects responsible for deploying and managing their Nutanix Frame environments. Readers of this document should already be familiar with Frame account basics.

## Purpose

In this document, we cover the following topics:

- Nutanix Frame architecture.
- Key design decisions and best practices.
- Nutanix Frame deployment details.

Unless otherwise stated, the solution described in this document is valid on all supported AOS releases.

*Table: Document Version History*

| Version Number | Published | Notes |
|---|---|---|
| 1.0 | January 2021 | Original publication. |
| 1.1 | February 2022 | Updated Planning a Frame Deployment and Cost Optimization sections. |

 

# 3. Nutanix Frame Architecture

## Control Plane

Nutanix operates the web-scale Frame control plane responsible for resource orchestration and user brokering, key parts of the Frame service. The Frame control plane (also referred to as the backplane) operates in the cloud and is multitenant. Customers typically register their own public or private cloud infrastructure and use the Frame service to provision workload resources in their infrastructure to deliver virtual applications and desktops to users.

The key components of the Frame cloud control plane include:

**Identity Management Gateway (IMG)**

Integrates with third-party SAML2 and OAuth2 identity providers through configuration. When the user authenticates to the customer's identity provider, IMG validates the claim and passes the authenticated user identity to the Frame Launchpad or Dashboard to determine the user's authorizations.

**Infrastructure as a Service (IaaS) Orchestrator**

Communicates with public IaaS providers' API gateways to provision and deprovision IaaS resources (network, storage, VMs, images) and to turn VMs on and off.

**Cloud Connector Service (for on-premises uses cases only)**

Customers who want to use AHV, AOS, and hyperconverged infrastructure (HCI) on-premises can provision or deprovision AHV resources (network, storage, VMs, images) and turn VMs on and off by using the Cloud Connector Service to communicate with the Prism Central or Element instance in the AHV cluster via the Cloud Connector Appliance (CCA).

 

### Workload Manager

The Workload Manager monitors and manages all public and private cloud workload VMs (sandboxes, production VMs, Utility Servers) and notifies workload VMs when a user needs to be connected to a workload VM.

### Broker

The Broker assigns the user to a workload VM when an authorized user requests a Frame session to access a virtualized application or desktop.

### Launchpad and dashboard

Users access their workload VMs from the Launchpad web application. Administrators use the dashboard to manage their Frame environments.

The following diagram shows these components and the overall architecture of the Frame control plane for orchestrating workloads in both public and private clouds.

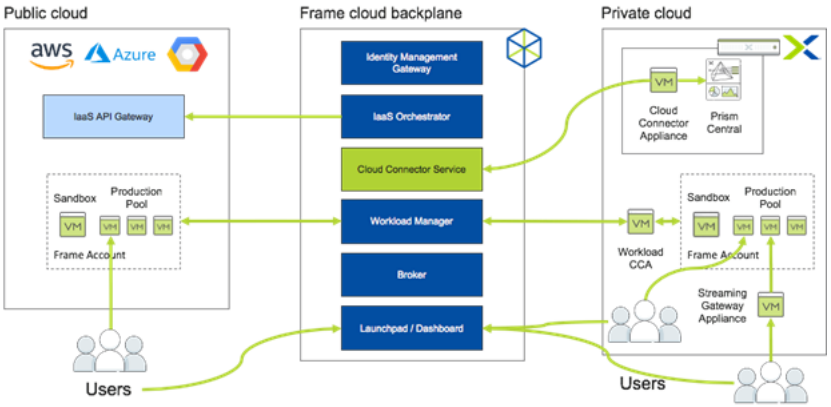


Figure 1: Frame Control Plane Architecture

We designed and built the Frame cloud control plane to be distributed for high availability, scalability, and resilience. Each component comprises multiple workers behind load balancers to eliminate single points of failure, and the workers use a messaging service to communicate. The Frame control plane distributes users into their respective Frame sessions. However, once the user has connected to the assigned workload VM, all communication (display video, audio, keyboard, and mouse events) is between the end user's device (browser) and the workload VM.

 

From a customer perspective, the entire control plane is delivered as a service, which means that they don't need to manage the control plane. The Frame team updates the control plane on a weekly basis, during which customers typically incur zero downtime. If scheduled maintenance requires any downtime, the Nutanix service status page sends notifications to subscribers.

## Account Hierarchy

Each Frame subscription has a hierarchy used to organize administration and access to Frame accounts:

- Customers: The highest tier in the Frame platform. The customer account is essentially the primary account for a single business entity.
- Organizations: The second highest tier in the Frame platform. Many organizations can be listed under one customer, depending on the use case. A business might use organizations to set up unique environments for its different departments or regions. For example, a business can link organizations to different cloud accounts for accounting purposes.
- Accounts: The lowest tier in the Frame platform. Admins use this tier to install and configure their applications in the sandbox (their gold image) and configure their production VMs or one or more instance types. Admins also use this tier to create Launchpads for their end users. When an end user signs in to Frame, they access one of the accounts listed under an organization and any of the workload VMs configured for it. You can't link a cloud account to the account tier, only to the organization or customer tiers.

For more information on the hierarchy and the various administrative roles associated with each tier, see the Frame Platform Hierarchy article.

 

# 4. Planning a Frame Deployment

There are five steps to deploy Frame:

1. Set up infrastructure (compute, graphics, network).
2. Authenticate and authorize users.
3. Install and onboard applications.
4. Configure storage.
5. Deliver to users.

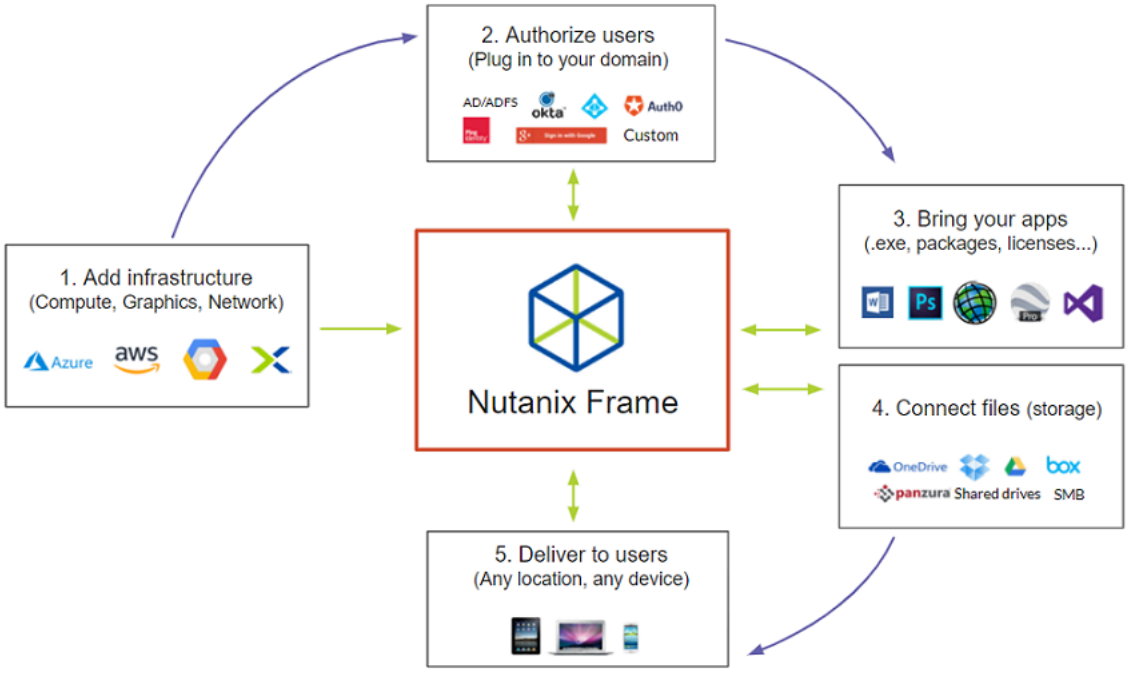


Figure 2: Nutanix Frame Deployment Steps

Nutanix recommends that you first answer the following discovery questions. These questions are encapsulated in the Frame Discovery Workbook (direct download). Your answers to these discovery questions determine your design choices.

 

- Workload profile
  - How many users do you have?
  - Where are the users?
  - What types of applications do you have (CPU, GPU)?
  - What data and files do you need?
  - What is your expected usage pattern (infrequent use, part-time, half-time, full-time)?
- Infrastructure and region
  - Do you need applications close to users or servers?
  - How many regions do you have?
  - Is your deployment on-premises, public cloud, or hybrid?
- Networking
  - How do users access the workload VMs?
  - How do the workload VMs access the internet?
  - How do applications on the workloads access data, files, and application services from the workload VMs?
- Authentication (identity provider)
  - How should users authenticate before accessing protected resources (SAML2, OAuth2 identity provider)?
  - Do you require users to authenticate to Microsoft Active Directory (Active Directory) before they access their Windows applications and desktops?
- Storage
  - Where do users store their personal files?
  - What file shares or file services do users need?

 

- End-user experience
  - Does your deployment only have applications?
  - Do you use nonpersistent or persistent desktops?
  - What are your peripherals?
  - Are you using Unified Communications?
  - Do you want the Frame Launchpad or customer user experience?

## Infrastructure

Each Frame account represents a set of workload VMs: a sandbox (gold template) VM, zero or more production VMs (of different instance types, if required), and zero or more Utility Servers. These workload VMs use a Dynamic Host Configuration Protocol (DHCP). If your customers need to run file servers, domain controllers, application servers, or database servers, Nutanix recommends that you deploy these resources independent of the workload VMs in the Frame account.

Since Nutanix Frame allows customers to deploy Frame accounts in any region, determining which regions to use is critical to the end-user experience and should be based on the answers to the following questions:

- Do you need the virtualized applications and desktops to be close to the users to minimize network latency?
- Do you need the virtualized applications and desktops to be close to the application servers or database servers (client-server) because of your client-server protocol?

If possible, Nutanix recommends that you conduct an experiment to confirm which region works best for your end users.

### Connect to a Cloud IaaS Account

Small businesses or smaller corporate departments can purchase cloud infrastructure through Nutanix. In this case, you don't need to set up a cloud

 

account; the customer admin can simply create an account and choose the preconfigured Nutanix Frame AWS/Azure/Google Account.

This approach has a few limitations, particularly that you can't connect the cloud network to your private network. For this reason, most enterprise customers choose to use their own cloud account to host the Nutanix Frame workloads. This option only takes a few minutes to set up if the customer uses the 30-day Frame trial, as outlined in the Sign Up or Start a Trial Frame document.

If you've prepaid for your subscription through a Nutanix back-end purchase order, you should receive an activation email inviting you to sign in to your my.nutanix.com account and access your paid Frame subscription.

Whether you start with the trial, purchase online, or subscribe through a purchase order, the configuration and connection to your cloud account is the same. Follow the instructions for your cloud provider to register your cloud subscription to your Frame customer entity:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

### Use On-Premises Datacenter Infrastructure with AHV

If you want to use your own on-premises infrastructure, there are several additional considerations. However, you can manage both on-premises and cloud workloads from the same Frame control plane and management interface. For details on setting up Frame with Nutanix AHV, see the Frame on Nutanix AHV article.

## Networking

Since Nutanix delivers Frame as a service, the Nutanix-operated control plane runs in the public cloud. Users and workload VMs must be able to reach the control plane, and the control plane must also be able to communicate with the workload VMs, regardless of whether the workload VMs are in public cloud

 

infrastructure or on-premises with Nutanix AHV infrastructure. The network architecture you choose depends on:

- How users access the workload VMs (inbound).
- How applications on the workload VMs reach the internet (outbound).
- Whether you want public cloud infrastructure or Nutanix AHV infrastructure (on-premises).

For public cloud infrastructure deployments, the customer can have the Frame platform automatically provision Frame accounts using one of three different network architectures:

**Public (default)**

The quickest way to deploy a Frame account. However, all workload VMs have public IP addresses, all ingress traffic connects directly to the workload VMs, and all egress traffic goes through the internet gateway on the virtual private cloud (VPC).

**Private networking**

All traffic inbound to and outbound from the workload VMs must route through the customer's existing private network (for example, a shared VPC or on-premises network). If the workload VMs must communicate with the internet, the traffic must go through the customer's security stack or a NAT gateway.

**Streaming Gateway Appliance (SGA) + private networking**

Inbound traffic from the internet must flow through a reverse proxy (SGA) to reach workload VMs. Only the SGA has a public IP address; all workload VMs have private IP addresses. All outbound traffic from the workload VMs must route through the customer's existing private network to the internet.

The following table illustrates the choices for network architecture based on the customer's requirements.

*Table: Network Architecture Configuration Options*

 

| Communication Direction | Communication Type | Public (Default) | Private Networking | Streaming Gateway Appliance + Private Networking |
|---|---|---|---|---|
| Inbound | From internet only (public IP address per VM) | Yes | No | No |
| Inbound | From internet only (only one specified public IP address) | No | No | Yes |
| Inbound | From private network only | No | Yes | No |
| Inbound | From both internet and private network | No | No | Yes |
| Outbound | Directly to internet with public IP address per workload VM | Yes | No | No |
| Outbound | Through NAT Gateway or existing security stack on private network | No | Yes | Yes |
| Outbound | Prohibited | No | Yes | No |

With Frame, you can also provision Frame accounts in an existing VPC or Azure Virtual Network (VNet; BYO networking). In this model, the customer is responsible for all network routing and security groups.

For AHV infrastructure deployments, specify the VLANs that Frame provides to its workloads. The customer is responsible for all network routing and security in their on-premises network.

 

Note: All Frame accounts created on AHV infrastructure follow the private networking or SGA + private networking deployment models.

For additional information about the different networking architectures and how to create Frame accounts with those network architectures, refer to these documents:

- Network Configuration Requirements
- Create Accounts

### VPC Requirements

The VPC that Frame uses to provision account workloads must have enough IP addresses for a sandbox VM, the customer's Utility Server VMs, and the customer's production VMs. Unless you enable the quick publish feature, the IP address range must also account for another set of production VMs provisioned from the sandbox gold image during publishing. A good estimate of the total number of IP addresses you need is 220 percent of the sum of the max capacity set for each production pool for the Frame account.

Additionally, the VPC must provide (or provide access to) a DHCP service in order for the workload VMs to obtain dynamic IP addresses during provisioning and boot. The VPC must also provide DNS to enable workload VMs to resolve Frame's fully qualified domain names (FQDNs).

Refer to the Network Configuration Requirements document for details on the required network ports and protocols for the three primary network architectures used. See the networking section of the Frame documentation for additional network management details.

## Authentication and Authorization

### Identity Management

With Frame, customers are responsible for identity management and user authentication. Customers can integrate one or more identity providers under their Frame customer entity to authenticate users. Once the user authenticates to the identity provider, they're authorized based on Frame's customer-defined authorization rules before they can access Frame-protected resources.

 

Nutanix recommends that you use an enterprise-grade SAML2 (preferred) or OAuth2 identity provider with multifactor authentication (MFA) mechanisms. These include:

- SAML2 providers (for example, Microsoft Azure Active Directory, Active Directory Federation Services, Okta, PingFederate, and Centrify).
- G Suite identity integration (SAML2 or OAuth2).

For customers who need a simple identity provider, Frame provides a built-in username and password identity provider. However, this built-in identity provider doesn't support MFA or custom password policies. It may be helpful to start with the basic included identity provider for initial setup and testing and then integrate with one of the identity providers mentioned and covered in our user management guide.

> Note: For Frame admin API integrations, Nutanix Frame requires that requests be signed with RESTful API in order to authenticate them. A client ID and client secret must be obtained from the API authentication provider with the appropriate authorization rules defined.

In general, customers should add their identity providers at the customer entity level so that customer, organization, and account levels can use the configured authentication provider. Managed service providers may choose to add an identity provider at the customer entity level and provide customers with the option to add their own identity providers at the organization level. This setup enables managed service providers to both control employee access and enable customers to manage their end users independently.

For more information about Frame's built-in and SAML2 or OAuth2 identity providers, see the User Management documentation. For more information on API authentication, check out the Nutanix Frame Admin API documentation.

Once end users have access to a Frame Launchpad, they can launch an application or a desktop. The VM they connect to doesn't have to be domain joined. Most use cases don't require domain-joined VMs, but if yours does, refer to the Windows Active Directory section for requirements and guidelines.

## Windows Active Directory

Customers use Windows Active Directory to enforce specific group policy objects (GPOs), map network drives or printers, and automatically authenticate

 

users when they run specific applications. For these use cases, customers can configure their Frame accounts for domain-joined VMs. When you turn on domain joining, Frame directs the provisioned production VMs to join themselves to the enterprise Windows Active Directory. You can manually join the sandbox and Utility Servers to the Windows domain. Domain-joined VMs require users to authenticate to the Windows domain before they access their virtualized applications and desktops.

You need the following to join the production VMs to the Windows domain:

- Organizational unit (OU) and its distinguished name. It's best practice to have a separate OU for Frame.
- GPO inheritance blocked. It's best practice to block GPO inheritance at the start and enable GPOs selectively.
- Service account username and password. It's best practice to set the Active Directory password to never automatically expire. Instead, use a coordinated password rotation schedule with Active Directory and the Frame domain settings.
- Domain name (FQDN).
- Domain controller IPs or FQDNs.
- DNS (primary and secondary).

> Note: Customers who enable Windows Active Directory have users authenticate to the SAML2 or OAuth2 identity provider and then authenticate again when they start a Frame session. A feature that allows administrators to have their users authenticate only once to Windows Active Directory and securely preserve the user's domain credentials for subsequent Windows sign-ins is on the Frame roadmap.

For more information on domain-joined instances, read the relevant section of the Account Management documentation. We also have documents on domain controller preparation and domain-join setup.

## Authorization

With Frame, customers can use role-based access control (RBAC) authorization rules to determine which authenticated users can access which protected resources. Frame provides four administrator roles and one user role. As part of

 

the authorization rule, the administrator defines which user has a specific role on a specific resource (customer entity, organization entity, account entity, or Launchpad entity).

When integrating a SAML2 identity provider, customers should configure their identity provider to provide group attributes so that they can define the SAML2 permission (authorization) rules using the user's group attributes instead of individual user email addresses. This method simplifies SAML2 permissions.

## Install and Onboard Applications

### Account Type

Before you create your first account, you need to know whether you're going to use persistent or nonpersistent desktops. In a typical Frame account, sessions are nonpersistent or stateless, which means that all changes made to an instance are wiped from the instance after the session is closed. The instance is then returned to a pool where it waits to be served to the next user.

Frame also offers persistent desktops. Persistent desktops are stateful, desktop-only instances permanently assigned to an individual user. Users are given administrative control over their own desktop—they can install and manage their own unique application sets and settings in their own persistent environment. Account administrators can still monitor usage and basic session activity through the account dashboard.

If you want to use persistent desktops, refer to the persistent desktop section of the Frame documentation before you create an account.

If you plan to use nonpersistent desktops, refer to the steps described in these links:

- Create an account by selecting a region and your default machine type.
- Install and onboard your applications in the sandbox—your gold image for the account. As part of this step, you need to understand how your applications are licensed. See this overview for a description of various approaches.
- Set capacity for your production pool of VMs.

 

- Publish your apps to your production pool with one click that automatically copies your primary VM to your production pool.
- Set up a new Launchpad to configure which applications your users have access to or whether they should have access to the whole desktop.
- Set up session settings to configure how your sessions run.

The following sections take a closer look at the key considerations for these steps.

### Base OS Image

Customers start with a base operating system (OS) image provided by Nutanix for public cloud deployments. These OS images are standard for each cloud provider with the addition of a preinstalled Frame guest agent and Frame-specific OS settings such as Windows Registry keys. When you create a Frame account, Frame clones the base image to create the account sandbox, the gold image VM customer administrators use to manage their Frame account images. Each Frame account has one sandbox.

### Maintain Images

The customer installs, manages, and licenses applications and the OS after they create the Frame account. Customers have two options for managing their gold image:

- Install, update, and delete applications and update the OS manually.
- Use third-party management solutions such as Microsoft SCCM, Puppet, or Chef.

In terms of disk size, Nutanix recommends that you don't increase the sandbox disk size unless absolutely necessary. Once you increase disk size, it's extremely difficult to shrink the disk. Total storage consumption depends on the combination of the sandbox disk size and the number of production instances you want to provision.

Consider setting up both a test and production environment (two Frame accounts) to maintain and test the image before you release it to production. Once you validate the image, you can clone it from the test sandbox to the

 

production sandbox and initiate a publish operation in the production sandbox to make the image available to all production instances and your users.

## Publishing

This section discusses the key decisions that affect the publishing process. Customers make an image available to users by publishing it. In a publishing event, Frame takes a backup of the sandbox image (in case the administrator wants to restore the image in the future), provisions the required number of production VMs, and attaches a clone of the sandbox image to them. If you want to join the production VMs to the Windows domain, run sysprep before you provision the production VMs to generalize the image.

> Note: The number of production VMs equals the sum of the max capacity setting for all production pools (instance types) in the Frame account.

> Note: If a Frame account configured for domain-joined instances fails to publish, sysprep is often the cause. Troubleshoot sysprep to determine if you need to modify the unattended.xml (answer file).

### Nonpersistent versus Persistent VMs

For Frame accounts configured for nonpersistent VMs, the publish operation replaces all production VMs with the new image so all users have access to the latest image. Any users in session aren't affected by this publishing process.

> Note: With nonpersistent VMs, you should disable any auto-update features in applications. Updates don't persist from session to session, and the downloads impact performance.

For Frame accounts configured for persistent VMs (persistent desktops), the publication operation only updates the image for newly provisioned persistent desktops. Persistent desktops provisioned and assigned to users prior to the publish operation aren't affected. Customers must use existing desktop management software tools to manage and update persistent desktops.

### Quick Publish versus Publish

By default, when an administrator publishes the sandbox for a Frame account, Frame uses the updated sandbox image to provision a new and duplicate set of VMs, known as the shadow pool. The number of new VMs in the shadow pool is the same as the number of production VMs. Once you've provisioned all the

 

shadow pool VMs, Frame marks the shadow pool VMs as the new production VMs and deletes the old production VMs. With this approach, you need twice as many VMs during the publishing process, which can cause you to run into your service limits (unless you increase them). The advantage of the default publishing process is that all new sessions use the new production VMs once they're published.

If your service limits are less than twice the number of max VMs for all production pools, the administrator can use the Quick Publish feature. With Quick Publish, Frame uses the sandbox image to provision a set number of new VMs for the shadow pool, typically fewer than the sum of the max VMs for all production pools. Once you've provisioned the shadow pool VMs, Frame marks them as new production VMs and terminates the old production VMs. Frame continues to incrementally quick publish until all old production VMs are replaced with new production VMs. The advantage of this publishing process is that peak capacity is much lower. However, users can still access the old production VMs while Frame is incrementally publishing.

### Production Pools

Frame supports various GPU and CPU instance types. You can find the latest supported instance types on the Frame pricing page.

With nonpersistent Frame accounts, administrators can publish the same sandbox image to one or more production pools, each associated with a specific instance type. At any time, customers can increase or decrease the capacity of a specific production pool by changing the max number of VMs under Default Capacity on the dashboard. Customers can also increase or decrease the capacity of a specific production pool using a Frame Admin API endpoint:

```
POST /pools/\${pool_id}/elasticity_settings
```

For more information on managing capacity, see the capacity management section of the Frame documentation.

 

## Storage

With Nutanix Frame, customers can select a storage approach from a wide range of options based on their desired user workflow and existing or future storage requirements. Choosing the right storage option for specific use cases and unique workflows can be challenging. Nutanix recommends choosing a storage solution based on the answers to the following questions:

- Where are you currently storing your data and files?
- Do users have to authenticate to the enterprise Windows Active Directory to access their files?
- What applications depend on these files?
- Do your users need to collaborate on the same files at the same time?
- Where are your users located?
- What size are the files your users typically open and save?
- How long does it currently take for your users to open and save files?
- What are your current and projected storage capacity needs?
- Are you going to implement a cloud storage strategy or keep your files on-premises?

The following sections summarize the most popular storage options. The data management section of the Frame documentation has more information.

### Local Device Storage

Uploading and downloading files to and from the Frame session is the simplest option for users to access their files through Frame. Users drag and drop files from their local file explorer into the Frame session. The file is then automatically uploaded into a dedicated Uploads folder in the session. The uploaded file persists in the VM until the session ends. This solution also allows your users to download files from their Frame session to their local machine by saving or dragging the desired files in their Frame session into the Download Now folder of the Frame system.

 

Using files from the user's local device with Nutanix Frame as a storage solution has the following benefits:

- This solution is supported out of the box and requires no additional setup.
- This solution is user-friendly and simple to use.
- There are no associated costs with this solution.

Nutanix recommends this solution if users don't have a cloud storage account and require access to some of their local files. Nutanix doesn't recommend this solution for scenarios where users need repeated access to large files or a large quantity of files. The upload and download option is best suited for short-term use unless you're using it with persistent desktops.

For more information, see the Upload/Download section of the Session Features documentation.

## Cloud Storage

Nutanix Frame integrates with four leading cloud storage providers: Box, Dropbox, Google Drive, and Microsoft OneDrive. In the Frame environment, you can use cloud storage as a shared drive between Frame team members or team members can access their own individual cloud storage accounts. These Frame integrations don't sync the whole cloud storage drive, but instead use a filter driver to intercept interactions with the user's cloud storage provider and make their files available on demand. Once a user interacts with a file, the Frame cloud storage driver in the workload VM immediately begins to transfer the file to a temporary folder on the workload VM's local disk for the user. Once the user saves the file, the cloud storage driver transfers the file back to the user's cloud storage.

For users who use Google shared drives and want higher performance, Nutanix recommends installing Google File Stream in the gold image. With Frame enterprise profiles, the Google File Stream session can persist across user sessions.

Using cloud storage drives as a storage solution on Nutanix Frame provides the following benefits:

- Cloud storage is easy to mount and unmount.

 

- Your end users manage the integration.
- File transfers are prompt and streamlined since the Frame session is connecting to another cloud service.
- Files are synced to the Frame session only as they are accessed by the user, which minimizes resource consumption.
- You can manage cloud storage capacity through the cloud storage provider.

This solution is applicable to many workflows and use cases for organizations already comfortable with cloud storage. We recommend this option if the customer hasn't established a storage solution yet and has a small to moderate amount of data. We don't recommend it for organizations that depend on simultaneous collaboration or frequently work with large files.

See the Cloud Storage/Network Share Drives section of the Session Features documentation.

### Nutanix Frame Personal Drive

Frame provides fast, privately hosted network storage for each Frame user in the form of a Personal Drive. Personal Drives rely on cloud storage (standard storage) and are mounted as mapped network drives (P: for the drive letter). Administrators configure the initial size of Personal Drives for their users and are given the option to enable autogrow settings. Autogrow settings are a set of customizable parameters that instruct the IaaS provider to automatically increase the storage capacity of each volume when a user begins to run out of free space. Personal Drive integrates differently with Frame depending on the infrastructure provider. End users can manage their own backups from their profile page, accessible from the Launchpad interface. Using Frame's Personal Drive feature as a storage solution provides the following benefits:

- Personal Drive provides per-user, dynamically scaled storage you can use with any workflow.
- End users can manage Personal Drive backups from their My Profile page.
- Administrators can schedule automatic backups for Personal Drives and set the retention duration directly from the Dashboard interface.

 

- Data is encrypted and stored in the cloud account.
- The Personal Drive is in the same VPC as the VM the user accesses, so you can expect better performance than if the user accessed the files from cloud storage or on-premises through a VPN gateway or interconnect.

This storage option is best suited to customers who want each authenticated user to have their own personal drive space managed by Frame.

### Nutanix Frame Enterprise Profiles

If you use the Frame Enterprise Profiles feature, each user gets their own dedicated volume that persists settings and personal preferences. These preferences include all files in the user's My Documents folder, so if you choose to implement Enterprise Profiles, you don't need the Personal Drive. As with Personal Drive, data from Enterprise Profiles is encrypted and stored in the cloud.

### Frame Utility Server as a Storage Server

From their dashboard, administrators can provision and configure a Frame Utility Server as a dedicated storage server. Admins can set up file shares that are available to end users as mapped network drives. Users can access the Utility Server from the account dashboard, and the Utility Server is stateful, so data persists on its VM as it does on an on-premises file server. Utility Servers are typically turned on to ensure that files are available to users whenever they need them.

Using a Utility Server as a storage solution provides the following benefits:

- Data is stored in the same VPC as the sandbox and production VMs, which makes this solution very efficient.
- Users always have access to the same file share, which is beneficial for use cases that require heavy team collaboration.
- You can configure and modify Utility Server system specifications at any time to meet your workflow requirements. Administrators select image family, VM type and size, and storage size (similar to sandbox configuration) at creation.

 

- The administrator can increase storage capacity at any time from the dashboard.
- Administrators can configure scheduled backups for Utility Servers for data redundancy.

We recommend this option if your users or applications require access to one or more shared files. This option is appropriate for workgroups and as a team drive. Don't use it if you need an enterprise-grade file storage solution.

For more information on configuring Utility Servers as network drives, read KB 9014: How to Create a Mapped or Network Drive from your Sandbox to a Utility Server.

### Existing Windows File Server

With Frame, customers can keep their data in their existing Windows file servers on-premises or in an existing VPC. The on-premises file server is a customer-managed file server that Frame users access from the workload VM through a VPN tunnel or over a private connection. Windows file servers in an existing VPC or VNet are customer-managed file servers that users access over a VPC network peer. In both cases, these file servers typically require user authentication to the customer's Windows Active Directory.

Using your existing Windows file server provides the following benefits:

- Allows you to use your established Windows storage servers.
- Removes the need to replicate file storage.
- Once the user authenticates to your Windows Active Directory, the user can see the mapped network shares in their Frame workload VM, corresponding to one or more network shares from one or more file servers based on Windows domain policies.

This solution is appropriate if you've made substantial investments in Windows file servers or have substantial data in Windows file servers.

If your Windows file server is on-premises, opening and saving large files might be slower than opening and saving files locally from on-premises workstations, because the files are copied from your on-premises file server to the cloud

 

and back again. Performance depends on the geographical distance, network bandwidth, and latency characteristics between the cloud VPC and the Windows file server.

### Cloud-Backed Global File Synchronization and Locking NAS

Customers with globally distributed users or many mobile users often need to collaborate on common file sets. These users need to be able to quickly read and write from any location at any time and need to edit files without other users writing to (and possibly corrupting) the same files. Additionally, globally distributed users must be able to consistently access their data, regardless of where they are or which file server they access. Users want the same overall performance they expect when they open and save files to servers in the same LAN. Customers with these requirements often use storage solutions that support multisite and cloud access with real-time global file synchronization and locking capabilities, such as a cloud-backed global file system with file synchronization and locking. Using this type of storage provides the following benefits:

- Users have a consistent view to all files on the global file system no matter where they are located.
- File open and save actions are performance optimized using data deduplication, caching, and compression for opening from and saving to cloud-backed storage.
- This solution syncs file changes in real time across the global file system.
- This solution uses file locking to ensure collaboration and file set consistency.
- All files are backed-up and archived securely in the cloud.

Nutanix recommends this storage solution for situations where users are geographically dispersed, need to collaborate on the same files, operate from two or more offices, or require efficient global file synchronization.

Relevant Google Cloud partners:

- Panzura
- Nasuni

 

### Backups

In addition to primary storage for user data, you can also back up your sandbox and Utility Servers to manage versions of your images. Utility Servers are general purpose servers you can add to your Frame environment for a variety of use cases beyond storage, such as to serve licenses for application software.

## Deliver the End-User Experience

When you design the solution architecture, define your desired end-user experience in terms of the type of Frame account you want to provision and how you want end users to access their applications and desktops and work with their data and files. You may just want to provide a URL or identity provider chiclet and point users to the End User System Requirements section of the Frame documentation.

However, there are often additional considerations you need to review for your deployment. For example, if they use Frame APIs, users can navigate to a website and click a button to launch an application (skipping the Launchpad entirely). Or they can click an icon in the Chromebook shelf to launch apps directly. The following sections take a closer look at these and other considerations for delivering the end-user experience.

### Frame Account Types

Frame enables customers to deliver three primary experiences, as described by the following table. The most common experience is a virtual desktop using a standard image (maintained by the customer administrator).

*Table: Frame Experience Options*

| Desired Experience | Nonpersistent Frame Account | Persistent Desktop Frame Account |
|---|---|---|
| Access individual applications | Yes | No |
| Use virtual desktop using standard image | Yes | No |

 

| Desired Experience | Nonpersistent Frame Account | Persistent Desktop Frame Account |
|---|---|---|
| Provide virtual desktop where users can maintain their own applications | No | Yes |

Note: Once you create a Frame account, you can't change the account type.

## User Workflow Options

Customers can choose how their users access their applications and desktop based on which options from the following table they want most.

### SAML2 permission configuration

With the default end-user experience of going to a Launchpad and connecting to a Frame session, administrators can configure their SAML2 permissions to authorize users to a specific Launchpad associated with a specific Frame account in a specific datacenter. Administrators often associate users to specific groups in their identity provider and pass the group claims to Frame. You could authorize a group of users to one Launchpad if the group isn't moving from one region to another. However, if the group is moving from one region to another, you can authorize it to more than one Launchpad in two or more datacenters.

### App or desktop launch URLs

If you want to direct users to a specific datacenter from your webpage, you can use app or desktop launch URLs. You can embed these URLs, obtained from the appropriate Launchpad under Advanced Integrations, in your website with an explanation of where to go. An example of a custom webpage is KPF's website: https://desktop.kpf.com/.

### Frame session API implementation

You can also use a custom implementation of the Frame session API where your webpage first verifies the latency to the cloud regions with Frame accounts, then automatically directs the user to the appropriate Frame account. The end-user workflow is completely up to you.

 

Selection depends on the end-user experience and implementation effort you want.

*Table: Platform Access Considerations*

| User Workflow Option | Advantages | Disadvantages |
|---|---|---|
| Application* or desktop Launchpad | Out-of-the-box capability, users can switch to other Launchpads, if allowed; users can change instance type on the Launchpad on the fly, if allowed. | Users must access applications or desktop from a standard Launchpad and can't change the URL in the location bar. |
| Application or desktop launch URL | Out-of-the-box capability, customer can insert launch URLs in any web page; after authentication, users go straight to the application or desktop; customers can implement Secure Anonymous Tokens to eliminate the identity provider integration. | The customer hosts the application or desktop launch URL; can't change the URL in the location bar. |
| Full custom user experience with Frame session API | Control the entire Frame session from start to finish; customize user experience with customer's own implementation of Frame session API. | Customer must have JavaScript developer resources to develop and maintain their custom workflow and integrations. |

Note: * Application Launchpads are only available for nonpersistent Frame accounts.

## Session Settings

You can further govern end-user experience with session settings, which are a set of configuration options that cover cloud storage integrations, copy-paste (bidirectional, unidirectional, or none), file upload and download, printing, microphone usage, and session time limits. You define these session settings at the account level, sandbox and Utility Server levels, and for each Launchpad.

 

Pay particular attention to the session time limits, as these parameters determine how long a user can remain in a session, how long a user can be inactive before they're disconnected from their session, and how long a user can be idle (after they're disconnected) before their session is closed.

## Performance

Users of virtualized applications and desktops are highly sensitive to increases in latency (keyboard events, cursor movement, and mouse button registration) and degradations in application responsiveness. Customers and solution architects must consider the following performance parameters to design an optimal end-user experience:

- Location of the workload VMs
  - Close to the users?
  - Close to data and application services?
- Instance types
  - How many vCPUs?
  - How much memory?
  - How much GPU power?

### Multiple Datacenters

Each Frame account is associated with a single cloud region. You may need to conduct a set of tests to determine the best cloud region for the workload VMs. Depending on the specific use case and test results, you can deploy your applications in one or more cloud regions to achieve the optimal balance between network latency and application interactions with data sources. For example, in the case of client-server applications, you might need to locate client applications that rely heavily on networked data sources or application services closer to the data sources than to the end users.

Once you create the Frame accounts in different cloud datacenters, administrators have several options for directing users to the closest datacenter, as detailed in the User Workflow Options section.

 

### Instance Types

To ensure application responsiveness, you must establish the appropriate instance configurations your users should use. The following table summarizes the most common instance configurations and their workloads.

*Table: Common Instance Type Configurations*

| Instance Configuration | Example Applications |
|---|---|
| 2 vCPU, 8 GB of memory | Microsoft Office, ERP clients, accounting, Adobe Creative Suite, Autodesk AutoCAD 2D |
| 4 vCPU, 16 GB of memory, GPU | Autodesk AutoCAD 3D, Maya, Revit, Inventor, ArcGIS Pro, video animation, editing |

### Display Resolution and Frame Rate

Nutanix Frame uses an H.264-based protocol to stream the display to the end user's browser. For non-GPU instance configurations, Frame relies on the CPU to encode the H.264 video stream. The following table summarizes the maximum display resolutions and frame rates that CPU-only and GPU-enabled instances can support. If you want to use multiple monitors with non-GPU instances, we encourage you to use instances with more than 2 vCPU to support encoding multiple H.264 video streams.

*Table: Instance Display Details*

| Instance Configuration | Display Resolution (pixels) | Frame Rate (frames per sec) |
|---|---|---|
| CPU instance types | Up to 1,920 × 1,080 | Up to 20 |
| GPU instance types | Up to 3,840 × 2,160 | Up to 60 |

### Network Bandwidth

Since the end user streams their virtualized application window or desktop to their browser from the cloud, you need to evaluate your existing network bandwidth capacity and usage once Frame is running. Frame remoting protocol constantly adjusts the network bandwidth consumption based on display resolution, frame rate, and what actually changes on the application window or

 

desktop. If there are no changes to the display, the bandwidth consumed drops to nearly zero.

The following table provides high-level guidance on average bandwidth consumption per Frame session based on the applications used, VM instance type (CPU-only or GPU-backed), display resolution, and frame rate.

*Table: Session Bandwidth Consumption Rates*

| Average Bandwidth (Mbps) | Applications | Instance Type, Display Resolution, and Frame Rate |
|---|---|---|
| 1 | Office productivity applications | CPU-only, up to 1,920 × 1,080, up to 20 fps |
| 5 | CAD applications | GPU, up to 1,920 × 1,080, up to 60 fps |
| 10 | Video editing/animation/ sustained playback | GPU, up to 1,920 × 1,080, up to 60 fps |
| 20 | Video editing/animation/ sustained playback | GPU, up to 3,840 × 2,160, up to 60 fps |

Note: When the user enables the microphone, they need 200 Kbps of additional bandwidth because the browser encodes and sends the audio from the user's microphone to the remote VM.

### Windows Sign-In Optimizations

If you want to join the production workload VMs to your Windows domain, you need to ensure that the time from when the user enters their domain credentials to when the application or desktop is available is as short as possible. The sign-in time is a function of multiple factors:

- Computer and user GPOs
- Windows services startup
- Application services startup
- Network shares
- Custom startup scripts

 

We encourage you to optimize your image and GPOs by disabling unnecessary Windows and application services and setting the workload VM to ignore irrelevant GPOs during the sign-in process. If you don't optimize carefully, the Windows sign-in can cause poor end-user experience and resistance to solution adoption.

 

# 5. Cost Optimization

Delivering virtualized applications and desktops from the cloud enables you to use the global reach, high-performing networks, and elasticity of the public cloud to match demand. You must actively manage your workload usage and right size your production pools to match cloud consumption with actual usage.

## Elasticity

Once you deploy a Frame account, determine the maximum number of concurrent users needed. With Nutanix Frame, administrators can optimize nonpersistent Frame accounts to support:

- The maximum number of concurrent users per production pool.
- The number of VMs per production pool that are powered on and available for user sessions. Having powered on and available VMs minimizes the time a user waits to connect to a Frame session (because the user doesn't have to wait for the VM to start).

Using the capacity management features as described in the capacity management section of the Frame documentation (or using a Frame Admin API endpoint), administrators can set the number of concurrent users in each production pool to support the concurrent number of users in Frame sessions while controlling both storage (when VMs are provisioned) and VM usage costs.

The following figure shows an example of the default and active capacity configurations.

 

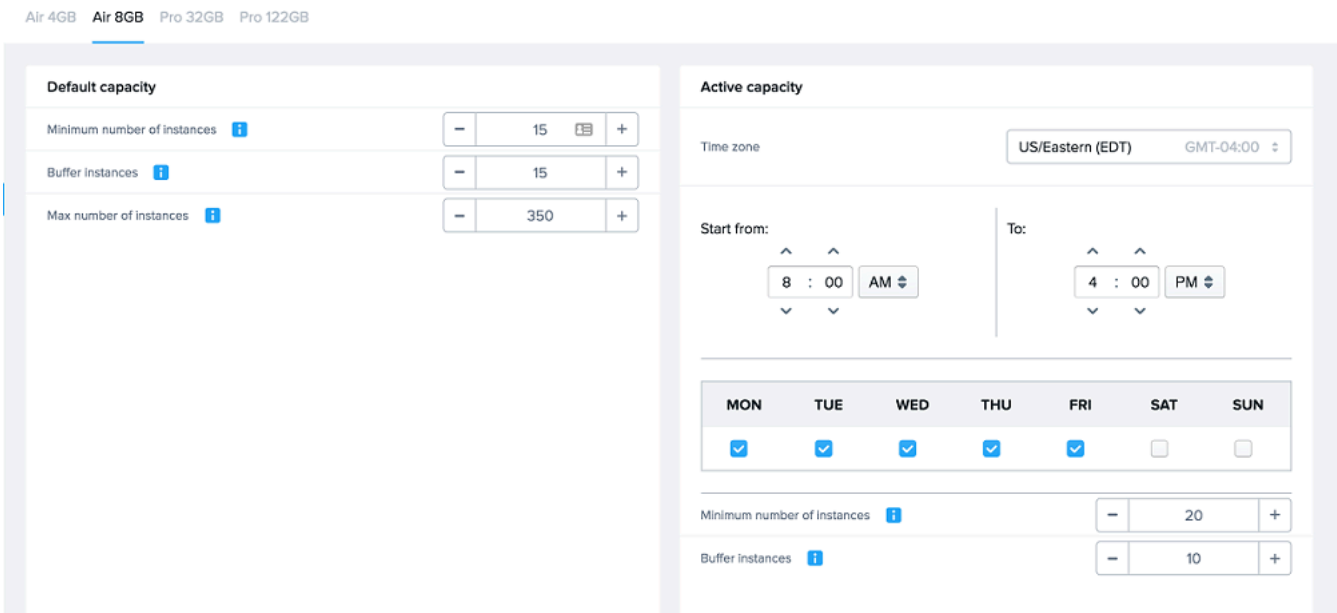


Figure 3: Default Capacity Configurations in a Standard Frame Account

In this example, the administrator configured 350 Air 8GB instances and ensured that at least 15 of these instances are always on. Additionally, the administrator configured 15 buffer instances, which are simply additional VMs that are ready for access at any time. The administrator has configured active capacity settings to ensure that at least 20 VMs are turned on, with a buffer of at least 10 additional VMs turned on and waiting for users from 8 AM to 4 PM Eastern Time.

With the elasticity graph, the administrator can verify whether the maximum number of VMs in a production pool is sufficient for the actual peak number of concurrent users. In the following example, the administrator can adjust the max from 350 down to 250 and still have plenty of capacity. This change removes the storage cost for the 100 deleted production VMs. The administrator could also reduce the minimum and buffer to zero during the weekends, so that weekend users have to wait for a VM to turn on. This adjustment reduces the VM hours the customer must pay for when there are no weekend users.

 

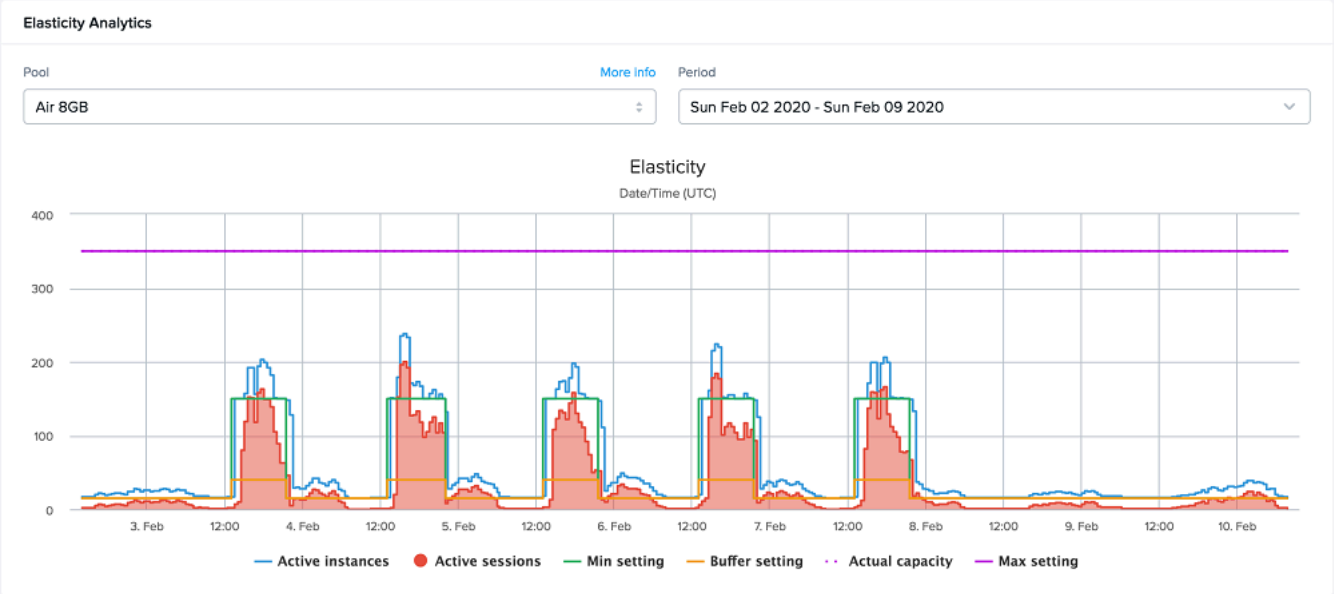


Figure 4: Elasticity Analytics View from a Standard Dashboard

Administrators can also adjust the inactivity, idle, and max session time settings in session settings to ensure that Frame closes sessions and turns off VMs as desired.

## Preemptible Instances

Because preemptible instances allow Google Cloud Platform to "terminate (preempt) these instances if it requires access to those resources for other tasks" (Google Cloud, "Preemptible VM instances"), preemptible instances aren't applicable to virtual application and desktop delivery situations. Consequently, Frame doesn't support preemptible instances on any infrastructure.

 

# 6. Conclusion

Nutanix Frame is a secure cloud platform that delivers applications, desktops, and software-defined workspaces to users. Users only require a connected device with a modern web browser. It's a public cloud-native platform that's been adapted for use with private cloud (AHV) contexts. Nutanix Frame is infrastructure as a service (IaaS) and provider-agnostic, so organizations can run on Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), or their on-premises Nutanix AHV cluster through a single management console. Using Nutanix Frame, organizations can automatically provision and deprovision capacity worldwide and across IaaS providers to adjust for fluctuations in end-user demand.

If you feel stuck, unsure, or have questions, Nutanix is always available to help. You can submit support tickets through the my.nutanix.com Support Portal (see how to create a support case).

For feedback or questions, contact us using the Nutanix NEXT Community forums.

 

# 7. Appendix

## References

1. Official Nutanix Frame Documentation
2. Frame Knowledge Base

 

# 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