Reduce Migration Times to AWS By Up to 79% with NetFoundry and CloudEndure Migration

By Nic Fragale, Sr. Sales Engineer and Solutions Architect at NetFoundry
Erico Penna, Sr. Partner Solutions Architect at AWS

Cloud-hosted applications can help organizations realize cost savings by reducing total cost of ownership (TCO). They can also help you increase staff productivity, improve operational resilience by leveraging Amazon Web Services (AWS) global infrastructure, and achieve business agility by “getting to revenue” faster while reducing infrastructure overhead.

Cloud migration introduces challenges for network systems, however. The network configurations designed for on-premises usually don’t work well for the cloud. Traditional methods of cloud connectivity that use private circuitry, virtual private networking (VPN) technologies, and dedicated MPLS connections are cumbersome, expensive, and can take months to deploy.

Much like how cloud implements software-defined and API-based services to deliver agility and scalability for infrastructure, cloud applications require networking that delivers agility, scalable performance on a global basis, and has next-generation security capabilities designed in.

NetFoundry implements cloud-based orchestration and APIs to instantly spin up and manage Zero Trust, performant, edge-to-cloud networks over the internet.

NetFoundry, an AWS Advanced Technology Partner, is collaborating with CloudEndure Migration to accelerate the entire application migration process to AWS. The NetFoundry Zero Trust platform optimizes network throughput performance for CloudEndure migrations.

CloudEndure streamlines application migrations with automation and orchestration to convert your physical or virtual servers from their source infrastructure to AWS.

In this post, you will see how the combined NetFoundry and CloudEndure Migration solution achieves a 23.5 percent to 79.2 percent reduction in the time required to migrate versus a baseline in four different scenarios. Keep in mind that many factors influence the performance of data movement over a network, such as latency, capacity of bandwidth, congestion, routing challenges, and others.

You’ll see NetFoundry and CloudEndure Migration components, architecture, how they integrate with each other, and how to set up each system.

About CloudEndure Migration

CloudEndure Migration simplifies, expedites, and automates migrations from physical, virtual, and cloud-based infrastructure to AWS.

If you're looking to quickly rehost a large number of machines to AWS, you can use CloudEndure Migration without worrying about compatibility, performance disruption, or long cutover windows. Any re-architecture that needs to be done can be performed more easily after your machines are running on AWS.

CloudEndure Migration continually replicates your source machines into a staging area in your AWS account, without causing downtime or impacting performance. When you are ready to launch the production machines, CloudEndure Migration automatically converts your machines from their source infrastructure into the AWS infrastructure so they can boot and run natively on AWS.

You can migrate all applications and databases that run on Windows Server versions 2003/2008/2012/2016/2019 and Linux distributions, such as CentOS, RHEL, OEL, SUSE, Ubuntu, and Debian. CloudEndure Migration supports common databases, including Oracle and SQL Server, as well as enterprise applications such as SAP.

CloudEndure Migration components:

- CloudEndure Migration Service (Console) – *Web-based orchestrator*. The administrator has options as to how migration is to be performed, including mass instruction through API interaction, a "blueprint" for how the orchestration occurs, and the ability to migrate via internet or VPN/AWS Direct Connect.

- CloudEndure Migration Client Agent – *Software* on an endpoint operating system (OS) that block-copies local disks and securely migrates the operating system and data to AWS.

- CloudEndure Migration Replication Server – *Software* instance created on-demand by the service in the target AWS location that receives the migrated data from the CloudEndure Migration Client Agent and stores it in Amazon Elastic Block Storage (EBS) volumes.

About NetFoundry

NetFoundry is a leader in application-specific networking, enabling businesses to instantly connect distributed applications with ease and simplicity. The NetFoundry platform tackles the challenges of speed to migrate to AWS with Network-as-a-Service (NaaS) orchestration of a dynamic high-performance global networking fabric.

Application-specific segmentation across this global cloud fabric is created through a methodology called AppWANs.

Media outlets have coined the phrase Secure Access Secure Edge, or SASE, to describe what is accomplished by a NetFoundry AppWAN. This enables organizations to quickly spin up and scale out secure, compliant, performant, distributed applications while securing traffic across multiple layers and adaptively optimizing performance and throughput.

Zero Trust networking and enhanced performance are core capabilities provided by the NetFoundry platform.

NetFoundry components:

- NetFoundry Service (Console) – *Web-based orchestrator*. The administrator has options as to how the network is segmented for access, as well as the ability to programmatically perform all actions through API interaction and automate intelligence for calls to action.

- NetFoundry Client [/Gateway] – *Software* on an endpoint OS that performs ingress translation into the NetFoundry fabric. This is co-installed with the CloudEndure Migration Client Agent.

- NetFoundry Cloud Gateway – *Software* image available in AWS Marketplace as an Amazon Machine Image (AMI) that performs egress translation out of the NetFoundry Transit Fabric towards an application service. This software is located where the CloudEndure Migration Replication Server will be created.

- NetFoundry AppWAN – *Logical groupings of services* (Application IP Hosts or IP Subnets) accessible in the Local Area Network (LAN) of one or more geographically differentiated NetFoundry Cloud Gateways. NetFoundry AppWANs are similar in function to Network Access Control Lists (ACLs) which occur in firewalls, except they are created in the NetFoundry Cloud and enforced at NetFoundry Clients and Gateways.

- NetFoundry Transit Fabric – *On-demand data transport network* that NetFoundry manages as a service, which customers control via web console and API.

Some of the enhancing features of the access method include:

- 99.99+ percent availability: NetFoundry managed network service is highly resilient and self-healing.
- Resilient, highly available fabric: Multiple tier one providers give all endpoints a set of resilient and robust paths.
- Zero Trust: Endpoints authenticate in the cloud before access is granted at the edges.
- Multi-circuit access: 1+ internet connections aggregate for a unified per-packet large logical circuit.
- Dynamic, real-time routing: Endpoint algorithms choose best paths in real-time (router to router).
- Performance enhancing transports: Endpoints utilize multiple protocols to improve performance.
- Edge to cloud: Routers run on edges, in cores and on clouds, providing maximum route diversity.
- Least privileged access: Each session only has access to specified services, providing app-level micro segmentation and isolation while preventing lateral attacks.

Solution Overview

A. The NetFoundry Gateway software endpoints are installed and registered to the customer's private NetFoundry Network.
B. An AppWAN is provisioned to permit access over the NetFoundry Fabric to the IP Host or Subnet within the Amazon Virtual Private Cloud (VPC).
C. The endpoints make real-time decisions on how to send and receive data using multiple paths over the NetFoundry Fabric (internet).

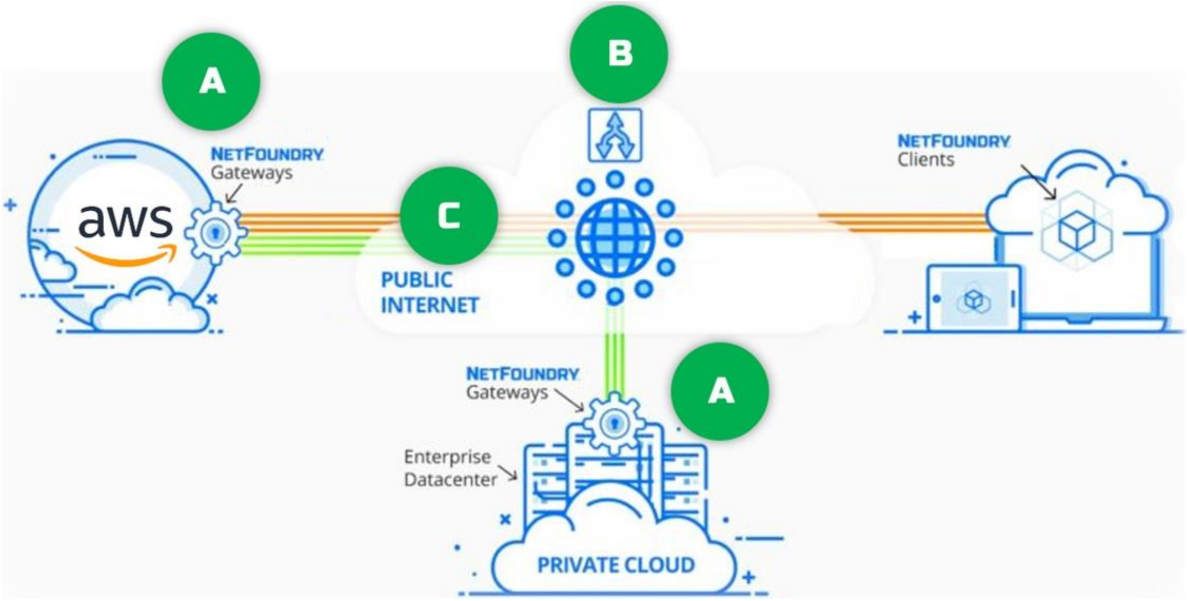


Figure 1 – NetFoundry overlay fabric and AppWAN segmented access.

Figure 2 illustrates the detailed interactions between CloudEndure Migration and the NetFoundry networking fabric.

1. Data replication is encrypted and compressed by the CloudEndure Migration software.
2. Data is sent to the private IP of the Replication Server in the target staging area. The destination will be recognized by the NetFoundry Gateway software and sent to the CloudEndure Replication Server over the NetFoundry Fabric.
3. Data exits the NetFoundry Fabric and is sent to the LAN reachable CloudEndure Replication Server for storage.

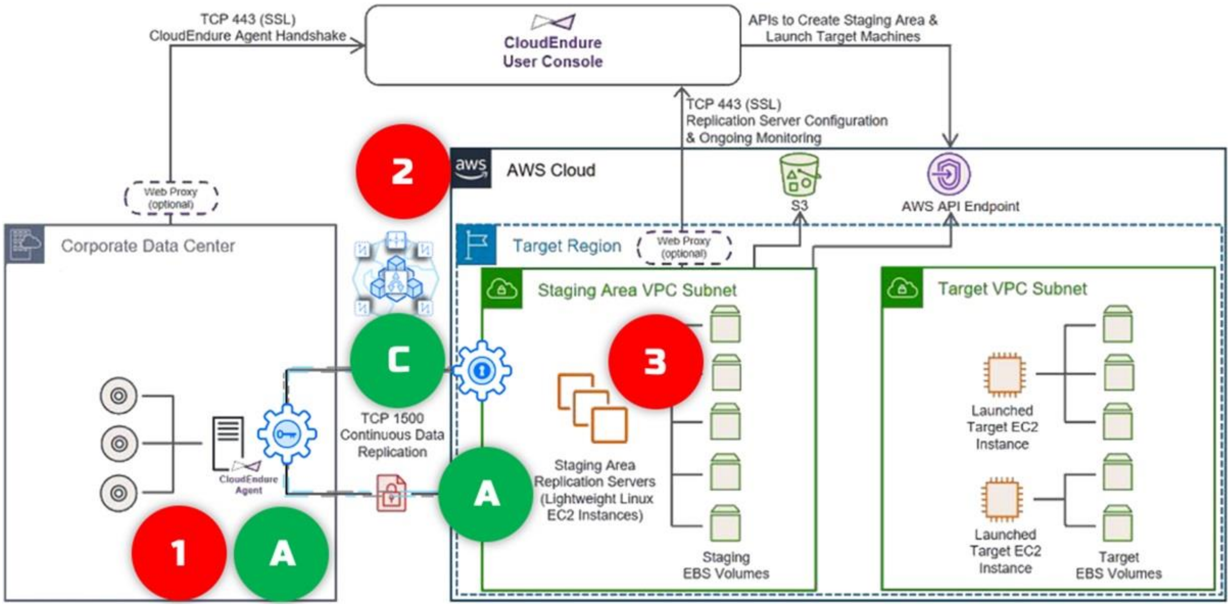


Figure 2 – CloudEndure Migration with NetFoundry fabric.

Walkthrough

The setup of the solution utilizes the CloudEndure Migration console and NetFoundry console. Automation through RESTful APIs are available in both systems for most steps, which reduces the already diminutive preparation time significantly.

Additionally, a NetFoundry Network may exist prior to a CloudEndure migration, or other available services, and be utilized for the purpose of migration when the need arises.

This section covers:

- Prerequisites
- Configuring NetFoundry
- Configuring AWS CloudEndure Migration
-

Prerequisites

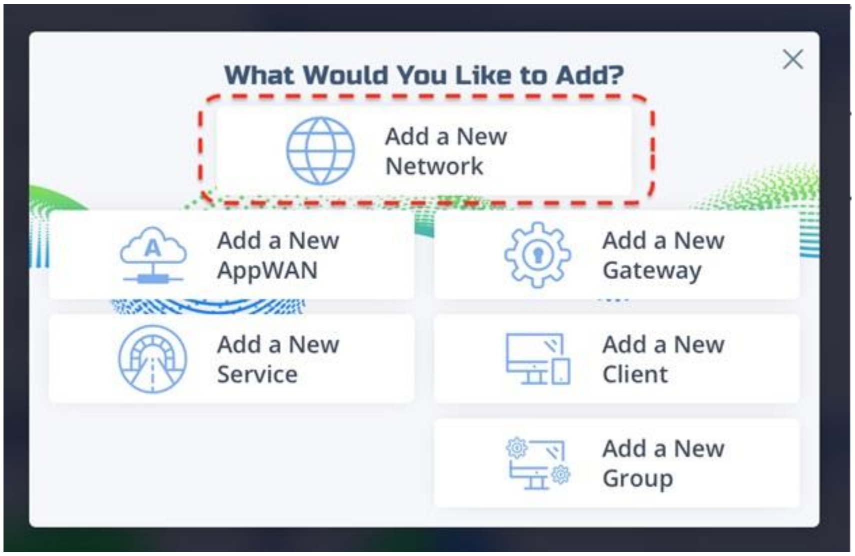
- Basic understanding of IP networking, VPCs, and NetFoundry AppWANs.
- CloudEndure Migration license, available at no cost.
- NetFoundry subscription.
- AWS account, so you can access a VPC in an appropriate region.

References

- AWS CloudEndure full documentation
- NetFoundry full documentation

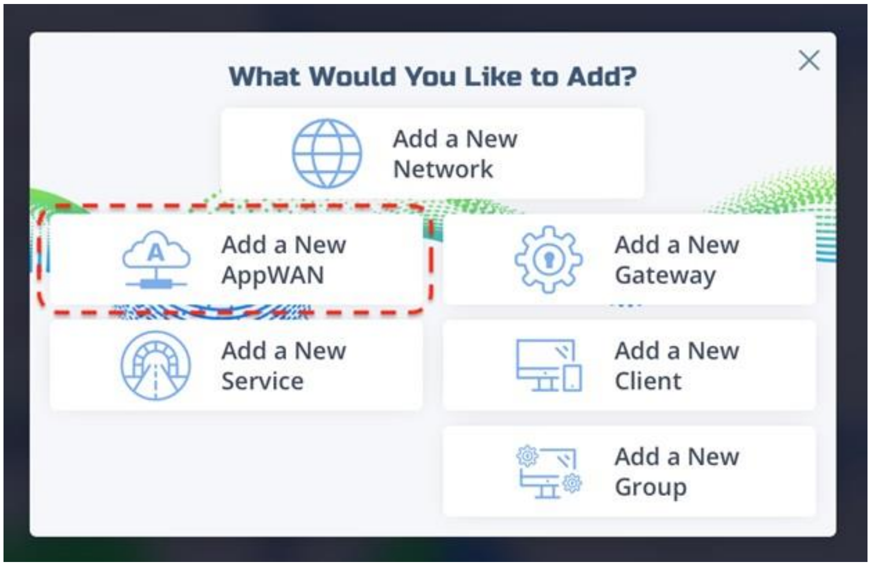
Configuring NetFoundry

- Sign in to the NetFoundry console.
- Click the + button in the upper left corner. Within the dialog, select Add a New Network.



What Would You Like to Add?

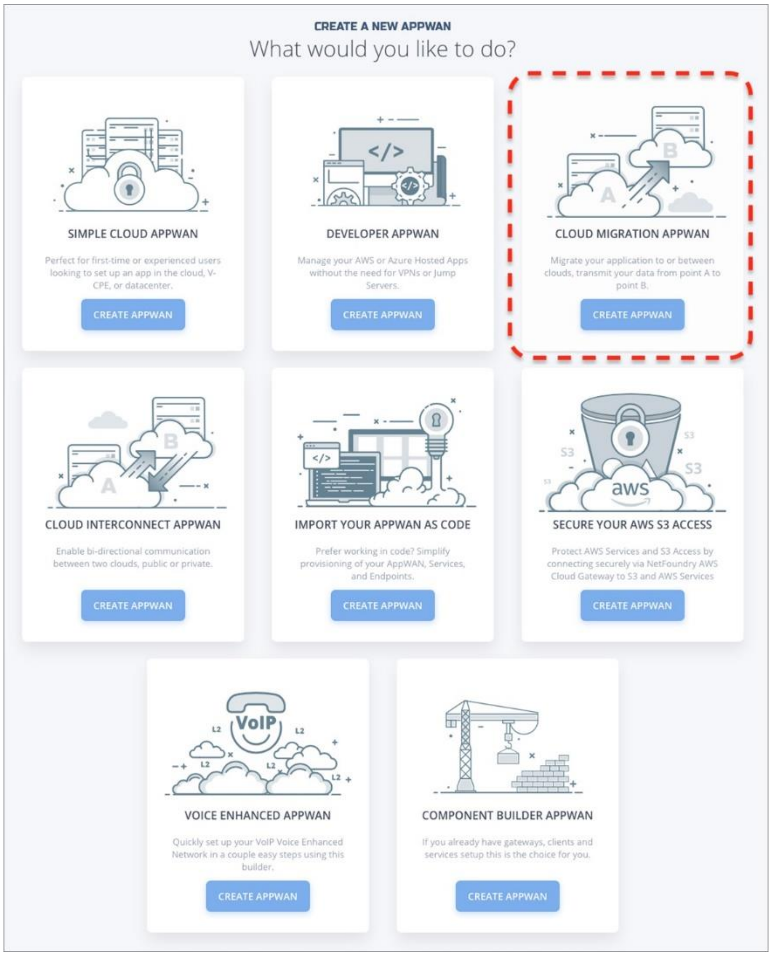
- Click the + button in the upper left corner. Within the dialog, select Add a New AppWAN.



What Would You Like to Add?

- Click the Cloud Migration AppWAN option.

- Follow the dialog questions to name and identify the involved components of the migration.



CREATE A NEW APPWAN

What would you like to do?

SIMPLE CLOUD APPWAN

Perfect for first-time or experienced users looking to set up an app in the cloud, V-CPE, or datacenter.

DEVELOPER APPWAN

Manage your AWS or Azure Hosted Apps without the need for VPNs or Jump Servers.

CLOUD MIGRATION APPWAN

Migrate your application to or between clouds, transmit your data from point A to point B.

CLOUD INTERCONNECT APPWAN

Enable bi-directional communication between two clouds, public or private.

IMPORT YOUR APPWAN AS CODE

Prefer working in code? Simplify provisioning of your AppWAN, Services, and Endpoints.

SECURE YOUR AWS S3 ACCESS

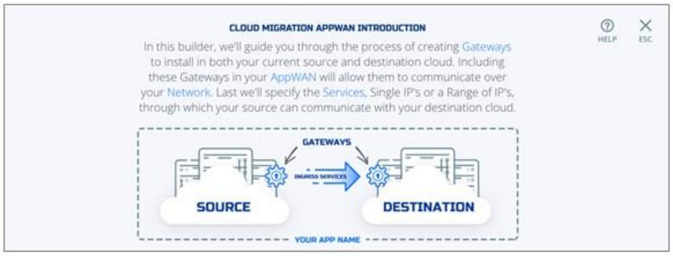
Protect AWS Services and S3 Access by connecting securely via NetFoundry AWS Cloud Gateway to S3 and AWS Services

VOICE ENHANCED APPWAN

Quickly set up your VoIP Voice Enhanced Network in a couple easy steps using this builder.

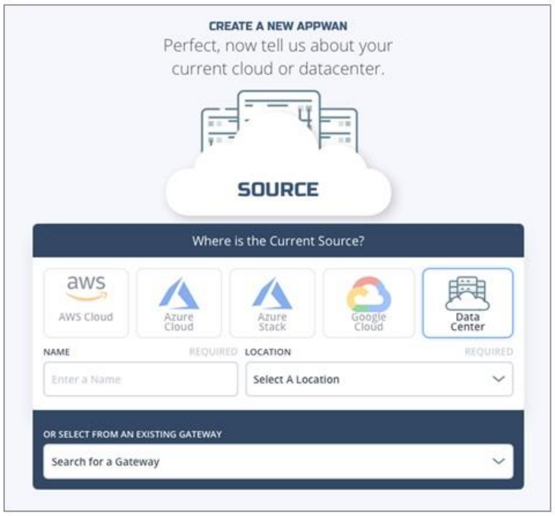
COMPONENT BUILDER APPWAN

If you already have gateways, clients and services setup this is the choice for you.



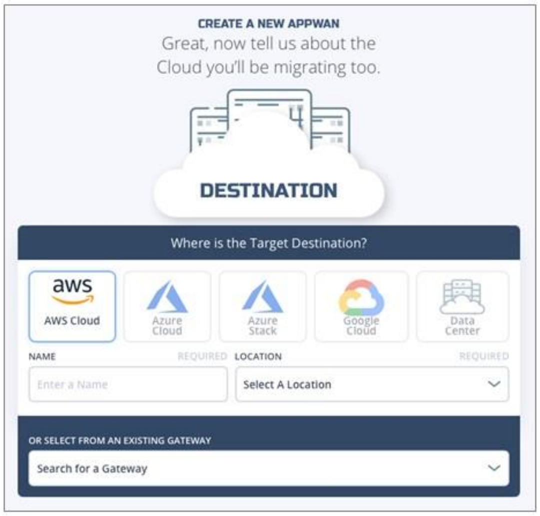
CLOUD MIGRATION APPWAN INTRODUCTION

In this builder, we'll guide you through the process of creating Gateways to install in both your current source and destination cloud. Including these Gateways in your AppWAN will allow them to communicate over your Network. Last we'll specify the Services, Single IP's or a Range of IP's, through which your source can communicate with your destination cloud.



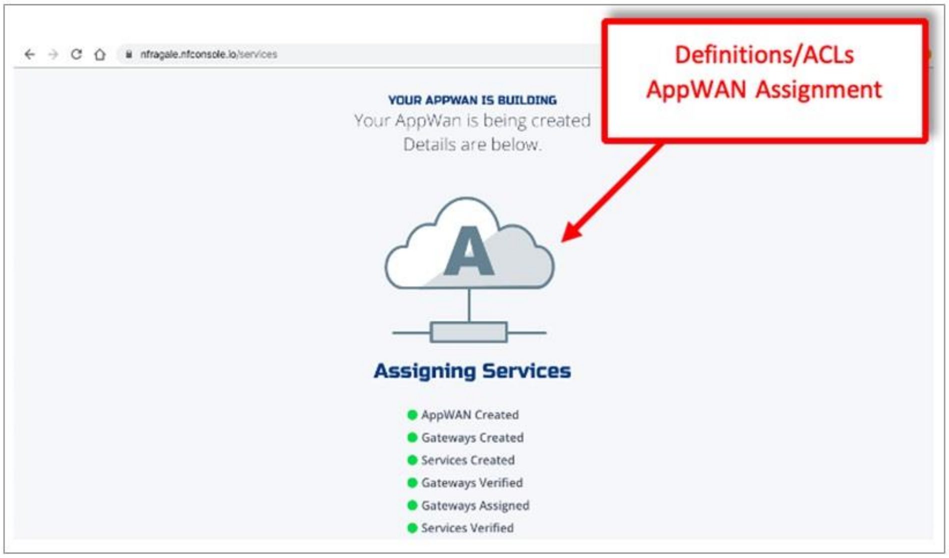
CREATE A NEW APPWAN

Perfect, now tell us about your current cloud or datacenter.



CREATE A NEW APPWAN

Great, now tell us about the Cloud you'll be migrating too.

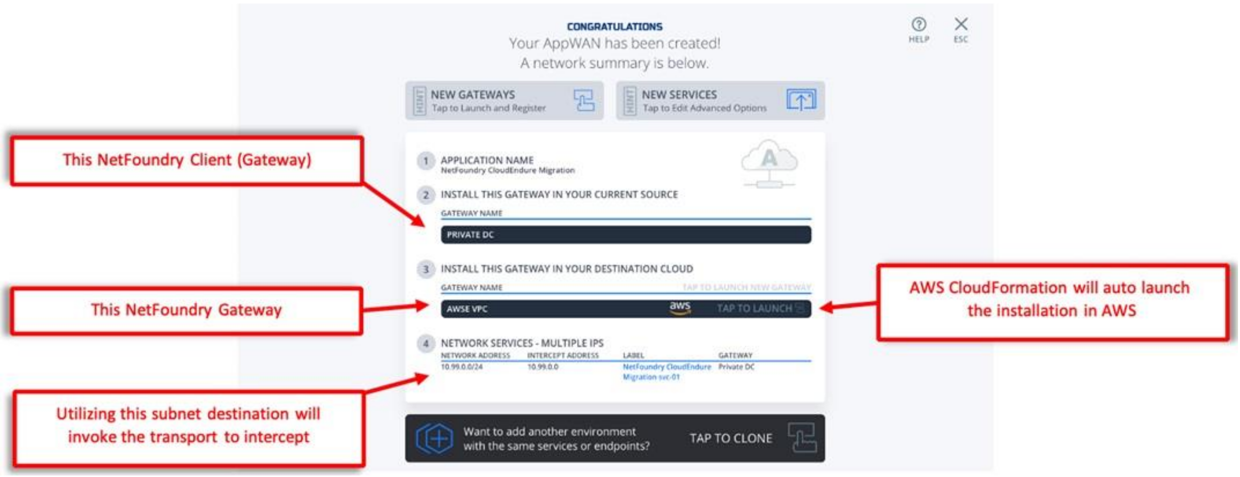


YOUR APPWAN IS BUILDING

Your AppWan is being created Details are below.

- AppWAN Created
- Gateways Created
- Services Created
- Gateways Verified
- Gateways Assigned
- Services Verified

- Review the configuration and ensure it's correct on the final dialog screen. Download software as required.
    - For the AWS endpoint, the Tap to Launch button brings up your AWS console manager and asks for confirmation of the networks and access permissions of the endpoint.
    - For the data center, the virtual machine software and registration code are shown to download.



HELP
ESC
NEW GATEWAYS
Tap to Launch and Register
NEW SERVICES
Tap to Edit Advanced Options
TAP TO LAUNCH NEW GATEWAY
TAP TO LAUNCH
TAP TO CLONE

CONGRATULATIONS

Your AppWAN has been created!

A network summary is below.

1 APPLICATION NAME

NetFoundry CloudEndure Migration

2 INSTALL THIS GATEWAY IN YOUR CURRENT SOURCE

GATEWAY NAME: PRIVATE DC

3 INSTALL THIS GATEWAY IN YOUR DESTINATION CLOUD

GATEWAY NAME: AWSE VPC

4 NETWORK SERVICES - MULTIPLE IPS

NETWORK ADDRESS	INTERCEPT ADDRESS	LABEL	GATEWAY
10.99.0.0/24	10.99.0.0	NetFoundry CloudEndure Migration svc-01	Private DC

Want to add another environment with the same services or endpoints?

This NetFoundry Client (Gateway)

This NetFoundry Gateway

Utilizing this subnet destination will invoke the transport to intercept

AWS CloudFormation will auto launch the installation in AWS

Configuring CloudEndure Migration Project and Network

- Sign in to the CloudEndure console.

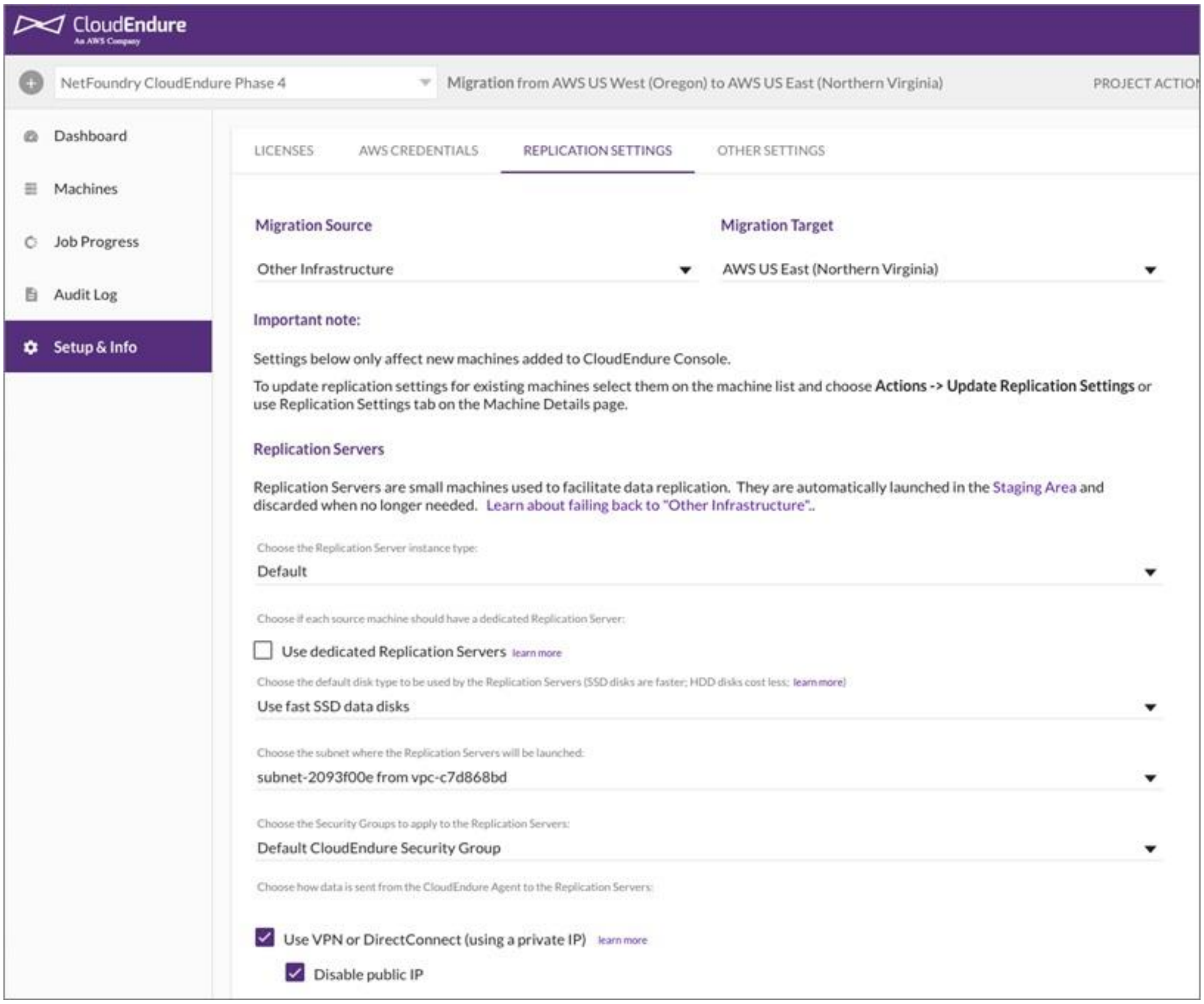
- On the user console, click the + button in the upper left corner.

- On the Create New Project dialog box, set the following, and then click Create Project:
  - *Project name* – Enter a unique name for the project. The name can contain up to 255 characters.
  - *Project type* – Select either Disaster Recovery or Migration.
  - *Target cloud* – CloudEndure exclusively utilizes the AWS Cloud as a target infrastructure.
  - *License* – Select a License Package to associate with your migration project.

- Next, go to Setup & Info and define your Migration Source and Migration Target.

- Select Subnet matching NetFoundry AppWAN.

- Select VPN or Direct Connect… to use the Replication Server’s private IP in the AWS target destination.



Migration from AWS US West (Oregon) to AWS US East (Northern Virginia)

Migration Source: Other Infrastructure

Migration Target: AWS US East (Northern Virginia)

Important note:

Settings below only affect new machines added to CloudEndure Console.

To update replication settings for existing machines select them on the machine list and choose **Actions -> Update Replication Settings** or use Replication Settings tab on the Machine Details page.

Replication Servers

Replication Servers are small machines used to facilitate data replication. They are automatically launched in the Staging Area and discarded when no longer needed. Learn about failing back to "Other Infrastructure"..

Choose the Replication Server instance type: Default

Choose if each source machine should have a dedicated Replication Server:

□ Use dedicated Replication Servers learn more

Choose the default disk type to be used by the Replication Servers (SSD disks are faster; HDD disks cost less; learn more): Use fast SSD data disks

Choose the subnet where the Replication Servers will be launched: subnet-2093f00e from vpc-c7d868bd

Choose the Security Groups to apply to the Replication Servers: Default CloudEndure Security Group

Choose how data is sent from the CloudEndure Agent to the Replication Servers:

☑ Use VPN or DirectConnect (using a private IP) learn more

☑ Disable public IP

Installing NetFoundry and CloudEndure Migration Agent

Download installation programs for NetFoundry Client software and CloudEndure Migration software to the source machine, which can be any CloudEndure Migration supported operating system.

NetFoundry also supports Gateway mode in which multiple CloudEndure Migration software utilizes one or more NetFoundry Gateways in the source LAN.

Install both programs from the command line of the OS. You can automate the process to simplify it:

- Instructions for CloudEndure – Click “Installing the CloudEndure Agents”
- Instructions for NetFoundry – Click “Client & Gateway Endpoints”

When you configured the products, you received a registration code for NetFoundry and an Agent Installation Token for CloudEndure Migration. These registration codes identify the machines involved to the respective Consoles.

After the Migration

When you are finished with the migration, remember to remove your CloudEndure project and NetFoundry AppWAN.

If desired, NetFoundry AppWAN may persist after the migration, for continual replication or other activities which require the source machine to communicate to the destination VPC.

Once migration is complete, you can install NetFoundry Client software on other endpoints, which may be given direct, secure, and highly performant access to the VPC by way of the AppWAN.

Performance Baselines

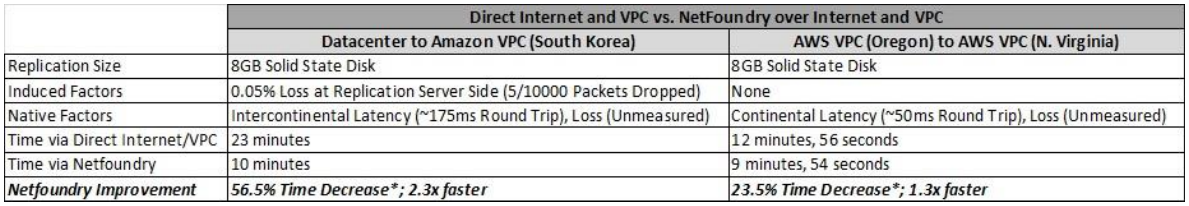
Now that you know how to configure the environment, let's move on to some experiments that illustrate common scenarios that CloudEndure Migration is used for, and how application of NetFoundry enhances the migration.

- Replication size: Size, in gigabytes, of the disk on the source machine that's being migrated.
- Induced factors: Changes to the transport showing performance of the migration in different situations.
- Native factors: Innate qualities of the transport such as latency and packet loss.

Experiments #1 and #2

For the following outcomes, % Time Decrease is measured with the formula:

*[(original_value – new_value)/original_value * 100]*



	Direct Internet and VPC vs. NetFoundry over Internet and VPC	
	Datacenter to Amazon VPC (South Korea)	AWS VPC (Oregon) to AWS VPC (N. Virginia)
Replication Size	8GB Solid State Disk	8GB Solid State Disk
Induced Factors	0.05% Loss at Replication Server Side (5/10000 Packets Dropped)	None
Native Factors	Intercontinental Latency (~175ms Round Trip), Loss (Unmeasured)	Continental Latency (~50ms Round Trip), Loss (Unmeasured)
Time via Direct Internet/VPC	23 minutes	12 minutes, 56 seconds
Time via Netfoundry	10 minutes	9 minutes, 54 seconds
Netfoundry Improvement	***56.5% Time Decrease*; 2.3x faster***	***23.5% Time Decrease*; 1.3x faster***

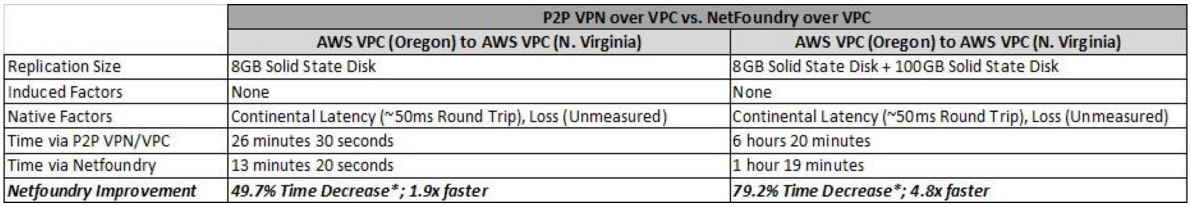
The South Korea experiment emphasized heightened performance for long-distance migrations with an added destructive (lossy) presence. Watch a demo video.

The Oregon to N. Virginia experiment emphasized heightened performance for USA centric (AWS to AWS) migrations. Watch a demo video.

Experiments #3 and #4

For the following outcomes, % Time Decrease is measured with the formula:

*[(original_value – new_value)/original_value * 100]*



	P2P VPN over VPC vs. NetFoundry over VPC	
	AWS VPC (Oregon) to AWS VPC (N. Virginia)	AWS VPC (Oregon) to AWS VPC (N. Virginia)
Replication Size	8GB Solid State Disk	8GB Solid State Disk + 100GB Solid State Disk
Induced Factors	None	None
Native Factors	Continental Latency (~50ms Round Trip), Loss (Unmeasured)	Continental Latency (~50ms Round Trip), Loss (Unmeasured)
Time via P2P VPN/VPC	26 minutes 30 seconds	6 hours 20 minutes
Time via Netfoundry	13 minutes 20 seconds	1 hour 19 minutes
Netfoundry Improvement	***49.7% Time Decrease*; 1.9x faster***	***79.2% Time Decrease*; 4.8x faster***

The Oregon to N. Virginia experiment emphasized heightened performance for USA centric (AWS to AWS) migrations when compared with an overlay VPN technology. Watch a demo video.

The last experiment emphasized heightened performance for larger disks for USA centric (AWS to AWS) migrations when compared with an overlay VPN technology. Watch a demo video.

Conclusion

In this post, you learned how to reduce time to ready for a migration. An increase of throughput delivered by the underlying network and transport directly correlates to a reduction of time to ready.

The conclusion we draw from the presence of NetFoundry while performing a CloudEndure Migration is a substantial reduction of time to ready in the range of 23 percent to 79 percent.

CloudEndure Migration natively utilizes many techniques to enhance its own application's throughput, and the enhancement to the transport network that NetFoundry complements results in an exponential boost to the throughput.

Disclaimer: The performance testing described in this post illustrates common scenarios, and every effort has been taken to ensure testing was conducted using real world conditions and variables. Many factors affect performance testing and results will vary due to unknown and uncontrollable factors. Performance improvement information provided in this post are provided as general guidelines only. This information in no way represents any form of warranty or guarantee of performance implied or otherwise.