



Education Solutions
The Holistic Data Approach to Student Success



Predictive Analytics

Turn data into insight, and insight into action.

[READ MORE](#)



Student Management

Teaching takes more than teaching.

[READ MORE](#)



Observation and Growth

Are you mentoring your teachers, or are you telling them facts? There's a difference.

[READ MORE](#)

March 11, 2020 | iPASS in AWS





Why AWS, Why now, What to expect?



From existing

- Expedient
- VMware, Centos 5
- Shared Web Server
- Progress Software
 - OpenEdge Enterprise RDBMS 10.2B
 - OpenEdge App Server Enterprise 10.2B

Benefits

To new

- Amazon Web Services
- Ubuntu 18.04 LTS (long term support)
- Split Web/RDBMS
- Progress Software 11.5
- Reliability/Resiliency/ Scalability
- Improved Compliance: FERPA/NIST 800/NY Education Law 2-d

AWS Services in Scope by Compliance Program

We include services in the scope of our compliance efforts based on the expected use case, feedback and demand. If a service is not currently listed as in scope of the most recent assessment, it does not mean that you cannot use the service. It is part of the **shared responsibility** for your organization to determine the nature of the data. Based on the nature of what you are building on AWS, you should determine if the service will process or store customer data and how it will or will not impact the compliance of your customer data environment.

We encourage you to discuss your workload objectives and goals with your AWS account team; they will be able to evaluate your proposed use case and architecture, and how our security and compliance processes overlay that architecture. **Need to connect with an AWS business representative?**

This webpage provides a list of AWS Services in Scope of AWS assurance programs. Unless specifically excluded, features of each of the services are considered in scope of the assurance programs, and are reviewed and tested as part of the assessment. Refer to the AWS Documentation for the features of an AWS service

✓ = This service is currently in scope and is reflected in current reports


Joint Authorization Board (JAB) Review = This service is currently undergoing a JAB Review

Third Party Assessment Organization (3PAO) = This service is currently undergoing an assessment by our third party assessor

SOC	PCI	ISO	FedRAMP	DoD CC SRG	HIPAA BAA	IRAP	MTCS	C5	K-ISMS	ENS High
SERVICES / PROGRAMS				FedRAMP Moderate (East/West)			FedRAMP High (GovCloud)			
Amazon API Gateway				✓			JAB Review			
Amazon Athena				3PAO Assessment			3PAO Assessment			

Why AWS? Why now? Compliance

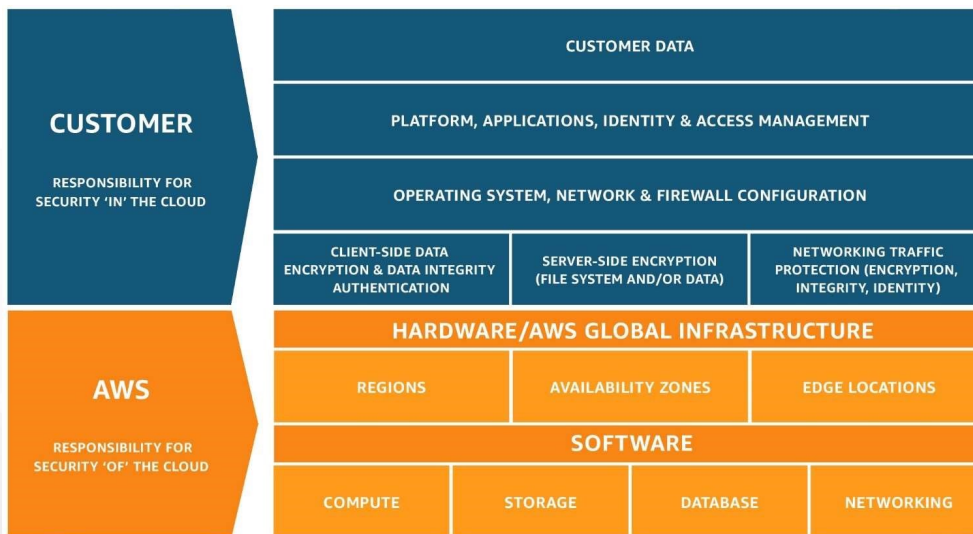
 <https://aws.amazon.com/compliance/services-in-scope/>

 SOC 1-3, PCI, ISO, FedRAMP, HIPPA....

 FERPA is covered by extension

Why AWS? Why now? Security

- ❁ AWS does not access content
- ❁ Data is encrypted in motion and at rest
- ❁ Data does not leave the US East N. Virginia Region
- ❁ Non-disclosure of information unless legally bound
- ❁ Independently validated security protections
- ❁ AWS ISO/FedRAMP compliance



AWS Regions

Reliability/Resiliency/Scalability

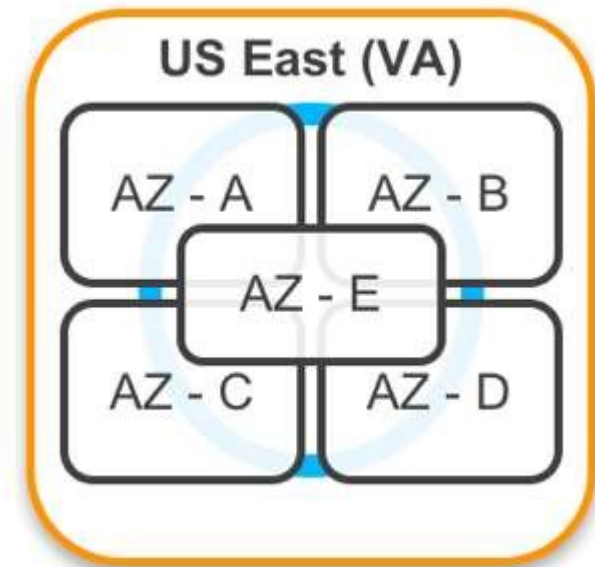
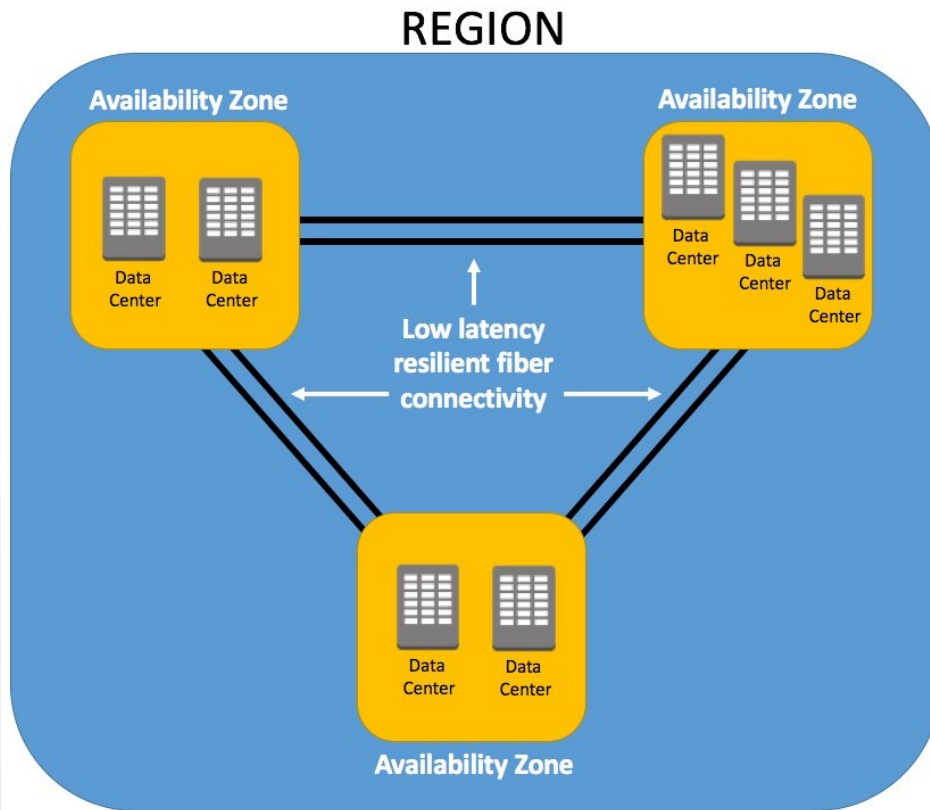


Harris Education Solutions

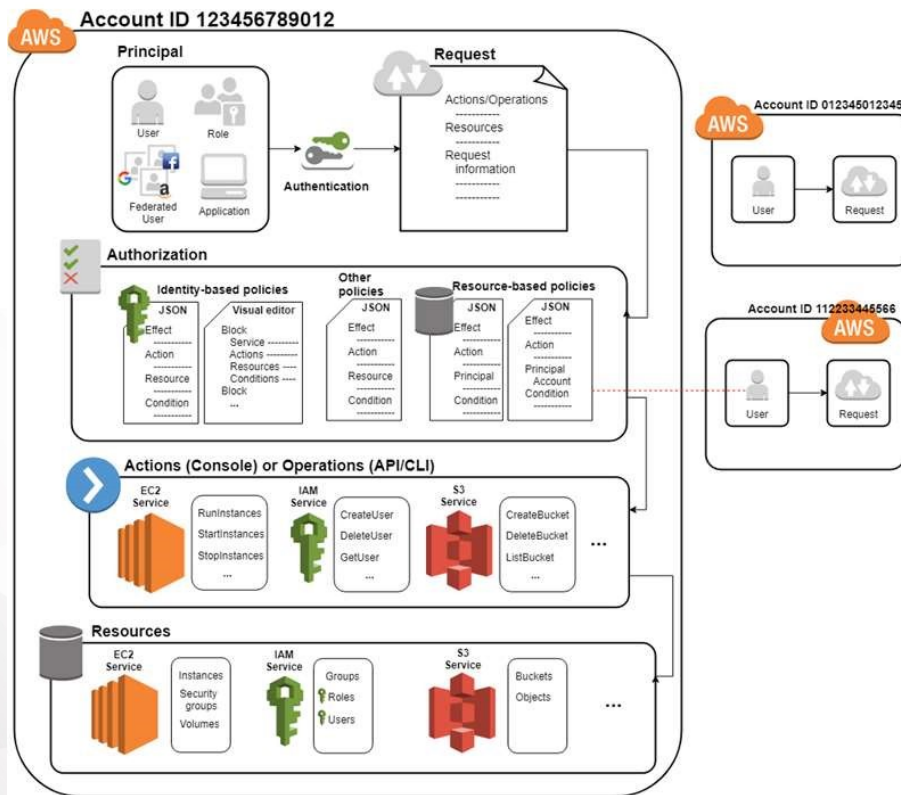


A region on AWS is comprised of Availability Zones, **each of which is a cluster of data centers.**

Reliability/Resiliency/Scalability



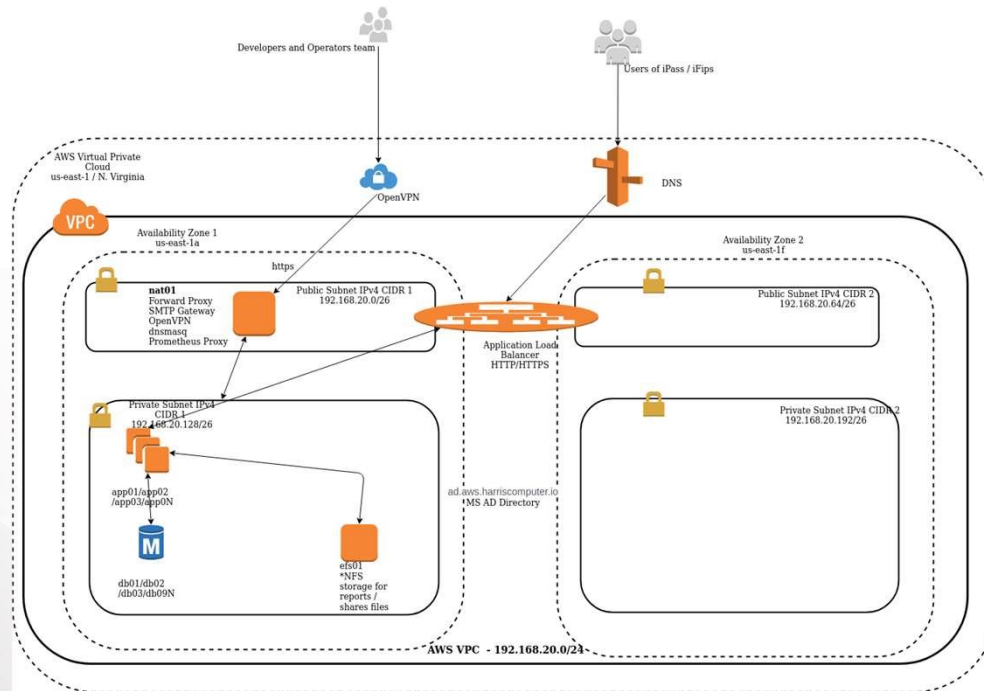
- Availability Zones on different flood plains
- Served by distinct public power utilities
- Multiple Tier 1 transit providers for network redundancy
- 25TB/sec connectivity between data centers



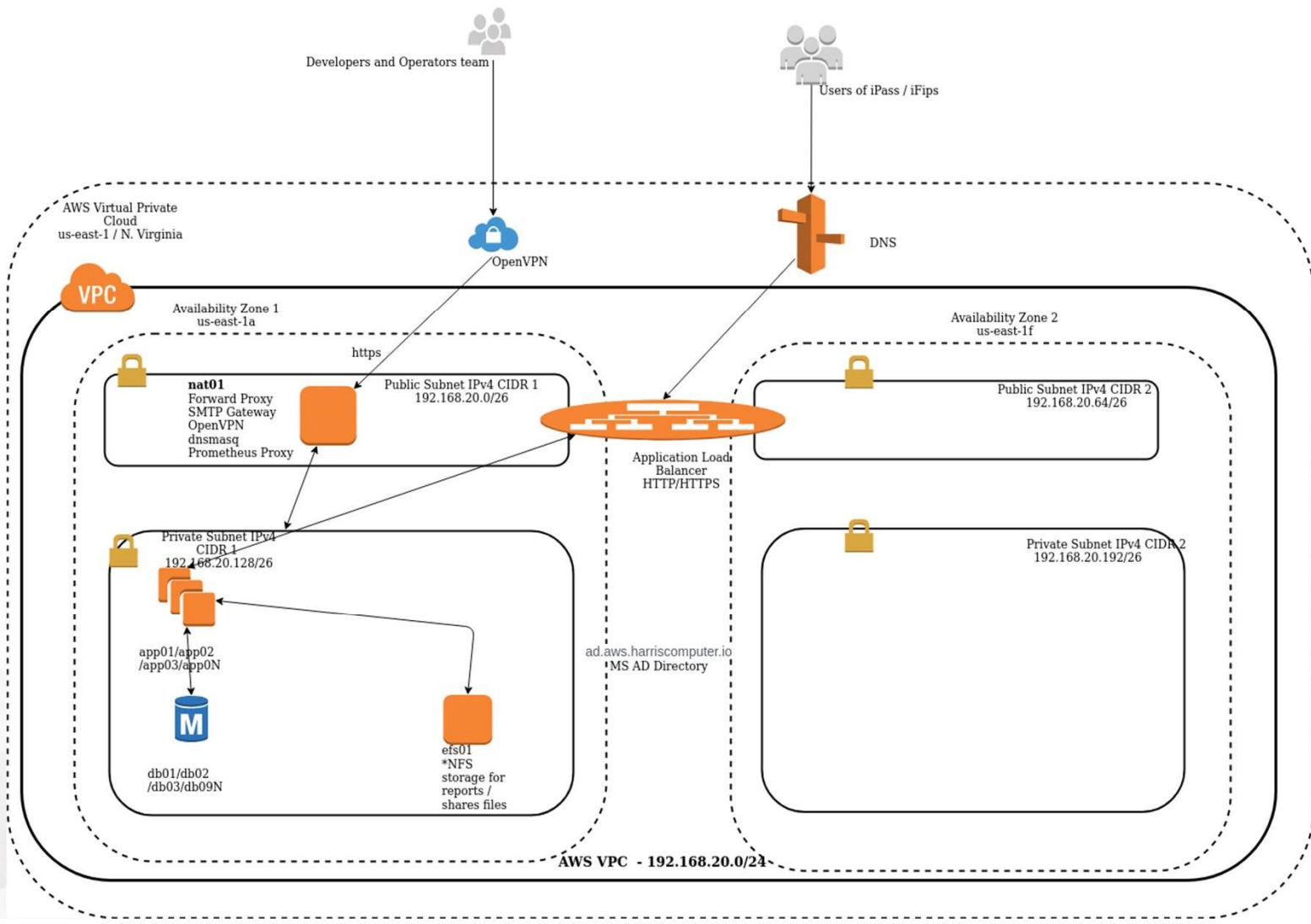
Key AWS Technologies

- AWS Organizations/Integrated Account Management (IAM)
- Key Management System (KMS) and CloudTrail auditing
- AWS service APIs
- Encrypted EBS volumes (SSD/SAN)
- Availability Zones

HES AWS Infrastructure Keys/Best Practices



- 🌀 Dedicated product accounts (via AWS Orgs/IAM)
- 🌀 Application and Development staff separated from access to the operating environment
- 🌀 Scripted infrastructure automation using Terraform (network) & Ansible (host configuration) to AWS APIs
- 🌀 Where possible recipes captured in docker
- 🌀 VPC perimeter/network firewall/ App Load Balancer (all ingress/egress controlled via OpenVPN & Forward Proxy)
- 🌀 Each VM wrapped in an individual host firewall
- 🌀 Stack hardened from OS on up at each layer (ex. TLS 1.2 for SSL)
- 🌀 Data sent to third parties controlled through 3 layers (Host Firewall then Edge Firewall then Forward Proxy)



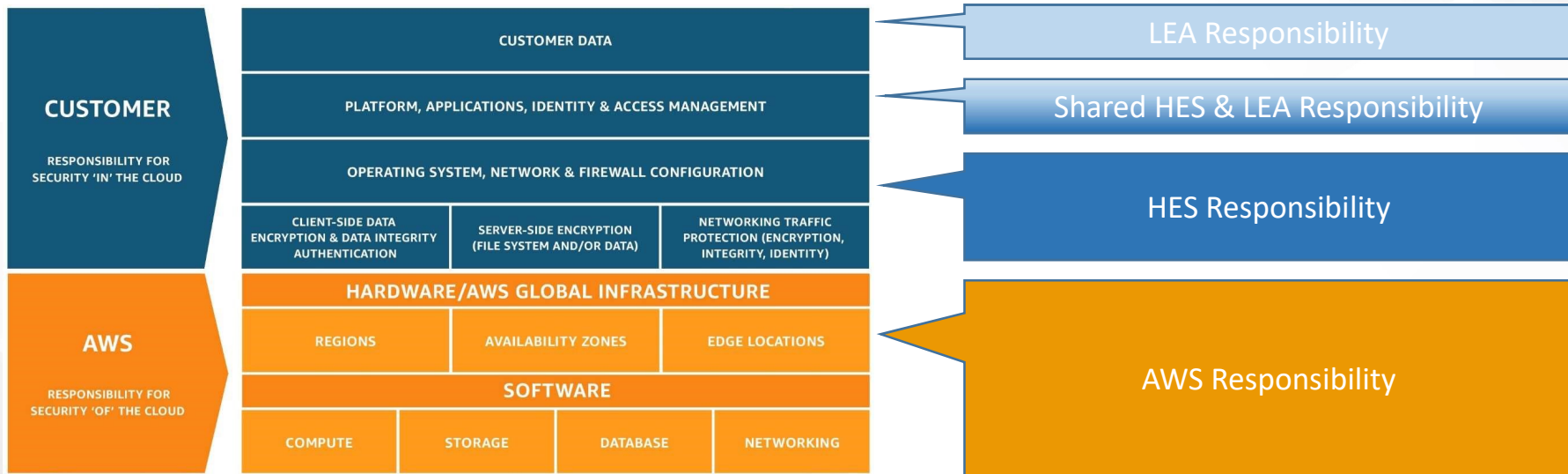
Compliance Requirement

HES Compliance Check

FERPA & NYED Law Section 2-d

Limit access	<p>Single access point for users (via web login) Username/PW management (by district admin) Only Application/Dev staff have access to iPASS (IAM/CloudTrail) Only Ops Team has access to infrastructure</p>
Only use data for authorized purposes	Specified in Privacy Policy and Contracts
Do not disclose PII without prior written consent or under legal order/statute with notice to LEA	HES contracts and AWS Terms comply
Maintain reasonable administrative, technical and physical safeguards	<p>Leveraging AWS best of breed tools (IAM, KMS, volume encryption) Physical environment is as secure as it gets (ISO, FedRAMP, SOC 3) HES infrastructure/AWS API scripting governs consistent and automated security control Staff receive annual FERPA training/encrypted drives/device management</p>
Use encryption while data is in motion or in custody	TLS 1.2 for SSL and Encryption at Rest via EBS/SAN volume encryption
Breach notification protocol	Detailed in HES - Information Security Plan

iPASS Security Responsibility Matrix



Cutover Methodology

Prior to cutover:

- HES copies production db to AWS for validation
- HES completes internal testing checks
- HES Requests client validation/sends checklist
- Client validates checklist
- Issue resolution as needed
- Schedule production cutover

Final cutover:

- Stop access to Expedient production
- Copy db to AWS, complete internal testing
- Release site to client for final validation
- Client notifies users of go-live
- HES staff on watch next day

Cutover Checklist

- ✓ Validate sample logins from all locations
- ✓ Validate record entry, editing, saving
 - ✓ iPASS Admin functions
 - ✓ Teacher functions
 - ✓ Student/Parent portal
- ✓ Run daily reports and other critical reports
- ✓ Validate printing and saving to local machines
- ✓ Validate Reporting connections/running/saving edits
- ✓ Validate connection to SIF
- ✓ Test exports for third party systems
- ✓ Cleanup old accounts from prior years & populate email address
- ✓ Notify users of what to expect

THANK YOU!

Any questions?