AWS re:Invent

STG305

Deep Dive: Build Hybrid Storage Architectures with AWS Storage Gateway

Asa Kalavade
General Manager
AWS Storage Gateway

Paul Reed
Principal Product Manager
AWS Storage Gateway

Rick Fath
Sr. Director Cloud Architecture
CME Group

Craig Bona
Sr. Director Platform Engineering
CME Group

Agenda

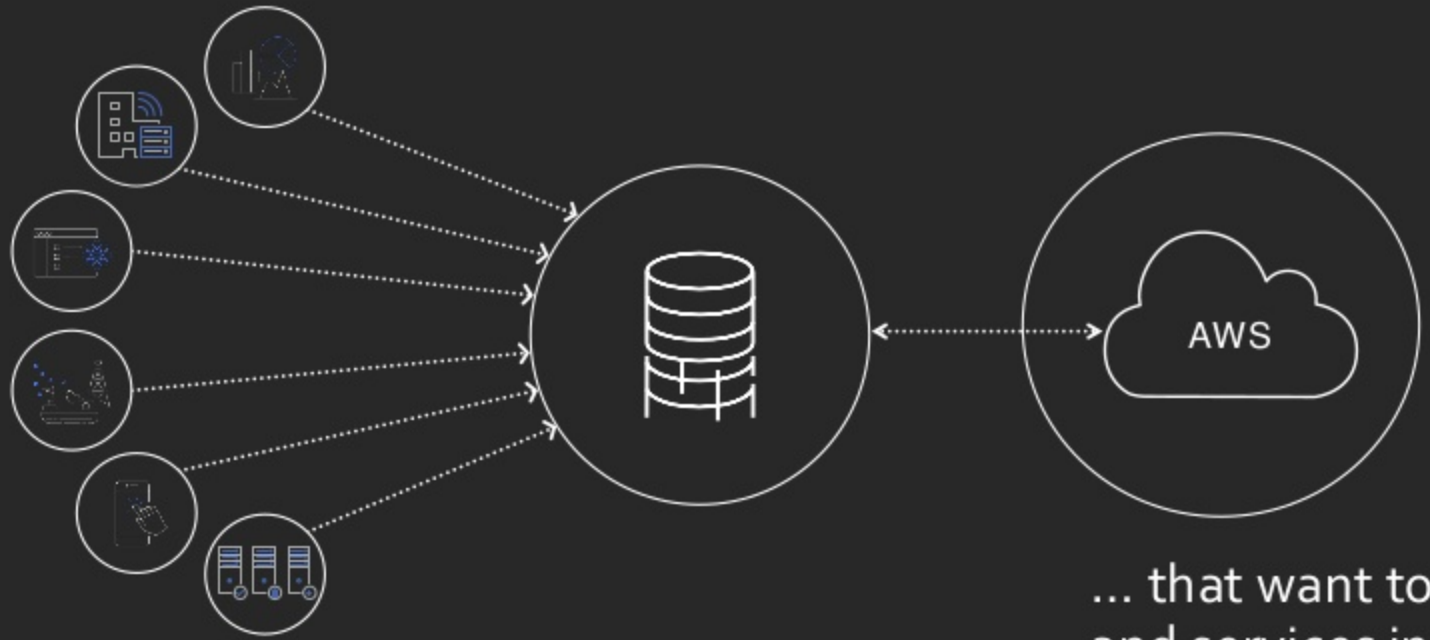
AWS Storage Gateway

- AWS Storage Gateway and hybrid storage
- What's new since re:Invent 2017
- How CME Group is using Storage Gateway
- Deep dive and best practices
- Q&A

Hybrid cloud storage overview

What's the hybrid storage problem?

You have on-premises data and applications …



… that want to use storage and services in the cloud

Hybrid storage

Bridge on-premises storage and operations with cloud storage

Backup on-premises
data and applications

Tier
cold data

Simplify
Branch Offices

Multi-protocol access

(in-cloud and on-prem
access same date)

Low-latency on-premises
access to in-cloud data

Content
Distribution

Regardless of your stage of cloud adoption …

Hybrid storage requirements

Hybrid storage with Storage Gateway

On-premises

1. Standard storage protocols
2. Low-latency access via fully managed cache
3. Multiple hardware and software deployment options
4. Optimized data transfers

AWS Storage Gateway

In-cloud

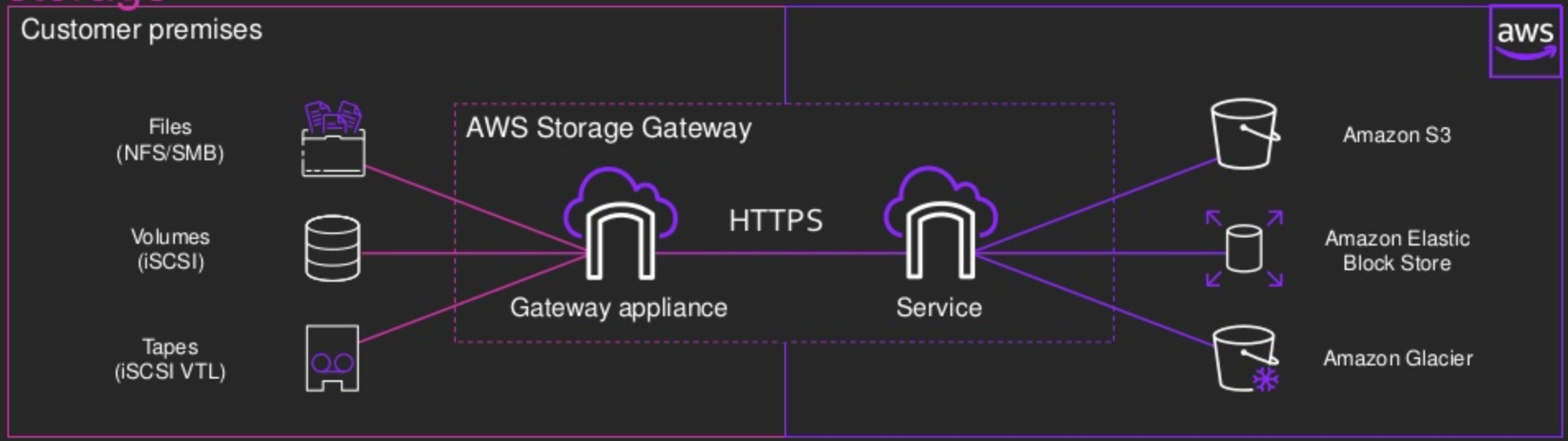
- Integrates with Amazon S3, Amazon EBS, and Amazon Glacier
- Notifications to enable automated data pipelines in the cloud
- Manage through the AWS console as another AWS Service
- Enables native AWS capabilities such as storage classes and replication

Hybrid cloud storage is experiencing a renaissance, with new storage offerings bridging the gap between on-premises and public cloud providers

Gartner, Oct. 2018

AWS Storage Gateway

Hybrid storage service enabling applications to seamlessly use AWS storage



Integrated with IAM, KMS, CloudTrail, CloudWatch services

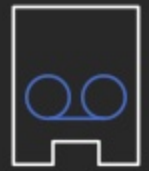
File, volume, and tape storage types

File Gateway

Store and access objects in Amazon S3 from file-based applications with local caching

Volume Gateway

Block storage on-premises backed by cloud storage with local caching, Amazon EBS snapshots, and clones



Tape Gateway

Drop-in replacement for physical tape infrastructure backed by cloud storage with local caching

Storage gateway

Cost effective, while providing enterprise compliance and security needs

Cost-effective

File Gateway	Billed as Amazon S3 storage
Volume Gateway	$0.023/GB storage $0.05/GB EBS snapshot storage
Tape Gateway	$0.023/GB virtual tapes storage $0.004/GB archived tape storage
Data written	$0.01/GB written to AWS, capped at $125/month

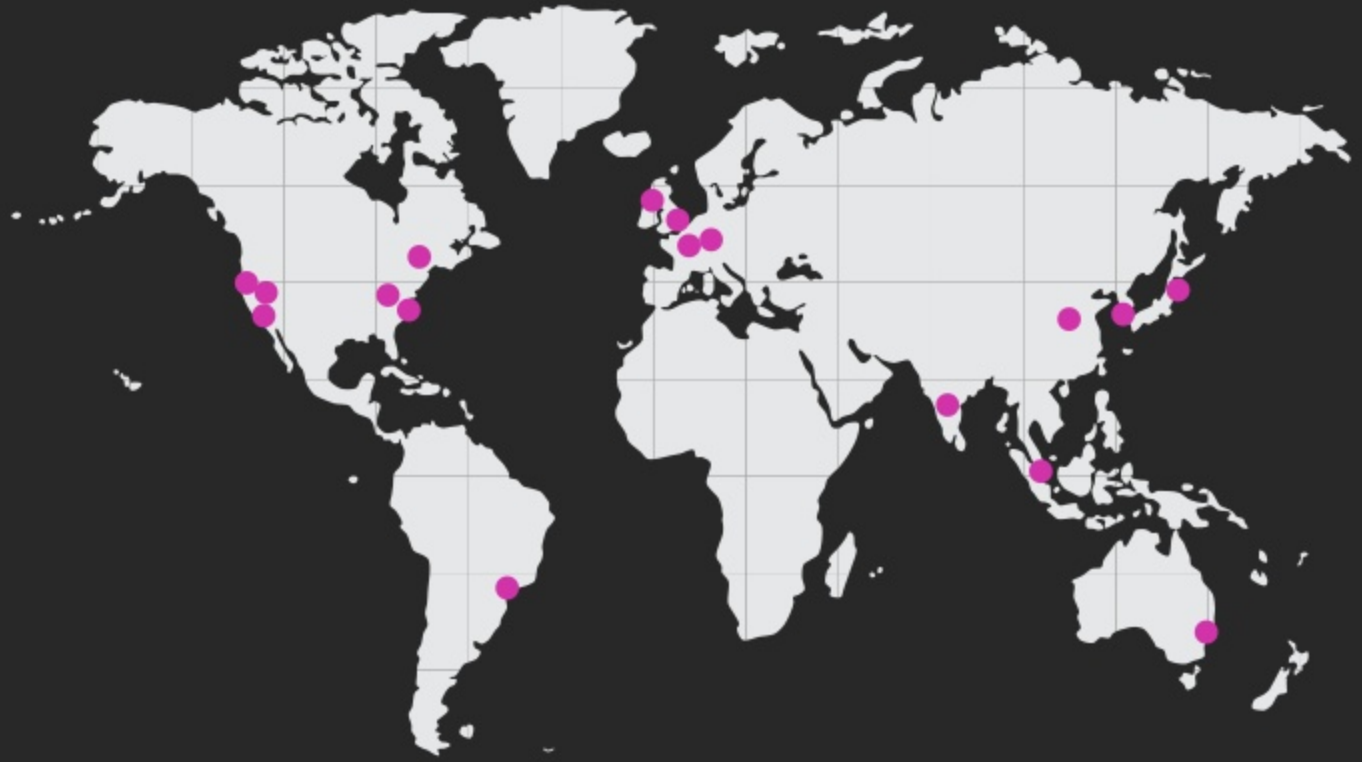
Pricing for us-east-1. Additional request and AWS Data Transfer pricing applies.

Compliance and security

- HIPAA, PCI, SOC* & ISO** compliant
- Data encrypted on the wire
- Server-side or AWS KMS encryption

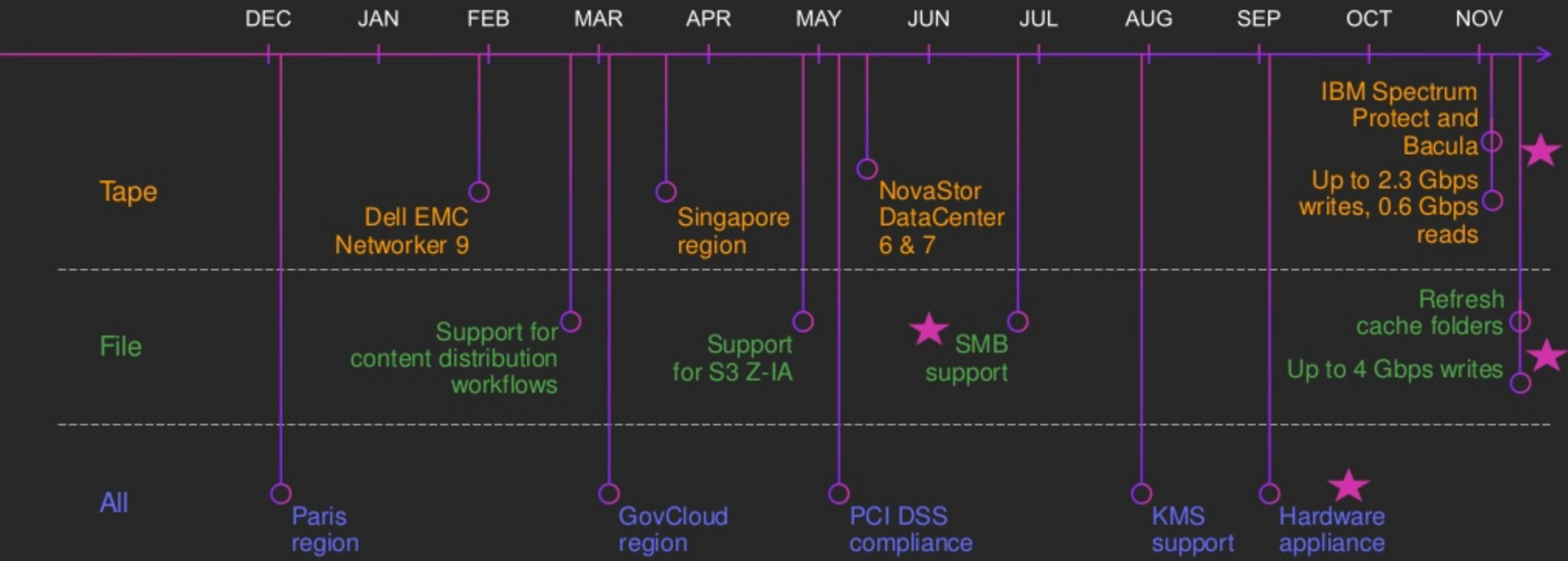
*SOC (1, 2, 3) **ISO (9001, 27001, 27017, 27018)

Available in 17 regions globally



* Tape Gateway not available in South America (São Paulo) Region

Launches since re:Invent 2017

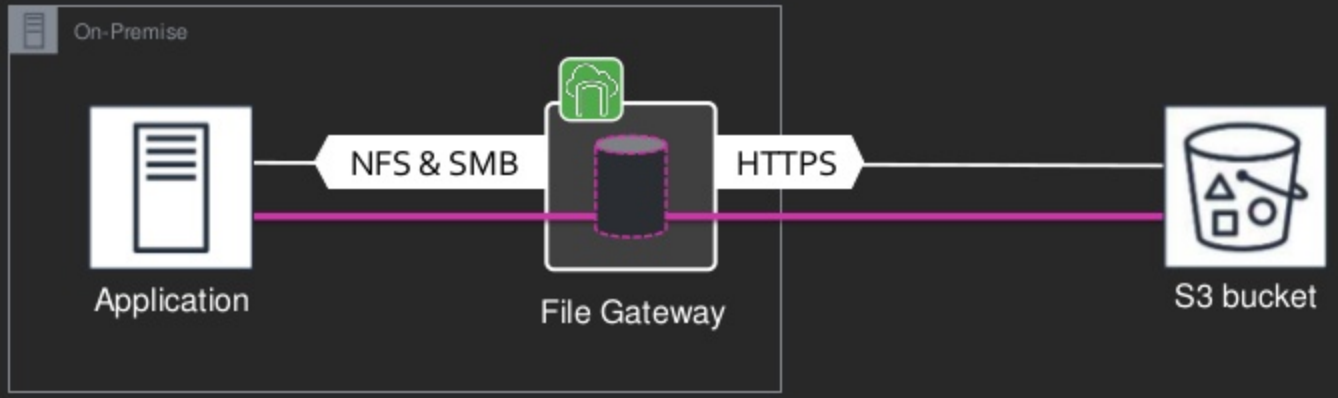


Some AWS Storage Gateway customers

AWS Storage Gateway overview

File gateway: overview and use cases

Store and access objects in Amazon S3 from file-based applications with local caching



Use cases

- Backup on-premises data to the cloud
- Hybrid cloud workflows
- Low-latency on-premises access to cloud storage
- Content distribution and collaboration via the cloud

Celgene

DIRECT SUPPLY

File gateway

Connect using NFS v3/v4 or SMB v2/v3 protocols
- Files stored as native S3 objects
- Metadata is preserved as object user metadata

Object-level encryption with SSE-S3 or SSE-KMS

Fully managed local cache
- Read-through, write-back, LRU managed

Notifications through Amazon CloudWatch (e.g., upload complete)

Optimized data transfers
- Uploads only sends changes, downloads retrieve file parts needed

NEW

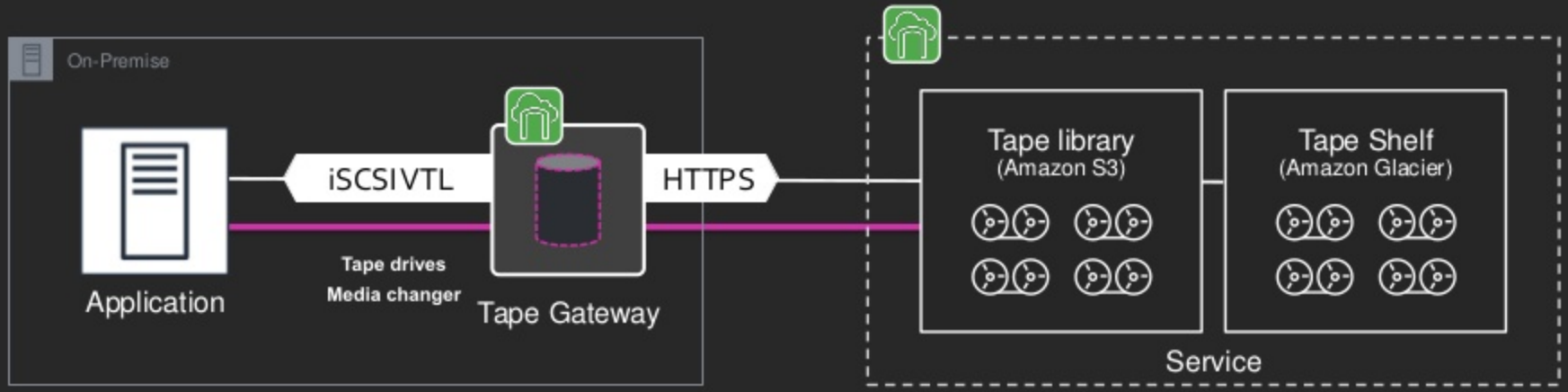
Refresh cache by prefix
- Optimizes content distribution workloads

NEW

Performance increase
- Client writes at up to 4 Gbps

Tape gateway: Overview and use cases

Virtual tapes presented to on-premises backup applications



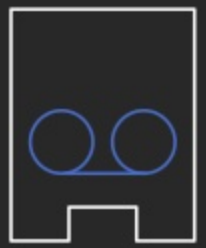
Use cases

- Tape based backup with existing backup apps
- Archive to Glacier

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Southern OREGON UNIVERSITY

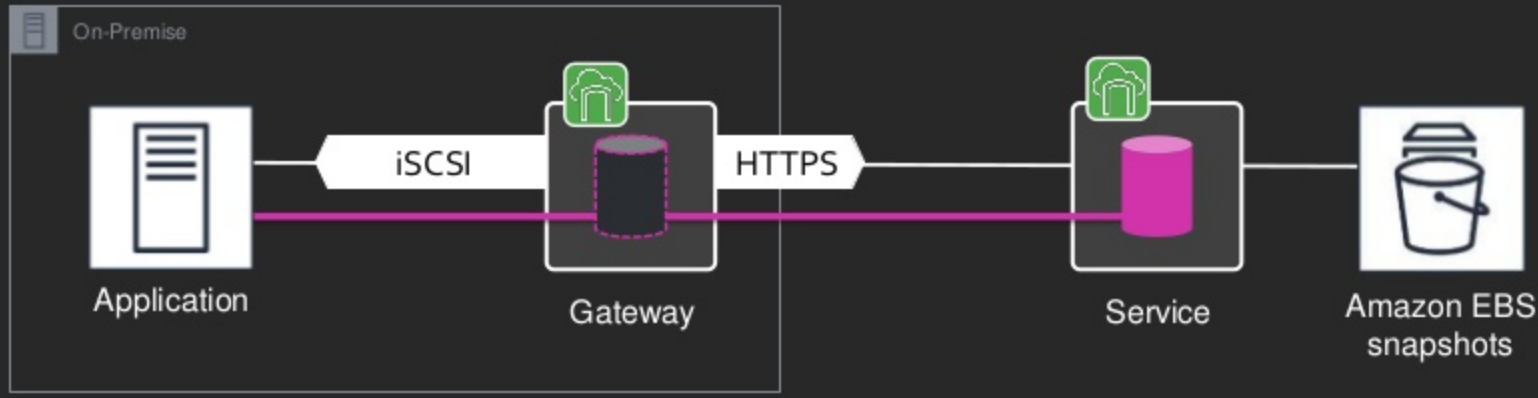
Tape gateway



- Emulates physical tape library through iSCSI-VTL protocol
- Fully managed local cache for recent backups
  - Read-through, write-back, LRU managed
- Virtual tapes stored in Amazon S3
- Ejected virtual tapes archived read-only in Amazon Glacier
- Retrieve archived tapes to library (3–5 hours)
- Configurable encryption SSE-S3 or SSE-KMS
- Compatible with all leading backup software
- NEW New backup apps: IBM Spectrum Protect, Bacula
- NEW Performance increase
  - Client writes up to 2.3 Gbps, downloads up to 0.6 Gbps

Volume gateway: Overview and use cases

Block storage on-premises backed by cloud storage



Use cases

- Backup on-premises data to the cloud
- Migration of volumes to the cloud
- DR to the cloud

STEMCELL TECHNOLOGIES

iRobot

Volume gateway

Connect using the iSCSI block protocol

- Volumes stored in AWS reducing on-premises SAN footprint
- Thin-provisioned (cached) or local (stored) volume types

Fully managed local cache

- Read-through, write-back, LRU managed

Configurable encryption with SSE-S3 or SSE-KMS

Volume snapshots stored in Amazon EBS

Storage Gateway is available on a variety of form factors

	Virtual machines	Amazon EC2	New Hardware appliance
	vmware ESXi, Microsoft Hyper-V		
Where	Corporate data centers	In AWS	Remote locations, branch offices
When	Leverage existing VM infrastructure	In-cloud data retrieval/access/DR	Out of the box simplified experience

Hardware appliance: Easy as 1, 2, 3 …

Simple procurement

Purchase on amazon.com with your Amazon or Amazon business account

Simple installation

1U rack-mounted appliance ships with Storage Gateway software pre-installed

Manage from AWS

Add and remove gateways on the appliance from AWS console. Software is automatically updated.

Hardware appliance: Configuration, redundancy & performance

Gateway configuration

- Supports file, volume (cached) and tape gateways
- Standardized cache and upload buffer configuration

Availability

- Software-based ZFS RAID
- Dual auto-switching power supplies
- Dual boot drives for software

Predictable performance

- Dedicated platform for storage gateway offers predictable throughput performance

Hardware appliance: Configuration, redundancy & performance

Support

- Contact AWS for support; we will engage Dell for hardware support
- Ability to open support channel on local hardware console for remote troubleshooting

Availability

- Sold and ships in the United States
- Use with four AWS US public regions – US East (N. Virginia), US East (Ohio), US West (Oregon), US West (Northern California)

Hardware appliance since launch

From customers

"Reduces need to involve multiple teams"

"Easier setup"

"Faster to market"

"Simplification"

"Managed from cloud"

Industry verticals

Media & Entertainment

Oil & Gas

Insurance

Health Care & Life Sciences

Gaming

Education

Technology

Examples

Constellation

Together for the common good.

Use case: backups

CAL POLY

Use cases: backups, file shares

TEMPUS

Use case: file shares

Building a hybrid cloud storage architecture at CME Group

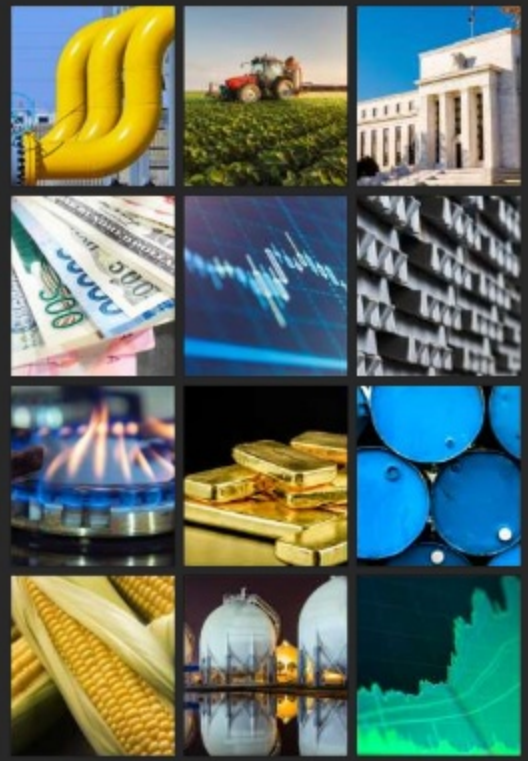
Rick Fath
Senior Director Cloud Architecture
CME Group

Craig Bona
Senior Director Platform Engineering
CME Group

Who is the CME Group?

CME Group

- World's leading and most diverse derivatives marketplace
- Global Distribution in 150 countries
- Connections through 11 Global Hubs
- Relationships with 12 Partner Exchanges
- Annual Revenue of $3.6B
- Notional Value of over $1 Quadrillion



Technology at CME Group

Ultra low-latency trading platform, measuring in µs

24x6 uptime requirements in highly regulated environment

Hundreds of private interconnections to customers and peers

Desire for more flexible compute, and to retire legacy systems and storage

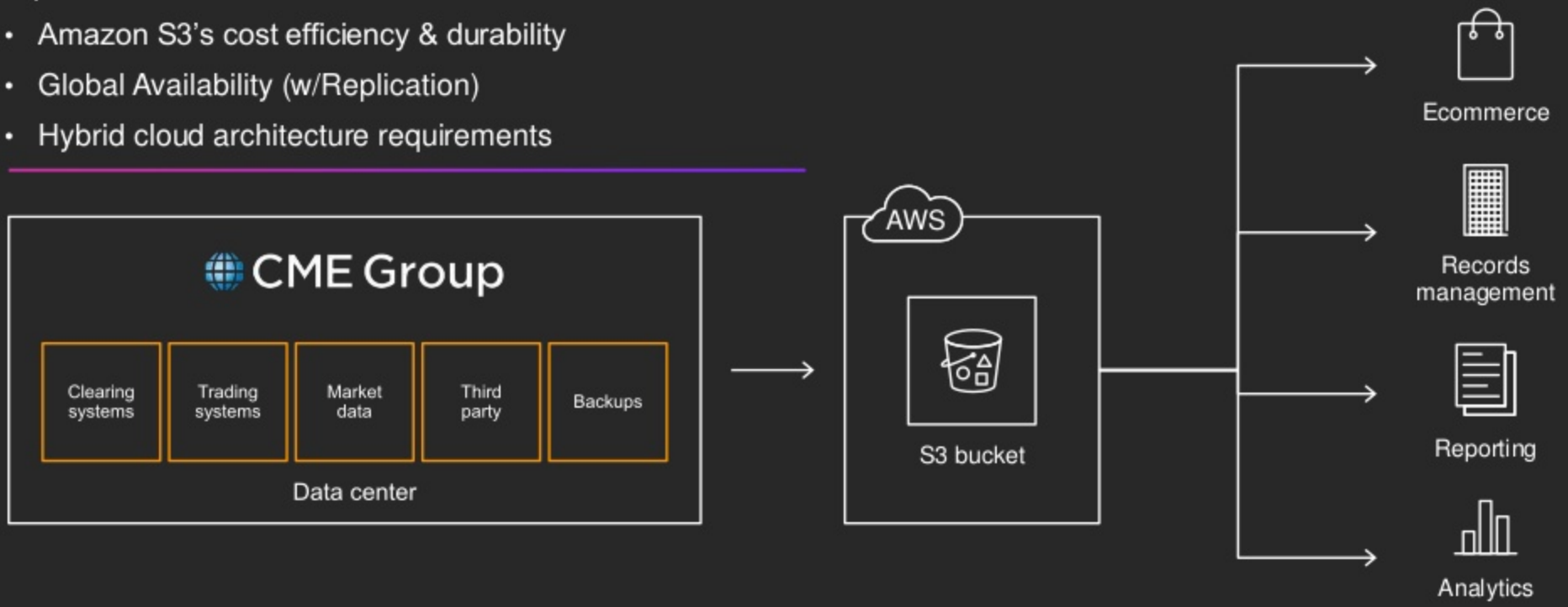
Need to partner with cloud-native vendors

Rapidly escalating storage needs (and costs)

Importance of Amazon S3 to our hybrid strategy

Operational Drivers

- Amazon S3's cost efficiency & durability
- Global Availability (w/Replication)
- Hybrid cloud architecture requirements



Life before…

IAM User Rotation—manual effort, dependent on application teams for coordination

Developer overhead—too many custom applications w/ secret management for simple Amazon S3 operation

Network path to Amazon S3—force Direct Connect for security and egress costs

Encryption—Developers had to code keys to be used which was out of our organizations control

No protection from connection failures

Existing cloud storage “off load” solutions at CME – propriety encryption, unnecessary middle-man, unable to scale

Notable use cases

Data Distribution / e-Commerce with Public Web and FTP Sites

Historical and ongoing data migration to Amazon S3

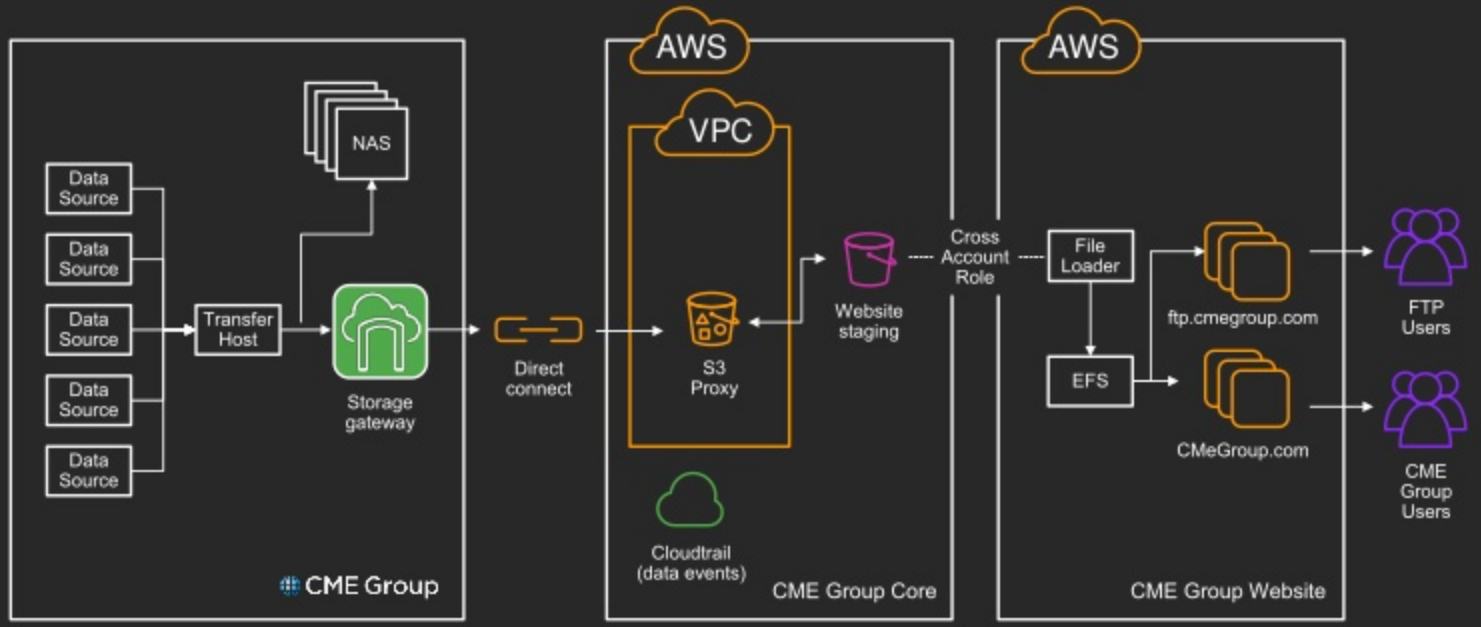
Data analysis and reporting workflows

Use case 1: distribution with Public Web and FTP Sites

Migration of Web and FTP solutions to AWS Frontend in segmented account

100+ legacy jobs transferring data to public sites

Leverage SGW with existing orchestration tool to minimize impact



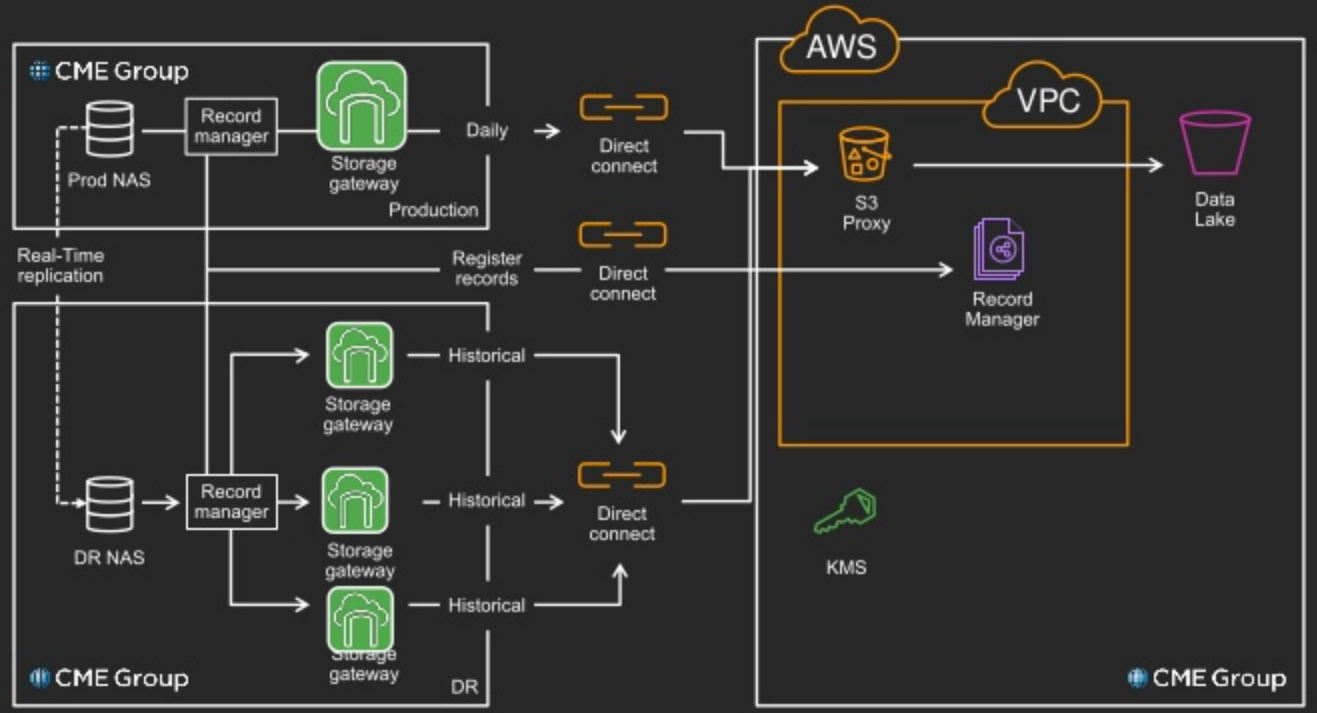
Use case 2: historical and ongoing data migration to Amazon S3

+10 years worth of data
- 5TBs Daily
- 500Tbs History

One-time bulk migration, plus daily uploads for records retention

Utilize idle DR Direct Connect to upload TBs of historical data to S3

Add multiple gateways to introduce more parallelism

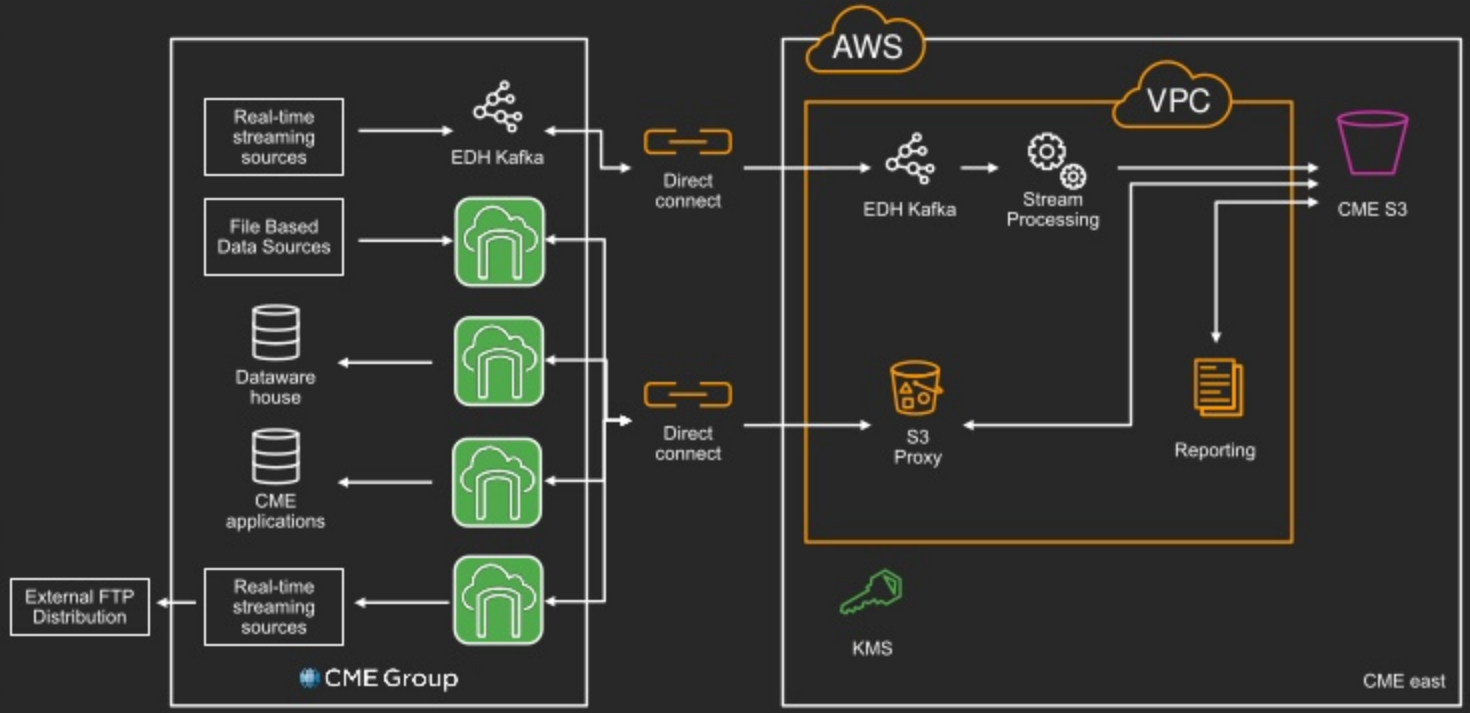


Use case 3: data dissemination in hybrid environment

Simplify Access to data for applications in Hybrid environment and leave Heavy Lifting in cloud

Separate Gateways provide fine-grained control to portions of a Bucket

Leverage Gateway cache to optimize for reads



Life after…

IAM User Rotation—manual effort, dependent on application teams for coordination

Developer overhead—too many custom applications w/ secret management for simple Amazon S3 operation

Network path to Amazon S3—force Direct Connect for security and egress costs

Encryption—Developers had to code keys to be used which was out of our organizations control

No protection from connection failures

Existing cloud storage “off load” solutions at CME – propriety encryption, unnecessary middle-man, unable to scale

Future considerations

AWS Transfer for SFTP

A new managed SFTP service we plan to use to

- Reduce operational costs of existing services
- Enable easier more secure methods to share data with external vendors

Cloud-native interactions with customers and vendors

Data Science workloads allowing new teams access to large data sets with AWS-native services

File gateway deep dive

Objects in Amazon S3 accessed as files on-premises

Each file share maps to an Amazon S3 bucket

- Up to 10 file shares per gateway

Each file share accessed by either NFS or SMB

- Share access restricted by IP (NFS) and password / AD (SMB)

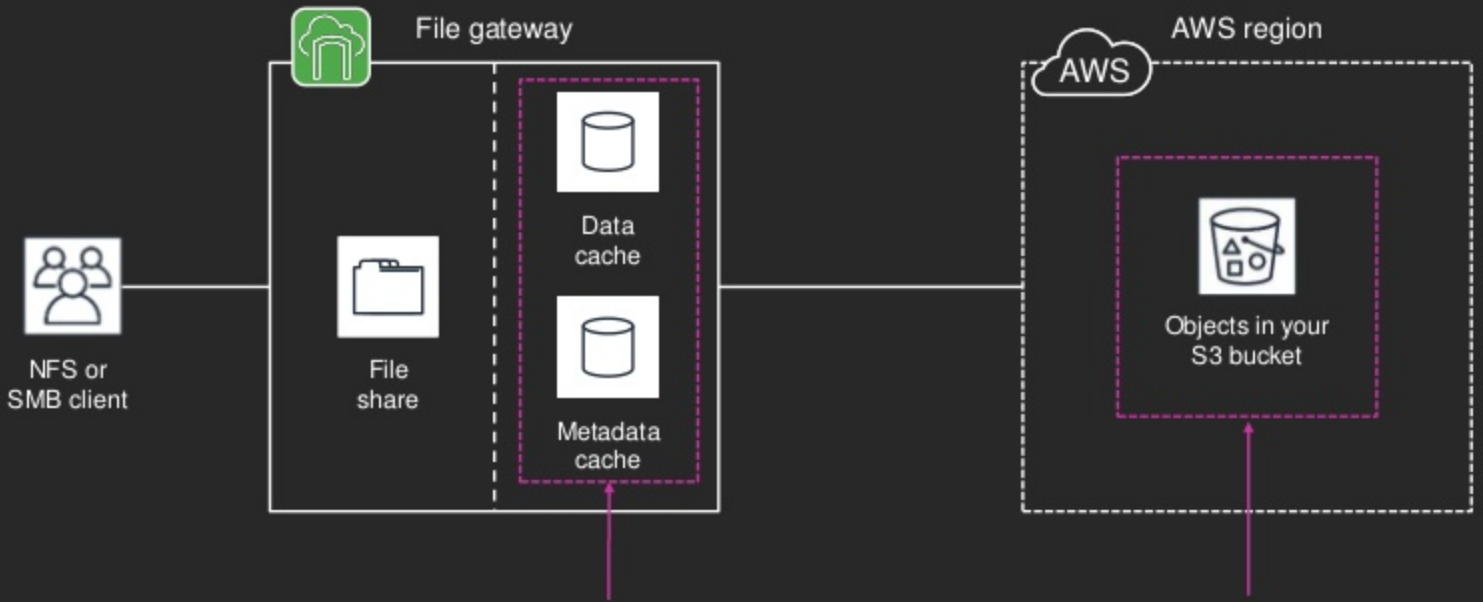
Each file is an object in Amazon S3

- Files access restricted by POSIX permissions
- File metadata stored in S3 object user metadata

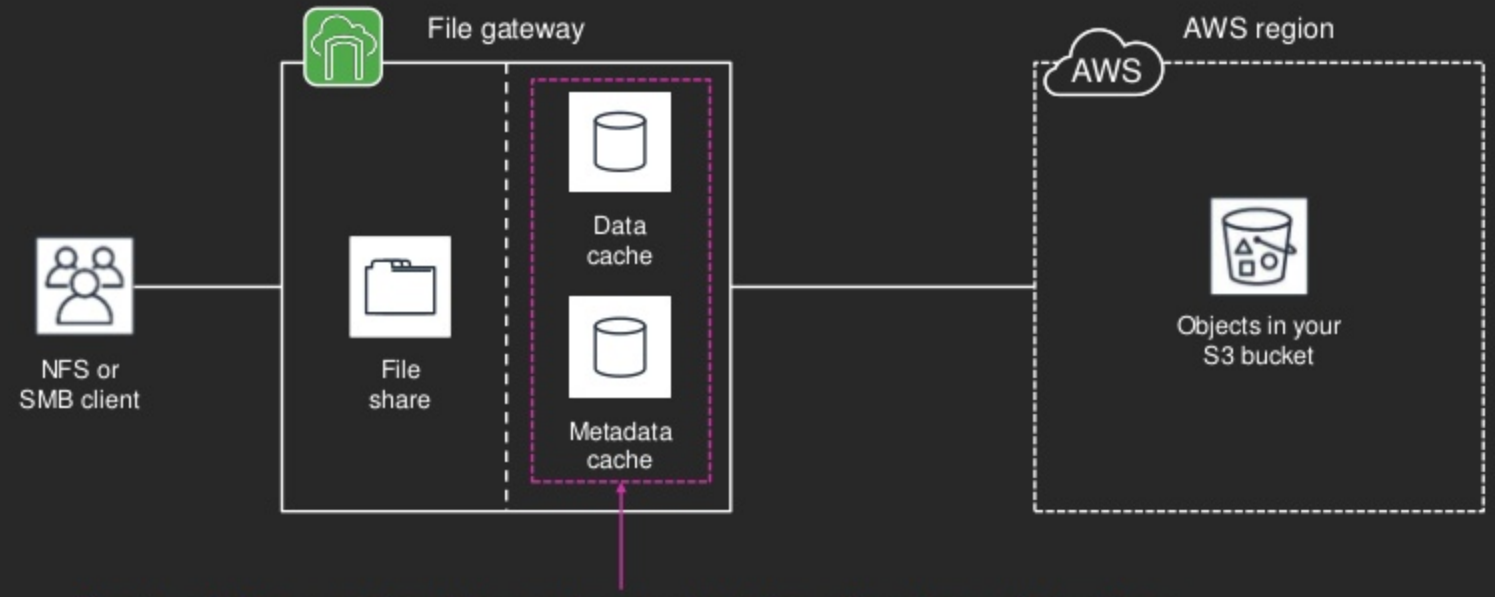
All operations are performed against local cache

- Read-through / write-back

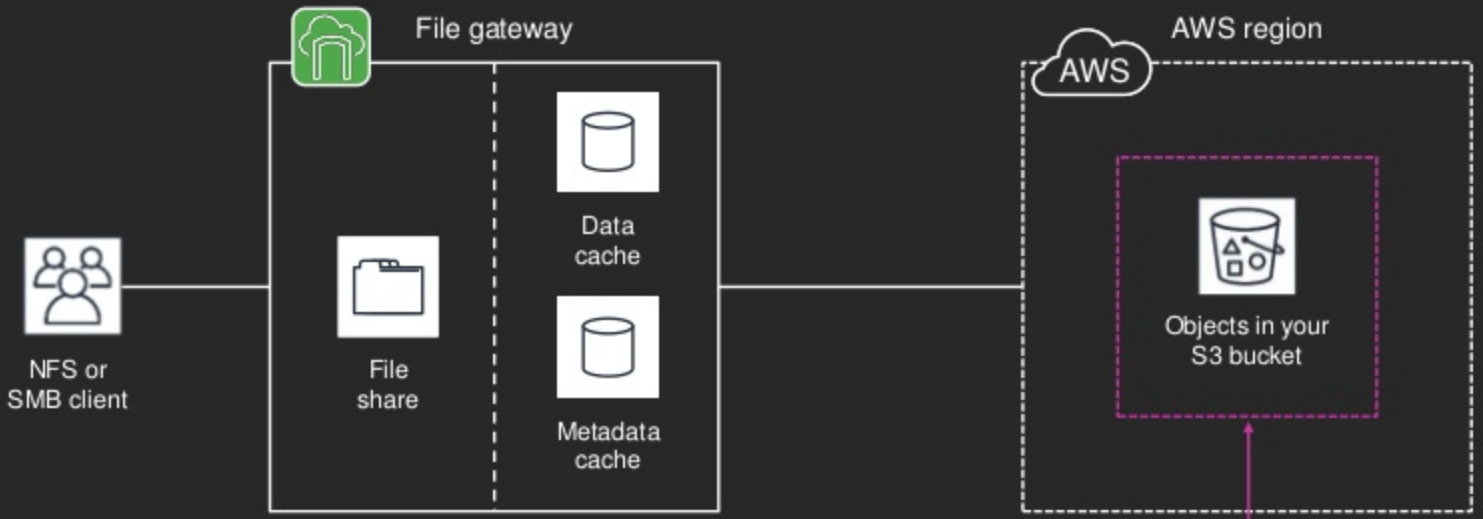
Objects in Amazon S3 accessed as files on-premises



Objects in Amazon S3 accessed as files on-premises

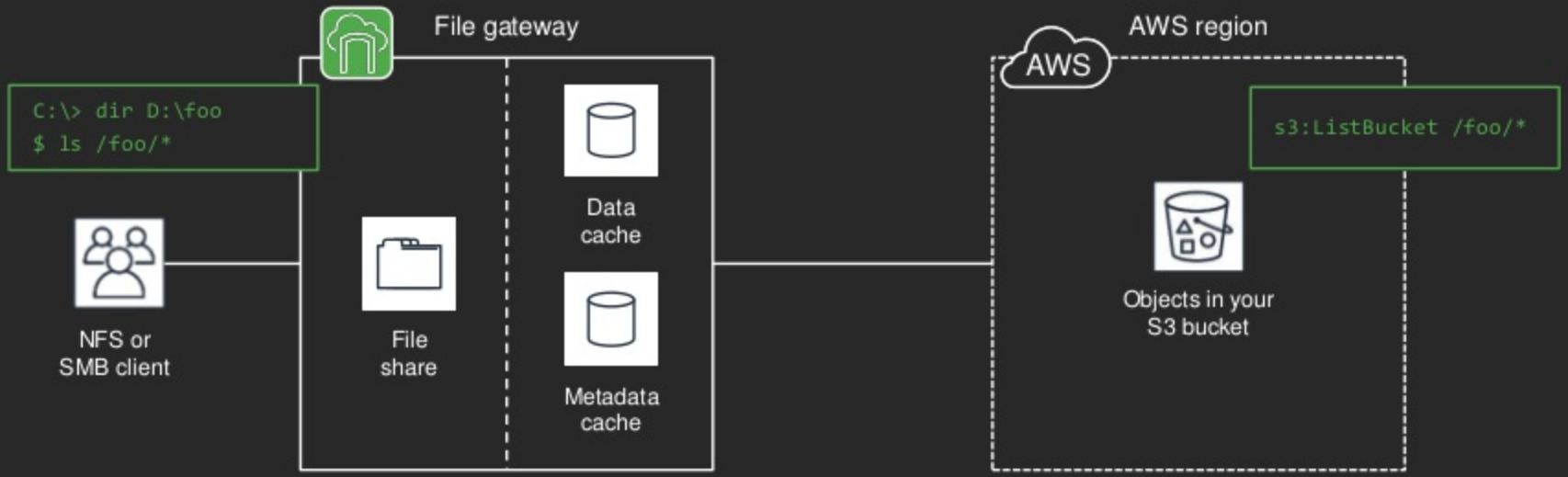


Objects in Amazon S3 accessed as files on-premises



Gateway assumes IAM role to PUT/GET from your bucket
Configure storage class, encryption with AWS KMS, MIME type, requester pays, …

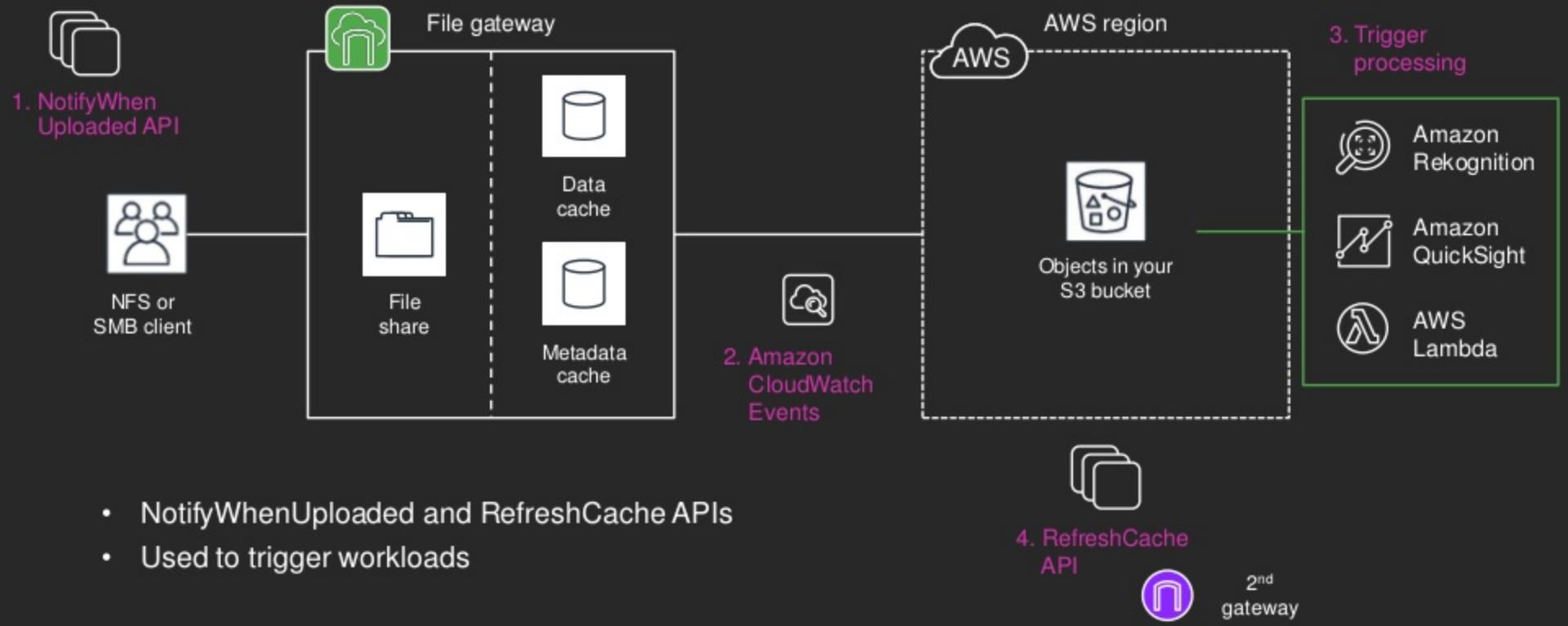
Cache management and file to object conversions



- File writes asynchronously uploaded to S3 objects
- Small writes aggregated into S3-sized PUTs
- Parallel MultipartPUTs
- Validation and automatic error handling
- CopyPUTs to optimize change objects

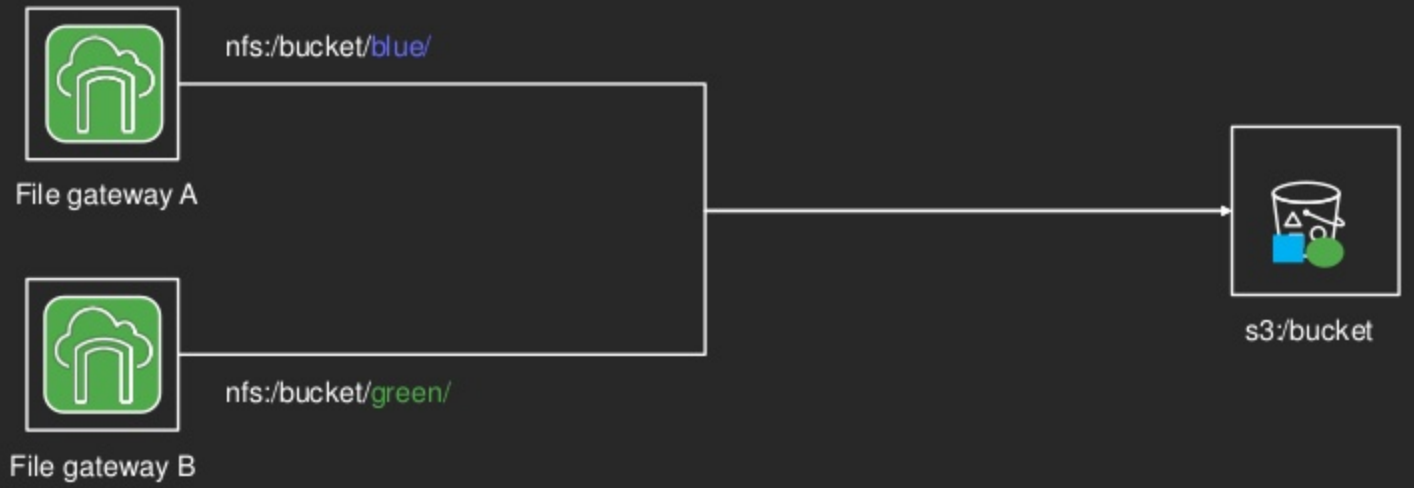
- File reads synchronously cached from S3
- Byte-range GETs from S3 with predictive pre-fetching

Active workloads with notifications



- NotifyWhenUploaded and RefreshCache APIs
- Used to trigger workloads

Content distribution: Separate folders

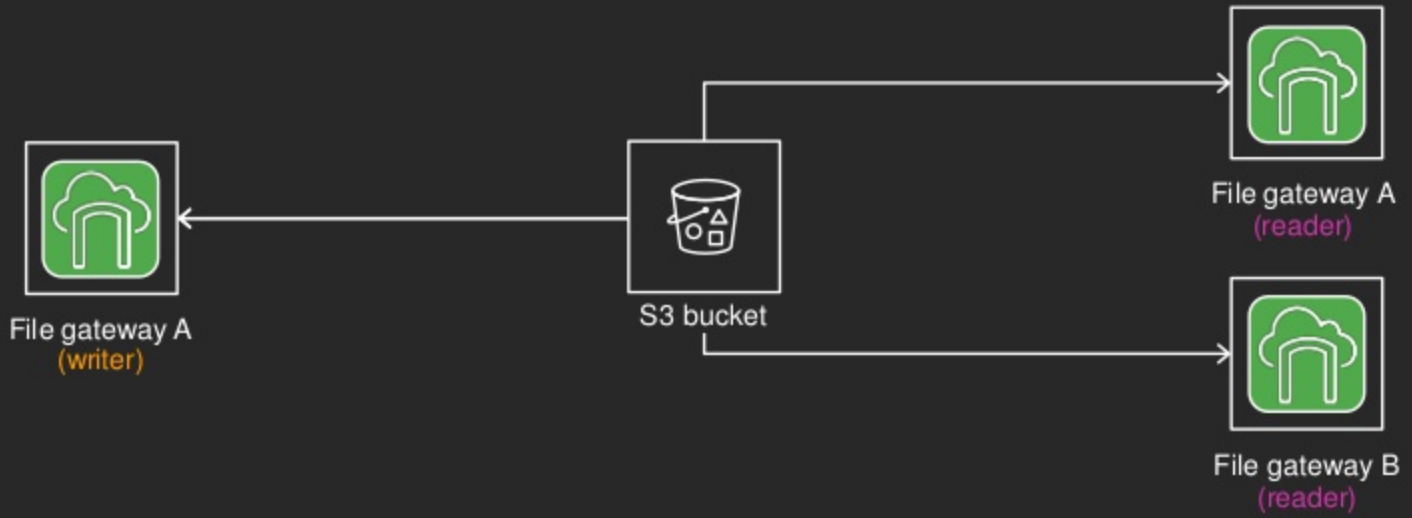


Each gateway mounts the bucket with a unique prefix

(+) Safe multi-write; no object collisions

(-) Can't share between A and B

Content distribution: Single writer, multiple readers

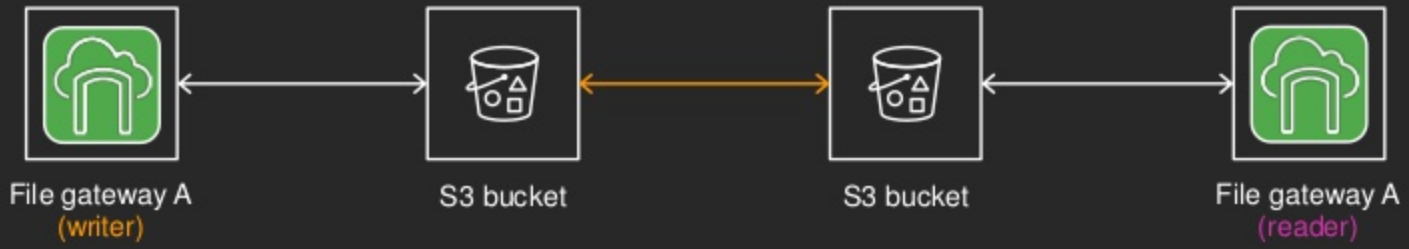


Single writable file share, multiple read-only file shares

Read-only call RefreshCache periodically or with UploadNotification

Can scope RefreshCache to refresh by folder to improve performance

Content distribution: Cross Region Replication



Use CRR for replicating your files to buckets in different regions

You can use Cross Region Replication and RefreshCache to distribute content across regions (e.g. regional and branch offices)

Best practices: Optimizing performance

Local storage used for cache

Use SSD / NVMe
Split cache across multiple disks
Adjust the IOPS based on workload by monitoring disks

Parallelize access

Parallel writes
Multiple clients

Scale-out with multiple gateways

Find a logical split for example by folders, tapes, volumes

Using CloudWatch to monitor your on-premises gateway like an AWS service

Client performance

ReadBytes

WriteBytes

Cache performance

CacheHitPercent

CachePercentUsed

CachePercentDirty

Upload performance

CloudBytesUploaded

CloudBytesDownloaded

Best practices: Leveraging Amazon S3 storage classes

Use lifecycle management for write-once workloads (e.g., archival)

Use Amazon S3 Standard for frequently used data

- Reading files in S3 Infrequent Access Classes (S-IA and Z-IA) costs retrieval fees
- Modifying files in S-IA and Z-IA creates new objects and could lead to deletion fees
- Glacier retrieval times leads to IO errors
- Modifying objects in Glacier not supported: retrieve files first

Best practices: Leveraging Amazon S3 storage classes

Use bucket versioning to maintain copies of your files

Setup version lifecycle retention policy

- Each time you change a file, you'll get a new version

To recover/restore an older version

- Use the S3 API/Console to replace the current object with the old object
- Then call RefreshCache to update the file in the gateway

Storage Gateway in summary

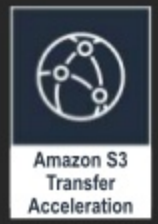
Storage Gateway in summary

Feature	Benefit
Standard storage protocols	No changes to existing applications
Fully managed cache	Low latency access to frequently used data
Automatic and optimized data transfer	Minimizes network bandwidth
Automated Hybrid workflows	Leverage in-cloud processing
Multiple Deployment options	Supports multiple configurations
Security and compliance	Meets enterprise customer needs
Managed from AWS console and CLI	Simplified management and monitoring
Pay as you go pricing	Cost effective

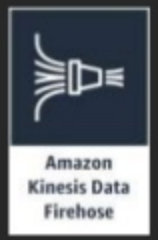
AWS data transfer & hybrid storage

Online data transfer

Edge locations for S3 enabled applications

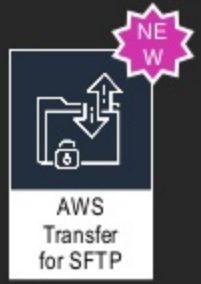


Load streaming data into Amazon S3



Online transfer of active data

Managed file transfers into Amazon S3



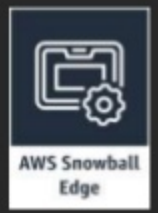
Offline data transfer

Ship static data into and out of Amazon S3

Hybrid storage

Access AWS storage from on-premises

Storage and compute in disconnected environments



How do I get started?

Visit aws.amazon.com/

Drop by one of the demo booths

See one of us

Breakout repeats

Friday, Nov 30

STG-305: Deep Dive Build Hybrid Storage Architectures with Storage Gateway

10:45 – Time | Venetian Level 3 Murano

Related breakouts

Monday, November 26

STG-201: Tape Is a Four Letter Word: Backup to the Cloud in under an Hour

2:30 PM - 3:30 PM | Venetian, Level 2, Titian 2202 - T1

Wednesday, November 28

NEW SERVICE: AWS DataSync

11:30 AM – 12:30 PM | Venetian, Level 4, Lando 4202

Wednesday, November 28

NEW SERVICE: AWS Transfer for SFTP

7:00 PM– 8:00 PM| Aria West, Level 3, Juniper 1 604

Thank you!

Asa Kalavade
kalavade@amazon.com

Paul Reed
paulreed@amazon.com

Please complete the session survey in the mobile app.