AWS Well-Architected Framework

Data Residency and Hybrid Cloud Lens

Data Residency and Hybrid Cloud Lens: AWS Well-Architected Framework

Table of Contents

Data Residency with Hybrid Cloud Services Lens - AWS Well-Architected

Publication date: **April 3, 2025** (*Document revisions*)

This paper describes the Data Residency with Hybrid Cloud Services Lens (DRHC) Lens for the AWS Well-Architected Framework. The document provides general design principles, as well as specific best practices and guidance for hybrid cloud workloads with data residency requirements following the six pillars of the AWS Well-Architected Framework.

Introduction

This lens is a comprehensive guide to best practices for designing and operating Well-Architected hybrid cloud workloads with data residency requirements. The DRHC Lens is a valuable resource offering practical recommendations to help you optimize your DRHC workloads for security, reliability, operational excellence, performance, cost optimization, and sustainability.

Drawing from our extensive experience in architecting cloud solutions, this lens provides a holistic approach to addressing the unique challenges and considerations involved in managing data residency requirements while benefitting from a hybrid cloud environment.

Key topics covered in the DRHC Lens include:

- Designing resilient and highly available hybrid cloud architectures
- Data sovereignty and compliance with local laws and regulations
- Implementing robust security measures across on-premises and cloud environments
- Optimizing costs through cloud elasticity and hybrid cloud solutions
- Automating processes to optimize operating DRHC workloads

By following the principles and best practices outlined in this lens, you can unlock the full potential of your hybrid cloud infrastructure. Use this document to seamlessly integrate your resources in the cloud and on-premises resources while maintaining control over your data's geographic location to be compliant with local laws and regulations.

Custom lens availability

Custom lenses extend the best practice guidance provided by AWS Well-Architected Tool. AWS WA Tool allows you to create your own custom lenses, or to use lenses created by others that have been shared with you.

To determine if a custom lens is available for the lens described in this whitepaper, reach out to your Technical Account Manager (TAM), Solutions Architect (SA), or Support.

Definitions

The following definitions are provided related to Data Residency and Hybrid Computing for AWS customers using the Well-Architected Framework. For additional information, see AWS Glossary.

AWS definitions

- **AWS Outposts Server:** AWS Outposts Servers are rack-mountable servers in 1U and 2U form factors for locations with limited space or smaller capacity requirements.
- **AWS Outposts rack:** AWS Outposts rack is a fully managed service that extends AWS infrastructure, services, APIs, and tools on premises for a truly consistent hybrid experience.
- **AWS Local Zones:** AWS Local Zones are a type of infrastructure deployment that places select AWS services closer to your end users and workloads.
- **Region:** AWS Regions are physical locations around the world where we cluster data centers. We call each group of logical data centers an Availability Zone. Each AWS Region consists of a minimum of three isolated and physically-separated Availability Zones within a geographic area.
- **Availability Zone (AZ):** One or more discrete data centers with redundant power, networking, and connectivity in an AWS Region.
- **Parent Availability Zone or Region:** The Region and Availability Zone pair that the Outposts service connects to in the Region.
- **Local gateway:** A local gateway connects your Outpost subnets and your on-premises network.
- **Service link:** The service link is a necessary connection between your Outposts and your chosen AWS Region (or home Region) and allows for the management of the Outposts.

Industry definitions

- **Data residency:** The requirement of keeping data in a certain region or country to comply with local laws and regulations.
- **Data sovereignty:** Refers to an organization or country's ability to have full control and ownership over the data they generate and store, including where that data is stored, who can access it, and providing resilience and independence from external factors. Key aspects include data residency, operator access restrictions, resiliency and survivability, and technological independence.

- **Low latency:** A technical use-case where application components need under ten millisecond latency between each other.
- **Local data processing:** A technical use-case where it is optimal to process the data where it is generated (locally) as opposed to sending it to a cloud region. This could be due to transfer costs, transfer time, and the size of the dataset.
- **Control plane:** Provides the administrative APIs used to create, read or describe, update, delete, and list resources. Example control plane actions are launching a new Amazon EC2 instance, creating an Amazon S3 bucket, and describing an Amazon SQS queue. When you launch an Amazon EC2 instance, the control plane has to perform multiple tasks such as finding a physical host with capacity, allocating the network interface, preparing an Amazon Elastic Block Store (Amazon EBS) volume, generating AWS Identity and Access Management (AWS IAM) credentials, adding the security group rules, and more. Control planes tend to be complicated orchestration and aggregation systems.
- **Data plane:** Provides the primary function of the service. For example, the data plane includes the running Amazon EC2 instance itself, reading and writing to an Amazon EBS volume, getting and putting objects in an Amazon S3 bucket, and Amazon Route 53 answering DNS queries and performing health checks.

Design principles

There are four general design principles to facilitate good design for hybrid cloud workloads. These design principles help keep data where it needs to be to meet regulatory or compliance needs. The design principles are as follows:

- **Classify data:** To comply with data residency requirements, it is important to understand and classify which workloads and which datasets need to stay on-premises and which ones can be moved to the Region.
- **Establish operational practices for data sovereignty:** Once you have identified which datasets and workloads needs to stay on-premises (Outposts) or in a certain geographical location with Local Zones, build an operational model with your teams to have different processes and procedures for the different data classifications. This can include different AWS accounts with the correct privileges and custom nomenclature for sensitive workloads for easy identification.
- **Use Regional cloud services to augment on-premise solutions:** Although Local Zones and Outposts rack come with a subset of the services available in the Region, customers should use Regional services such as AWS Organizations, AWS Control Tower, and IAM Access Analyzer to provide data residency and regulatory compliance. Use Regional services to offer your builders pre-approved configurations, self-service provisioning, and service quotas.
- **Automate infrastructure:** Consider building different automation runbooks or automation stacks based on the type of data that is being used or stored inside a workload. Your operational teams can build compliant technical stacks quickly while removing the manual work that introduces mistakes (for example, sending a regulatory workload to the Region by accident).

Summary of key DRHC practices across the six Well-Architected Framework pillars

Operations: Achieving operational excellence for hybrid edge workloads

Operational excellence for hybrid edge workloads focuses on effective system operations, gaining operational insights, and continuous process improvement to deliver business value. It involves understanding data residency regulations and organizational policies, considering Recovery Time Objective (RTO) and Recovery Point Objective (RPO), and being aware of consequences of data residency violations or data loss. Key steps include monitoring performance, managing incidents, centralizing oversight, automating processes, updating policies, and fostering continuous improvement to enhance operational efficiency and reliability. For more information on Operational excellence, see Operational excellence pillar.

Security: Protect information, systems, and assets through risk assessments and mitigation strategies, balanced with delivering business value

The security design principles for data residency focuses on establishing control objectives, separating workloads based on data residency needs. Configuring detection mechanisms for unauthorized resource creation. Restrict physical access to AWS Outposts locations, and comply with environmental and networking requirements. Control data access tightly, and use data recovery mechanisms like snapshots, versioning, and replication on Outposts. For more information on Security, see Security pillar.

Reliability: Build reliable infrastructure services

Verify application recovery or availability during component failures (network, server, rack, and application). Deploy multiple Outposts anchored to multiple Availability Zones for high-availability and resiliency, and plan for disaster recovery with Outposts or Local Zones. Monitor and forecast storage, compute, and network capacity regularly while planning for high availability during on-premises maintenance activities. For more information on Reliability, see Reliability pillar.

Performance: Align services, configurations, and monitoring for efficient and adaptable workloads

Select the appropriate AWS services, Regions, and configurations that align with your workload requirements, and consider factors like latency, bandwidth, and data residency. Monitor performance metrics end-to-end, and adjust resources accordingly. Embrace modularity and loose coupling to easily integrate new technologies as they emerge. Periodically review your architecture, and make informed trade-offs based on evolving application needs, technical requirements, and the expanding AWS service offerings. For more information on Performance, see Performance pillar.

Cost optimization: Optimizing costs in hybrid cloud environments through tagging, monitoring, and workload placement strategies

Evaluate workload requirements to help determine the optimal placement across on-premises, cloud, and hybrid edge environments. Implement a tagging strategy for cost attribution and resource governance across hybrid environments. Monitor and optimize the utilization of fixed-capacity resources like Outposts to provide maximum value. Optimize network configuration and data transfer costs between these environments. Hybrid architectures should be designed with cost in mind, using local VPC peering and following networking best practices. Regularly monitor and review your workloads to identify opportunities for ongoing cost optimization over time. For more information on Cost optimization, see Cost optimization pillar.

Sustainability: Prioritizing renewable energy, efficient resource utilization, and continuous optimization

While designing sustainable cloud solutions, prioritize Region selection based on proximity to renewable energy sources and CO2 emissions. Align infrastructure scaling with demand through auto scaling, monitoring, and right-sizing to optimize usage with minimum resources. Optimize software architecture by refactoring unnecessary components and resizing over-provisioned instances. Manage data efficiently by removing redundant or unneeded data to reduce storage requirements. Use the minimum hardware and services necessary, continuously monitoring for more energy-efficient options. Foster a culture of keeping workloads up to date to adopt

efficient features and improve overall sustainability. For more information on Sustainability, see Sustainability pillar.

Scenarios

This section explores common data residency scenarios, framing out best practices and implementation guidance within the context of the Well-Architected pillars. These scenarios serve as foundational experiences shaping the guidance offered in the lens. By exploring each case, we provide actionable guidance tailored to the complexities of data residency requirements.

> **Note**
>
> While the following presented guidelines for data residency, you should consult internally with legal and security teams for specific organizational requirements.

Before exploring the scenarios detailed in this section, it is essential to make an informed design choice to meet your specific legal and compliance requirements using AWS building blocks.

While AWS provides a wide range of tools and resources to help support your infrastructure, it is ultimately your responsibility to comply with local laws and regulations. As described in the AWS Shared Responsibility Model, we encourage you to engage with your legal and compliance teams to thoroughly assess your needs. To support these discussions and help you make informed decisions that account for potential trade-offs, consider the following key points:

Application summary information

- Provide a brief description of the application.
- List the countries and industries the application will serve.
- Describe the application's main functions and the key data types it handles. Detail the data classification conducted for individual fields in the datasets handled by the application
- Specify your Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- Outline any significant timelines for deployment or compliance.

Data residency considerations

- Identify the acceptable use policies (AUP) for the data managed by the application. If these policies are not yet established, consider creating them. This should involve:
  - Conducting data classification exercises.

  - Aligning the data with relevant data privacy laws and industry-specific regulations.
  - Thoroughly detailing the use-cases that need support, such as data and analytics model building, digital forensics, or law enforcement. Additionally, clarify the permissible locations for storing and processing this data, and explore the possibilities for encryption, masking, or tokenization to anonymize data.
- Once sensitive data is identified and the use-cases are clearly defined, determine how the application separates the storage and processing of sensitive data from non-sensitive data.

> **Note**
>
> Some regulators require additional guarantees that the same person would never have access to both the regulated and non-regulated data points.

System design requirements

- Evaluate the requirement for low-latency access, identifying specific latency targets, and determine whether the data needs to be accessible on-premises or by external applications. To provide maximum resilience, test your application flows that transit the AWS network between Regions and Local Zones or Outposts against the maximum latency expected for your applications.
- Is there a need for data to be shared across borders or exported from its primary storage location? If so, identify the parties involved, detail how the data transport is secured, and describe any adequacy or reciprocal agreements that are in place.

Compliance and monitoring

- Determine the necessary level of logging and whether logs can be centralized in an AWS Region.
- Identify required audit information for system events, access control, and configuration management.

Backup and recovery

- Establish the backup and recovery strategies required for your business needs, and specify the retention period for stored data.

- Assess if these can be stored centrally in an AWS Region.

> **Note**
>
> Outposts and Local Zones (LZs) act as an extension to an AWS Availability Zone (AZ). However, for disaster recovery (DR) purposes, store backups across multiple Availability Zones and, where possible, in multiple Regions. The Availability Zone that connects to the Outposts or Local Zone should not be used as a backup, which provides greater resilience and protection against failures in the primary Availability Zone.

Data access and security

- Assess if there are any geographical or logical data viewing restrictions.
- Address data privacy concerns by asking if the data going to be shared internally. If so, please list the use cases.

Reporting and data management

- Detail the reporting requirements involving in-scope data, including whether aggregated in-scope data can be used for reporting purposes. Assess if these reporting activities can be managed from outside the jurisdiction.
- Determine if in-scope data is used for business logic or solely for reporting purposes.

Navigating data residency scenarios

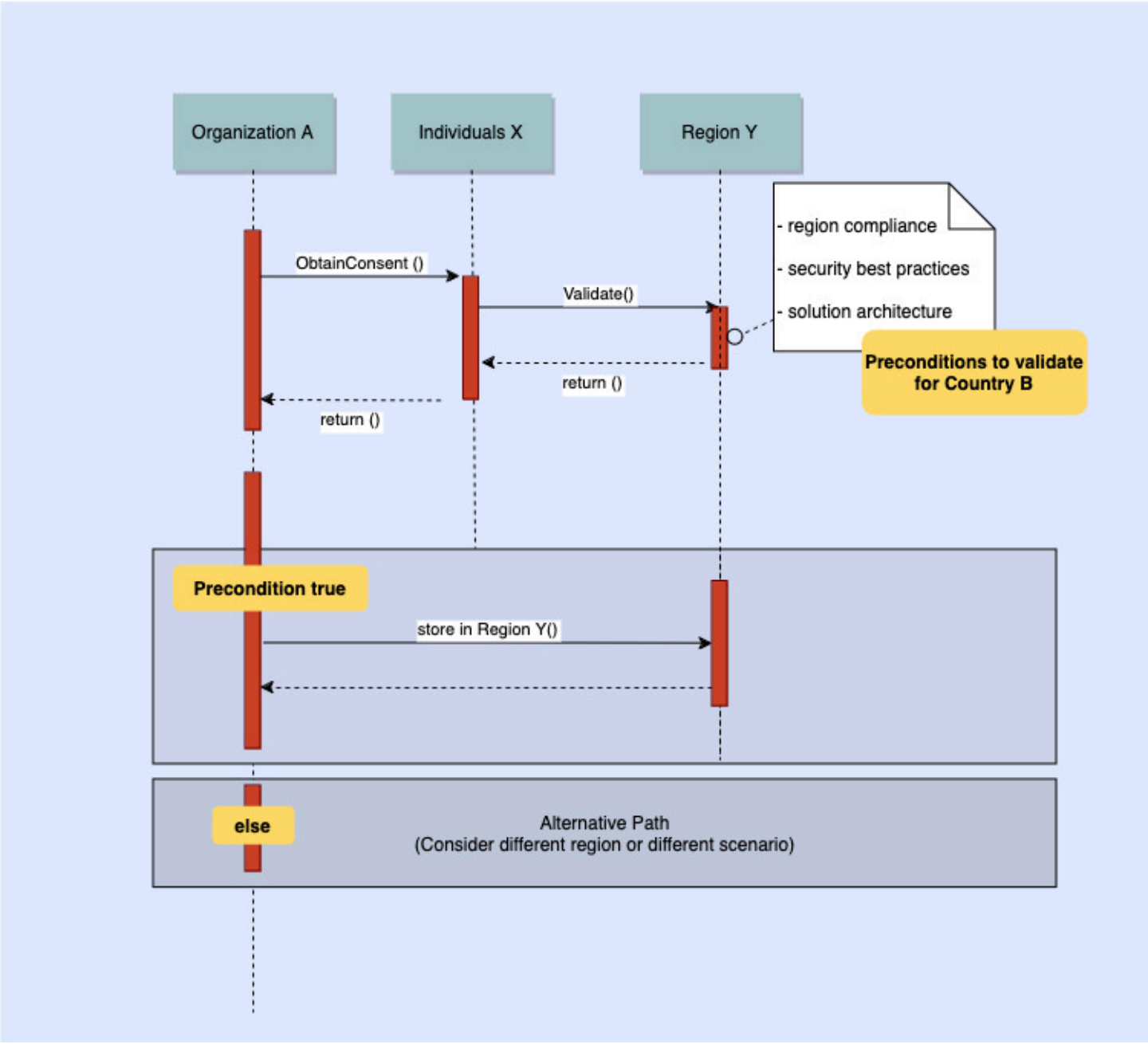
The following scenarios are presented in order of increasing data residency constraints, from the least to the most stringent requirements. This structure is intended to help you easily identify the level of data residency requirements relevant to your needs.

Scenarios

- Scenario A: User and audit consent for data storage outside country
- Scenario B: Sharing data across countries that adhere to same specific set of standards
- Scenario C: Maintain primary service copy within country or jurisdiction
- Scenario D: In-scope data must be stored and processed in country

Scenario A: User and audit consent for data storage outside country

This scenario covers situations where regulations allow data storage outside the country with user consent as data subjects or the permission or notification of the regulators (or both).



Scenario A

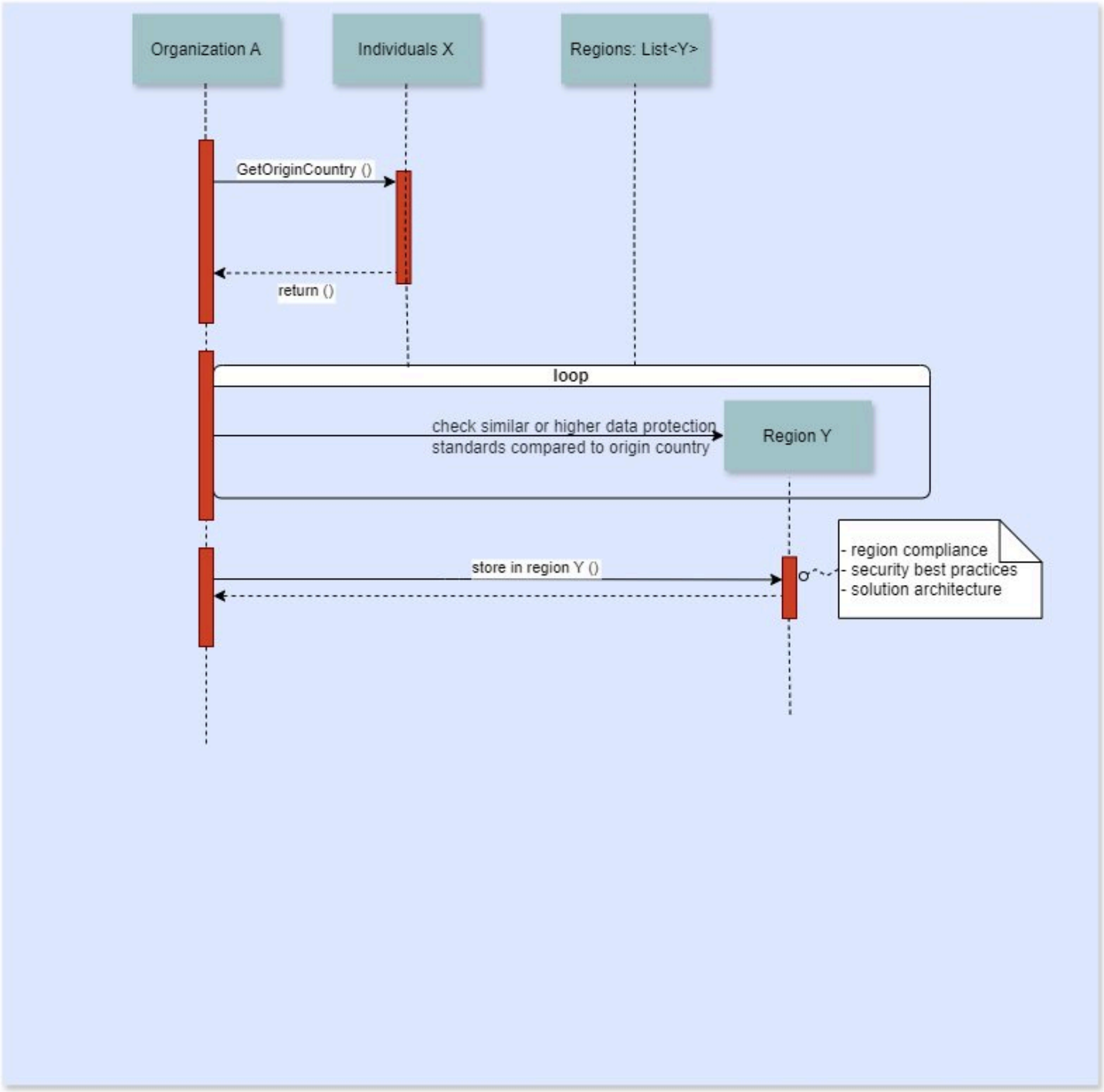
The use case diagram depicts the following:

- Organization A in Country B seeks consent from Individuals X (the data subjects).

- Validation checks the consent and verifies compliance.
- A precondition is validated based on Country B's regulations, which must be met before storing data in Region Y.
- If the precondition is satisfied, the data can be stored in Region Y, which may be outside of Country B. This suggests that the data storage could occur in a different geographical region while still complying with Country B's legal requirements.
- If the precondition fails, an Alternative Path is triggered, which may involve considering a different region or scenario that meets compliance requirements.

Scenario B: Sharing data across countries that adhere to same specific set of standards

Transfer of in-scope data may be allowed to countries that adhere to the same specific set of standards (or higher) than the originating country with permissions or notification to the regulators.



Scenario B

This diagram shows the process of selecting a Region to store data based on its origin country:

- Organization A retrieves the origin country of the data from Individuals X.

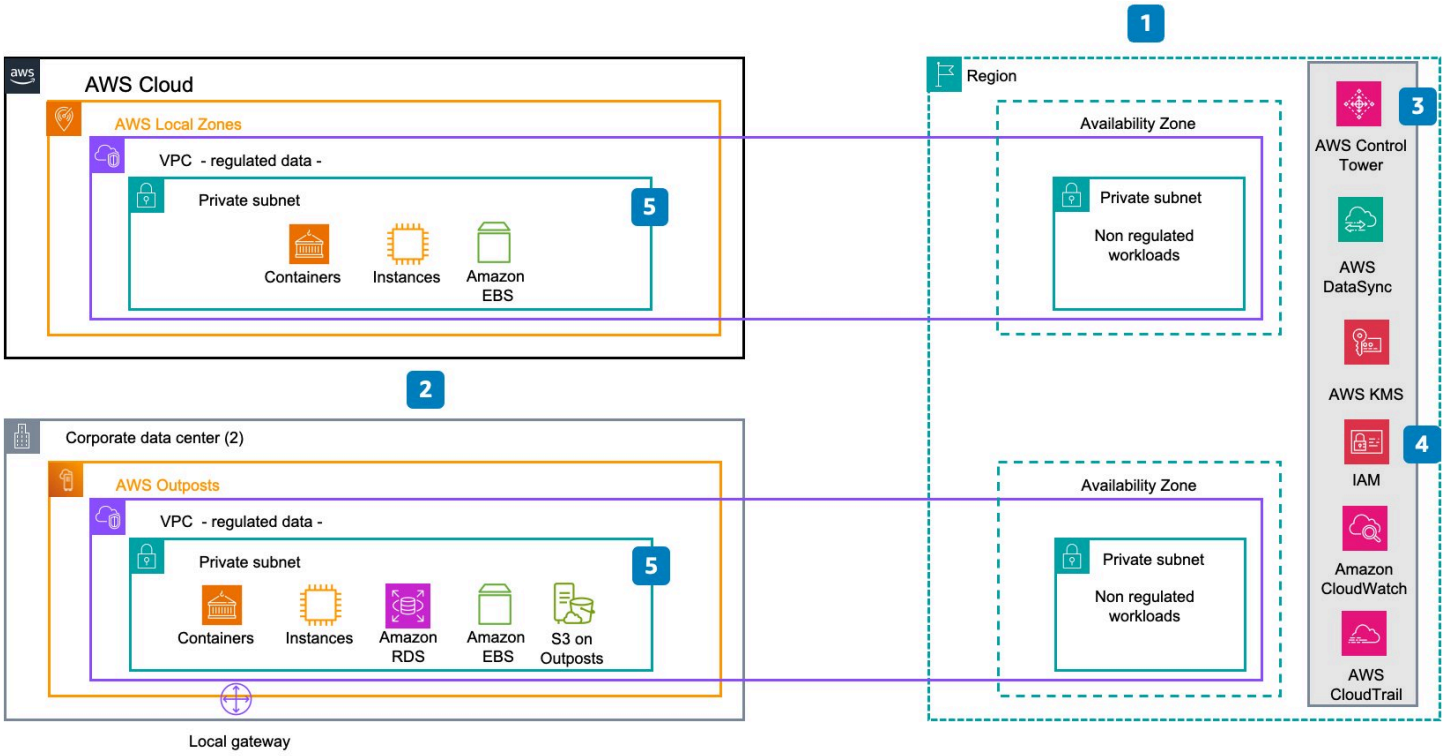
- Organization A checks available Regions for different countries that potentially have similar or higher data protection standards compared to the origin country.
- When Region Y meets the requirements, the data is stored in that Region.

Scenario C: Maintain primary service copy within country or jurisdiction

In a scenario where the law mandates data residency requirements that specify that the primary copy of the data must be maintained within the country or jurisdiction, several factors should be considered.

In this case, in-scope data can be stored or transferred outside the borders, but the primary servicing copy must be held within the border of your jurisdiction.

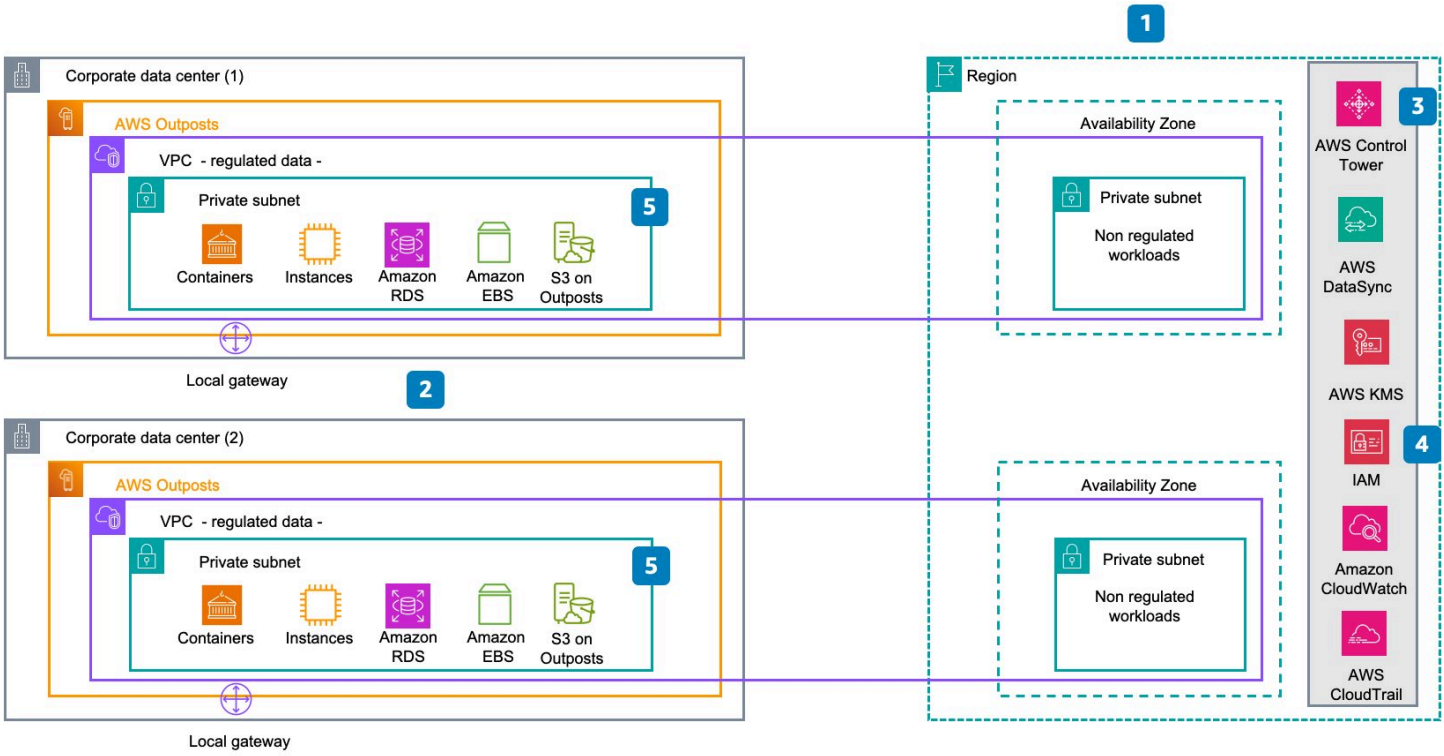
For your deployment needs, you have two options depending on the availability of Local Zones in your location and the specific workloads you need to deploy, as outlined in the following diagrams:



Scenario C, option one: AWS Local Zones

The first option for deploying AWS services specifically focuses on the use of AWS Local Zones and AWS Outposts:

1. Assess data residency requirements specific to the organization and regulatory environment, and identify regulated data.
2. Plan, order, and deploy AWS Outposts racks in the corporate data centers for high availability alongside AWS Local Zones.
3. (Optional) Set up the landing zone for centralized management and governance. Then add the Outpost accounts to your AWS Organization.
4. Configure access levels for your accounts for proper permissions and security.
5. Deploy regulated workloads on AWS Local Zones and AWS Outposts. Optionally, you can configure backups and snapshots to be stored within the Region and synchronize your Amazon S3 data accordingly.



Scenario C, option two: AWS Outposts

The second option for deploying AWS services focuses on the use of AWS Outposts:

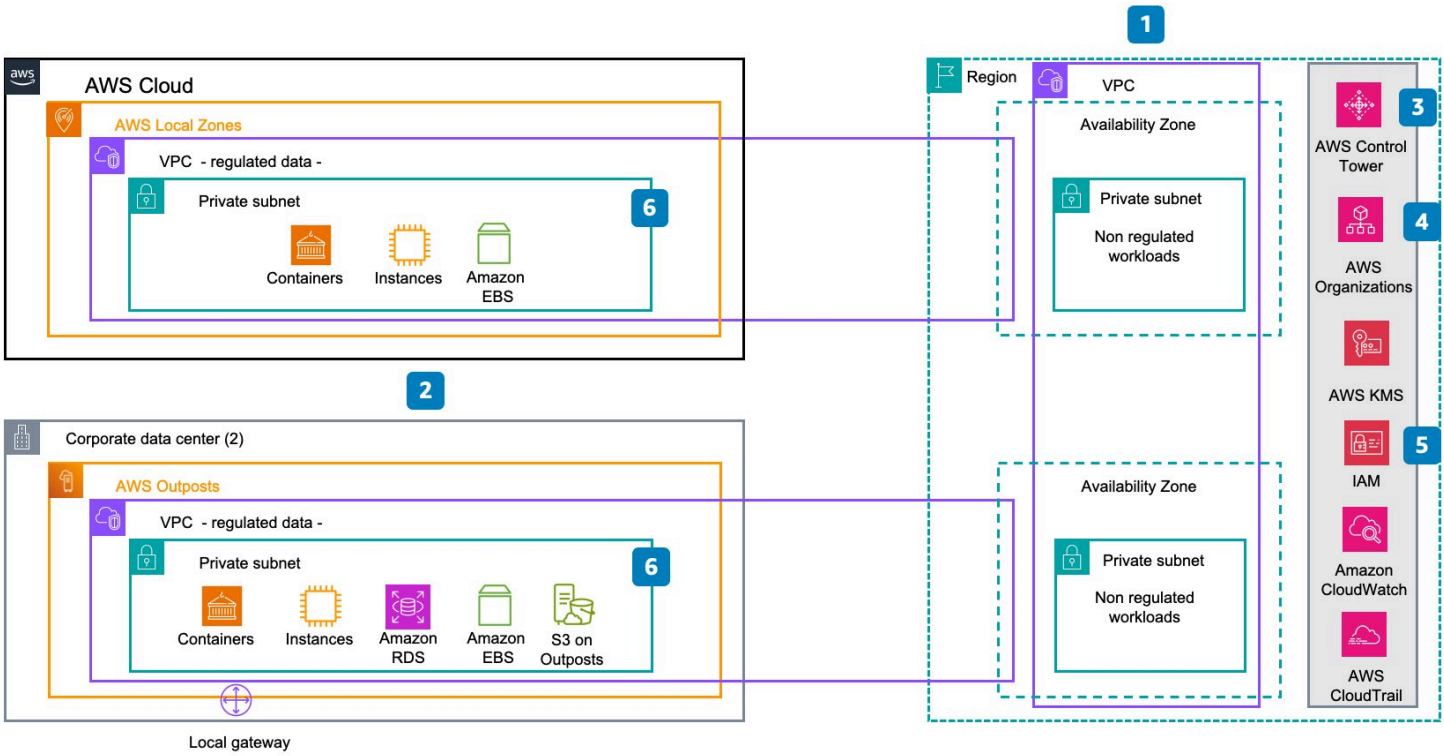
1. Assess data residency requirements specific to the organization and regulatory environment, and identify regulated data.
2. Plan, order, and deploy AWS Outposts racks in the corporate data centers with high availability.

3. (Optional) Set up the landing zone for centralized management and governance. Then add the Outpost accounts to your AWS Organization.
4. Configure access levels for your accounts for proper permissions and security.
5. Deploy regulated workloads on AWS Outposts. Optionally, you can configure backups and snapshots to be stored within the Region and synchronize your Amazon S3 data accordingly.

Scenario D: In-scope data must be stored and processed in country

In a scenario where the law mandates that data must be stored and processed within the borders of a specific country, organizations operating within that jurisdiction must adhere to strict data localization policies.

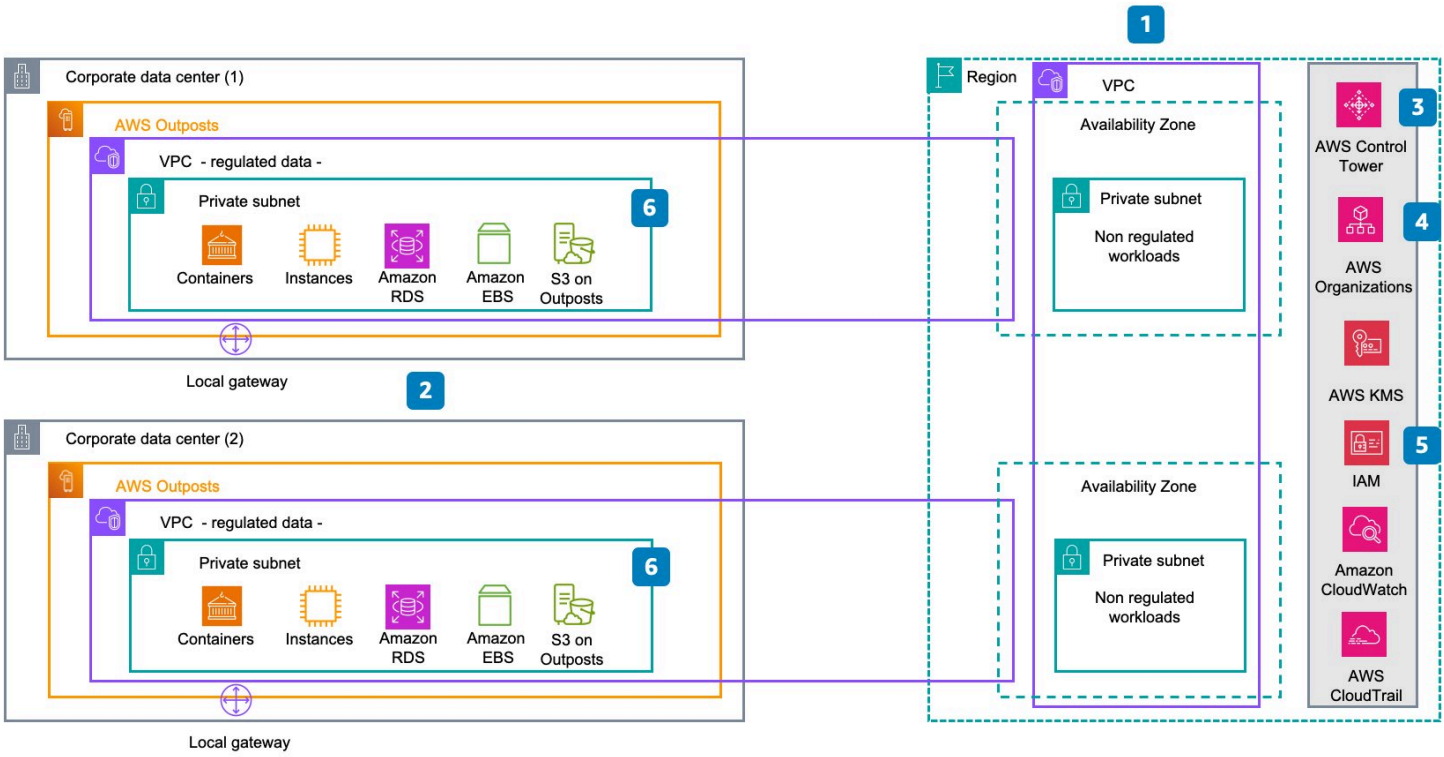
For your deployment needs, you have two options depending on the availability of Local Zones in your location and the specific workloads you need to deploy, as outlined in the following diagrams:



Scenario D, option one: AWS Local Zones

The first option for deploying AWS services focuses on the use of AWS Local Zones and AWS Outposts:

1. Assess data residency requirements specific to the organization and regulatory environment. And identify regulated data.
2. Plan, order, and deploy AWS Outposts racks in the corporate data centers for high availability alongside AWS Local Zones.
3. Set up the landing zone for centralized management and governance. Then add the Outpost accounts to your AWS Organization.
4. Configure service-control policies (SCPs) in the Organizational Unit (OU) that belongs to regulated data, using some or all of the Local Zone data residency custom guardrails. For Outposts, you can use custom controls.
5. Configure access levels for your accounts for proper permissions and security.
6. Deploy the regulated workload on the Local Zone and Outpost.



Scenario D, option two: AWS Outposts

The second option for deploying AWS services focuses on the use of AWS Outposts without AWS Local Zones. Follow steps 1 to 5 as above in Option 1: AWS Local Zones, and deploy the regulated workload on AWS Outposts.

Note: For business continuity and disaster recovery (DR) purposes, backup and snapshot considerations are not included in this step. Since data is being stored within a specific Region or Local Zone, backup or snapshot to a remote Region may be necessary for meeting RTO and RPO requirements. These aspects should be validated with relevant regulators.

Summary

The scenarios outlined in this section demonstrate that data residency architectures are not one-size-fits-all. Data residency encompasses a spectrum of considerations. Each scenario is presented to encourage customers to think beyond conventional solutions and help them navigate the complex landscape of regulatory compliance. By exploring these diverse scenarios, customers can use the full spectrum of AWS services within their Region and its continuum, aligning with regulatory demands while maximizing the benefits of AWS offerings.

Operational excellence

Operational excellence includes the ability to support development and run workloads effectively, gain insight into their operations, and to continuously improve supporting processes and procedures to deliver business value. This section provides an overview of design principles, questions, best practices, and guidance on implementation. For more information, see Operational Excellence Pillar whitepaper.

Definitions

This whitepaper covers operational excellence in the cloud, describing best practices in the following areas:

- Organization
- Prepare
- Operate
- Evolve

Design principles

- **Local Zones:** Operational design principles for Local Zones should focus on seamless integration with cloud-based monitoring and management tools, same as for deployments in an AWS Region. Implement robust incident response plans tailored to the specific metropolitan area, ensuring continuous service availability and regulatory compliance. For more information, see Connectivity options for Local Zones.
- **Outposts:** Operational design principles for Outposts should focus on automating deployment and configuration processes and aligning with existing on-premises operational procedures and governance frameworks. Implement centralized monitoring, logging, and incident response mechanisms to maintain consistent compliance, as AWS Outposts requires additional accountability within the shared responsibility model.

Organization

DRHCOPS01: What are the specific data residency regulations and organizational policies that apply to your hybrid edge workloads?

Thoroughly understand your organization's data residency regulations and policies across locations to ensure operational alignment.

DRHCOPS02: How do you decide between using AWS Local Zones and AWS Outposts for data residency workloads?

AWS Outposts can help address data residency requirements by allowing you to control the physical location of your data. AWS Local Zones provide low-latency access to clients from specific geographic locations, which is important when evaluating data residency requirements around latency and access.

DRHCOPS03: How do you plan for business continuity for Hybrid Edge workloads?

Establishing clear RTO and RPO requirements is crucial for designing an effective disaster recovery solution when using AWS Outposts or Local Zones for your workloads.

Implement the right data replication strategy, build redundant network connectivity, automate failover processes, and maintain comprehensive monitoring and documentation to ensure business continuity and alignment with your data residency needs.

Best practices

- DRHCOPS01-BP01 Understand your organization's specific legal and compliance requirements specific to data residency
- DRHCOPS02-BP01 Consider AWS Outposts for data residency requirements when you need to evaluate data residency requirements, including control over data and its physical location

- DRHCOPS02-BP02 Consider AWS Local Zones for low-latency access from specific geographic locations while evaluating data residency requirements around latency and access from specific geographic locations
- DRHCOPS03-BP01 Understand your organization's RTO and RPO requirements, and build out your disaster recovery solution
- DRHCOPS03-BP02 Understand factors that determine your data replication strategy
- DRHCOPS03-BP03 Build redundant network connectivity
- DRHCOPS03-BP04 Implement failover automation, and test your disaster recovery strategies
- DRHCOPS03-BP05 Keep your monitoring, alerting, and documentation up to date and in-line with your RTO and RPO targets

DRHCOPS01-BP01 Understand your organization's specific legal and compliance requirements specific to data residency

Your use of AWS Hybrid Edge services should be guided by your data residency requirements. Clearly understand those requirements to ensure your operational practices meet them.

Desired outcome: Operational practices are aligned to meet your organization's data residency requirements.

Benefits of establishing this best practice: Clarifies requirements which facilitates implementation of those operational best practices including monitoring.

Level of risk exposed if this best practice is not established: High

Implementation guidance

While AWS provides services for local data storage, the responsibility to comply with local laws and regulations lies with you. This is a non-exhaustive list with examples, and you should review specifics based on your business, industry, and geographic location.

- General Data Protection Regulation (GDPR) for any personal data of EU citizens
- Health Insurance Portability and Accountability Act (HIPAA) for protected health information in the United States
- Payment Card Industry Data Security Standard (PCI DSS) for credit card and financial data
- Industry-specific regulations like Sarbanes-Oxley Act (SOX) for financial data
- Country or region-specific data privacy laws like the California Consumer Privacy Act (CCPA)

Thoroughly understand the specific regulations and internal policies that govern your organization's data residency requirements in different locations. This typically involves collaborating with your legal, compliance, risk management, and information security teams to identify and document all applicable rules and constraints.

Once established, list the countries and industries the application will serve. Review the Scenarios section in this lens for examples of how different data residency requirements inform your architecture decisions.

DRHCOPS02-BP01 Consider AWS Outposts for data residency requirements when you need to evaluate data residency requirements, including control over data and its physical location

Consider AWS Outposts to run AWS services on-premises and meet data residency requirements for regulatory compliance or data sovereignty reasons.

Desired outcome: You chose AWS Outposts to meet your data residency requirements while maintaining complete control over data and its physical location.

Benefits of establishing this best practice: Use the right AWS service offering for your requirements.

Level of risk exposed if this best practice is not established: High

Implementation guidance

You can use AWS Outposts to run AWS services on-premises, providing the same infrastructure, services, and operational models as the AWS Cloud while keeping sensitive data within your data center. Review the updated shared responsibility model to understand additional responsibilities when using AWS Outposts. For more detail, see Available locations for AWS Outposts racks and Servers.

DRHCOPS02-BP02 Consider AWS Local Zones for low-latency access from specific geographic locations while evaluating data residency requirements around latency and access from specific geographic locations

Consider AWS Local Zones for applications with low latency requirements and data residency requirements.

Desired outcome: You choose AWS Local Zones to meet your low-latency access from specific geographic locations while still adhering to data residency rules.

Benefits of establishing this best practice: You use the right AWS service offering for your latency and data residency requirements. Diversify your geographical locations with AWS Local Zones.

Level of risk exposed if this best practice is not established: High

Implementation guidance

AWS Local Zones are ideal when you require low-latency access to cloud services from specific geographic locations while still adhering to data residency rules. Local Zones extend the AWS Cloud closer to users or on-premises facilities, which helps your organization process and store data within the defined geographic boundaries without compromising performance. For more detail, see AWS Local Zones locations.

DRHCOPS03-BP01 Understand your organization's RTO and RPO requirements, and build out your disaster recovery solution

Understand your organization's RTO and RPO requirements and build a tailored disaster recovery solution to minimize disruptions, data loss, and financial impacts. When using AWS Outposts or Local Zones, consider data replication, network redundancy, failover automation, and capacity planning to meet desired RTO and RPO targets across on-premises and AWS environments.

Desired outcome: Establish clear recovery time and recovery point objectives that align with the business's tolerance for downtime and data loss related to your data residency requirements.

Benefits of establishing this best practice: Implementing a disaster recovery solution tailored to the defined RTO and RPO targets helps your organization minimize disruptions, data loss, and financial impacts in the event of a disaster or major outage.

When using AWS Outposts or Local Zones for hybrid workloads, consider data replication strategies between Outposts and AWS Regions, network connectivity redundancy, failover automation, and capacity planning to meet desired RTO and RPO targets across on-premises and AWS environments.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Recovery Time Objective (RTO) defines the maximum acceptable duration of downtime or service interruption before the recovery of applications and data must be completed. A shorter RTO implies a need for faster recovery mechanisms and failover strategies.

AWS Outposts and AWS Local Zones can be used to extend the AWS cloud to edge locations, enabling low-latency data processing and potentially faster recovery times. By deploying critical workloads on Outposts or Local Zones, organizations can achieve a shorter RTO by using local redundancy and failover capabilities.

Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss or the age of the most recent recoverable data point in the event of a failure or disaster. A shorter RPO implies a need for more frequent data backups and replication mechanisms.

By using local storage and compute resources, Outposts and Local Zones can facilitate frequent data backups and replication, helping organizations achieve a shorter RPO. Additionally, these services can be integrated with AWS services like Amazon Elastic Block Store (Amazon EBS) snapshots, for efficient data protection and recovery mechanisms.

The choice of using AWS Outposts or AWS Local Zones for hybrid edge workloads can be influenced by your organization's RTO and RPO requirements, which are key metrics for ensuring data availability and business continuity in the event of failures or disasters. To understand failure scenarios and resiliency options, see Reliability.

Depending on your organizational complexity, you might have multiple use cases based on the policies of different countries. Evaluate the specific requirements, laws and regulations, data volumes, and recovery strategies to determine the most appropriate solution for each use case.

DRHCOPS03-BP02 Understand factors that determine your data replication strategy

Understand the factors that determine your data replication strategy, and implement replication within the boundaries of your data residency requirements to align with disaster recovery objectives, data integrity, and compliance mandates.

Desired outcome: Your data replication strategy, including its technology, process, and policies, are developed and align to your disaster recovery objectives, data integrity and residency requirements, and compliance mandates.

Benefits of establishing this best practice: Having a clear grasp of data replication strategies allows for effective evaluation, optimization, and alignment with disaster recovery objectives, data integrity and residency requirements, and compliance mandates.

Level of risk exposed if this best practice is not established: High

Implementation guidance

- Implement data replication between Outposts, Local Zones, and AWS Regions within your cross-border requirements to provide data availability and minimize data loss in case of failures.
- Evaluate replication technologies like AWS DataSync or third-party solutions based on your workload requirements and RPO targets.
- Consider multi-site or multi-Region replication for mission-critical workloads to achieve lower RPOs.

DRHCOPS03-BP03 Build redundant network connectivity

Create redundant network connections to avoid connectivity loss to the Region and your workloads.

Desired outcome: Redundant network connectivity improves your availability posture and supports your business continuity needs along with data residency requirements

Benefits of establishing this best practice: Deploying redundant network connectivity using Outposts and Local Zones helps organizations maintain high availability, minimize latency, and keep data within specified geographic boundaries, addressing performance, resilience, and regulatory needs.

Level of risk exposed if this best practice is not established: High

Implementation guidance

- Establish redundant network connections between Outposts and AWS Regions using AWS Direct Connect or VPN connections.
- Implement failover mechanisms to automatically switch over to a secondary network connection in case of a failure, reducing downtime and meeting RTO targets.

DRHCOPS03-BP04 Implement failover automation, and test your disaster recovery strategies

Implement failover automations, and validate the automations through ongoing tests. Verify that your automation adheres to the boundaries of the data residency requirements.

Desired outcome: Automate the failover process and regularly test disaster recovery strategies to validate their effectiveness and identify potential gaps or areas for improvement.

Benefits of establishing this best practice: Implement failover automation and conducting periodic testing of disaster recovery strategies verifies that recovery plans are reliable, up to date, and can be run efficiently, minimizing downtime and data loss in the event of an actual disaster scenario.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Failover automation

Implementing failover automation to maintain availability during outages or disasters:

- Failover within the boundaries of your data residency requirement.
- Use AWS services like AWS Lambda, Amazon CloudWatch, and AWS Systems Manager to automate failover processes between Outposts, Local Zones, and AWS Regions. AWS Elastic Disaster Recovery Service might also be an option for failovers between Outposts to Region or Outposts and on-premises workloads.
- Implement scripts or tools to automate the failover of workloads, reducing manual intervention and meeting RTO targets.

Testing and validation

- Regularly test and validate your disaster recovery strategies, including failover and failback processes, to verify that they meet your RTO and RPO targets.
- Identify and address any bottlenecks or issues that may impact recovery times or data loss.

DRHCOPS03-BP05 Keep your monitoring, alerting, and documentation up to date and in-line with your RTO and RPO targets

Implement monitoring and alerting in line with your failover strategy, security and operations strategy, and data residency requirements.

Desired outcome: Maintain comprehensive monitoring, alerting, and documentation systems that are aligned with the organization's defined RTO and RPO targets and key performance indicators (KPIs). For more information on RTO and RPO see DRHCOPS03-BP01 best practice in DRHCOPS03.

Benefits of establishing this best practice: Keeping monitoring, alerting, and documentation up to date and in sync with RTO, RPO, KPIs, and your data residency requirements enables proactive identification of potential issues, timely incident response, and accurate tracking of recovery progress. This practice helps your organization meet its business continuity and data protection goals.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Monitoring and alerting

- Implement comprehensive monitoring and alerting mechanisms to promptly detect failures or issues that may initiate a failover or recovery process.
- Especially on Outposts, monitor key metrics related to replication, network connectivity, and resource utilization to proactively address potential issues. You can implement a set of metrics that use AWS CloudWatch and the AWS Health API. Familiarize yourself with notifications that provide warnings for business-critical impact, including service link down and EC2 retirement notices.

Documentation and training

- Maintain up to date documentation for your DR strategies, including failover and recovery procedures.
- Provide regular training to relevant personnel to ensure they are prepared to execute DR plans effectively during an outage or disaster.

Resources

- Architecting for Disaster Recovery on AWS Outposts racks with AWS Elastic Disaster Recovery
- Recovery objectives
- Plan for Disaster Recovery (DR)
- Resilience in AWS Outposts
- Automate data synchronization between AWS Outposts racks and Amazon S3 with AWS DataSync
- Monitoring best practices for Outposts

Prepare

DRHCOPS04 Which operational considerations do you make when designing your data residency workloads for operations in hybrid edge?

Verify Outposts facilities meet requirements, design robust network connectivity, and select data storage solutions that keep data within required geographic boundaries.

When designing data residency workloads for hybrid edge operations, it is crucial to verify Outposts facilities meet requirements, design robust network connectivity, and select data storage solutions that keep data within required geographic boundaries. Adhering to these best practices helps ensure compliance with relevant laws and regulations while benefiting from the capabilities of Outposts and Local Zones.

Best practices

- DRHCOPS04-BP01 Verify that your Outposts facilities are meeting the requirements to operate within the laws for your regulated workloads
- DRHCOPS04-BP02 Design your Outposts and Local Zone workloads to consider network connectivity
- DRHCOPS04-BP03 Review the available data storage options for Local Zones and Outposts to build architectures that keep data within required geographic boundaries

DRHCOPS04-BP01 Verify that your Outposts facilities are meeting the requirements to operate within the laws for your regulated workloads

Using Outposts rack requires that you procure and manage the data center within the city, state, province, or country boundary for your applications' regulated components, as required by local regulations.

Desired outcome: Validate that the facilities housing AWS Outposts deployments comply with all relevant laws and regulations governing the operation of regulated workloads.

Benefits of establishing this best practice: When your facilities meet the necessary requirements for running Outposts with regulated workloads, you mitigate the risk of non-compliance, potential fines, and legal consequences. Your organization can gain the benefits of Outposts in a secure and compliant manner.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Verify that your facility meets the requirements for Outposts racks or Outposts servers. For a list of various site requirements, see Site requirements for Outposts racks.

DRHCOPS04-BP02 Design your Outposts and Local Zone workloads to consider network connectivity

With the updated shared responsibility model for Outposts, you own the operations of the network connectivity and bandwidth.

Desired outcome: Architect Outposts and Local Zone workloads with robust network connectivity designs that account for factors such as bandwidth requirements, latency constraints, and secure communication channels.

Benefits of establishing this best practice: You have carefully considered network connectivity when designing Outposts and Local Zone workloads, which provides optimal performance, reliability, and security, helps you seamlessly integrate with on-premises infrastructure and cloud resources, and verifies that you adhere to data residency and compliance requirements.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Outposts network connectivity

AWS Outposts provides several network connectivity options to enable communication between your on-premises resources, Outpost instances, and AWS services.

- **Local gateway:** Outposts establish an external BGP peering from each Outpost network device to your local network device for connectivity to your on-premises resources.
- **Service link:** This is a necessary connection from the Outpost to your chosen AWS Region, allowing management of the Outposts and exchange of traffic between Outpost instances and AWS services.
- **Local Network Interfaces (LNI):** LNIs enable communication between your VPC and your on-premises network over the local gateway. This includes traffic from Outpost instances to your local network or the internet through your network.
- **Private connectivity:** Outposts can connect privately to your datacenter using AWS Direct Connect or a VPN, allowing communication between your on-premises resources and Outpost instances without going over the public internet.
- **Direct VPC routing:** Outpost instances can communicate directly with resources in your VPCs in the same AWS Region using private IP addresses without the need for a VPN or AWS Direct Connect.

Use the local gateway path instead of the service link path, and route internet traffic over the local gateway path wherever possible. Provision redundant network paths between the Outpost LGW and critical on-premises application resources. Use dynamic routing to automate traffic redirection around on-premises network failures. For more detail, see Application/workload routing.

Local Zones Network Connectivity

Local Zones are built into your network architecture the same way as an Availability Zone. You can extend any VPC from a parent Region into a Local Zone by creating a new subnet and assigning it to the Local Zone. The Local Zone network can have public subnets, internet gateways, and AWS Direct Connect gateways to your On-premises data center. For additional guidance, see Connectivity options for Local Zones.

DRHCOPS04-BP03 Review the available data storage options for Local Zones and Outposts to build architectures that keep data within required geographic boundaries

Thoroughly understand the applicable data laws and regulations for your specific workloads (as per DRHCOPS01).

Be aware that while Outposts and Local Zones allow data processing closer to users, they may still be across geographic borders from the connected AWS Availability Zone or Region. Account for the fact that logging, monitoring, and snapshot data may be transferred back to the AWS Region, which could have cross-border data transfer implications.

Desired outcome: Evaluate and select appropriate data storage solutions for Local Zones and Outposts that store data within specified geographic boundaries, adhering to data residency and compliance mandates.

Benefits of establishing this best practice: Using the right data storage options for Local Zones and Outposts helps organizations maintain control over their data's physical location, verifying that they comply with regional regulations and internal policies and benefit from the low-latency and local processing capabilities of these AWS offerings.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Review preferred storage options for Outposts, including instance storage like Amazon Elastic Block Store (Amazon EBS) or Amazon Simple Storage Service (Amazon S3) on Outposts. For Amazon S3 on Outposts, use Amazon S3 versioning or Amazon S3 replication.

Preferred storage options for Local Zones might include landing zone controls. For more information, see Best Practices for managing data residency in AWS Local Zones using landing zone controls.

Operate

DRHCOPS05: Which metrics do you need to understand your workload and operational health?

For Local Zones and Outposts, focus on establishing similar observability and alerting capabilities as in an Availability Zone.

To understand the workload and operational health of your Local Zones and Outposts, you should focus on establishing similar observability and alerting capabilities as in an Availability Zone. For Local Zones, this involves implementing comprehensive monitoring and alerting at both the infrastructure and application layers. For Outposts, you should also account for the shared responsibility model by adding alerts for security, networking, and capacity management.

DRHCOPS06: How do you consistently perform incident response and remediation practices across your organization's different teams and projects to operate your hybrid edge environment?

Develop a well-defined process for each alert generated by monitoring systems for Outposts and Local Zone workloads, clearly identifying the responsible teams and their respective incident response and remediation procedures.

Best practices

- DRHCOPS05-BP01 Understand monitoring requirements in your Local Zones
- DRHCOPS05-BP02 Understand monitoring requirements in your Outposts
- DRHCOPS06-BP01 Develop a process for each alert that you defined for your Outposts and Local Zone workloads

DRHCOPS05-BP01 Understand monitoring requirements in your Local Zones

Focus on similar observability and alerting as in an Availability Zone.

Desired outcome: Establish monitoring capabilities that align with the architecture and deployment model of workloads within an Availability Zone, ensuring comprehensive visibility and observability across the entire stack.

Benefits of establishing this best practice: Implementing monitoring solutions enables granular monitoring, accurate detection of issues, and targeted troubleshooting, ultimately improving operational efficiency.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Use the same mechanism for your workloads as you do in Availability Zones by implementing monitoring and alerting at infrastructure and application layer through CloudWatch or third-party tools.

DRHCOPS05-BP02 Understand monitoring requirements in your Outposts

Focus on similar observability and alerting as in an Availability Zone. In addition, add alerts for added responsibility such as security, networking, and capacity.

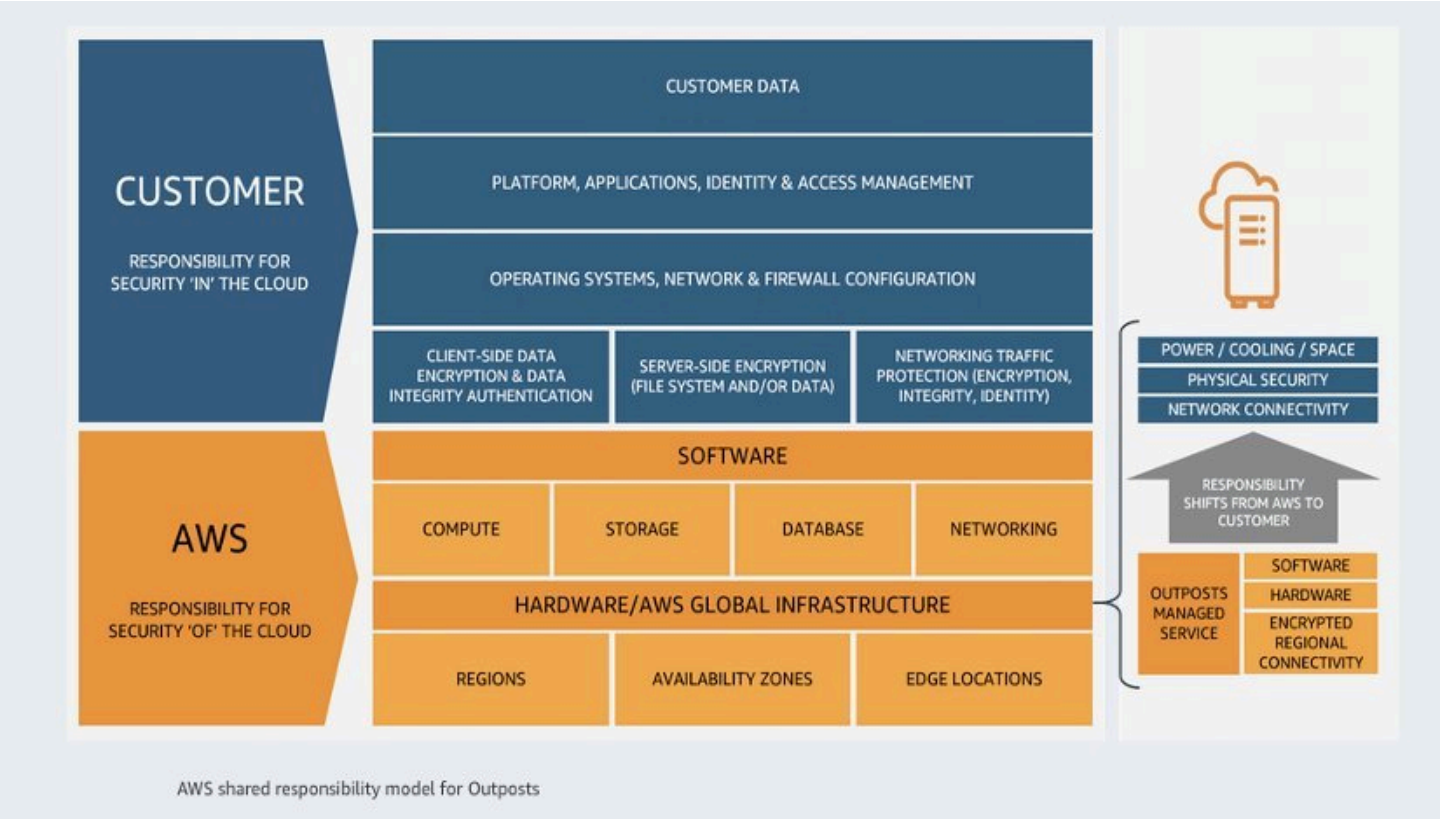
Desired outcome: Implement comprehensive monitoring for AWS Outposts workloads that aligns with the Availability Zone structure and accounts for the shared responsibility model.

Benefits of establishing this best practice: Enables end-to-end visibility, accurate issue detection, and targeted troubleshooting across cloud and on-premises components, improving operational efficiency.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Outposts have an updated shared responsibility model, as the hardware is not within an AWS-owned facility. As a result of this model, customers take on additional ownership of network, capacity, and security management, and they work with AWS in collaboration for any hardware maintenance. Set up specific metrics for Outposts at infrastructure and application layers, and provide visibility into AWS Health events.



Outposts shared responsibility model

Set up CloudWatch metrics, and enable cross-account observability where possible. Set up metrics to understand your connected status to the Region and traffic in and out. Implement capacity monitoring and follow N+1 capacity guidance which means you provision additional capacity for each instance family for redundant hardware. to follow N+1 guidance. Consider VPC Flow Logs and ELB access logs. If further detail is required, AWS X-Ray is an additional option for a complete view of requests across your applications.

Resources

- CloudWatch metrics for Outposts racks Deploying an automated Amazon CloudWatch dashboard for AWS Outposts using AWS CDK
- Monitor your Outposts rack
- Monitoring best practices for AWS Outposts
- CloudWatch metrics for Outposts racks

DRHCOPS06-BP01 Develop a process for each alert that you defined for your Outposts and Local Zone workloads

For Outposts, understand who owns different alerts. Instance-level alerts should likely be owned by the account owners, whereas application owners on those resources can stay informed. Loss of network or power should be owned by the team operating the infrastructure.

Desired outcome: Implement well-defined and tested processes. Implement procedures for each alert generated by monitoring systems for Outposts and Local Zone workloads, which provides consistent and effective incident response and remediation.

Benefits of establishing this best practice: Having a structured process for each alert for Outposts and Local Zone workloads enables prompt and coordinated actions, minimizes the risk of overlooking critical issues, and facilitates efficient troubleshooting and resolution.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Define runbooks for different scenarios and communication channels that engage the responsible teams to each identified scenario. Set up rack- and instance-level alerts that align with your runbooks.

Evolve

DRHCOPS07: How can you automate to streamline deployment, configuration, and monitoring processes across edge and cloud environments?

Use AWS services and tools for automation and infrastructure as code (IaC) to consistently provision, manage, and maintain hybrid and edge environments, including AWS Outposts and Local Zones, to streamline deployment, configuration, and monitoring processes across these environments.

DRHCOPS08: What processes have you implemented to regularly review and update data residency to align with evolving regulatory landscape and organizational needs?

Establish feedback loops to continuously adapt to evolving data residency requirements for Outposts and Local Zones, enabling proactive compliance with data sovereignty and localization mandates by facilitating timely adjustments to deployments as new AWS infrastructure becomes available.

Best practices

- DRHCOPS07-BP01 Use AWS services and tools for automation and infrastructure as code (IaC) across hybrid and edge environments
- DRHCOPS08-BP01 Build feedback loops to adapt to changing data residency requirements

DRHCOPS07-BP01 Use AWS services and tools for automation and infrastructure as code (IaC) across hybrid and edge environments

Automation helps you provide consistent deployment, configuration, and monitoring processes, even for applications and data that need to reside in specific locations due to data residency requirements. This approach improves operational efficiency, reduces errors, and facilitates governance and compliance across your hybrid and edge infrastructure.

Desired outcome: Adopt AWS services and tools for automation and infrastructure as code (IaC) to consistently provision, manage, and maintain hybrid and edge environments, including AWS Outposts and Local Zones.

Benefits of establishing this best practice: Using AWS automation across hybrid and edge deployments enables consistent configuration management, streamlined deployments, and efficient scaling of resources. It reduces manual effort, minimizes human errors, and promotes standardization.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Use AWS services like AWS CloudFormation, AWS Outposts installer for servers, and AWS Serverless Application Model (AWS SAM) to automate infrastructure provisioning and application deployments across edge and cloud environments. Implement infrastructure as code (IaC) principles, which produces consistent and repeatable processes for deploying, configuring, and managing resources, even in locations with data residency requirements.

Additionally, tools like Terraform and Ansible can be used for automation and deployment on AWS Outposts, which are AWS-managed infrastructure and services deployed at your on-premises facilities.

DRHCOPS08-BP01 Build feedback loops to adapt to changing data residency requirements

Data residency requirements can change over time. As AWS expands its Local Zones and Region footprint, new options may become available that allow you to move your data closer to AWS-managed infrastructure while still meeting your residency needs.

For example, if a new Local Zone launches in a location that meets your data residency requirements, you can move data that was previously hosted on Outposts into the Local Zone, which is an AWS-managed environment. Similarly, if a new AWS Region launches in a country or region where you previously had to use a Local Zone or Outposts to meet data residency needs, you can move that data into the new AWS Region.

Desired outcome: Establish feedback loops to continuously adapt to evolving data residency requirements for Outposts and Local Zones.

Benefits of establishing this best practice: Enables proactive compliance with data sovereignty and localization mandates by facilitating timely adjustments to deployments.

Level of risk exposed if this best practice is not established: Low

Implementation guidance

Regularly checking for updates on new Local Zone and AWS Region launches, and assessing how they align with your data residency requirements, can help you optimize your architecture and potentially move workloads closer to AWS-managed infrastructure while still complying with your data residency needs.

Key AWS services

- AWS Outposts
- AWS Local Zones
- Amazon CloudWatch
- Amazon S3

- AWS Elastic Disaster Recovery

Resources

Documentation and blogs:

- Architecting for data residency with AWS Outposts rack and landing zone guardrails
- Establishing RPO and RTO Targets for Cloud Applications
- Monitoring best practices for AWS Outposts
- Connectivity options for Local Zones
- Best Practices for managing data residency in AWS Local Zones using landing zone controls

Whitepapers:

- Data Residency Whitepaper
- Addressing Data Residency Requirements with AWS
- Operational observability
- Hybrid Networking Lens - Operational excellence pillar

Security

The security pillar provides guidance to help you apply best practices, current recommendations in the design, delivery, and maintenance of secure AWS workloads. While this lens focuses on preventing data storage in locations not aligned with data residency requirements, in all conceivable scenarios where data residency is required, each of the best practices identified in the Well-Architected Security Pillar whitepaper also apply.

Definitions

This whitepaper covers security in the cloud, describing best practices in the following areas:

- **Security foundations:** Fundamental principles address security threats and protect assets from attacks.
- **Identity and access management:** Securely manage identities and access to AWS services and resources.
- **Detection:** Identification of unexpected or unwanted configuration, and identification of unexpected behavior.
- **Infrastructure protection:** Control methodologies that are necessary to meet best practices and organizational or regulatory obligations.
- **Data protection:** Consists of both data classification to provide a way to categorize data based on levels of sensitivity, and encryption protects data by way of rendering it unintelligible to unauthorized access.
- **Incident response:** Respond to and mitigate the potential impact of security incidents
- **Application security:** Overall process of how you design, build, and test the security properties of the workloads you develop.

Design principles

All design principals from the Well-Architected Framework security pillar whitepaper apply to this lens, and there are no unique design principles for this lens.

Security foundations

DRHCSEC01: Have you updated and validated your control objectives to address data residency compliance requirements?

Based on your requirements and risks identified from your data residency compliance requirements, update and validate the control objectives and controls that apply to the workload. Ongoing validation of control objectives and controls help you measure the effectiveness of risk mitigation.

DRHCSEC02: Does your account management strategy separate workloads that have different data residency requirements?

Separating workloads at the AWS account level is recommended, as it provides a strong separation boundary and simplifies the implementation of preventative controls, such as Identity and Access Management (IAM) policies and service control policies (SCPs), as well as detective controls.

Best practices

- DRHCSEC01-BP01 Update your control objectives to address your data residency compliance requirements
- DRHCSEC01-BP02 Document any differences in the treatment of log data into the control objectives
- DRHCSEC02-BP01 Separate workloads that have different data residency requirements
- DRHCSEC02-BP02 Manage workloads with similar data residency requirements efficiently

DRHCSEC01-BP01 Update your control objectives to address your data residency compliance requirements

Control objectives should be updated to clearly indicate where data is expected to be located due to data residency requirements.

Desired outcome: Control objectives identify the locations and conditions where specific data is required to be stored.

Benefits of establishing this best practice: Clarifies requirements which facilitates implementation of those requirements as well as control automation and audit.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Update documentation of data residency requirements and control objectives with specific details on which data elements are subject to allowed or disallowed storage and transmission locations. For more detail, see SEC01-BP03 Identify and validate control objectives.

DRHCSEC01-BP02 Document any differences in the treatment of log data into the control objectives

As data residency requirements have the potential to apply to Log data, control objectives should explicitly state which data elements are subject to data residency requirements and if there is differences is requirements when stored in the form of logs.

Desired outcome: Control objectives address the allowed location of specific data elements present in log data.

Common anti-patterns:

- Enabling logging without awareness or control of where the logs are stored and what data is stored
- Only reviewing log data attributes and location during the testing phase of project

Benefits of establishing this best practice: Addressing requirements for log data up front can lower cost and risk of non-compliance by avoiding rework later in the initiative cycle.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

1. For each AWS service your architecture will use to store or transmit data, review the logging section of the service's user guide.

2. Identify what data elements are always logged if logging is enabled, which data elements are optionally logged, and if the location of storage of the logs is configurable. Many services can be configured to use Amazon CloudWatch Logs, and some also store logs in files. Include all forms of logs, including AWS service logs, application logs generated by the workload, operating system, agent, and other system level logs.
3. Update control objectives if they do not clearly address log data elements.
4. If compliance requirements prohibit any of those data elements from being stored in the Region, then implement controls which prevent or detect enablement of that specific logging. Examples where logs can only be configured to be stored in the Region are ALB access logs, VPC Flow Logs, any CloudWatch Logs, and AWS X-Ray logs. Example of potentially sensitive data element in logs is source (client) IP address.
5. If any logs are replicated to other locations, then explicitly define controls for the location of those servers or services.

Resources

- SEC04-BP01 Configure service and application logging

DRHCSEC02-BP01 Separate workloads that have different data residency requirements

As attempting to implement different sets of preventative and detective controls in the same AWS account is complicated at best, we highly recommend separating workloads into different accounts especially when their data residency requirements are different.

Desired outcome: An account structure that allows for separation of workloads with different data residency requirements into separate accounts, increasing compliance across the cloud infrastructure.

Common anti-patterns:

- Placing multiple workloads with different data residency requirements into the same account

Benefits of establishing this best practice: Lowers risk of non-compliance by eliminating sources of exceptions to preventative and detective control implementations. Lowers cost of implementation and testing of controls by minimizing complexity.

Level of risk exposed if this best practice is not established: High

Implementation guidance

AWS accounts provide a security isolation boundary between workloads or resources that operate at different sensitivity levels. AWS provides tools to manage your cloud workloads at scale through a multi-account strategy to leverage this isolation boundary. For guidance on the concepts, patterns, and implementation of a multi-account strategy on AWS, see Organizing Your AWS Environment Using Multiple Accounts.

Implementation steps

1. Identify and group workloads which have the same set of data residency requirements
2. **Design an organizational unit structure:** A properly designed organizational unit structure reduces the management burden required to create and maintain service control policies and other security controls. Your organizational unit structure should be aligned with your data residency requirements, business needs, data sensitivity, and workload structure.
3. **Create a landing zone for your multi-account environment:** A landing zone provides a consistent security and infrastructure foundation from which your organization can quickly develop, launch, and deploy workloads. You can use a custom-built landing zone or AWS Control Tower to orchestrate your environment.

Resources

- SEC01-BP01 Separate workloads using accounts

DRHCSEC02-BP02 Manage workloads with similar data residency requirements efficiently

When there are at least some control policies applicable to more than one account, configuring those accounts to be with the same Organizational Units (OUs) then applying the Service control policies (SCPs) at the OU level is more efficient than applying to each account, and much better than duplicating the policy statements into multiple SCPs.

Desired outcome: Service control policies (SCPs) for data residency are deployed without unnecessary duplication.

Common anti-patterns:

- SCPs are attached directly to multiple accounts
- You have duplicated statements in multiple SCPs

Benefits of establishing this best practice: Lowers cost of development and testing of preventative controls by minimizing duplication

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

1. Identify accounts with overlapping data residency requirements. The most relevant details are requirements that can be enforced with SCPs.
2. If there are relevant requirements that apply to a smaller subset than others, then it may be appropriate to create nested Organizational Units (OUs). However, when you create a nesting like this, you should factor in other business requirements for OU nesting, as well as AWS Organizations' service limit of five nested OU levels under a root.
3. Create OUs that match your grouping of overlapping data residency requirements.
4. Move your accounts into the relevant OU.
5. Attach SCPs at the OU level to minimize the overhead of applying them at account level, which also reduces risk of failing to apply the policies to new accounts.

Resources

Related best practices:

- SEC01-BP01 Separate workloads using accounts

Related documentation:

- Organizing Your AWS Environment Using Multiple Accounts
- Best Practices for Organizational Units with AWS Organizations
- Identity and Access Management

Identity and access management

DRHCSEC03: Have you implemented controls designed to enhance your digital sovereignty governance posture?

Digital sovereignty means control over digital assets. Data residency is control over the location of your data.

DRHCSEC04: How do you control access to support data residency requirements?

While some least privilege review processes focus decisions on access to actions and data, even more scrutiny is needed on actions that can move data. This helps you reduce the risk of non-compliance with data residency by restricting access using the resources of policies.

Best practices

- DRHCSEC03-BP01 Implement controls that enhance your digital sovereignty governance posture
- DRHCSEC04-BP01 Restrict access by location of resource
- DRHCSEC04-BP02 Grant least privilege access with a strong focus on actions that enable the storage of data

DRHCSEC03-BP01 Implement controls that enhance your digital sovereignty governance posture

Consider implementing controls which are not data residency specific as these controls help enable a defense in depth approach to security and are often easy to enable without requiring customization.

Desired outcome: Preventative controls deny storage of data in locations that lack compliance with data residency regulations.

Common anti-patterns:

- Attempting to author and maintain all the controls within your organization rather than using controls maintained by AWS, AWS partners, or others who invest continuously in maintaining controls focused on digital sovereignty

Benefits of establishing this best practice: Rigorously tested controls are deployed through automated procedures that improve your ability to securely scale more rapidly and cost-effectively.

Level of risk exposed if this best practice is not established: High

Implementation guidance

- Enable the AWS Control Tower digital sovereignty group of controls. Evaluate each control's applicability to your scenario, as some controls have very limited use cases where they should be applied. One of the most commonly deployed controls is the OU Region deny control.
  - While the same set of preventative and detective controls can be reproduced without deployment through Control Tower, it is highly recommended to use Control Tower to eliminate the undifferentiated heavy lifting of maintaining these controls yourself. This practice also facilitates easier deployment of new controls as they become available.
- Disable any Local Zones (at the account level) that are currently enabled but not required.
- Deploy an SCP to deny the ec2:ModifyAvailabilityZoneGroup IAM action to all principals that do not have explicit approval to opt in to Local Zones for the account.
- Establish a data perimeter as discussed in SEC03-BP08 Share resources securely within your organization, as controlling which principals have access to data is a foundational step to controlling the location where data can be stored.
- Deploy encryption controls to enforce usage of encryption. Where supported, require AWS KMS customer-managed keys, and implement fine grained AWS KMS key policies to promote security-in-depth and add another level of data access control.

Resources

Related best practices:

- SEC03-BP05 Define permission guardrails for your organization
- SEC03-BP08 Share resources securely within your organization
- SEC08-BP01 Implement secure key management

Related documentation:

- Digital sovereignty controls
- Region deny control applied to the OU
- Evaluating Resources with AWS Config Rules
- Building Data Perimeter on AWS
- Establishing a data perimeter on AWS: Allow only trusted identities to access company data
- Data Perimeter Policy Examples

DRHCSEC04-BP01 Restrict access by location of resource

Specify IAM actions to restrict based on where the resource's storage of data would be located.

Desired outcome: Access management policies allow data storage only in locations that comply with data residency regulations.

Common anti-patterns:

- Allowing unrestricted access to all resources
- Allowing the launching of instances in the Region when requirements for a given workload only require launching in an Outpost or Local Zone
- Allowing creation of roles, users, and attach policies without attaching AWS IAM permission boundaries

Level of risk exposed if this best practice is not established: High

Implementation guidance

- Analyze location of data in your least privilege access analysis. This requires awareness of the actions that can impact the location of data.
- If need to allow principals to store data in Amazon S3 on Outposts but not in Region buckets, then deny the `s3:PutObject` action on the Resource `arn:aws:s3:::*`, or only allow the action s3:PutObject on specific S3 buckets using resource values that match the pattern `arn:aws:s3-outposts:${region}:${account-id}:outpost/outpost-id/accesspoint/${accesspoint-name}`.

- Restrict the creation of instances and network interfaces to specific subnets by using policy resources to create a dynamically-composed list of authorized subnets for the following IAM actions:
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:RequestSpotFleet`
  - `ec2:RequestSpotInstances`
  - `rds:CreateDbSubnet`
  - `elasticache:CreateCacheSubnetGroup`
  - `autoscaling:CreateAutoScalingGroup`
  - `elasticloadbalancing:CreateLoadBalancer`
  - `ec2:CreateLaunchTemplate`
- The `ec2:CreateSnapshot*` actions should not be allowed to principals that don't need it. For principals that do, you can deny data transfer from an Outpost to a Region by attaching a deny policy using the condition key `ec2:SourceOutpostArn` for designated Outposts, where `ec2:OutpostArn` is null (the destination is not the Outpost).
- The `ec2:CopySnapshot*` actions should not be allowed to principals that don't need it. Transfer of snapshots from an Outpost to a Region is not currently supported. However, snapshots can be copied from Region to an Outposts (for example, a valid use case is to move an Amazon Machine Image (AMI) from Region to an Outpost for faster launching or removing repeated bandwidth consumption). You can use the ec2:OutpostArn condition key if you need to restrict the copying of snapshots to a specified Outpost. If you need to restrict copying snapshots to specific Regions, then specify the Region portion of the ARN within the resource attribute of the policy statement.
- For each of the following actions, only grant them if there is a known requirement for the principal, and use the policy's resource section to only allow the storage in the required Region:
  - `rds:CreateDBSnapshot`
  - `rds:CreateDBClusterSnapshot`
  - `elasticache:CreateSnapshot`
  - `elasticache:CopySnapshot`
  - `ec2:CopyImage`
  - `ec2:CreateInstanceExportTask`

- `ec2:CreateVolume`
- `ec2:AttachVolume`
- `ec2:ImportSnapshot`
- `ec2:ImportVolume`
- `datasync:Create*`
- `datasync:Update*`

- Implement permission guardrails for which include each of the applicable restrictions defined in this best practice

Resources

Related best practices:

- SEC03-BP02 Grant least privilege access
- SEC08-BP04 Enforce access control
- SEC03-BP05 Define permission guardrails for your organization

Related documentation:

- Architecting for data residency with AWS Outposts rack and landing zone guardrails
- Best Practices for managing data residency in AWS Local Zones using landing zone controls
- Permission boundaries for IAM entities

DRHCSEC04-BP02 Grant least privilege access with a strong focus on actions that enable the storage of data

Restricting access to actions which store data should be a strong focus of least privilege access analysis.

Desired outcome: Principals are only allowed to perform actions that are required within that specific account.

Common anti-patterns:

1. Implementing policies that deny specific services but allow all other services, as the policies would need to be maintained whenever new services are released.
2. Attaching the `AWSPowerUser` or `AdministratorAccess` AWS-managed policy to roles.
3. Allowing actions that store or move data when these actions are not required.

Benefits of establishing this best practice: Least privilege minimizes options to store data, which reduces the risk of noncompliant storage locations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

- While allowing access only to required services is part of SEC03-BP02 Grant least privilege access, it is even more important in data residency scenarios, as there are many services that store data in Regions.
- Grant the `ec2:CreateSubnet` action only to principals that have complete knowledge of the data residency requirements, and set expectations to only create subnets in locations where instances are expected to be aligned with data residency requirements. There are two reasons for this: instances can't exist in locations without subnets, and the location of attached EBS volumes is controlled by the location of the instances. Where possible, add conditions to the granted permissions to allow creation of resources only in Regions aligned with data residency requirements.
- Deny `ram:AcceptResourceShareInvitation`, `ram:AssociateResourceShare*`, `ram:Create*`, and `ram:Update*` when not required, as performing these actions combined with other actions where the resource element is `*` enables storage to resources that may be in unapproved locations.
- Deny `ec2:ExportImage`, `ec2:ImportImage`, `ec2:ImportInstance`, and `ec2:CreateTrafficMirror*` unless you have an approved use case that requires these actions.
- Implement permission guardrails for which include each of the applicable restrictions defined in this best practice.

Resources

Related best practices:

- SEC03-BP02 Grant least privilege access
- SEC03-BP05 Define permission guardrails for your organization

Detection

Detection

DRHCSEC05: How do you detect resources created in unauthorized locations?

Configure detective controls to notify you if someone in your organization creates resources in unapproved locations according to your data residency compliance requirements.

Best practices

- DRHCSEC05-BP01 Implement detective controls that notify a security operations team when resources are found in unauthorized locations

DRHCSEC05-BP01 Implement detective controls that notify a security operations team when resources are found in unauthorized locations

Automate the detection and notification to security operations teams if data is stored is locations out of compliance with your data residency compliance requirements.

Desired outcome: Security operations teams are automatically notified when detective controls find resources in noncompliant locations.

Common anti-patterns:

- Lack of automated mechanisms to detect data in unauthorized locations
- No one follows up on notifications that no one follows up on

Benefits of establishing this best practice: Security operations teams are alerted to data in unauthorized locations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

- Create detective controls, such as AWS Config Rules or open source solutions like Cloud Custodian rules, and configure them to detect and notify when resources are found in unapproved locations.
  1. For EC2 instances, subnets, EBS volumes, and snapshots (like EBS, Amazon RDS, and Amazon ElastiCache):
     - **Outposts**: Implement rules that detect resources where value of OutpostArn attribute is null, which means that the resource is located in a Region. Alternatively, create a strict implementation that checks if the actual value is not in a specific allowlist of OutpostArns.
     - **Local Zones**: Implement rules that detect resources where the value of AvailabilityZone is not the expected Local Zone.
  2. Implement rules for EC2 instances, Auto Scaling groups (ASGs), NetworkInterfaces, RDS instances, and Application Load Balancers (ALB) to detect when the value of the SubnetId attribute value is not present in an allowlist.
- Automate remediation of findings in scenarios where precise rules without exceptions can be enforced. One example would be to automatically end an instance launched in an in-Region subnet when data residency requirements prohibit data storage in that Region. Another example would be to turn on default encryption for S3 buckets and EBS volumes.
  1. Automated remediation is an example of a control. Automated remediation can be implement using AWS Security Hub custom actions, AWS Config integration with Systems Manager Automation documents, and Cloud Custodian actions.

Resources

Related documentation:

- Evaluating Resources with AWS Config Rules
- AWS Systems Manager Automation
- AWS Security Hub custom actions

Related partner solutions:

- Cloud Custodian actions

Infrastructure protection

DRHCSEC06: How do you physically secure your AWS Outposts?

If AWS Outposts is part of your solution, there are customer responsibilities for the physical security of the Outpost.

DRHCSEC07: How do you protect your network resources?

Do you have any form of firewall or other mechanisms to block traffic, such as by port, CIDR block range, or protocol?

Best practices

- DRHCSEC06-BP01 Restrict the number of people authorized to gain physical access to your AWS Outposts
- DRHCSEC06-BP02 Control access to locations where AWS Outposts are deployed using systems like keys and biometrics
- DRHCSEC07-BP01 Implement network traffic inspection-based protection

DRHCSEC06-BP01 Restrict the number of people authorized to gain physical access to your AWS Outposts

Physical access should only be provided to those who have a legitimate business need for it.

Desired outcome: Physical access to Outposts is limited, and access is only granted with an accompanying business requirement.

Common anti-patterns:

- Granting access to anyone without justified reason for the physical access
- Lack of awareness of the shared responsibility model for Outposts, as well as its differences to other AWS services

- Lack of periodic access reviews to make sure access requirements still exist

Benefits of establishing this best practice: Reduce security risk by minimizing ability to physically interact with hardware.

Level of risk exposed if this best practice is not established: High

Implementation guidance

- Review the AWS Outposts section of the Terms of Service with specific attention to the responsibilities for physical security and access controls.
- Review the AWS Outposts Shared Responsibility Model in the AWS Outposts High Availability Design and Architecture Considerations whitepaper.
- Update your access control mechanisms to only allow physical access to those who have a business need and when needed, rather than 24x7 access for people who's business need is only for short durations, such as electricians, fiber cable pullers, HVAC personnel, and staff designated to escort AWS maintenance technicians.
- Create a process for periodic access reviews, and automatically revoke access when not used for a certain duration.

DRHCSEC06-BP02 Control access to locations where AWS Outposts are deployed using systems like keys and biometrics

This practice verifies that only authorized personnel can gain physical access to AWS Outposts racks or servers.

Desired outcome: Reduced risk of data stored on Outposts becoming unreadable due to lack of access to the encryption key.

Common anti-patterns:

- Uncontrolled or untraceable physical access to the Outpost

Benefits of establishing this best practice: Reduce security risk by minimizing ability to physically interact with the hardware.

Level of risk exposed if this best practice is not established: High

Implementation guidance

- Controlling physical access to AWS Outposts racks and servers is of particular importance because the Nitro Security Key (NSK) plays a key role in the encryption at rest and protection of data. As a result, purposeful or inadvertent destruction can lead to irrevocable loss of customer data. For a deeper understanding of the AWS Nitro system and how the NSK fits into it, see The components of the Nitro System.
- Review Tamper monitoring on AWS Outposts equipment section of the AWS User Gude for Outposts Racks.
- Maintain video surveillance of access points to locations where AWS Outposts are deployed so that physical access can be monitored and made available for event forensics.

Resources

Related documentation:

- Encryption at rest
- The Security Design of the AWS Nitro System
- Infrastructure Security in AWS Outposts

DRHCSEC07-BP01 Implement network traffic inspection-based protection

Set up traffic inspection points between your network layers to make sure data in transit matches the expected categories and patterns. Analyze traffic flows, metadata, and patterns to help identify, detect, and respond to events more effectively. Traffic Inspection can be implemented using EC2 instances, including those running on Outposts or Local Zones.

Desired outcome: Traffic that traverses between your network layers is inspected and authorized. Allow and deny decisions are based on explicit rules, threat intelligence, and deviations from baseline behaviors. Protections become stricter as traffic moves closer to sensitive data**.**

Common anti-patterns

- Relying solely on rules based on ports and protocols.

Benefits of establishing this best practice: Inspection systems help you author intelligent rules, such as allowing or denying traffic only when certain conditions within the traffic data are met.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Be aware that while Local Zones and Outposts support VPC security groups and network ACLs (NACLs), these Edge services do not support AWS WAF, AWS Network Firewall, and the Advanced level of AWS Shield. Local Zones support the standard level of AWS Shield, while Outposts does not.
- Implement network inspection through hybrid inspection architectures with AWS Local Zones or by implementing network traffic inspection on AWS Outposts rack.
- AWS WAF support can be implemented using F5 on Outposts for AWS WAF and security inspection.

Resources

Related best practices:

- SEC05-BP03 Implement inspection-based protection

Related documentation:

- Hybrid inspection architectures with AWS Local Zones
- Implementing network traffic inspection on AWS Outposts rack

Data protection

DRHCSEC08: What mechanisms are you using to recover from data corruption and data deletion, or do you have a way to provide point-in-time views of your data?

Do you have any form of backups of your data that are verified to work in scenarios where data is unintentionally or intentionally changed or deleted? Do you have a mechanism to view what the data was at a given point in time?

Best practices

- DRHCSEC08-BP01 Implement backups to enable recovery from data corruption and data deletion, as well as point-in-time views of data

DRHCSEC08-BP01 Implement backups to enable recovery from data corruption and data deletion, as well as point-in-time views of data

Configure backups to be taken automatically based on a periodic schedule informed by the Recovery Point Objective (RPO), or by changes in the dataset. Critical datasets with low data loss requirements need to be backed up automatically on a frequent basis, whereas less critical data where some loss is acceptable can be backed up less frequently.

Desired outcome: Successful periodic test results of ability to recover data.

Common anti-patterns:

- Failing to fully test if your data backup and recovery procedures are functional

Benefits of establishing this best practice: Helps you detect and fix backup and recovery misconfigurations if they occur.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Configure Amazon EBS snapshots. If your compliance requirements allow backups to be stored in-Region, that can be a lower cost option. Otherwise, configure Amazon EBS local snapshots on Outposts, or implement a third-party backup solution.
  1. For implementations details, see Amazon Elastic Block Store Local Snapshots on AWS Outposts and Amazon EBS local snapshots on Outposts.
- Enable S3 Versioning on Outposts to preserve, retrieve, and restore every version of every object stored in your S3 buckets on Outposts.
- Enable S3 Replication on Outposts to replicate the Amazon S3 objects to another Outpost or even another bucket on the same Outpost. If copies of data may be stored in-Region, then configure AWS Datasync to replicate the data to the S3 bucket in the Region.
- Perform capacity planning, and periodically review your plans to reduce risk of running out of capacity within S3 Outposts.

- Third-party backup solutions are available from AWS Partners who have tested their solutions on Outposts.
- Periodically test your ability to fully recover data, including from specific points in time.

Resources

Related best practices:

- REL09-BP03 Perform data backup automatically
- Incident Response

Incident response

DRHCSEC09: Have your incident responders been trained on your data residency policies?

Incident responders should be aware of your data residency policies, and they should check for data that is located in unapproved locations.

DRHCSEC10: Have your threat models been updated to cover data in unauthorized locations?

While threat models typically focus on exfiltration of data, they should be updated to include scenarios where data gets stored in locations that aren't compliant with data residency regulations and control objectives.

Best practices

- DRHCSEC09-BP01 Train and test incident responders on policies specific to data residency
- DRHCSEC10-BP01 Update your threat models to cover the accidental or malicious storage of data in unauthorized locations

DRHCSEC09-BP01 Train and test incident responders on policies specific to data residency

Train and test incident responders on regulations on storage location based on data classification.

Desired outcome: Incident responders have passed tests of their ability to respond to data being stored in noncompliant locations.

Common anti-patterns:

- Playbooks not being tested by people responsible for using them

Benefits of establishing this best practice: You can prepare for a data residency incident by having incident management and investigation policy and processes that align to your data residency requirements.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Update your incident response playbooks with the impact of policies specific to data residency, such as authorized and unauthorized locations for data.
- Update expected incidents and known security findings or alerts with the findings for each data residency-related detective control.
- For each preventative control, create at least one test hat proves that the attempted action is denied.
- For each detective control, create at least one test, perform the test, then assess if the detection occurred and was visible where expected for responders.
- If you use Outposts or Local Zones and have policies that prohibit data from being stored within Region locations, create a test for each service you use in the workload, and configure iterations of the test for all Regions that aren't covered by the organization-wide Region deny SCP.
- Evaluate AWS Security Incident Response to determine if it's an appropriate option for your organization.

Resources

Related best practices:

- SEC10-BP03 Prepare forensic capabilities
- SEC11-BP01 Train for application security
- SEC10-BP04 Develop and test security incident response playbooks

Related documentation:

- Application security

Related videos:

- re:Invent 2024 SEC360: Respond and recovery faster with AWS Security Incident Response

DRHCSEC10-BP01 Update your threat models to cover the accidental or malicious storage of data in unauthorized locations

Threat models should include specific scenarios where the threat is data stored in unauthorized locations due to accidental storage as well as maliciously intent.

Desired outcome: Threat models cover all risks to data residency compliance.

Common anti-patterns:

- Threat models do not include specific location of data as a risk

Benefits of establishing this best practice: Up to date threat models help prepare people to respond to incidents.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

- Review existing threat models, and remediate if they don't already address exfiltration to unauthorized internal accounts, unauthorized external accounts, or locations outside of AWS.
- Add threat scenarios where data is stored in an unauthorized location, such as in any or specific Regions, due to data residency policies within the same account.

Resources

Related documentation:

- How to approach threat modeling

Reliability

The reliability pillar includes the ability of a workload to perform its intended function correctly and consistently when it's expected to. This includes the ability to operate and test the workload through its total lifecycle. This paper provides in-depth, best practice guidance for implementing reliable workloads on AWS. The reliability pillar provides an overview of design principles, best practices, and questions.

Definitions

This whitepaper covers reliability in the cloud, describing best practices in the following areas:

- Foundations
- Workload architecture
- Change management
- Failure management

To achieve reliability, you must start with the foundations: an environment where service quotas and network topology accommodate the workload. The workload architecture of the distributed system must be designed to prevent and mitigate failures. The workload must handle changes in demand or requirements, and it must be designed to detect failure and automatically heal itself.

Design principles

While meeting data residency requirements in AWS Regions, Local Zones, and Outposts, there are a number of principles that can help you increase reliability. Keep these in mind as we discuss best practices:

- **Automatically recover from failure while maintaining data residency requirements:** By monitoring a workload for key performance indicators (KPIs), you can run automation when a threshold is breached. These KPIs should be a measure of business value, not of the technical aspects of the operation of the service. This allows for automatic notification and tracking of failures, as well as automated recovery processes that work around or repair the failure. The failure recovery must be designed to comply with your data residency requirements. With prediction and testing, it is possible to anticipate and remediate most of the failures before they occur.

- **Plan capacity requirements:** In an AWS Region, you can monitor demand and workload utilization and automate the addition or removal of resources to maintain the optimal level that satisfies demand without over- or under-provisioning. There are still limits, but some quotas can be controlled and others can be managed (for more detail, see Manage service quotas and constraints). With Outposts, capacity is finite and should be planned ahead of time using prediction and testing to forecast capacity correctly ahead of time.

Foundations

DRHCREL01: How do you manage Service Quotas for resources running in AWS Local Zones and AWS Outposts?

For cloud-based workload architectures, there are Service Quotas (also referred to as service limits). These quotas exist to prevent accidentally provisioning more resources than you need and to limit request rates on API operations to protect services from abuse. Both AWS Local Zones and AWS Outposts are homed to specific AWS Regions. Regional service quotas apply to AWS resources (for example, Amazon EC2 instances) running on Local Zones or Outposts.

DRHCREL02: Do you have redundant power and network to on-premises AWS components?

AWS Outposts depends on a resilient connection to its anchor Availability Zone for management, monitoring, and service operations to function properly. Redundant network connections for each Outpost are needed for reliable connectivity back to the anchor points in the AWS Cloud. Outposts have documented power requirements, and it is recommended to provide dual power sources for resilience in case of power failure.

Best practices

- DRHCREL01-BP01 Set service quotas to accommodate for the peak usage of AWS resources on Outposts for their homed Regions
- DRHCREL02-BP01 Provision redundant power and network to on-premises components
- DRHCREL02-BP02 Use AWS Direct Connect with redundant tunnels and connections to the AWS Region for Outposts control plane actions and high availability requirements

DRHCREL01-BP01 Set service quotas to accommodate for the peak usage of AWS resources on Outposts for their homed Regions

AWS Outposts and Local Zones adhere to the service quotas of their parent AWS Regions, requiring management of service quotas to accommodate peak usage.

Desired outcome: Proactively adjust service quotas to meet your capacity requirements in specific Regions, which helps you maintain data residency in those Regions.

Benefits of establishing this best practice: Proper service quota management and planning validates availability of AWS resources on Outposts and Local Zones, reducing the risk of service disruptions due to resource limitations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

AWS Outposts and AWS Local Zones are homed to specific AWS Regions. Regional service quotas apply to AWS resources (for example, Amazon EC2 instances) running on Outposts or Local Zones and should be managed. The best practices to manage service quotas and constraints apply to the Regions that the chosen Outposts or Local Zones are homed to. Apply service quotas best practices to Outpost and Local Zones.

DRHCREL02-BP01 Provision redundant power and network to on-premises components

To ensure high availability for AWS Outposts deployments, implement redundant power sources and network connectivity while considering multi-Outpost distribution across different Availability Zones.

Desired outcome: Achieve high availability of on-premises systems, helping to provide consistent data access and processing capabilities in compliance with data residency requirements.

Benefits of establishing this best practice: Redundant power and network infrastructure improves the reliability and availability of on-premises components, minimizing potential downtime.

Level of risk exposed if this best practice is not established: High

Outpost Racks are designed with redundant power and networking equipment. Customer racks will house individual Outposts servers. To meet high availability objectives, we recommend providing dual power sources and redundant network connectivity to Outposts and customer racks.

Implementation guidance

- Provide dual power sources to Outposts and Customer racks.
- Provision redundant network connectivity (for example, redundant network devices) to Outposts.
- For higher availability, deploy applications on multiple Outposts, each attached to a different Availability Zone, to build additional application resilience and avoid dependence on a single Availability Zone.

DRHCREL02-BP02 Use AWS Direct Connect with redundant tunnels and connections to the AWS Region for Outposts control plane actions and high availability requirements

AWS Outposts maintains connectivity to its parent Region through encrypted service link tunnels to anchor points in designated Availability Zones, requiring redundant network paths and dynamic routing for high availability of control plane operations.

Desired outcome: Achieve high availability and reliability for Outposts management and data operations while maintaining compliance with data residency requirements through dedicated, redundant AWS Direct Connect connections.

Benefits of establishing this best practice: AWS Direct Connect with redundant connections provides a reliable and low-latency communication channel between Outposts and AWS Regions, improving the reliability of control plane operations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

When you create AWS Outposts, you select an Availability Zone from an AWS Region. Outposts connects back to its parent Region through a set of encrypted VPN tunnels called the service link. The service link ends on a set of anchor points in an Availability Zone in the Outpost's parent Region. This Availability Zone supports control plane operations such as responding to API calls, monitoring Outposts, and updating Outposts.

To benefit from the reliability provided by Availability Zones, you can deploy applications on multiple Outposts, each attached to a different Availability Zone. By doing so, you can build additional application resilience and avoid a dependence on a single Availability Zone. For more information about Regions and Availability Zones, see AWS Global Infrastructure.

This makes this connectivity to the AWS Region from AWS Outposts important. Where the data does need to flow to the AWS Region and has high availability requirements, we recommend using redundant connectivity back to the AWS Region. AWS Direct Connect can be set up with redundant tunnels and connections to AWS Region.

In the case of AWS Outposts, this connectivity is needed for control plane actions like launching new Amazon EC2 instances, which are necessary for auto scaling. Provision redundant network paths between the Outpost and the anchor points in the Region with connections that end on separate devices in more than one location.

Dynamic routing should be configured to automatically reroute traffic to alternate paths when connections or networking devices fail. You should provision sufficient network capacity to verify that the failure of one WAN path does not overwhelm the remaining paths. For guide to this configuration, see Anchor connectivity.

Workload architecture

DRHCREL03: What strategies should you implement to provide reliable data access and processing across on-premises, edge, and cloud environments?

If a resource failure occurs, healthy resources should continue to serve requests. When you have effective failover strategies, your systems in place can fail over to healthy resources in unimpaired locations. The failover must be implemented in accordance with your data residency requirements across on-premises, edge, and cloud environments.

Best practices

- DRHCREL03-BP01 Use AWS Outposts or Local Zones for scenarios where data must reside within a country or jurisdiction without a local AWS Region
- DRHCREL03-BP02 Implement failover mechanisms to maintain highly-available data access and processing across on-premises, edge, and cloud environments

DRHCREL03-BP01 Use AWS Outposts or Local Zones for scenarios where data must reside within a country or jurisdiction without a local AWS Region

To meet data residency requirements in Regions without local AWS infrastructure, leverage AWS Outposts across multiple locations or AWS Local Zones with redundancy, while utilizing services like Amazon S3 on Outposts for resilient local data management.

Desired outcome: Achieve seamless integration of AWS Cloud capabilities into local operations while maintaining strict adherence to data residency requirements even in countries with no AWS Regions.

Benefits of establishing this best practice: AWS Outposts and Local Zones enable organizations to use AWS services while keeping data within specific geographical boundaries, facilitating compliance with local data sovereignty laws and regulations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

When data must remain within the country and a local AWS Region isn't available, deploy on Outposts in different physical locations with redundant power and network sources or AWS Local Zones. Use services like Amazon S3 on Outposts for backup and recovery to achieve high availability while adhering to data residency regulations.

DRHCREL03-BP02 Implement failover mechanisms to maintain highly-available data access and processing across on-premises, edge, and cloud environments

Data residency requirements can be addressed through various high-availability architectures, ranging from fully local deployments using redundant Outposts to hybrid solutions leveraging AWS Regions where regulations permit data transfer with proper consent and controls.

Desired outcome: Achieve seamless operational continuity and data availability across hybrid infrastructures and consistently meet data residency requirements even during system failures or disruptions.

Benefits of establishing this best practice: Failover mechanisms enhance reliability, minimize downtime, and help maintain continuous data accessibility while complying with data residency regulations.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Depending on the specific data residency requirements for your use-case, high availability can be achieved with the right architecture and failover strategies in place. We will use the following five categories of data residency requirements and apply design reliability best practices and failover requirements to each.

Regulations allow data storage outside the country with user consent as data subjects or the permission or notification of the regulators (or both).

As data can reside outside of the country with user consent, backup and failover strategies can be employed if data controls are place. Where there are no Local Zones, Outposts should be deployed with sufficient redundant power and network to meet availability requirements. To avoid disruptions, the Outposts should be set up in different physical locations with different power and network sources (for example, data centers in different cities). Amazon S3 is available on Outposts racks, and data can be backed up and recovered from Amazon S3 on the Outposts similarly to how this is done in the Region.

With consent, the data can be backed up in redundant AWS Region in the nearest country. AWS Backup, Amazon EBS snapshots, and Amazon EC2 AMIs offer options for backup of data from EC2 instances to Amazon S3 in the Region. These can also be copied with consent across Regions if required for additional reliability. Applications can also be served from the AWS Region specifically only using the data that has consent and permission to leave the country.

Regardless of whether Outposts, Local Zones, or Regions are used to preserve data residency requirements, the failover mechanism must meet the availability recovery time objectives. AWS offers Amazon Route 53 and high availability services for failover, where you can use APIs failover in response to events like failed health checks.

Failover of on-premises local traffic across Outposts can be done using networking techniques such as using Border Gateway Protocol (BGP) Bidirectional Forwarding Detection (BFD) to failover across Outposts using load balancers or DNS. Fast failover requires monitoring to be in place to initiate the failover. This can be done using local health checks or using Amazon Cloudwatch.

On Outposts, you can replace failed instances with new instances using automated mechanisms like Amazon EC2 Auto Scaling groups. Instance auto recovery can restart instances that fail due to server failures provided there is sufficient spare capacity available on the remaining servers. Outposts also supports AWS Application Load Balancer for targets local to the Outposts (for example, Amazon EC2 instances or containers).

The transfer of data should also be done in a high availability manner. Outposts offer local gateway (for Outposts racks) and local network interface (for Outposts Servers), which can send traffic to the Region over AWS Direct Connect. Direct Connect offers SLAs, allows private connectivity into one or more AWS Regions, and can be set up with redundancy. For guidance on setting up AWS Direct Connect resiliency, see AWS Direct Connect Resiliency Recommendations.

From a Local Zone, data can be transferred using the VPC if the local zone is the in same Region as the destination service (for example, Amazon S3, Amazon EC2, or Amazon EFS). If the traffic needs to go across Regions or VPCs, VPC peering or AWS Transit Gateway can be used.

Transfer of in-scope data may be allowed to countries that adhere to the same specific set of standards (or higher) than the originating country with permissions or notification to the regulators.

In this scenario, retention requirements can be met using Local Zones and Regions for backup, restore, and failover. However, the Regions must be carefully selected to ensure that they are allowed by the country's requirements.

Primary servicing copy: In a scenario where the law mandates data residency requirements that specify that the primary copy of the data must be maintained within the country or jurisdiction.

In this scenario, in-scope data can be stored or transferred outside the borders, but the primary servicing copy must be held within the border of your jurisdiction. Data can be backed up outside of the country in the nearest AWS Region into Amazon S3. If the data is large, use a dedicated virtual interface (VIF) with Direct Connect for high performance connectivity to Amazon S3. The data must be backed up with sufficient frequency to meet your recovery point objective (RPO). Since the primary servicing copy must be in the country, it's not possible to failover outside the country. As a result, failover must occur across Local Zones or Outposts within the country.

In-scope data must be stored and processed in country.

In this scenario, if there is no AWS Region or Local Zone present in the country, then AWS Outposts must be used. Outposts should be deployed with sufficient redundant power and network to meet

availability requirements. To avoid impact from local events, the Outposts should be set up in different physical locations with different power and network sources (for example, data centers in different cities). Amazon S3 is available on Outposts, and data can backed-up and recovered from S3 buckets.

Change management

DRHCREL04: Have you planned your hybrid storage, compute, and network capacity ahead of time?

As part of the AWS Shared Responsibility Model, customers are responsible for capacity planning while using AWS Outposts. Customers must forecast compute and storage needs in addition to data center space, power, and HVAC requirements along with associated lead times.

Best practices

- DRHCREL04-BP01 Due to the finite capacity of Outposts on-premises, plan ahead for required compute, storage, and network resources
- DRHCREL04-BP02 Implement proper monitoring and observability practices to track resource utilization, capacity availability, and application health

DRHCREL04-BP01 Due to the finite capacity of Outposts on-premises, plan ahead for required compute, storage, and network resources

Proactively manage AWS Outposts capacity by planning compute, storage, and network resources to ensure high availability and optimal performance while following Well-Architected best practices.

Desired outcome: Achieve efficient allocation and management of Outposts resources, improving availability and compliance with data residency requirements while accommodating future growth and workload demands.

Benefits of establishing this best practice: Proactive resource planning for Outposts validates that there is enough capacity to run workloads even with failures to maintain data residency requirements.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Plan and allocate sufficient compute, storage, and network capacity ahead of time for your workloads on AWS Outposts to meet high availability requirements, right-sizing, and avoiding bottlenecks. Engage AWS Cloud specialists and Support to assist with capacity planning, right-sizing, and monitoring best practices for your Outposts environment, aligning with the operational excellence pillar of the AWS Well-Architected Framework. Use Outposts capacity management to view, plan, and modify capacity configuration.

DRHCREL04-BP02 Implement proper monitoring and observability practices to track resource utilization, capacity availability, and application health

Plan and monitor AWS Outposts capacity proactively through right-sizing, forecasting, and CloudWatch metrics to ensure sufficient N+M capacity for high availability.

Desired outcome: Achieve comprehensive observability over hybrid infrastructure and applications, which provides efficient resource allocation, high availability, and consistent adherence to data residency requirements.

Benefits of establishing this best practice: Following observability best practices enables early detection of potential issues and high availability across hybrid environments while maintaining data residency compliance.

Level of risk exposed if this best practice is not established: High

Implementation guidance

AWS Outposts on-premises has finite capacity. For your workloads to run with high availability, plan your compute and storage capacity ahead of time. Some workloads can also require high network bandwidth or packets per second, which would also require planning to avoid bottlenecks. We recommend right-sizing, benchmarking, and forecasting capacity ahead of time. For guidance on monitoring Outposts capacity, see Monitoring AWS Outposts capacity.

AWS Cloud specialists and Support can assist with right-sizing. The approaches for monitoring Local Zones are the same as Availability Zones in the Region.

For high availability, you can provision additional built-in and always-active capacity on Outposts Rack. Outpost capacity configurations are designed to operate in production environments and support N+M instances for each instance family, where N is the required number of hosts and M is the number of spare hosts provisioned to accommodate failures.

AWS recommends that you allocate sufficient additional capacity for your mission-critical applications to enable recovery and failover if there is an underlying host issue. As a result, capacity planning is very important during the design process. Similarly, it's important to have the right observability in place to allow for fast failover across your resources. You can use Amazon CloudWatch capacity availability metrics and set alarms to monitor the health of your applications, create CloudWatch actions to configure automatic recovery options, and monitor the capacity utilization of your Outposts over time.

Due to the on-premises nature of Outposts, it is important to monitor capacity utilization of both Amazon EC2 and Amazon EBS resources across the Outposts to manage capacity, especially if multiple teams are using the Outpost. In addition to the individual resource level capacity CloudWatch metrics, Capacity Exceptions are also populated and detailed in CloudWatch metrics for AWS Outposts.

CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view. These dashboards are useful for regular reviews of metrics (for example, weekly) to review trends, which is a best practice highlighted in the Well Architected Framework's Operational Excellence Pillar. For an Outposts-specific CloudWatch dashboard, see Deploying an automated Amazon CloudWatch dashboard for AWS Outposts using AWS CDK.

Failure management

DRHCREL05: How do you manage and recover from failure to maintain reliable data access and processing across on-premises, edge, and cloud environments?

Running workloads are subject to disruptions for a number of reasons. Therefore, you must take steps to implement resiliency if you need your workload to be reliable while also meeting your data residency requirements.

DRHCREL06: Is your application resilient to on-premises maintenance activities?

Under the shared responsibility model, AWS is responsible for the hardware and software that run AWS services. This applies to AWS Outposts, just as it does to an AWS Region. AWS monitors the performance, health, and metrics for your Outposts rack and determines whether any maintenance is required. If AWS detects an irreparable issue with hardware during the server provisioning process or while hosting Amazon EC2 instances running on your Outposts server, we will notify the Outpost owner and the owner of the instances that the affected instances are scheduled for retirement. For high availability, your workloads must be resilient during maintenance activities while also preserving data residency requirements.

Best practices

- DRHCREL05-BP01 Provision spare compute capacity following an N+M model
- DRHCREL05-BP02 To mitigate the impact of Availability Zone or Region failures, deploy multiple Outposts anchored to different Availability Zones or Regions
- DRHCREL05-BP03 Maintain high availability during on-premises maintenance activities
- DRHCREL05-BP04 Design your environment to maintain availability and recover in case of failure in a critical sub-system like networking, server, rack, or within the application itself
- DRHCREL06-BP01 Use AWS Health to receive EC2 instance retirement notifications and scheduled events on Outposts that may require instance failover ahead of time

DRHCREL05-BP01 Provision spare compute capacity following an N+M model

Provision spare compute capacity following an N+M availability model, where N is the required capacity and M is the spare capacity to accommodate server failures. Use features like Amazon EC2 Auto Scaling groups, shared storage services, and AWS Elastic Disaster Recovery for reliable recovery.

Desired outcome: Achieve high availability with sufficient spare capacity and seamless failover capabilities in hybrid environments while consistently meeting data residency requirements, even during hardware failures or maintenance events.

Benefits of establishing this best practice: The N+M model improves availability and resilience by providing buffer capacity to handle unexpected server failures or maintenance events, minimizing downtime and maintaining consistent performance while meeting data residency requirements.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Use placement groups with a spread strategy to improve reliability across hardware components. Prepare for network, instances, compute, racks or data centers, and Availability Zone or Region failure modes, and adopt highly-available design. Implement redundant network paths, and map application dependencies to understand the impact of disconnect events. Provide sufficient network redundancy to meet your application's availability requirements.

DRHCREL05-BP02 To mitigate the impact of Availability Zone or Region failures, deploy multiple Outposts anchored to different Availability Zones or Regions

Design workloads across multiple AWS Outposts to ensure resilience against failures through load balancing and failover capabilities, similar to multi-AZ architectures in AWS Regions.

Desired outcome: Achieve a highly available and fault-tolerant hybrid infrastructure that can withstand failures while consistently meeting data residency requirements by using multiple availability zones or Regions for Outposts.

Benefits of establishing this best practice: Deploying multiple Outposts across different Availability Zones or Regions enhances reliability and availability while maintaining data residency compliance.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Design your workload to operate in a distributed, multi-Outpost deployment model, similar to architectural patterns used on AWS. Mitigate the risk of rack, data center, or AWS Availability Zone and Region failures by deploying infrastructure across multiple locations, carefully architecting applications to run across separate logical Outposts, and using distributed multi-Outpost deployment models.

In such architectures, while the application servers may be spread across different Outposts, customers can load balance traffic across Outposts during failover through their Application Load Balancers (ALB) and Amazon Route 53.

DRHCREL05-BP03 Maintain high availability during on-premises maintenance activities

AWS Outposts hardware failures require proactive management through EC2 retirement notifications and automated failover mechanisms.

Desired outcome: Achieve high availability during scheduled maintenance in compliance with residency regulations throughout the maintenance process.

Benefits of establishing this best practice: Maintaining high availability during on-premises maintenance activities minimizes service disruptions and provides high availability while adhering to data residency requirements.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Hardware on AWS Outposts can eventually fail and will need to be replaced. If AWS detects an irreparable issue with hardware hosting Amazon EC2 instances running on your Outpost, AWS notifies the owner of the Outpost and the owner of the instances that the affected instances are scheduled for retirement. As a design precaution, customers should architect for resiliency, just as they do in Regions (for example, by subscribing to instance retirement notifications).

The Outposts owner and EC2 instance owner (these can be different AWS accounts, as resources on the Outposts can be shared) can work together to resolve the issue. The instance owner could stop and start an affected instance to migrate it to available capacity. Instance owners can stop and start the affected instances at a convenient time.

Otherwise, AWS stops and starts the affected instances on the instance retirement date. If there is no additional capacity on the Outpost, the instance remains in the stopped state. The Outpost owner can try to free up used capacity or request additional capacity for the Outpost so that the migration can complete.

If AWS detects an irreparable issue with hardware hosting EC2 instances running on your Outpost, AWS sends an instance-retirement notice for the affected instance. For more information, see

Outposts rack maintenance. When the AWS installation team arrives on site, they replace the unhealthy hosts, switches, or rack elements and bring the new capacity online.

AWS Health events such as instance-retirement are surfaced using AWS EventBridge and the AWS Health API. We recommend updating the correct contact information, especially the operations contact as described in our accounts documentation so that the correct individuals receive these events.

DRHCREL05-BP04 Design your environment to maintain availability and recover in case of failure in a critical sub-system like networking, server, rack, or within the application itself

You should consider the failure modes in this section when planning your Outposts and application deployments. The following sections review how to mitigate these failure modes to provide an increased level of high availability for your application environment.

Desired outcome: Achieve a fault-tolerant application architecture that can withstand failures at various levels of the infrastructure stack and application, which provides high availability and consistent adherence to data residency regulations, even during unexpected system disruptions.

Benefits of establishing this best practice: Implementing high availability mechanisms across all critical sub-systems and application components enhances overall system reliability, minimizes downtime, and maintains compliance with data residency requirements.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Failure mode 1: Network

An Outpost deployment depends on a resilient connection to its parent Region for management and monitoring. Network disruptions may be caused by a variety of failures, such as operator errors, equipment failures, and service provider outages. An Outpost, which may be comprised of one or more racks connected together at the site, is considered disconnected when it cannot communicate with the Region through the service link.

Redundant network paths can help mitigate the risk of disconnect events. You should map application dependencies and network traffic to understand the impact disconnect events will have

on workload operations. Plan sufficient network redundancy to meet your application's availability requirements (for more detail, see AWS Direct Connect Resiliency Recommendations).

During a disconnect event, instances running on an Outpost continue to run and are accessible from on-premises networks through the Outpost local gateway. Local workloads and services may be impaired or fail if they rely on services in the Region. Mutating requests (like starting or stopping instances on the Outpost), control plane operations, and service telemetry (for example, CloudWatch metrics) will fail while the Outpost is disconnected from the Region. It is best to practice to run game days to test service link and local gateway connection failures.

Failure mode 2: Instances

EC2 instances may become impaired or fail if the server they are running on has an issue or if the instance experiences an operating system or application failure. How applications handle these types of failures depends on the application architecture. Monolithic applications typically use application or system features for recovery, while modular service-oriented or microservices architectures typically replace failed components to maintain service availability.

On Outposts racks with local Amazon S3 storage, you can replace failed instances with new instances using automated mechanisms like EC2 Auto Scaling groups and using shared storage service like Amazon S3, multi-AZ Amazon RDS, or Amazon EBS to maintain stateful application data.

AWS Elastic Disaster Recovery (AWS DRS) is available on AWS Outposts racks for reliable recovery in the event of a site failure (for more detail, see Architecting for Disaster Recovery on AWS Outposts racks with AWS Elastic Disaster Recovery). Use AWS Outposts static stability for Amazon EC2 instances backed by EC2 instance store. This enables automatic recovery for workloads running on such EC2 instances from power failures or reboots, even when the connection to the parent AWS Region is temporarily unavailable.

Failure mode 3: Compute

Compute hardware can fail or become impaired and may need to be taken out of operation (temporarily or permanently) for a variety of reasons, such as component failures and scheduled maintenance operations. How services on Outposts rack handle hardware failures and impairments varies and can depend on how customers configure high availability options.

You should order sufficient compute capacity to support an N+M availability model, where N is the required capacity and M is the spare capacity provisioned to accommodate server failures.

On-premises hardware replacements for failed components are completed by AWS as part of the fully-managed AWS Outposts Rack service. AWS actively monitors the health of all servers and networking devices in an Outpost deployment. If there is a need to perform physical maintenance, AWS schedules a time to visit your site to replace failed components.

Provisioning spare capacity allows you to keep your workloads running while failed servers are taken out of service and replaced. To improve reliability across hardware components, placement groups with a spread strategy on an Outpost can spread instances across hosts or racks. Outposts servers with hardware failures can be returned, and replacements are shipped out as part of the replacement process.

Failure mode 4: Racks or data centers

Rack failures may occur due to a total loss of power to racks or due to environmental failures like loss of cooling or physical damage to the data center from a flood or earthquake. Deficiencies in data center power distribution architectures or errors during standard data center power maintenance can result in loss of power to one or more racks or even the entire data center.

These scenarios can be mitigated by deploying infrastructure to multiple data center floors or locations that are independent from one another within the same campus or metro area. Taking this approach with AWS Outposts rack requires careful consideration for how applications are architected and distributed to run across multiple separate logical Outposts to maintain application availability.

Failure mode 5: AWS Availability Zone or Region

Each Outpost is anchored to a specific Availability Zone within an AWS Region. Failures within the anchor Availability Zone or parent Region could cause the loss of Outpost management and mutability and may disrupt network communication between the Outpost and the Region.

Similar to network failures, Availability Zone or Region failures may cause the Outpost to become disconnected from the Region. The instances running on an Outpost continue to run and are accessible from on-premises networks through the Outpost local gateway and may be impaired or fail if they rely on services in the Region.

To mitigate the impact of Availability Zone and Region failures, you can deploy multiple Outposts each anchored to a different Availability Zone or Region. You may then design your workload to operate in a distributed multi-Outpost deployment model using many of the similar mechanisms and architectural patterns that you use to design and deploy on AWS today.

DRHCREL06-BP01 Use AWS Health to receive EC2 instance retirement notifications and scheduled events on Outposts that may require instance failover ahead of time

Configure AWS Health event monitoring and maintain current operations contact information while ensuring adequate capacity to minimize impact during maintenance activities.

Desired outcome: Use AWS Health for getting AWS events signals and taking recommended actions, providing high availability while meeting data residency requirements.

Benefits of establishing this best practice: Using AWS Health for proactive notifications allows for timely planning and initiation of instance failovers, minimizing potential downtime while meeting data residency requirements during maintenance events.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Monitor AWS Health events through AWS EventBridge, AWS Health API, or email. We recommend updating the correct contact information, especially the operations contact as described in our accounts documentation so that the correct individuals receive these events. Provide sufficient capacity and highly available design to avoid any impact during maintenance activities.

Key AWS services

- AWS Outposts
- AWS Local Zones

Resources

- Outposts disaster recovery and resiliency
- AWS Outposts High Availability Design
- AWS Local Zones
- Outposts monitoring best practices
- Hybrid Architectures to address Personal Data Processing Requirements
- Architecting for Disaster Recovery on AWS Outposts racks with AWS Elastic Disaster Recovery

- Direct Connect resiliency recommendation
- Implementing backup for workloads running on AWS Outposts servers

Performance efficiency

The performance efficiency pillar includes the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve. This section provides an overview of design principles, best practices, and questions. You can find further implementation guidance in the Performance Efficiency Pillar whitepaper.

Definitions

This whitepaper covers performance efficiency in the cloud, describing best practices in the following areas:

- Architecture selection
- Data management
- Networking and content delivery
- Process and culture

Design principles

The performance efficiency pillar focuses on the efficient use of resources to meet requirements and the maintenance of that efficiency as demand changes and technologies evolve. Performance optimization is not a one-time activity. It is an incremental and continual process of confirming business requirements, measuring the workload performance, identifying under-performing components, and tuning the components to meet your business needs. This section includes best practice considerations to maintain performance efficiency at the edge.

The following best practices are provided for customers with data residency requirements. Please use these to access your architecture in addition to the general best practices found in the Well-Architected Performance Efficiency Pillar.

Architecture selection

DRHCPERF01: How do you achieve performant workload configuration?

To achieve performant workload configuration in a hybrid edge architecture, organizations should understand their workload requirements to achieve optimal architecture.

Best practices

- DRHCPERF01-BP01 Understand your data residency requirements when selecting the platform for your workload
- DRHCPERF01-BP02 Monitor hybrid edge-specific metrics, and update resource configurations

DRHCPERF01-BP01 Understand your data residency requirements when selecting the platform for your workload

Assess your data residency requirements first to guide your workload deployment location.

Desired outcome: You should understand your data residency requirements in order to decide where to deploy the workload.

Benefits of establishing this best practice: You can understand how workload location impacts where the data resides.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

You should consider all workload requirements when planning hybrid edge configurations, and assess the different services available in AWS Regions, Local Zones, and Outposts to best suit your needs.

DRHCPERF01-BP02 Monitor hybrid edge-specific metrics, and update resource configurations

Monitor your current capacity and plan for scaling to meet demand.

Desired outcome: You are aware of what capacity you have, and you scale as needed.

Benefits of establishing this best practice: You can proactively make decisions to acquire the appropriate capacity for your workloads.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Outposts surfaces Amazon CloudWatch metric data, including CPU, network, and storage. You should monitor these metrics as you would in-Region to verify that you are achieving your performance targets. Monitor your resource consumption, and right-size compute and storage configurations based on the metric data. This is an iterative process as workloads change over time. Each server has a specific slotting configuration based on initial order. This can be modified based on metric data as long as the configuration is supported by the underlying server. For supported configurations, see Modify AWS Outposts instance capacity.

Compute and hardware

There are no compute and hardware best practices specific to digital residency with hybrid cloud services workloads.

Data management

DRHCPERF02: Is your workload modular in design such that components can be easily altered to embrace new technologies?

AWS is constantly releasing new services, features, and functionality. Keeping workloads modular and loosely coupled enables faster adoption of these capabilities.

Best practices

- DRHCPERF02-BP01 Design workloads with modularity and loose coupling

DRHCPERF02-BP01 Design workloads with modularity and loose coupling

New capability deployment starts in the commercial regions and moves out to the edge based on feedback from customers.

Desired outcome: You can simplify management and reduce architectural complexity by adopting new services as they become available.

Benefits of establishing this best practice: You can easily implement the latest features and functionality into the workload.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Cloud architectures differ from traditional on-premises in providing reliable compute, storage, and networking capabilities. An instance is an instantiation of an application component. Application components can operate independently thanks to loosely coupled instances, allowing for flexible scaling and seamless replacement without disrupting the overall system architecture.

This approach helps organizations seamlessly integrate new hybrid edge capabilities into their existing workloads. Periodically review data residency compliance requirements, as these can impact the overall design and implementation strategy. You can monitor the What's New with AWS webpage and AWS Blogs to stay updated on the latest hybrid edge offerings from AWS.

By staying informed about these new capabilities and their potential integration into existing workloads, you can meet evolving business and regulatory requirements while realizing the benefits of hybrid edge computing.

Networking and content delivery

DRHCPERF03: How do you engineer network traffic flow to meet workload performance requirements?

In order to maintain performant workloads, you should keep network flows local to the compute environment.

Best practices

- DRHCPERF03-BP01 Engineer optimal traffic flow for the edge solution

DRHCPERF03-BP01 Engineer optimal traffic flow for the edge solution

Design network routing for data residency requirements.

Desired outcome: You use the most optimal network path.

Benefits of establishing this best practice: Optimal routing helps provide the best user experience for applications while working within data residency requirements.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Within a multi-VPC configuration, use VPC peering over AWS Transit Gateway to keep inter-VPC traffic within AWS Outposts and AWS Local Zones. For traffic that needs to leave the Outposts and Local Zones, engineer network traffic flow to align the network path to the desired performance profile. You can identify latency to AWS Regions and Local Zones using a tool like AWS latency test. AWS Outposts rack customers should use the local gateway path instead of the service link path where possible. AWS Outposts servers should use the local network interface instead of the service link path where possible.

Process and culture

DRHCPERF04: How do you know if your edge workload performance characteristics are healthy or at risk?

In order for you to meet the application requirements, monitor the system end-to-end. The application at edge can span hybrid edge services as well as on-premises infrastructure.

Best practices

- DRHCPERF04-BP01 Establish hybrid edge workload health KPIs

DRHCPERF04-BP01 Establish hybrid edge workload health KPIs

Demonstrate your workload is meeting your business requirements.

Desired outcome: You can illustrate you are meeting your business requirements for the workload.

Benefits of establishing this best practice: Metrics can provide data for continuous workload improvement.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

You should develop key performance indicators (KPIs) to show how effectively you're achieving objectives applicable to your workload. AWS Outposts has additional metrics that should be monitored. Determine the application KPI's to monitor to provide the optimal user experience.

Instrument your code using a tool such as AWS X-Ray, and use Amazon CloudWatch to monitor in-Region dependencies. You should monitor service link bandwidth and round trip latency to provide optimal performance. Hybrid edge services must meet unique minimum requirements as defined in the User Guide for Outposts racks and servers.

Key AWS services

- AWS Local Zones
- AWS Outposts
- AWS X-Ray
- Amazon CloudWatch
- AWS Transit Gateway
- Amazon VPC

Resources

Related documentation:

- Monitoring best practices for AWS Outposts
- Deploying an automated Amazon CloudWatch dashboard for AWS Outposts using AWS CDK
- Creating computing quotas on AWS Outposts rack with EC2 Capacity Reservations sharing
- Recommended practices for application/workload routing from AWS Outposts High Availability Design and Architecture Considerations
- AWS Outposts High Availability Design and Architecture Considerations

Cost optimization

The cost optimization pillar includes the ability to use all resources to deliver business value at the lowest price point. This section provides you with an overview of design principles, best practices, and questions. You can find further implementation guidance in the Cost Optimization Pillar whitepaper.

Definitions

This whitepaper covers cost optimization in the cloud, describing best practices in the following areas:

- Practice Cloud Financial Management
- Expenditure and usage awareness
- Cost-effective resources
- Manage demand and supply resources
- Optimize over time

Design principles

The cost optimization pillar focuses on the efficient use of resources to meet requirements and the maintenance of that cost as demand changes and technologies evolve. Cost optimization is not a one-time activity. It is an incremental and continual process of confirming business requirements, measuring the workload performance and cost, identifying under-performing components, and tuning the components to meet your business needs. The goal of this pillar is to only pay for what you need to run your workload.

Cost optimization includes the continual process of refinement and improvement of a system over its entire lifecycle. In a hybrid cloud environment that spans on-premises customer data centers, AWS Cloud, and AWS's hybrid edge offerings such as Outposts, Local Zones, and Wavelength, cost optimization becomes a multifaceted challenge.

This section provides guidance and best practices to help organizations achieve cost-effective and efficient operations across this diverse infrastructure landscape. By following the principles outlined in this pillar, organizations can gain visibility into expenditure, select cost-effective resources for workloads, manage demand and supply effectively, and optimize costs over time.

With a hybrid cloud approach involving on-premises data centers and hybrid edge offerings, organizations must carefully evaluate factors such as data transfer costs between environments, pricing models across different services and locations, and the potential for resource sharing.

The cost optimization pillar offers strategies to address these challenges so that organizations can maximize the financial benefits of a hybrid cloud architecture while maintaining operational excellence, security, reliability, and performance across all environments.

Practice Cloud Financial Management

DRHCCOST01: Have you defined a tagging strategy for your hybrid edge workloads?

Tagging helps you meter usage and facilitate cost attribution.

Best practices

- DRHCCOST01-BP01 Implement a comprehensive tagging strategy for hybrid edge workloads

DRHCCOST01-BP01 Implement a comprehensive tagging strategy for hybrid edge workloads

Implement cost attribution using resource tagging.

Desired outcome: You use tags to attribute workload costs.

Benefits of establishing this best practice: You can have a better understanding of what is driving the cost of the workload.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Implementing a comprehensive tagging strategy is crucial for effectively managing hybrid edge workloads. Tagging enables cost attribution and usage metering through the use of identifiers and cost allocation tags in the Cost and Usage Report (CUR). It also facilitates management and governance and lifecycle management through automation of policies and processes using custom tags and services like AWS Config and AWS Systems Manager.

Tagging in hybrid edge environments like Outposts and Local Zones operates similarly to cloud Regions, providing a consistent experience and familiar tools. Organizations can use existing tools and services to manage tagging strategies at scale across hybrid edge workloads, including implementing automated tagging policies and remediation workflows to comply with tagging standards.

Tagging enables organizations to derive total cost of ownership associated with workloads. Tagging in hybrid edge (Outposts and Local Zones) operates similarly as in-Region. Once a tag is activated as a cost allocation tag, data appears in the Cost and Usage Report (CUR) for analysis.

Expenditure and usage awareness

DRHCCOST02: How do you achieve the maximum value out of Outposts?

Outposts are fixed and finite capacity that can be scaled. Understanding available capacity helps you plan accordingly and maximize value in the investment.

Best practices

- DRHCCOST02-BP01 Monitor and manage Outposts capacity and utilization effectively

DRHCCOST02-BP01 Monitor and manage Outposts capacity and utilization effectively

Understand available edge capacity and its utilization.

Desired outcome: You are aware of what capacity they have, and you scale as needed.

Benefits of establishing this best practice: You can proactively make decisions to provide the appropriate capacity and minimize unexpected cost.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Actively monitor and manage Outposts capacity and utilization. AWS recommends Amazon CloudWatch to track usage and available Outposts CloudWatch metrics for Amazon EC2, Amazon

EBS, Amazon S3, and network resources, which helps organizations meet their business objectives and proactively make scaling decisions.

Outposts capacity scales in fixed increments, with cost increasing accordingly, and scaling actions can extend the service term. You should plan for future generation Outposts, as it is a managed service and AWS retrieves Outposts at the end of the service period. You can extend the existing term or consider replacement Outposts to adopt new services and features.

Maintaining appropriate spare capacity is crucial, as Outposts has redundant components, and spare compute and storage capacity ensure hardware failures do not affect workloads and minimize sunk costs. AWS tools like AWS Compute Optimizer can be used for rightsizing workloads in Outposts while considering business objectives and utilization goals.

Monitor the What's New with AWS webpage to evaluate new services and offerings for Outposts and Local Zones. Adopt services that can reduce the cost profile of workloads and foster innovation.

Cost-effective resources

DRHCCOST03: How do you target workload placement to achieve greatest cost efficiency?

In order to properly place of a workload, you must understand workload profiles. Outposts, Local Zones, and Regions offer different capabilities at different costs.

Best practices

- DRHCCOST03-BP01: Optimize placement of running workloads

DRHCCOST03-BP01: Optimize placement of running workloads

Select the most economical location by comparing costs.

Desired outcome: You choose the cost-effective place to run your workload by reviewing service costs across the cloud continuum.

Benefits of establishing this best practice: You realize savings by selecting a location that offers the required services to build your workload and achieve your data residency requirements.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

To properly place a workload, you must understand your workload profiles and requirements. AWS offers a range of options across the cloud continuum, including AWS Outposts, Local Zones, and Regions, each with different capabilities and costs. By evaluating workload requirements, you can select the most cost-effective location to run your workloads while meeting your data residency and service requirements.

Manage demand and supply resources

DRHCCOST04: How do you manage the lifecycle of your edge data?

Lifecycle management is important regardless of where you run your workload. It is cost effective to only retain needed data according to business requirements.

Best practices

- DRHCCOST04-BP01 Implement mechanisms to manage the lifecycle of Amazon S3 data, EBS volumes, and snapshots

DRHCCOST04-BP01 Implement mechanisms to manage the lifecycle of Amazon S3 data, EBS volumes, and snapshots

Apply data lifecycle management practices to hybrid edge environments.

Desired outcome: You can implement familiar mechanisms like you would in-Region to manage the lifecycle of your hybrid edge data.

Benefits of establishing this best practice: Through the use of familiar mechanisms, you can retain relevant data.

Level of risk exposed if this best practice is not established: High

Implementation guidance

Outposts contain fixed capacity specific to their configuration. You can manage the lifecycle of your data with familiar services such as S3 Lifecycle for Amazon S3 on Outposts and Data Lifecycle Manager for Amazon EBS. Consider archiving Amazon S3 content to AWS Regions using DataSync if possible.

Optimize over time

DRHCCOST05: How do you optimize network configuration for edge services?

Services have different costs depending on where they are run in the cloud continuum.

Best practices

- DRHCCOST05-BP01 Monitor data transfer to and from your hybrid edge workload

DRHCCOST05-BP01 Monitor data transfer to and from your hybrid edge workload

Regularly track and analyze data transfer costs.

Desired outcome: You monitor the costs associated with data transfer.

Benefits of establishing this best practice: You can recognize the cost associated with your network flows.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

While using hybrid edge services like AWS Outposts and Local Zones, monitor data transfer patterns and costs, and design your network configurations with cost optimization in mind. Data transfer from Outposts to AWS Regions is free, but transfers from Regions to Outposts are more expensive over the internet compared to AWS Direct Connect. Local Zones have internet gateways for local egress, but routing traffic to AWS Regions incurs additional charges similar to inter-AZ transfers. You can use local VPC peering for Outposts and Local Zones, which incurs lower costs

than using AWS Transit Gateway and minimizes network overhead. Additionally, you should design hybrid architectures following networking best practices to meet low latency requirements while optimizing costs.

Key AWS services

- AWS Cost Explorer
- AWS Local Zones
- AWS Outposts
- Amazon S3
- AWS DataSync
- AWS Compute Optimizer
- AWS Config

Resources

- CloudWatch metrics for Outposts
- What's New with AWS

Sustainability

The sustainability pillar includes the ability to deliver business value while minimizing resource usage, environmental impacts, and energy consumption. This section provides you with an overview of sustainability design principles, best practices, and questions. You can find implementation guidance in the Sustainability Pillar whitepaper.

Definitions

This whitepaper covers sustainability in the cloud, describing best practices in the following areas:

- Region selection
- Alignment to demand
- Software and architecture patterns
- Data management
- Hardware and services

Design principles

The Well-Architected Framework identifies a set of general design principles to facilitate sustainability while deploying hybrid services and workloads:

- **Consider workload placement:** It is always a best practice to use AWS Regions when building workloads, as Regions offer tools for managing service and instance elasticity. If a workload has latency or data residency requirements that cannot be addressed in a Region, consider using an AWS Local Zone where workload elasticity is still easily achieved with Amazon EC2. If a Local Zone cannot meet workload requirements, consider using AWS Outposts, where capacity must be more precisely matched with requirements.
- **Characterize workload requirements:** Before using AWS hybrid services, fully assess and understand your workload resource requirements. Always engage an AWS migration specialist, and use the AWS Migration Evaluator to capture workload resource utilization to make a data-driven decision on which hybrid services to use and how much capacity to deploy.
- **Match EC2 instance size to measured load:** Use tools such as Amazon CloudWatch and AWS Compute Optimizer to track EC2 instance resource utilization and right-size instances based on data-driven recommendations.

Region selection

DRHCSUS01: How do you assess the sustainability of anchor AWS Regions when selecting an AWS Local Zone?

The sustainability characteristics of an AWS Local Zone's anchor region should be considered when more than one Local Zone can address your data residency requirements.

Best practices

- DRHCSUS01-BP01 Choose the Local Zone anchored to the Region that best aligns with your sustainability goals if more than one meets your data-residency requirements
- DRHCSUS01-BP02 Anchor your AWS Outposts to the Region that best aligns to both your cloud deployment patterns and sustainability goals

DRHCSUS01-BP01 Choose the Local Zone anchored to the Region that best aligns with your sustainability goals if more than one meets your data-residency requirements

It may be possible to evaluate and choose an AWS Local Zone that is anchored to a more sustainable AWS Region when there are several which meet your data residency requirements.

Desired outcome: Services are deployed to the Local Zone anchored to the most sustainable parent AWS Region.

Benefits of establishing this best practice: You can choose an AWS Local Zone that is anchored to a more sustainable AWS Region to support your sustainability objectives.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

AWS Local Zones are always anchored to a parent AWS Region where control plane functions and the full set of AWS services are made available for building solutions. When considering a Local Zone for data residency use cases, there may be only one that meets your requirements. However, there may be times where more than one Local Zone can be used, each anchored to different parent Regions. When this is the case, select an AWS Region based on sustainability and

deploy to the Local Zone that is anchored to that Region. For more detail on Local Zone to Region relationships, see AWS Local Zones locations.

DRHCSUS01-BP02 Anchor your AWS Outposts to the Region that best aligns to both your cloud deployment patterns and sustainability goals

You have the flexibility to anchor an AWS Outposts to any supported AWS Region and can consider anchoring to an AWS Region that helps you meet your sustainability objectives.

Desired outcome: Your AWS Outposts are anchored using a service link connection to the most sustainable AWS Region.

Benefits of establishing this best practice: Choosing to anchor your AWS Outposts to a more sustainable AWS Region can help you meet your sustainability objectives.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

AWS Outposts must be anchored to service link endpoints exposed in an AWS Region. The Region to which an AWS Outpost is anchored is determined at the time an order is placed. Unlike with Local Zones, an AWS Outpost can be anchored to any supported Region, so you have more flexibility to select the anchor Region based on your sustainability goals. When deploying an AWS Outpost to address data residency requirements, consider anchoring it to the most sustainable Region that also aligns with your overall networking and application architecture patterns.

Alignment to demand

DRHCSUS02: How are you scaling and sizing your infrastructure to match demand and minimize resource consumption?

Infrastructure resources such as Amazon EC2 instances and load balancers should be dynamically scaled to match observed demand.

Best practices

- DRHCSUS02-BP01 When using Local Zones, monitor and scale your workloads to match demand, and use only the minimum required resources

- DRHCSUS02-BP02 Before ordering an AWS Outpost, engage with an AWS Outposts specialist to verify that the ordered capacity aligns with your workload requirements

DRHCSUS02-BP01 When using Local Zones, monitor and scale your workloads to match demand, and use only the minimum required resources

Resources and services in AWS Local Zones, like those in AWS Regions, can be scaled dynamically to match measured demand, minimizing energy consumption.

Desired outcome: The number and type of Amazon EC2 instances deployed will be optimized to support workload requirements while adhering to sustainability goals

Benefits of establishing this best practice: Resource utilization can be reduced to minimize energy consumption and support your sustainability objectives.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Although Local Zones provide only a subset of the Amazon EC2 instance families and types available in an AWS Region, you should still use AWS capabilities that support elasticity to monitor and scale workloads to meet the measured demand and improve sustainability.

Services such as Auto Scaling groups, Amazon CloudWatch, and AWS Compute Optimizer can be used to optimize the number and sizes of EC2 instances to meet workload demands. For Amazon EKS workloads, consider using Karpenter to automatically scale Kubernetes clusters to match instantaneous demand using instances aligned exactly to compute demands. For more detail on scaling for sustainability, see SUS02-BP01 Scale workload infrastructure dynamically and SUS02-BP03 Stop the creation and maintenance of unused assets .

DRHCSUS02-BP02 Before ordering an AWS Outpost, engage with an AWS Outposts specialist to verify that the ordered capacity aligns with your workload requirements

Care should be given to aligning AWS Outposts capacity to actual resource requirements before placing an order to avoid overprovisioning capacity that cannot be scaled down after deployment.

Desired outcome: Outposts configurations will be developed to address workload requirement while minimizing overprovisioning of capacity

Benefits of establishing this best practice: Only the capacity needed to support your workload and resiliency requirements will be ordered, minimizing energy consumption.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

AWS Outposts provide fixed and finite capacity which cannot be quickly scaled to accommodate changes in demand. Outposts are instead configured to meet your unique data-residency requirements, and it is important to work with your AWS account team to engage AWS hybrid specialists to verify that both workload and sustainability requirements are considered to develop the most efficient Outposts configuration before ordering.

Because Outposts are frequently used to migrate existing physical or virtual workloads from on-premises data-centers, and because these workloads are commonly over-provisioned, use tools such as the AWS Migration Evaluator to correctly size Outposts for the actual observed demand, plus any margin for resiliency and growth.

Software and architecture patterns

DRHCSUS03: How do you monitor workloads and evaluate architectures to support your sustainability goals?

Workloads should be monitored to support optimal sizing, scaling, and alignment to sustainability objectives.

Best practices

- DRHCSUS03-BP01 Monitor workload and component resource utilization to identify any that are unneeded or over-provisioned when using Local Zones
- DRHCSUS03-BP02 Monitor both workload resource utilization and Amazon EC2 instance consumption to maximize the use of AWS Outpost resources and improve sustainability

DRHCSUS03-BP01 Monitor workload and component resource utilization to identify any that are unneeded or over-provisioned when using Local Zones

Monitoring workload utilization is critical to identifying those which are overprovisioned and can be scaled down to reduce energy consumption.

Desired outcome: Workloads are deployed on Amazon EC2 instances that are aligned to requirements and provide optimal performance.

Benefits of establishing this best practice: Workloads and resources which are overprovisioned can be scaled down to reduce energy consumption and support sustainability objectives.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Monitor and capture workload metrics such as CPU utilization, memory utilization, network connections, and network throughput using Amazon CloudWatch metrics to identify workloads or components that are no longer used or are under-utilized. Routinely review the recommendations made by AWS Compute Optimizer to identify instances that have been over-provisioned, and adjust as necessary to match instance type and size to the workload requirements. With AWS Local Zones, it is possible to maximize sustainability by using the large variety of Amazon EC2 instances to match resource consumption to workload requirements.

DRHCSUS03-BP02 Monitor both workload resource utilization and Amazon EC2 instance consumption to maximize the use of AWS Outpost resources and improve sustainability

Portable workloads can be migrated from AWS Regions onto unused or underutilized compute resources on AWS Outposts to minimize energy consumption and maximize the use of fixed AWS Outposts resources.

Desired outcome: Outpost capacity is aligned to workload requirements and desired resiliency objectives. If, over time, an Outpost becomes underutilized, suitable workloads can be migrated from the Region to use the Outpost's capacity (while maintaining capacity for resiliency), reducing consumption in AWS Regions to support sustainability objectives.

Benefits of establishing this best practice: You can maximize utilization of your fixed, underutilized AWS Outposts compute resources by migrating portable workloads out of AWS Regions to minimize overall energy consumption.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

AWS Outposts provide a long-term, fixed, and finite pool of compute resources for addressing data residency and low latency use cases. Because AWS Outposts capacity is both fixed and purchased for terms spanning one to five years, it is critical that it be used to the fullest extent possible.

Use services such as Amazon CloudWatch metrics and AWS Compute Optimizer to monitor workload and instance metrics such as CPU utilization, memory utilization, network connections, and network throughput. Identify instances that have been over-provisioned and adjust as necessary to match instance type and size to the workload requirements. By matching instance type and size to workload requirements, you can free capacity on an Outpost to support workloads that would otherwise be deployed in the parent Region, which provides maximum value from the capacity already purchased on the Outpost.

When moving workloads to AWS Outposts, maintain spare capacity to absorb workloads if hardware in the Outpost fails. An Amazon EC2 server to spare ratio of eight to one is commonly used when planning for instance resiliency and potential hardware failures.

Data management

DRHCSUS04: How do you optimize the use of AWS block and object storage to meet your sustainability goals?

Sizing and placement of block and object storage should be optimized to use the most efficient and sustainable storage services.

DRHCSUS05. How does your organization minimize the duplication of data?

Shared storage services that minimize duplication of data should be implemented whenever possible with workloads to reduce overall storage requirements and energy consumption.

Best practices

- DRHCSUS04-BP01 Consider sustainable object storage options for Local Zones
- DRHCSUS04-BP02 Use elasticity and automation to optimize storage volumes usage in AWS Local Zones
- DRHCSUS04-BP03 Consider sustainable storage options for AWS Outposts
- DRHCSUS05-BP01 Consider using supported AWS-managed file services to minimize data duplication in Local Zones
- DRHCSUS05-BP02 Consider Amazon S3 for Outposts, or deploy a self-managed shared-file sharing solution

DRHCSUS04-BP01 Consider sustainable object storage options for Local Zones

Amazon S3 Object storage in AWS Regions used by workloads deployed in AWS Local Zones can be optimized to use the most energy-efficient and sustainable service tiers, based on data access and resiliency requirements.

Desired outcome: Data and objects are stored in the lowest cost and most sustainable Amazon S3 service tier based on access profiles.

Benefits of establishing this best practice: The energy and cost efficiency of Amazon S3 object storage will be aligned to the data resiliency and access requirements.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Although Amazon S3 is not available natively in Local Zones, you can still use S3 buckets located in AWS Regions to store data that is not, or is no longer, subject to data residency policies. When doing so, review the Amazon S3 Storage Classes, and implement Amazon S3 storage lifecycle policies to migrate infrequently accessed data into more sustainable storage Classes such as Amazon S3 Glacier.

This practice not only optimizes storage costs and improves data management but also reduces energy consumption and environmental impact through the use of the most energy-efficient storage technologies.

DRHCSUS04-BP02 Use elasticity and automation to optimize storage volumes usage in AWS Local Zones

EBS volumes attached to EC2 instances in AWS Local Zones should be provisioned as small as possible to meet workload requirements and then grown as needed when more capacity is required.

Desired outcome: EBS volumes will be sized to meet workload requirements and minimize energy consumption, while growing dynamically via automation when needed.

Benefits of establishing this best practice: Your workloads will be provisioned to use the minimum required EBS storage, decreasing energy consumption, while retaining the ability to grow storage via automation when needed.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Create and use Amazon EBS volumes in Local Zones with size, throughput, and latency characteristics appropriate for your data residency workloads. Provision the smallest suitable EBS volumes, and use elasticity and automation to expand volumes as data grows. This improves sustainability by preventing over-provisioning of workload storage. Use Amazon CloudWatch Agent to collect and monitor guest disk utilization, and set thresholds to initiate EBS volume expansion when thresholds are reached.

DRHCSUS04-BP03 Consider sustainable storage options for AWS Outposts

Both Amazon S3 on Outposts and Amazon EBS provide tools for data lifecycle management, the functions of which should be considered in advance when sizing and ordering storage for an AWS Outposts.

Desired outcome: Amazon S3 resources deployed on Outposts can be minimized to align with workload demands, not over-provisioned.

Benefits of establishing this best practice: Amazon S3 and Amazon EBS storage sizing can be minimized through the implementation of data retention and lifecycle management tools.

Level of risk exposed if this best practice is not established: Medium

Amazon S3 on Outposts provides object storage on-premises for use with data residency workloads. AWS Outposts have a fixed amount of Amazon EBS and Amazon S3 storage capacity that is pre-configured while ordering. Because capacity can be scaled up or down after deployment, it is recommended that both Amazon EBS and Amazon S3 storage be sized appropriately for your data residency storage requirements, accounting for future needs but not excessively over-provisioned.

When sizing Amazon S3 on Outposts storage before ordering, consider the potential of using Amazon S3 lifecycle polices to expire bucket objects, delete non-current objects, or delete incomplete multi-part uploads to reduce overall Amazon S3 storage requirements. By managing Amazon S3 buckets and objects to maintain only current or necessary data, you can improve sustainability by minimizing Outposts storage resources and power requirements.

Also consider the potential of using Amazon Data Lifecycle Manager to manage Amazon EBS snapshot and Amazon EBS-backed AMI retention policies to reduce overall Amazon S3 storage requirements.

DRHCSUS05-BP01 Consider using supported AWS-managed file services to minimize data duplication in Local Zones

Shared file services can be implemented using AWS managed file services, AWS marketplace offerings, or even self-managed solutions to minimize data duplication for your data-residency workloads.

Desired outcome: Duplication of data is minimized using managed or self-managed shared storage services in Local Zones.

Benefits of establishing this best practice: Data duplication and overall storage consumption can be minimized to reduce energy utilization and support your sustainability objectives.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

A growing number of AWS Local Zones now support Amazon FSx for Windows File Server and Amazon FSx for Lustre. These managed shared-file services can be used to efficiently store and share data between large numbers of data residency workloads, minimizing the environmental costs of duplicating data for individual workloads or users. While choosing a Local Zone, review the Local Zone feature matrix to determine if these services are available in location that meets your data residency requirements.

If Amazon FSx services are not available in the Local Zone you choose, consider using self-managed or AWS Marketplace shared storage solutions for Windows SMB or NFS shares to minimize the duplication or movement of data within the Local Zone.

DRHCSUS05-BP02 Consider Amazon S3 for Outposts, or deploy a self-managed shared-file sharing solution

Amazon S3 for Outposts or EBS-backed shared storage solutions which are self-managed or procured from the AWS Marketplace can be used to reduce data duplication and overall storage consumption.

Desired outcome: Duplication of data will be minimized using local S3, managed, or self-managed shared storage services on Outposts

Benefits of establishing this best practice: Data duplication can be minimized, reducing overall storage requirements and energy consumption for on-premises data-residency workloads.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

AWS Outposts supports Amazon S3 for AWS Outposts, which can be used for on-premises shared object storage. The use of shared data provides data consistency and prevents the inefficient use of per-user or per-application data duplication. Where Amazon S3 for AWS Outposts is not deployed or is unsuitable for workload requirements, consider using self-managed or AWS Marketplace shared storage solutions that are compatible with Amazon Elastic Block Store (EBS) on Outposts volume-types as their backing storage.

Hardware and services

DRHCSUS06: How do you choose and update EC2 instances to support both data-residency workload and sustainability goals?

Using the latest available instance families, which are frequently more efficient than their predecessors, can improve efficiency and reduce energy utilization for your data-residency workloads.

Best practices

- DRHCSUS06-BP01 Monitor Local Zone hardware introductions, and choose the latest EC2 Instances to take advantage of energy efficiency improvements
- DRHCSUS06-BP02 Track AWS Outposts roadmaps, and structure contracts to enable timely upgrades to the latest EC2 instances

DRHCSUS06-BP01 Monitor Local Zone hardware introductions, and choose the latest EC2 Instances to take advantage of energy efficiency improvements

As new more powerful and efficient Amazon EC2 instance families are introduced into AWS Local Zones they should be adopted to reduce the number of EC2 instances used and overall energy consumption.

Desired outcome: You use most energy efficient and performant Amazon EC2 offerings to deploy workloads.

Benefits of establishing this best practice: By adopting the latest Amazon EC2 families, it may be possible to reduce the number of Amazon EC2 instances needed to support your data-residency workloads.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Monitor AWS Local Zones features to discover the latest generation of Amazon EC2 instances, and use these whenever possible. New Amazon EC2 instance types often incorporate energy

efficiency improvements using the latest Intel processor families or AWS-optimized processor architectures such as AWS Graviton. Some of the latest instance types integrate specialized hardware accelerators such as GPUs or FPGAs to offload compute-intensive tasks from the CPU, resulting in overall improved performance per watt. This improved performance per watt in turn reduces energy consumption to help meet your sustainability goals and improve performance for data residency workloads.

DRHCSUS06-BP02 Track AWS Outposts roadmaps, and structure contracts to enable timely upgrades to the latest EC2 instances

When new more powerful and efficient AWS Outposts offerings are on the near-term roadmap you should consider refreshing at the end of your current AWS Outposts term, or consider using a shorter term with the existing generation if current needs must be met before the next generation is available.

Desired outcome: You have option to refresh your Outposts deployment with the latest, most efficient, and performant hardware.

Benefits of establishing this best practice: You will be able to leverage the latest, most efficient and powerful AWS Outposts offerings as early as possible for your data-residency workloads.

Level of risk exposed if this best practice is not established: Medium

Implementation guidance

Unlike with AWS Local Zones, AWS Outposts EC2 families and instances remain fixed over the life of a deployment contract term (typically one, three, or five years). This can present a challenge for customers wishing to adopt the newest Amazon EC2 instances.

When there is a need or desire to take advantage of the latest AWS Outposts and EC2 instance offerings, consult with your AWS account team and Outposts hybrid specialists to review roadmaps and timelines. Consider using shorter contract terms to pursue AWS Outposts upgrades and meet future data residency compute requirements.

Process and culture

There are no process and culture best practices unique to data residency and hybrid cloud services workloads.

Key AWS services

- AWS Compute Optimizer
- AWS Migration Hub
- AWS Trusted Advisor
- Instance Auto Scaling
- AWS Carbon Footprint Tool
- AWS Systems Manager Inventory

Resources

- Sustainability Pillar for AWS Well-Architected Framework
- Reducing carbon by moving to AWS
- The Cloud - Amazon Sustainability
- Sustainable Cloud Computing

Conclusion

The DRHC Lens provides comprehensive guidance for designing and operating Well-Architected hybrid cloud workloads with data residency requirements. By following the recommendations in this lens, organizations can unlock the full potential of AWS Hybrid Cloud services while maintaining control over their data's geographic location.

The lens covers strategies for designing resilient and highly available hybrid architectures. It provides guidance on classifying data, establishing operational practices for data sovereignty, and using regional cloud services to augment on-premises solutions. The lens also discusses implementing controls to enhance digital sovereignty and restrict access based on location. It covers deployment of robust security measures across on-premises and cloud environments. Additionally, the lens recommends strategies for optimizing costs. This includes cost attribution through tagging, monitoring and managing Outposts capacity, optimizing workload placement, and managing data lifecycle to reduce storage costs.

Finally, the lens emphasizes the importance of automating processes to optimize DRHC workloads. This involves using AWS services and tools for automation and infrastructure as code, as well as establishing feedback loops to adapt to changing data residency requirements.

By applying the principles and best practices in this lens, organizations can seamlessly integrate on-premises and cloud resources while maintaining compliance. This unlocks the full benefits of hybrid cloud computing.

Document revisions

Change	Description	Date
Initial release	Initial release of the Data Residency with Hybrid Cloud Services Lens.	April 3, 2025

Contributors

The following individuals and organizations contributed to this document:

- Abeer Naffa, Senior Solutions Architect, Amazon Web Services
- Brian Daugherty, Principal Solutions Architect, Amazon Web Services
- Chris Gisseler, Enterprise Support Lead, Amazon Web Services
- David Filiatrault, Principal Cloud Security Architect, AWS Professional Services
- Dolly Akiki, Senior Solutions Architect, Amazon Web Services
- Enrico Liguori, Networking Solutions Architect , Amazon Web Services
- Harsha Sanku, Senior Solutions Architect, Amazon Web Services
- Ina Rademacher, Senior Enterprise Support Manager, Amazon Web Services
- Matt Price, Enterprise Support Lead, Amazon Web Services
- Sedji Gaouaou, Senior Solutions Architect, Amazon Web Services
- Tareq Rajabi, Senior Solutions Architect, Amazon Web Services
- Tipu Qureshi, Senior Principal Engineer, Support, Amazon Web Services
- Bruce Ross, Well-Architected Lens Leader, Senior Solutions Architect, Amazon Web Services
- Bruce Ross, Lens Lead Solutions Architect Well-Architected, Amazon Web Services
- Stewart Matzek, Sr. Technical Writer Well-Architected, Amazon Web Services
- Madhuri Srinivasan, Sr. Technical Writer Well-Architected, Amazon Web Services

Subject matter expert (SME) reviewers

- Angelo Malatacca, Partner Solutions Architect, Amazon Web Services
- Eric Vasquez, Senior Solutions Architect, Amazon Web Services
- Kate Sposato, Senior Solutions Architect, Amazon Web Services
- Leonardo Solano, Principal Hybrid Cloud Solutions Architect, Amazon Web Services
- Mark Nguyen, Principal Solutions Architect, Amazon Web Services
- Swapnonil Mukherjee, Senior Partner Solutions Architect, Amazon Web Services

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.