Service Name

AWS PrivateLink

Service Overview

AWS PrivateLink is a highly available, scalable technology that enables private connectivity between VPCs, AWS services, and on-premises networks without using the public internet. It creates secure connections using private IP addresses within Amazon's network infrastructure, eliminating the need for internet gateways, NAT devices, public IP addresses, Direct Connect connections, or VPN connections. Users control specific API endpoints, sites, services, and resources that are reachable from their VPC, significantly reducing attack surface and enhancing security. Traffic remains entirely within the AWS network backbone, providing improved performance, security, and simplified network architecture for accessing AWS services, third-party SaaS applications, and custom services across VPCs and accounts.

Key Use Cases

- SaaS Application Access: Privately access third-party SaaS applications from VPCs without public internet exposure or complex network configurations
- Shared Services Architecture: Enable common services in shared VPCs to be consumed by workloads in separate VPCs without VPC peering limitations
- Hybrid Cloud Integration: Extend services to on-premises resources by connecting endpoint services to data center resources via Network Load Balancers
- Microservices Communication: Facilitate secure inter-service communication where teams create endpoint services for their microservices and allow controlled access by other teams
- Multi-Region Service Access: Provide cross-region access to services while maintaining private communication over Amazon's network infrastructure

Features

- **Interface VPC Endpoints**: Elastic network interfaces that provide private connectivity to AWS services, third-party services, and VPC endpoint services
- **VPC Endpoint Services**: Allow service providers to expose their applications behind Network Load Balancers for private consumption by other AWS customers
- **Resource VPC Endpoints**: Direct private connectivity to specific VPC resources like databases and clusters without requiring load balancing
- **Cross-Region Connectivity**: Extends private connectivity to AWS services across regions without internet or inter-region peering
- **Security Group Integration**: Apply VPC security groups to control access at the network interface level for granular security policies

- **Endpoint Policies**: Fine-grained access control policies to restrict access to specific AWS principals, actions, and resources
- **DNS Resolution**: Private DNS names for endpoints enabling seamless application integration without code changes
- **High Availability**: Horizontally scalable and redundant across multiple Availability Zones for fault tolerance

Value Proposition

AWS PrivateLink offers superior security by keeping all traffic within Amazon's private network, eliminating internet exposure and reducing attack surface. It provides significant cost savings by avoiding NAT gateway charges and internet data transfer costs, with potential reductions of up to 92% compared to traditional internet-based connectivity:

- The service simplifies network architecture by removing the need for complex VPC peering, internet gateways, or VPN connections while supporting overlapping IP address ranges between VPCs
- PrivateLink delivers consistent low-latency performance through Amazon's high-speed backbone network and scales automatically to handle millions of requests per second
- It enables compliance with strict data residency and security requirements while facilitating seamless cloud migration and hybrid architectures

Service Integration

AWS PrivateLink integrates with over 100 AWS services including Amazon S3, DynamoDB, Lambda, EC2, RDS, CloudWatch, IAM, and many others through interface endpoints. It works seamlessly with AWS Direct Connect and Site-to-Site VPN for hybrid connectivity, enabling on-premises access to PrivateLink endpoints:

- The service integrates with Amazon VPC security groups, NACLs, and route tables for comprehensive network security
- It supports AWS CloudFormation for infrastructure-as-code deployments and integrates with AWS CloudTrail for audit logging
- PrivateLink works with Elastic Load Balancing (specifically Network Load Balancers) to publish services and connects with Amazon VPC Lattice for service mesh architectures
- It also integrates with AWS Resource Access Manager for cross-account resource sharing

Onboarding and Offboarding

Customers begin by creating VPC endpoints through the AWS Management Console, AWS CLI, or CloudFormation templates to connect to desired services. For consuming AWS

services, select the service from available options and specify target subnets and security groups:

- For accessing custom services, coordinate with service providers to obtain endpoint service names and ensure proper allowlisting
- Service providers create endpoint services by setting up Network Load Balancers and configuring VPC endpoint services with appropriate acceptance settings
- The process includes configuring DNS settings, security groups, and endpoint policies for access control
- Testing connectivity and monitoring through CloudWatch metrics ensures proper functionality
- Documentation provides step-by-step tutorials for common scenarios including connecting to CloudWatch, S3, and custom applications

Getting Started Guide: https://docs.aws.amazon.com/vpc/latest/privatelink/getting-started.html

Data Removal

Offboarding involves deleting VPC endpoints through the AWS Management Console, CLI, or API, which immediately terminates private connectivity. Service providers must delete endpoint services and associated Network Load Balancer configurations. All endpoint policies, security group rules, and DNS configurations should be cleaned up. VPC endpoint connections are automatically removed when endpoints are deleted, and no residual data remains within the PrivateLink service itself as it only facilitates connectivity.

Backup/Restore and Disaster Recovery

AWS PrivateLink itself does not provide backup or disaster recovery capabilities as it is a networking service that facilitates connectivity. However, it enables private access to AWS Backup and AWS Elastic Disaster Recovery services, allowing customers to implement backup and DR strategies while maintaining private network connectivity. The service supports multi-AZ deployments for high availability and can be configured across regions for disaster recovery architectures.

Backup Capabilities

PrivateLink does not have inherent backup capabilities as it is a networking connectivity service. Configuration settings for VPC endpoints and endpoint services can be captured through AWS Config and replicated via CloudFormation templates. The service enables private connectivity to AWS Backup service, allowing customers to implement backup strategies while maintaining network isolation and security.

Disaster Recovery

PrivateLink supports disaster recovery by enabling cross-region connectivity and multi-AZ deployments for high availability. While not directly integrated with AWS Elastic Disaster Recovery, it provides the private network connectivity required for DR scenarios. Customers can configure PrivateLink endpoints in multiple regions and leverage the service's inherent redundancy across Availability Zones for resilient architectures.

Recovery Objectives

PrivateLink supports RPO and RTO objectives by providing highly available, low-latency connectivity with automatic scaling and redundancy across multiple Availability Zones. The service enables rapid failover scenarios through DNS-based routing and supports cross-region connectivity for disaster recovery. By eliminating internet dependencies and providing consistent private network performance, it helps maintain predictable recovery timeframes and minimizes data exposure during recovery operations.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-limits-endpoints.html

FAQ: https://aws.amazon.com/privatelink/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html

User Guide: https://docs.aws.amazon.com/vpc/latest/privatelink/getting-started.html

API Reference: https://docs.aws.amazon.com/AWSEC2/latest/APIReference/operation-list-privatelink.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/privatelink/pricing/

Cost Optimization

PrivateLink offers significant cost optimization by eliminating NAT gateway charges and reducing internet data transfer costs, with potential savings up to 92% compared to traditional internet-based connectivity. Customers can optimize costs by consolidating multiple service connections through single VPC endpoints where possible:

- Resource endpoints provide cost-effective access to databases and specific resources without requiring load balancers
- Cross-region connectivity should be evaluated against data transfer costs versus security and compliance benefits
- Proper endpoint policy configuration prevents unnecessary data processing charges by restricting access to only required resources and principals

Savings Considerations

Primary cost savings include elimination of NAT gateway hourly charges and internet data transfer fees, particularly significant for high-volume data processing workloads. PrivateLink's per-GB processing fees are often lower than equivalent internet data transfer and NAT gateway costs:

- Organizations can reduce network infrastructure complexity and associated management costs
- Cross-region private connectivity eliminates the need for expensive dedicated connections while maintaining security
- For SaaS integrations, private connectivity reduces bandwidth costs and improves predictable billing
- Shared endpoint services can distribute costs across multiple consumers, making enterprise services more cost-effective