VPC Endpoints

## Service Overview

*A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network. Endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic*

## Use cases / Considerations

[***Interface VPC endpoints (AWS PrivateLink***](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html)*) - An interface VPC endpoint (interface endpoint) allows you to connect to services powered by AWS PrivateLink. These services include some AWS services, services hosted by other AWS customers and Partners in their own VPCs (referred to as endpoint services), and supported AWS Marketplace Partner services. The owner of the service is the service provider, and you, as the principal creating the interface endpoint, are the service consumer.*

*A* [***Gateway Load Balancer endpoint***](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway-load-balancer.html) *enables you to intercept traffic and route it to a service that you've configured using*[*Gateway Load Balancers*](https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/)*, for example, for security inspection. The owner of the service is the service provider, and you, as the principal creating the Gateway Load Balancer endpoint, are the service consumer.*

[**VPC endpoint services**](https://docs.aws.amazon.com/vpc/latest/privatelink/endpoint-service.html). *You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an endpoint service). Other AWS principals can create a connection from their VPC to your endpoint service using an*[*interface VPC endpoint*](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html)*or a*[*Gateway Load Balancer endpoint*](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway-load-balancer.html)*, depending on the type of service. You are the service provider, and the AWS principals that create connections to your service are service consumers.*

[***Gateway Endpoints***](https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-gateway.html) *Currently Gateway Endpoints Support • Amazon S3 • DynamoD*

## Governance

## Cautions

* *Gateway VPC endpoints per Region – 20. You cannot have more than 255 gateway endpoints per VPC.*
* *Interface and Gateway Load Balancer endpoints per VPC - 50. This is the combined quota for the maximum number of interface endpoints and Gateway Load Balancer endpoints in a VPC. To increase this quota, contact AWS Support.*
* *VPC endpoint policy size - 20,480 characters (including white space). This quota cannot be increased.*
* *You cannot use an AWS prefix list ID in an outbound rule in a network ACL to allow or deny outbound traffic to the service specified in an endpoint. If your network ACL rules restrict traffic, you must specify the CIDR block (IP address range) for the service instead. You can, however, use an AWS prefix list ID in an outbound security group rule. For more information, see*[*Security groups*](https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html#vpc-endpoints-security-groups)*.*
* *Endpoints are supported within the same Region only. You cannot create an endpoint between a VPC and a service in a different Region.*
* *Endpoints support IPv4 traffic only.*
* *You cannot transfer an endpoint from one VPC to another, or from one service to another.*
* *You have a quota on the number of endpoints you can create per VPC. For more information, see*[*AWS PrivateLink quotas*](https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-limits-endpoints.html)*.*
* *Endpoint connections cannot be extended out of a VPC. Resources on the other side of a VPN connection, VPC peering connection, transit gateway, AWS Direct Connect connection, or ClassicLink connection in your VPC cannot use the endpoint to communicate with resources in the endpoint service.*

## Pricing considerations

*https://aws.amazon.com/vpc/pricing/*

## More details

[AWS PrivateLink and VPC endpoints - Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/privatelink/endpoint-services-overview.html)