



Connecting to Salesforce Hyperforce by using AWS Direct Connect with
Megaport

AWS Prescriptive Guidance



AWS Prescriptive Guidance: Connecting to Salesforce Hyperforce by using AWS Direct Connect with Megaport

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

Introduction	1
Solution components	2
Direct Connect	2
Hosted connection	2
Public virtual interface	2
Salesforce	3
Hyperforce	3
Salesforce Express Connect (SEC)	3
Megaport	4
Megaport Port	4
Megaport Virtual Edge (MVE)	4
Megaport Cloud Router (MCR)	5
Use cases	6
Key considerations	6
Use case: branch offices	6
Use case: VPN-connected workforce	10
Use case: multicloud virtual desktop infrastructure	13
Pricing	16
Resources	17
AWS documentation	17
Megaport documentation	17
Salesforce documentation	17
Document history	18

Connecting to Salesforce Hyperforce by using AWS Direct Connect with Megaport

Bennett Borofka and Kranthi Pullagurla, Amazon Web Services

ABHIRAM GAJJALA, Salesforce

Kevin Dresser, Megaport

Many AWS users have hybrid workloads that span the cloud and on-premises locations. To adequately provide private, reliable network connectivity between these environments, you can choose from a variety of options to ensure business value and cost optimization.

Users who have branch offices, enterprise data centers, and a VPN-connected workforce have unique requirements for enabling access to Salesforce Hyperforce running on AWS.

This guide describes use cases to help Salesforce Hyperforce and AWS users configure private, reliable connectivity to Hyperforce by using Direct Connect and the Megaport software-defined networking (SDN) platform.

[Salesforce Hyperforce](#) is a next-generation Salesforce infrastructure architecture that is built to run on cloud providers such as AWS. You can use Hyperforce to benefit from its enhanced compliance, security, agility, scalability, and privacy. Hyperforce provides multiple options for establishing private, reliable network connectivity to Hyperforce from your on-premises location, other AWS accounts, or other cloud providers.

[Direct Connect](#) is a cloud service that bypasses the internet to link branch offices and data centers to AWS. It offers the shortest path from your location to Hyperforce, where network traffic remains on the AWS backbone network and never traverses the public internet.

[Megaport](#) is an SDN platform and Direct Connect partner. Megaport provides a variety of network connectivity options for users who want fast, reliable connectivity to AWS and other cloud providers.

This guide is for practitioners, architects, administrators, and operators of networking, cloud infrastructure, and Salesforce Hyperforce.

Solution components

Direct Connect requires you to either create your own [dedicated connection](#) to AWS, or work with an Direct Connect Partner to create a [hosted connection](#). This article provides guidance for using Megaport as an Direct Connect Partner to facilitate hybrid and multiple use cases for connecting to Salesforce Hyperforce.

Direct Connect

Direct Connect establishes a private, dedicated network connection between on-premises data centers and AWS. This direct link helps organizations bypass the public internet and provides reliable and private communication with AWS resources.

Although Hyperforce runs on AWS infrastructure, using Direct Connect to access it requires you to manage an AWS account for billing and configuration of the connection. Using Direct Connect to connect to the Salesforce-managed Hyperforce AWS account isn't supported.

Hosted connection

A [hosted connection](#) is a physical Ethernet connection that an Direct Connect Partner provisions on behalf of a user. The use cases and architectures covered in this guide use a hosted connection with the Direct Connect Partner, Megaport. Hosted connections offer bandwidth ranges between 50 Mbps to 25 Gbps in multiple increments, whereas dedicated connections are provided in 1 Gbps, 10 Gbps, and 100 Gbps capacities. For more information about Direct Connect bandwidth and costs, see [Direct Connect pricing](#).

Public virtual interface

The Hyperforce architecture requires access to the public IP address space of AWS resources from on-premises and multicloud locations. A public virtual interface (VIF) is used to connect your remote location to public AWS services and public IPs deployed on AWS. Using a private VIF to access Hyperforce is not supported.

Notes:

- Using a public VIF requires the use of unique public IPv4 addresses. You will need to provide your own IPv4 CIDR or request a /31 CIDR from [AWS Support](#). For more information, see the [prerequisites for virtual interfaces](#) in the Direct Connect documentation.

- Using a public VIF to connect to AWS from your on-premises or multicloud environment changes the way traffic is routed from AWS public prefixes to your users. We recommend that you use a prefix filter (route map) to make sure that the accepted Amazon prefixes are limited to the Hyperforce infrastructure and any other necessary AWS resources. For more information, review [public virtual interface prefix advertisement rules](#) in the Direct Connect documentation.
- The prefixes that are advertised by Direct Connect must not be advertised beyond the network boundaries of your connection. For example, these prefixes must not be included in any public internet routing table. For information, review [public virtual interface routing policies](#) in the Direct Connect documentation.

Salesforce

Salesforce is a customer relationship management (CRM) platform that's designed to help you sell, service, market, analyze, and connect with your customers.

Hyperforce

[Salesforce Hyperforce](#) is a next-generation Salesforce infrastructure architecture that's built for the public cloud. It provides enhanced scalability, flexibility, and agility by using the AWS infrastructure. It is the fastest and simplest way to run Salesforce on public cloud infrastructure.

Salesforce Express Connect (SEC)

[Salesforce Express Connect \(SEC\)](#) enables private, reliable connectivity from users to Salesforce-operated data centers. Ensuring private connectivity to Hyperforce currently requires a SEC connection in conjunction with Direct Connect.

Notes:

- A limited number of Salesforce services still run in Salesforce-managed infrastructure. To maintain connectivity to all services in Salesforce-managed infrastructure and Hyperforce, users who require private network access to Salesforce must continue to run SEC along with Direct Connect.
- Salesforce and AWS do not sell SEC. If you require private network connectivity to Salesforce-managed infrastructure, you will need a SEC connection. This article covers establishing a new [SEC connection to Salesforce by using Megaport](#).

- SEC is not used for any data migration between Salesforce-managed infrastructure and Hyperforce. If you are migrating to Hyperforce, Salesforce facilitates data migrations in your organization on a private backbone. SEC is necessary for ongoing, private connectivity to Salesforce by users.

Megaport

[Megaport](#) simplifies and accelerates hybrid cloud connectivity to AWS Regions in a scalable, private, and on-demand manner. Megaport acts as a facilitator in this connectivity ecosystem, and offers SDN solutions to simplify and optimize the process of connecting to cloud services, including the AWS Cloud. Megaport connections are called *virtual cross connects (VXCs)*, which are Layer 2 Ethernet circuits that provide private, flexible, and on-demand connectivity between any of the locations on the Megaport network. To access the Megaport network, you must first create a Port, Megaport Virtual Edge (MVE), or Megaport Cloud Router (MCR), which are covered in the next sections.

Megaport Port

[Megaport Port](#) is a high-speed Ethernet interface that creates a network-to-network interface (NNI) between your network and the Megaport network. It is configured as an 802.1Q virtual local area network (VLAN) trunk to support up to 100 VXCs, each presented as a unique VLAN. The Port provisioning process enables the Megaport interface and generates a Letter of Authorization (LOA) with instructions for the data center operator to establish the physical cross connect from your equipment to the new Port.

Note

Your network device requires either 10 or 100 Gbps interfaces with 10GBASE-LR (duplex on single-mode optical fiber [SMOF]) or 100G-LR4 (duplex on SMOF) optical transceivers.

Megaport Virtual Edge (MVE)

[Megaport Virtual Edge \(MVE\)](#) is a network functions virtualization (NFV) platform that provides virtual infrastructure for network services at the edge of Megaport's global SDN. You can use MVE to deploy a virtual network stack (or point of presence) without any physical data center presence or hardware. MVE is available in 27 metro regions across the globe and is aligned closely with

Direct Connect peering locations (NNIs). MVE supports third-party VNF appliances from vendors such as Aruba, Cisco, Fortinet, Palo Alto Networks, Versa Networks, and VMware.

 Note

MegaPort doesn't sell third-party licenses and requires that you use a Bring Your Own License (BYOL) model.

MegaPort Cloud Router (MCR)

[MegaPort Cloud Router \(MCR\)](#) is a managed virtual router service that enables direct Layer 2 and Layer 3 networking between endpoints on the MegaPort network, including other cloud providers. The MCR can be deployed as a standalone service to route traffic between different cloud environments without requiring you to have a physical presence in that data center. It can also be connected to your Port to route pertinent traffic back to a physical location. The MCR is managed through the MegaPort Portal to configure both static and dynamic Border Gateway Protocol (BGP) routing functions, including Bidirectional Forwarding Detection (BFD), Multi-Exit Discriminator (MED), Autonomous System Number (ASN), and NAT. For more information, see [Configuring BGP Advanced Settings](#) in the MegaPort documentation.

Use cases

The use cases in the following sections provide examples for how you can enable your users to have private, reliable connectivity to Hyperforce.

- [Branch offices](#)
- [VPN-connected workforce](#)
- [Multicloud virtual desktop infrastructure](#)

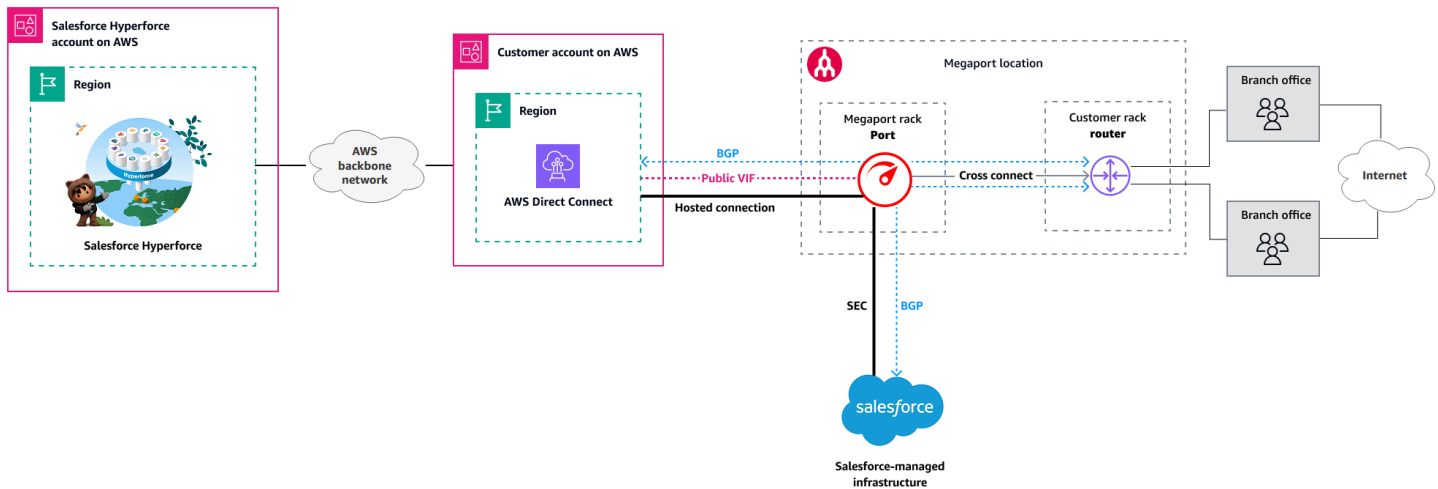
Key considerations

- Hyperforce can be used for both private and public connectivity.
- You can use any combination of the use cases that are described.
- Both new Salesforce users and users who are migrating from Salesforce-managed data center infrastructure can use Hyperforce. The use cases cover both scenarios.
- Migration of data from a Salesforce-managed data center instance to Hyperforce is managed by Salesforce behind the scenes, and doesn't use the network architecture described in these use cases.
- Some aspects of user application logins to Hyperforce still require network connectivity to Salesforce-managed data centers. For this reason, if you require fully private connectivity, you must use SEC with Direct Connect.

Use case: branch offices

This use case covers a scenario where you have a physical router in one Megaport location, and you use it as an on-ramp to Direct Connect. In this scenario, you also have one or more branch offices connected to this location through private circuits.

Using Megaport Port with Direct Connect gives your users who work in branch offices private connectivity to Salesforce Hyperforce. The branch offices consist of a single office or a cluster of offices inter-networked across a metropolitan area network (MAN). The offices on-ramp to Direct Connect by using a Megaport location. The following diagram shows the architecture for this use case.



Requirements

- Your users access Salesforce over private network connections.
- Your users work primarily from branch offices that have private connectivity to a Megaport-enabled location.
- You own an AWS account to manage the Direct Connect hosted connection with Megaport.
- You have a physical router that's deployed at a Megaport location that facilitates a cross connect with Megaport's router.

Configuring Megaport Port with VXC

The Megaport Port is configured with a VXC and provides the private Layer 2 network segment to AWS. The Direct Connect connection is provisioned as a hosted connection and attached to a public VIF. For step-by-step instructions, see the following Megaport documentation:

- [Creating a Port](#)
- [Configuring and Maintaining AWS Hosted Connections](#)

Configuring your network devices

Network devices that are deployed at the Megaport location within your rack are configured to support the connectivity to the Hyperforce instances through Direct Connect. These devices might include a router, switch, firewall, or a combined network stack of multiple devices. The vendor and

model types are optional, depending on your requirements. We recommend that you work with your network administrator to configure these devices.

The device that is used to establish the physical cross connect to the Megaport rack must support 802.1Q VLAN tagging to establish Layer 2 adjacency. Layer 3 adjacency is then established between your router and the AWS public VIF by using BGP.

Notes:

- The BGP prefixes advertised from your router to AWS are configured in the AWS Management Console when you create the public VIF.
- The prefixes advertised by Direct Connect must not be advertised beyond the network boundaries of your connection. For example, these prefixes must not be included in any public internet routing table. For more information, see [Public virtual interface routing policies](#) in the Direct Connect documentation.

Configuring Direct Connect

Accept a hosted connection

In your AWS account, accept the VXC created previously as a hosted connection. For instructions, see the [Direct Connect documentation](#).

Create a public VIF

In your account, provision a public VIF under the connection you accepted from Megaport. Before you create this VIF, you need to obtain the following:

- The BGP ASN of the router that's deployed to the Megaport location.
- Public IPv4 addresses for peering (typically /31 CIDR). You can own these or request them from AWS Support. For more information, see *Peer IP addresses* in the section [Prerequisites for virtual interfaces](#) in the Direct Connect documentation.

To create a public VIF, follow the steps in the [Direct Connect documentation](#).

After you create the public VIF, you need to make sure that the BGP authentication key matches both ends of the BGP peer for the peering state to become available.

Note

Using a public VIF to connect to AWS from your on-premises environment changes the way traffic is routed from AWS public prefixes to your users. We recommend that you use a prefix filter (route map) to make sure that the accepted Amazon prefixes are limited to the Hyperforce infrastructure and any other necessary AWS resources. For more information, see [Public virtual interface prefix advertisement rules](#) in the Direct Connect documentation.

Configuring Megaport Port with SEC

You can also provision the Megaport Port with a SEC VXC, which provides the Layer 2 networking elements for the private connection to Salesforce-managed data centers. SEC lets you access Salesforce applications and services directly with a private, dedicated connection. SEC is delivered as a Layer 3 routed service. You access Salesforce services by using public IPs and must run BGP to receive Salesforce routes. Megaport allocates a /31 public IP range for each Salesforce peering.

Note

SEC offers a choice between two IP addressing options:

- Source NAT your LAN traffic to use the /31 public IP space provided by Megaport.
- Advertise your own public IP address space to Salesforce. (Salesforce won't accept [RFC1918](#) blocks of IP address space.)

For step-by-step instructions, see [Connecting to Salesforce Express Connect](#) in the Megaport documentation.

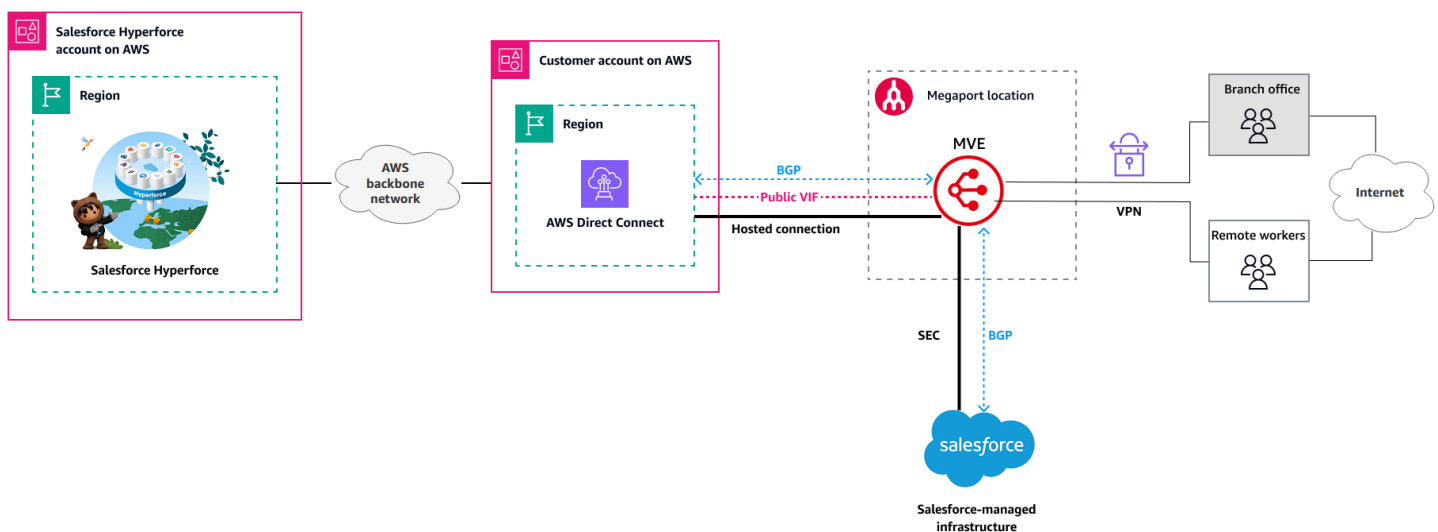
Configuring Salesforce Hyperforce

To enable inbound connections from your corporate network into Salesforce, you need to configure inbound access to Hyperforce as a security measure. To [allow the required domains](#), follow the instructions in [Allow Domains for a Salesforce Console in Salesforce Classic](#) in the Salesforce documentation. Do not use IP addresses.

Use case: VPN-connected workforce

This use case covers a scenario where you use a virtual VPN concentrator at a Megaport location as an on-ramp to Direct Connect. In this scenario, you have remote branch offices or workers with site-to-site VPNs that connect to the VPN concentrator.

Using Megaport MVE with a third-party virtual firewall and Direct Connect gives your remote workers private connectivity to Salesforce Hyperforce. The remote workers connect to the VPN concentrator from an internet-connected router at a branch office or from a VPN client that is running on their device. The remote workers then on-ramp to Direct Connect by using a Megaport location.



Requirements

- Your remote workers access Salesforce over private network connections.
- Your remote workers or users at branch offices have site-to-site VPN connectivity to a Megaport-enabled location over the internet.
- You own an AWS account to manage the Direct Connect hosted connection with Megaport.

Configuring Megaport MVE with VXC

The Megaport MVE that's configured with a VXC provides the private Layer 2 network segment to AWS. The MVE is a virtual solution and doesn't require a Port. However, you must specify the third-party virtual network appliance to be deployed. The VXC deployment process and functionality are

the same, whether you use a Port, MVE, or MCR. Direct Connect should be provisioned as a hosted connection and attached to a public VIF.

For an overview and step-by-step instructions, see the following Megaport documentation:

- [Introducing MVE](#)
- [Configuring and Maintaining AWS Hosted Connections](#)

Configuring VNF appliances

MVE supports third-party virtual network function (VNF) appliances from vendors such as Aruba, Cisco, Fortinet, Palo Alto Networks, Versa Networks, and VMware. You can choose a vendor to handle routing, security, and the SSL VPN functions of the MVE. For a full list of MVE integration partners, see the [Megaport documentation](#).

For example, this use case describes a high-level architecture where Megaport MVE supports VPN/SD-WAN connections from regional branch offices and remote users who have an SSL VPN connection. This MVE peers with AWS and routes these connections privately to Hyperforce through Direct Connect.

The key elements of this architecture include:

- Route filters to limit AWS prefixes for relevant Hyperforce instances
- SSL VPN policies based on Hyperforce fully qualified domain name (FQDN) and IP address ranges
- NAT policy for Hyperforce users behind a single public IP address that faces AWS

Configuring route filters

When the VNF has established BGP peering with the AWS public VIF, the route table should populate with prefixes for all AWS public services and Hyperforce. You can apply route filtering by using IP lists or BGP community tags. We recommend that you configure a route map of prefixes that include a range of Hyperforce instances in an AWS Region.

Notes:

- The BGP prefixes advertised from your router to AWS are configured in the AWS Management Console when you create the public VIF.

- The prefixes advertised by Direct Connect must not be advertised beyond the network boundaries of your connection. For example, these prefixes must not be included in any public internet routing table. For more information, see [Public virtual interface routing policies](#) in the Direct Connect documentation.

Configuring Direct Connect

Accept a hosted connection

In your AWS account, accept the VXC created previously as a hosted connection. For instructions, see the [Direct Connect documentation](#).

Create a public VIF

In your account, provision a public VIF under the connection you accepted from Megaport. Before you create this VIF, you need to obtain the following:

- The BGP ASN of the VNF appliance.
- Public IPv4 addresses for peering (typically /31 CIDR). You can own these or request them from Support. For more information, see *Peer IP addresses* in the section [Prerequisites for virtual interfaces](#) in the Direct Connect documentation.

To create a public VIF, follow the steps in the [Direct Connect documentation](#).

After you create the public VIF, you need to make sure that the BGP authentication key matches both ends of the BGP peer for the peering state to become available.

Note

Using a public VIF to connect to AWS from your on-premises environment changes the way traffic is routed to your on-premises location from AWS. We recommend that you use a prefix filter (route map) to make sure that the accepted Amazon prefixes are limited to the Hyperforce infrastructure and any other necessary AWS resources. For more information, see [Public virtual interface prefix advertisement rules](#) in the Direct Connect documentation.

Configuring Megaport MVE with SEC

In some cases, Hyperforce login requests are redirected to Salesforce-managed data centers. To keep this traffic on a private network, you can add a Megaport VXC to Salesforce by using SEC. You can configure your VNF security policies with rules by using the Salesforce login FQDN. This is similar to the Direct Connect architecture described earlier in this guide.

For step-by-step instructions, see [Connecting to Salesforce Express Connect](#) in the Megaport documentation.

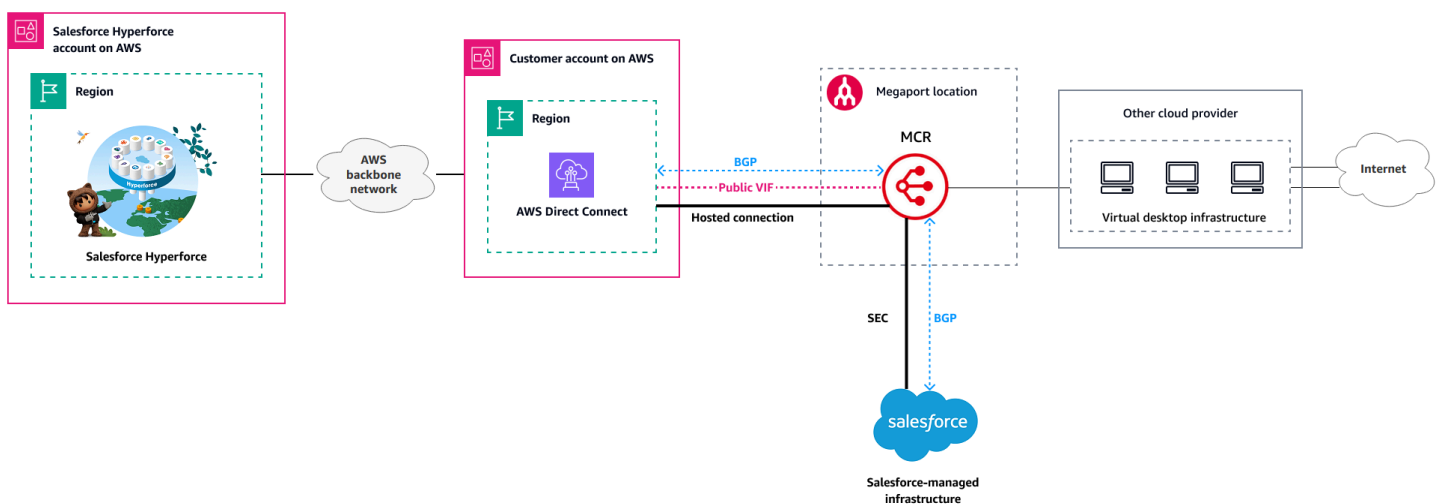
Configuring Salesforce Hyperforce

To enable inbound connections from your corporate network into Salesforce, you need to configure inbound access to Hyperforce as a security measure. To [allow the required domains](#), follow the instructions in [Allow Domains for a Salesforce Console in Salesforce Classic](#) in the Salesforce documentation. Do not use IP addresses.

Use case: multicloud virtual desktop infrastructure

This use case covers a scenario where you have a virtual desktop infrastructure (VDI) running in another cloud provider that has a private connection to Megaport and is used as an on-ramp to Direct Connect.

Using Megaport MCR with Direct Connect gives your VDI users private connectivity to Salesforce Hyperforce. VDI users use their desktops for their daily work, and the VDI provides an on-ramp to Direct Connect by using a Megaport location.



Requirements

- Users access Salesforce over private network connections.
- Users use a VDI.
- The VDI runs in an alternate cloud provider and has a private connection established to Megaport.
- You own an AWS account to manage the Direct Connect hosted connection with Megaport.

Configuring Megaport MCR with VXC

For step-by-step instructions, see the following Megaport documentation:

- [Creating an MCR](#)
- [Creating MCR Connections to AWS](#)

Notes:

- The BGP prefixes advertised from your router to AWS are configured in the AWS Management Console when you create the public VIF.
- The prefixes advertised by Direct Connect must not be advertised beyond the network boundaries of your connection. For example, these prefixes must not be included in any public internet routing table. For more information, see [Public virtual interface routing policies](#) in the Direct Connect documentation.

Configuring Direct Connect

Accept a hosted connection

In your AWS account, accept the VXC created previously as a hosted connection. For instructions, see the [Direct Connect documentation](#).

Create a public VIF

In your account, provision a public VIF under the connection you accepted from Megaport. Before you create this VIF, you need to obtain the following:

- The BGP ASN of the MCR.

- Public IPv4 addresses for peering (typically /31 CIDR). You can own these or request them from Support. For more information, see *Peer IP addresses* in the section [Prerequisites for virtual interfaces](#) in the Direct Connect documentation.

To create a public VIF, follow the steps in the [Direct Connect documentation](#).

After you create the public VIF, you need to make sure that the BGP authentication key matches both ends of the BGP peer for the peering state to become available.

 Note

Using a public VIF to connect to AWS from your on-premises or multicloud environment changes the way traffic is routed from AWS public prefixes to your users. We recommend that you use a prefix filter (route map) to make sure that the accepted Amazon prefixes are limited to the Hyperforce infrastructure and any other necessary AWS resources. For more information, see [Public virtual interface prefix advertisement rules](#) in the Direct Connect documentation.

Configuring Megaport MCR with SEC

For step-by-step instructions, see [Creating MCR Connections to Salesforce Express Connect](#) in the Megaport documentation.

Configure Salesforce Hyperforce

To enable inbound connections from your corporate network into Salesforce, you need to configure inbound access to Hyperforce as a security measure. To [allow the required domains](#), follow the instructions in [Allow Domains for a Salesforce Console in Salesforce Classic](#) in the Salesforce documentation. Do not use IP addresses.

Pricing

Cost considerations for the solutions described in this guide depend on various factors, such as scale, consumed bandwidth, selected products, and vendor discounts. When pricing the various components, consider the following:

- Direct Connect – The price varies based on Region, port type, capacity, and data transferred. Use the [AWS Pricing Calculator](#) to estimate your costs.
- Megaport hosted connection to AWS – The price varies depending on product usage and capacity. Megaport Port, MVE, and MCR are available [directly from Megaport](#) or can be procured through [AWS Marketplace](#).
- Megaport SEC – This is available directly through [Megaport](#).
- Salesforce Hyperforce – This is available directly through [Salesforce](#).

Resources

AWS documentation

- [Direct Connect](#)
- [Direct Connect User Guide](#)

Megaport documentation

- [Creating a Port](#)
- [Configuring and Maintaining AWS Hosted Connections](#)
- [Connections Overview](#)
- [MCR Overview](#)
- [Introducing MVE](#)
- [Connecting to Salesforce Express Connect](#)

Salesforce documentation

- [Introducing Hyperforce – General Information & FAQ](#)
- [Allow Domains for a Salesforce Console in Salesforce Classic](#)
- [Allow the Required Domains](#)

Document history

The following table describes significant changes to this guide.

Change	Description	Date
Initial publication	—	August 30, 2024