Configuring a VPN for SaaS on AWS

ScienceLogic Version 11.2.0

Table of Contents

Introduction 1

- SaaS Connectivity 2
- Terminology 2

Configuring a VPN for SaaS on SL1 4

- Prerequisites 5
- Creating Private Connectivity for SaaS in AWS (Required) 5
- Configuring a Site-to-Site VPN (Optional) 7
- Setting Up a Virtual Private Network (VPN) (Optional) 9

Chapter 1

Introduction

Overview

This manual describes how to build a Virtual Private Network (VPN) between a SL1 Software-as-a-Service (SaaS) environment and the customer network, specifically on Amazon Web Services (AWS).

This chapter covers the following topics:

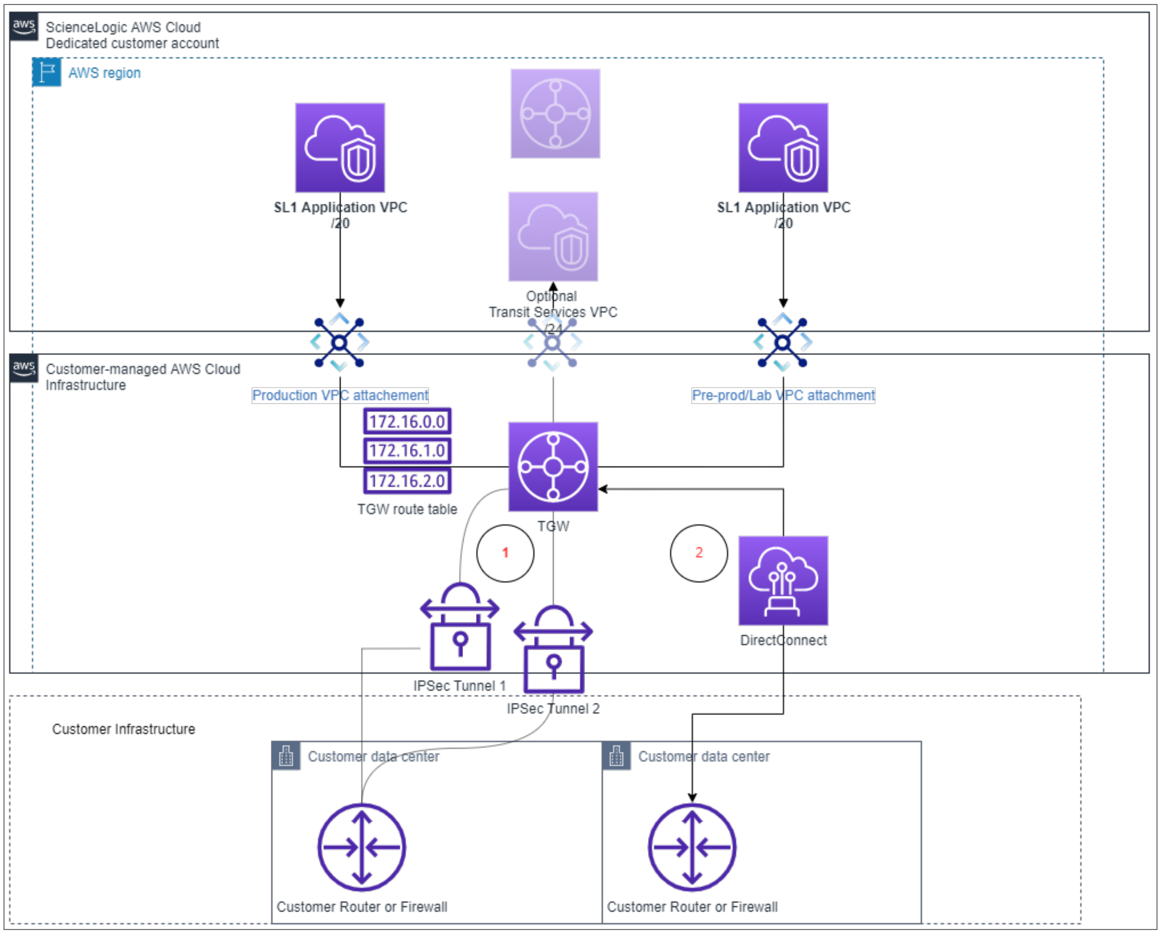
SaaS Connectivity 2

Terminology 2

SaaS Connectivity

SaaS on SL1 is currently a single-tenant application hosted in a dedicated Virtual Private Cloud (VPC). This method provides a direct path for the data engine to connect to and pull data from every Data Collector in your SL1 system. You must have private connectivity from the SL1 VPC to the customer network deployed within a customer-managed AWS Transit Gateway. This Transit Gateway can be connected to the customer's on-premises environment using the following methods:

- An existing or new AWS Site-to-Site IPSec VPN
- An existing AWS Direct Connect connection



Terminology

This section defines some of the common terminology you will encounter when configuring a site-to-site VPN:

- ***VPN connection***. A secure connection between on-premises equipment and AWS VPCs.
- ***VPN tunnel***. An encrypted link where data can pass from the customer network to or from AWS. Each VPN connection includes two VPN tunnels which you can simultaneously use for high availability.

- ***Customer gateway device (CGW)***. A physical device or software application on the customer side of the site-to-site VPN connection.
- ***Transit gateway (TGW)***. A transit hub that can be used to interconnect multiple VPCs and on-premises networks. It also serves as a VPN endpoint for the Amazon side of the site-to-site VPN connection.

Chapter

2

Configuring a VPN for SaaS on SL1

Overview

This chapter describes how to configure your virtual private network (VPN) in Amazon Web Services (AWS).

This chapter covers the following topics:

Prerequisites 5

Creating Private Connectivity for SaaS in AWS (Required) 5

Configuring a Site-to-Site VPN (Optional) 7

Setting Up a Virtual Private Network (VPN) (Optional) 9

Prerequisites

Before you can build a VPN between an SL1 Software-as-a-Service (SaaS) environment and AWS, you must have the following prerequisites:

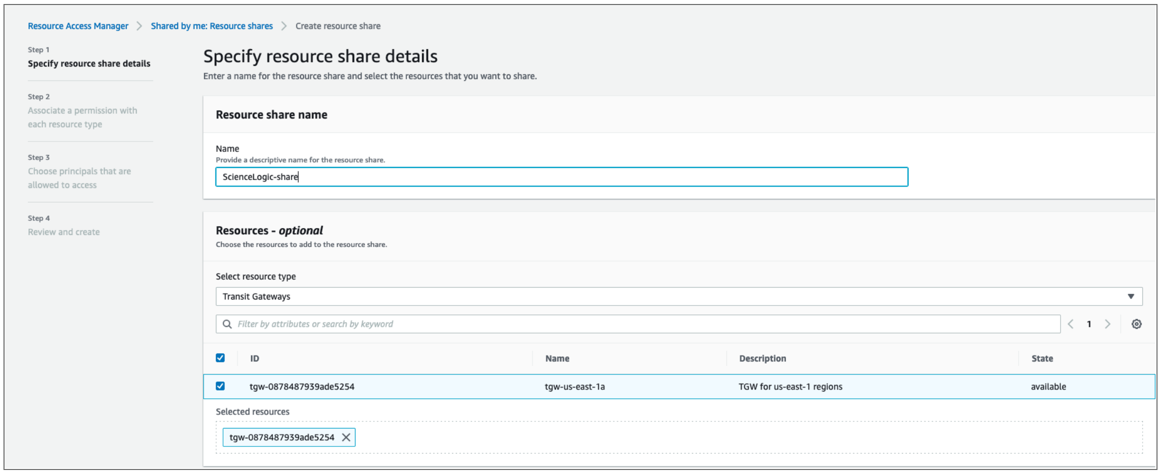
- An existing AWS account with an AWS region
- A connection to data centers in which you are planning to deploy SL1 Data Collectors
- A list of prefixes and subnets in which you are planning to deploy SL1 Data Collectors

Creating Private Connectivity for SaaS in AWS (Required)

To set up a VPN for SaaS on an existing AWS Transit Gateway or AWS Direct Connect account:

NOTE: You might need to enable resource sharing within your AWS Organizations from your AWS management account.

1. Log in to your AWS account as a Cloud Administrator.
2. Select the AWS account on which your AWS Transit Gateway is running.
3. Select the **AWS Management Console** associated with the role allowing administrative access.
4. Select the appropriate AWS region.
5. Navigate to **Resource Access Manager**.
6. Click the **[Create a resource share]** button.
7. In the **Specify resource share details** page, type a name for your resource share in the ***Name*** field.
8. In the ***Select resource type*** drop-down, select *Transit Gateways*. A list of available Transit Gateways will appear. Select the checkbox for the Transit Gateway you want to share with ScienceLogic.



Resource Access Manager > Shared by me: Resource shares > Create resource share

Step 1
Specify resource share details

Step 2
Associate a permission with each resource type

Step 3
Choose principals that are allowed to access

Step 4
Review and create

Specify resource share details

Enter a name for the resource share and select the resources that you want to share.

Resource share name

Name
Provide a descriptive name for the resource share.
ScienceLogic-share

Resources - *optional*
Choose the resources to add to the resource share.

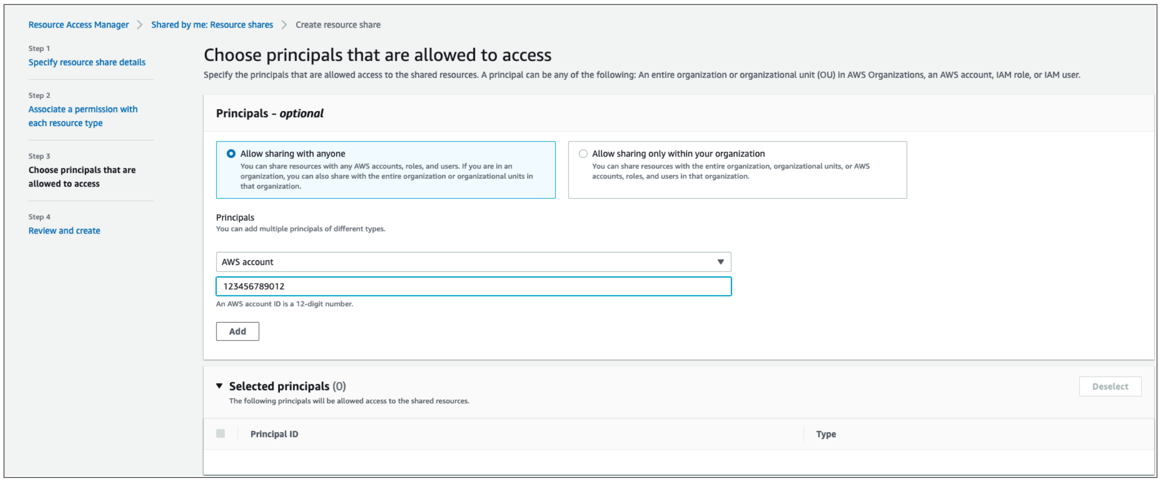
Select resource type
Transit Gateways

Filter by attributes or search by keyword

☑	ID	Name	Description	State
☑	tgw-0878487939ade5254	tgw-us-east-1a	TGW for us-east-1 regions	available

Selected resources
tgw-0878487939ade5254

9. Click **[Next]** to go to the **Associate permissions** page. Permissions are not modified for Transit Gateways, so click **[Next]** again.
10. In the **Choose principals that are allowed to access** page, select ***Allow sharing with anyone***.
11. In the ***Principals*** drop-down, select *AWS account* and type the ScienceLogic-provided 12-digit number in the *AWS account ID* field.
12. Click **[Add]**. Repeat these steps if ScienceLogic has provided multiple account numbers.



Resource Access Manager > Shared by me: Resource shares > Create resource share

Step 1
Specify resource share details

Step 2
Associate a permission with each resource type

Step 3
Choose principals that are allowed to access

Step 4
Review and create

Choose principals that are allowed to access

Specify the principals that are allowed access to the shared resources. A principal can be any of the following: An entire organization or organizational unit (OU) in AWS Organizations, an AWS account, IAM role, or IAM user.

Principals - *optional*

● Allow sharing with anyone
You can share resources with any AWS accounts, roles, and users. If you are in an organization, you can also share with the entire organization or organizational units in that organization.

○ Allow sharing only within your organization
You can share resources with the entire organization, organizational units, or AWS accounts, roles, and users in that organization.

Principals
You can add multiple principals of different types.

AWS account ▼

123456789012

An AWS account ID is a 12-digit number.

Add

▼ **Selected principals** (0)
The following principals will be allowed access to the shared resources.

Deselect

□	Principal ID	Type

13. Click **[Next]** to go to the **Review and create** page. Review the information you entered and then click the **[Create resource share]** button.

When you have completed sharing your AWS resource, ScienceLogic will attach a single virtual private cloud (VPC) or multiple VPCs to your Transit Gateway.

If your Transit Gateway is not configured to automatically accept sharing requests, you must approve the request in your account. To do so:

1. Log in to your AWS account as a Cloud Administrator.
2. Select the AWS account on which your AWS Transit Gateway is running.
3. Select the **AWS Management Console** associated with the Role allowing administrative access.
4. Select the appropriate AWS region.
5. Navigate to **VPC**.
6. In the left navigation panel, click **Transit Gateway Attachments**.
7. In the **Transit gateway attachments** page, you will see a list of your Transit Gateway attachments that are "pending acceptance".
8. Select the checkbox for your Transit Gateway attachment, and then click the **[Actions]** drop-down and select ***Accept***.

Next, you must create the Transit Gateway route table for your VPC attachment. To do so:

1. From your **AWS Management Console**, click **VPC**.
2. In the left navigation panel, click **Transit Gateway Route Tables**.

3. In the **Transit gateway route tables** page, click the **[Create transit gateway route table]** button.
4. Type a name for your Transit Gateway table in the ***Name tag*** field.
5. In the ***Transit gateway ID*** drop-down, select your Transit Gateway.
6. Click the **[Create transit gateway route table]** button.

After creating your Transit Gateway route table, you must associate the route table with your VPC attachment by performing the following steps:

1. From your **AWS Management Console**, click **VPC**.
2. In the left navigation panel, click **Transit Gateway Route Tables**.
3. In the **Transit gateway route tables** page, when the ***State*** of the route table transitions to *Available*, select the **Associations** tab.

NOTE: You might have to refresh the **Transit gateway route tables page** to see the ***State*** change.

4. Click ***Create association***.
5. Select the Transit Gateway attachment you want to associate with your VPC, and then click **[Create association]**.

Finally, to allow traffic from your site-to-site VPN connection to be routed to the ScienceLogic workload VPC, you must add a propagation for the VPC attachment to the network services route table. To do so:

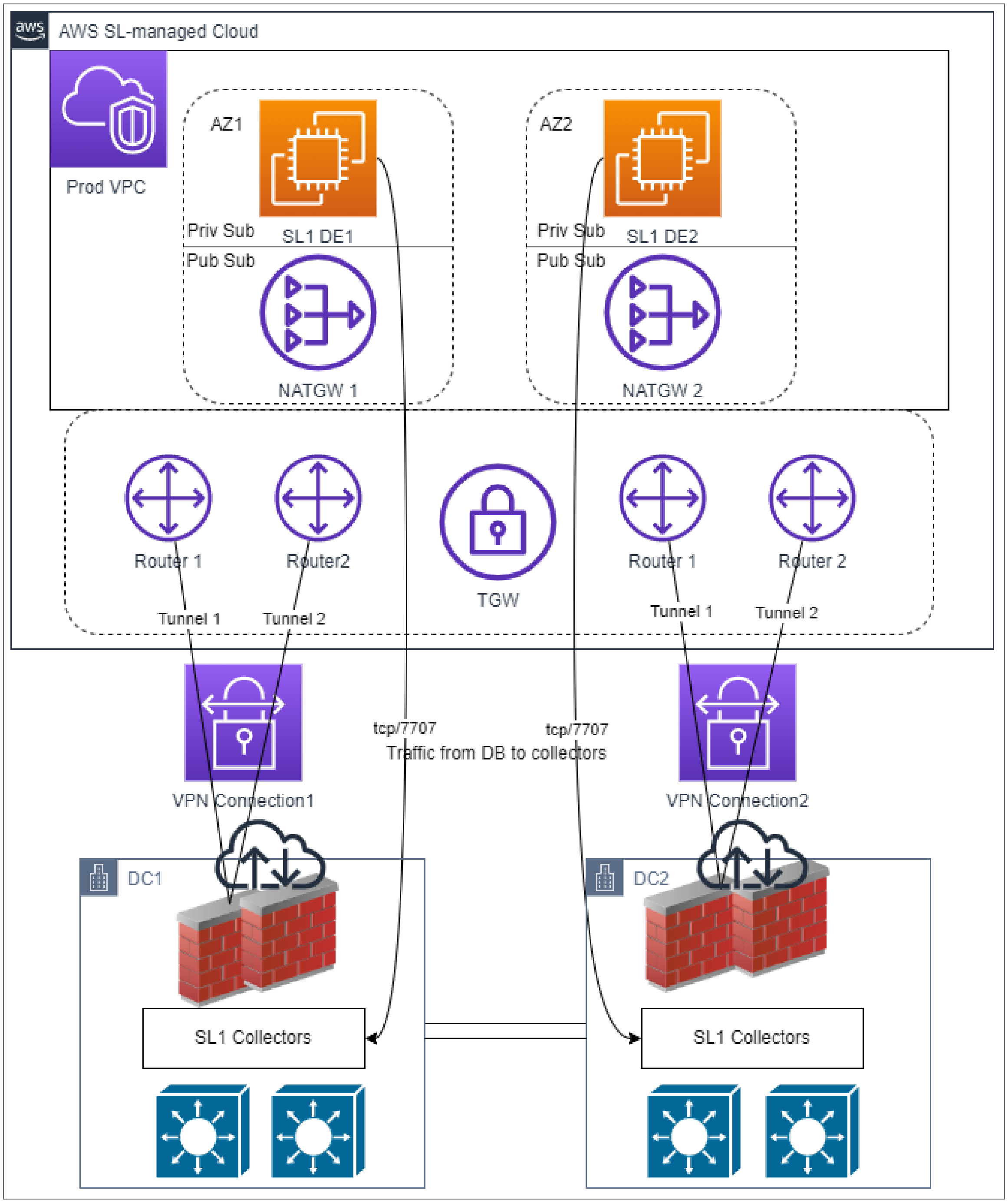
1. From your **AWS Management Console**, click **VPC**.
2. In the left navigation panel, click **Transit Gateway Route Tables**.
3. In the **Transit gateway route tables** page, select the route table you use for routing traffic outside of AWS.
4. Click the ***Actions*** drop-down and select *Create propagation*.
5. Select the Transit Gateway attachment to propagate.

Configuring a Site-to-Site VPN (Optional)

An alternative option for configuring your VPN is to have ScienceLogic work with you to set up a site-to-site VPN, available as a premium service. If you would prefer to set up a VPN on your own, see the ***Setting Up a Virtual Private Network (VPN) (Optional)*** section.

This high-availability VPN option provides the following:

- Two customer gateway devices, or CGWs, in different geolocations, with the VPN tunnel terminating on the same Transit Gateway
- A private autonomous system number (ASN) in the 64512 to 65534 range. The default ASN is 65000.



For select customers, AWS will produce example configuration files to be applied your device(s).

Configuration provided in this method may not satisfy all of your requirements, but may be adjusted as needed.

Setting Up a Virtual Private Network (VPN) (Optional)

If you do not have connectivity from AWS to your on-premises environment, you will need to configure your VPN. If you have opted to have ScienceLogic set up your VPN, see the ***Configuring a Site-to-Site VPN (Optional)*** section.

Before you set up a VPN, you will need to determine the following:

- What is your desired topology—a single VPN connection or multiple VPN connections?
- What type of device are you planning to use for the VPN termination?
- Are there specific internal requirements or standards for setting up your VPN?

At a minimum, you will need to know the public IP address of your Customer Gateway to begin setup.

You will also need to determine the following VPN properties:

- IKE version: IKEv1 vs IKEv2
- Inside tunnel IP addresses
- Minimum encryption algorithms for phase 1 and phase 2
- Minimum integrity algorithms
- Allowed Diffie-Hellman (DH) group numbers
- See the AWS Tunnel options for your Site-to-Site VPN connection documentation for information on optional parameters

You will also need to determine your routing options:

- Static (single VPN only)
- Dynamic (BGP only)

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010