snowflake®   **ENGINEERING BLOG**   **CATEGORIES** ⌄
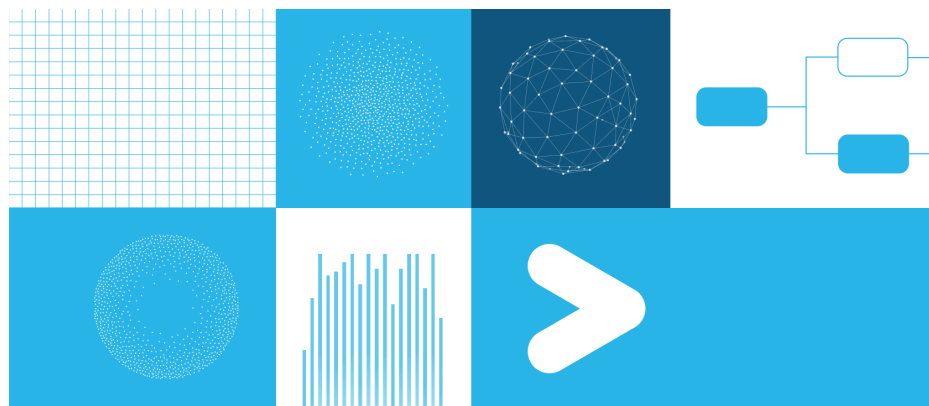
AUG 20, 2024

AUTHOR

Bhanu Prakash

Prasoon Shukla

Secure Connections with New Outbound Private Link with Snowflake Support in Preview

Machine Learning

SHARE

f   in   ✉   or various data engineering, AI and ML workloads, customers need to connect to external systems and resources outside of Snowflake — whether hosted on a cloud provider (AWS, Azure or Google Cloud Platform), a private cloud or on premises. To secure these outbound communications from Snowflake and minimize the risk of data exposure to the internet, customers can use private link from the cloud service providers (CSP) to keep data traffic within that CSP network and without traversing the public internet. We are thrilled to announce the support of outbound private link connectivity from your Snowflake account to connect to resources on Microsoft Azure (public preview) and AWS (private preview).

Outbound private link connectivity from Snowflake

We are excited to announce the launch of four major outbound use cases:

1. Access resources on Azure over **Azure Private Link** using Snowpark **external access** (available in public preview)

2. Access resources on AWS over **AWS PrivateLink** using Snowpark external access (available in private preview)

AUTHOR

Bhanu Prakash

Prasoon Shukla

3. Access your third-party services or customer apps hosted behind Azure API gateways via Snowflake **external functions** (available in public preview)

4. Load data from your named Azure external stages (Azure Blob Storage) over **Azure Private Link** (available in private preview)

This feature is available for customers on Snowflake's Business Critical edition.This feature is available for customers on Snowflake's Business Critical edition. More information about accessing and costs associated with cloud service provider private link usage can be found **here**.
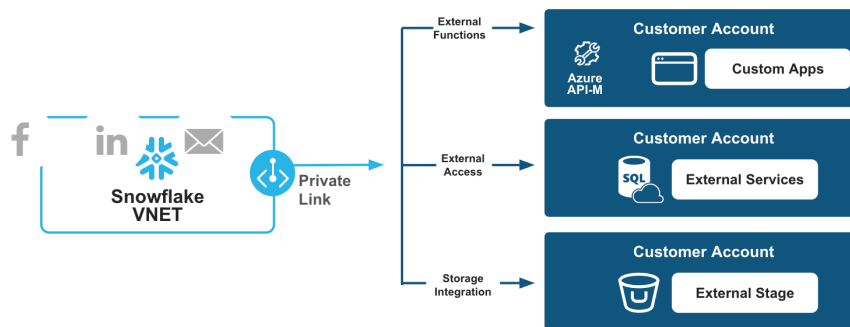
SHARE

Figure 1. Architecture diagram shows different outbound connection options with private link endpoints.

Private link in Snowflake today

Today, inbound access to the Snowflake service and Snowflake managed storage (internal stages) is secured by configuring private link connectivity to the Snowflake account. This connectivity is used for data ingestion via stages, BI or data app access, as well as user or programmatic access to all the Snowflake workloads.
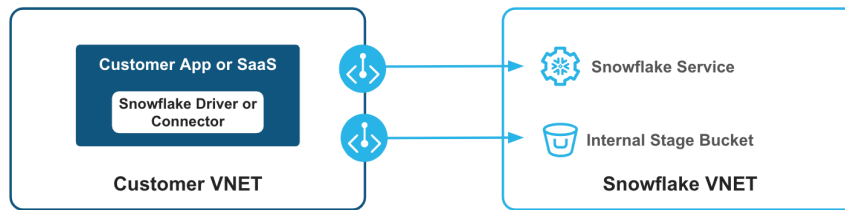
AUTHOR

Bhanu Prakash

Prasoon Shukla

Figure 2. Architecture diagram highlights inbound connectivity to Snowflake account.

Access external resources with private link

Azure Private Link enables you to access Azure PaaS services (for example, Azure Storage and SQL Database) and Azure-hosted customer-owned/partner services over a private endpoint in your virtual network. As such, you can provision a private endpoint in your Snowflake account (hosted within a virtual network) to access your external resource from Snowflake over a private endpoint. Once the connection is established using a consent-based call flow, all data that flows between your Snowflake account and external service is isolated from the internet and stays on the Microsoft network. There is no need for gateways, network address translation (NAT) devices or public IP addresses to communicate with the service.

Using external access, external functions and external stages

Customers want to load data from their cloud storage accounts via named external stages. While external stages secure the existing access to Azure Storage accounts via public connectivity, customers may want to move to private channels and further lock down access by allowing private IP addresses or disabling public access to their blob storage buckets altogether.

Last year, we launched **external access**, which enables customers to reach external endpoints from Snowpark seamlessly and securely. With this, users can easily connect to external network locations from their Snowpark code (UDFs/UDTFs and Stored Procedures) in Python or Java. This enables various use cases, such as:

Data enrichment: Data engineering pipelines sometimes require access to various APIs for different lines of business use cases. For example, Maps API can be used to get location data, which can optimize supply chain routes. Similarly, customers also have their own API endpoints running outside of Snowflake that need to be accessed.

AUTHOR

Bhanu Prakash

Prasoon Shukla

Ingest data from various systems: Customers looking to ingest data from sources, such as X, Google Sheets, MySQL or other data sources, can use external access.

Generative AI and LLM services: The recent surge in gen AI — **such as text generation from GPT-4, text summarization, code generation and image generation from Stable Diffusion, video and audio** — is paving a path that will revolutionize productivity in various sectors. Outside of accessing leading LLMs within Snowflake, customers can also directly call web-hosted LLM APIs using external access to work with gen AI.

Reverse ETL: Enables copying data from Snowflake to

operational systems and SaaS tools, such as Slack, so that business teams can leverage data to personalize customer experiences or drive actions.

A lot of these external resources and services (such as Azure SQL or Azure OpenAI) are not exposed on the public internet. Rather organizations configure them to be blocked by the internet and only accessible by private pink. With this announcement, customers can now create a private endpoint, use it as part of the **network rule**, and bind it with external access to access the external resources over the private endpoint.
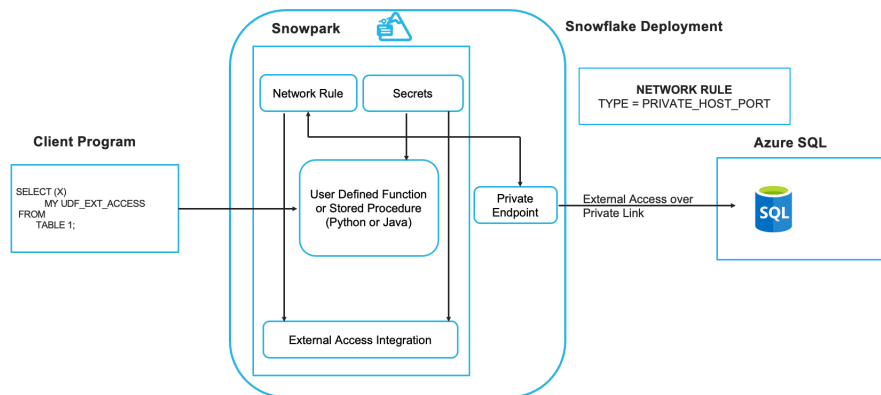
Figure 3. Architecture diagram showing Snowpark external access with outbound private link

Similar to external access, external function allows users to connect to remote resources but does so while requiring a proxy setup on the cloud provider.

With an external function, you can call code that is executed outside Snowflake. An external function is a type of user-defined function (UDF). Unlike other UDFs, an external function does not contain its own code; instead, the external function calls code that is stored and executed outside Snowflake. The remotely executed code is known as a remote service. Snowflake does not call a remote service directly. Instead, Snowflake calls a proxy service, which relays the data to the remote service. In the case of Azure, the proxy service is Azure API Management Service.

You can configure your Azure API Management Service to be blocked from public internet access and authorize access only from private endpoints. With this announcement, customers can now create a private endpoint, use it as part of the API integration, and access the proxy service (API-M) over that private endpoint.

AUTHOR

Bhanu Prakash
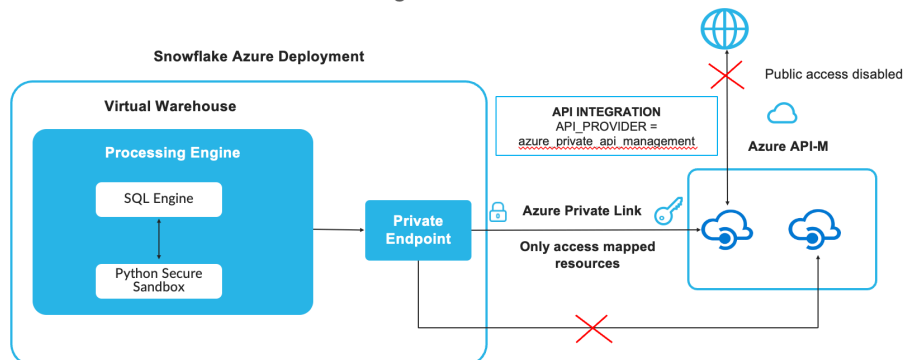
Prasoon Shukla

SHARE

Figure 4. Architecture diagram showing external function on Azure using Azure API-M.

Simplified way to configure and connect using private link

AUTHOR

Bhanu Prakash

Prasoon Shukla

In order to provide a simplified and consistent experience across different cloud providers (Azure, AWS, GCP), we let users create and manage private endpoints on Snowflake using a system function provided by Snowflake. As such, users don't have to create or manage the private endpoints directly on the cloud provider. Not only that, using system function, users can also list their private endpoints for the specific resources, as well as delete the endpoints when not in use.

Below are the steps to configure and connect to external resources on Azure using Snowpark external access:

1. **External Service Setup:** The prerequisite to connect using Azure Private Link is that the external resource/service must be enabled. You can refer to this **documentation** to identify the services enabled with private link on Azure. Create an instance of the service (e.g., Azure SQL) and block the public internet access so that Azure SQL can only be accessed via private endpoint.

2. **Create the Private Endpoint on Snowflake:** To do this, you need to call **SYSTEM$PROVISION_PRIVATELINK_ENDPOINT**.

```
SYSTEM$PROVISION_PRIVATELINK_ENDPOINT(
   '', '' ,
   [ '' ]
);
```

In the below example, we pulled the resource ID, host_name and sub resource from Azure portal. See **here** on identifying the values.

```
SELECT SYSTEM$PROVISION_PRIVATELINK_ENDPOINT(
'/subscriptions/11111111-2222-3333-4444-555555
   'testdb.database.windows.net',
   'sqlServer'
);
```

3. **Create the Network Rule** with TYPE = PRIVATE_HOST_PORT

```
CREATE OR REPLACE NETWORK RULE ext_network_acc
MODE = EGRESS
TYPE = PRIVATE_HOST_PORT
VALUE_LIST = ('externalaccessdemo.database.wir
```

4. **Create the SECRET** and then bind them together within an external access integration

AUTHOR

Bhanu Prakash

Prasoon Shukla

```
CREATE OR REPLACE EXTERNAL ACCESS INTEGRATION
azure_private_access_sql_store_integration
ALLOWED_NETWORK_RULES = (ext_network_access_dk
ALLOWED_AUTHENTICATION_SECRETS = (ext_network_
ENABLED = TRUE;
```

In this example, all the objects including SECRET, NETWORK RULE and EXTERNAL ACCESS INTEGRATION have role-based access controls (RBAC), which enable fine-grained access control enforcement for outbound connectivity.

5. Now, you can **create a procedure or UDF to call the external service**, where the traffic will go over Azure's backbone network without traversing the internet. Refer to the **documentation** to see an example of this.

f *or* in *ur* ✉ *private preview, reach out to your account representative to request access.*
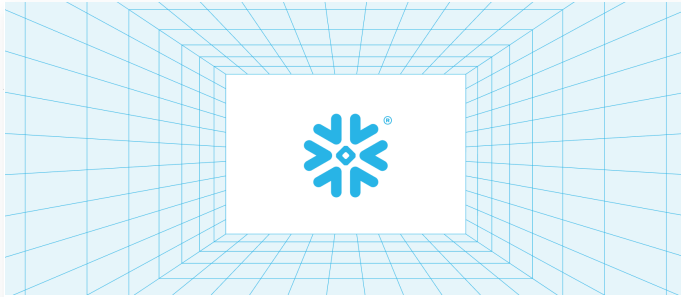
How to get started

You can get started with external access by following usage instructions in our **documentation**, which includes step-by-step setup instructions.

We're continuously looking for ways to improve, so if you have any questions or feedback about the product, make sure to let us know in the **Snowflake Community Forums**.
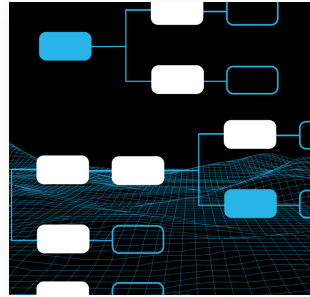
RELATED CONTENT

AUG 14, 2024

Snowflake Cortex Analyst: Behind the Scenes

Building a conversational self-service analytics product for business users is a complex and challenging endeavor. Trust and accuracy have to be at the core of such a product, as business...
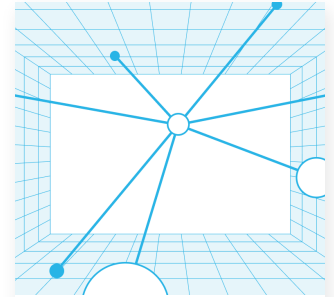
More

AUG 08, 2024

Snowflake Cortex Search: High-Quality, Performant Search and Retrieval for Enterprise AI

Search and retrieval systems have always been a critical backbone for knowledge management in enterprises....

Here's How

AUG 06, 2024

Accelerating Hyperparameter Tuning in Snowflake ML

Hyperparameter optimization (HPO) is a frequently used machine learning technique to select the best parameter...

Find Out More

VIRTUAL HANDS-ON LAB:
GETTING STARTED WITH DATA
ENGINEERING
USING SNOWFLAKE NOTEBOOKS

REGISTER HERE

Snowflake Inc.

AUTHOR

Bhanu Prakash

Prasoon Shukla

PLATFORM	SOLUTIONS	RESOURCES	EXPLORE	ABOUT
Cloud Data Platform	Snowflake for Financial Services	Resource Library	News	About Snowflake
Pricing		Webinars	Blog	Investor Relations
Marketplace	Snowflake for Advertising, Media, & Entertainment	Documentation	Trending	Leadership & Board
Security & Trust		Community	Guides	Snowflake Ventures
	Snowflake for Retail & CPG	Procurement	Developers	Careers
	Healthcare & Life Sciences Data Cloud	Legal		Contact
	Snowflake for Marketing Analytics			

SHARE   f   in   ✉

Sign up for Snowflake Communications

diana.shaw@sn⋯   United States

By submitting this form, I understand Snowflake will process my personal information in accordance with their **Privacy Notice**. Additionally, I consent to my information being shared with Event Partners in accordance with Snowflake's **Event Privacy Notice**. I understand I may withdraw my consent or update my preferences **here** at any time.

SUBSCRIBE NOW

Privacy Notice | Site Terms | Cookie Settings | Do Not Share My Personal Information

© 2024 Snowflake Inc. All Rights Reserved | If you'd rather not receive future emails from Snowflake, unsubscribe here or customize your communication preferences