



# AWS PrivateLink Onboarding Guide for Informatica Intelligent Cloud Services

<sup>©</sup> Copyright Informatica LLC 2022, 2024. Informatica, the Informatica logo, and Informatica Cloud are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html.

### **Abstract**

If you use an Amazon Virtual Private Cloud (VPC), you can configure a private connection between your VPC and Informatica Intelligent Cloud Services using Amazon Web Services (AWS) PrivateLink.

You can use AWS PrivateLink with the following services:

- API Manager
- Application Integration
- B2B Gateway
- Data Governance and Catalog
- Data Integration
- Data Marketplace
- Data Profiling
- Data Quality
- Integration Hub
- Data Ingestion and Replication (Databases, Files, and Streaming)
- MDM SaaS services (Customer 360 SaaS, Multidomain MDM SaaS, Product 360 SaaS, Reference 360 Saas, and Supplier 360 SaaS)
- Metadata Command Center

## **Supported Versions**

• Informatica Intelligent Cloud Services August 2024

## **Table of Contents**

Overview
Before you begin.
Step 1. Open a support case with Informatica Global Customer Support
Step 2. Create a VPC endpoint in your Amazon account
Step 3. Configure networking rules on AWS
Step 4. Open the hosted zone and create a record for each Informatica Intelligent Cloud Services service 9
Step 5. Set up a VPC endpoint for disaster recovery (optional)
Step 6. Verify the IP address
Step 7. Provision an interface endpoint for Data Quality and Data Profiling
Step 8. Configure AWS PrivateLink for Advanced Data Integration
Create EC2, S3, Autoscaling, Elastic Load Balancing, and STS endpoints
Add the artifact hub to the Informatica Cloud hosted zone
Configure the NAT gateway for AWS IAM and the AWS CLI
Enable AWS PrivateLink in the advanced cluster
Using Application Integration with AWS PrivateLink
Appendix A: DNS names for Informatica Intelligent Cloud Services services

ppendix B: Worksheet for setting up AWS PrivateLink	24
	-

#### **Overview**

If you use an Amazon Virtual Private Cloud (VPC), you can configure a private connection between your VPC and Informatica Intelligent Cloud Services using Amazon Web Services (AWS) PrivateLink.

To use AWS PrivateLink, you must purchase the appropriate SKU through Informatica. AWS PrivateLink communication works with Intelligent Data Management Cloud instances that are deployed on AWS infrastructure.

You can use AWS PrivateLink with the following services:

- API Manager
- Application Integration
- B2B Gateway
- Data Governance and Catalog
- Data Integration
- Data Marketplace
- Data Profiling
- Data Quality
- Integration Hub
- Data Ingestion and Replication (Databases, Files, and Streaming)
- MDM SaaS services (Customer 360 SaaS, Multidomain MDM SaaS, Product 360 SaaS, Reference 360 Saas, and Supplier 360 SaaS)
- Metadata Command Center

**Note:** For Advanced Data Integration, you can use AWS PrivateLink only on a private cluster on AWS. You can't use AWS PrivateLink on a local or self-service cluster, or on an advanced cluster in a serverless runtime environment.

When you use AWS PrivateLink, the Secure Agent in your VPC communicates with Informatica Intelligent Cloud Services securely through AWS PrivateLink instead of going over the public internet.

The following image shows an overview of the communication between your AWS account and Informatica Intelligent Cloud Services when you use AWS PrivateLink:



For all services except Application Integration, communication between Informatica Intelligent Cloud Services and the Secure Agent in your VPC is two-way. For Application Integration, communication is from Application Integration to the Secure Agent only. For more information about using Application Integration with AWS PrivateLink, see <u>"Using</u> Application Integration with AWS PrivateLink" on page 16.

To configure Informatica Intelligent Cloud Services to work with AWS PrivateLink, complete the following steps:

- 1. Open a support case with Informatica Global Customer Support to request access to Informatica Intelligent Cloud Services using AWS PrivateLink.
- 2. Create a VPC endpoint in your Amazon account.
- 3. Configure the networking rules on AWS.
- 4. Open the hosted zone and create a record for each Informatica Intelligent Cloud Services service that you use.
- 5. Optionally, set up a VPC endpoint for disaster recovery.
- Verify the IP address to ensure that you're connecting to Informatica Intelligent Cloud Services using AWS PrivateLink.
- 7. If you use Data Quality or Data Profiling, provision an interface endpoint to enable private communication between the Secure Agent and the Data Quality/Data Profiling S3 storage bucket.
- 8. If you use Advanced Data Integration, perform additional configuration steps to use AWS PrivateLink.

The following sections in this guide provide details about each of these steps.

### Before you begin

Before you begin, note the IP address that you use to connect to Informatica Intelligent Cloud Services over the public internet. When you finish configuring an AWS PrivateLink connection to Informatica Intelligent Cloud Services, you'll need to verify that this IP address differs from the one you use to connect to Informatica Intelligent Cloud Services using AWS PrivateLink.

To verify the IP address, open a terminal on AWS and use the ping command to ping Informatica Intelligent Cloud Services from a server in your AWS account.

For example, if your Informatica Intelligent Cloud Services login URL is <a href="https://dm-us.informaticacloud.com/">https://dm-us.informaticacloud.com/</a> identity-service/home, use the following command to ping Informatica Intelligent Cloud Services:

ping dm-us.informaticacloud.com

The command returns output like the following example:

PING iics-gaprod-ids-elb-123456789.us-west-2.elb.amazonaws.com (128.01.23.456): 56 data bytes

The IP address is the value within the parentheses. You can record this value in <u>"Appendix B: Worksheet for setting up</u> AWS PrivateLink" on page 24.

# Step 1. Open a support case with Informatica Global Customer Support

To start, you'll need to open a support case with Informatica Global Customer Support requesting access to Informatica Intelligent Cloud Services through AWS PrivateLink. Informatica Global Customer Support will add your AWS account ID to the allowlist and provide you with the Amazon Resource Name (ARN) for your POD and region.

If you need help creating a support case, contact your client services manager.

- 1. Open a support case with Global Customer Support and request access to Informatica Intelligent Cloud Services using AWS PrivateLink. Provide the following information in your support case:
  - Your Informatica Intelligent Cloud Services organization ID.
  - Your AWS region and backup region.

Your VPC endpoint and the AWS PrivateLink account managed by Informatica will be in the same region. For more information about finding your AWS region, see <u>Regions</u>, <u>Availability Zones</u>, <u>and Local Zones</u> in the AWS documentation.

• Your AWS account ID and backup account ID.

The account ID will be in the following format: arn:aws:iam::<account ID>:root. For more information about finding your AWS account ID, see Your AWS account identifiers in the AWS documentation.

You can record these values in "Appendix B: Worksheet for setting up AWS PrivateLink" on page 24.

2. Wait for Informatica to respond to your request and provide you with the ARN.

You should receive a response within two business days.

When Informatica responds to your request, we'll add your AWS account ID to the allowlist so that you can request an AWS PrivateLink connection to Informatica Intelligent Cloud Services. We'll also provide you with the ARN for your POD and region and enable the appropriate license for your organization.

## Step 2. Create a VPC endpoint in your Amazon account

After Informatica Global Customer Support accepts your request, create a VPC endpoint (VPCE) in your Amazon account.

- 1. In the AWS Management Console, under **Services**, select **VPC**.
- 2. Under Virtual private cloud, click Endpoints.
- 3. On the Endpoints page, click Create endpoint.

## The **Create Endpoint** page appears:

me tag - optional   ates a tag with a key of 'Name' and a value that you specify.   y-endpoint-01   rvice category   ext the service category   AWS services   Services provided by Amazon   AWS Marketplace services   Services that you've purchased through AWS Marketplace     rvice settings
y-endpoint-01  rvice category  ext the service category  AWS services Services provided by Amazon  AWS Marketplace services Services that you've purchased through AWS Marketplace  rvice settings
rvice category         et the service category         AWS services         Services provided by Amazon         AWS Marketplace services         Services that you've purchased through AWS Marketplace         rvice settings
AWS services         Services provided by Amazon         AWS Marketplace services         Services that you've purchased through AWS Marketplace         O Other endpoint services         Find services shared with you by service name
AWS Marketplace services Services that you've purchased through AWS Marketplace Other endpoint services Find services shared with you by service name rvice settings
rvice settings
vice name
m.amazonaws.vpce.us-west-2.vpce-svc-
Service name verified.

- 4. Under Endpoint settings, enter a name tag and select the service category PrivateLink Ready partner services.
- 5. Under Service settings, enter the ARN name provided by Informatica and click Verify service.

You should see a message saying that the service name was verified.

If service verification fails, verify that your VPC endpoint and the AWS PrivateLink account managed by Informatica are in the same region as your Informatica Intelligent Cloud Services organization. If they're not, you'll need to set up VPC peering to route traffic to an endpoint that is in the same region as the AWS PrivateLink account managed by Informatica. For more information about setting up VPC peering, see the <u>Amazon VPC Peering Guide</u>.

- Under VPC, select the VPC that you want to use to connect to Informatica Intelligent Cloud Services. This is the VPC where your Secure Agents are or will be installed.
- 7. Under **Subnets**, select the availability zones and subnet IDs that you want to communicate over AWS PrivateLink.

You can select multiple subnets in different availability zones to ensure that your interface endpoint is resilient to availability zone failures.

- 8. For the IP address type, select IPv4.
- 9. Under Security groups, select the security groups that define the subnet access.

Create or select a security group with an inbound rule that allows the following access:

Property	Value
IP version	IP
Protocol	ТСР
Port range	443
Source	The IP address of your subnets

- 10. Click Create endpoint.
- 11. Update your support case with Informatica Global Customer Support to let Informatica know that you've completed the endpoint request. Include the VPC endpoint ID in the support the case.

Informatica Global Customer support will notify you when your request has been accepted. Normally, notification takes two business days or less.

## Step 3. Configure networking rules on AWS

When your request has been accepted, configure the networking rules on AWS.

1. In the AWS Management Console, under **Services**, select **Route 53**.

2. In the Route 53 Dashboard, under DNS management, click Create hosted zone.

Route 53 > Hosted zones > Create hosted zone

#### Create hosted zone Info

Hosted zone configuration A hosted zone is a container that holds information subdomains.	about how you want to route traffic for a domain, such as example.com, and its
Domain name Info This is the name of the domain that you want to rou	te traffic for.
example.com	
Valid characters: a-z, 0-9, ! " # \$ % & ' ( ) * + , - / : ; <	= > ? @ [\]^_`{ }.~
Description - optional Info This value lets you distinguish hosted zones that have	<i>i</i> e the same name.
The hosted zone is used for	
The description can have up to 256 characters. 0/25	6
Type Info The type indicates whether you want to route traffic Public hosted zone A public hosted zone determines how traffic is routed on the internet.	<ul> <li>on the internet or in an Amazon VPC.</li> <li>Private hosted zone         A private hosted zone determines how             traffic is routed within an Amazon VPC.     </li> </ul>
VPCs to associate with the hosted To use this hosted zone to resolve DNS queries for o VPC was created using a different AWS account, you	<b>ZONE Info</b> ne or more VPCs, choose the VPCs. To associate a VPC with a hosted zone when the must use a programmatic method, such as the AWS CLI.
For each VPC that you associate with enableDnsHostnames and enableDns	a private hosted zone, you must set the Amazon VPC settings X Support 🔀 to true.
Region Info	VPC ID Info
US West (Oregon) [us-west-2]	Q vpc-
Add VPC	

- 3. Under Domain name, enter informaticacloud.com.
- 4. Optionally, enter a description.
- 5. Under Type, select Private hosted zone.
- 6. Under **VPCs to associate with the hosted zone**, select the region and the VPC and subnets that you configured when you created the VPC endpoint.
- 7. Optionally, under **Tags**, create and apply tags to identify the hosted zone.
- 8. Click Create hosted zone.

You should see a message saying that the domain "informaticacloud.com" was successfully created.

## **Step 4. Open the hosted zone and create a record for each Informatica Intelligent Cloud Services service**

Open the hosted zone and create a record for each Informatica Intelligent Cloud Services service that you use.

Note: To use a private hosted zone, the VPC must have DNS host names enabled.

- 1. In the AWS Management Console, under Services, select VPC.
- 2. Under Virtual private cloud, click Endpoints.
- 3. On the **Endpoints** page, copy the DNS name for the VPC endpoint:

pce-(			Actio
Details			
Endpoint ID	Status	Creation time	Endpoint type
🗇 vpce-tal	⊘ Available	Tuesday, July 19, 2022 at 14:05:16 CDT	Interface
VPC ID	Status message	Service name	Private DNS names enabled
vpc (my_vpc-01)		🗗 com.amazonaws.vpce.	No
INS record IP type	IP address type		
ipv4	ipv4	DNS names	
		C vpce-	
		- (ZT)	
		🗇 vpce-	
		the part of the second state of the second state	
		1.vpce.amazonaws.com	

You can record this value in "Appendix B: Worksheet for setting up AWS PrivateLink" on page 24.

- 4. Close the Endpoints page.
- 5. In the AWS Management Console, under Services, select Route 53.
- 6. Select Hosted zones.
- 7. Under Hosted Zones, click the informaticacloud.com domain.
- 8. Under Records, click Create record.

The Quick create record page appears:

Quick create record Info		Switch to wizard
▼ Record 1		Delete
Record name Info		Record type Info
Keep blank to create a record for the root	.informaticacloud.com domain.	CNAME – Routes traffic to another domain name and to some AWS reso ▼
vpce-( Enter multiple values on separate lines.		vpce.amazonaws.com
TTL (seconds) Info		Routing policy Info
300		Simple routing
1m 1h 1d Recommended values: 60 to 172800 (two	days)	
		Add another record
		Cancel Create records

9. Under Record name, enter the DNS name you use to access the service over the public internet.

For information on how to obtain the DNS name for each service, see <u>"Appendix A: DNS names for</u> <u>Informatica Intelligent Cloud Services services" on page 16</u>. You can record the DNS names you need in "Appendix B: Worksheet for setting up AWS PrivateLink" on page 24.

- 10. Under Record type, select CNAME.
- 11. Under Value, enter the VPC endpoint to which you want to route traffic to, for example, vpce-svsabcdefg012345.us-west-2.vpce.amazonaws.com.

This is the DNS name that you copied from the endpoint in step  $\underline{3}$  above.

- 12. If you use more than one Informatica Intelligent Cloud Services service, click **Add another record** and repeat steps 9-12 for each of the other services.
- 13. Click Create records.

#### Step 5. Set up a VPC endpoint for disaster recovery (optional)

Optionally, set up a VPC endpoint for disaster recovery. In the event of a faillover, you can move your DNS to the backup location.

To set up a VPC endpoint for disaster recovery, repeat the steps in <u>"Step 2. Create a VPC endpoint in your Amazon</u> account" on page 5 for the VPC endpoint that you want to use for disaster recovery.

## Step 6. Verify the IP address

To verify that you are using AWS PrivateLink to connect to Informatica Intelligent Cloud Services, verify the IP address. The IP address you use should differ from the one you noted in the "Before you begin" step.

Open a terminal in your AWS VPC and use the ping command to verify that the IP address now differs from the one returned in <u>"Before you begin" on page 4</u>.

For example, if your Informatica Intelligent Cloud Services login URL is <a href="https://dm-us.informaticacloud.com/">https://dm-us.informaticacloud.com/</a> identity-service/home, use the following command to ping Informatica Intelligent Cloud Services:

ping dm-us.informaticacloud.com

The command now returns output like the following example:

PING iics-gaprod-ids-elb-123456789.us-west-2.elb.amazonaws.com (10.98.76.543): 56 data bytes

The new IP address should start with the same numbers as the IP address for your VPC.

## Step 7. Provision an interface endpoint for Data Quality and Data Profiling

If you use Data Quality or Data Profiling, you can configure a private connection between the Secure Agent and the Data Quality/Data Profiling S3 storage bucket.

Note: If you don't use Data Quality or Data Profiling, skip this step.

To configure a private connection, provision an interface endpoint for Data Quality and Data Profiling in your VPC and enable private DNS names for your VPC endpoint. An interface VPC endpoint creates an elastic network interface (ENI) with private IP addresses in your VPC subnets.

Note that interface VPC endpoints incur hourly and per-GB data processing charges. For more information, see <u>AWS PrivateLink Pricing</u> in the AWS documentation.

For more information about configuring interface endpoints, see <u>Configure an interface endpoint</u> in the AWS documentation.

- 1. In the AWS Management Console, under **Services**, select **VPC**.
- 2. Under Virtual private cloud, select Endpoints.
- 3. On the Endpoints page, click Create endpoint:

aws III Services Q Search	h	[Option+5]	<u></u> 2 4 0 0	Oregon 🔻 InfaNetwork
VPC dashboard X	Endpoints (20) Info		C	Actions V Create endpoint 0 V V V V V V V V V V V V V V V V V V V
Filter by VPC:	□ Name マ	VPC endpoint ID 🛛 🗢	VPC ID 🗸	Service name
Select a VPC		vpce-0cf53	vpc-069a5	com.amazonaws.us-west-2.execute-api
▼ Virtual private cloud			<u>vpc-04fb3</u>	com.amazonaws.us-west-2.execute-api
Your VPCs	-		vpc-0f1c4a	com.amazonaws.us-west-2.execute-api
Subnets	<b>—</b>	vpce-0694	vpc-0e95	com.amazonaws.us-west-2.execute-api
Route tables	-	vpce-0d4aa		com.amazonaws.us-west-2.execute-api
Internet gateways	<b>—</b>	vpce-0322		com.amazonaws.us-west-2.execute-api
Egress-only internet		vpce-097cc	vpc-0434f	com.amazonaws.vpce.us-west-2.vpce-svc-025d
Garrier nateways	maharshiTest		vpc-0db1e	com.amazonaws.us-west-2.execute-api
DHCP option sets				
Elastic IPs				
Managed prefix lists	Select an endpoint			
Endpoints				
Endpoint services				
NAT gateways				
Peering connections				
▼ Security				
Network ACLs				
Security groups		August 1 1991		

The Create endpoint page appears:

a search	[Option+S]	Σ	\$	0	۲	Oregon 🔻	InfaNetwork(	-	
<u>C</u> > <u>Endpoints</u> > Create endpoint									G
reate endpoint Info ere are three types of VPC endpoints – Interface endpoints, Ga vateLink, and use an Elastic Network Interface (ENI) as an entr e service, while Gateway endpoints and Gateway Load Balance	iteway Load Balancer endpoints, and Gateway endpoints. Inter y point for traffic destined to the service. Interface endpoints a r endpoints serve as a target for a route in your route table for	face endpo ire typically traffic dest	ints and accesse tined for	l Gatewa ed using r the ser	ay Load I the pu vice.	Balancer end blic or private	points are powe DNS name asso	red by AWS ociated with	C
Endpoint settings									
Name tag - optional									
Creates a tag with a key of 'Name' and a value that you specify.									
Service category									
Service category Select the service category	PrivateLink Ready partner services Services with an AWS Service Ready designation		) AWS Servic	Market ces that y	place se	rvices rchased through	AWS Marketplace		
Service category Select the service category	PrivateLink Ready partner services Services with an AWS Service Ready designation      Other endpoint services Find services shared with you by service name		AWS Servic	Market tes that y	place se ou've pu	rvices chased through	AWS Marketplace		
Service category Select the service category     Services provided by Amazon	PrivateLink Ready partner services Services with an AWS Service Ready designation     Other endpoint services     Find services shared with you by service name		AWS Servic	Marketi	place se ou've pur	rvices chased through	AWS Marketplace	C	
Service category Select the service category	PrivateLink Ready partner services Services with an AWS Service Ready designation      Other endpoint services Find services shared with you by service name		AWS Servic	Market; ses that y	place se ou've pur	rvices chased through 4 5 6	AWS Marketplace	© <	

4. Under Endpoint settings, enter a name tag and select the service category AWS services.

If you're using any other DNS provider and can't use the AWS private hosted zone, contact Informatica Global Customer Support.

- 5. Under Services, search for S3 and select the endpoint for your region, for example, com.amazonaws.uswest-2.s3. Be sure that the Type is Interface.
- 6. Under VPC, select the VPC in which to create your endpoint.
- 7. Under **Subnets**, select the availability zones and subnet IDs associated with your endpoint. Be sure to choose subnets that aren't public.

8. Under **Security groups**, select the security groups that define the subnet access or create a new security group and select it.

To create a new security group:

a. In the AWS Management Console, under **Security**, select **Security groups** and click **Create security** group:

aws	Services	Q Search		[Option+S]		D	\$	0	9	Oregon 🔻	InfaNetwork		•
VP	C dashboard		Security Groups Info		Actions <b>v</b>					•	Create securi	ty group	0
EC. Filt	2 Global View 🗠 er by VPC:		Q Find resources by attribute or tag								< 1	> ©	
S	elect a VPC	•	Name V Security group ID		▼   Security g	proup nar	ne			VPC ID			▼
▼ Vir	tual private cloud												
Yo	ur VPCs												
Sul	bnets ute tables												
! Int	ernet gateways												
Egi gat	ress-only internet teways												
Ca	rrier gateways												
DH	CP option sets												
Ela	stic IPs										Ľ		
Ma	naged prefix lists												
En	dpoints												
En	dpoint services												
NA	T gateways												
Pe	ering connections												
▼ Sec	urity												
Ne	twork ACLs												
Se	curity groups					-							

The Create security group page appears:

aws Ervices Q Search	[Option+S]	Σ	\$	0	٢	Oregon 🔻	InfaNetwork(	-
VPC > Security Groups > Create security group								(i)
Create security group as								-
A security group acts as a virtual firewall for your instance to control i	inbound and outbound traffic. To c	reate a new security group, comp	lete the	fields be	low			6
A second group acts as a virtual memory our instance to control i		cate a new security group, comp		netus bi				
Basic details								
Security group name Info								
s3_security_group								
Name cannot be edited after creation.								
Description Info					k			
s3_security_group								
vnc-0073d8ci	•							
Inbound rules Info								
This security group has no inbound rules.								
Add rule								
				-				

- b. Enter a name for the security group.
- c. Optionally, enter a description for the security group.
- d. Select your VPC.
- e. Under **Inbound rules**, create a rule of type **HTTPS** and choose the appropriate number of CIDR blocks. The number of CIDR blocks should match the IP address range for the VPC.
- f. Click Create security group and note the security group ID.

You'll need the security group ID when you select the security group for the endpoint.

- g. In the AWS Management Console, switch back to the **Create endpoint** page, and under **Security groups**, select the security group you created.
- 9. On the **Create endpoint** page, under **Policy**, select **Full access**, or select **Custom** and enter a custom policy for the VPC endpoint to control access to the service.
- 10. Optionally, add tags for the endpoint.
- 11. Click Create endpoint.

It takes several minutes for the endpoint to become available. When the endpoint is available, its state changes to "Available" on the **Endpoints** page.

12. When the endpoint is available, on the **Endpoints** page, select the endpoint and choose **Actions** > **Modify private DNS name**:

aw	Services	Q Search		[Option+S]	۵	\$ Ø	۲	Oregon 🔻 InfaNetwork	-	•
V	PC dashboard C2 Global View 🖸	×	Endpoints (1/21) Info Q. Search				C	Actions A Create Create	inc <mark>point</mark>	3 0
F	ilter by VPC: Select a VPC	•	■ Name ▼ MDMnext-ga-mrel-8-30	VPC endpoint ID	▼ VPC ID		▼   :	Manage subnets Manage security groups	pre-svc-0aa3;	
• V Y	i <b>rtual private cloud</b> our VPCs		jfrogendpoint Artifactory-MREL	vpce-0603 vpce-094e	vpc-0073c	MDMCLOUD		Manage policy Modify private DNS name	pce-svc-060f5 pce-svc-05dfa	
R	oute tables nternet gateways		test-s3 S3-INTERFACE-ENDPOINT	vpce-00159	vpc-0dd25		( (	Modify endpoint settings Manage tags Delete VPC endpoints		
9 5 0	gress-only internet ateways arrier gateways		Netops-Test     PROMPUSH	vpce-0192 eice-056b	vpc-08a2	NETOPS-Pri.	c c e	com.amazonaws.vpce.us-west-2 eice-056b	,\;	
E	HCP option sets lastic IPs		unco 01191	FEDEACE ENDOINT						
E	ndpoints		Details Subnets Securi	ty Groups Notification	Policy Monitoring	Tags				

13. On the Modify private DNS name page, under Modify private DNS name settings, check Enable for this endpoint, uncheck Enable private DNS only for inbound endpoint, and then click Save changes:



After you provision the endpoint, you can use the Linux dig command to verify that communication between the Secure Agent and S3 bucket goes through the VPC. To do this, enter the following command and verify that the IP addresses returned are part of the subnet where you created your interface endpoint:

dig s3.<region>.amazonaws.com +short

## Step 8. Configure AWS PrivateLink for Advanced Data Integration

If you use Advanced Data Integration, perform additional configuration steps to use AWS PrivateLink between your VPC and Informatica Intelligent Cloud Services.

Complete the following tasks:

- Create EC2, S3, Autoscaling, Elastic Load Balancing, and STS endpoints.
- · Add the artifact hub to the Informatica Cloud hosted zone.
- Configure the NAT gateway for AWS IAM and the AWS CLI.
- Enable AWS PrivateLink in the advanced cluster.

#### Create EC2, S3, Autoscaling, Elastic Load Balancing, and STS endpoints

Create endpoints for EC2, S3, Autoscaling, Elastic Load Balancing, and STS in your AWS account.

- 1. In the AWS Management Console, under Services, select VPC.
- 2. Under Virtual private cloud, click Endpoints.
- 3. On the Endpoints page, click Create endpoint to create an EC2 endpoint.
  - a. Under Endpoint settings, enter a name tag and select the service category AWS Services.
  - b. Under Services, select the EC2 service such as com.amazonaws.eu-west-1.ec2.
  - c. Under VPC, select the VPC that you want to use to connect to Informatica Intelligent Cloud Services.
  - Under Subnets, select the availability zones and subnet IDs that you want to communicate over AWS PrivateLink.

You can select multiple subnets in different availability zones to ensure that your interface endpoint is resilient to availability zone failures.

- e. Under Security groups, select the security groups that define subnet access through port 443.
- 4. Click Create endpoint to create an S3 endpoint
  - a. Under Endpoint settings, enter a name tag and select the service category AWS Services.
  - b. Under Services, select the S3 service with type Gateway such as com.amazonaws.eu-west-1.s3.
  - c. Under VPC, select the VPC that you want to use to connect to Informatica Intelligent Cloud Services.
  - d. Under Route Tables, select the route table associated with the private subnet.
- 5. Click Create endpoint to create an Autoscaling endpoint.
  - a. Under Endpoint settings, enter a name tag and select the service category AWS Services.
  - b. Under Services, select the Autoscaling service such as com.amazonaws.eu-west-1.autoscaling.
  - c. Under VPC, select the VPC that you want to use to connect to Informatica Intelligent Cloud Services.
  - d. Under **Subnets**, select the availability zones and subnet IDs that you want to communicate over AWS PrivateLink.

You can select multiple subnets in different availability zones to ensure that your interface endpoint is resilient to availability zone failures.

- e. Under Security groups, select the security groups that define subnet access through port 443.
- 6. Click Create endpoint to create an Elastic Load Balancing endpoint.
  - a. Under Endpoint settings, enter a name tag and select the service category AWS Services.
  - b. Under Services, select the Elastic Load Balancing service such as com.amazonaws.euwest-1.elasticloadbalancing.
  - c. Under **VPC**, select the VPC that you want to use to connect to Informatica Intelligent Cloud Services.
  - d. Under **Subnets**, select the availability zones and subnet IDs that you want to communicate over AWS PrivateLink.

You can select multiple subnets in different availability zones to ensure that your interface endpoint is resilient to availability zone failures.

- e. Under Security groups, select the security groups that define subnet access through port 443.
- 7. Click Create endpoint to create an STS endpoint.
  - a. Under Endpoint settings, enter a name tag and select the service category AWS Services.
  - b. Under Services, select the STS service such as com.amazonaws.eu-west-1.sts.
  - c. Under VPC, select the VPC that you want to use to connect to Informatica Intelligent Cloud Services.
  - d. Under **Subnets**, select the availability zones and subnet IDs that you want to communicate over AWS PrivateLink.

You can select multiple subnets in different availability zones to ensure that your interface endpoint is resilient to availability zone failures.

e. Under Security groups, select the security groups that define subnet access through port 443.

#### Add the artifact hub to the Informatica Cloud hosted zone

In the Informatica Cloud hosted zone, create a record for the artifact hub.

- 1. In the AWS Management Console, under Services, select Route 53.
- 2. Select Hosted zones.
- 3. Under Hosted Zones, click the informaticacloud.com domain.
- 4. Under Records, click Create record.
- 5. Under Record name, enter artifacthub.informaticacloud.com.
- 6. Under **Record type**, select **CNAME**.
- 7. Under Value, enter the VPC endpoint to which you want to route traffic to, for example, vpce-svsabcdefg012345.us-west-2.vpce.amazonaws.com.
- 8. Click Create records.

#### Configure the NAT gateway for AWS IAM and the AWS CLI

Configure the NAT gateway to enable AWS IAM and the AWS CLI.

- 1. On an EC2 instance in your VPC, run the following commands to get the IP addresses of the AWS IAM and AWS CLI services:
  - nslookup iam.amazonaws.com to get the IP address of the AWS IAM service
  - nslookup awscli.amazonaws.com to get the IP address of the AWS CLI service
- 2. In the AWS Management Console, under Services, select VPC, and select your VPC.
- 3. Under Resource map, select the route table associated with the private subnet.

- 4. Click Edit Routes.
- 5. Click Add route to add a route to enable AWS IAM.

In the route entry, add the IP address of the AWS IAM service as the destination and select NAT Gateway as the target. You can also use a dynamic IP address like 44.216.0.0/16 as the destination since the IP address can change at any time.

6. Click Add route to add a route to enable the AWS CLI.

In the route entry, add the IP address of the AWS CLI service as the destination and select NAT Gateway as the target.

7. Click Save changes.

#### Enable AWS PrivateLink in the advanced cluster

Edit the advanced configuration for the advanced cluster to enable AWS PrivateLink.

- 1. In Administrator, navigate to the Advanced Clusters page.
- 2. Edit the advanced configuration for the advanced cluster.
- 3. Under **Runtime Configuration**, add a runtime property.
- 4. Enter the runtime property name css.aws.enable.service.endpoint.config and set it to true.

## **Using Application Integration with AWS PrivateLink**

Application Integration supports only one-way communication through AWS PrivateLink, that is, from Application Integration to the Secure Agent.

You can invoke processes that are published on a Secure Agent through any REST client such as Postman or cURL only if the ports are allowed in the AWS security group. However, you cannot access Amazon resources using an Application Integration service connector or connection.

After you enable a Secure Agent that is installed in an AWS VPC, the agent connects directly to the connection endpoints through AWS PrivateLink. You can perform all the Application Integration operations that the Secure Agent supports. However, if the process runs on a Secure Agent that is installed on an AWS VPC, you cannot invoke the process using the endpoint URL in a browser. Instead, you can invoke the process endpoint URL using the cURL command from a machine where the Secure Agent is installed.

To invoke a process using the cURL command, use the following syntax:

curl -X PUT -k https://<host name>:<port number>/process-engine/public/rt/<process name>

You can also invoke scheduled processes.

For more information about Application Integration, see the Application Integration help.

## Appendix A: DNS names for Informatica Intelligent Cloud Services services

When you create records in the hosted zone for the informaticacloud.com domain, you need to allow the DNS names for each Informatica Intelligent Cloud Services service that you use. DNS names vary based on your POD.

When you enter DNS names to allow, enter the global service DNS names and the Data Integration DNS name for your POD. If you use any service other than Data Integration, you also need to enter the DNS names for the service.

For example, if you're on the APSE1 POD and you use the Application Integration (CAI) and API Manager services, you would allow the following DNS names:

```
dm-ap.informaticacloud.com
content.dm-ap.informaticacloud.com
apsel.dm-ap.informaticacloud.com
global-package.dm.informaticacloud.com
icsdownloadsecure.informatica.com
apsel-cai.dm-ap.informaticacloud.com
apsel-apim.dm-ap.informaticacloud.com
```

If you are unsure of your POD or your organization uses a custom URL to log in to Informatica Intelligent Cloud Services, contact your Informatica representative to find the DNS names.

Asia/Pacific/Japan (APNE2)

If your POD is APNE2, allow the following DNS names:

Service	DNS names
Global Identity Service	dm-apne.informaticacloud.com content.dm-apne.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	apne2.dm-apne.informaticacloud.com

Service	DNS names
API Manager	apne2-apim.dm-apne.informaticacloud.com apne2-apigw.dm-apne.informaticacloud.com
Application Integration (CAI)	apne2-cai.dm-apne.informaticacloud.com
Application Integration (Salesforce)	apne2-sfdc-cai.dm-apne.informaticacloud.com
Data Governance and Catalog, Data Marketplace and Metadata Command Center	<pre>cdgc-api.dm-apne.informaticacloud.com cdgc.dm-apne.informaticacloud.com cdmp-app.dm-apne.informaticacloud.com idmcp-api.dm-apne.informaticacloud.com idmcp-mgmt.dm-apne.informaticacloud.com mcc.dm-apne.informaticacloud.com idmc-api.dm-apne.informaticacloud.com</pre>
Data Profiling (CDP)	apne2-dqprofile.dm-apne.informaticacloud.com
Data Quality (CDQ)	apne2-dqcloud.dm-apne.informaticacloud.com
Integration Hub (CIH)	apne2-cih.dm-apne.informaticacloud.com
Data Ingestion and Replication (CMI)	apne2-ing.dm-apne.informaticacloud.com

#### Asia/Pacific/Japan (APSE1)

If your POD is APSE1, allow the following DNS names:

Service	DNS names
Global Identity Service	dm-ap.informaticacloud.com content.dm-ap.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	apsel.dm-ap.informaticacloud.com

Service	DNS names
API Manager	apsel-apim.dm-ap.informaticacloud.com apsel-apigw.dm-ap.informaticacloud.com
Application Integration (CAI)	apsel-cai.dm-ap.informaticacloud.com
Application Integration (Salesforce)	apsel-sfdc-cai.dm-ap.informaticacloud.com
B2B Gateway	apse1-b2bgw.dm-ap.informaticacloud.com
Data Governance and Catalog, Data Marketplace and Metadata Command Center	<pre>cdgc.dm-ap.informaticacloud.com mcc.dm-ap.informaticacloud.com cdmp-app.dm-ap.informaticacloud.com idmc-api.dm-ap.informaticacloud.com cdgc-api.dm-ap.informaticacloud.com idmcp-api.dm-ap.informaticacloud.com</pre>
Data Profiling (CDP)	apsel-dqprofile.dm-ap.informaticacloud.com
Data Quality (CDQ)	apsel-dqcloud.dm-ap.informaticacloud.com
Integration Hub (CIH)	apsel-cih.dm-ap.informaticacloud.com
Data Ingestion and Replication (CMI)	apse1-ing.dm-ap.informaticacloud.com

#### European Union (EMW1)

If your POD is EMW1, allow the following DNS names:

Service	DNS names
Global Identity Service	dm-em.informaticacloud.com content.dm-em.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	emw1.dm-em.informaticacloud.com

Service	DNS names
API Manager	emw1-apim.dm-em.informaticacloud.com emw1-apigw.dm-em.informaticacloud.com
Application Integration (CAI)	emw1-cai.dm-em.informaticacloud.com
Application Integration (Salesforce)	emw1-sfdc-cai.dm-em.informaticacloud.com
B2B Gateway	emw1-b2bgw.dm-em.informaticacloud.com
Data Governance and Catalog, Data Marketplace and Metadata Command Center	<pre>cdgc.dm-em.informaticacloud.com mcc.dm-em.informaticacloud.com cdmp-app.dm-em.informaticacloud.com cdgc-api.dm-em.informaticacloud.com idmcp-api.dm-em.informaticacloud.com idmc-api.dm-em.informaticacloud.com</pre>
Data Profiling (CDP)	emw1-dqprofile.dm-em.informaticacloud.com
Data Quality (CDQ)	emw1-dqcloud.dm-em.informaticacloud.com
Integration Hub (CIH)	emw1-cih.dm-em.informaticacloud.com
Data Ingestion and Replication (CMI)	emw1-ing.dm-em.informaticacloud.com

#### United Kingdom (UK1)

If your POD is UK1, allow the following DNS names:

Service	DNS names
Global Identity Service	dm-uk.informaticacloud.com content.dm-uk.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	uk1.dm-uk.informaticacloud.com

Service	DNS names
API Manager	uk1-apim.dm-uk.informaticacloud.com uk1-apigw.dm-uk.informaticacloud.com
Application Integration (CAI)	ukl-cai.dm-uk.informaticacloud.com
Application Integration (Salesforce)	ukl-sfdc-cai.dm-uk.informaticacloud.com
B2B Gateway	uk1-b2bgw.dm-uk.informaticacloud.com
Data Governance and Catalog, Data Marketplace and Metadata Command Center	<pre>cdgc.dm-uk.informaticacloud.com mcc.dm-uk.informaticacloud.com cdmp-app.dm-uk.informaticacloud.com cdgc-api.dm-uk.informaticacloud.com idmcp-api.dm-uk.informaticacloud.com idmc-api.dm-uk.informaticacloud.com</pre>
Data Profiling (CDP)	ukl-dqprofile.dm-uk.informaticacloud.com
Data Quality (CDQ)	ukl-dqcloud.dm-uk.informaticacloud.com
Integration Hub (CIH)	uk1-cih.dm-uk.informaticacloud.com
Data Ingestion and Replication (CMI)	ukl-ing.dm-uk.informaticacloud.com

#### United States East (USE2)

If your POD is USE2, allow the following DNS names:

Service	DNS names
Global Identity Service	dm-us.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	na2.dm-us.informaticacloud.com

Service	DNS names
API Manager	apim-pod2.dm-us.informaticacloud.com apigw-pod2.dm-us.informaticacloud.com
Application Integration (CAI)	na2.ai.dm-us.informaticacloud.com
Application Integration (Salesforce)	na2.sfdc-ai.dm-us.informaticacloud.com
B2B Gateway	use2-b2bgw.dm-us.informaticacloud.com
Data Governance and Catalog, Data Marketplace and Metadata Command Center	<pre>cdgc.dm-us.informaticacloud.com cdmp-app.dm-us.informaticacloud.com mcc.dm-us.informaticacloud.com icd-app.dm-us.informaticacloud.com cdgc-api.dm-us.informaticacloud.com idmc-api.dm-us.informaticacloud.com</pre>
Data Profiling (CDP)	na2-dqprofile.dm-us.informaticacloud.com
Data Quality (CDQ)	na2-dqcloud.dm-us.informaticacloud.com
Integration Hub (CIH)	cih-pod2.dm-us.informaticacloud.com
Data Ingestion and Replication (CMI)	na2-ing.dm-us.informaticacloud.com

#### United States East (USE6)

If your POD is USE6, allow the following DNS names:

Service	DNS names
Global Identity Service	dm-us.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	use6.dm-us.informaticacloud.com

Service	DNS names
API Manager	use6-apim.dm-us.informaticacloud.com use6-apigw.dm-us.informaticacloud.com
Application Integration (CAI)	use6-cai.dm-us.informaticacloud.com
Application Integration (Salesforce)	use6-sfdc-cai.dm-us.informaticacloud.com
B2B Gateway	use6-b2bgw.dm-us.informaticacloud.com
Data Governance and Catalog, Data Marketplace and Metadata Command Center	<pre>cdgc.dm-us.informaticacloud.com cdmp-app.dm-us.informaticacloud.com mcc.dm-us.informaticacloud.com icd-app.dm-us.informaticacloud.com cdgc-api.dm-us.informaticacloud.com idmc-api.dm-us.informaticacloud.com</pre>
Data Profiling (CDP)	use6-dqprofile.dm-us.informaticacloud.com
Data Quality (CDQ)	use6-dqcloud.dm-us.informaticacloud.com
Integration Hub (CIH)	use6-cih.dm-us.informaticacloud.com
Data Ingestion and Replication (CMI)	use6-ing.dm-us.informaticacloud.com
MDM SaaS services	use6-mdm.dm-us.informaticacloud.com

#### United States West (USW5)

If your POD is USW5, allow the following DNS names:

Service	DNS names
Global Identity Service	dm-us.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	usw5.dm-us.informaticacloud.com

Service	DNS names
API Manager	usw5-apim.dm-us.informaticacloud.com usw5-apigw.dm-us.informaticacloud.com
Application Integration (CAI)	usw5-cai.dm-us.informaticacloud.com
Application Integration (Salesforce)	usw5-sfdc-cai.dm-us.informaticacloud.com
B2B Gateway	usw5-b2bgw.dm-us.informaticacloud.com
Data Governance and Catalog, Data Marketplace and Metadata Command Center	<pre>cdgc.dm-us.informaticacloud.com cdmp-app.dm-us.informaticacloud.com mcc.dm-us.informaticacloud.com icd-app.dm-us.informaticacloud.com cdgc-api.dm-us.informaticacloud.com idmc-api.dm-us.informaticacloud.com</pre>
Data Profiling (CDP)	usw5-dqprofile.dm-us.informaticacloud.com
Data Quality (CDQ)	usw5-dqcloud.dm-us.informaticacloud.com
Integration Hub (CIH)	usw5-cih.dm-us.informaticacloud.com
Data Ingestion and Replication (CMI)	usw5-ing.dm-us.informaticacloud.com
MDM SaaS services	usw5-mdm.dm-us.informaticacloud.com

## Appendix B: Worksheet for setting up AWS PrivateLink

Use the following worksheet to record the information that you need to configure Informatica Intelligent Cloud Services to work with AWS PrivateLink.

The following table lists the information you'll need and the reason you need it:

Information needed	Reason	My value
Original Informatica Intelligent Cloud Services IP address	Used to verify your AWS PrivateLink connection.	
Informatica Intelligent Cloud Services organization ID	Needed by Informatica Global Customer support.	
AWS region	Needed by Informatica Global Customer support.	
AWS backup region	Needed by Informatica Global Customer support.	
AWS account ID	Needed by Informatica Global Customer support.	
ARN for your POD and region	Needed to create your VPC endpoint.	
VPC endpoint ID	Needed by Informatica Global Customer support.	
DNS name for the VPC endpoint	Needed to create records in the hosted zone for your Informatica Intelligent Cloud Services services.	
DNS names for the Informatica Intelligent Cloud Services services for which you want to create an AWS PrivateLink connection	Needed to create records in the hosted zone for your Informatica Intelligent Cloud Services services. To find the DNS names, see <u>"Appendix A: DNS names for</u> <u>Informatica Intelligent Cloud</u> <u>Services services" on page 16</u> .	
New Informatica Intelligent Cloud Services IP address	Used to verify your AWS PrivateLink connection. If successful, this address will differ from the original IP address.	

### **Author**

Informatica Cloud Trust Team