How-To Library

Informatica

Microsoft Azure Private Link Onboarding Guide for Informatica Intelligent Cloud Services

Abstract

If you use a Microsoft Azure private virtual network (VNet), you can configure a private connection between your Azure account and Informatica Intelligent Cloud Services using Azure Private Link.

As of the November 2024 release, you can use Azure Private Link with the following services:

- API Manager
- Application Integration
- B2B Gateway
- Cloud Data Integration for PowerCenter (CDI-PC)
- Data Governance and Catalog
- Data Integration, excluding Data Integration Elastic
- Data Marketplace
- Data Profiling
- Data Quality
- Integration Hub
- Data Ingestion and Replication
- Metadata Command Center

Supported Versions

- Informatica Intelligent Cloud Services November 2024

Table of Contents

Overview

If you use a Microsoft Azure private virtual network (VNet), you can configure a private connection between your Azure account and Informatica Intelligent Cloud Services using Azure Private Link.

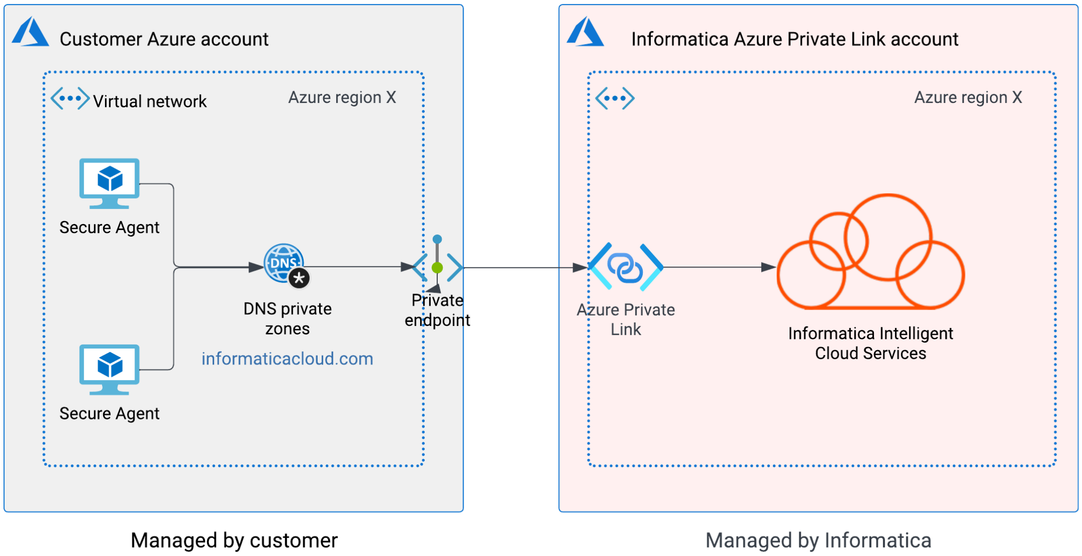
To use Azure Private Link, you must purchase the appropriate SKU through Informatica. Azure Private Link communication works with Intelligent Data Management Cloud instances that are deployed on Microsoft Azure infrastructure

As of the November 2024 release, you can use Azure Private Link with the following services:

- API Manager
- Application Integration
- B2B Gateway
- Cloud Data Integration for PowerCenter (CDI-PC)
- Data Governance and Catalog
- Data Integration, excluding Data Integration Elastic
- Data Marketplace
- Data Profiling
- Data Quality
- Integration Hub
- Data Ingestion and Replication
- Metadata Command Center

When you use Azure Private Link, the Secure Agent in your VNet communicates with Informatica Intelligent Cloud Services securely through Azure Private Link instead of going over the public internet.

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



For all services except Application Integration, communication between Informatica Intelligent Cloud Services and the Secure Agent in your VNet is two-way. For Application Integration, communication is from Application Integration to the Secure Agent only. For more information about using Application Integration with Azure Private Link, see "Using Application Integration with Azure Private Link" on page 18.

To configure Informatica Intelligent Cloud Services to work with Azure Private Link, complete the following steps:

1. Open a support case with Informatica Global Customer Support to request access to Informatica Intelligent Cloud Services using Azure Private Link.
2. Set up an Azure virtual network and subnet if you don't already have one.
3. Create a private endpoint in your Azure account.
4. Create a private DNS zone and link it to your virtual network.
5. Associate the private DNS zone with the private endpoint.
6. Launch a virtual machine (VM) where the Secure Agent will be installed.
7. Install a Secure Agent on the VM.
8. Verify the IP address to ensure that you're connecting to Informatica Intelligent Cloud Services using Azure Private Link.

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

Before you begin

Before you begin, verify that you have an Azure account with an active subscription. You'll also need to note the IP address that you use to connect to Informatica Intelligent Cloud Services over the public internet.

If you don't have an Azure account, you can create one for free.

You'll also need to note the IP address that you use to connect to Informatica Intelligent Cloud Services. When you finish configuring an Azure Private Link connection, you'll need to verify that this IP address differs from the one you use to connect to Informatica Intelligent Cloud Services using Azure Private Link.

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

For example, if your Informatica Intelligent Cloud Services login URL is `https://dm1-us.informaticacloud.com/identity-service/home`, use the following command to ping Informatica Intelligent Cloud Services:

```
ping dm1-us.informaticacloud.com
```

The command returns output like the following example:

```
Pinging dm1-us.informaticacloud.com [40.12.34.567] with 32 bytes of data:
Reply from 40.12.34.567: bytes=32 time=58ms TTL=111
Reply from 40.12.34.567: bytes=32 time=41ms TTL=111
Reply from 40.12.34.567: bytes=32 time=39ms TTL=111
Reply from 40.12.34.567: bytes=32 time=44ms TTL=111

Ping statistics for 40.12.34.567:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 58ms, Average = 45ms
```

The IP address is the value within the square brackets. You can record this value in "Appendix B: Worksheet for setting up Azure Private Link" 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 Azure Private Link. Informatica Global Customer Support will provide you with the resource ID and target sub-resource 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 Azure Private Link. Provide the following information in your support case:
   - Your Informatica Intelligent Cloud Services organization ID.
   - Your Azure region.

     For more information about finding your Azure region, see Find or change your organization region in the Azure documentation.

   You can record these values in "Appendix B: Worksheet for setting up Azure Private Link" on page 24.
2. Wait for Informatica to respond to your request.

   You should receive a response within two business days.

When Informatica responds to your request, we'll provide you with the resource ID and target sub-resource for your POD and region. You can record these values in "Appendix B: Worksheet for setting up Azure Private Link" on page 24. We'll also enable the appropriate license for your organization.

Step 2. Set up a virtual network and subnet

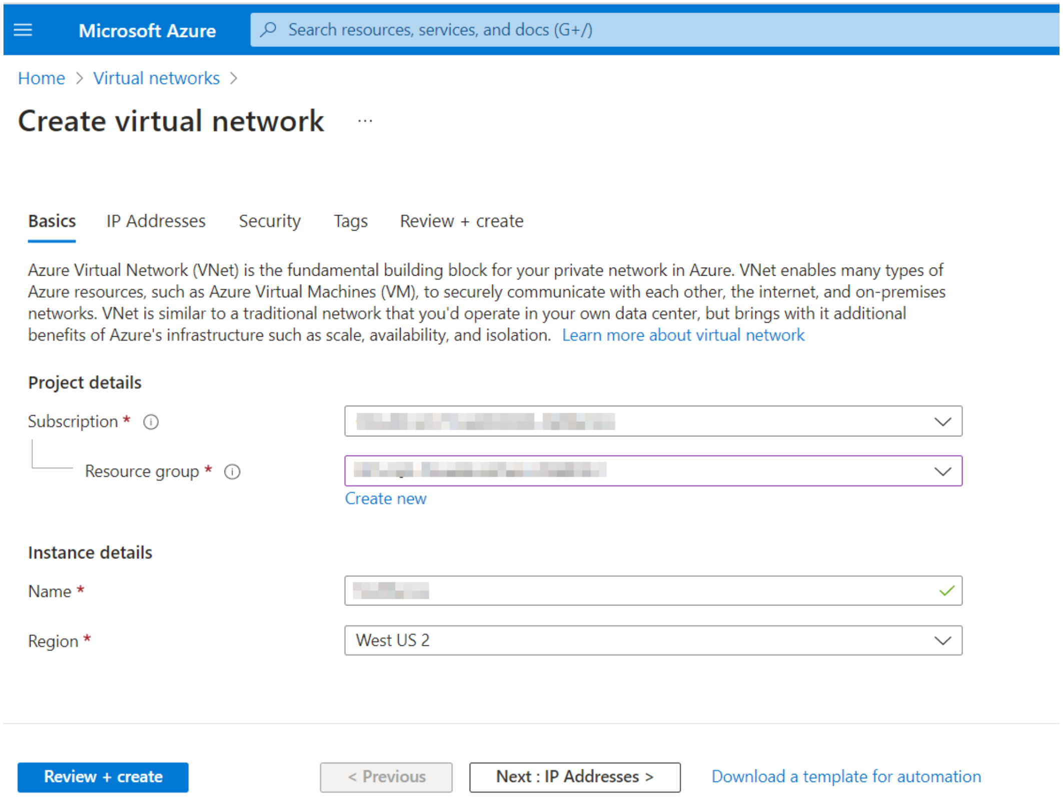
If you don't already have a VNet and subnet that you'll use to connect to Informatica Intelligent Cloud Services, you'll need to set one up. Your VNet will contain the virtual machines (VMs) that host the Secure Agent.

If you plan to use an existing VNet to connect to Informatica Intelligent Cloud Services, you can skip this step and go to "Step 3. Create a private endpoint" on page 6.

1. Sign in to the Azure portal.
2. In the portal, search for and select **Virtual networks**.
3. On the **Virtual networks** page, select **Create**.
4. On the **Basics** tab of the **Create virtual network** screen, enter or select the following values:

Property	Value
Subscription	Select your subscription.
Resource group	Select the resource group or create a new one. The resource group you choose should have the Network Contributor role assigned so that you can create resources in this group.

Property	Value
Name	Enter a name for the VNet.
Region	Select your region. The region should be the same as your Informatica Intelligent Cloud Services region.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual networks >
Create virtual network ...
Basics
IP Addresses
Security
Tags
Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network

Project details

Subscription * : [redacted]

Resource group * : [redacted]

Create new

Instance details

Name * : [redacted]

Region * : West US 2

5. Click **Next: IP Addresses**.
6. Select a subnet.

   If a subnet is not available, on the **IP Addresses** tab, click **+ Add subnet** and enter the subnet name and IP address range.
7. Click **Review + create**.
8. Click **Create**.

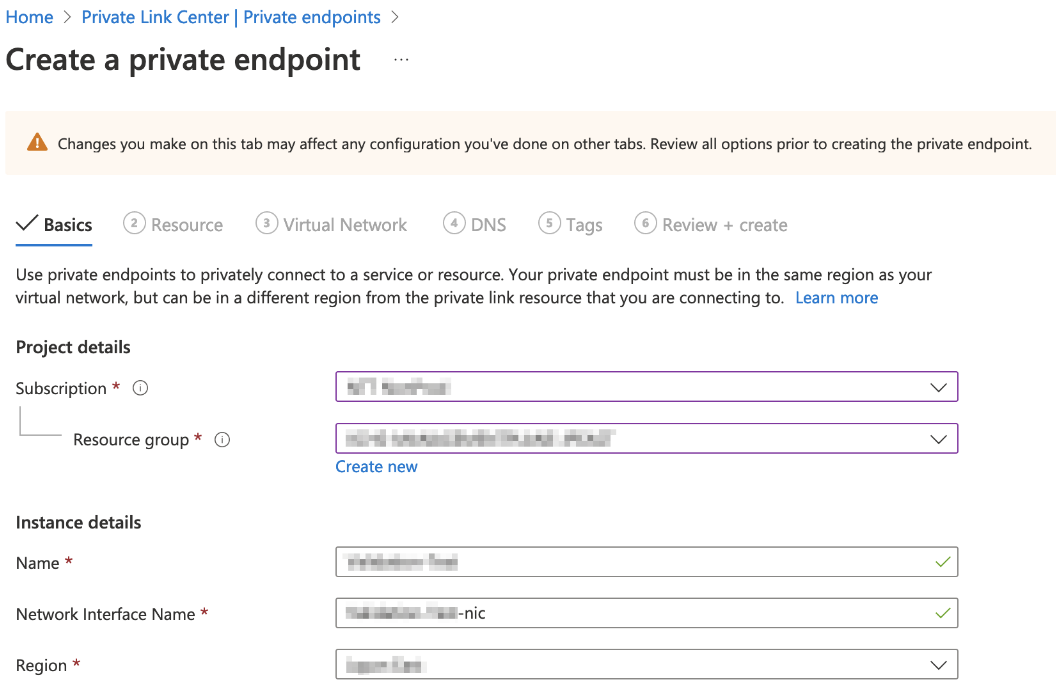
Step 3. Create a private endpoint

After you've created your VNet and subnet, create a private endpoint. A private endpoint is a network interface that uses a private IP address from your VNet. You connect privately and securely to Informatica Intelligent Cloud Services through the private endpoint that you create.

1. Sign in to the Azure portal.
2. In the search box at the top of the portal, search for and select **Private endpoints**.
3. On the **Private endpoints** page, select **+ Create**.

4. On the **Basics** tab of the **Create a private endpoint** screen, enter or select the following values:

Property	Value
Subscription	Select your subscription.
Resource group	Select the resource group. This is the same resource group that you selected when you created the VNet.
Name	Enter a name for the private endpoint.
Network interface name	Enter a network interface name.
Region	Select the region where your VNet is located.



Create a private endpoint ...

⚠ Changes you make on this tab may affect any configuration you've done on other tabs. Review all options prior to creating the private endpoint.

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. Learn more

Project details

Subscription * ⓘ [redacted]

Resource group * ⓘ [redacted]

Instance details

Name * [redacted] ✓

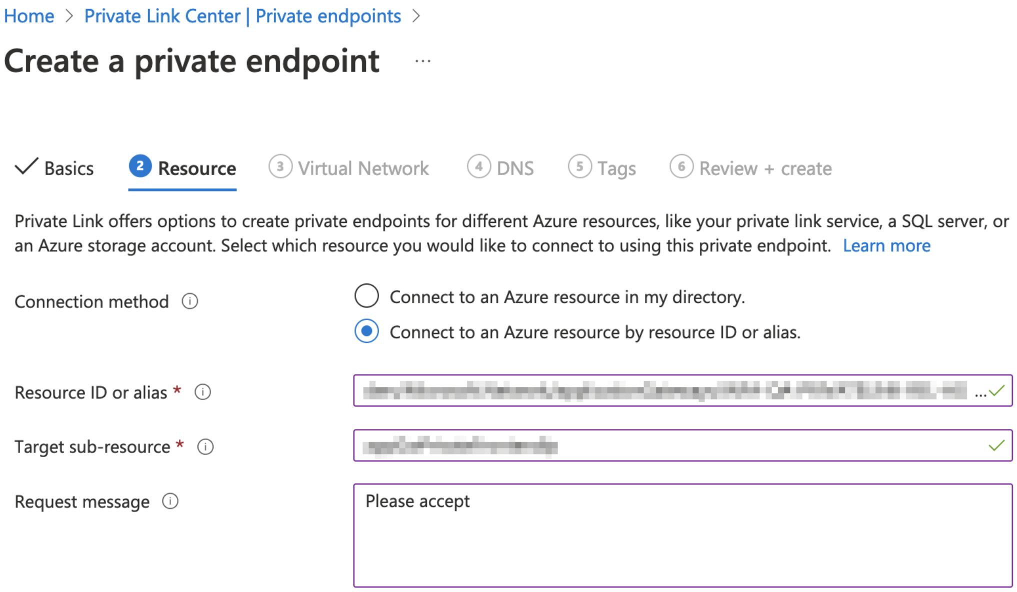
Network Interface Name * [redacted]-nic ✓

Region * [redacted]

5. Click **Next: Resource**.
6. On the **Resource** tab, enter or select the following values:

Property	Value
Connection method	Select **Connect to an Azure resource by resource ID or alias**.
Resource ID or alias	Enter the resource ID that you received from Informatica.

Property	Value
Target sub-resource	Enter the target sub-resource that you received from Informatica.
Request message	Enter a message like, "We'd like to use this endpoint to connect to IICS through Azure Private Link." Include your customer name and organization ID in the message.



Create a private endpoint ...

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. Learn more

Connection method ⓘ
○ Connect to an Azure resource in my directory.
● Connect to an Azure resource by resource ID or alias.

Resource ID or alias * ⓘ [redacted] ...✓

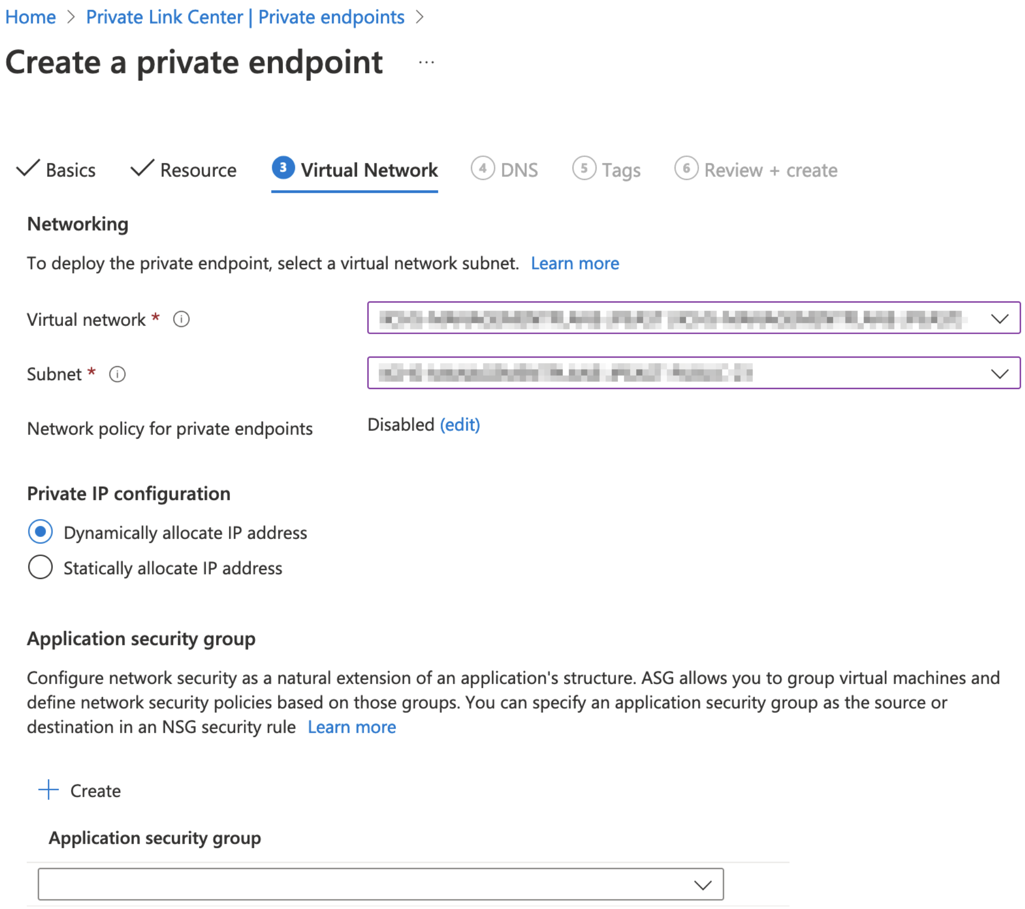
Target sub-resource * ⓘ [redacted] ✓

Request message ⓘ Please accept

7. Click **Next: Virtual Network**.
8. On the **Virtual Network** tab, enter or select the following values:

Property	Value
Virtual network	Select your VNet.
Subnet	Select your subnet.

Property	Value
Network policy for private endpoints	Accept the default value (**Disabled**).
Private IP configuration	Select **Dynamically allocate IP address**.



Home > Private Link Center | Private endpoints >

Create a private endpoint ...

✓ Basics ✓ Resource ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. Learn more

Virtual network * ⓘ [redacted]

Subnet * ⓘ [redacted]

Network policy for private endpoints Disabled (edit)

Private IP configuration

● Dynamically allocate IP address

○ Statically allocate IP address

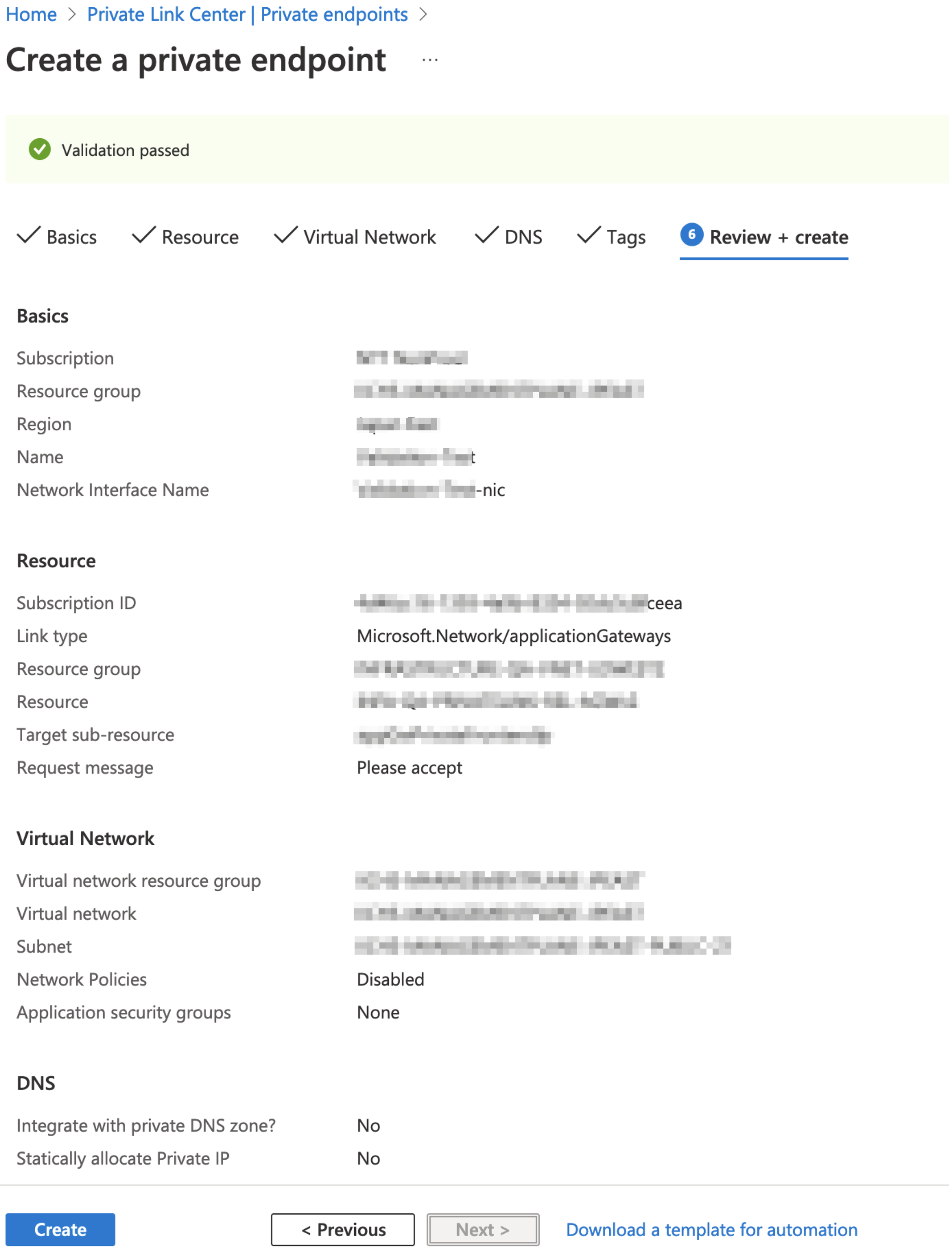
Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule Learn more

Application security group

9. Click **Next: DNS** and accept the default values.
10. Click **Next: Tags** and, optionally, add tags.

11. Click **Next: Review + create**.



Home > Private Link Center | Private endpoints >

Create a private endpoint ...

✓ Validation passed

✓ Basics ✓ Resource ✓ Virtual Network ✓ DNS ✓ Tags 6 Review + create

Basics

Subscription	[redacted]
Resource group	[redacted]
Region	[redacted]
Name	[redacted]t
Network Interface Name	[redacted]-nic

Resource

Subscription ID	[redacted]ceea
Link type	Microsoft.Network/applicationGateways
Resource group	[redacted]
Resource	[redacted]
Target sub-resource	[redacted]
Request message	Please accept

Virtual Network

Virtual network resource group	[redacted]
Virtual network	[redacted]
Subnet	[redacted]
Network Policies	Disabled
Application security groups	None

DNS

Integrate with private DNS zone?	No
Statically allocate Private IP	No

12. Click **Create** to create the private endpoint.

13. When the private endpoint has been created, click the **DNS** tab and copy the IP address.

    You can record the IP address in “Appendix B: Worksheet for setting up Azure Private Link” on page 24.

    You'll need the IP address when you create a private DNS zone and link it to your VNet.

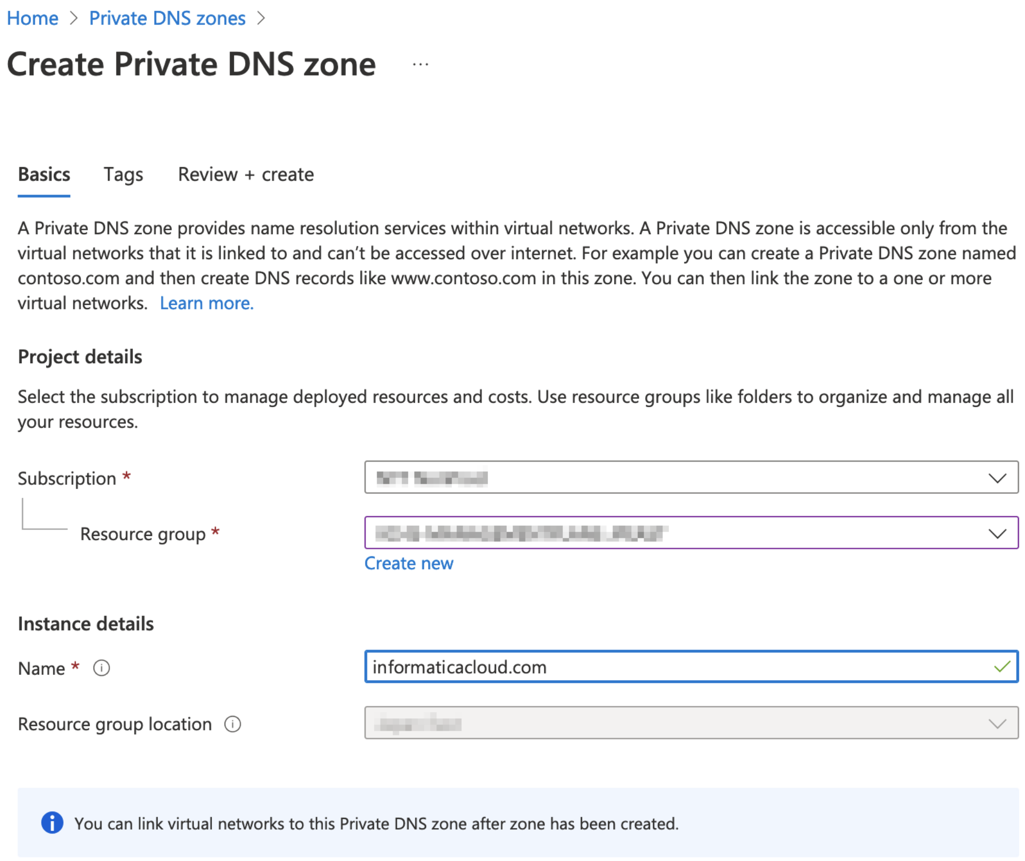
Informatica Global Customer Support will notify you when your request has been approved. Normally, notification takes two business days or less.

Step 4. Create a private DNS zone and link it to your virtual network

After Informatica accepts your endpoint connection request, you'll need to create a private DNS zone and link it to your VNet. A DNS zone contains the DNS entries for a domain. A linked VNet is allowed to resolve records within the DNS zone.

1. In the search box at the top of the Azure portal, search for and select **Private DNS zones**.
2. Select **Create private DNS zone**.
3. On the **Basics** tab of the **Create Private DNS zone** screen, enter or select the following values:

Property	Value
Subscription	Select your subscription.
Resource group	Select the resource group. This is the same resource group that you selected when you created the VNet.
Name	Enter `informaticacloud.com`.



Home > Private DNS zones >

Create Private DNS zone ...

A Private DNS zone provides name resolution services within virtual networks. A Private DNS zone is accessible only from the virtual networks that it is linked to and can't be accessed over internet. For example you can create a Private DNS zone named contoso.com and then create DNS records like www.contoso.com in this zone. You can then link the zone to a one or more virtual networks. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * [redacted]

Resource group * [redacted]

Create new

Instance details

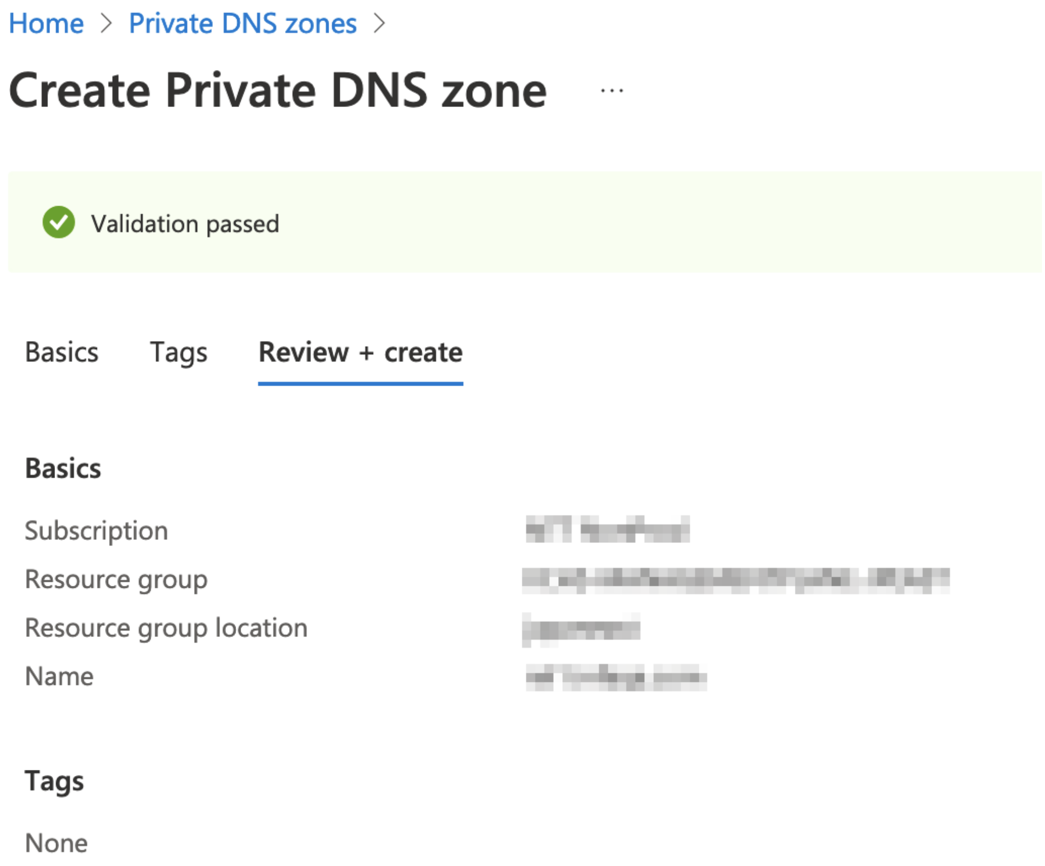
Name * informaticacloud.com

Resource group location [redacted]

You can link virtual networks to this Private DNS zone after zone has been created.

4. For the **Resource group location**, select the same region as your VNet.
5. Click **Next** and optionally add tags.

6. Click **Next**.
7. Click **Review + Create**.



Home > Private DNS zones >

Create Private DNS zone ...

Validation passed

Basics | Tags | Review + create

Basics

Subscription	[redacted]
Resource group	[redacted]
Resource group location	[redacted]
Name	[redacted]

Tags

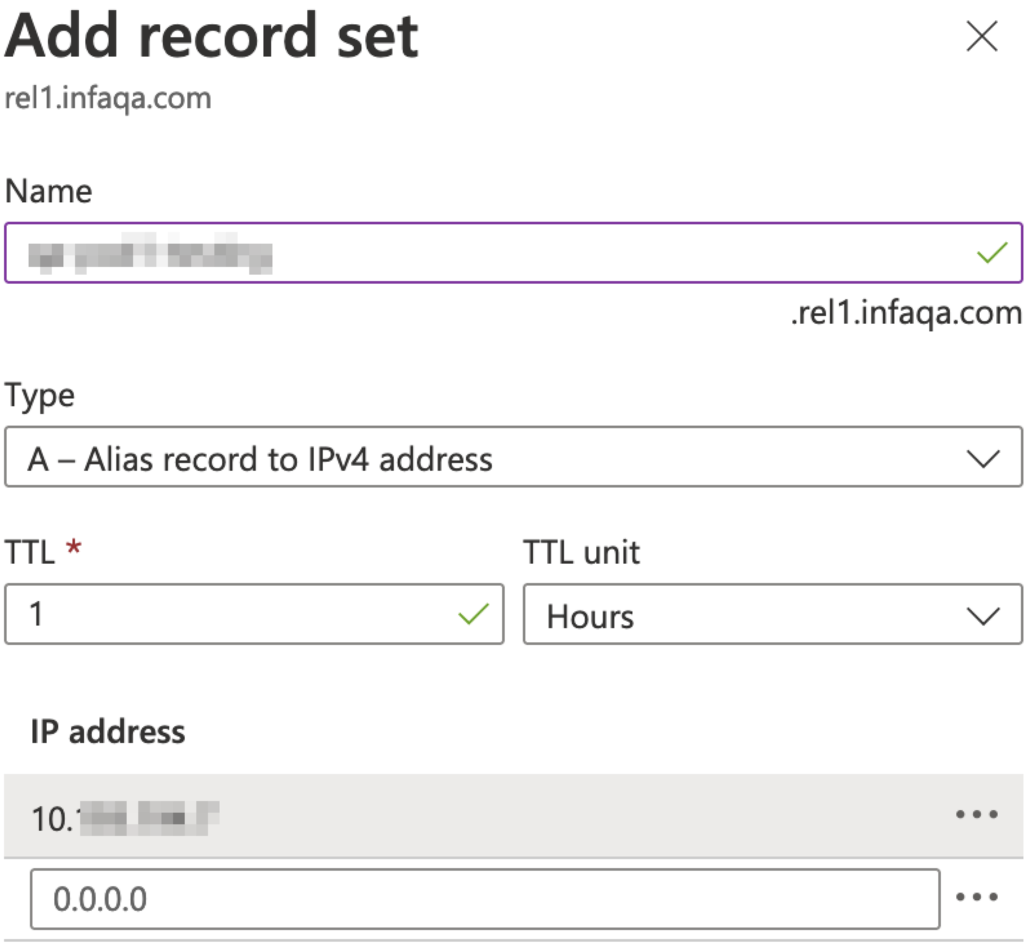
None

8. Click **Create**.

   It might take a few minutes to create the DNS zone.
9. Open the private zone you created and click **+ Record set**.
10. On the **Add record set** page, enter or select the following values:

Property	Value
Name	Enter the DNS name that you use to access the service over the public internet. For information on how to obtain the DNS name for each service, see "Appendix A: DNS names for Informatica Intelligent Cloud Services services" on page 18. You can record the DNS names you need in "Appendix B: Worksheet for setting up Azure Private Link" on page 24.
Type	Select **A - Alias record to IPv4 address**.
TTL	Enter a time-to-live (TTL) of the DNS request or accept the default value.

Property	Value
TTL unit	Select a time unit for the TTL or accept the default value.
IP address	Enter the IP address of the private endpoint. This is the IP address you copied at the end of "Step 3. Create a private endpoint" on page 6.



Add record set

rel1.infaqa.com

Name

[redacted]

.rel1.infaqa.com

Type

A – Alias record to IPv4 address

TTL *

1

TTL unit

Hours

IP address

10.[redacted]

0.0.0.0

11. Click **OK** to create the record.
12. If you use more than one Informatica Intelligent Cloud Services service, repeat steps 9 - 11 for each of the other services.
13. When the records are created, under **Settings**, select **Virtual network links**.
14. Click **Add**.

15. On the **Add virtual network link** page, enter or select the following values:

Property	Value
Link name	Enter a name for the link.
Subscription	Select your subscription.
Virtual network	Select the VNet you created.

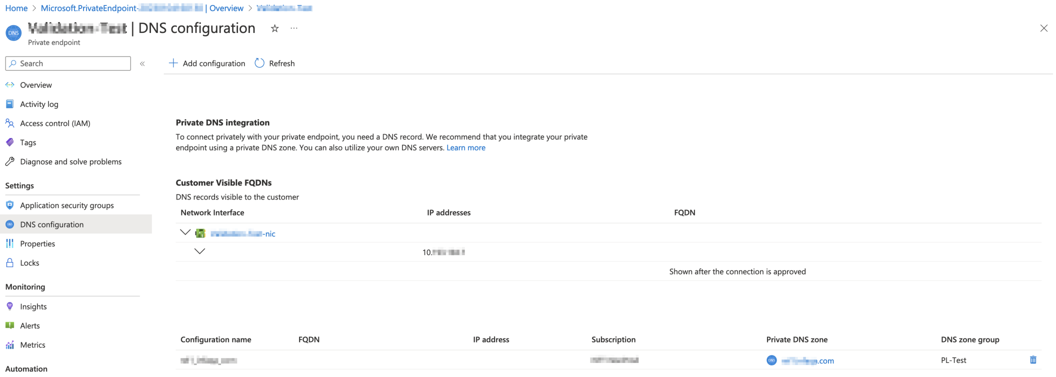
16. Click **OK**.

Step 5. Associate the private DNS zone with the private endpoint

After you link your private DNS zone to your VNet, you'll need to add the DNS zone details to your private endpoint.

1. In the search box at the top of the Azure portal, search for and select **Private endpoints**.
2. Select the private endpoint you created.
3. Under **Settings**, select **DNS configuration**.
4. Click **+ Add configuration**.
5. On the **Add configuration** tab, enter or select the following values:

Property	Value
Configuration name	Enter a configuration name.
Subscription	Select your subscription.
Private DNS zone	Select the private DNS zone you created.
DNS zone group	Select the same group as the DNS zone you already created.



Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint using a private DNS zone. You can also utilize your own DNS servers. Learn more

Customer Visible FQDNs

DNS records visible to the customer

Network Interface	IP addresses	FQDN
[redacted]-nic		
	10.[redacted]	
		Shown after the connection is approved

Configuration name	FQDN	IP address	Subscription	Private DNS zone	DNS zone group
[redacted]			[redacted]	[redacted].com	PL-Test

6. Click **Add**.

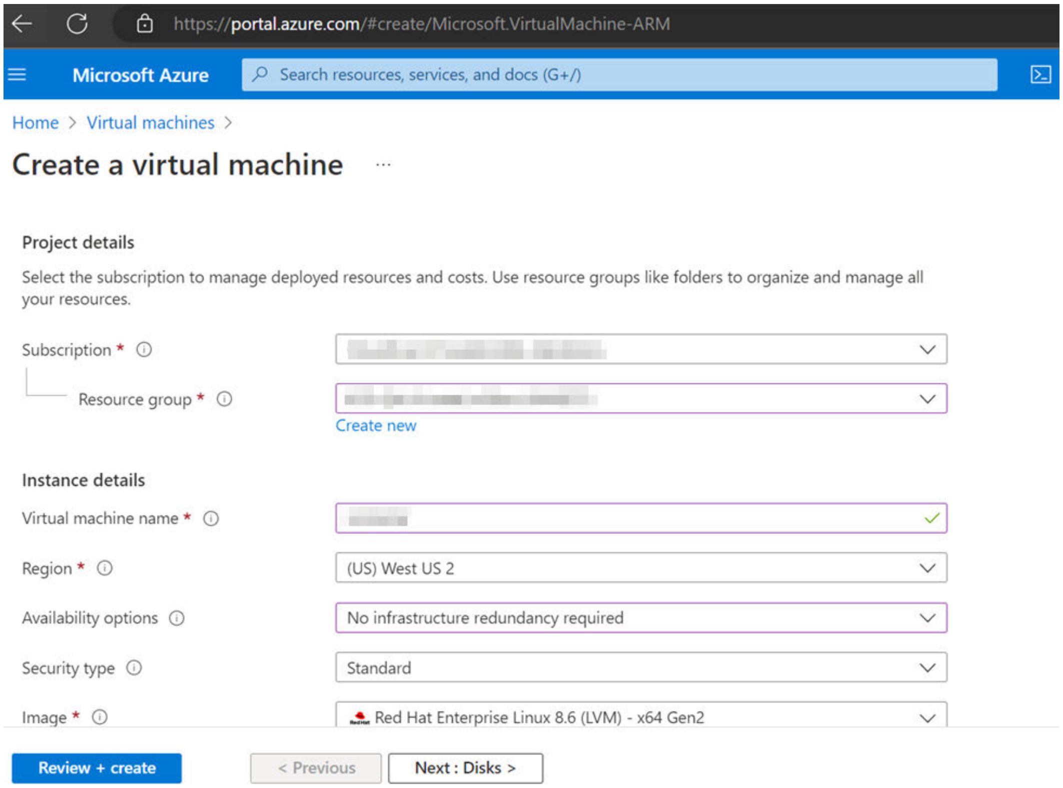
Step 6. Launch a VM where the Secure Agent will be installed

After you create and link the DNS zone, create a VM where you'll install the Secure Agent. Be sure that you create the VM in the same VNet as the private endpoint you created.

1. In the search box at the top of the Azure portal, search for and select **Virtual machines**.
2. On the **Virtual machines** page, click **+ Create**, and select **Azure virtual machine**.
3. On the **Create a virtual machine** screen, enter or select the following values:

Property	Value
Subscription	Select your subscription.
Resource group	Select the resource group. This is the same resource group that you selected when you created the VNet.
Virtual machine name	Enter a name for the VM.
Region	Select the region where your VNet is located.
Availability options	Select **No infrastructure redundancy required**.
Security type	Select the security type you plan to use or accept the default value.
Image	Select the appropriate image type. You can create a Linux or Windows machine.

For the other properties, enter or select the appropriate values according to your usage.


https://portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual machines >

Create a virtual machine

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * [redacted]

Resource group * [redacted]

Instance details

Virtual machine name * [redacted]

Region * (US) West US 2

Availability options No infrastructure redundancy required

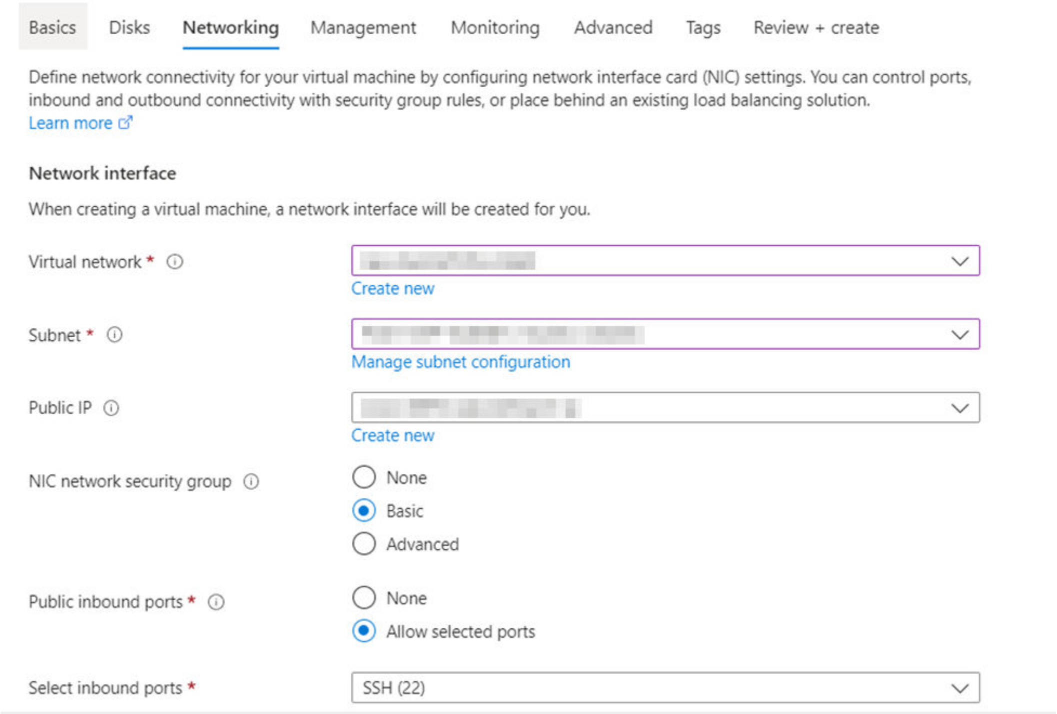
Security type Standard

Image * Red Hat Enterprise Linux 8.6 (LVM) - x64 Gen2

4. Select the **Networking** tab at the top of the page.
5. On the **Networking** page, enter or select the following values:

Property	Value
Virtual network	Select the VNet that you used to when creating the private endpoint.
Subnet	Select the subnet inside the virtual network that you used when creating the private endpoint.

For the other properties, enter or select the appropriate values according to your usage.



Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * [redacted]
Create new

Subnet * [redacted]
Manage subnet configuration

Public IP [redacted]
Create new

NIC network security group
○ None
● Basic
○ Advanced

Public inbound ports *
○ None
● Allow selected ports

Select inbound ports * SSH (22)

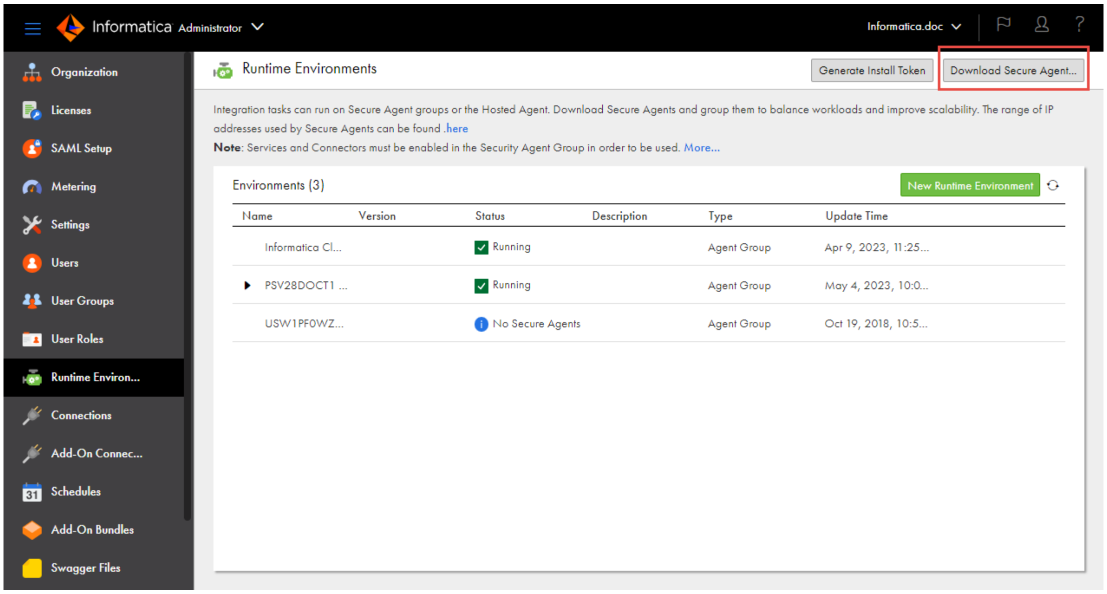
6. Click **Review + create**.
7. Review the settings and then click **Create**.

Once the VM is deployed, you can install a Secure Agent on the machine.

Step 7. Install the Secure Agent on the virtual machine

Download and install a Secure Agent from Informatica Intelligent Cloud Services Administrator. You download the Secure Agent installer on the **Runtime Environments** page.

The following image shows the **Download Secure Agent** button on the **Runtime Environments** page:



Runtime Environments

Integration tasks can run on Secure Agent groups or the Hosted Agent. Download Secure Agents and group them to balance workloads and improve scalability. The range of IP addresses used by Secure Agents can be found .here

Note: Services and Connectors must be enabled in the Security Agent Group in order to be used. More...

Environments (3)

Name	Version	Status	Description	Type	Update Time
Informatica Cl...		✓ Running		Agent Group	Apr 9, 2023, 11:25...
PSV28DOCT1 ...		✓ Running		Agent Group	May 4, 2023, 10:0...
USW1PFOWZ...		ⓘ No Secure Agents		Agent Group	Oct 19, 2018, 10:5...

The steps you perform to install a Secure Agent vary based on whether you are installing the agent onto a Windows or Linux VM:

- To install a Secure Agent onto a Windows VM, see Secure Agent installation on Windows in the Administrator *Runtime Environments* guide.
- To install a Secure Agent onto a Linux VM, see Secure Agent installation on Linux in the Administrator *Runtime Environments* guide.

Step 8. Verify the IP address

To verify that you are using Azure Private Link 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 Azure VNet and use the ping command to verify that the IP address now differs from the one returned in "Before you begin" on page 4.

For example, if your Informatica Intelligent Cloud Services login URL is `https://dm1-us.informaticacloud.com/identity-service/home`, use the following command to ping Informatica Intelligent Cloud Services:

```
ping dm1-us.informaticacloud.com
```

The command returns output like the following example:

```
Pinging dm1-us.informaticacloud.com [10.98.76.543] with 32 bytes of data:
Reply from 10.98.76.543: bytes=32 time=58ms TTL=111
Reply from 10.98.76.543: bytes=32 time=41ms TTL=111
Reply from 10.98.76.543: bytes=32 time=39ms TTL=111
Reply from 10.98.76.543: bytes=32 time=44ms TTL=111

Ping statistics for 10.98.76.543:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 58ms, Average = 45ms
```

The IP address is the value within the square brackets. The new IP address should start with the same numbers as the IP address for your VNet.

Using Application Integration with Azure Private Link

Application Integration supports only one-way communication through Azure Private Link, 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 Azure security group. However, you cannot access Azure resources using an Application Integration service connector or connection.

After you enable a Secure Agent that is installed in an Azure VNet, the agent connects directly to the connection endpoints through Azure Private Link. 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 Azure VNet, 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 APNE1 POD and you use Application Integration (CAI), Data Profiling (CDP), and Data Quality (CDQ), you would allow the following DNS names:

```
dm1-ap.informaticacloud.com
content.dm-ap.informaticacloud.com
global-package.dm.informaticacloud.com
icsdownloadsecure.informatica.com
apne1.dm1-ap.informaticacloud.com
apne1-cai.dm1-ap.informaticacloud.com
apne1-dqprofile.dm1-ap.informaticacloud.com
apne1-dqcloud.dm1-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 Northeast (APNE1)

If your POD is APJ Northeast (apne1), allow the following DNS names:

Service	DNS names
Global Identity Service	dm1-ap.informaticacloud.com content.dm-ap.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	apne1.dm1-ap.informaticacloud.com

If you use any of the following services, allow their DNS names as well:

Service	DNS names
API Manager	apne1-apim.dm1-ap.informaticacloud.com apne1-apigw.dm1-ap.informaticacloud.com
Application Integration (CAI)	apne1-cai.dm1-ap.informaticacloud.com
Application Integration (Salesforce)	apne1-sfdc-cai.dm1-ap.informaticacloud.com
B2B Gateway	apne1-b2bgw.dm1-ap.informaticacloud.com
Data Profiling (CDP)	apne1-dqprofile.dm1-ap.informaticacloud.com
Integration Hub (CIH)	apne1-cih.dm1-ap.informaticacloud.com
Data Ingestion and Replication	apne1-ing.dm1-ap.informaticacloud.com

Asia/Pacific/Japan Southeast (APSE2)

If your POD is APSE2, allow the following DNS names:

Service	DNS names
Global Identity Service	dm1-apse.informaticacloud.com content.dm-ap.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	apse1.dm1-apse.informaticacloud.com

If you use any of the following services, enter their DNS names as well:

Service	DNS names
API Manager	`apse1-apim.dm1-apse.informaticacloud.com` `apse1-apigw.dm1-apse.informaticacloud.com`
Application Integration (CAI)	`apse1-cai.dm1-apse.informaticacloud.com`
Application Integration (Salesforce)	`apse1-sfdc-cai.dm1-apse.informaticacloud.com`
B2B Gateway	`apse1-b2bgw.dm1-apse.informaticacloud.com`
Cloud Data Integration for PowerCenter (CDI-PC)	`apse1-idms.dm1-apse.informaticacloud.com`

Data Governance and Catalog, Data Marketplace, and Metadata Command Center	`cdgc.dm1-apse.informaticacloud.com`
	`cdmp-app.dm1-apse.informaticacloud.com`
	`mcc.dm1-apse.informaticacloud.com`

Data Profiling (CDP)	`apse1-dqprofile.dm1-apse.informaticacloud.com`
Integration Hub (CIH)	`apse1-cih.dm1-apse.informaticacloud.com`
Data Ingestion and Replication	`apse1-ing.dm1-apse.informaticacloud.com`

European Union (EMC1)

If your POD is EMC1, allow the following DNS names:

Service	DNS names
Global Identity Service	`dm1-em.informaticacloud.com` `content.dm-ap.informaticacloud.com`
Global Package Delivery Manager	`global-package.dm.informaticacloud.com` `icsdownloadsecure.informatica.com`
Data Integration (CDI)	`emc1.dm1-em.informaticacloud.com`

If you use any of the following services, allow their DNS names as well:

Service	DNS names
API Manager	`emc1-apim.dm1-em.informaticacloud.com` `emc1-apigw.dm1-em.informaticacloud.com`
Application Integration (CAI)	`emc1-cai.dm1-em.informaticacloud.com`
Application Integration (Salesforce)	`emc1-sfdc-cai.dm1-em.informaticacloud.com`
B2B Gateway	`emc1-b2bgw.dm-em.informaticacloud.com`

Service	DNS names
Cloud Data Integration for PowerCenter (CDI-PC)	`emc1-idms.dm1-em.informaticacloud.com`

Data Governance and Catalog, Data Marketplace, and Metadata Command Center	`cdgc-api.dm1-em.informaticacloud.com`
	`cdgc.dm1-em.informaticacloud.com`
	`cdmp-app.dm1-em.informaticacloud.com`
	`icd-app.dm1-em.informaticacloud.com`
	`idmc-api.dm1-em.informaticacloud.com`
	`idmcp-api.dm1-em.informaticacloud.com`
	`idmcp-mgmt.dm1-em.informaticacloud.com`
	`mcc.dm1-em.informaticacloud.com`

Data Profiling (CDP)	`emc1-dqprofile.dm1-em.informaticacloud.com`
Integration Hub (CIH)	`emc1-cih.dm1-em.informaticacloud.com`
Data Ingestion and Replication	`emc1-ing.dm1-em.informaticacloud.com`

European Union (EMSE1)

If your POD is EMSE1, allow the following DNS names:

Service	DNS names
Global Identity Service	`dm1-emse.informaticacloud.com` `content.dm-ap.informaticacloud.com`
Global Package Delivery Manager	`global-package.dm.informaticacloud.com` `icsdownloadsecure.informatica.com`
Data Integration (CDI)	`emse1.dm1-emse.informaticacloud.com`

If you use any of the following services, allow their DNS names as well:

Service	DNS names
API Manager	`emse1-apim.dm1-emse.informaticacloud.com` `emse1-apigw.dm1-emse.informaticacloud.com`
Application Integration (CAI)	`emse1-cai.dm1-emse.informaticacloud.com`
Application Integration (Salesforce)	`emse1-sfdc-cai.dm1-emse.informaticacloud.com`
B2B Gateway	`emse1-b2bgw.dm1-emse.informaticacloud.com`
Cloud Data Integration for PowerCenter (CDI-PC)	`emse1-idms.dm1-emse.informaticacloud.com`

Service	DNS names
Data Governance and Catalog, Data Marketplace, and Metadata Command Center	cdgc-api.dm1-emse.informaticacloud.com cdgc.dm1-emse.informaticacloud.com cdmp-app.dm1-emse.informaticacloud.com idmc-api.dm1-emse.informaticacloud.com idmcp-api.dm1-emse.informaticacloud.com idmcp-mgmt.dm1-emse.informaticacloud.com mcc.dm1-emse.informaticacloud.com
Data Profiling (CDP)	emse1-dqprofile.dm1-emse.informaticacloud.com
Integration Hub (CIH)	emse1-cih.dm1-emse.informaticacloud.com
Data Ingestion and Replication	emse1-ing.dm1-emse.informaticacloud.com

United States West 1 (USW1-1)

If your POD is USW1-1, allow the following DNS names:

Service	DNS names
Global Identity Service	dm1-us.informaticacloud.com content.dm-ap.informaticacloud.com
Global Package Delivery Manager	global-package.dm.informaticacloud.com icsdownloadsecure.informatica.com
Data Integration (CDI)	usw1.dm1-us.informaticacloud.com

If you use any of the following services, allow their DNS names as well:

Service	DNS names
API Manager	usw1-apim.dm1-us.informaticacloud.com usw1-apigw.dm1-us.informaticacloud.com
Application Integration (CAI)	usw1-cai.dm1-us.informaticacloud.com
Application Integration (Salesforce)	usw1-sfdc-cai.dm1-us.informaticacloud.com
B2B Gateway	usw1-b2bgw.dm1-us.informaticacloud.com
Cloud Data Integration for PowerCenter (CDI-PC)	usw1-idms.dm1-us.informaticacloud.com
Data Governance and Catalog, Data Marketplace, and Metadata Command Center	cdgc-api.dm1-us.informaticacloud.com cdgc.dm1-us.informaticacloud.com cdmp-app.dm1-us.informaticacloud.com idmc-api.dm1-us.informaticacloud.com idmcp-api.dm1-us.informaticacloud.com idmcp-mgmt.dm1-us.informaticacloud.com mcc.dm1-us.informaticacloud.com

Service	DNS names
Data Profiling (CDP)	`usw1-dqprofile.dm1-us.informaticacloud.com`
Integration Hub (CIH)	`usw1-cih.dm1-us.informaticacloud.com`
Data Ingestion and Replication	`usw1-ing.dm1-us.informaticacloud.com`

United States West 3 (USW3-1)

If your POD is USW3-1, enter the following DNS names:

Service	DNS names
Global Identity Service	`dm1-us.informaticacloud.com` `content.dm-ap.informaticacloud.com`
Global Package Delivery Manager	`global-package.dm.informaticacloud.com` `icsdownloadsecure.informatica.com`
Data Integration (CDI)	`usw3.dm1-us.informaticacloud.com`

If you use any of the following services, allow their DNS names as well:

Service	DNS names
API Manager	`usw3-apim.dm1-us.informaticacloud.com` `usw3-apigw.dm1-us.informaticacloud.com`
Application Integration (CAI)	`usw3-cai.dm1-us.informaticacloud.com`
Application Integration (Salesforce)	`usw3-sfdc-cai.dm1-us.informaticacloud.com`
B2B Gateway	`usw3-b2bgw.dm1-us.informaticacloud.com`
Cloud Data Integration for PowerCenter (CDI-PC)	`usw3-idms.dm1-us.informaticacloud.com`

Data Governance and Catalog, Data Marketplace, and Metadata Command Center	`cdgc-api.dm1-us.informaticacloud.com`
	`cdgc.dm1-us.informaticacloud.com`
	`cdmp-app.dm1-us.informaticacloud.com`
	`idmc-api.dm1-us.informaticacloud.com`
	`idmcp-api.dm1-us.informaticacloud.com`
	`idmcp-mgmt.dm1-us.informaticacloud.com`
	`mcc.dm1-us.informaticacloud.com`

Data Profiling (CDP)	`usw3-dqprofile.dm1-us.informaticacloud.com`
Integration Hub (CIH)	`usw3-cih.dm1-us.informaticacloud.com`
Data Ingestion and Replication	`usw3-ing.dm1-us.informaticacloud.com`

Appendix B: Worksheet for setting up Azure Private Link

Use the following worksheet to record the information that you need to configure Informatica Intelligent Cloud Services to work with Azure Private Link.

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 Azure Private Link connection.	
Informatica Intelligent Cloud Services organization ID	Needed by Informatica Global Customer Support.	
Azure region	Needed by Informatica Global Customer Support.	
Resource ID that you received from Informatica	Needed to create your private endpoint.	
Target sub-resource that you received from Informatica	Needed to create your private endpoint.	
IP address for the private endpoint	Needed to create records in the private DNS zone for your Informatica Intelligent Cloud Services services.	
DNS names for the Informatica Intelligent Cloud Services services for which you want to create an Azure Private Link connection	Needed to create records in the private DNS zone for your Informatica Intelligent Cloud Services services. To find the DNS names, see "Appendix A: DNS names for Informatica Intelligent Cloud Services services" on page 18.	
New Informatica Intelligent Cloud Services IP address	Used to verify your Azure Private Link connection. If successful, this address will differ from the original IP address.	

Author

Informatica Cloud Trust Team