Azure Private Link for Azure Data Factory

Private Link allows you to connect to various PaaS services in Azure via a **private endpoint**. For a list of PaaS services that support Private Link functionality, go to the [Private Link Documentation](#) page. A private endpoint is a private IP address within a specific **VNet** and subnet.

**Secure communication between customer network and Azure Data Factory service**

To protect your Azure resources from attacks in public network or let them securely communicate with each other, you can setup an Azure Virtual Network (VNET) as a logical representation of your network in the cloud. You can also connect an on-premises network to your VNET by setting up IPSec VPN (site-to-site) or ExpressRoute (private peering). The Self-hosted Integration Runtime can be installed on an on premise machine or virtual machine in Virtual Network to run copy activities between a cloud data store and a data store in a private network or dispatch transform activities against compute resources in an on-premises network or an Azure virtual network.

There are several communication channels required between Data Factory and customer VNET.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.{region}.datafactory.azure.net</td>
<td>443</td>
<td>Required by the Self-hosted Integration Runtime to connect to the Data Factory service.</td>
</tr>
<tr>
<td>*.servicebus.windows.net</td>
<td>443</td>
<td>Required by the Self-hosted Integration Runtime for Interactive Authoring.</td>
</tr>
<tr>
<td>download.microsoft.com</td>
<td>443</td>
<td>Required by the Self-hosted Integration Runtime for downloading the updates.</td>
</tr>
</tbody>
</table>

With the support of Azure Private Link for Azure Data Factory, you can create a Private Endpoint (PE) in your VNET and enable the private connection to specific Azure Data Factory. The communications to Azure Data Factory service go through Azure Private Link which provides secured private connectivity. And you don’t need to configure above domain and port in VNET or your corporate firewall which provide a more secure way to protect your resources.
Here are the benefits for enabling Private Link Service for each of the communication channels depicted above:

1. (Supported) You can do authoring and monitoring of Azure Data Factory in your VNET even you block all outbound communications.
2. (Supported) The command communications between Self-hosted Integration Runtime and Azure Data Factory service can be performed securely in a private network environment. The traffic between Self-hosted Integration Runtime and Azure Data Factory service goes through Private Link.
3. (To be enabled) Interactive authoring using Self-hosted Integration Runtime go through Private Link such as test connection, browse folder list and table list, get schema and preview data.
4. (To be enabled) The new version of Self-hosted Integration Runtime can be automatically downloaded from the download center if you enable auto-update.

Note: We currently support item 1 and 2. For item 3 and 4, you still need to configure above domain and port in VNET or your corporate firewall. The support of item 3 and 4 are coming soon.

Warning: When you create Linked Service, please make sure the credential is stored in Azure Key Vault. Otherwise it doesn't work when you enable Private Link Service in Azure Data Factory.

How to set up Private Link for Azure Data Factory

Private Endpoints can be created using the Azure portal, PowerShell, or the Azure CLI:
The portal

You can also navigate to your Azure Data Factory in Azure portal and create Private Endpoint (PE):

If you want to block public access to this Azure Data Factory and only allow access through Private Link, you can disable network access of Azure Data Factory in Azure Portal:

Note: Disabling public network access is only applicable to Self-hosted Integration Runtime, not to Azure Integration Runtime and SSIS Integration Runtime.

Note: Users can still access ADF Portal through public network after disabling public network access.