Hybrid Distribution

JFrog Subscription Levels

CLOUD (SaaS)

ENTERPRISE+

Page Contents

Overview

Hybrid Distribution as part of JFrog Platform on the cloud, supports the distribution of your Release Bundles from JFrog Distribution on the cloud to multiple Cloud and On-Prem Edge nodes within the same organisation. Enterprise customers can develop their software using the JFrog Platform on the cloud while gaining the flexibility of consuming the software on the Cloud and On-Prem.

Hybrid Distribution supports:

- Balancing your distribution workloads in response to changing workloads, new challenges, and increasing security requirements.
- Distributing sensitive, highly regulated, and mission critical Release Bundles to Artifactory On-Prem Edges while using the JFrog Platform on the cloud for mainstream public distributions and thereby gaining significant cost savings.

⚠ **WebUI Changes implemented in Artifactory 7.38.x and above**

- **Identify & Access** is now called **User Management**.
- **Platform Deployments** is now called **Platform Management**.

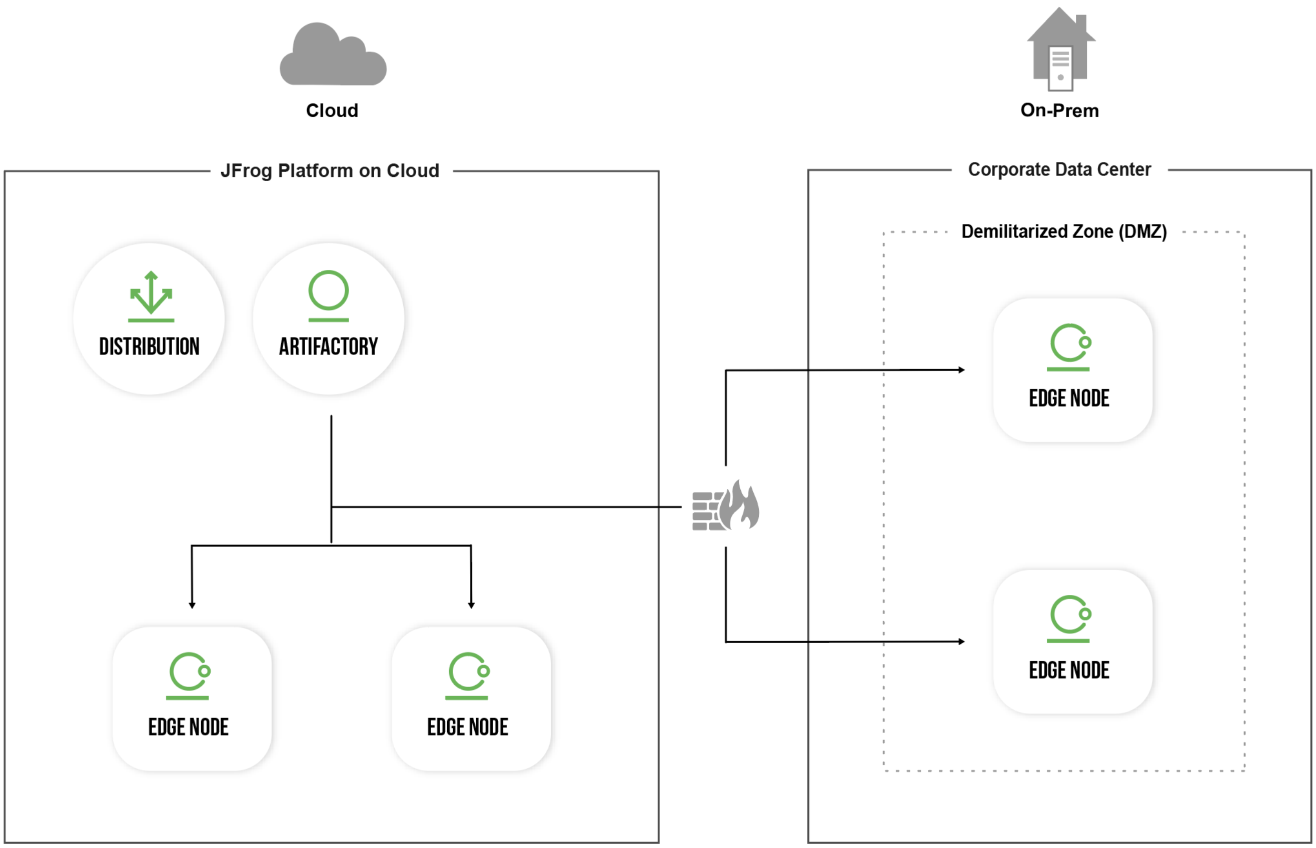
All the relevant text and images on this page have been updated to reflect this change.

Hybrid Environment Requirements

The Artifactory On-Prem Edge node within the JFrog Platform on the cloud is commonly located within the corporate network protected by a firewall. Within your corporate network, you can choose to set up the On-Prem Edge within a DMZ (Demilitarized Zone) or alternatively build a VPN tunnel or using any other secure method.

⚠ **Enable Ingress Traffic for Hybrid Distribution**

The JFrog distribution process requires enabling ingress communication between the JFrog Platform on the cloud and Artifactory On-Prem Edge nodes. Please ensure that your corporate firewall is configured to accept this type of traffic.



Setting up Hybrid Cloud Distribution

The workflow for adding the an Artifactory On-Prem Edge Node to the JFrog SaaS environment includes:

1. Install an Artifactory On-Prem Edge node and register your Artifactory Edge node in the SaaS cluster as a “Platform Deployment”.
2. Establish trust between the source Artifactory and the Edge nodes.

Prerequisites

1. Set up your JFrog Platform on the cloud. For more information, see JFrog Cloud.
2. Artifactory Edge node requires a valid license. The license for on-premises Artifactory Edge node is allocated using Bucket License mechanism.
   a. Obtain a License Bucket.
      Once your license bucket is created, you will receive an email with a link to a dedicated web page.
   b. Add the License Bucket in the JFrog Platform on the cloud by navigating to **Administration module | Licenses| License Buckets**, and click **Add New Bucket**. For more information, see Adding a License Bucket.

Step 1: Set up and Connect the On-Prem Artifactory Edge Node to the SaaS Artifactory Instance

> ⚠ **WebUI Changes implemented in Artifactory 7.38.x and above**
>
> **Platform Deployments** is now called **Platform Management**.

1. Install the Artifactory Edge Node.
2. Register your Edge node as a JFrog Platform Deployment (JPD) in **Administration module | Platform Management | Registered JPDs** of your SaaS Artifactory instance. For more information, see Managing Platform Deployments.
3. Optional: Attach a license from the license bucket on SaaS Artifactory instance to the Edge node via **Administration module | Licenses | License Buckets**. For more information, see Attaching Licenses.

Step 2: Establish a Secure Connection for Distribution Between the Source Artifactory and the Artifactory Edge Nodes

Use one of the following methods to connect Artifactory and the Edge nodes.

> ⚠ **WebUI Changes implemented in Artifactory 7.38.x and above**
>
> **Identify & Access** is now called **User Management**.

Using a Pairing Token

From Artifactory version 7.29.7, the recommended method for connecting between the source Artifactory and the Artifactory Edge nodes is the *pairing token*.

1. In the **Administration** tab, go to **User Management | Access Tokens | Pairing Token**.
2. In the Generate Pairing Token for field, select the purpose of the pairing token.
3. Click **Generate** to generate the token.
   This displays the token window, which includes the token's expiration (in seconds, set by default to 300 seconds = 5 minutes), the token ID, and the actual token, which you can copy by clicking **Copy**.

Using the Scoped Tokens API (Manual)

Creating a connection using the scoped token API, requires generating a token on the Edge node that is scoped for Distribution, and then providing that token to the SaaS Artifactory. To do this you will need to the following.

1. Generate a scoped token using the REST API Create Token call.
   For example:

   ```
   curl -X POST http://localhost:8084/access/api/v1/service_trust/pairing/mission-control -H
   "Authorization: Bearer $TOKEN"
   ```

2. Copy the token.
3. Upload the token to the SaaS instance using the REST API.

Establishing a Circle of Trust

Establish trust between servers by establishing a "Circle of Trust" between the SaaS environment and the On-Prem Artifactory Edge node. To do that you will need to do the following:

1. Make the Edge node trust the Artifactory SaaS instance by doing the following:
   a. Obtain the `root.crt` from the Artifactory SaaS instance by running the Get Root Certificate REST API against the SaaS instance.
   b. Set the `root.cert` received in step 1 above as the trusted certificate in each Edge node by copying the service's root certificate to the new Edge service's **`$JFROG_HOME`**`/artifactory/var/etc/access/keys/trusted` folder.
2. Next, make the Artifactory SaaS instance trust the Edge node by doing the following:
   a. Obtain the `root.crt` from the Edge nodes by running the Get Root Certificate REST API against each Edge.
   b. To add the `root.cert` from the Edges, open a support request to copy the root certificate from step 2a to your SaaS instance.

> ⚠ From release 7.29.7, paired tokens are the default option used for connecting the source and node. If you are unable to upgrade your self-hosted instance, or need to continue using the circle of trust, refer to the explanation above.