Optional Palantir Components

You can include a number of optional components in deployments of the Palantir Platform. These optional components include:

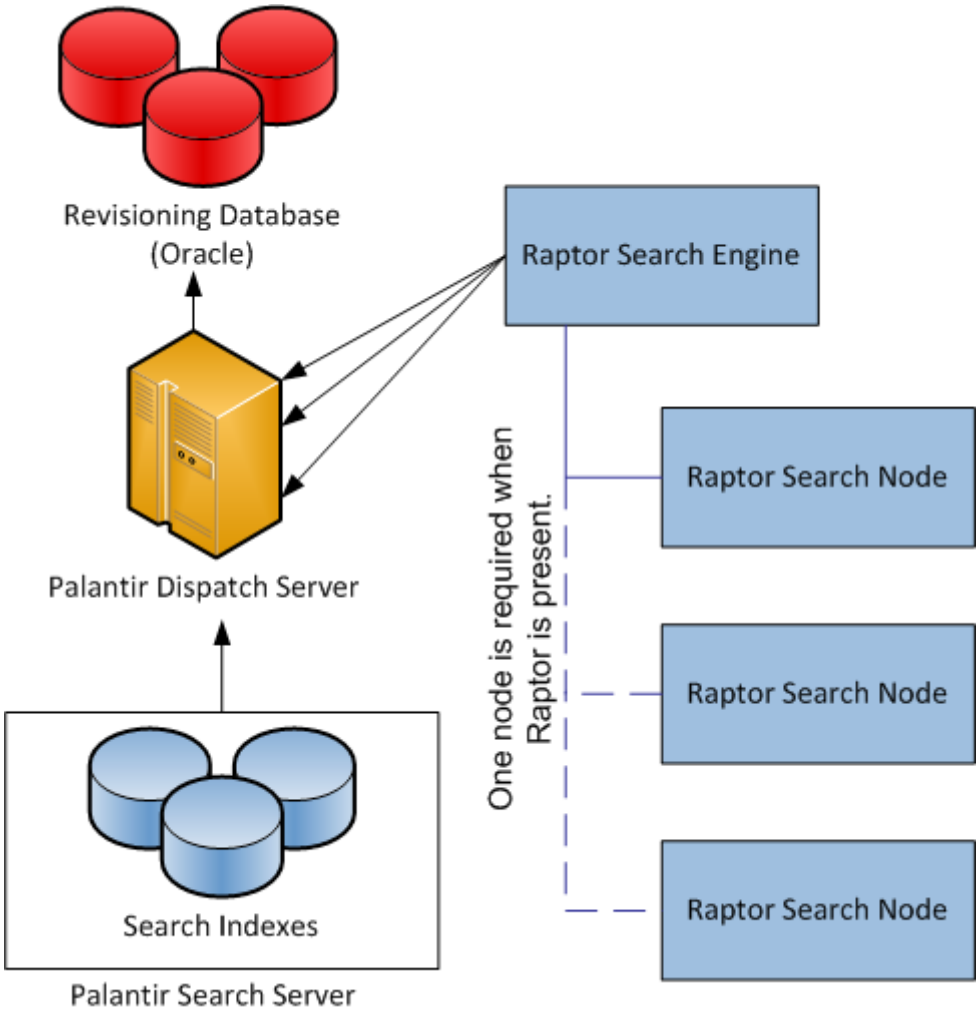
- Raptor Search Engine
- Monitoring Server
- Authentication Server
- Extraction Integration Server
- Palantir Web
- Palantir Phoenix

Raptor Search Engine

The Palantir architecture supports federated searches through the Raptor Search Engine. Raptor complements, but does not replace, the searching capability provided by the core Search Server. Raptor can search and analyze data that resides in external data sources without duplicating the data within the Palantir Platform.

The following diagram illustrates the architecture of the Raptor Search Engine.

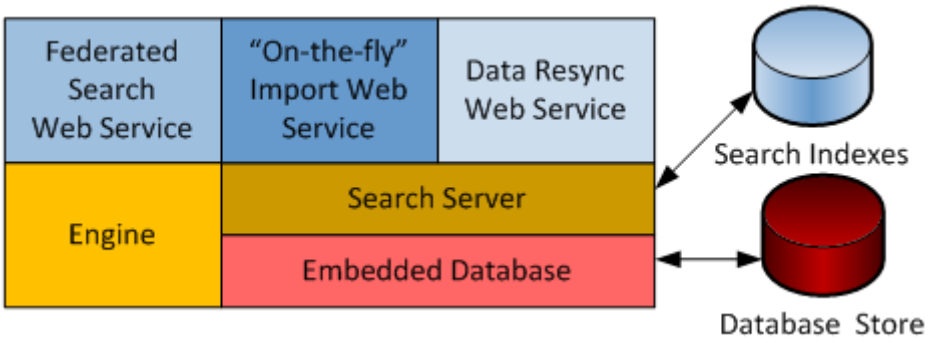
Raptor Search Engine Server Components



Raptor indexes each external data source. The Dispatch Server connects directly to the Raptor Server (Raptor Search Engine) just as it does with the Search Server and sends it search queries. The Raptor Search Nodes

process the search requests for each external data sources. Each Raptor Search Node is the equivalent of a standard Palantir Search Server.

Raptor Search Engine Components



You can either directly import data sources into Palantir or access data from existing, external data sources using Raptor indexing. You can use both methods in any Palantir installation, but you can use only one method on any given data source. Advantages of importing data directly into Palantir include:

- histogram-eligible data sets
- quicker search capabilities
- enhanced entity resolution

Advantages of using Raptor indexing include:

- reduced requirements on the Palantir database
- built-in resynchronization from the external data sources
- data owners control their data using existing infrastructures

Once Raptor indexes a data source, it continues to monitor that source. When the data sources change, Raptor captures the changes and sends them to Palantir. For a detailed discussion of using Raptor, see the *Palantir Data Integration Guide*.

Monitoring Server

The Monitoring Server tracks the health and performance of a Palantir installation. The Monitoring Server provides notifications of changes in these mission-critical systems. The Monitoring Server stores the data it collects. Over time, administrators can see a window of historical data. With the Monitoring Server installed, a Palantir administrator can:

- diagnose performance problems by surveying the activity across the entire installation
- receive alerts on high system load, swap usage, faulty configuration property values, and slow response times
- monitor server restarts and downtime
- track the execution and ongoing status of jobs

The Monitoring Server relies on a client process installed on each host machine where Palantir servers are installed. This client returns values to the Monitoring Server. View these values in the Palantir Enterprise Manager GUI.

Authentication Server

Use an Authentication Server to connect to an authentication service in your network instead of using the Palantir internal authentication mechanism. The Palantir Platform provides a choice of two versions of the Authentication Servers. You can choose to install either, both, or neither of them depending upon the requirements of your deployment.

Install the LDAP Authentication Server if your organization uses Lightweight Directory Access Protocol (LDAP) services or in conjunction with a custom authentication plugin to connect to a service that is neither LDAP nor Active Directory. If you need a custom authentication plugin, then consult your Palantir

representative. Use the Palantir Enterprise Manager GUI to configure authorization sources so that the Palantir system uses the existing LDAP service to authenticate users who access Palantir servers and software.

Install the Active Directory Authentication Server if your organization uses Active Directory authentication services. Use the Palantir Enterprise Manager GUI to configure authorization sources so that the Palantir system uses the existing Active Directory service to authenticate users who access Palantir servers and software.

Note: Install the Active Directory Authentication Server using its own separate installation program. You can neither use the Palantir Enterprise Manager to install it nor use the Monitoring Server to monitor its status.

Extraction Integration Server

The Extraction Integration Server allows users to extract entities from documents that are imported into the Palantir system. Use the Palantir Technologies Entity Extractor (PTEE) SDK to connect Palantir to entity extractors in your environment. For details, see the *Palantir Developer's Guide*.

Palantir Web

The Palantir Web is a front end for the Palantir product. Use this browser application as a light-weight alternative to the Workspace. The Palantir Web contains a subset of the functionality available with the full Workspace client. Use the Palantir Web to search and browse objects in the Palantir Repository. Additionally, you can Web Start the Workspace application from the heading panel. For details, see the *Palantir Web User's Guide*.

Palantir Phoenix

Palantir Phoenix is a highly scalable, distributed data store designed for enormous structured data, such as network logs and call data. These extensive and distributed structured data sources are often more useful if users can import a segment of them into the Palantir Platform for in-depth contextual analysis. Using a Phoenix plugin in the Palantir Workspace, users identify interesting log records in the distributed data store, select those records, and import them. The Phoenix Server process purges the remaining log records at the intervals you define for your "rolling window of data." To learn more about Phoenix, see the *Palantir Phoenix Guide*.

Getting Started > Palantir Architecture > Optional Palantir Components