General Security Infrastructure Considerations

Operating system

OS-level hardening and secure configuration of your operating system is of course imperative. Please consider and implement your own system security based on the operating system you're using. Hardening should include enabling local firewalls on the server with default deny policies. The Center for Internet Security offers excellent benchmarks for OS hardening.

RDBMS

Controlling database access based on the principle of least privilege will help to isolate potential exposure in the event of account compromise. This includes creating read-only permissions for each separate database, and not using privileged credentials to connect to databases where not required.

Configuration database

Determine the server that will host the Yellowfin configuration database. The Yellowfin application will require credentials with full privileges to the configuration database. To reduce the risk of unintended interaction with other content on your database sere (like dropping databases, adding databases or making global changes), the credentials you use to access the Yellowfin configuration database should be limited to accessing this database only. We recommend that you use the minimum privileges necessary for these credentials:

- Create/Update DB
- Create/Update/Insert Table
- Create/Update/Delete Index
- Create/Update/Delete Stored Procedures
- Create/Update/Delete functions

In addition to these, some databases also require Sequences permissions (Oracle, Postgres).

It's also worth noting that the CREATE DB permission is not needed if you're choosing to install into an existing DB.

Do not use global administrator or super user credentials for the connection to this database.

Running the installer

The Yellowfin installer will create your application folder structure at a directory of your choosing, and prompt you for the Configuration Database location. During this install process, you can also assign a port to the application server, as well as assign your dedicated memory allocation to the application. When installed on Windows, you can elect to install Yellowfin as a service.

For more information on system performance, visit the Estimating Capacity Requirements page

Linux considerations

Installation

When installing on Linux, we recommend that you create a dedicated service account for the application. This will ensure the application is running in a limited context on the server. Since this is a service user, specify no login.

```
sudo useradd -s /bin/false yellowfin
```

Make your target Yellowfin directory and assign the proper permissions to the new directory.

```
sudo mkdir /opt/Yellowfin && sudo chown yellowfin /opt/Yellowfin
```

From here you can sudo into a prompt as the yellowfin user and execute the installer.

```
sudo -u yellowfin bash

java -jar yellowfinInstaller.jar
```

Note that ownership can also be granted after installation if desired by issuing a recursive chown command.

Service

The Yellowfin installer does not have a native option to create a Linux service file during installation. This can be created, dependent on system type. We’ve provided some example service files on Yellowfin Community.

Port redirection

We recommend that you use port redirection to serve the application over standard HTTP/HTTPS ports to remove the requirement of running the service under a privileged account. Any ports lower than 1024 require Administrative or root permissions to bind to. In Linux, this can be done using iptables:

```
iptables -A PREROUTING -p tcp –dport 8080 -j REDIRECT –to-ports 80

iptables -A PREROUTING -p tcp –dport 8443 -j REDIRECT –to-ports 80
```

Windows makes use of the netsh command to achieve this:

```
netsh interface portproxy add v4tov4 listenport=8080 listenaddress=$IP connectport=80 connectaddress=$ip
```

Encrypt RDBMS connections

SSL/TLS encryption is handled at the JDBC level and can be enabled on both configuration database and data source levels for more granular control. This is typically enabled using parameters on the JDBC URL. Consult the third-party documentation for the RDBMS/JDBC type you are using for specific information.

An example can be found in our Configure SSL For Data Source Connection article.

Deployment and Hardening Guide

Back to the Overview

- General Security Infrastructure Considerations
- Application Server Security
- Yellowfin UI Security Settings

General security infrastructure considerations #top