Onboarding Pre-Requisites

Before starting the installation, make sure your system and environment meet all the requirements for a secure and successful deployment. This section walks you through each step needed to prepare for installation.

System Requirements

- OS: Linux → Ubuntu 20.04 LTS or higher; Rocky OS version 8+
- CPU: 4 cores or more
- Memory: 8GB or higher
- Storage: 100GB (Min)
- Privileged access (root access)
- Libraries and Tools: Git 1.8+
- Open Port 443 accessible from the internet

- ☐ **System Requirements** — Verify that your system meets the minimum hardware, software, and network specifications for installation. This typically includes supported operating systems, processor type, memory, disk space, and network bandwidth.
- ☐ **License Key —** Obtain a valid License Key to activate and validate your software access.
- ☐ **SSH Key —** Generate and register an SSH Key to securely connect your deployment environment and enable authorized communication.
- ☐ **SSL Certificate —** Set up an SSL Certificate to protect sensitive information through encrypted connections.
- ☐ **Fully Qualified Domain Name (FQDN) —** Configure an FQDN to ensure the application is accessible from a consistent, verified domain.
- ☐ **SMTP Server —** Prepare an SMTP Server to handle system alerts, notifications, and user emails.

License Key

A License Key is a unique identifier used to activate and validate your software access. Before installation, make sure you have received a valid key from your FDSA support team (fdsa.support@alzherimersdata.org), after the data agreements with AD Data Initiative partnership team. This key ensures your deployment is authorized and linked to your organization's subscription.

You'll typically receive the License Key in your welcome email or through a secure portal provided by the vendor. During setup, you'll be prompted to enter or upload this key to unlock full system functionality.

If your key expires or becomes invalid, you may lose access to certain features or updates. To prevent interruptions, confirm that your License Key:

- Matches the version of the software being installed
- Has not expired or been revoked
- Is registered under the correct organization account

If you haven't received your key or encounter an activation issue, contact your FDSA support to request a new or updated License Key before proceeding with the installation.

SSH Key

To get the project we will need the SSH Key. Here is how to create one:

1. In the server where FDSA is going to be installed, start the root user mode:
   ```
   sudo su
   ```
2. Generate an SSH Key using your email (you can leave the passphrase empty, but it's optional):
   ```
   ssh-keygen -t rsa -b 4096 -C
   "your_email@example.com"
   ```
3. View the generated SSH Key:
   ```
   cat /root/.ssh/id_rsa.pub
   ```
4. Copy and send the Public Key to fdsa.support@alzheimersdata.org. Our support team will add your key to the GitHub FDSA-Release repository and notify you when it's ready.

Onboarding Pre-Requisites

SSL Certificate

An SSL certificate ensures that data transmission between your appliance and users is encrypted and secure. You can obtain an SSL certificate in the following manner:

1. SSL Purchase: Purchase a public SSL/TLS v1.2+ CA Certificate (.crt and .key) from a reputable Certificate Authority (CA) like GoDaddy, DigiCert, or Comodo. Avoid using free solutions like 'Let's Encrypt.'
2. CSR generation: Follow the CA's instructions to generate a Certificate Signing Request (CSR) and submit it. Once approved, you'll receive the SSL certificate files, including the public key, private key, and intermediate certificates. Keep these secure.
3. Certificate Note: When obtaining your SSL certificate, remember to coordinate with your administrator to extract the private key.

Fully Qualified Domain Name and Public IP Address

A Fully Qualified Domain Name (FQDN) is necessary to access your Federated Data Sharing Appliance over the internet. Here's how to set up a FQDN:

1. DNS Selection: Choose a domain name registrar (e.g., GoDaddy, Namecheap) and register a domain name.
2. DNS Configuration: Configure the DNS records for your domain to point to your server's public IP address.
3. DNS Resolution: Ensure that your chosen FQDN resolves correctly to your server.
4. Email the FQDN to fdsa.support@alzheimersdata.org for ADWB FAIR Whitelisting. If using a Load Balancer, send the Public facing FQDN.

SMTP Mail Server

NOTE: When you install our default SMTP configuration emails could go to spam since it is a gmail.com address.

An SMTP (Simple Mail Transfer Protocol) mail server is essential for sending email notifications, alerts, and system updates from your Federated Data Sharing Appliance. Setting up an SMTP mail server is crucial for effective communication. Here's how to add it as a prerequisite:

1. Select an SMTP Server: Choose an SMTP server or service provider that meets your needs. Popular choices include Gmail, Microsoft Exchange, or a self-hosted server like Postfix or Sendgrid.
2. Configure SMTP Settings: Obtain SMTP server details such as the hostname or IP address, port number, and encryption settings (SSL/TLS). If you're using a third-party service like Gmail, ensure you have an email account and create an "App Password" or enable "Less Secure Apps" as needed.
3. Set Up SMTP Relay: Depending on your Federated Data Sharing Appliance's requirements, you may need to configure it to use the SMTP server as a relay. This typically involves specifying the SMTP server's details, username, and password for authentication.
4. Testing: Before proceeding with the installation, test your SMTP server's configuration by sending a test email from the command line or through the appliance's settings.
5. Secure SMTP Credentials: Ensure that any credentials (username and password) required to access the SMTP server are stored securely. Use environment variables or a secure credentials manager to protect sensitive information.