Deployment Instructions for online NDR

1、 Preface

This operation manual provides a detailed description of the process steps for deploying the online National Does Registry(NDR) developed by National Institute for Radiological Protection, China CDC, with the support from IAEA, on a computer server, to release the system on the internet.

2、 Hardware preparation and operating system installation

a. Hardware inspection and preparation:

- Ensure that the server hardware is complete, including processors, memory, hard drives, network adapters, etc.
- Connect the server to the power supply and network.

b. Operating system installation:

- Choose an operating system version that is suitable for the system requirements, such as Windows Server 2012 R2. Obtain and install the original installation files for Windows 2012 R2. You can purchase genuine CDs from Microsoft's official website or obtain them through other legal means.
- Start the server using the installation media and enter the installation interface.
- Choose the installation language, configure keyboard layout and time zone.
- Configure disk partitions, create root directories, swap partitions, and necessary file systems.
- Set the network configuration, including host name, IP address, subnet mask, default gateway, DNS server, etc.
- Set passwords for administrator user or create other user accounts.
- After completing the installation, restart the server.

c. Driver installation:

- Install various drivers, including motherboard, graphics card, sound card, network card, etc. Ensure that there are server hardware drivers, which are usually included when purchasing a server.

3、 Server environment configuration

a. Update system and drivers:

- Update the operating system and installed drivers to the latest version through the system's built-in update tools or package managers (such as APT, yum, etc.). This helps to ensure the security and stability of the system.

b. Set up network:

- Configure the network settings of the server, including IP address, subnet mask, default gateway, DNS server, etc. Ensure that the server can connect to the network normally.

- Disable unnecessary services and ports to enhance system security.

c. Configuration storage:

- Configure the storage settings of the server according to requirements, including disk partitions, file system types, mount points, etc. Ensure that the server can correctly identify and manage storage devices

d. Configure security settings:

- Set security policies for the server, including firewall rules, user permissions, password policies, etc. Ensure that the server can effectively resist external attacks and unauthorized access.

e. Optimize performance:

- Optimize the performance of the server based on its hardware configuration and application requirements. This may include adjusting system parameters, optimizing database queries, configuring load balancing, and so on.

f. Backup and Recovery:

- Configure backup strategies and regularly backup important data on the server. At the same time, ensure that data and services can be quickly restored in the event of unexpected situations.

4、 Installation and configuration of necessary software and services

a. Database server:

- Install MySQL database, version: MySQL 8.0.23.
- Set the MySQL username and password for the project. And set permissions to access the database
- Create a new database: Individual_dose.
- Import the initial database file dose.SQL for the project
- Install Redis database to store temporary data, reduce database access pressure, and improve system response speed.

b. Application server:

- Web services, such as Apache HTTP servers or Nginx, are responsible for processing HTTP requests, forwarding requests to application servers, and returning response generated by the application.
- Application containers Tomcat provide the environment required to run applications, including class loaders, thread management, security management, and more.
- Load balancers, such as Nginx or HAProxy. They are responsible for distributing requests to multiple application servers, achieving load balancing and high availability.
- HTTPS configuration is usually configured on the application server to ensure the security of data transmission. This includes installing and configuring SSL/TLS certificates, as well as ensuring that communication between servers and clients uses encryption

protocols.

5、 Project deployment and configuration

a. Environmental installation

- Install version 1.8 of JDK and configure environment variables.

b. Project deployment

- The application is a war package, which can be placed in Tomcat's webapps or configured as a conf/service.cfg file.

c. Set startup script

- For system services, create a service unit file that defines how to start, stop, and restart your application.

d. Start the application

- Run the startup script for the settings.

e. Monitoring and logging

- Use tools such as Prometheus and Grafana for monitoring. Configure logging and send logs to the log management system (such as ELK stack: Elasticsearch, Logstash, Kibana). Ensure appropriate monitoring and logging mechanisms are in place to track the running status and performance of applications.

6、 System testing and performance optimization

a. System testing:

- Conduct comprehensive testing of the entire system, including functional testing, performance testing, security testing, etc.
- Use automated testing tools and frameworks to improve testing efficiency and accuracy.

b. Performance optimization:

- Analyze system performance bottlenecks based on test results and make corresponding optimizations.
- Optimize database query statements and index design to improve

data access performance.

- Adjust server resource configuration, such as increasing memory, optimizing network bandwidth, etc.

7、 System launch and maintenance

a. Backup data:

- Fully backup system data before going live to ensure data security.

- Develop backup strategies, regularly backup data, and prevent data loss.

b. System launch:

- Formally deploy the system to the production environment, configure load balancing and disaster recovery backup, etc.

- Monitor the operational status and performance indicators of the system to ensure stable operation.

c. System maintenance:

- Regularly update system software packages and security patches to fix known vulnerabilities