Primero “Tier 4” Hybrid-Local Server Deployment Resources Allocation and Work Plan

Introduction

For those of you who are interested in self hosting Primero v2, in addition to the guidance we have shared on Self-hosting background and set up and Installation Guidance, there are programmatic considerations that must be taken into account. The self hosting model for Primero is an implementation model we call “Tier 4”. This model has 2 sites, one “*demo*” and one “*production*”. We use the demo CPIMS+ to manage configurations (forms, roles, reports), to receive updates and security patches, and to test and train. *Demo has no real data on it*. In the Tier 4 model, the demo site lives on UNICEF’s Microsoft Azure servers. For the production site, we use the server that in the partner selected data center managed by a capable technical team who can support the infrastructure set up and maintenance. All the *real* data is stored on this server. This implies a higher level of accountability and management for the in-country team. A work plan template for a Tier 4 implementation can be found here: https://docs.google.com/spreadsheets/d/1TBBl4qj5mC_N-2KmkaN_uITw-O7bRxTde5YUpFxG9e8/edit?usp=sharing

Roles and Responsibilities

In this model, it should be clear that the Primero Team cannot be responsible for managing or supporting any of the following and partners are responsible for:

1. All infrastructure including setting up servers, hosting, setting up monitoring and security measures, security certificates, data durability/data storage, backups, DNS, and configuration of the demo and production instance
2. Owning, protecting and securing the data
3. Disaster recovery protocols and data breach protocols

4. Clear process in place for configuration promotion from “demo” to “production” to receive the most up-to-date releases (which include updates and security patches)
5. Primero v2 is a progressive web application (PWA) and we have an identity provider that helps us securely authenticate and manage users. If a mobile device management solution is requested for mobile devices, this must be procured and maintained.

The set-up of local infrastructure demands ongoing technical support and budgets. Therefore, you must select a technical partner which has demonstrated a very good capacity, strong technical infrastructure skills and understanding of the work for the project sustainability.
Primero will be handling highly sensitive, personal data, it is crucial that a Terms of Use is signed by the Deputy Representative (if UNICEF is involved) or Minister or Head of Country Operations for this implementation. An Information Sharing Protocol and Data Breach Protocol is required for an implementation which is a case management tool, and is part of the Information Management standards for case management. This ensures you have a clear risk mitigation strategies in place, as well as governance and accountability for decisions that impact child safeguarding, data protection and cyber security. There must be considerations made for the on-going sustainability of the system which includes accounting for on-going costs and resourcing.

To be ensure we are all on the same page, the local production server, which we call Primero Tier 4 package, includes:

- A supported production instance running on infrastructure owned by the local team.
- Automated updates to local Primero, delivered in lock step with UNICEF-hosted Primero.
- Access to the latest Child Protection configurations.
- An additional, UNICEF-hosted non-production instance of Primero used for demonstrations, training sessions, and configuration management.
- Primero implementation support for your programming.

It is up to the local ICT team (government or the leading agency) to implement mechanisms for security that ensure application availability, data confidentiality, and system integrity. Please read the eloquent warning in the **Primero Self Hosting Guide.** It fully applies to Tier 4 infrastructure. **Could you confirm if the in-country team can take on this responsibility for implementing and installing the software?**

Of course we understand that Tier 4 service assumes a shared responsibility between the **UNICEF Primero Team** and the **Local Team** for the application and infrastructure. To be very clear the key roles and responsibilities are:

UNICEF Primero Team Responsibilities: UNICEF will continue to be responsible for maintaining and releasing the Primero application. It will provide Level 3 support to ensure application integrity and stability. A Global Team focal point will be available for consultation and support requests from the Local Team. The main responsibilities are:

- **Primero X SaaS Infrastructure:** The Local Team will not have any backend access to the Tier 3 infrastructure. The Tier 4 demo instance will still be operated by UNICEF. Configuration promotion from demo to production will work against this new infrastructure.
- **Primero Production SaaS application deployment:** UNICEF will be responsible for the initial installation of the latest supported version of Primero v2 on the local infrastructure. UNICEF will offer standard configuration templates as baselines for new Tier 4 Primero instances.
- **Primero Production SaaS application delivery:** UNICEF will be responsible for the ongoing and scheduled delivery of the latest versions of Primero to the Tier 4 localized infrastructure. This involves:
    - A "push" approach to delivery: UNICEF delivery tools will have access to the localized infrastructure to deliver updates *on a schedule established by UNICEF*. The Local Team will have the opportunity to object to the changes and delay the scheduled release.
    - Performing occasional manual data migrations that may be required when upgrading from one version to another. Note, that these migrations will require direct access by the UNICEF Primero Team engineers to the localized infrastructure.
- **Primero application operation and support:** The UNICEF Primero team will ensure that Primero is up and running on the local infrastructure. This includes:
    - Checking for service availability; Docker is up and running, containers are up.
    - Triggering application restarts.
    - Review of Primero bugs and errors.
- **Transition to Primero Tier 3:** If the overhead for running the Primero Tier 4 service package is too significant and if the regulation changes, the UNICEF Primero Team will support a transition to a UNICEF-hosted Tier 3 service. This process will require support from the Local Team and would incur additional costs.

Local Team Responsibilities: the Local Team will be broadly responsible for operating the infrastructure, managing the data, and ensuring the availability of Primero to the local programme team. That means the Local Team needs to have access to the right resources and staff with the relevant skill set such that the infrastructure can be responsibly operated. **If the team cannot support this work, then the decision to use Primero Tier 4 should be reconsidered or appropriate roles should be staffed for or outsourced to technology and infrastructure vendors.** The team's main responsibilities are:

- **Local Production Infrastructure:** The Local Team will procure, operate, maintain, and support the new local production infrastructure. Responsibilities include:
    - Identifying vendors and procuring infrastructure services or hardware.
    - Setting up the local infrastructure according to the minimum standards required by Primero Tier 4 (see below.) System availability in accordance with locally established SLAs. This does not account for any interruptions of service due to application updates from Tier 4.
        1. Infrastructure security: ensuring only authorized access to the system and the data.
        2. Keeping up with software updates for core systems that operate on the local infrastructure. This includes Ubuntu LTS updates and PostgreSQL updates.
        3. Setting up an approach to monitor for and react to unusual system resource usage: excessive use of disk space, memory, CPU.
        4. Rescaling the system in response to increase in system load and usage.
        5. Procuring and setting up a non-production sample infrastructure that will be used by UNICEF to test the Tier 4 delivery approach.
- **Access to Local Production Infrastructure:** The team is wholly responsible for managing access by external users and services to the infrastructure. This includes local support staff, UNICEF Primero Global Team support staff, and Primero system services used for application delivery.
- **Email services:** The Local Team is responsible for procuring and securely operating the SMTP server necessary to send email messages out of Primero.
- **DNS and TLS:** The Local Team is responsible for registering the domain for their service. The team will procure a TLS certificate to register this domain. Primero Tier 4 does not allow the use of the **primero.org** subdomain. **Make sure that the procured TLS certificate includes the entire certificate chain!**
- **Backups:** Back up production case data and relevant attachments to servers owned by the country team or designated as appropriate backup targets. The local team is responsible for identifying and coordinating implementation of the appropriate solution for connecting backup resources to the local Primero

infrastructure. The backup policies and constraints (frequency, retention, projected backup size) will be determined by the local team. UNICEF Primero Team to provide a sample approach.

- **Disaster Recovery Plan:** A documented approach for system recovery in the event that the localized Primero infrastructure becomes unavailable or corrupt.
- **Disaster Recovery:** The local team will be responsible for taking the lead on executing the plan above, in coordination with the UNICEF Primero Team.
- **Establish and document operational procedures**: how to grant system access, how to conduct system access auditing, troubleshooting guide, reference the Disaster Recovery Plan (above).
- **SLA:** The Local team will establish a service level agreement (SLA) for the system availability. This will be the rubric against which the success of the Tier 4 transition will be judged. For example, a locally operated Primero can aim for 99% availability: allowing under 88 hours of downtime per year. Note that compared to the UNICEF-operated Tier 3, Tier 4 assumes a degradation in availability.
- **Audited Access:** Keep a log of all backend access attempts by support staff from both UNICEF and local team staff and regularly review for suspicious activity.
- **Compliance Review:** Review of localized Primero Tier 4 solution for compliance with local law, regulation, or organizational policy.
- **Future change of host:** Any future changes of the hosting provider for the Tier 4 solution or a downgrade away from UNICEF support will be the sole responsibility of the local team to plan and execute.

Could you confirm if the in-country team can take on these responsibilities?

The structure of the local team will vary based on needs and available resources. Typically it will involve some combination of:

- **Primero Administrator:** A power user who is responsible for configuring and managing the application. The administrator usually works with the program rather than with IT.
- **IT Team:** Technologists working for the implementing organization, responsible for providing first and second tier support for the infrastructure. The team should:
    - Be comfortable Linux administrators.
    - Be able to manage access to production servers over SSH.
    - Be familiar with basic Linux security practices.
    - Be familiar with Docker.
- **Hosting Provider:** The team responsible for operating the physical infrastructure at a data center or a secure server room. This team can be

within the same implementing organization and be a part of the IT team, an external government technology institute, or a vetted private vendor. It is expected that the Hosting Provider will be able to:
    - Provision physical or virtual infrastructure.
    - Provide physical security controls (badged access, etc.) to the server location.
    - Configure and secure networks.
    - Provide infrastructure for backups and system disaster recovery.
- **Technology Vendor:** The implementing organization's IT team might not have the necessary capacity to operate Primero hardware and offer first tier application support. This role may be outsourced to a third party vendor.

For production support, responsibility between the UNICEF Primero Team and the Local Team will be divided up for system support:

- **Level 1:** Local Team administrative team (Primero power users and administrators) to provide user support activities.
- **Level 2:** Local team will provide infrastructure support. As needed, they may perform activities such as restarting physical servers or application services, increasing allocated disk space, or updating local TLS certificates.
- **Level 3:** UNICEF Primero Team will provide Primero application support, bug resolution, and security updates. This will require access to the local infrastructure by UNICEF services. If the Local Team has robust access controls in place, they may grant individual UNICEF Primero Team support engineers access to the local system.

It is up to the Local Team to determine the infrastructure approach for Primero Tier 4. The Primero v2 Self-Hosting Checklist is a good starting point. The team should consider the following:

- **Hosting:** The infrastructure host will be determined by regulation, capacity, and cost. In some cases this means that hosting will be with a vetted government technology provider, in others a cloud hosting account (e.g. Azure or AWS) fully owned and operated by a government agency will be sufficient. The host must:
    - Comply with the overall regulation driving the choice for Tier 4
    - Support the technical specification (see below)
    - **Be as convenient and as easy to support as possible for the Local Team. A hard-to-use and misunderstood hosting platform will not provide better security and cannot be sustainably operated.**
- **Server:** For an implementation with up to 100,000 records and up to 200 active users the specifications are:
    - Hardware

        - 8+GB memory (4GB absolute minimum, but not recommended)
        - Roughly two CPU cores (e.g. 2.5 GHz, Intel Xeon)
        - Storage: we recommend 500GB or more. Primero v2 puts no physical cap on the number of image and PDF attachments. If attachments become heavily used by the program (as signed material, images, media files), the server storage capacity should be able to grow.
    - Operating system: Ubuntu 20.04. Note that the End of Life for this version of Ubuntu will be in March 2025. The Local team should plan for upgrades if the program's duration will exceed that date.
    - Networking rules:
        - All permitted outbound traffic:
            1. Ubuntu/Canonical package repositories, Dockerhub, Azure Devops repos, optionally Let's Encrypt
        - Inbound traffic permitted on ports 80, 443
        - Inbound traffic permitted on port 22 (whitelisted to only the Bastion Server and the UNICEF Primero X deployment pipeline.)
    - A passwordless non-root user with passwordless sudo privileges accessible only via SSH.
- **Database:** The database can be deployed along with the rest of Primero, but **the recommended approach is to use an external managed PostgreSQL database service** such as that provided by MS Azure or Amazon Web Services. A Local Team that has experience managing PostgreSQL database servers may elect to provision and separately manage a standalone database, but this should only be attempted if the team has the capacity to responsibly and sustainably operate it.
- **Document Storage:** Default document storage uses the data volume where Primero is installed. If the program relies on file attachments it is recommended to either:
    - Project data growth and allocate sufficient file storage. The team will need to monitor and periodically increase the disk size. The minimum recommended storage of 500 GB assumes roughly 4 Mb worth of attachments per record.
    - Use a third party blob storage service. Primero supports Azure Blob Storage and AWS S3.
- **Bastion Server:** A bastion server should be used to manage access to the production servers. This can be a minimal virtual machine. **It is not recommended to access the production infrastructure directly from the Local Team's personal devices.** See the Self-Hosting Guide for more on Bastion Servers.
- **DNS/TLS:** See Local Team responsibility above. Primero does not recommend the use of wildcard certificates or Let's Encrypt for production instances.

- **SMTP:** Primero will send email notifications and will use email during the user onboard workflow. It is recommended to use a managed SMTP service such as MS Exchange. The Local team must make sure that email communication is encrypted. The SMTP service (and the associated DNS zone file) should be configured to prevent mail sent by Primero being marked as spam.
- **Backup:** The data backup precautions are wholly left up to the Local Team. Some considerations:
    - Remember to backup both the **database** and the **document storage**.
    - Managed cloud databases and storage already have robust backup guarantees but these might not be compliant with policy or regulation.
    - The UNICEF Primero Team will offer a templated local backup solution based on Cron and RSync. This may be used and customized by the Local Team as needed.

Sample Infrastructure

The infrastructure in this diagram represents a Primero Tier 4 setup that uses Microsoft Azure with a local data center providing a redundant backup for compliance. **Could you confirm if the in-country team can take on this responsibility for infrastructure set up?**

The Local Team is responsible for ensuring basic security standards for the local infrastructure. This includes:

- **Local Security Policies:** Primero Tier 4 should aim to comply with organizational security policies set by the Local Team.
- **Minimum Security Standards:** Must be met in order to responsibly operate local infrastructure for Tier 4:
    - Commitment to regular security patching by the local team
    - Firewall rules: only ports 80/443 exposed.
    - Production server hardening. Some security configurations are applied automatically during the Primero Tier 4 server onboarding process.
- **Secret Management:** Secrets such as TLS certificates, managed database credentials, and SMTP credentials. These will be made available on the production host system via a formatted and restricted file. The UNICEF Tier 4 infrastructure may generate additional system secrets (such as internal Primero encryption keys). UNICEF will manage these secrets, but the Local Team will always have precedence for managing secrets.
- **System Access Management:** Access by users to the local infrastructure is granted by the Local Team. It must rely on key-based, passwordless SSH. The Local Team must develop procedures for handling SSH keys and access requests.

Could you confirm if the in-country team can take on this responsibility for security standards?

Key Considerations for Security

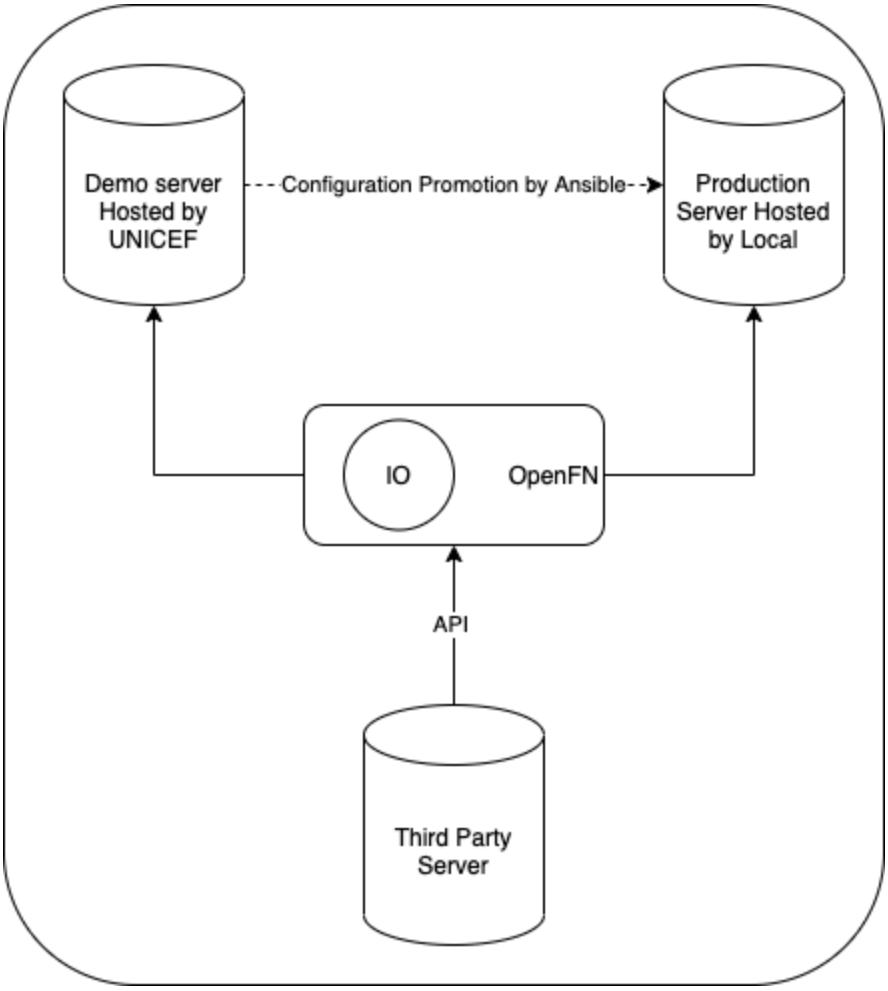
1. **Data Encryption:** Ensure that all data, both in transit and at rest, is encrypted using strong encryption algorithms. This prevents unauthorized access to sensitive information even if there is a security breach.
2. **Access Controls and Authentication:** Implement robust access controls to restrict access to the system and sensitive data based on roles and permissions. Multi-factor authentication (MFA) should be employed to add an extra layer of security for user logins.
3. **Audit Trails and Logging:** Establish comprehensive logging and audit trails to monitor system access and activity. This helps detect and investigate any unauthorized access or suspicious activities.
4. **Secure Development Practices:** Ensure that secure coding practices are followed during the development of the case management system to minimize vulnerabilities that could be exploited by attackers.
5. **Regular Security Updates and Patch Management:** Keep the system and all associated software up to date with the latest security patches to address known vulnerabilities and reduce the risk of exploitation.
6. **Data Backup and Disaster Recovery:** Regularly back up all data and establish a robust disaster recovery plan to ensure that critical information can be recovered in case of any data loss or system failure.
7. **Data Retention Policies:** Define clear data retention policies to avoid storing unnecessary data and to comply with relevant data protection regulations.
8. **Physical Security:** If the system is locally hosted, ensure physical security measures are in place to protect the servers and infrastructure from unauthorized access.
9. **Vendor Security:** If using a cloud-based service, carefully vet the cloud service provider's security practices, compliance certifications, and data protection measures.
10. **Employee Training and Awareness:** Train all employees and users on security best practices, such as identifying and reporting potential security threats or phishing attempts.
11. **Incident Response Plan:** Develop a comprehensive incident response plan to handle security breaches or data breaches effectively and minimize their impact.
12. **Regular Security Assessments:** Conduct regular security assessments, penetration testing, and vulnerability scanning to identify and address potential weaknesses in the system.

13. **Monitoring and Intrusion Detection:** Implement monitoring and intrusion detection systems to identify and respond to security incidents promptly.
14. **Legal Considerations:** Ensure that the deployment and use of the case management system comply with all applicable laws and regulations, especially those related to child protection and data privacy.

Guidance Documents

- Programmatic Guidance
- Want to know if you are ready to host Primero: Hosting Requirements Checklist
- Self-hosting background and set up
- Installation Guidance

Architecture for Interoperability



Sharing Details with Primero Technical Teams for Set up

The domain, security certificate and email for notifications must be set up and shared with the Primero Technical Team to help you with Tier 4 deployment. This includes:

Domain (this is what the users will put in the browser to use Primero)

****

primero_host: 'somedomain.gov.ae'

Security Certificate (this email will receive information about the security certificate)

****
****

certbot_email: 'primero@example.org.ae'

Email (for notifications etc)

****

SMTP_ADDRESS: 'mail.server.org.ae'
SMTP_PORT: '587'
SMTP_DOMAIN: 'server.org.ae'
SMTP_AUTH: 'plain'
SMTP_STARTTLS_AUTO: 'true'
MAILER_NOTIFICATION_HOST: 'domain.gov.ae'
MAILER_DEFAULT_FROM: 'noreply@domain.org.ae'
MAILER_DELIVERY_METHOD: 'smtp'’