Preparing to Create Productions

Version 2023.3
2024-05-16

InterSystems Corporation 1 Memorial Drive Cambridge MA 02142 www.intersystems.com

Preparing to Create Productions
InterSystems IRIS Data Platform Version 2023.3 2024-05-16

For Support questions about any InterSystems products, contact:

InterSystems Worldwide Response Center (WRC)
Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

Table of Contents

1

Road Map to Using InterSystems IRIS Productions

The following sections provide an outline of the documentation resources where you may want to start, depending on your role.

1.1 InterSystems IRIS Production Developer

If you are a developer preparing to create or use InterSystems IRIS® productions, see the following resources:

1. *Introducing Interoperability Productions* provides an overview of InterSystems IRIS Interoperability and options that you may want to include in your productions, with pointers to more detailed information.
2. *Best Practices for Creating Productions* describes best practices for designing, developing, and maintaining productions.
3. *Developing Productions*, which, in turn, points you to specific topics in the set *Application Development: Creating Productions* and other guides.
4. *Configuring Productions* describes the details of configuring items in a production.

1.2 InterSystems IRIS Administrator

If you are an administrator preparing to work with productions, see the following resources:

1. *Introducing Interoperability Productions* provides an overview of product features.
2. *Managing Productions* explains how to use the browser-based Management Portal to manage the production environment and points to detailed descriptions of the specific functions performed using the Management Portal.
3. *Configuring Productions* explains how to build and configure productions and production components as well as update configurations of existing productions.
4. *Monitoring Productions* explains how to monitor your production environment and the various production components.

2

Planning an InterSystems IRIS Server Deployment

This topic describes the major issues you must account for when deploying a production InterSystems IRIS® server.

If you are responsible for planning an InterSystems IRIS server deployment, this topic can serve as a checklist of items to plan for, although there will be additional items you will need to consider as well.

This checklist identifies some critical issues that must be dealt with to deploy a reliable, efficient, and maintainable InterSystems IRIS system, but does not attempt to provide detailed guidance on these issues. This document organizes the issues into the following checklists:

- Capacity plan and checklist—ensures that the InterSystems IRIS server is able to efficiently handle your peak load.
- Robustness checklist—ensures that the InterSystems IRIS server has a high availability configuration and can recover from a disaster.
- Security checklist—ensures data privacy and resistance to attacks.
- Maintenance checklist—ensures that the InterSystems IRIS server continues to function well over long periods of time and with software and hardware updates.

2.1 Capacity and Performance Checklist

The performance of an InterSystems IRIS server is measured by its ability to handle the peak message load. The performance of an InterSystems IRIS server is dependent on the complex interaction between many components and settings. The load of an InterSystems IRIS server is dependent chiefly on:

- Number and size of messages—both the peak load and daily load are important.
- Processing required for each message—In most cases, you want to streamline the processing of messages. For example, while there are advantages to validating messages, complete validation can add a significant processing load to handling each message.

In many cases, the message load on an InterSystems IRIS system increases over time. This increase can be due to supporting more business functions in the production or by an increase in business volume. The capacity of a server to handle this load is dependent on a complex interaction between many components and configuration settings including number of CPU cores, multiprocessor architecture, storage size and speed, network bandwidth and configuration, operating system buffer allocation, and InterSystems IRIS configuration. There is no simple formula that can predict the performance of an Inter-

Systems IRIS server because it is a complex interaction, but you can estimate, plan, prototype, and track performance to ensure that the InterSystems IRIS server is meeting your business needs.

To ensure that your InterSystems IRIS server has sufficient capacity and can efficiently handle its load, you should:

1. Estimate load—What are the number of messages that the InterSystems IRIS system will process? Is the load going to gradually increase after starting the server? How long do messages need to be preserved before they can be archived and removed from server storage?
2. Plan capacity—Planning skills depend on experience implementing similar InterSystems IRIS servers. If your organization does not have this experience, you should work with someone who has this experience: a consultant or an InterSystems Sales Engineer. You can contact InterSystems Worldwide Response Center (WRC) for a referral.
3. Prototype server and load testing—Once you have estimated load and planned the needed capacity, it is important to run a prototype system and monitor its performance. The prototype should confirm your capacity plan and provide you with a baseline to compare performance of the deployed system.
4. Plan disk layout for code and databases—By default all code and data created in an interoperability-enabled namespace are stored in the same database file. By mapping data to multiple database files, you can gain more control over where the data is stored, which can help with performance of high end systems as well as making it easier to upgrade to new versions. It is also important to store journal files on a different disk than the database files to ensure a disk failure doesn't cause loss of data.
5. Deploy server—Install and configure your live system including any redundant failover machines.
6. Track load and performance—It is important to track the server performance to establish a baseline before there are any performance issues that need to be solved. You should collect metrics such as overall and peak message load, CPU utilization, disk free space, and average elapsed time to process a message.
7. Solve performance problems before they become critical—By tracking performance and forecasting growth, you should be able to plan upgrades and efficiency improvements before performance problems become major roadblocks in your organization's performance.

2.2 Robustness Checklist

Robustness is the ability of an InterSystems IRIS server to remain available and to be able to recover quickly from any disasters. Robustness is dependent on the following issues:

- Ensuring that the server has high availability. See the High Availability Guide for more information.
- Backup of data so that it can be recovered and the server restarted in case of failure.
- Redundant network access so server can continue functioning if there is a network failure.
- Use a robust web server.

If you upgraded from a previous release, it is possible that you are using the private web server, which is provided as a convenience during development and is not a fully capable web server. If so, you should reconfigure your system to use one of the supported full-functioning web servers.

2.3 Security Checklist

Security is the ability to control access to data and to protect the server from malicious attacks. In addition to maintaining privacy for business reasons, there are often privacy compliance requirements. Potential attacks can be aimed at gaining access to confidential information, maliciously updating or deleting information, or compromising system performance. Security is dependent on the following issues:

- User accounts and password policies—Ensures that users who access the system are authenticated.
- Careful definition of permissions and roles—Ensure that users have the correct authorization and that they have access that they need, but not any greater access.
- Audit trail to track all configuration changes—Auditing provides a mechanism to track changes to the system that could potentially compromise security.
- Documentation that may be required to meet privacy compliance.
- User and operator security training—The most secure system can be compromised if users are not vigilant about security.
- Apply operating system and application security patches and upgrades in a timely manner.
- Control physical and network access to the server—Security requires robust firewalls, network protection, and limited physical access to server and network hardware.
- Database and journaling encryption—Although the firewall around a data center protects the security and integrity of the data, encrypting databases and journal files provides an extra level of security.

2.4 Maintenance Checklist

In addition to ensuring that after deploying an InterSystems IRIS server, it robustly and securely handles its load, you need to ensure that it continues to perform well over time. You need procedures to handle updates to software and hardware and how to respond to unexpected demands. Maintenance is dependent on the following issues:

- Regular message purging and backup—There are trade-offs between retaining messages after they have been processed so that they are available for viewing and purging messages to free storage for new messages.
- Backup and Restore—Perform regular backups and occasional testing of the restore from backup process.
- Hardware, software, and application updates—Plan to allow these updates without compromising system performance or security. Issues to consider include:
  - Schedule hardware maintenance, software patches and upgrades without losing server access at critical times.
  - Plan the deployment of components from a development system to a test environment, and finally to a live running production. This staging can include the use of system default settings, the export for deployment functionality, a source control system or all three. It is important to test the installation procedure as well as the updates on a test system before applying to the production server.
  - Source control provides a mechanism to control, monitor, and stage production upgrades. This is especially important where multiple people are updating related components, but is also often used as part of the promotion from development to production and for version control.
- Active monitoring procedures to detect any problems early—You should have defined procedures on how to respond to any potential problems discovered through monitoring. Monitoring can include:

- Production monitoring—Operations staff should become familiar with the various monitoring screens
- Enterprise monitoring—If you have multiple namespaces or systems, you can use the Enterprise monitor to provide an overview of how the overall system is performing. The Enterprise Message Bank and Enterprise Message Viewer provide a way to monitor messages from multiple productions.
- Alerts—InterSystems IRIS alerts can be used to quickly alert the right people to a failure without having operators monitoring a screen. However, generating too many alerts can be counterproductive and the right balance has to be found. Alert Management provides a mechanism to track resolution of alerts.

2.5 Other Resources

Although planning and deploying an InterSystems IRIS server is a challenging process, it is an easier process than trying to fix a critical InterSystems IRIS deployment that is in a troubled state. The documentation and class library documentation provides detailed information on features and installation. The following are key documents for deploying a server:

- Monitoring Productions
- Managing Productions
- Installation Guide
- Monitoring Guide
- About InterSystems Security, which introduces authentication, authorization, auditing, managed key encryption, TLS, and other aspects of InterSystems security
- Data Integrity Guide
- High Availability Guide

InterSystems provides the following resources to help you plan and deploy InterSystems IRIS:

- The InterSystems Worldwide Response Center (WRC) can provide guidance on deploying InterSystems IRIS servers and can connect you with additional resources when needed. To access WRC Direct, go to: http://wrc.InterSystems.com and enter your username and password. Contact the WRC (support@intersystems.com or +1.617.621.0700) for a username and password if you do not already have them.
- InterSystems Learning Services provides classes on InterSystems IRIS.
- The InterSystems Developer Connection and support communities provide a way for you to get your questions answered by InterSystems employees and by other InterSystems customers who may have experienced similar issues.