InterSystems™
IRIS Data Platform

Monitoring and Operations Guide

Version 2024.2
2024-09-05

Table of Contents

List of Tables

1

Defining a Monitoring and Operations Plan

Performing the relevant monitoring and operations tasks will help keep your systems running smoothly and without interruption.

This set of topics describes recommended day-to-day operations and monitoring tasks that InterSystems IRIS administrators can perform when administering InterSystems IRIS systems. You should review these tasks and include them in your own monitoring and operations plan, with appropriate role assignments and frequency, based on your systems and the needs of your organization. Depending on the needs of your organization and systems, you may need to perform other tasks not mentioned here.

To help you define your own monitoring and operations plan, these topics list the tasks by category, frequency of task performance, and role of the task performer. You can find descriptions of the tasks and instructions for performing them in the task reference.

Many of these tasks can be automated via tools that are natively available to InterSystems IRIS systems, such as the Health Monitor and the Log Monitor. In many cases, you may be able to use third-party system and infrastructure monitoring solutions to automate these tasks. Many UNIX® System Administrators use Nagios, which offers plug-ins to extend its functionality.

2

Tasks by Category

This topic organizes the day-to-day operations and monitoring tasks by category.

2.1 Disk and File System

Performing operations and monitoring tasks related to your disks and file systems is a critical part of ensuring the integrity, consistency, and reliability of your data. For example, failure to monitor disk space can lead to a stopped system, which will halt your applications.

The following tasks fall under this category:

- Monitor disk fill rate

- Monitor disk space

- Monitor for file system errors

- Monitor journal space

- Monitor size of IRIS.DAT

- Run database backups

- Run DataCheck for mirrored systems

- Run integrity checks

- Verify integrity of database backups

2.2 CPU and Memory Utilization

You should monitor various aspects of your CPU and memory utilization. For example, you should monitor the average CPU and memory load on your system so that you can issue alerts when CPU and memory usage pass certain thresholds. Failure to monitor CPU and memory usage can lead to slow or stopped systems.

The following tasks fall under this category:

- Monitor CPU utilization

- Monitor for memory swapping

- [Monitor memory utilization](#)

- [Monitor total processes](#)

2.3 Network

You should perform various monitoring and day-to-day operations tasks that are related to your system's network.

The following tasks fall under this category:

- [Monitor DNS infrastructure](#)

- [Monitor externally mounted file systems](#)

- [Monitor for network packet dGOPS or retransmissions](#)

- [Monitor system clock time](#)

2.4 Web Servers

You should perform various monitoring and day-to-day operations tasks that are related to your web servers.

The following tasks fall under this category:

- [Check ping](#)

- [Check SSH](#)

- [Monitor uptime](#)

- [Monitor web servers](#)

- [Review web server error log](#)

2.5 InterSystems IRIS Instances

You should perform various monitoring and day-to-day operations tasks that are related to your InterSystems IRIS instances. The tasks are divided into the following categories:

- [Production-related tasks](#)

- [Configuration-related tasks](#)

- [Other tasks](#)

2.5.1 Productions

The following tasks are related to your InterSystems IRIS productions:

- [Check Production Event Log](#)

- [Monitor InterSystems IRIS productions](#)

- Monitor InterSystems IRIS queues

2.5.2 Configuration

The following tasks are related to your InterSystems IRIS configurations:

- Check messages.log

- Ensure tasks are running correctly

- Evaluate global buffer size

- Evaluate lock table size

- Evaluate maximum memory per process size

- Evaluate routine buffer size

- Evaluate size of shared memory heap

- Monitor certificate expiration dates

- Monitor for errors using Health Monitor and Log Monitor

- Monitor for mirror differences

- Monitor InterSystems IRIS license status

- Monitor journal purging

- Monitor license usage

- Monitor mirror health

- Review Web Gateway error log

2.5.3 Other

- Check system file permissions

- Create system performance report

- Determine if auditing namespace needs more audit databases

- Monitor email

- Monitor endpoints

- Monitor web services

- Run the Tune Table utility on the ATNA audit database tables

2.6 See Also

- Defining a Monitoring and Operations Plan

- Monitoring and Operations Task Reference

3

Tasks by Frequency of Performance

This topic organizes the day-to-day operations and monitoring tasks by frequency of performance.

3.1 Constantly

The following table lists tasks that either require constant monitoring or should be performed more than once every five minutes:

Table 3–1: Constantly

Task	Notes
Check ping	
Check SSH	
Monitor CPU utilization	Alert on high CPU utilization.
Monitor for errors using Health Monitor and Log Monitor	
Monitor for memory swapping	
Monitor for mirror differences	Each time you make manual changes on a mirror member, you should decide if you need to make the same changes on the other mirror members.
Monitor for network packet dGOPS or retransmissions	Alert when excessive rates of network packet dGOPS or retransmissions occur.
Monitor InterSystems IRIS queues	Alert when memory swapping occurs.
Monitor memory utilization	Alert on high memory utilization.
Review Web Gateway error log	Alert on errors.
Review web server error logs	Alert on errors.

3.2 Hourly

The following table lists tasks that should be performed hourly:

Table 3–2: Hourly

Task	Notes
Monitor any externally mounted file systems	
Monitor disk fill rate	Alert on sudden increase in disk fill rate.
Monitor DNS infrastructure	
Monitor endpoints	
Monitor InterSystems IRIS productions	
Monitor journal space	Running out of space might cause an instance to become unavailable.
Monitor license usage	
Monitor system clock time	
Monitor total processes	Alert on sudden increase in total processes.
Monitor web servers	
Monitor web services	

3.3 Daily

The following table lists tasks that should be performed daily:

Table 3–3: Daily

Task	Notes
Check messages.log	
Check Production Event Log	
Ensure tasks are running correctly	
Monitor certificate expiration dates	
Monitor disk space	
Monitor email	
Monitor for file system errors	
Monitor InterSystems IRIS license status	
Monitor journal purging	

Task	Notes
Monitor mirror health	
Monitor size of IRIS.DAT	
Monitor uptime	
Create system performance report	

3.4 Monthly

The following table lists tasks that should be performed monthly:

Table 3–4: Monthly

Task	Notes
Determine if auditing namespace needs more audit databases	
Run DataCheck for mirrored systems	

3.5 Biannually

The following table lists tasks that should be performed biannually:

Table 3–5: Biannually

Task	Notes
Evaluate global buffer size	
Evaluate routine buffer size	

3.6 Annually

The following table lists tasks that should be performed annually:

Table 3–6: Annually

Task	Notes
Evaluate lock table size	
Evaluate maximum memory per process size	
Evaluate size of shared memory heap	

3.7 Variable

The following table lists tasks that should be performed as needed. Review them to determine appropriate timing based on your systems and the needs of your organization.

Table 3–7: Variable

Task	Notes
Run database backups	
Run integrity check	
Verify integrity of database backups	
Run the Tune Table utility on the ATNA audit database tables	If you make a change to your system's data ingestion, for example adding IHE documents or DICOM data, run tune table after one month of collecting the new data.
Check system file permissions	

3.8 See Also

- Defining a Monitoring and Operations Plan

- Monitoring and Operations Task Reference

4

Tasks by Role

This topic organizes the day-to-day operations and monitoring tasks by the role of the administrator who is performing them. Note that these roles are examples and may not exactly match roles in your organization.

4.1 OS Administrator

An operating system (OS) administrator should perform the following tasks:

- Monitor email
- Monitor web servers
- Review web server error logs

4.2 SAN Administrator

A storage area network (SAN) administrator should perform the following tasks:

- Monitor CPU utilization
- Monitor disk fill rate
- Monitor disk space
- Monitor for file system errors
- Monitor for memory swapping
- Monitor memory utilization

4.3 Network Administrator

A network administrator should perform the following tasks:

- Check ping

- Check SSH

- Monitor DNS infrastructure

- Monitor endpoints

- Monitor externally mounted file systems

- Monitor for network packet dGOPS or retransmissions

- Monitor system clock time

- Monitor total processes

- Monitor uptime

4.4 IRIS Administrator

An InterSystems IRIS administrator should perform the following tasks:

- Check messages.log

- Check system file permissions

- Create System Performance report

- Determine if auditing namespace needs more audit databases

- Ensure tasks are running correctly

- Evaluate global buffer size

- Evaluate lock table size

- Evaluate maximum memory per process size

- Evaluate routine buffer size

- Evaluate size of shared memory heap

- Monitor certificate expiration dates

- Monitor for errors using Health Monitor and Log Monitor

- Monitor for mirror differences

- Monitor InterSystems IRIS license status

- Monitor journal purging

- Monitor license usage

- Monitor mirror health

- Monitor web services

- Review Web Gateway error log

- Run the Tune Table utility on the ATNA audit database tables

4.5 Interface Administrator

An interface administrator should perform the following tasks:

- Check Production Event Log

- Monitor InterSystems IRIS productions

- Monitor InterSystems IRIS queues

4.6 Database Administrator

A database administrator should perform the following tasks:

- Monitor journal space

- Monitor size of IRIS.DAT

- Run database backups

- Run DataCheck for mirrored systems

- Run integrity checks

- Verify integrity of database backups

4.7 See Also

- Defining a Monitoring and Operations Plan

- Monitoring and Operations Task Reference

5

Troubleshooting Assistance

This topic provides tasks and actions that may be useful when trying to troubleshooting an issue.

Important: If your problem requires urgent attention, call the WRC for immediate help.

5.1 General Troubleshooting

This section contains advice and steps to follow in any troubleshooting scenario.

Pinpoint where and when the issue originated.

- What do you observe when the problem happens? Is there an error message? What specifically goes wrong?

- What time did the issue start?

- Does the problem appear at a certain time of day or day of the week?

- Where did the problem first appear? If your system has multiple instances, on which one did the problem start?

- Has anything changed on the system recently that may have caused the issue?

Review the logs for warnings, errors, and alerts.

The following logs may contain useful information about the issue. Look for warnings, errors, or alerts around the time that the issue began.

- Check messages.log.

- Check Production Event Log.

- Review Application Error Log.

- Check the audit log. In particular, look for <PROTECT> errors. See Auditing Guide.

- Review Web Gateway Error Log.

- Review Web Server Error Log.

5.2 Troubleshooting Licensing

Ensure the InterSystems IRIS license is valid and current.

- Monitor License Usage.

- Monitor License Status.

5.3 Troubleshooting Mirroring

Check the Mirror Monitor and Mirror Status Monitor.

- Is journaling caught up?

- Monitor Mirror Health.

- Monitor for Mirror Differences.

Ensure the InterSystems IRIS license is valid and current.

- Monitor License Usage.

- Monitor License Status.

5.4 Contact the WRC

The InterSystems Worldwide Response Center (WRC) is available to help diagnose and resolve any issues that may arise. Whatever information you have can help the WRC quickly identify what is causing the issue. This section describes steps you can perform to provide the WRC with as much information as possible.

Note: If your problem requires urgent attention, the fastest way to receive help is by calling the WRC.

Summarize the issue.

- Can the issue be reproduced? Does it occur consistently?

- Has anything changed on the system recently that may have caused the issue?

Record the version information for InterSystems IRIS and its operating system.

- The $ZVERSION variable contains this useful information.

Run monitoring utilities.

- Run Diagnostic Report in Management Portal.

- If the system is in a hung state, run IRISHung.

- If this is a performance problem, create System Performance Report using ^SystemPerformance.

Get in touch with the WRC

- Go to the InterSystems Worldwide Response Center (WRC) site for assistance.

- Inform the WRC about the urgency of your issue, how soon you need it to be resolved, and how to best communicate with you.

Monitoring and Operations Tasks

This reference section provides instructions for each monitoring and operations task.

Check messages.log

Check the messages.log file and configure email alerts.

Description

Manually check the messages.log file for error or warning messages. Alternatively, you can configure your instance to send alerts to an administrator via the Log Monitor. If you do not configure automatic alerts, you should manually check messages.log at least once per day.

Instructions

You can access the messages.log file either via your file system (`<install-dir>/mgr/messages.log`) or via the Management Portal (**System Operation** > **System Logs** > **Messages Log**).

Check Ping

Check web server response to ping.

Instructions

Use an automation tool of your choice to periodically ping your web servers and confirm that they are responding correctly.

Check Production Event Log

Check the Production Event Log for errors and warnings.

Description

Periodically check the Production Event Log for errors and warnings. You can also configure the Event Log to send alerts when errors or warnings occur.

Instructions

For more information on the Production Event Log, see Viewing the Event Log.

Check SSH

Check ability to connect to web server via Secure Shell (SSH).

Instructions

Use an automation tool of your choice to periodically confirm that you can connect to your web servers via SSH.

Check System File Permissions

Check whether InterSystems IRIS system files conform to necessary permission settings.

Description

Check whether InterSystems IRIS system files conform to necessary permission settings, to ensure that the instance does not encounter problems starting or running due to incorrect permissions, owners, or groups.

This utility first checks directories and files created at installation against /mgr/filecheck.isc, which contains a snapshot of the files captured at the end of installation. The user can edit this file if necessary. Then it checks databases, journals, and WIJ files.

By default, `filecheck` checks for the following:

- `rw` for databases and streams.

- `rwx` for database and stream directories.

- `rw` for journals and WIJ files.

- `rwx` for journal and WIJ directories.

Discrepancies are logged in filecheck.log, with one error per line. If no errors are found, this file will be empty.

Instructions

Accessing the Utility

You can access the `filecheck` utility in the following ways:

- Directly: `> iris filecheck <instance> [format]`

- As a parameter during startup: `> iris start <instance> filecheck`

Recreating /mgr/filecheck.isc

If /mgr/filecheck.isc is deleted or otherwise corrupted, it can be recreated using the **iris filecheck update** command. Note that the update could include temporary files created after installation, which could cause errors if they are deleted. The **update** command should therefore only be used if necessary, and may require manual edits to /mgr/filecheck.isc.

Overriding Default Permission Checks

To override default permission checks, create entries in /mgr/filecheck_perm.isc (This file does not exist initially and must be created if needed). The system defaults as entries in /mgr/filecheck_perm.isc would look like this:

```
****rw-*** * irisusr DatabaseFile
****rwx*** * irisusr DatabaseDirectory
****rw-*** * irisusr JournalFile
****rwx*** * irisusr JournalDirectory
```

The use of asterisks in the strings for permissions and owners (and potentially groups) instructs `filecheck` to allow any values for those positions. Only the positions with explicit values (the group permissions in the examples) are checked.

Logging Errors in Machine-Readable Format

By default, errors are logged in text format. Users can use the optional `format` parameter to log errors in the following machine-readable CSV format:

```
<ErrorType>,<FileType>,<MismatchType>,<ExpectedString>,<CurrentString>,<FileName>
```

ErrorType

Mismatch

Table A–1:

MismatchType	Permitted values are `Permission`, `Owner`, or `Group`.
ExpectedString	The permission, owner, or group string that is required.
CurrentString	The actual current permission, owner, or group string.

Missing

The file is missing.

Error n

n is an error number.

FileType

Table A–2:

t	Top directory (from filecheck.isc)
i	Installation directory (from filecheck.isc)
d	Database file or directory
s	Stream file or directory
j	Journal file or directory
w	WIJ file or directory

FileName

The complete file name or directory path.

For example, a machine-readable entry might look like this:

Mismatch,i,Permission,-r--r--r-x,-r--r--r--,/usr/local/etc/irissys/CSP_options

Create System Performance Report

Create system performance reports.

Description

Periodically create system performance reports, which you can examine or archive. An archive of daily system performance reports can also help the InterSystems Worldwide Response Center (WRC) diagnose problems in your system.

Instructions

You should use the **^SystemPerformance** utility to create performance reports. For more information, see Monitoring Performance Using ^SystemPerformance.

Determine if Auditing Namespace Needs More Audit Databases

Determine if the auditing namespace needs more audit databases.

Description

Periodically determine if you should add more auditing databases to your audit namespace in response to large audit databases sizes. Having large audit databases can create a logistical challenge as creating database backups, running integrity checks, and other maintenance tasks may take a long time to complete.

Instructions

Contact the Worldwide Response Center (WRC) for more information about how you can use IRIS for Health tools to separate a large audit repository database into multiple, smaller databases.

Ensure Tasks are Running Correctly

Ensure that your Task Manager tasks are running correctly.

Description

InterSystems IRIS systems contain scheduled tasks for a variety of activities, like updates to usage dashboard data and purges of outdated messages. Ensure that these tasks are running correctly and without errors. Ensure that your audit aggregation tasks are not suspended.

Instructions

For more information on the Task Manager, see Using the Task Manager.

Evaluate Global Buffer Size

Evaluate your global buffer size.

Description

Periodically evaluate the size of your global buffers and decide whether or not to increase their size based on the size and growth of your systems.

Evaluate Lock Table Size

Evaluate your lock table size.

Description

Periodically evaluate the size of your lock table and decide whether or not to increase its size based on the size and growth of your systems.

Evaluate Maximum Memory per Process Size

Evaluate the size of the maximum memory per process.

Description

Periodically evaluate the maximum memory per process of your instance and decide whether or not to increase its size based on the size and growth of your systems.

Instructions

For information on `bbsiz`, see bbsiz. If you need further guidance, contact InterSystems support, who will put you in touch with the InterSystems Sizing and Performance group.

Evaluate Routine Buffer Size

Evaluate your routine buffer size.

Description

Periodically evaluate the size of your routine buffers and decide whether or not to increase their size based on the size and growth of your systems.

Evaluate Size of Shared Memory Heap

Evaluate the size of the shared memory heap (`gmheap`).

Description

Periodically evaluate the size of your shared memory heap and decide whether or not to increase its size based on the size and growth of your systems.

Monitor Certificate Expiration Dates

Ensure that your certificates will not expire soon.

Description

Monitor when your certificates will expire. You should send alerts at certain thresholds prior to certificate expiration dates. For example, you might choose to send alerts 60 days prior to expiration and 30 days prior to expiration.

Instructions

You can use ObjectScript to determine whether certificates have expired, using the **X509GetField()** method of the %SYSTEM.Encryption class, as follows:

```
set expDate = %SYSTEM.Encryption.X509GetField(certificateText,'ValidityNotAfter')
```

By comparing the current date to the value of `expDate`, you can determine whether to send alerts.

If you prefer, you can use a third-party monitoring tool to automate this task.

Monitor CPU Utilization

Monitor the system for heavy CPU utilization.

Description

Monitor your system for heavy CPU utilization by comparing the current load on the system with the average load.

Instructions

You can use either the InterSystems IRIS Health Monitor or a third-party monitoring tool to monitor your CPU utilization. For more information on the Health Monitor, see Using the System Monitor.

Monitor Disk Fill Rate

Monitor the disk fill rate of your file system.

Description

Monitor the amount of data that is being written per hour in your file system, as well as the amount of time remaining until your file system is full.

Instructions

Use any tool that can graph disk space over time and give the disk fill rate for a system. The InterSystems IRIS Systems Alerting and Monitoring Application (SAM) provides this functionality. For more information on SAM, see System Alerting and Monitoring.

Monitor Disk Space

Monitor the available disk space in your file system.

Description

Monitor the percentage of free disk space available in your file system. Running out of disk space can lead to stopped applications, slow systems, and potential halts to the operation of your business.

Instructions

You can use a third-party monitoring tool to monitor the percentage of free disk space available in your file system. InterSystems IRIS instances also provide this information in the Management Portal (**System Operation** > **Databases** > **Free Space View** radio button) and via `^%FREECNT`.

Monitor DNS Infrastructure

Monitor your DNS infrastructure.

Description

Monitor your DNS infrastructure as you see fit, for example by checking if the local DNS server is responding and returning what you expect within the expected time frame.

Instructions

Determine the best solution for your organization based on your systems and available tools.

Monitor Email

Monitor your system's ability to send email.

Description

If you have a system that regularly sends emails, periodically confirm that the system can successfully send emails.

Instructions

Determine the best solution for your organization based on your systems and available tools.

Monitor Endpoints

Optionally monitor your important endpoints.

Description

Optionally monitor your important endpoints to ensure that they are functioning correctly, for example by logging in to your instances and exercising those endpoints through automation software. However, if you decide to perform this type of monitoring for your important endpoints, you should ensure that you do so in a secure manner.

Instructions

You should use an automation tool of your choice to automate this task.

Monitor Externally Mounted File Systems

Monitor any externally mounted file systems.

Description

If you are using externally mounted file systems, monitor them as you see fit.

Instructions

Determine the best solution for your organization based on your systems and available tools.

Monitor for File System Errors

Monitor for file system errors.

Description

Monitor for errors in your file system. File system errors can lead to database degradation and should be addressed as soon as possible. If file system errors occur where IRIS.DAT files are stored, InterSystems recommends that you perform an InterSystems IRIS database integrity check.

Instructions

Use SAN or OS utilities of your choice.

Monitor for Errors Using the Health Monitor and Log Monitor

Monitor for errors and warnings using the Health Monitor and Log Monitor

Description

Ensure that you have properly configured the Health Monitor to write error and warning messages to messages.log. You should additionally ensure that you have properly configured the Log Monitor to send alerts to administrators based on the errors and warnings in messages.log.

Several other monitoring tasks that are described in this reference, such as monitoring CPU utilization and license status, can be performed with the Health Monitor and the Log Monitor. The Health Monitor will also report on many other types of errors, such as <STORE> errors and lock table full errors.

Instructions

More information on the Log Monitor can be found in Log Monitor.

You can use either the InterSystems IRIS Health Monitor or a third-party monitoring tool to monitor your CPU utilization. For more information on the InterSystems IRIS Health Monitor, see Health Monitor.

Monitor for Memory Swapping

Monitor if memory swapping is occurring in your system.

Description

Monitor whether or not memory swapping is occurring in your system. If memory swapping occurs, an administrator should be notified.

Instructions

Use a third-party monitoring tool of your choice.

Monitor for Mirror Differences

Monitor for differences between mirror instances.

Description

Monitor for differences in your mirror instances that are not mirrored across instances. For example, if you make a change to scheduled tasks on one instance, you should ensure that you make the same change on all other mirror members that are a part of the same mirror. For more information on differences that are not mirrored across instances, see Mirror Configuration Guidelines.

Instructions

Manually inspect changes to each instance and ensure that you make the same change on all other mirror members that are a part of the same mirror.

Monitor for Network Packet DGOPS or Retransmissions

Monitor if network packet dGOPS or retransmissions occur.

Description

Monitor whether or not packet dGOPS or retransmissions occur in your network. If excessive rates of packet dGOPS or retransmissions occur, an administrator should be notified.

Instructions

Use a third-party monitoring tool of your choice.

Monitor InterSystems IRIS License Status

Ensure that your InterSystems IRIS license will not expire soon.

Description

Monitor when your InterSystems IRIS license is going to expire. You should send alerts at certain thresholds prior to the expiration date of your license. For example, you might choose to send alerts 60 days prior to expiration and 30 days prior to expiration.

Instructions

You can use the Health Monitor to monitor your InterSystems IRIS license status. For more information, see Health Monitor.

Monitor InterSystems IRIS Productions

Monitor your InterSystems IRIS productions.

Description

Monitor the state of your InterSystems IRIS productions. For example, you can monitor whether or not your productions are running, and whether or not they are in bad states.

Instructions

You should use the Production Monitor to monitor your productions. For more information, see Using the Production Monitor Page.

Monitor InterSystems IRIS Queues

Monitor your InterSystems IRIS queues.

Description

Monitor your queues to ensure that excessive queueing is not occurring.

Instructions

You should use the Production Monitor to monitor your queues. For more information, see Monitoring Production Queues.

Monitor Journal Purging

Monitor if journals are purging normally.

Instructions

You should check messages.log for error or warning messages related to journal purging and check your journal file directories to ensure that the files are being purged correctly. You can perform these tasks manually or create automation to do so.

Monitor Journal Space

Monitor your journal space.

Description

Monitor the percentage of free space and fill rate in the two directories where your primary and alternate journals are stored.

Instructions

You can use either a third party monitoring tool or the Health Monitor and the Log Monitor to perform this task.

Monitor License Usage

Monitor your license usage.

Description

Monitor your InterSystems IRIS license usage so that you do not add more users or cores than you have licenses for.

Instructions

Your InterSystems IRIS instance maintains an independent local view of its license capacity and current use. For more information, see Managing InterSystems IRIS Licensing.

Monitor Memory Utilization

Monitor the memory utilization of your system.

Description

Monitor the memory utilization of your system. Monitor both the percentage of available memory and the percentage of available swap space.

Instructions

You can use either the InterSystems IRIS Health Monitor or a third-party monitoring tool to monitor your memory utilization. For more information on the Health Monitor, see Health Monitor.

Monitor Mirror Health

Monitor the health of your mirrors.

Description

Monitor the health of your mirrors, such as by ensuring that are all databases are caught up on the backup and async instances.

Instructions

Use the Mirror Monitor to monitor the health of your mirrors. In addition, many mirroring-related error and warning messages are logged in messages.log. For more information on the Mirror Monitor, see Managing Mirroring.

Monitor Size of IRIS.DAT

Monitor the size of your IRIS.DAT file.

Instructions

Determine the best solution for your organization based on your systems and available tools.

Monitor System Clock Time

Monitor that system clocks across all your systems are set to the same time.

Instructions

Determine the best solution for your organization based on your systems and available tools.

Monitor Total Processes

Monitor the total number of processes running on your system, including user and system processes.

Description

Monitor the total number of processes running on your system. Failure to properly monitor total processes can lead to performance issues or server crashes.

Instructions

The tools available for monitoring processes differ based on your operating system. As a guideline, you may want to obtain a baseline number of processes during normal operation of your system, and send alerts when the number of processes is two or more standard deviations above the baseline.

Monitor Uptime

Monitor the amount of time that your system has been running.

Instructions

The tools available for monitoring uptime differ based on your operating system. System uptime information for InterSystems IRIS instances is available on the Management Portal home page.

Monitor Web Servers

Verify that web servers are responding, and in a timely manner.

Instructions

You can use a third-party monitoring tool to automate this task.

Monitor Web Services

Verify that your SOAP and REST web services are responding, and in a timely manner.

Instructions

You can use a third-party monitoring tool to automate this task. For example, you might use your monitoring tool to test one SOAP or REST web service method per namespace in your federation. If you do so, ensure that you are testing methods that execute quickly and that don't make any changes to data.

Review Application Error Log

Review errors and warnings in your Application Error Log.

Instructions

You can review the Application Error Log via a user interface in the Management Portal, or programmatically. For more information, see Monitoring InterSystems IRIS Using the Management Portal.

Review Web Gateway Error Log

Review errors in your Web Gateway error log.

Description

Review errors and warnings in your Web Gateway error log file, CSP.log.

Instructions

Use a third-party monitoring tool to examine your Web Gateway error log and alert administrators when errors or warnings occur.

Review Web Server Error Log

Review errors and warnings in your web server error log.

Instructions

Use a third-party monitoring tool to examine your web server's error log and alert administrators when errors or warnings occur.

Run Database Backups

Run database backups for your system.

Description

Run database backups for your system on a regular basis, so that you can restore your databases and configuration after a data loss event.

Instructions

Use the tools that your hardware vendor provides for taking disc snapshots. For more information on creating external backups, see External Backup. InterSystems strongly recommends that you *do not use* InterSystems IRIS online backup for production InterSystems IRIS systems.

Run DataCheck for Mirrored Systems

Run DataCheck if you have a mirrored system.

Description

If your system is mirrored, you should periodically run DataCheck to confirm that your mirrored databases are consistent with each other.

Instructions

For instructions on setting up and running Datacheck, see Data Consistency on Multiple Systems.

Run Diagnostic Report

Run a Diagnostic Report and send the results to the WRC

Description

When diagnosing an issue or problem with the Worldwide Response Center (WRC), create a Diagnostic Report. The report contains information that the WRC can use to identify the issues with your instance.

Instructions

You can run a Diagnostic Report from the **Diagnostic Report** page of the Management Portal (**System Operation** > **Diagnostic Reports**). For more information, see Using the InterSystems Diagnostic Report.

Run Integrity Checks

Run and examine the output of integrity checks.

Description

Periodically run integrity checks on your databases and examine the output. If a production runs on a database that has an integrity issue, it's possible that the issue will spread and cause even more integrity issues. Running integrity checks to find integrity issues is very important for the health of your system. Finding integrity issues early makes it possible to remedy them and prevent them from spreading.

Instructions

You can run integrity checks via the Management Portal or the Terminal. For more information, see Verifying Structural Integrity.

Run IRISHung

Run and examine the output of IRISHung.

Description

When diagnosing an issue or problem with an InterSystems IRIS® data platforms instance in a hung state, use the `IRISHung` utility.

Instructions

1. Log in as an administrator

2. In a terminal window, run the IRISHung script in the directory, <install-dir>/bin.

    The scripts corresponding to supported systems are:

    *   Windows: IRISHung.cmd

    *   UNIX®, Linux, AIX, and so on: IRISHung.sh

3. Send the resulting output file to the InterSystems Worldwide Response Center. You can email the file to support@inter-systems.com, open a new problem using the WRC Online, or call the Center directly for additional assistance.

For more information, see IRISHung Script.

Run the Tune Table Utility on the ATNA Audit Database Tables

Optimize SQL querying of the audit tables for management reports and custom queries

Description

In order to minimize the time that it takes to run management reports based on audit data, or to query the audit tables using a custom query, your audit tables should be optimized with the Tune Table utility.

Instructions

Tune Table requires a representative set of data in your audit tables in order to effectively analyze and optimize querying. After one month of receiving data and having users log in and look up data in your system, run tune table on the following ATNA schemas:

• HS_IHE_ATNA_Repository

• HS_IHE_ATNA_Repository_Data

If you receive DICOM data, also run tune table on the following schema:

• HS_IHE_ATNA_Repository_DICOMData

If you make a change to your system's data ingestion, for example adding IHE documents or DICOM data. You should run tune table again after one month of collecting the new data.

Note: As tune table uses system resources, it should be run in off hours. Running tune table on a very large audit database with terabytes of data in a live system is not recommended. If a test system has a representative set of data, then one option is to run tune table on the test system and export the result to the live system.

For details on running the tune table utility, see Tune Table.

Verify Integrity of Database Backups

Verify the integrity of your database backups.

Description

Periodically verify the integrity of your database backups to ensure that your database backup mechanism is creating backups correctly.

Instructions

Verifying the integrity of a database backup is a highly manual process. You should restore your backup to a test system and perform smoke tests to ensure that your system continues to function normally. Ensure that your productions can start and that there are not large numbers of error or warning messages in your log files. If possible, you may want to attempt processing new data.