WHITEPAPER

DISASTER RECOVERY PLANNING FOR INGRES

Specific Information and Issues to Recovery of an Ingres Installation

BY CHIP NICKOLETT, INGRES CORPORATION

TABLE OF CONTENTS:

About the Author

Chip Nickolett is the Director of Consulting Services for the Americas at Ingres. He has over 23 years of business and IT experience, and has been using Ingres RDBMS technology for over 20 years. Chip has been developing Disaster Recovery Plans since 1991, and he is a recognized expert in performance tuning and management of mission-critical Ingres installations.

DISASTER RECOVERY PLANNING FOR INGRES

PREFACE

The "unexpected" has just happened. The cost and business impact to your company now depends on just how well prepared you are. This white paper discusses key concepts and considerations in planning and preparing for the post-disaster recovery of an Ingres installation.

OVERVIEW

Disaster recovery planning can mean different things to different people. To many organizations, it is as simple as having offsite backups available. To other organizations it involves having warm sites for machine restoration and infrastructure, and even workspace for business continuity. In order to keep this article brief and focused on Ingres, we will primarily review information and issues specific to the recovery of an Ingres installation on an alternate machine.

Does your site require a Disaster Recovery Plan (DRP), and if so, why? This is a question that only you can answer, but here are a couple of questions to think about: Does your organization rely on applications that run on Ingres? What is the business impact of not having those applications available? Is there a cost associated with not having these systems available? For example, if your sales order entry and processing system is not available, what is the cost of lost sales and/or products not delivered on schedule? What will the perception of your company be if your customers are unable to obtain products or services when they need them? Are there service level agreements that your organization has committed to? The answers to these questions can give you a good idea as to whether or not a disaster recovery plan is required for your site.

What is the cost of a DRP? There is no simple answer for this, but assume that it will be expensive. It will require plan development and testing, project management, additional hardware and infrastructure (purchased, leased, or provided by a third party), and frequent plan review and testing. Generally a cost/benefit analysis is performed to determine if the cost of a significant loss of service (generally > 24 hours) and/or loss of data exceeds the cost of developing and maintaining a DRP.

DEVELOPING A PLAN

Plan development is very important. Information needs to be comprehensive and extremely detailed. Nothing should be left to chance. The plan and procedures should be developed as if someone with only minimal technical experience is going to execute them (as, indeed, may be the case). Specific commands should be provided, along with representative output from those commands. Each specific procedure then provides background as to the goal of the procedure, prerequisite steps, detailed instructions, and troubleshooting. A decision tree that is easy to read and follow (see example below), and that references specific sections within a procedure, should be created along with the detailed procedures. These become "living and breathing" documents that need to be reviewed and updated frequently. Below are some specific issues that need to be addressed for an Ingres DRP.

Do you know what your specific Ingres release and patch levels are? Is your site running with any non-standard binaries/executables? Do you have the installation and patch media available at an offsite location? Has that media been validated? Without having this baseline product information and installation media, your site could be forced to recover under a different version of Ingres. Don't assume that you will be able to obtain the desired release or patch level from Ingres Corporation, since they primarily provide only current releases and patch levels. Running an untested release/patch level has the potential to introduce new problems and should therefore be avoided whenever possible.

ASSUMPTIONS

First, it is assumed that your recovery machine will be of the same type and capacity as the production machine. The machine can be larger and/or have greater capacity, but trying to recover on a different platform or on a machine that has less capacity introduces numerous issues and significantly complicates this process. The goal is to make the recovery machine look and behave identically to the production machine. This includes peripheral devices such as tape drives. For example, if the production machine performs a parallel checkpoint to several tape drives then ideally the recovery machine should have the same number of compatible drives, and those tape devices should have the same system identification. Failure to do this will require manual intervention and likely script / command file modifications.

CUSTOMIZATION AND CONFIGURATION

Have there been any site-specific modifications? Two examples of this that I have encountered several times are customized keymap files and customized checkpoint files. Other information that should be gathered on a frequent basis is symbol table information/logical definitions, a list of physical locations and paths, "infodb" output for all databases (including iidbdb), copies of the config.dat and protect.dat files, and ASCII output from the SQL statements "help table *; help index *; select * from iifile_info;". Finally, don't forget about operating system configuration. Ingres generally requires some OS tuning on most platforms to run and therefore it is important to have that information readily available. This information will allow you to re-create your production environment in the shortest possible amount of time, and provide additional information required to troubleshoot problems.

RESTORING THE DATA

Once the machine is configured and Ingres is installed it will be time to restore the database. This can either be performed using the rollforwarddb process, or using the output from "unloaddb" (ASCII unloads, while larger, are preferred for portability and recoverability reasons). Hopefully the media containing the recovery data has been validated and is good. It is good practice to have more than one set of media available for recovery in the event of problems. This could either be duplicate / mirror copies from the same date, or a backup from an earlier date. Generally it is desirable to try to recover up to the point of failure, and that requires current journal files and the Ingres configuration file (aaaaaaaa.cnf). One method of minimizing data loss is to have a process that periodically copies these files to another machine, ideally at another location.

TROUBLESHOOTING

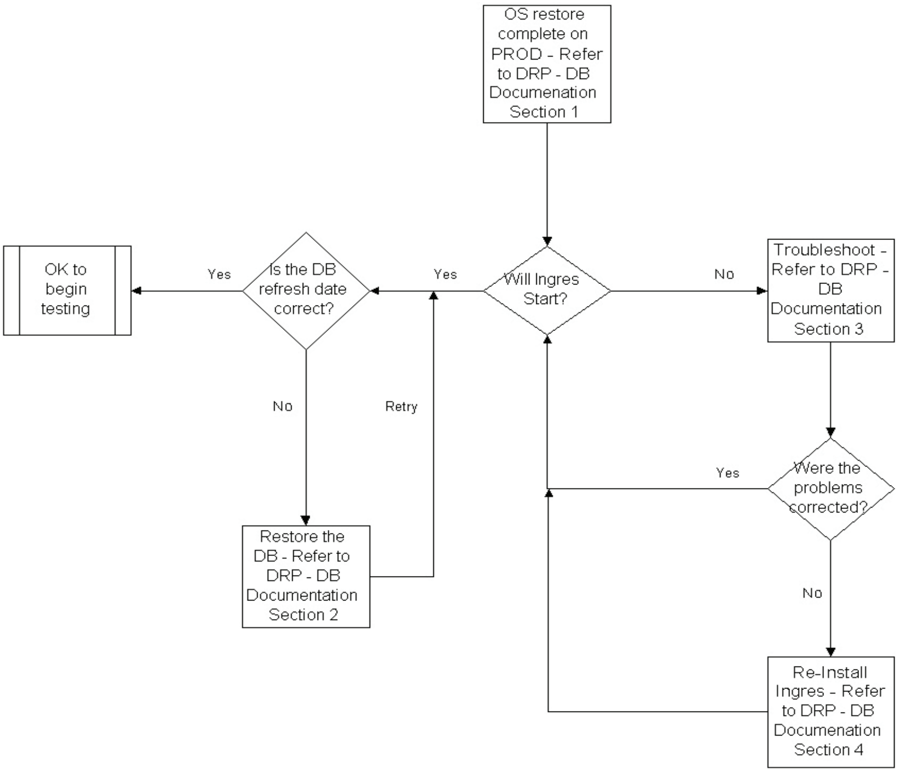
Common problems encountered during recovery on another machine include: missing or incorrect directory path; incorrect directory permission or ownership; OS kernel parameters are insufficient to support Ingres; the hostname is incorrect. Whenever possible the hostname of the recovery machine should be the same as on the production machine. This is because Ingres embeds that information in several locations and files. If using the same hostname is not possible then Ingres will likely require manual changes to the configuration files before it will start. Those changes including substitution of the new hostname for the old hostname in the $II_SYSTEM/ingres/files/config.dat and protect.dat files, possible changes to the symbol table (use "ingprenv" to view the current settings and "ingsetenv" to make changes). If your installation uses Ingres/NET then you will also need to rename files in the $II_SYSTEM/ingres/files/name directory, again substituting the current hostname with the old hostname (this time for the file name, not the contents). If you are still encountering problems then review the $II_SYSTEM/ingres/files/errlog.log file to see what Ingres states the problem is.

With some of the older versions of Ingres (OpenIngres 2.0 to some early patch levels of Advantage Ingres 2.5) may encounter problems with LicenseIT, the license management system used many years ago. LicenseIT uses the "MAC" address on a machine to uniquely identify it for the purposes of authentication. This can cause problems with things like redundant network cards on the production machine, and will almost definitely cause problems on a different machine. The very first thing that should be done if a recovery scenario is anticipated is to contact Ingres Technical Support and request a temporary license file (a.k.a. "lifeboat string"). If you are not using other CA products that use LicenseIT then it is possible to just perform a "fresh", generic install and then overlay the non-license directories from a backup tape (on Unix the license directories are '/ca_lic'and '/usr/local/Calib'). This will place your installation in the 30-day grace period and provide an extra buffer for getting an authorized license file.

On even older Ingres 6.x or OpenIngres 1.x Installations you may need to contact Ingres Technical Support for a "lifeboat string" for the license string (found in the symbol table and displayed using the "ingprenv" command). These older versions are mentioned because many are still in production - a testament to the production quality and enterprise strength of Ingres. But, for the sake of support and recovery, it should be noted that it is always a best practice to have production systems running currently support versions of products.

ALMOST THERE!

Once the procedures have been developed and unit tested, it is time for a comprehensive test of the entire plan. During plan execution it is important to take good notes on everything that is done or that occurs. This provides data for analysis in the event of problems (e.g., did a step fail because a predecessor step was not executed?), including specific error messages and information about the problem. It is important to collect this information as you go since it is very easy to forget what was done or exactly what happened. It is also good practice to document the amount of time required for each step. That will allow you to provide accurate estimates in the event of a real recovery situation.


OS restore complete on PROD - Refer to DRP - DB Documenation Section 1
OK to begin testing
Yes
Is the DB refresh date correct?
Yes
Will Ingres Start?
No
Troubleshoot - Refer to DRP - DB Documentation Section 3
No
Retry
Yes
Were the problems corrected?
Restore the DB - Refer to DRP - DB Documentation Section 2
No
Re-Install Ingres - Refer to DRP - DB Documenation Section 4

Once the Ingres installation is restored how will you know that it works? The validation process needs to include some type of data validation, validation that your "customers" can access their applications, and that those applications can access the database. If any special equipment is required (barcode scanners, printers, wireless devices, etc.) then it is important to test those devices as well. Often you will find that little problems such as hostnames or IP addresses being different cause startup or connectivity problems, or routing and/or firewall problems cause remote access issues. These are the types of issues that the full test of the plan is intended to uncover. There is usually, but not always, a work-around for these problems. For that reason it is important to develop a contingency plan for areas that are more prone to encountering problems.

And finally, once everything is up and running, has been validated, and is ready to go, your first instinct will probably be to allow users into the system, but resist! We recommend that you checkpoint the database(s) and enable journaling. This provides the maximum amount of protection while running at the hotsite, and makes it easier to transport the new database back to the production machines once that environment has been restored. After the checkpoint completes then it is safe to proceed with business as usual. *Please note that this is now your production environment and should therefore be treated as such. The restored environment should include routine maintenance and checkpoints, just as would be done in ordinary production.*

SUMMARY

With the proper planning it is possible to restore mission-critical systems in a minimal amount of time. When care is taken to address the specific issues mentioned above, it is fairly easy to restore a production Ingres installation. The procedures developed can also be used for things such as system migrations, addressing minor failures, and DBA training, so there is other value associated with their development. A good DRP is similar to a life insurance policy. Premiums are paid on a regular basis with the hope of not having to “take advantage” of that policy. But, if and when needed, that protection can prove to be priceless.

NOTES

NOTES

About Ingres Corporation

Ingres Corporation is a leading provider of open source database management software. Built on over 25 years of technology investment, Ingres is a leader in software and service innovation, providing the enterprise with proven reliability combined with the value and flexibility of open source. The company's partnerships with leading open source providers further enhance the Ingres value proposition. Ingres has major development, sales and support centers throughout the world, supporting thousands of customers in the United States and internationally.

INGRES CORPORATION : 500 ARGUELLO STREET : SUITE 200 : REDWOOD CITY, CALIFORNIA 94063
PHONE 650.587.5500 : FAX 650.587.5550 : www.ingres.com : For more information, contact info@ingres.com