COMPETITION SENSITIVE

FIT Database HA and DR Strategy Guide

Forcepoint

THESE ITEMS ARE CONTROLLED BY THE U.S. GOVERNMENT AND AUTHORIZED FOR EXPORT ONLY TO THE COUNTRY OF ULTIMATE DESTINATION FOR USE BY THE ULTIMATE CONSIGNEE OR END-USER(S). THEY MAY NOT BE RESOLD, TRANSFERRED, OR OTHERWISE DISPOSED OF, TO ANY OTHER COUNTRY OR TO ANY PERSON OTHER THAN THE AUTHORIZED ULTIMATE CONSIGNEE OR END-USER(S), EITHER IN THEIR ORIGINAL FORM OR AFTER BEING INCORPORATED INTO OTHER ITEMS, WITHOUT FIRST OBTAINING APPROVAL FROM THE U.S. GOVERNMENT OR AS OTHERWISE AUTHORIZED BY U.S. LAW AND REGULATIONS.

Overview

The Forcepoint Insider Threat (FIT) product requires an Oracle database to store product configuration and collected data. This database is key to the operation of the FIT system and customers should be aware of related high availability (HA) and disaster recovery (DR) options and intentionally decide on the balance between cost and risk of potential downtime.

This guide describes several levels of HA and DR options and related details.

General Recommendations

When determining the proper level of HA and DR for your FIT Oracle database, the following are basic recommendations to consider:

- Use enterprise-grade hardware with redundant power, RAID controllers, host bus adapters (HBAs), raided disks, etc., especially in the SAN.
- Ensure all hardware is under warranty with at least next business day response time.
- Ensure backups are stored on separate storage, not on the same storage as the data, and preferably in a geographically separate location.
- Where possible, ensure all database data files are stored on a SAN separate from the database server.
- Keep separate copies of important files like the Oracle Wallet.

Forcepoint vs Customer-Provided Hardware and Software

Forcepoint offers a full shrink-wrap system that makes use of enterprise-grade hardware and software that has been tested specifically with the FIT product and with which the Forcepoint product support team is most familiar.

Forcepoint also offers an Oracle database appliance built on top of the same G2CP OS platform used for the FIT master and collector nodes, including all the related security and compliance configuration and documentation. This appliance is included in a full shrink-wrap system but may also be used on its own. This is the Oracle database environment with which all internal product testing is performed, the product support team is most familiar, and with which customers will have the greatest likelihood of success.

Advantages of using the Forcepoint-provided G2CP Oracle database appliance include:

- Security and compliance hardening has been applied, tested, and documented.
- It is the same environment against which Forecepoint internal testing is performed, including for the quarterly updates.
- Quarterly updates will be provided by Forcepoint to keep security and compliance current.
- This is the environment with which Forcepoint product support is most familiar.

Other customer-provided Oracle database hardware & software configurations are also supported by the FIT product, however the scope of support and assistance will be limited to the FIT product itself. The Forcepoint product support team will not be able to help with OS, database, SAN, security, and compliance configurations with which they are not familiar, and customers may encounter unexpected issues.

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.

Disaster Recovery Levels

When choosing the appropriate plan for HA and DR, consider the following levels:

LEVEL 1 – PROTECTION AGAINST SOFTWARE FAILURE ON DB SERVER

The most basic level of protection is a plan to handle software failure on the local DB server, including problems from misconfiguration, user error, or that might occur when applying the latest OS & DB patches.

Options to consider:

a. Be prepared to reinstall, reconfigure, and reconnect to database storage
   - Reinstall the software from scratch in the event of a problem
   - Estimated Recovery Time – 1-2 days.
   - Cost – None.
   - See FIT Product Installation & Upgrade Guides for details and steps.

b. Use VMWare ESXi virtualization & snapshots (Researching)
   - Make use of virtualization and snapshots to roll back to a known good OS & software image in the event of a problem.
   - Estimated Recovery Time – 2 hours.
   - Cost – Additional VMWare ESXi node licenses.
   - See *Appendix A – Using ESXi Virtualization and Snapshots to Revert to Known Good State* on page 8 for more details & steps.

LEVEL 2 – PROTECTION AGAINST HARDWARE FAILURE ON DB SERVER

In the event of hardware failure on the Oracle DB server, how will the system be recovered and made operational again? These options also cover level 1 recovery.

Options to consider:

a. Cold standby database server – hardware or virtual (Recommended)
   - Use of a separate cold standby server that is installed and updated and ready to take over the database load in the event of a problem.
   - Estimated Recovery Time – 2 hours.
   - Cost – 2nd database server.
   - See *Appendix B – Cold Standby DB Server* on page 9 for more details and steps.

b. Wait for warranty support
   - Wait until the system can be recovered through hardware warranty support.
   - Estimated Recovery Time – 2+ days, depending on warranty response time and severity of failure. May require reinstall from level 1a.
   - Cost – None.

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.

c. Oracle RAC (Requires dedicated DBA and custom install, not using G2CP)
    - Run Oracle RAC for immediate failover.
    - Estimated Recovery Time – Immediate.
    - Cost – 2nd database server, FC switch, double Oracle licenses, RAC licenses.

Note

Oracle RAC is a complex configuration that requires a dedicated Oracle DBA familiar with RAC. It also requires a custom OS install since it is not supported on the Forcepoint-provided G2CP platform. Forcepoint product support is not familiar with RAC, has not tested the product with RAC, and will not be able to help with general system management problems.

LEVEL 3 – PROTECTION AGAINST DATA LOSS ON SAN / NFS SHARE / LOCAL STORAGE

Data loss on the SAN could be caused by user error, corruption, or hardware failure. This kind of loss is the most impactful because it cannot be recreated. If the SAN data is lost, then it is important to have some form of backup of the data itself. If using the option to store Large Object Binary (LOB) outside of Oracle on an NFS share, then the NFS share should be included in this assessment.

Options to consider:

a. Backup data using standard Oracle RMAN or SAN Replication (Recommended)
    - Setup recurring full and incremental backups of the Oracle database and NFS share using Oracle RMAN, SAN replication, etc.
    - Estimated Recovery Time – 1+ days.
        - Recoverable to the point of the last successful backup.
    - Cost – Backup software, storage space for backups.
    - Contact Forcepoint Professional Services to discuss recommended backup options.

b. Backup only core schema configuration & wallet keys data (Recommended Minimum)
    - Estimated Recovery Time:
        - Configuration only – 1 day.
            - Recoverable to the point of the last successful backup.
        - Collected data – **Not possible to recover**.
    - Cost – Minimal storage for core schema.
    - Contact Forcepoint Professional Services to discuss recommended backup options.

LEVEL 4 – PROTECTION AGAINST HARDWARE FAILURE OF SAN

The SAN holds all FIT system configuration and collected data. If the SAN hardware fails, the system will be down until the hardware can be repaired. If a second SAN and database server can be allocated, then the system can be redirected to

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.

use this alternate hardware. Often this duplicate hardware is in a geographically separate data center to achieve geographic redundancy. Full duplication of hardware also addresses protection levels 1-3 above.

Options to consider:

a. Replication to a 2nd complete FIT system using Oracle Data Guard
    - Estimated Recovery Time – 4 hours.
        - DataGuard has multiple protection modes to consider, which vary the time window for data loss. Max Protection mode results in the least amount of data loss.
    - Cost – Double hardware – servers, SAN, etc., offsite hosting location. Double Oracle licenses, plus cost of DataGuard.
    - Contact Forcepoint Professional Services to discuss recommended replication options.

b. Wait for warranty support
    - Estimated Recovery Time – 2+ days, depending on warranty response time and severity of failure. May require reinstall from level 1B.
    - Cost – None.

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.

Data Archival/Removal to Manage Costs

For the above protection levels 3 and 4, the cost and complexity will depend on the volume of the online data to be backed up, restored, replicated, etc. As the size of the online data becomes large, customers may decide to archive off older data to reduce the size of the data that must be protected.

ORACLE DATABASE

Reducing the size of the Oracle database will reduce the associated costs of data storage as well as the complexity of running nightly backups and recovering the event of a failure.

Options to consider:

a. Move the LOB data out to a separate NFS share
   - This feature can reduce total Oracle DB size by 70+% for most customers.

b. Mark old partitions as read only
   - This allows these older partitions to be skipped during backup.

c. Archive and remove older partitions
   - Recovery usually involves using transportable tablespaces and there may be complications if the schema has changed since the archival was done.

d. Delete old partitions
   - Simplest option.

e. FIT Fusion (Future option)
   - Future ability to dump the collected data out to a common file format to allow it to be merged from multiple source systems to a common destination system. If these transfer data files are preserved and archived, they could be used later to recreate the data. More details to come.

NFS SHARE FOR LOBS

Large Object Binary (LOB) is the mechanism used to store the collected binaries such as Word docs, Email bodies, Video capture, Images, etc. Moving the LOBs outside of the Oracle database can reduce the total Oracle DB size by 70+% for most customers. The LOBs are more easily managed on a separate NFS share. The LOBs are organized into a simple YYYY/MM/DD directory structure, making it easy to find older data and delete it, archive it, etc.

If files are removed from the NFS share, the only noticeable degradation will be that when analysts try to download a binary or play video for that time period, the system will give an error saying it cannot find the data. Putting the data back it the original location on the NFS share will allow the system to find it and allow the binary download or video replay again.

The data is organized by file type, so selective pruning/archiving is also possible if customers desired to hold on to one type of data longer than others, for example video replay vs print binaries.

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.

Options to consider:

a. Move older data folders to cheaper, slower storage
    - Move older data folders to cheaper, slower storage on premise or in the cloud and then use symbolic links on the primary NFS host to link those folders back into the structure. The system will be able to access that data as though it were still on the primary system. Access times will be slower, but that is okay since it is infrequently accessed data.

b. Archive and remove older data folders
    - Zip up whole root folders at the YYYY or YYYY/MM level and send them to cloud or other cheap storage. In the event the data is needed again, restore the files back to where they were located previously.

c. Delete older data folders
    - This is the simplest option if you no longer need the data.

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.

PROPRIETARY

Appendices

Appendix A – Using ESXi Virtualization and Snapshots to Revert to Known Good State

In order to use this option, the database server must be running in a virtual machine on top of VMWare ESXi and a previous snapshot of the system virtual disks must have been taken while the system was in a known good state. This process restores the system disks with the OS, Oracle software, and configuration. It does not protect from loss of data on the SAN.

In the event of a software failure:

1. The database server local system disks will be reverted to a prior snapshot.
2. The database will be started up.

Important

Oracle requires licensing of all servers and clusters where the DB server could potentially move automatically, for example due to vMotion. Therefore it is important to restrict the VM from vMotion or other automatic balancing so that it is pinned to only one server/cluster. Request the *Forcepoint FIT Oracle Licensing* document from Forcepoint Support for more details on the optimal way to license the Oracle Database for use with the FIT product.

Contact Forcepoint Professional Services to discuss recommended options for reverting a snapshot.

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.

Appendix B – Cold Standby DB Server

This option requires a separate standby database server with the same hardware specs as the primary, including fiber-channel connections to the SAN. This standby server will assume control of the SAN and take the place of the primary server.

In the event of a primary server failure:

1. The standby server will be connected to the SAN if not already connected.
2. The standby server will take ownership of the SAN data LUNs.
3. The database will be started up on the standby server.
4. The master and collector nodes will be configured to point at the standby server IP.
5. The standby server has now become the primary.
    a. Verify archivelog and nightly backup jobs settings.
6. The primary server can now be repaired, reinstalled, and configured as standby.

To ensure that the standby server is ready and the failover will be successful:

1. Ensure the standby server can be connected to the SAN.
    a. Make sure there are adequate ports and cables and that they are long enough.
    b. Configure the SAN to allow access from the secondary host.
2. Install the G2CP and Oracle DB software on the standby server and keep them patched and synchronized with the production server.
3. Think through network connectivity.
    a. If you use a separate IP address on the secondary server, then you will need to be prepared to switch master and collector nodes to use the new IP address at the time of failover.
    b. If you use the same IP address on the secondary server, be careful to only connect one at a time to the main switch or you will have IP conflicts. In this case, keep the primary interface disconnected and use a secondary network to access both servers, apply patches, etc.
4. Make sure you have good backups of the primary server.
5. Make sure you have captured the configuration of the primary server – IPs, disks, LUNs, groups, Keystore Wallet, etc.
6. Verify the Oracle configuration – disk groups, cron jobs, sqlnet.ora files, etc.

Contact Forcepoint Professional Services for more details and recommended recovery options.

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.