

Blackboard Managed HostingSM
Disaster Recovery Planning Document



Blackboard

- 1. OBJECTIVES..... 3**
- 2. SCOPE 3**
- 3. ASSUMPTIONS..... 3**
- 4. DATACENTER AND COMPONENT FAULT TOLERANCE 4**
- 5. DISASTER RECOVERY STRATEGY 4**
 - 5.1. Backup Architecture.....5
 - 5.2. File Level Recovery.....5
 - 5.3. Database Recovery.....5
 - 5.4. Application Server Recovery.....6
- 6. DR PLAN ADMINISTRATION..... 6**
 - 6.1. Business Continuity Coordinator (BCC)6
 - 6.2. Updating the Plan.....6
- APPENDIX A..... 7**
- 7. HIGH AVAILABILITY OFFERINGS..... 8**
 - 7.1. Business Continuity Service.....8
 - 7.2. RAC.....8
 - 7.3. Load Balanced Environments8
- APPENDIX B..... 9**
 - 7.4. Blackboard’s Automated and Managed Monitoring System.....10
 - 7.5. Redundant ISP Provider Configurations.....11

1.Objectives

This document outlines the Blackboard Managed HostingSM Disaster Recovery (DR) plan for clients with the standard Managed Hosting offering. It defines the measures the Managed Hosting group has taken to ensure that client data is recoverable in the event of a disaster. In the context of this document, a disaster encompasses both failures at the hardware and software levels as well as site failures that are unplanned and cause data damage or loss. Also covered in the scope of this document are a review of individual course or content restorations, and a definition of escalation procedures and recovery strategies.

2.Scope

This plan will cover all Managed Hosting clients, both in and outside of the US. Datacenters in question reside in Virginia, Amsterdam, and Sydney. Due to the scale difference of the Amsterdam and Sydney datacenters, recovery practices are different than those at the Virginia facilities. The following serve as criteria for a disaster:

- Fire
- Natural disasters (Mother Nature)
- Sabotage
- Accidental human error
- Flooding
- Equipment failure
- Application / database failure
- Other unlikely events that impact service

3.Assumptions

This plan was developed using leading industry best practices for Disaster Recovery process and takes into account the following assumptions:

- This DR strategy assumes key BbMH personnel in the datacenter locations (Amsterdam, Australia or Metropolitan-DC) are not incapacitated due to a catastrophic attack, a nuclear incident, or a natural doomsday event. It is important to note that while the BbMH DR Team is spread out throughout the world, certain apocalyptic circumstances would impair the MH Team's ability to restore a client system.
- Backups of content and database occur at least one time during a 24-hour period, and as a result, BbMH aims to have less than 24 hours worth of data loss in the event of a disaster. In other words, if a catastrophic failure occurs

- at the end of a business day before a backup is taken; ALL changes made to the system that day will be lost.
- Most database backups occur via backup scripts executed on Oracle over NFS (ONFS). Oracle Dumps are used for clients who are not utilizing ONFS technology.
 - Content Snapshots are taken at least once a day and retained for 30 total days.
 - Content Snapshots and Database backups are replicated nightly to an opposing datacenter.
 - BbMH standard offering issues clients a 24x7 Support Manager or escalation option via phone, web, and email based ticketing.
 - Potential outages are proactively caught via a fully managed monitoring system which polls each system every 5 minutes (*see appendix B, diagram 1*).

4.Datacenter and Component Fault Tolerance

The Managed Hosting datacenters and devices are equipped with many levels of fault tolerance and redundancies at a global level. These include:

- RAID and mirror protection at the Server and Filer level
- Two separate paths for communication lines ensuring a remote hot manual failover
- Multiple ISP connections to different Tier-1 ISP's results in aggregate bandwidth greater than 4.5 Gbps
- All production Filers are clustered to ensure quick failover
- Highly available network design with multiple Load Balancers, Firewalls and Intrusion Detection Systems at each datacenter, ensures a Hot "B side failover" path
- Enterprise-class Network and Security devices attach to a configuration with no single point of failure
- Multiple PDU power supplies resulting in 4 levels of power protection

5.Disaster Recovery Strategy

If an outage occurs on an individual client system at a particular datacenter, BbMH monitoring will display the disruption and appropriate engineers will own the issue **until resolution**. Monitoring of this nature occurs 24x7x365 so that there is always a set of eyes monitoring alerts for all clients. Upon assignment of the outage, engineers will assess the situation and determine the resolution path needed, which will include one of the following:

1. Server failover
2. Application or Database restore
3. Operating System reload or clone
4. Site failover (if applicable)

In the unlikely event our redundancy fails in a manner that affects multiple clients, BbMH will utilize all spare equipment on site to restore those clients to a working configuration. The immediate priority is to get the affected clients up and running as soon as possible. However, the condition of the environment may not be in an optimal state in which case downtime will be scheduled with the clients to resume optimal configuration.

If a disaster is declared which affects the entire datacenter, an immediate assessment by the DR Team will take place to determine the scope of damage. If the datacenter is completely incapacitated, BbMH will make every attempt to restore their configuration on spare hardware or emergency-ordered hardware. There are no SLA guarantees in this case. The decision to failover or declare a disaster is determined by the Crisis Management Team. (*Appendix B*)

This situation assumes that a catastrophic natural or man-made incident where key employees are incapacitated or both datacenters are eliminated has not occurred.

5.1. Backup Architecture

BbMH offers snapshots and snapmirroring as a standard offering for data protection.

A Snapshot is a highly reliable Point-in-Time picture of the File System. It allows for near instantaneous backup, quick recovery, and ease of management.

A Snapmirror, which is based off the same technology as a Snapshot, takes backups to the next level. It replicates a consistent Snapshot image of the Filer volume to a designated target at an opposing datacenter.

There are multiple levels of backups which occur on a client system:

- **Level 1:** Utilizes Snapshot technology to backup the File System and Database to Network Attached Storage (NAS) where they are stored on-line, on disk media, for 30 days
- **Level 2:** Secondary facilities replicate (snapmirror) offsite nightly to disk

5.2. File Level Recovery

When the BbMH team receives a request to restore a deleted file, the engineering specialists attempt to locate the missing data from recent snapshots. Once the file is found, it is restored to its original location. Maintaining one month of all client data in local snapshots allows the BbMH team to satisfy most restore requests within a short time period.

5.3. Database Recovery

Backup scripts run daily for ONFS clients. If clients are installed on local disk, database dumps are taken once nightly and stored on a Filer for a period of 30 days. Oracle snapshots and dumps are replicated to an offsite datacenter daily.

In the event of an Oracle database failure, Blackboard Managed Hosting engineers will immediately begin the process of restoring the complete database from a local snapshot or off-site backup. Snapshot recovery will be used if a snapshot from a suitable timeframe is available on the local file system. The time it takes to recover from a total database failure largely depends on the size of the database.

Spare Database servers will be kept at the primary datacenter if the physical server needs to be replaced. In this case, the cold spare server will be configured with the client's Database configuration. If a client encounters a Database failure due to an entire site failure, every attempt will be made to restore the system on spare hardware. In this instance, there are no SLA guarantees.

5.4. Application Server Recovery

Upon notification of the application server failure, BbMH engineers will diagnose whether it is a hard-failure (i.e. irrecoverable failure on the server) or a soft-failure (i.e. reboot will restore server back into service). If the diagnosis is a hard-failure, BbMH engineers will immediately move the application persona to a healthy server waiting in the available pool.

6. DR Plan Administration

Due to ever changing technologies and environment scaling, this is a considered a dynamic plan which may change frequently. This is one reason why a single point of contact needs to be identified to own the DR process.

6.1. Business Continuity Coordinator (BCC)

The BCC is responsible for the overall creation, maintenance, training, administration and awareness of the DR plan. The BCC is a member of the MH Management Team and can approve changes to the plan and has immediate access to senior Blackboard management. The BCC also leads the team in the event of a disaster.

6.2. Updating the Plan

The BCC is the only person that can update this plan. This is not only because they are intimately familiar with the environment, but as members of the MH Change Review Board, they are aware of any changes that could affect DR. Any global change to the environment affecting this plan is reflected in an immediate revision. The revision is then communicated to the rest of the Crisis Management Team.

APPENDIX A

7. High Availability Offerings

In addition to Blackboard's standard offering, we offer clients several additional options to raise the bar for high availability and security. For specific questions and pricing regarding these services, please contact your Client Manager.

7.1. Business Continuity Service

Business Continuity service is a proactive risk management service offered by Blackboard Managed Hosting to minimize the application downtime in the event of a catastrophic failure. This allows clients to quickly resume mission critical functions with minimal data loss. For existing BbMH clients with the Business Continuity service, a total site failure will result in their environment being brought up to their hot standby environment at an opposing datacenter. The environment is considered "Warm" because there is constant replication of the content via Snapmirrors and database replication using Oracle Dataguard and the services will be restored within a guaranteed timeframe and a point of data backup.

7.2. RAC

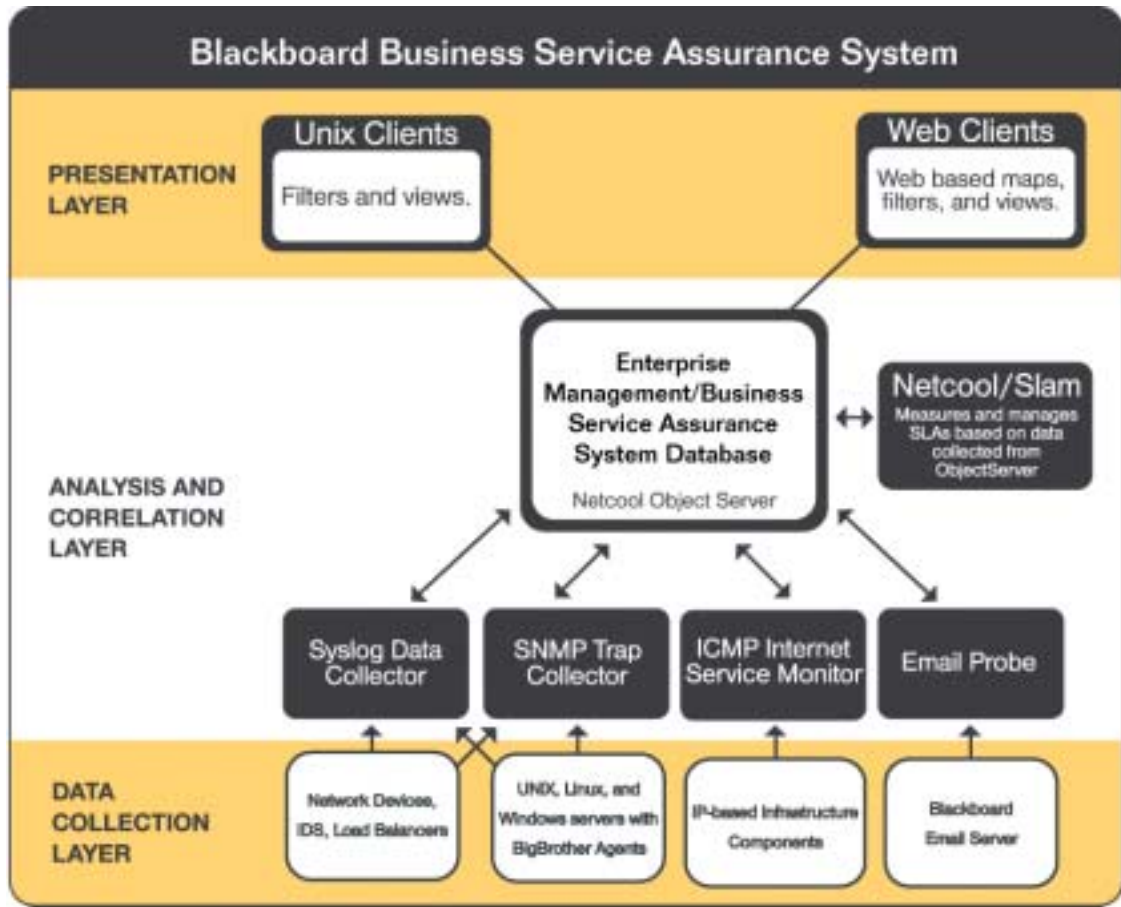
To reduce unplanned outages caused by single points of failure on the Database, BbMH offers an enhanced Oracle configuration called Oracle RAC (Real Application Clusters). Real Application Clusters is a component of Oracle that allows a database to be installed across multiple servers. Each server has its own memory and processors but shares a virtual directory on a shared storage array. The end result is a single database that has a separate instance on each node. Clustering a database offers many advantages including: scalability, lower TCO (Total Cost of Ownership) and availability. It is easier to add a server, distribute the load across lower end servers, and increase uptime by eliminating single points of failure.

7.3. Load Balanced Environments

Blackboard offers the option to load balance more than one application server. A Load Balancer divides the amount of work over multiple devices for the purpose of redundancy and faster service. If one server in the LB is incapacitated, the other(s) will pick up the processes. The advantage of a pool of load-balanced application/web servers is that it provides for a high-availability, fault-tolerant application environment. BbMH engineers will be notified of a failure of a single application server through the monitoring system. Upon confirmation of the problem, if necessary, BbMH engineers can safely and quickly remove the errant server from the pool to troubleshoot and diagnose the issue. The overall environment may experience slight performance degradation while a single server is being serviced. Upon repair of an application server, BbMH engineers will seamlessly return it to the application load-balanced pool without any downtime to the client.

APPENDIX B

7.4. Blackboard's Automated and Managed Monitoring System



7.5. Redundant ISP Provider Configurations

