



UNIT / CENTER XXX

Disaster Recovery Plan

Last Revision: **Date**

Version: **x.xx**

Prepared, Reviewed and Approved by:

Unit IT Manager Name

Unit IT Manager Title

Reviewed and Approved by:

Name of Unit Head

Unit Head Title

Executive Summary

This document provides a comprehensive disaster recovery plan for resources within the [FILL IN YOUR DEPARTMENT OR CENTER NAME HERE] as required by Texas Administrative Code 202.74 Section 4 for Institutions of Higher Education.

Scope

The scope of this disaster recovery plan covers only IT services managed by resources within the [FILL IN YOUR DEPARTMENT OR CENTER NAME HERE].

Table of Contents

Executive Summary	2
Emergency Telephone Numbers.....	4
Objectives of Texas A&M AgriLife Disaster Recovery Plan	5
Assumptions of Disaster Recovery Plan	5
Disaster Recovery Team	6
Testing Procedure	6
Impact Analysis	6
Risk Analysis	7
Water	8
Fire	9
Electrical	9
Theft	10
Malicious Viral Attack	11
Criteria for Invoking Disaster Recovery Plan	11
Damage Assessment Process	11
Operation Backup Site Matrix.....	12
Emergency Shutdown Procedures	13
Operations of Recovery Site	14
Procedures for Return to Normal Operations	14
Appendices	16
Appendix A: Password Escrow	17
Appendix B: Business Impact Analysis	18
Appendix C: Vendor Contact List	19
Appendix D: Disaster Recovery Plan Distribution List	20
Appendix E: Restoration, Backup and Test Procedures	21

Emergency Telephone Numbers

Contact	Contact Name	Phone Number
Campus Police		979-845-2345 or 9-911
Fire/Ambulance		9-911
Physical Plant		979-845-4311
Vice Chancellor		
Unit IT Lead		
Dept Head		
Assoc Dept Head		
Key Researchers etc.		

Objectives of Disaster Recovery Plan

The overall objectives of the Disaster Recovery Plan (DRP) are to protect unit resources and employees, to safeguard the unit's vital records, and to ensure the ability of unit to function effectively in the event of a severe disruption to normal operating procedures. The primary purpose of the DRP is to document the plan for response, recovery, restoration, and return to normal server after severe disruption.

A disaster is defined as the occurrence of any event that causes a significant disruption in unit capabilities. The central theme of the plan is to minimize the effect a disaster will have upon on-going operations.

The plan is a systematic guide from disaster to recovery. The basic approach, general assumptions, and sequence of events that need to be followed are included below. While using the plan during a severe disruption, it may be in the best interest of AgriLife to modify directions for many reasons. All alternative actions should be documented, and as soon as appropriate the plan should be resumed and revisions made as appropriate. The plan will be distributed to all key personnel, and they will receive periodic updates. The approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs.

Assumptions of Disaster Recovery Plan

1. Recovery will be achievable for anything that is less than complete destruction (e.g. nuclear holocaust, global electromagnetic pulse (EMP) event).
2. Some staff members may be rendered unavailable by a disaster or its results.
3. Procedures are detailed to a level that can be performed by someone other than the primary responsible person.
4. Recovery of critical subset functions of unit will allow for continuance of critical operations adequately.
5. A disaster may require employees to function with limited service capacity, until a full recovery is able to be performed.
6. This plan does not detail LAN/WAN networking issues maintained by Texas A&M University or the Trans-Texas Videoconference network (TTVN), as these are maintained by TAMU Computing and Information services and the TTVN wide area network management teams.
7. This plan does not detail any applications maintained and operated by Texas A&M System utilized by unit. It is understood that TAMUS provides for these services and all disaster recovery availability.
8. This plan does not detail any Enterprise services provided by Texas A&M AgriLife IT as understood those plans are outlined in AIT's disaster recovery plan.

Disaster Recovery Team

Name	Office Phone number	Alternate Phone Numbers(home/mobile)	Position/Title
Team Member 1	xxx-xxx-xxxx	xxx-xxx-xxxx	Title

Members of this team will be involved in the initial damage assessment and review as well as any relocation or service remediation efforts. The [redacted] and [redacted] positions will be in charge of handling communications to unit leadership as well as any related media relation coordination efforts.

Testing Procedure

The disaster recovery plan is to be tested on an annual basis. A test simulation will be performed where the disaster recovery team will verify documented procedures are functioning as defined. The test will primarily include activating various backup systems that are deemed critical for unit operations (in the context of a disaster).

Annual testing is scheduled via the unit operations calendar. This calendar contains all required annual reviews (documentation and TAC required tasks) in addition to tactical IT operation management tasks.

Impact Analysis

The impact of loss of each service platform is outlined below in the Business Impact Analysis section found in Appendix B of this document.

ADJUST AS NEED BE FOR YOUR UNIT: If employee computer workstations or network connections are damaged or lost during the disaster, certain functions for these employees impacted would not be able to be performed temporarily. PC's would be replaced through either available on-site inventory or through any state approved vendor provider. Network connectivity could be re-established through relocation of critical employees to sites where network connectivity was not impacted or through other providers (i.e. 3G/4G Carrier networks).

Risk Analysis

An effective and efficient risk assessment and mitigation effort requires active support and ongoing participation from multiple disciplines and all levels of management within the unit. Responsibilities include identifying the vulnerabilities that may affect information assets and implementing the cost effective security and risk management practices that function to minimize or eliminate their effects:

The term "vulnerability" refers to threats to information assets such as:

- Water damage (local flooding or building roof fault)
- Fire
- Electrical Failure
- Theft
- Malicious Viral Attack

Risk refers to effects or consequences associated with the vulnerabilities, such as the:

- Inability to maintain or assure data or application systems integrity;
- Loss of confidential information (data leakage);
- Unavailability of technical support services or information; or,
- Financial loss.

The focus of information security is ensuring the protection and the continuation of the unit's business. Providing efficient accessibility to necessary information is a requirement for

establishing and maintaining automated information systems. Protecting that information and the assets that surrounds it is the impetus for establishing an information security and risk management program. Protecting information assets include the:

- Physical protection of information processing facilities and equipment;
- Maintenance of applications and data integrity;
- Assurance that automated information systems perform their critical functions correctly, in a timely manner and operate under adequate controls;
- Protection against unauthorized disclosure of information;
- Assurance of the continued availability of reliable and critical information.

The following describes how this risk analysis was conducted:

- Conduct Individual Risk Assessments for each unit, center and institute within the organization utilizing the ISSAC and ISSAC-S tools provided by Texas A&M University.
- Conduct Annual Information Security Management Program activities and reviews (described within).
- Review of annual operations management and IT metric reports.
- Results of the above are reviewed and synthesized in this report by the Director of Texas A&M AgriLife Information Technology for executive management review and discussion.

1. Water damage (local flooding or building roof fault)

Describe how the unit would deal with a water flooding event .

2. Fire

Describe how the unit would deal with a fire based event.

3. Electrical Failure

Describe how the unit would deal with any electrical failures (short and long term)

4. Theft

Describe how the unit would deal with any theft event.

5. Malicious Viral Attack

Damage or destruction resulting from malicious viral attacks could result in the loss of critical computing operations. To guard against this happening, enterprise servers and desktops are protected by Sophos anti-virus software.

Add any additional or different info here relative to your unit operations.

Criteria for Invoking Disaster Recovery Plan

The detection of an event which could result in an impact to information technology services is the responsibility of ____{ENTER NAME or POSTION of Person Responsible within UNIT}____.

Upon recognition of a sever service disruption, the emergency response team personnel should take steps to immediately minimize property damage and/or injury to people in the area.

The following people would then be notified of the event:

- Contact #1
- Contact #2
- Etc.

Damage Assessment Process

An immediate function in any disaster is an initial and expedited assessment of the scope of damages incurred. The coordinator of the Disaster Recovery Team is the ____NAME____. If he is unavailable for any reason, the ____NAME____ becomes the acting coordinator for damage assessment and recovery.

Upon notification of a disaster, the coordinator will perform the following:

- Notify members of the disaster recovery team of the situation and proceed to the damaged site.
- Upon arrival at the site take any temporary actions to safeguard equipment and personnel. Request assistance from facility providers as required.
- Assemble the disaster recovery team in order to begin assessing the extent of damage, scope the situation, and determine what physical equipment or services are available for stable use.

- If any damage was incurred to the physical building, work with the building manager/provider to assess the short and long term viability of the building.
- Conduct a meeting after the initial assessment to discuss the following:
- Determine and define a plan of action based upon the following:
 - If normal operations can be continued at the site
 - If limited operations can be continued at the site
 - If the operation must be relocated to a secondary site.
- Define goals and responsibilities of each team member
- Designate tasks as needed
- Notify equipment vendor of any hardware replacements that are needed per 24/7 maintenance plan agreements.
- Brief unit administration of the situation and the defined action plan.
- Advise AgriLife IT of the event and how it may be of impact of relevance to Enterprise IT operations or end user access needs relative to Enterprise IT services.
- Document tasks and assignments noting area of operation, owner and contact information.

Operations Backup Site Matrix

If it is determined by the disaster recovery team that some or all of the operations will need to be relocated to an alternate site the following site matrix has been compiled

Location	Alternate Site
Primary Location (Existing)	Alternate Location Site #1
etc	Alternate Location Site #2
	Etc.

Procedures for Relocation

1. Organize disaster recovery team.
2. Obtain all backup media and equipment needed for remote site operation
3. Initiate network and DNS planning needs with network service providers.
4. Place any required emergency orders for any equipment or software
5. Arrange for transportation.
6. Relocate to secondary backup site.

Emergency Shutdown Procedures

In some cases there may be enough forewarning of an event to allow for emergency shutdown of computing platforms. This is recommended as to avoid abrupt halts to systems which could result in data or configuration loss.

The following procedures outline the methods used to perform emergency shutdowns when there is ample warning provided to provide sufficient time to assess and implement.

These procedures are also used regularly throughout the state on an active basis to provide for preventive maintenance operations and protect systems from electrical storms in regional centers.

Shutdown Process

1. Assess the situation based upon available information.
2. If an emergency shutdown of a system is warranted then proceed with the following steps based upon the system type:

Windows Servers

1. Describe your step by step windows shutdown process.
2. Step 2, etc.

Linux Servers

1. Describe your step by step linux shutdown process.
2. Step 2, etc.

Operations of Recovery Site

When an alternate site is required to conduct recovery the following process will be applied to efficiently restore operations.

1. Assemble the disaster recovery team
2. Assess to make sure all required equipment is present and available.
3. Assess any needed additional supplies (power cables, network cables etc.)
4. Prioritize recovery of services as indicated in Business Impact Analysis (Appendix B)
5. Initiate individual service recovery procedures.
6. Initiate DNS and networking arrangements as required.
7. Perform service testing procedures for each service as it is brought online.

8. Arrange with vendors to ship replacement hardware to original site in preparation of rebuilding at primary location.
9. Begin coordination efforts for facility services recovery at primary site.
10. Continuously communicate and unit leadership to status of recovery efforts.
11. Continuously update end users on status of recovery.

Procedures for Return to Normal Operations

Once access has been regained/permited to the original operation site the following basic procedures would be followed:

1. Begin any salvage operations to clean up original operations site.
2. Coordinate with facility providers on any service remediation efforts
3. Coordinate with computing system platform provider to arrange for shipment and receipt of replacement hardware.
4. Coordinate disaster recovery team member tasks for rebuilding core platforms.
5. Configure all firewall, DNS and other network routing needs as required.
6. Insure that all documentation and testing procedures are applied.
7. Verify repairs and/or replacements of system platforms and facility have been made.
8. Initiate burn in and power tests for new platforms and facility services for minimum of 2 days to assure stability.
9. Verify that an up to date backup of data at recovery site is made.
10. Communicate status and transition planning with unit leadership and AgriLife IT.
11. Establish cut over date and time.
12. Initiate cut over and continue to perform service testing and backups on a daily basis until stability of operations has obtained original status prior to disaster

Appendices

Appendix A: Password Escrow

Copies of all system administration passwords are stored in the following locations:

1. **Location 1: Details on where escrowed password file is stored and how has access to it. Be detailed and specific (i.e. room numbers, directory locations, etc.)**
2. **Redundant Location 2: Details on where escrowed password file is stored and how has access to it. Be detailed and specific (i.e. room numbers, directory locations, etc.)**

Appendix B: Business Impact Analysis

Instructions: List all unit based IT services or applications and associated servers (by name). Describe impact and agreed upon maximum downtime for each. This list should be sorted from small to largest maximum downtime days for prioritization purposes.

Service	Server	Impact	Max Downtime(Days)
Example Application "A"	Xyz.tamu.edu	Would result in diminished ability to XYZ	1

Appendix C: Vendor List

Vendor Name	Supplier of/Contact if Any
Microsoft Corporation Stonebridge Plaza, 9606 N. Mopac, St. 200, Austin, TX 78759 (512) 795-5300 (512) 343-8498 (fax) Technical support phone numbers can also be found at: http://support.microsoft.com/directory/directory/phonepro.asp	OS, Application software
Sophos Inc. 3 Van de Graaff Drive 2 nd Floor Burlington, MA 01803 Tech Support: 1-866-510-2913 Technical support can be found at: http://www.sophos.com/support	Anti-Virus / Data Leakage Vendor Premium License Number:
Add additional vendor Contact Information	

Appendix D: Disaster Recovery Plan Distribution List

Contact	Contact Name	Phone Number
Unit Head	Name	Home: 111-111-111 Cell: 222-222-2222
Contact #2		
Contact #3		

Appendix E: Restoration, Backup and Test Procedures

Overview

The following information describes the IT backup, recovery, and testing procedures for operational areas under the direct control and management of the [FILL IN YOUR DEPARTMENT OR CENTER NAME HERE]. These procedures are intended to meet requirements established by Texas Administrative Code and Agency procedures.

Backup/Recovery/Testing is performed in the following operational groups:

Instructions: The majority of units manage backup and recovery operations of servers in groups. Backup, Recovery and Testing can therefore be “grouped” in the documentation for these systems. Define below the distinct groups of systems that are managed. You may only have one “group” as you unit may have only one procedure for backup and recovery using the same tools.

- **Group 1 NAME:** Describe first group of servers (or systems) you may backup, restore and test using the same process and tools. Description should include what functions and general services these systems supply to the unit. LIST THE SERVERS BY NAME THAT FIT INTO THIS GROUP
- **Group 2 NAME :** If you have a second group of servers (or systems) you backup , restore and test with a different process describe those systems. LIST THE SERVERS BY NAME THAT FIT INTO THIS GROUP.
- List any systems that are uniquely managed in addition to any groups of systems.

NOTICE:

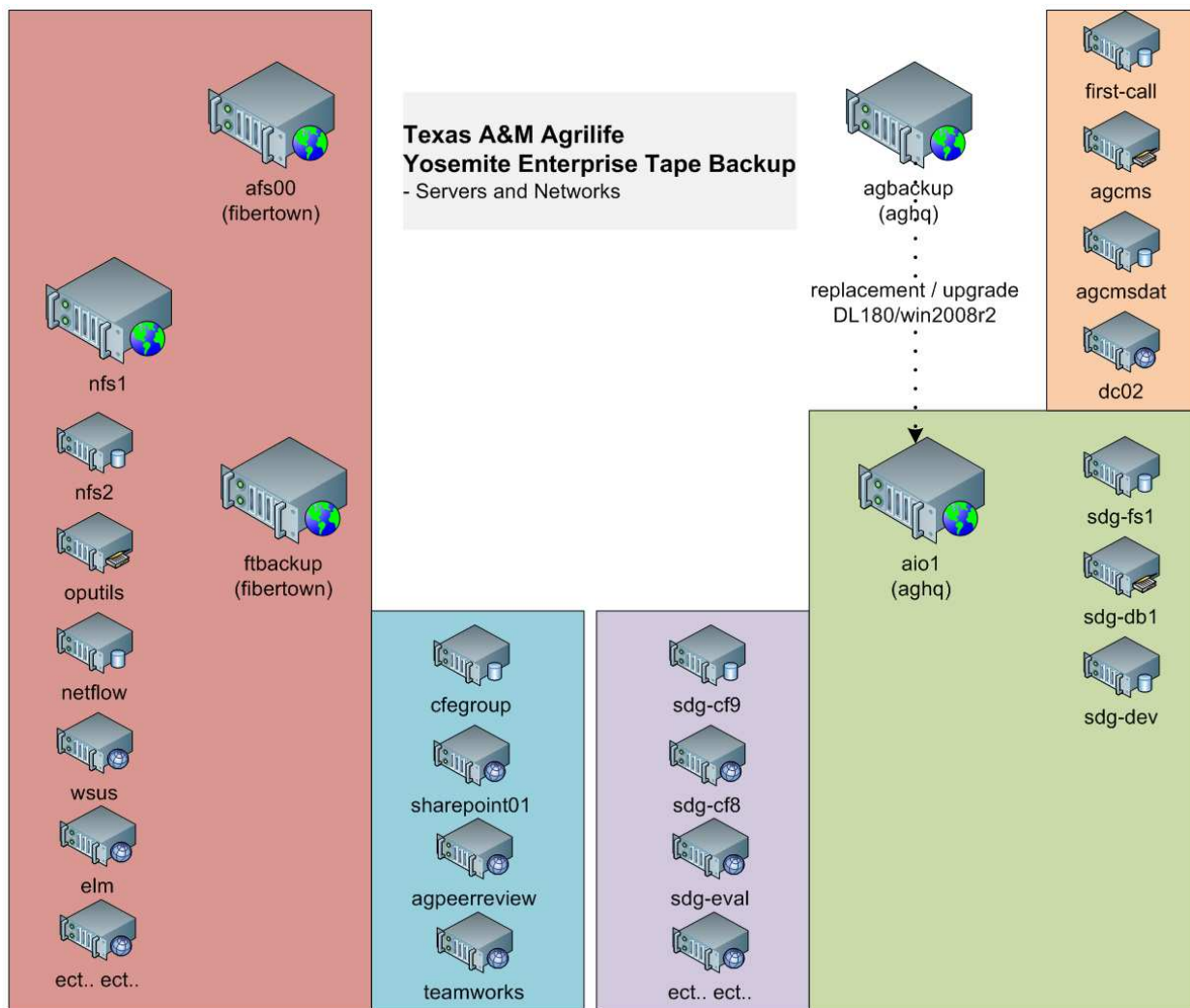
The Following Pages represent EXAMPLE Backup and Restoration Procedure Documentation. Please Remove these pages and replace with your own detailed backup and restoration procedure documentation.

You should have a separate backup and restoration process documented for each GROUP you described above.

GROUP 1: SDG Operations Services

Backup, Recovery, Testing Procedures

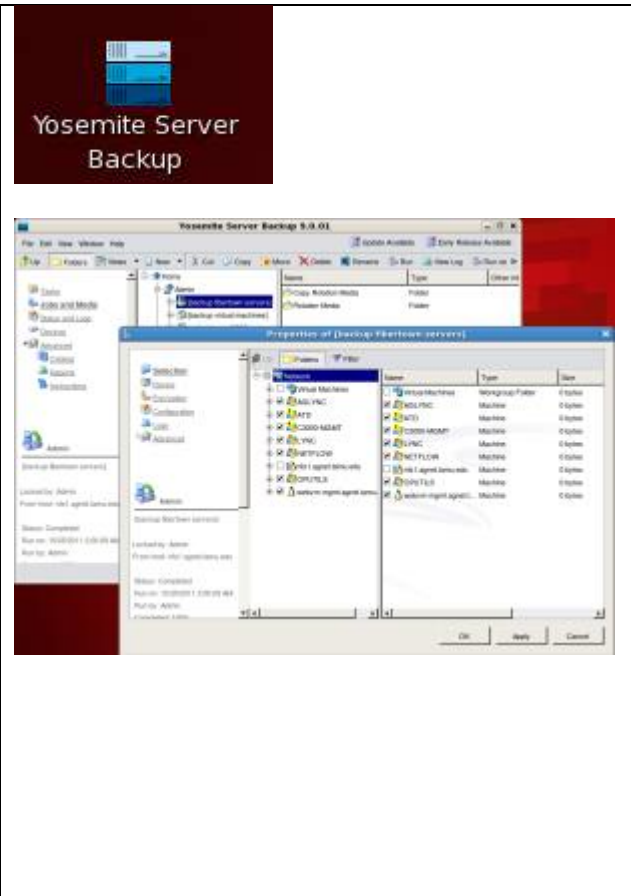
The following diagram shows systems backed up at the AGLS Headquarters and Fiber Town Locations utilizing the Yosemite Backup Cores. This is meant for overview/reference only.



Backup Procedures

All SDG servers are backed up to the Yosemite Server Backup (YSB) installation in AGLS server room, utilizing a 48-tape LTO-4 library. Within the servers MySQL-ZRM is used to backup any MySQL databases to the file system, which is then backed up using YSB.

1. Install "Yosemite Server Backup" client. Stored in Software repository location as defined in password escrow file.
2. Configure client to point to AGLS-Backup (172.24.1.xxx)
3. Login to AGLS-Backup via RDP
4. Use the Yosemite Management Console to add server to the **[backup ait servers]** backup job. Right click **[backup ait servers]** select properties.
5. Minimally backup /var/log, /etc, /opt/coldfusionX, etc plus any application specific directories and application data directories. If a database should be dumped to the file system first, create and schedule a separate pre-, post- script backup job which executes a script to perform the task before the ait servers backup job. Alternately, use cron to trigger the database backup job to complete the task.
6. The backup target device, encryption, and schedule are preconfigured for the site backup job. Tapes are automatically labeled and assigned to a media set as needed.

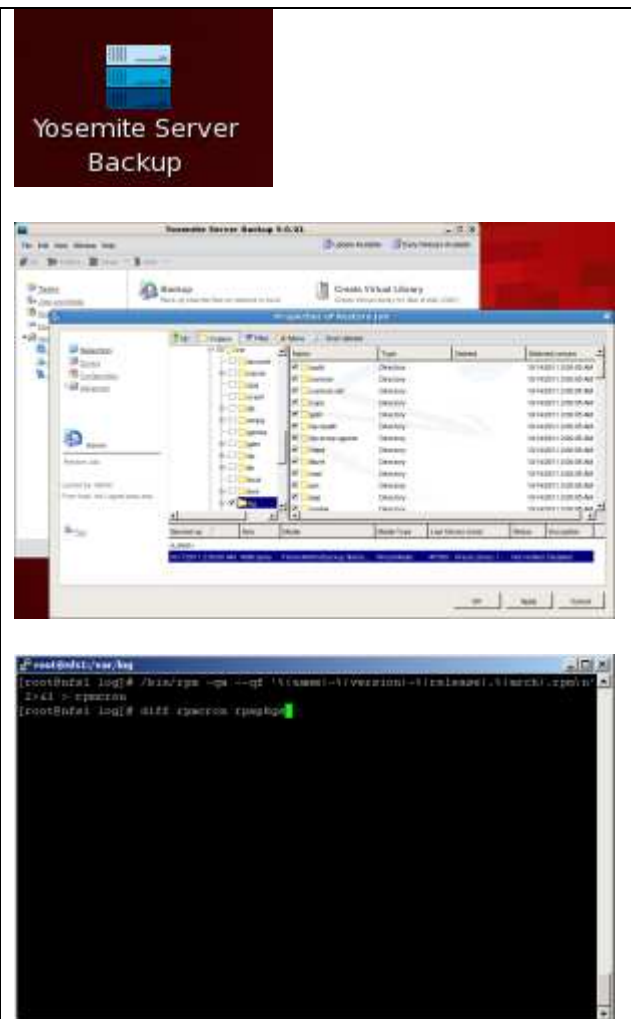


Furthermore, virtual machine servers have their full disk images backed up (copied) to disk on a periodic basis.

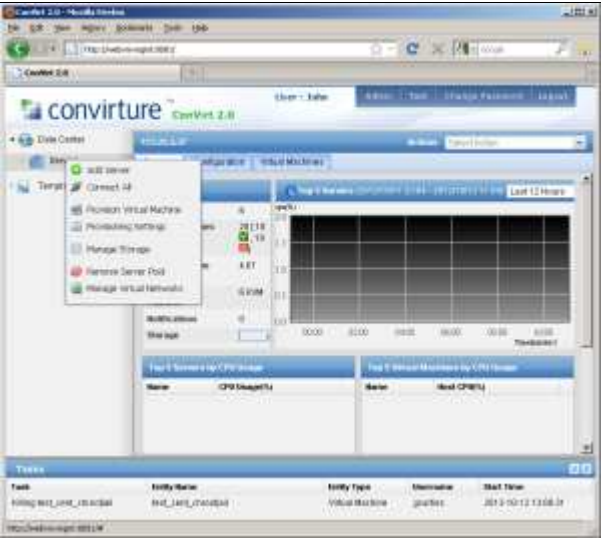
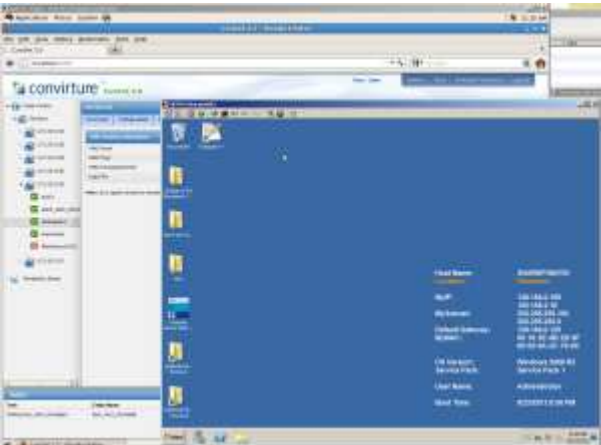
Recovery Procedures

- A. Recovery of MySQL databases is accomplished by running a restore job in YSB and selecting the appropriate MySQL-ZRM backup set, writing it back to the file system. Then using MySQL-ZRM command line tool [restore] option, recover the database.
- B. Recovery of SDG servers:

1. Install RHEL5 – x86_64, register with Red Hat, install current patches from Red Hat Network
2. Install Fedora Project EPEL5 repository rpm
3. Install “Yosemite Server Backup” client
4. Login to AGLS-Backup via RDP
5. Use the Yosemite Management Console to confirm client registration and create a restore job, being sure to redirect folders to the new client.
6. Restore /var/log
7. Login to the new server.
8. Change to /var/log
9. Compare the installed system packages to the restored last daily rpm packages file.
10. # /bin/rpm -qa --qf '%{name}-%{version}-%{release}-%{arch}.rpm\n' 2>&1 > rpmcron
11. # diff rpmcron rpmpkgs
12. Use # yum to resolve any differences
13. Use the Yosemite Management Console to create a restore job
14. Restore /etc, and any other backed up directories.
15. Verify – Centrify authentication, ELM remote logging, Sophos antivirus, Yosemite backup job, applications and services



Testing Procedures

<ol style="list-style-type: none"> 1. Login to http://XXXXXXXXXX 2. Add a new kernel virtual machine server (see VM creation documentation for details) 3. Disable the YSB agent on the production server 4. Enable the YSB agent on the virtual machine personified as the production server 5. Perform the recovery procedure for that server 6. Shutdown the kernel virtual machine 7. Reconfigure the networking of the kernel virtual server such that it is isolated from the production network 8. Re-enable the YSB agent on the production server 9. Conduct testing on the kernel virtual server appropriate to the production data or services for that server. <ol style="list-style-type: none"> a. Provide Access to end user for validation testing. b. Document end user validation testing. 	 
--	--

Testing SUMMARY Log for SDG Operations

(See Detailed Testing Log Report Documentation for Details)

Date	Tested By	Result
2012.10.12	Gene Tierney	Success

Hardware Specifications

The following information describes current hardware platform specifications relative to this area of operations within the unit. This information can be utilized to determine appropriate replacement hardware needs if required for recovery efforts.

Instructions: List all information for hardware platforms within this group that would be critical/required for the recovery process.

Hardware Vendor	HP
Original Vendor Contact Info	Microage Phone: xxx-xxx-xxx Email: Info@there.com
Original Purchase Date	4/12/12
Equipment Model	DL 180
# of Processors and Type	(8) 3.2GHZ Intel
Storage Configuration and Size	(12 Disk) 3 TB Raid 5 Array
Internal Operating Memory Size	48 GB
Tape Sub System Information	HP LTO-4 Model # XXXX/YYYY 4 Head SCSI Attached System
Warranty Contract Period and Status	DL-180 3 Year Hardware/Maintenance Expires: 12/12/15 HP LTO-4 Tape System: Maintenance Expires: 12/12/15

Software Specifications

The following lists any information related to software utilized within this group of systems that would assist in the disaster recovery process.

Instructions: List information such as Software license keys or vendor contact information that would be critical / required for the recovery process.

Software Name	License Information or Vendor Contact Info
Windows Server 2008 R2	xxxx-tttt-ssss-ffff-ffff-ssss