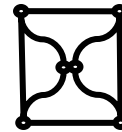


---

# NETWORK ASSESSMENT PLAN

## MetaArchive of Southern Digital Culture Project



2005-08-15

### Summary

This document describes the plan for assessing the Preservation Network of the MetaArchive of Southern Digital Culture Project. This deployment equates to Project Phase D3 in the project plan. Required steps and responsibilities are detailed for this phase, and notes concerning other project activities are summarized. This document makes reference to the project plan and other project documents which provide more details about other aspects of the project.

### Background from Proposal

Two sections from the original project proposal are relevant for context:

Network Synchronization. Once the preservation network is deployed and configured properly, the content harvest will be disseminated throughout the network nodes. This synchronization of archived content will hopefully occur relatively rapidly (we anticipate no more than ten days, based on preliminary estimates), especially if the Internet 2 linkages between the sites can be utilized (this would enormously speed up the data transfer rate). However, a full 13 weeks has been allocated in case this synchronization takes longer than expected. *(Note: This phase is scheduled to take place from Monday 8/29/05 to Friday 11/25/05. It is no longer strictly necessary, but we may wish to look at this as the period during which we finish remaining hardware deployment.)*

Network Testing. More than a year has been allocated for testing of the preservation network, guided by the preservation network assessment plan developed at the third all-project meeting. Various elements of reliability, security, fault tolerance and recovery processes will be tested. At least one simulated catastrophic data loss and recovery case study will be conducted. *(Note: This phase is scheduled to take place from Monday 11/28/05 to Friday 2/23/07.)*

### Remaining Hardware Deployment

At this point the essential vault servers required to constitute the preservation network appear to be on track to be installed and configured this month as planned, with the exception of the Auburn server (still awaiting purchase due to administrative issues). The gate servers have not yet been deployed, and will need to be configured and installed in coming months to provide the planned security functionality.

Because of the modular nature of our preservation network, these remaining hardware deployments can be decoupled with the overall process of network assessment, and can occur in parallel with many planned assessment activities. ***We should nevertheless plan to complete all remaining hardware acquisition and deployment activities by the end of November 2005.***

This will require some tasks. The Auburn team will plan to purchase and complete installation of their vault server by October 31, 2005. The technical subcommittee will plan to develop a separate Security and Continuity Plan by October 31, 2005 which will lay out scenarios for firewall protection, security breaches, and hardware failures. Among other details, this plan will describe the specifics of deploying the Gate Servers (if the site wants to implement one), and the process for adding them to the individual preservation nodes. This plan will also identify other related documents that will be needed by the time the Cooperative Agreement is developed. All sites will deploy remaining hardware according to this plan by November 25, 2005.

These tasks will complete the remaining hardware deployment activities required for the Preservation Network.

### **What**

There are several different assessment activities that we will undertake. These activities logically build on one another in terms of infrastructure and complexity. The Development Sites will take the lead on these activities, and documenting what needs to be done:

1. **Collection Recovery:** This assessment would test the capability of the preservation network to recover from the loss on a particular node of a full collection. In such an assessment, a test collection will be intentionally deleted from one of the vault servers in the preservation network. We will test the functionality of the network in recovering the data, as well as the time it takes to recover. We will undertake this test both when an original source site is up and when it is down. All institutions will perform this assessment following an asynchronous, coordinated schedule.
2. **Security Compromise Test:** This assessment will examine the vulnerability of the vault servers to network security compromises, by running a battery of network attacks against a vault server. All institutions will perform this assessment following an asynchronous, coordinated schedule.
3. **Disk Recovery Test/Training:** This assessment would test the process to recover from the loss on a particular node of a full disk volume. In such an assessment, a disk from A) the AX100 unit, and B) the mirrored internal OS disk will be intentionally substituted and recovered from the vault servers in the preservation network. We will test the systems administration process for repairing the hardware and recovering the data, as well as the time it takes to recover. All institutions will perform this assessment following an asynchronous, coordinated schedule.
4. **Vault Recovery Test/Training:** Here we will test the capability of the preservation network to recover from the loss of a complete vault node of the network. In such an assessment, all information on the hard drives one of the vault servers in the preservation network will be totally clobbered. We will document the process of recovery, test the functionality of the network in recovering the data, take notes concerning the time it takes to recover, and generally test the core recovery concepts of the system. All institutions will perform this assessment.

### **Who / How**

The Technical Working Group will prepare tactical plans for the details of accomplishing each of the assessment activities described above, in a time frame that enables the activities to be accomplished according to the schedule below. The Technical Working Group currently includes at least the following individuals: Thomas Robertson, Robert McDonald, Kyle Fenton, Johnny Healey, Weiling Liu,

Lance French, Kamini Santhangopalan, Beth Nicol, Curtis Carr, Larry Hansard, and additional technical hires at the partner sites as they become available.

The respective members of the Steering Committee will be responsible for ensuring that the Network Assessment activities take place according to the schedule below. Technical staff working on the project will be the ones who actually do much of the work in practice, but the Steering Committee members are the individuals responsible for ensuring that the work gets done in time to meet the project timeline.

**When**

- 9/05 – 3/06: Conduct Collection Recovery Tests.
- 11/05 – 7/06: Conduct Security Compromise Tests.
- 3/06 – 9/06: Conduct Disk Recovery Tests/Training at all institutions.
- 3/06 – 12/06: Conduct Node Recovery Tests/Training at all institutions.

**Notes on this document**

This document was completed at the third MetaArchive All-Project Meeting held at Emory University on Monday 2005-08-15 by the Steering Committee and additional attending project participants. The document was last updated by Martin Halbert on 2005-08-15.