ActiveNet

Disaster Recovery Plan

Version History

Version No.	Author/Editor	Approved By	Editing Date
1.0	Dwain Gilliam		March 28, 2016

Table of Contents

1. Plan Introduction

This Disaster Recovery Plan (DRP) covers the failover and recovery procedures for the ActiveNet environment in the event of a disaster at ACTIVE Network's primary data center.

The objectives of the plan are to:

- Ensure recovery of the applications and systems in the timeframes established for this application
- Document the Recovery Team organization and responsibilities

1.1. Terms

Term	Definition
Disaster	A complete failure of the entire primary site due to a regional disaster, the data center facility itself, or a critical dependency that results in the Application or public facing website being unavailable for all users for a period of 8 hours or more with no foreseeable recovery for more than 4 hours.
Primary Site	The ACTIVE Network facility that hosts the installation of the web application that is used under 'normal' conditions (i.e. when no disaster is active). The primary site is configured for full system capacity.
DR or Standby Site	An alternative facility that hosts standby equipment that is configured and ready to take over active serving of the web application. The secondary site will have capacity for 'normal' usage loads. The secondary site will be used temporarily until the primary site is re-activated.
Recovery Time Objective (RTO)	The time in which the web application needs to be restored to full operating capacity and functionality.
Recovery Point Objective (RPO)	Maximum potential loss of data due to a disaster scenario

1.2. Local Redundancy

All our facilities are Tier III or greater with our Las Vegas, NV primary datacenter being Tier IV. This includes fully redundant Power distribution, UPS, generators, cooling and network. Primary datacenter has a 99.995% uptime guarantee for all facilities infrastructure. In the event of a failure of any one component, redundant equipment will seamlessly provide equivalent capacity and functionality.

All systems are part of fully redundant pools of devices. This means that the loss of a single web server or network device, for example, would not impact functionality and the majority of device failures would be completely transparent to the user. In many cases multiple devices could be lost or removed from service to perform maintenance activities without user disruption. Load balancers are utilized to spread customer load across web and application servers and continuously optimize end-user performance and availability. The critical database tier is also part of a clustered pair enabling maintenance activities as well as failure recovery with a minimum of customer interruption.

1.3. DRP Scope

The DRP involves many complex and interconnected systems. The following are considered in scope of this plan and for any recovery and/or testing activities.

RTO and RPO:

As of this document version, recovery of the following services with:

- RTO of 80 hours
- RPO of 4 hours

In Scope:

Restoration of service for ActiveNet production applications includes the recovery of the following systems:

- Application Tier
  - ACM (Consumer UI)
  - Web Pools
  - Reporting
  - Email
  - Scheduling
- Data Tier
  - Related Databases
- Enterprise Services
  - AMS
  - Asset
  - OFS
  - AAS
  - Site Catalyst

Not in Scope:

Business Continuity Planning and any other services or applications not specifically listed above.

2. DR Organization

The Recovery Team is responsible for managing the recovery effort as a whole, ensuring restoration occurs within planned RTO. The Recovery Team consists of the SVP of IT, the Incident Manager, and the technical team. The DR team organization is set up to accomplish the following:

- Documentation and maintenance of the DRP
- Periodic testing of the disaster recovery process
- In the event of a disaster scenario, execute on the recovery of ActiveNet services per the DRP

2.1. Recovery Team Responsibilities

2.1.1. SVP of IT Responsibilities

Pre-Disaster

- Approves the final DRP
- Authorizes periodic DRP testing

Post-Disaster

- Declares that a disaster has occurred and that the recovery effort should begin
- Authorizes any expenditures that would be required
- Monitors the overall recovery process and advises ACTIVE Network Executive management and client stakeholders on the status of the disaster recovery efforts
- Following restoration of services in the secondary datacenter, authorizes any failback to the primary datacenter

2.1.2. Incident Manager Responsibilities

Pre-Disaster

- Maintains and updates the plan as scheduled
- Develops criteria for declaration of disaster
- Distributes DRP to recovery team members
- Appoints recovery team members and alternates as required
- Coordinate testing of the plan
- Trains disaster recovery team members in regard to the Plan

Post-Disaster

- Assesses extent of damage to ACTIVE Network facilities and ability to provide service

- Determines if the situation meets the disaster criteria, provides the initial communication of disaster declaration to recovery team, and presents recommendation to enact the DRP to the SVP of IT for authorization
- Coordinates all technical resource teams during the execution of the DRP
- Should the primary data recovery option (Replication) fail, authorizes team to initiate secondary recovery option (Backups)
- Reports to SVP of IT the status of recovery effort at regular intervals

2.1.3. Technical Resource Responsibilities

In general the technical resources assigned to the recovery team will consist of systems, database, network, storage, and software engineers but may encompass others as needed.

Pre-Disaster

- Maintains both the primary and secondary site infrastructure and services
- Ensures that data replication is occurring between sites as designed
- Ensures that application code is kept up to date in both locations
- Setup and maintain monitoring to detect error conditions
- Ensure backups are occurring

Post-Disaster

- Assess damage and impact to functionality within the environment as specified in the Damage Assessment Plan section and report that assessment to the incident manager
- Attempt to recover services in the primary datacenter if the damage assessment indicates recovery is possible in less than eight (<8) hours.
- Execute the DRP recovery procedures under direction of the incident manager if a disaster scenario has been declared.

2.1.4. Client Resource Responsibilities

Some responsibilities and actions will need to be performed by the client

Post-Disaster

- Ensure connection to DR site to access application

3. Data Backup Details

3.1. Databases

Databases will be recovered from the most recent database backup and the transaction log backups. Daily full and hourly transaction log backups occur and are stored in an online repository that is replicated to the disaster recovery location. Once the database is restored the logs are applied.

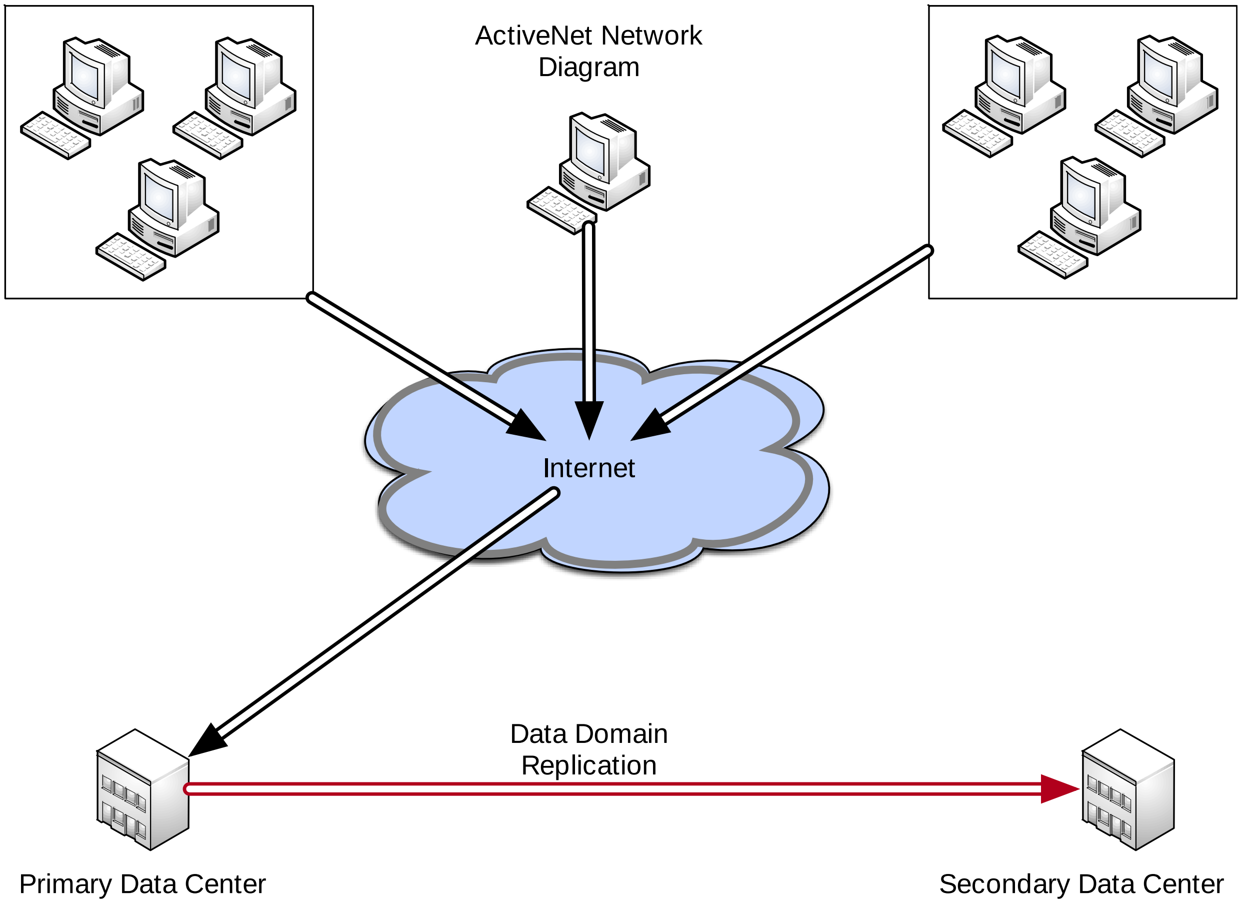
3.2. Applications

The application code base is stored in a code repository that is located in a secure facility. This ensures the very latest versions of source code are available at both the production and DR sites

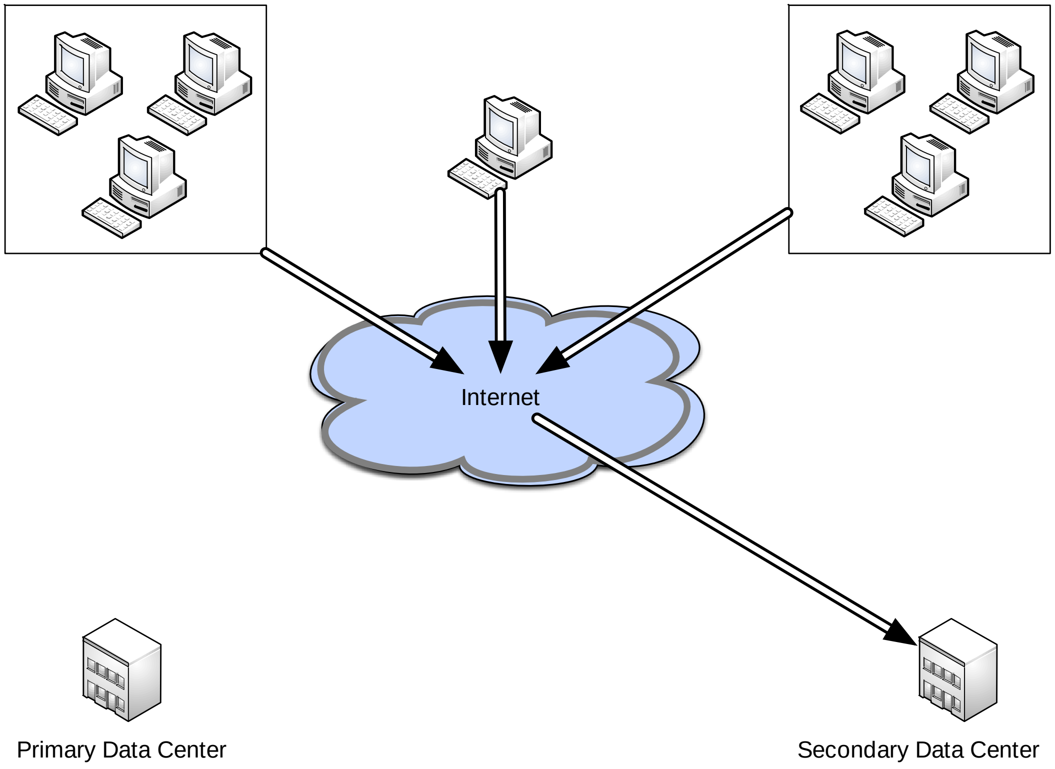
4. DR Emergency Procedures

4.1. Overview

Under normal operations all services operate from the primary site. All user activities are directed from the Internet to the primary site. Backups are replicated from the primary site to the DR site in real time.

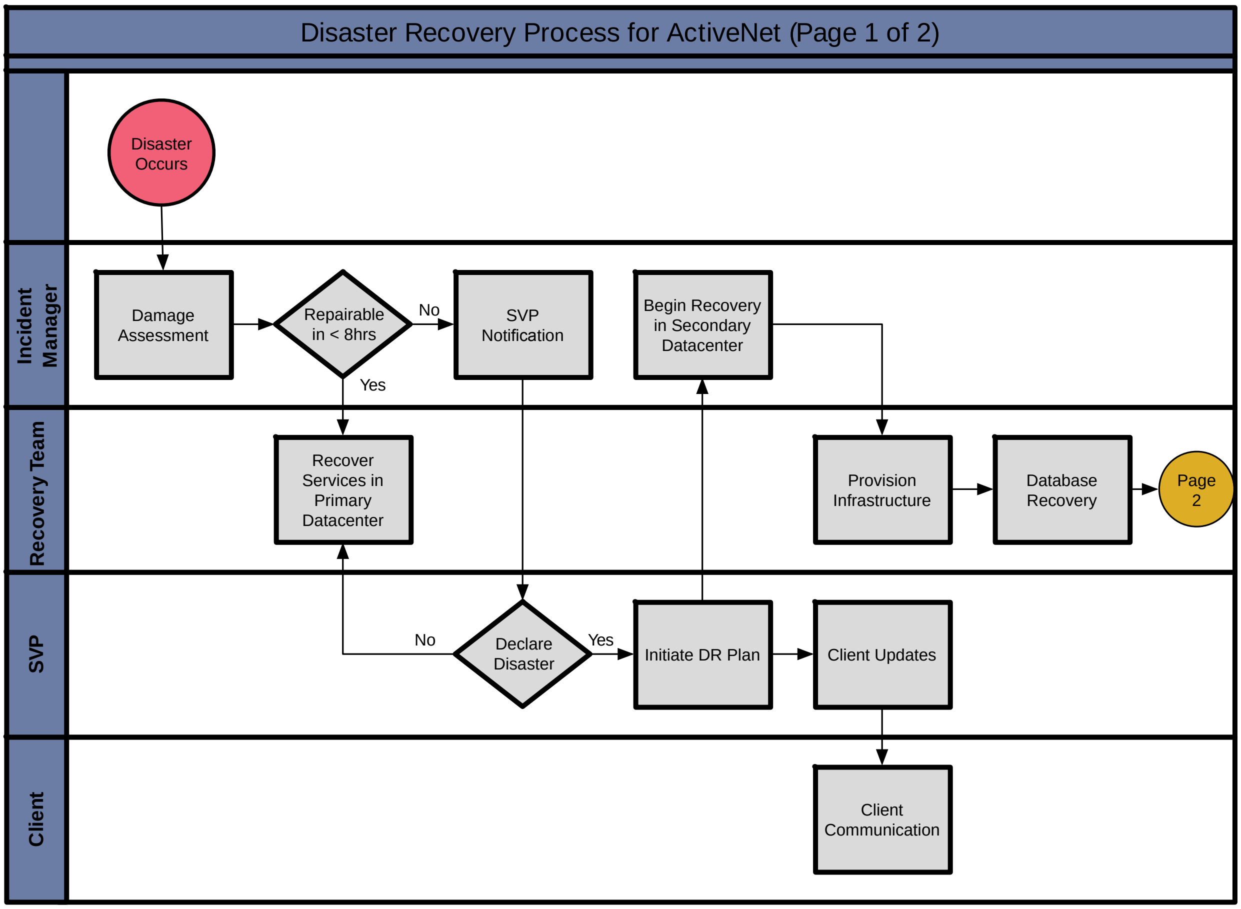


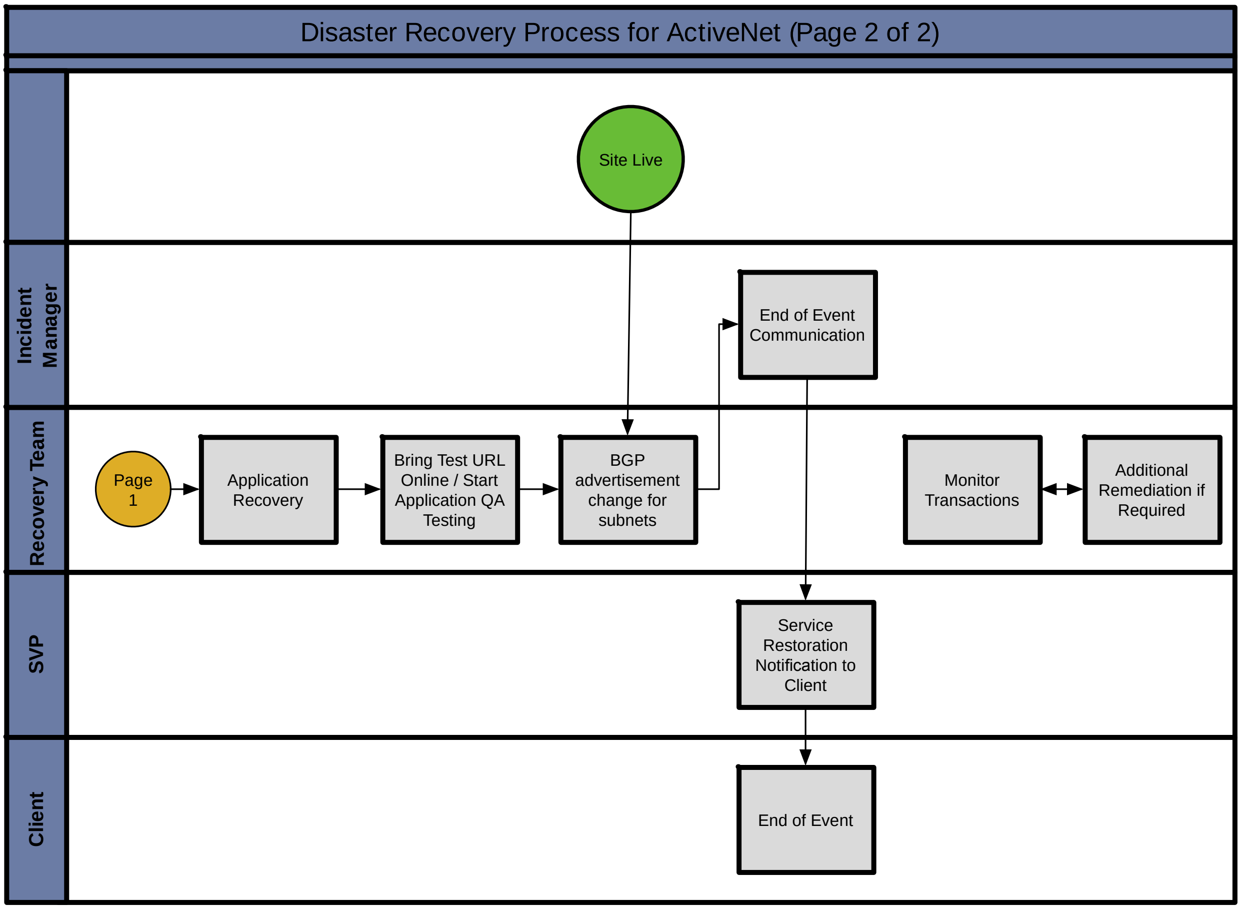
In a disaster scenario, the secondary data center becomes the primary data center and all user activities are directed to the secondary site. Failback to the primary site would occur at a pre-scheduled date and time following complete recovery of all services in that facility.


Internet
Primary Data Center
Secondary Data Center

4.2. System Recovery Process Overview

The high level DR process is outlined in the following two (2) diagrams:




Disaster Recovery Process for ActiveNet (Page 2 of 2)
Incident Manager
Recovery Team
SVP
Client
Site Live
End of Event Communication
Page 1
Application Recovery
Bring Test URL Online / Start Application QA Testing
BGP advertisement change for subnets
Monitor Transactions
Additional Remediation if Required
Service Restoration Notification to Client
End of Event

4.3. Escalation and Communication Plan

The following steps should be followed to notify customer, senior management, and user community of a disaster event and the recovery status.

Ref	Task	Task Owner
1	Upon detection of a potential or actual disaster, immediately notify the Recovery Team members to conduct a survey and damage assessment of the primary data center.	Incident Mgr
2	Assemble all resources on an available incident bridge at and enact the standard incident process.	Incident Mgr
3	Notify the SVP of IT of a possible disaster situation.	Incident Mgr
4	If the damage assessment indicates that no recovery of application functionality and availability in the primary data center is possible in < 8 hours, declare a disaster scenario and instruct the recovery team to executer the DRP	SVP of IT
5	Notify Customer Executive Sponsor and ACTIVE Network Executive Management on the severity of the disaster and the estimated recovery time.	SVP of IT
6	Conduct a briefing with all Recovery Team members and apprise them of the severity of disaster and of initiation of the DRP.	Incident Mgr
7	Monitor the Recovery Team that are performing the failover to the secondary data center and provide updates as per the standard incident management process.	Incident Mgr
8	Upon successful failover and return to operations within the secondary datacenter, notify the SVP of IT and resolve the incident. SVP of IT will notify Executive Sponsor and ACTIVE Executive Team	Incident Mgr SVP of IT

4.4. Damage Assessment Plan

The following steps should be used to assess the damage to the Primary Data Center environment as a result of the Disaster Event

Ref	Task	Task Owner
1	Determine if the application and all in-scope functionality is available to users.	Technical Team

2	If unavailable due to loss of facility or equipment, what must be done to recover so that the ActiveNet system can be returned to an operational state within the Primary DC?	Technical Team
3	Assess the following Data Center Infrastructure: • Facility • Datacenter Building • Power • Cooling • Equipment • Servers • SAN or Storage Devices • Data Network Services • WAN/Internet Communications • Telephony	Technical Team
4	Based upon damage assessment, determine the estimated time to recover based upon to following guidelines: Minimal damage to facility and/or equipment. Estimated time to complete repairs is less than < 8 hours. Extensive damage to facility and/or equipment. Estimate time to complete repairs is equal to or greater than 8 hours	Technical Team
5	Verbally notify the Incident manager of the assessment of damage, estimated time to recover from damage as per Section 4.3	Technical Team
6	Document findings from the survey and damage assessment and send to incident manager and SVP of IT.	Technical Team

4.5. Declaration of Disaster

If the damage assessment indicates that no recovery of application functionality and availability in the primary facility is possible in < 24 hours, the SVP of IT shall declare a disaster scenario. Recovery processes specified below in Section 5, DR Procedure, will then be executed to recover all application functionality in the secondary datacenter.

5. DR Procedure

Critical customer facing components will be brought online. Those include:

BUSINESS PROCESS	DESCRIPTION	MAIN DEPENDENCIES

Access to ActiveNet	Users must be able to access ActiveNet via the Internet	WAN Network Infrastructure Web Servers Application Servers Database
Credit Card Transaction Processing and reconciliation	Users must be able to purchase product via the site.	Access to ActiveNet
Reporting	Administrative users must be able to run reports	Access to ActiveNet Report Servers

Network infrastructure exists at the DR site. This network infrastructure is hot which means that it is always running. In the event of a major disaster the network team will force the advertisement of the external IP blocks from the DR site.

5.1. Infrastructure Restoration

Upon declaration of a disaster the ACTIVE team will begin deploying the necessary infrastructure to return ActiveNet to service.

5.2. Data Tier Restoration

The secondary site contains a backups of the primary site's databases and transaction logs. Once the databases and transaction logs are restored the transaction logs will be used to bring the databases as close to the same state they were prior to the failure.

5.3. Application Tier Restoration

The latest version of all application components will be restored. Once the application is restored the ACTIVE team will verify that the application Tier is communicating to the database layer. Credit card processing is functioning. Reporting is functioning.

5.4. Enterprise Services Tier Restoration

Once the Enterprise Services tier is restored and brought online the ACTIVE team will verify that the integration between the Application Tier and the Enterprise Services Tier is functioning as designed..

5.5. BGP Failover

If the primary site is completely inaccessible, BGP will automatically direct end user network traffic to the secondary site.

If the primary site is accessible but non-functional, manual steps must be performed to force end user traffic to the secondary site.

5.6. Application and QA Testing

Once all Tiers are online the ACTIVE application and QA teams will begin testing. The customer may also be involved in testing. Once testing is complete the decision will be made to go live.

5.7. Go Live

One the go live decision has been made the application will be made available to all users. All stakeholders will be notified at this point that the restoration of service is complete.