Chabot – Las Positas Community College District

Information Technology Services

Disaster Recovery Plan

Supplement to August 1, 2014 Plan (General Version)

Note: Selected charts and tables are blanked out for security purposes

September 2014

Submitted By
J. Methe
Chief Technology Officer

INTRODUCTION

This document provides an update to the Information Technology Services *"Disaster Recovery Plan"*, dated August 1, 2014. The major changes described in this document are as a result of CLPCCD's transition from Novell Netware network operating system and Groupwise messaging to Microsoft Active Directory Services and Exchange.

In June 2014, CLPCCD District Office migrated from Netware version 6.5 to Windows 2012 Active Directory. Subsequently in January 2015, CLPCCD to include District Office, Las Positas College, and Chabot College, migrated from Groupwise version 7 to Microsoft Exchange 2013 messaging for email, calendaring, and collaboration.

To support the new infrastructure, new physical and virtual servers with the corresponding systems and applications software were deployed: Hewlett Packard (HP) blade and stand-alone servers, Storage Area Network (SAN), Unitrends appliance for disk-to-disk backup and data restoration, VMWare and Microsoft Hyper-V virtualization technologies.

The subsequent narrative, below, further explains the changes to the Disaster Recovery Plan as a result of CLPCCD's migration to Active Directory and Exchange.

It should be noted that this document includes sensitive information with detailed descriptions of hardware and software computer systems which is confidential to the Information Technology Services staff within the district. Given the level of detail that is presented, this information, if used improperly, could place CLPCCD in a vulnerable position with respect to viruses and other threats that could impact the IT infrastructure. As such, this entire document will be circulated to a limited set of District ITS and LPC IT staff, and is considered "For ITS Limited Distribution only" to those individuals who have a need to know this information in performance of their daily jobs. This "General Version" of the Disaster Recovery plan document has been modified for security purposes to blank our selected charts and tables with sensitive information and to remove the Appendices containing additional detailed information. This information is available for viewing upon request to the Chief Technology Officer.

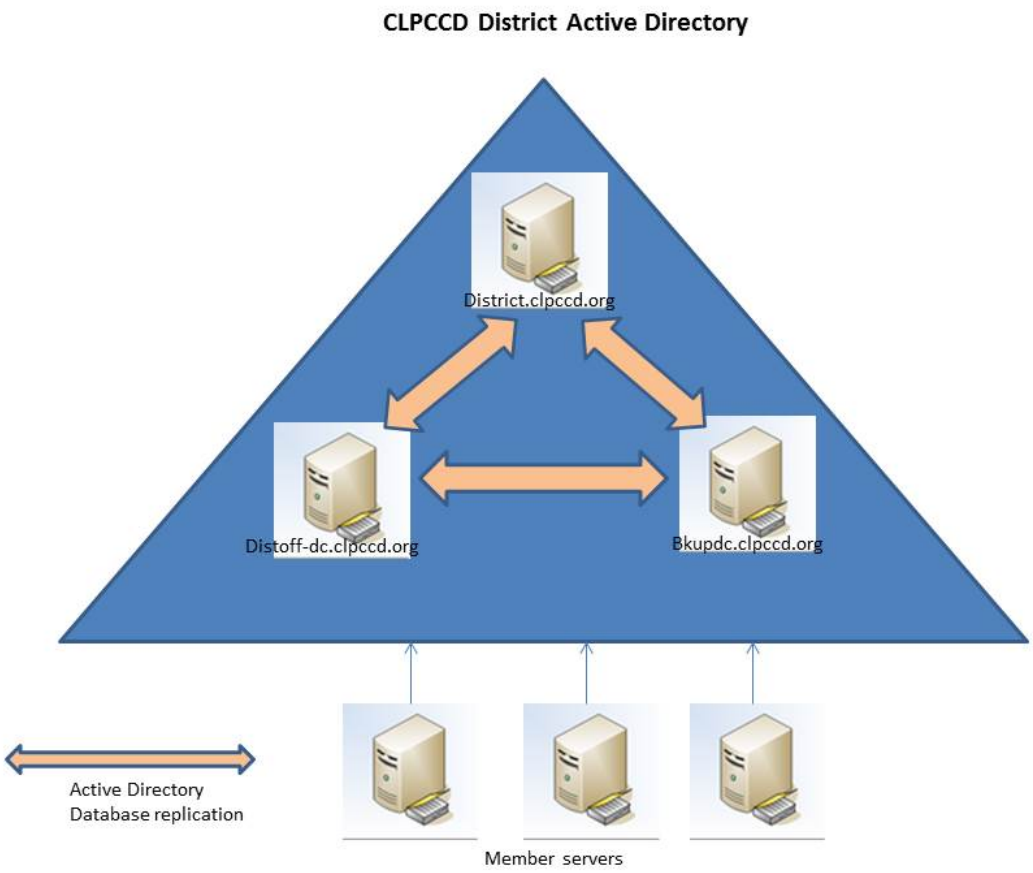
MIGRATION FROM NOVELL NETWARE DIRECTORY SERVICES (NDS) TO MICROSOFT WINDOWS 2012 ACTIVE DIRECTORY SERVICES (AD)

CLPCCD has completed a major project to migrate District office users from Novell Netware NDS to Microsoft Windows 2012 Active Directory (AD). Windows AD provides network authentication and authorization services and the appropriate rights and privileges to allow users access to network resources. It is an LDAP-based directory services that centrally stores and manages network resources or objects such as user accounts, passwords, groups, security credentials, application servers, workstations, e-mail accounts, shared files and folders, and printers.

The servers that manage the Windows Active Directory are called domain controllers. The District is served with a primary domain controller, which is housed on an HP server in the District Administrative Computer room located in the LPC IT Building, and a virtualized redundant domain controller located in the Dublin District office. If one domain controller fails, users can still authenticate against the other domain controller. The domain controllers also provide internal Domain Name Resolution (DNS) and Dynamic Host Configuration Protocol (DHCP). DNS provides mapping of IP addresses to computer names internally. DHCP provides dynamic IP address to users when they log on to the network.

Additionally, printing services have been configured on print servers located in the District office at Dublin and in District Administrative Computer room located in the LPC IT Building. Printer queues and drivers are centrally stored and managed on the print servers. Users on their PCs can simply point to the print queues to print documents. If the print server located in Dublin fails, users can point to the queues stored on the LPC print server.

CLPCCD District Active Directory infrastructure is illustrated below:



The table below shows the IP addresses and server names for the domain controllers and member servers to include data servers and print servers.

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. **This information is available for viewing upon request to the Chief Technology Officer.**

Server Name	IP Address	Function	Hardware	OS	Location

The three domain controllers provide redundancy in case of a server failure on one of the controllers. This is possible as the Active Directory database containing user accounts and credentials are replicated to all three domain controllers. Additionally the physical and virtual server images are backed up on the Unitrends appliance's disk. In the event of a virtual or hardware server failure, the images can be readily reconstituted with no impact to the production environment.

MIGRATION FROM NOVELL GROUPWISE TO MICROSOFT EXCHANGE 2013

In early January 2015 CLPCCD, which includes all LPC, Chabot, and District users, migrated from Novell Groupwise version 7 to Microsoft Exchange 2013 messaging system for email, calendaring, and collaboration. On user desktops, Outlook 2010 and 2013 were installed to replace Groupwise as the email client software. Microsoft's Outlook Web Access (OWA), using a web browser, is now available for remote users to access their emails and calendars. For users with smartphones, users can access emails and calendars using Microsoft ActiveSync protocol.

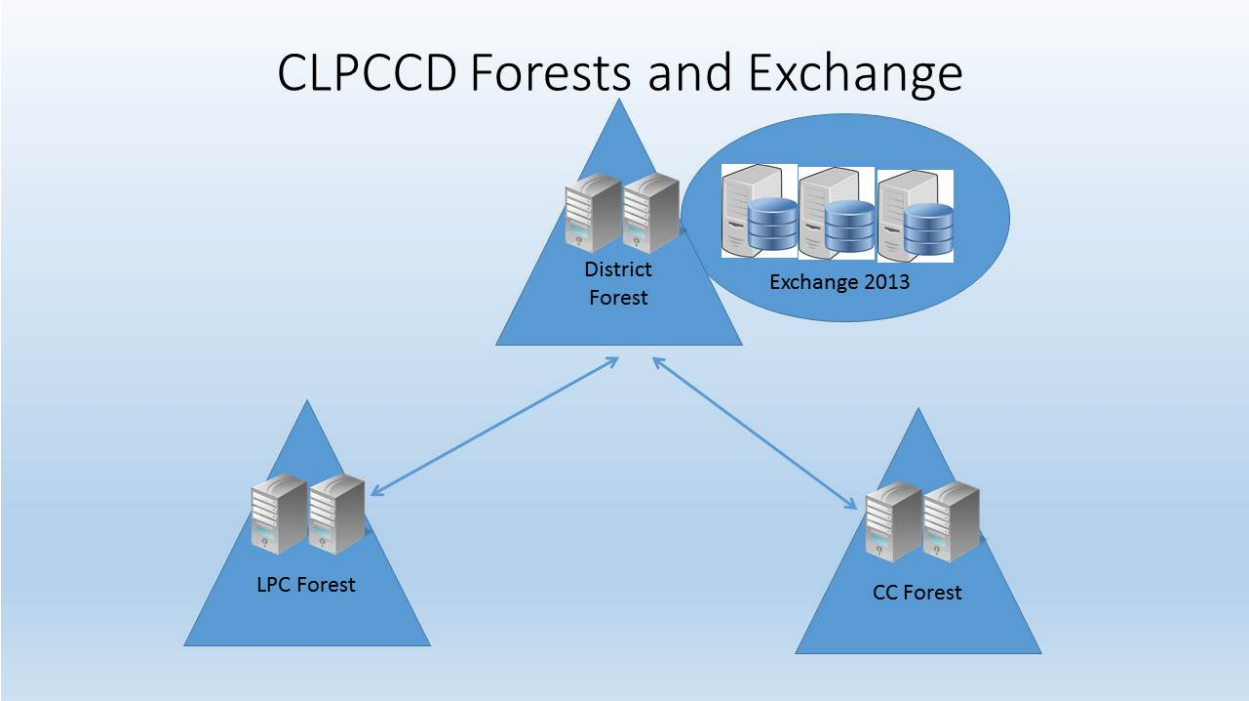
The goal of the Exchange architecture is to provide a robust, state-of-the art, highly available messaging infrastructure for CLPCCD employees anytime anywhere utilizing their PCs, laptops, smartphones, and tablets securely in the office, home, and various remote locations. With this in mind, Exchange was designed to adhere to disaster recovery, high availability, site resilience, and business continuity best practices.

To achieve this goal, the following hardware and software systems were deployed:

- Hardware
    - HP blade enclosures with 16 HP BL460c Gen 8
    - 32x16 GB = 512 GB RAM
    - Intel Xeon CPU E5-2650
    - Flex Fabric Switch with 10 gig core uplink
    - HP 3PAR StoreServ 7200 SANS, Fiber Channel, 8TB
    - Datacove for E-discovery and legal retention

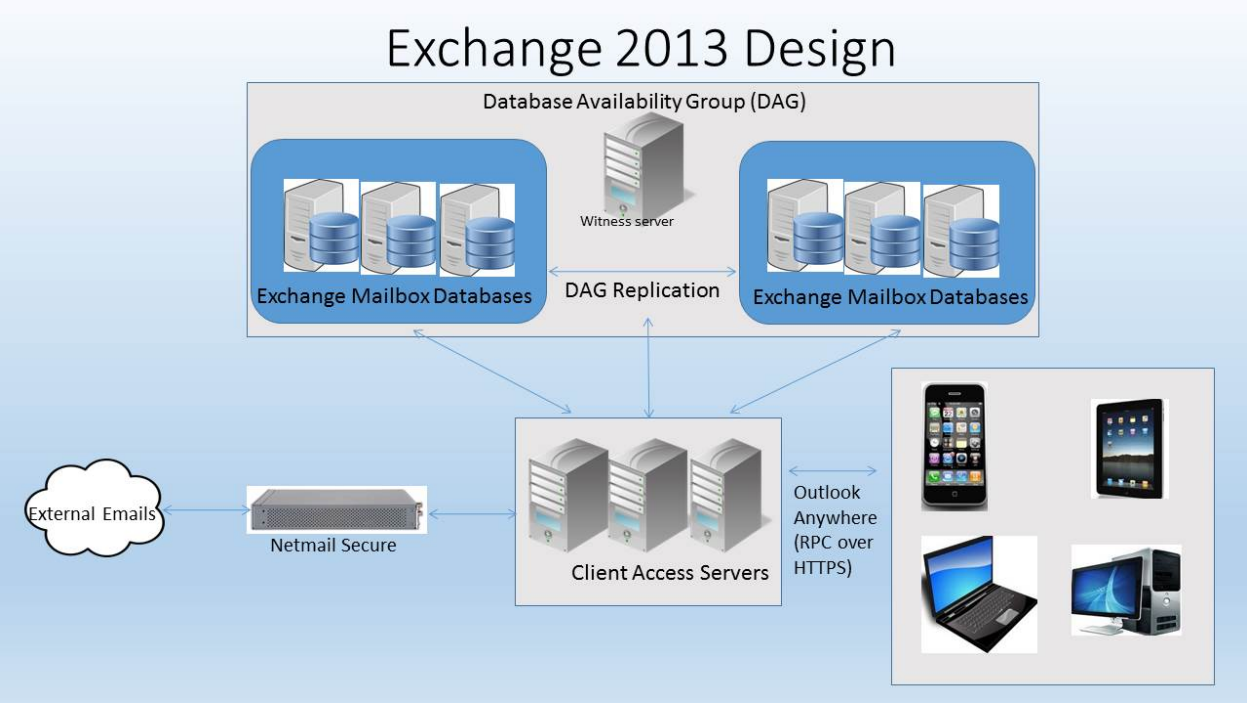
- Software
    - Windows 2012 Active Directory Domain Services
    - Microsoft Exchange 2013 Enterprise SP1
    - VMWARE VSPHERE 5 Enterprise, 14 CPU license
    - Microsoft Systems Center Operations Manager (planned)
    - Netmail Netsecure (provides anti-SPAM and virus filtering)

Since Exchange is tightly integrated with Active Directory, a robust fully functional district-wide Active Directory infrastructure is essential. Below depicts CLPCCD's Active Directory architecture and how Exchange is integrated:



Five Exchange servers consisting of three VMWARE virtual servers and two HP physical servers are deployed to provide redundancy and resiliency. Additionally Microsoft's Database Availability Group (DAG) is configured to provide a robust, highly available messaging and redundant platform. A DAG enables the replication of Exchange databases that are stored on the five servers. If one or two servers or databases become unavailable, services can be readily restored and users will not experience any prolonged downtime.

An illustration of the Microsoft Exchange environment is provided below:



Additionally, a load balancer is configured to provide redundant, round-robin client access to any of the five database servers. If one or two servers fail, the other servers take over automatically to provide uninterrupted user access.

The table below shows the server names and IP addresses of the Exchange servers and load balancer.

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. **This information is available for viewing upon request to the Chief Technology Officer.**

Server Name	IP Address	Function	Hardware	OS	Location

For backup and backup recovery, Unitrends 933S appliance with 22 TB of useable disk storage is deployed to provide disk-based backups for user emails, user files, VMWARE and Hyper-V virtualized servers, and bare-metal physical servers. Unitrends can recover single or multiple emails that are accidentally deleted. It backs up entire Exchange databases to disk for restoration purposes. It can back up physical or virtual Windows operating system and Exchanges servers,

and Linux servers. If a physical or virtual server is damaged, the server, operating system, and applications can be restored from Unitrends within minutes. An HP Ultrium tape drive is connected to the Unitrends appliance to offload backups from disk to tape to provide off-site storage of backup tapes.

For Exchange, only the replicated databases are backed up; in other words, the live databases do not need to be backed up as the replicated databases are mirror copies of the live databases. The replicated databases are fully backed up on the weekends and differentially backed up from Monday to Friday. The Exchange server images containing the Windows 2012 operating system, Exchange 2013 application, and databases are backed up once a month. User data, both IT and District office, are backed up fully on weekends and differentially from Monday to Friday.

The table below illustrates a sample backup plan:

Server Name	OS	Directories	Backup Schedule
Mail1	Win2012	F:\Program Files\Microsoft\Exchange Server\V15\Mailbox	Sat (Full), M-F (Diff)
Mail2	Win2012	F:\Program Files\Microsoft\Exchange Server\V15\Mailbox	Sat (Full), M-F (Diff)
Mail3	Win2012	F:\Program Files\Microsoft\Exchange Server\V15\Mailbox	Sat (Full), M-F (Diff)
Mail4	Win2012	F:\Program Files\Microsoft\Exchange Server\V15\Mailbox	Sun (Full), M-F (Diff)
Mail5	Win2012	F:\Program Files\Microsoft\Exchange Server\V15\Mailbox	Sun (Full), M-F (Diff)
Distoffdata	Win2012	F:\Data\	Sat (Full), M-F (Diff)
ITSData	Win2012	F:\Data\	Sun (Full), M-F (Diff)