# Report on Backup, Restoration and Archiving

08-28-2016

## TABLE OF CONTENTS

## 1. INTRODUCTION

This document summarizes the architecture and procedures used to back up and restore the Technical Infrastructure. The document also addresses potential issues and recommended changes.

For discussion purposes, the current state of the backup and restoration architecture / environment is presented in the following subsections:

- Archiving
- Data backup and restoration
- Oracle vServer backup and restoration
- Network backup and restoration
- Other backup and restoration
- Enterprise backup recommendation
- Backup retention period
- Servers currently not backed up

There are no Service Level Agreements (SLA) or Liquidated Damages (LD) associated with backup, restoration and archiving.

## 2. DEFINITIONS

| Term | Definition |
|---|---|
| AD | Active Directory |
| BCS | Backup Central Site |
| DBA | Database Administrator |
| DNS | Domain Name Service |
| DR | Disaster Recovery |
| LAN | Local Area Network |
| LD | Liquidated Damages |
| NAS | Network Attached Storage |
| NCM | Network Configuration Manager |
| NIS | Network Information Service |
| ODA | Oracle Database Appliance |
| OEM | Oracle Enterprise Manager |
| OVS | Oracle Virtual Server |
| PCS | Primary Central Site |
| PMO | Program Management Office |
| RMAN | Recovery Manager |
| SLA | Service Level Agreement |
| SOW | Statement of Work |
| TB | Terabytes |
| VDI | Virtual Desktop Interface |
| VM | Virtual Machine |
| WAN | Wide Area Network |

**Table 1 Definitions**

## 3. ARCHIVING

### 3.1. CURRENT SITUATION

Archiving of data is accomplished through the backup infrastructure components and processes. There is no dedicated archiving equipment or third-party off-site storage environment.

### 3.2. RESTORATION

Archive is a repository of historical records and data. Archive records and data are not used for systems restoration.

### 3.3. FUTURE SITUATION

The company is not aware of any planned changes to the current archiving design.

### 3.4. CHALLENGES/GAPS

Without dedicated archiving equipment, searching through large volumes of years-old data and meta-data will be a difficult and time-consuming process.

### 3.5. SUMMARY

The customer confirmed that no archiving equipment will be used and seemed unconcerned with any challenges to searching through large volumes of storage to retrieve old data.

## 4. DATA BACKUP AND RESTORATION

### 4.1. CURRENT SITUATION

Active DataGuard replicates the Exadata database in real time from the PCS to the BCS for the Production environment only. Each of these identical databases is backed up daily to the local ZFS appliance using RMAN. Active DataGuard will not be implemented in any other environment.

The architecture for data backup and restoration is shown in the figure below.

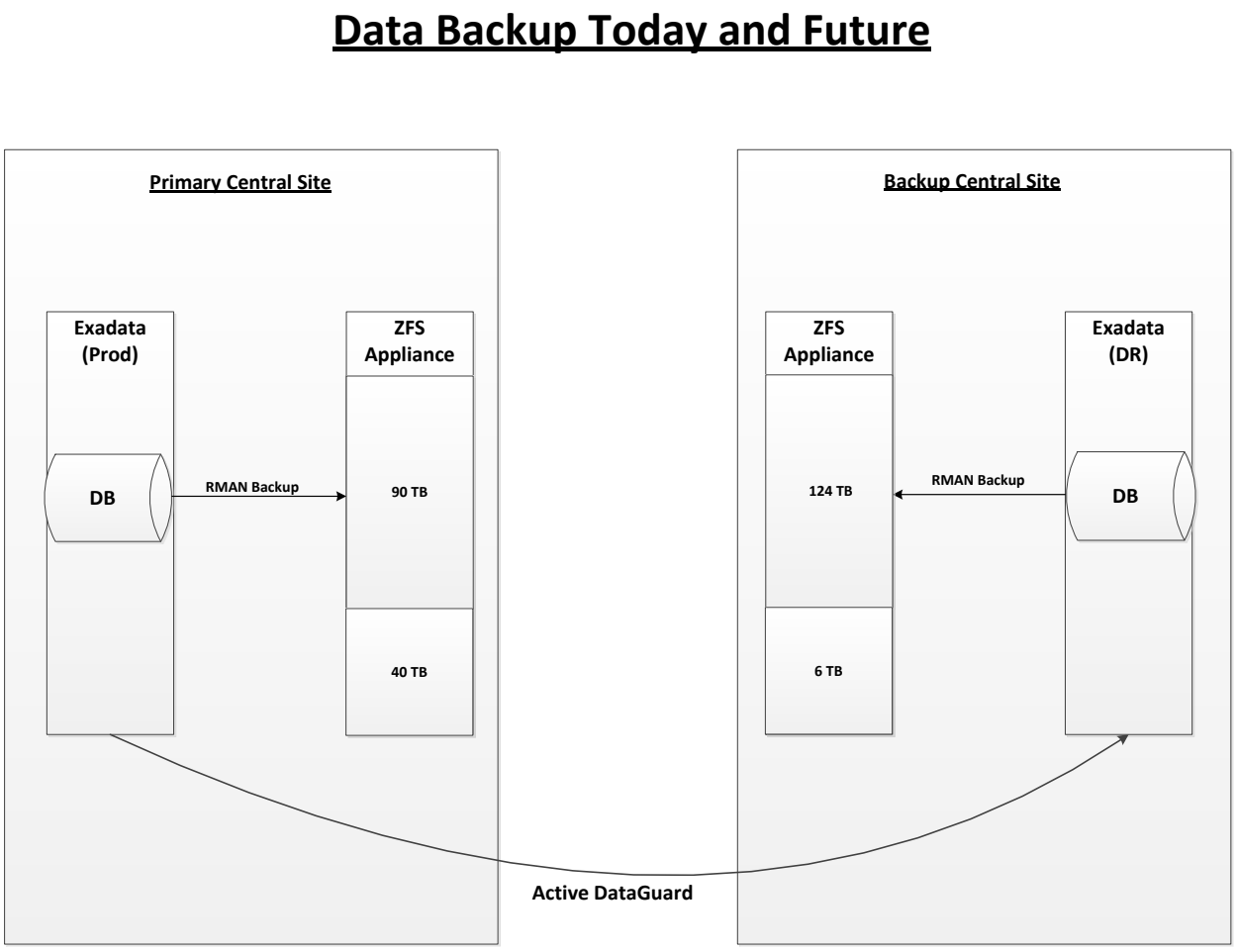


**Figure 1 Current Data Backup Architecture**

### 4.2. **RESTORATION**

The Active DataGuard is a one-way technology. The backup occurs from PCS to BCS, but not in the other direction. Because Active DataGuard only replicates data in one direction, failing back from BCS to PCS will involve copying the database back manually, unless an alternate technical solution or a new operational procedure is incorporated to address this issue.

### 4.3. **FUTURE SITUATION**

The company understands the current Active DataGuard design is the final design and that there are no additional planned changes.

In light of Active DataGuard's one-way limitation, we recommend that either a) a two-way solution, such as Oracle's GoldenGate, be incorporated into the design, or b) an operational procedure be established in which Active DataGuard is used to both replicate the PCS to the BCS under normal operation and replicate the BCS back to the PCS (after it comes back online) in the event of a disaster.

The company further recommends that whatever solutions is chosen, it be incorporated into the production and development environments.

### 4.4. **INDUSTRY BEST PRACTICES**

For disk-based backup of databases, Oracle recommends the following:

- Use a Fast Recovery Area (FRA)
- Perform an initial RMAN level 0 (full) backup
- Perform daily RMAN incremental level 1 backups
- Roll incremental backups into full backup and delay by 24 hours

### 4.5. **CHALLENGES/GAPS**

a. Active DataGuard will not be implemented in any environments other than Production. The company understands additional Active DataGuard licenses would need to be purchased to provide the service to these environments.

b. Unless a two-way solution is installed or an operational procedure established to use Active DataGuard in both directions, restoring data from the BCS to the PCS will be a manual and time consuming operation. There are two scenarios to account for:

   i. Graceful Failover – If the failover is graceful, meaning the DBA team has time to gracefully shutdown the databases before the failover, then after the issue which caused the failover is corrected, it may be possible to failback by reversing the direction of DataGuard synchronization from BCS

to PCS. Then, once the synchronization is complete, the DNS can be updated to resolve back to the PCS.

ii. Cut over – If graceful failover is not an option (power outage, fire, flood, earthquake, etc.), then to failback, a copy of the database will need to be PHYSICALLY retrieved from the BCS. As the timeframe (duration) for WAN transfer of the data is expected to take over 277 days (transfer of ~ 10TB), The company would plan on copying the database to a locally attached storage device and then transporting it back to the PCS where it will be uploaded to the Exadata. If all goes well, reversal of synchronization can still take place to cover the lag in time for when the database was in transit.

### 4.6. SUMMARY

The customer confirmed that an operational procedure has been established to utilize Active DataGuard in syncing the new PCS to the BCS in the event that the old PCS experiences a catastrophic failure.

## 5. ORACLE VSERVER BACKUP AND RESTORATION

### 5.1. CURRENT SITUATION

A snap shot is taken of the /U01 file for the vServers on Exalogic at the end of the day and stored on the Exalogic's own internal storage (the same process is deployed at the PCS and BCS). There is no off-site backup for the vServers today. This architecture and procedure are the same for the Development environment.

Also, per customer design, DR vServers are not exact replicas of Production vServers.

The architecture for Oracle vServer backup and restoration is shown in the figure below.

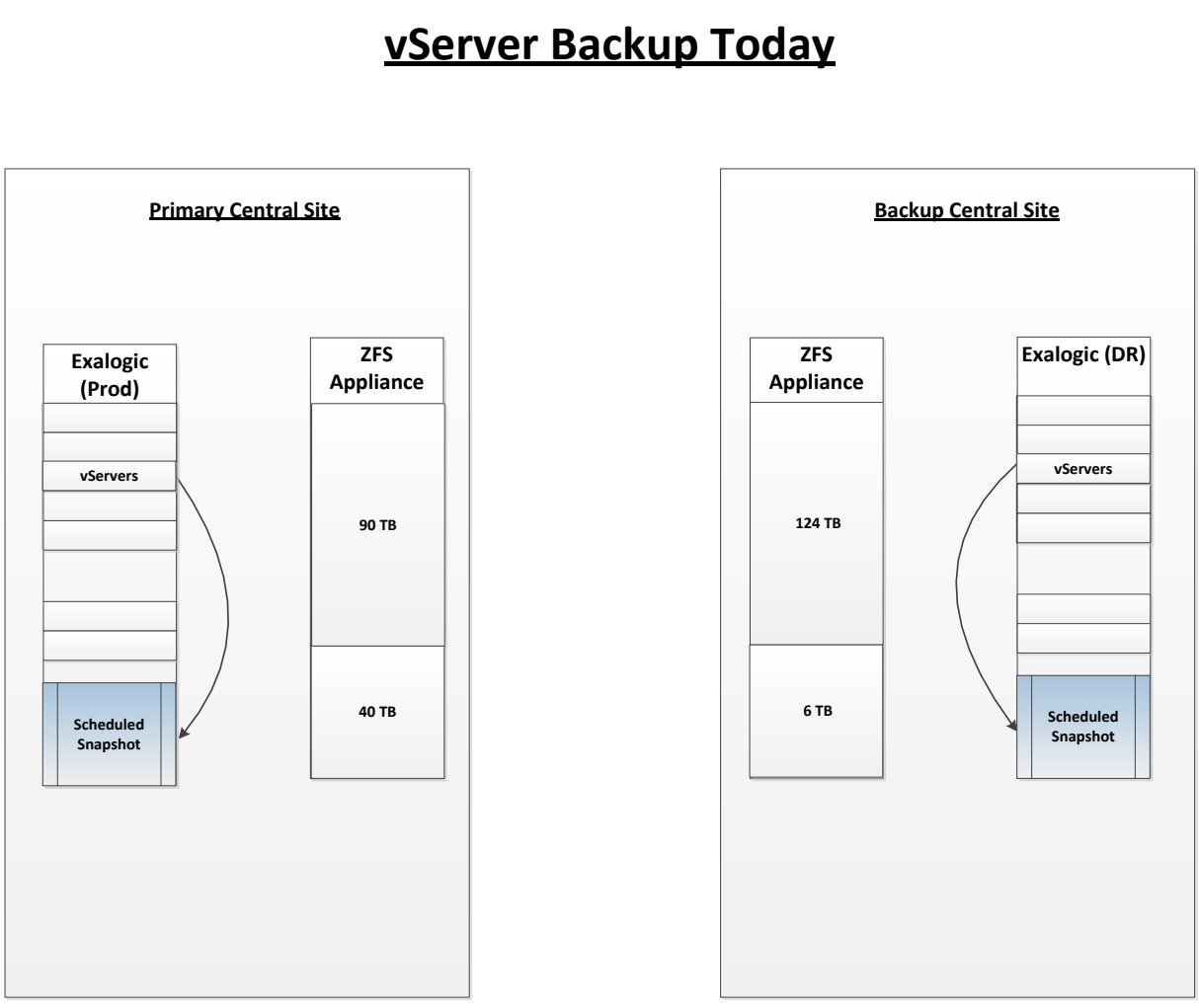


**Figure 2 Current vServer Backup Architecture**

### 5.2. **RESTORATION**

vServers have been successfully restored from the local snapshot. They have not yet been restored from a remote location. Once remote backup is implemented, a checksum will be performed to confirm that the remote backup was successful. If the checksum is okay, the restoration should be okay.

### 5.3. **FUTURE SITUATION**

In August 2016, daily remote backup will be implemented to save a copy of the vServers on the ZFS appliance at the other central site. The same holds for the Development environment. This situation is depicted in the figure below.

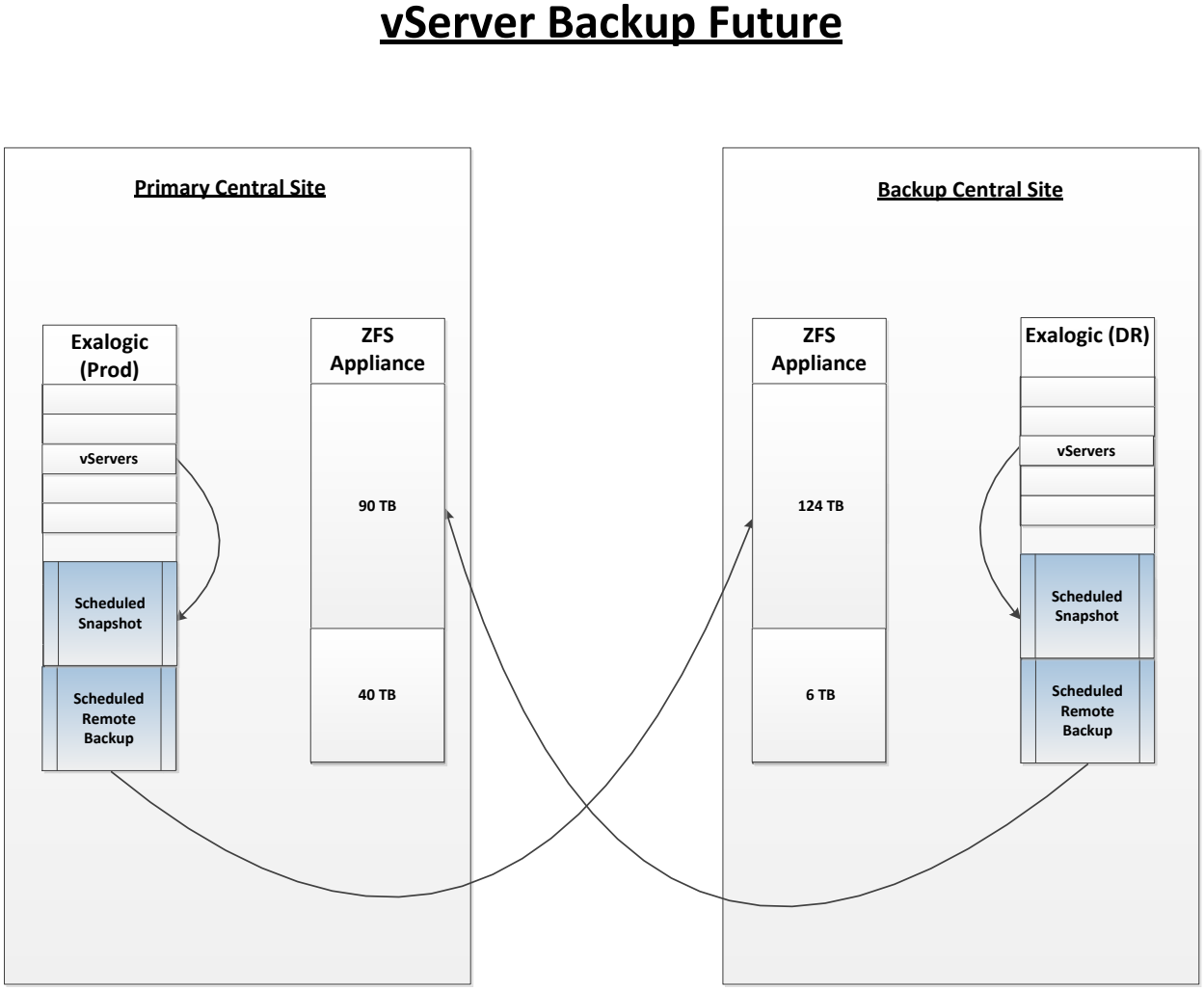


**Figure 3 Anticipated Future vServer Backup Architecture**

## 5.4. **INDUSTRY BEST PRACTICES**

The following text was taken from the Oracle Whitepaper Oracle VM3: Backup and Recovery Best Practices Guide:

> *Retention periods for snapshots are usually measured in terms of a few days to a week, necessarily short due to the way the software tracks changes between the live data and static data.*
>
> *The snapshots can be taken to tape periodically which captures 100% of the data associated with a volume including the SAN boot LUNs – it automatically combines the data from the original volume as well as the changed data contained in the snapshot to form a full backup. The snapshot can be deleted once the data from a snapshot has been captured on tape. Tape allows for retention windows of snapshots to be measured in weeks, months and years.*

## 5.5. **CHALLENGES/GAPS**

a. DR vServers are not exact replicas of Production vServers. This could potentially be an issue if changes are not synced between Production and DR. This is a process that the customer would need to create in order to make sure the two environments are synced. The company recommends a policy that changes not be made to Production vServers unless they are also made to DR vServers.

b. vServers have not yet been restored by remote replication. When these get restored by replication depends on whether it is engineered or non-engineered systems, and is also dependent on the environment.

c. Using snapshot, as opposed to archiving, is a very inefficient long-term (i.e., quarterly or annually) storage method because snap shots are not static and must continue to grow in size (disk storage size) each time a single change is made. The ZFS is almost certain to run out of storage space using this approach for long-term storage. The company does not have any numbers at present to estimate when it will run out as the design is still changing. A better solution would be to incorporate an enterprise storage solutions (e.g., NetBackup or TSM), which would create static backups that would roll off as the retention requirements are fulfilled.

d. Initially, Oracle did an analysis confirming that the storage solution would be adequate using a ZFS Appliance as backup to disk with 4-10TB of data and no NFS services or FileServer Applications running on the ZFS. No analysis has been done on the actual implementation, which does run NFS services on the ZFS and has 40+TB of data. Consequently it is unclear if the ZFS appliances are capable of storing seven years' worth of snapshot data. It will take considerable time to

figure out how this can be calculated. Regular SysAdmin may be able to determine this, or help may be required via an Oracle Service Request. However, since the production environment is still being developed and the company does not know how much data will end up being managed, there is not currently enough information to make an accurate projection. We understand Oracle recommended the Exadata solution with the expectation that it would be used entirely as "backup to disk" storage. If it is determined that there is insufficient storage available, a plan will be needed to either expand the storage environment with the existing technology or switch to a larger storage device.

e. Before any calculations can be made on the storage capacity of the ZFS, a documented agreement is needed that establishes exactly what gets backed up, and for how long, in accordance with Exhibit 5. Questions that need addressing include, what gets backed up to the ZFS, data or everything? What environments get backed up, Production, DR, Development? Will the ZFS continue to be allocated as a file server? Does everything have to be backed up for seven years, or just the data?

f. When the ZFS Appliance was first implemented, it was believed that the database would be between 4TB and 10TB. Today the database already exceeds 40TB (before the pilot). Additionally, more than 40TB of the ZFS at the PCS has been allocated to accommodate VDI backups and restorations. The company had recommended that the VDI Environment be implemented in a separate storage device, but as of yet this has not happened. It is likely that storage will run out using the current model, but exact numbers cannot be provided until building is complete and the design stops changing.

g. Snapshots are made up of two components: 1) the *base* file that has unchanged data and 2) the *changed blocks* that contain the snapshot of all changes in a given time period. Because of this, if the base file becomes corrupted, then all of the snapshots become corrupt. What is not known is whether ZFS replication also keeps the BCS copy up to date automatically. If so, then whenever the base file becomes corrupted at the PCS, the remote copy at the BCS will also be corrupt, essentially invalidating all backups. What would mitigate this is if a compare procedure is run on the two base files to validate they match prior to replication. We do not know if there is such a utility as part of the replication process.

### 5.6. SUMMARY

The customer confirmed that DR vServers are not exact replicas of Production vServers and they are okay with that since Production vServers are replicated off-site and could be restored if needed. There is no reason that Production and Development need to be in sync.

The customer agreed that given the current architecture and methodology for backing up vServers, more storage capacity will be required and they have agreed they will procure more storage. How much storage will be procured and when was not discussed.

They did not directly address our concern regarding how to deal with corrupted snapshot base files.

## 6. NETWORK BACKUP AND RESTORATION

### 6.1. CURRENT SITUATION

The configuration files of all of the central site switches, routers and firewalls, in both the primary and secondary racks, are backed up daily by SolarWinds NCM to a SolarWinds SQL database that resides in the Monitoring infrastructure rack. The Syslog files for these same devices are backed up by ArcSight to the local ZFS appliance.

In addition, the SolarWinds VM and the Control-M VM, which both reside on the Monitoring infrastructure rack, are backed up daily to storage on the same rack using Veeam.

The configuration files for all of the ArcSight applications are backed up manually, only after a configuration change, to a predefined area on the local ZFS appliance.

The architecture for network backup is shown in the figure below. Currently there is no off-site backup of any of the aforementioned.

# Network Backup Today

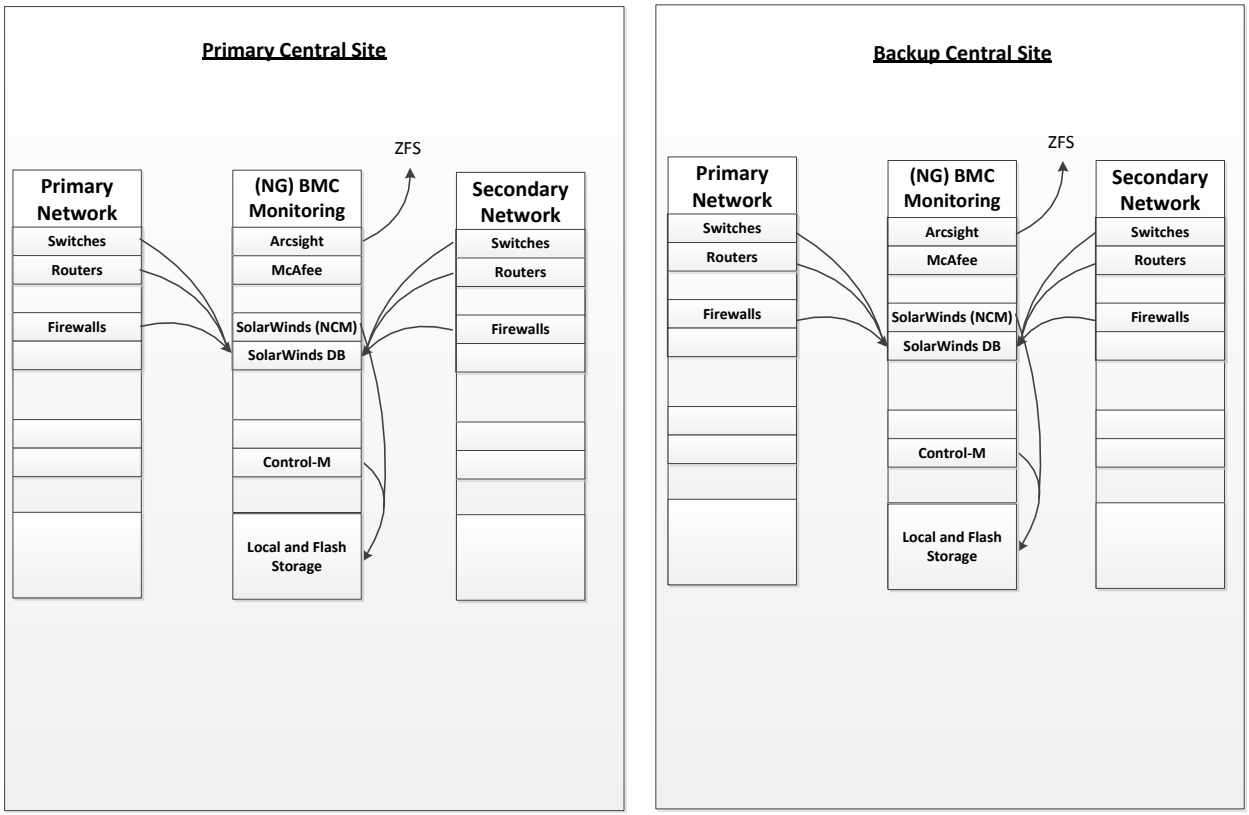


**Figure 4 Current Network Backup Architecture**

## 6.2. **RESTORATION**

Backup configurations can be applied to the various devices easily as long as there is access to the network device. If the devices are un-reachable over the network, they can only be restored either by being physically at the device, or using a non-Ethernet connection to reach the device. Companies such as Lantronix offer such remote access products using non-Ethernet technology.

### 6.3. **FUTURE SITUATION**

As we understand it there are no planned changes to the network backup design.

### 6.4. **INDUSTRY BEST PRACTICES**

Cisco best practices recommends the following with regard to backing up their equipment:

> *Store copies of the software images and configuration files so that you can quickly replace any damaged or deleted files. Store the copies on other non-removable flash devices, on removal media that is not kept in the switch's slot, or on a TFTP, HTTP, or RCP server. Store a copy of the configuration files on the RP bootflash: device.*

In addition, there are different versions of IOS that can run on different routers. In a rebuild situation, it would be quicker to have the Cisco IOS download for each router in the backup location with the *.bin configuration file.

### 6.5. **CHALLENGES/GAPS**

a. The company needs to verify the Syslog files for these same devices are being backed up by ArcSight to the local ZFS appliance.

b. The management of TippingPoint has just recently been transitioned to the company. The Network team is studying TippingPoint to come up with a methodology for backing it up.

c. There is no offsite backup for any network configurations. The system administrators should be able to create database transfers between sites. This can be done using VMware tools. The network team, in conjunction with the systems administrators, will create a backup plan for the network and security infrastructure.

### **6.6. SUMMARY**

The challenges/gaps for network backup are primarily company items that are being addressed by our SysAdmin and Network teams.

## 7. OTHER BACKUP AND RESTORATION

### 7.1. CURRENT SITUATION

The AD/DNS and Rational application, which reside in the Spare LAN/WAN rack in the PCS, are backed up daily using the native Windows backup utility to an NAS storage in that rack. The Rational back up is written over each time which means there are no historical backups.

Full backups of physical servers are not done. Only the important files on physical servers, as determined by the SysAdmin who built it, are backed up. In the Development Tools rack, there are three different types of backups:

1. NIS Master, Wikid, Wikid Sec and the Firewall VMs are backed up daily to the local ZFS appliance using a script.

2. The ODA is backed up daily to the local ZFS appliance using RMAN.

3. The OEM Cluster is backed up manually on an as-needed basis to the local ZFS appliance. The last backup was in May, 2016. A new backup is anticipated to happen the week of 8/3/16.

A daily snap shot of the Production Tools VDIs are stored on the local ZFS appliance. These backups occur in a separate storage location within the ZFS from where the vServers are stored.

In the BCS, the AD/DNS in the Spare LAN/WAN rack is not backed up as there is no storage in that rack.

In the DR Tools rack, there are also three different types of backups:

1. NIS Replica and Wikid are backed up daily to the local ZFS appliance using a script.

2. The ODA is backed up daily to ZFS using RMAN.

3. A daily snap shot of OVS VMs are stored in a separate storage area in the ZFS.

There is also an AD/DNS at the PMO that gets backed up daily to a local NAS. There may be cause to move them to the PCS later, but for now the AD/DNS will reside at the PMO.

The architecture for other backup is shown in the figure below.

# Other Backup Today

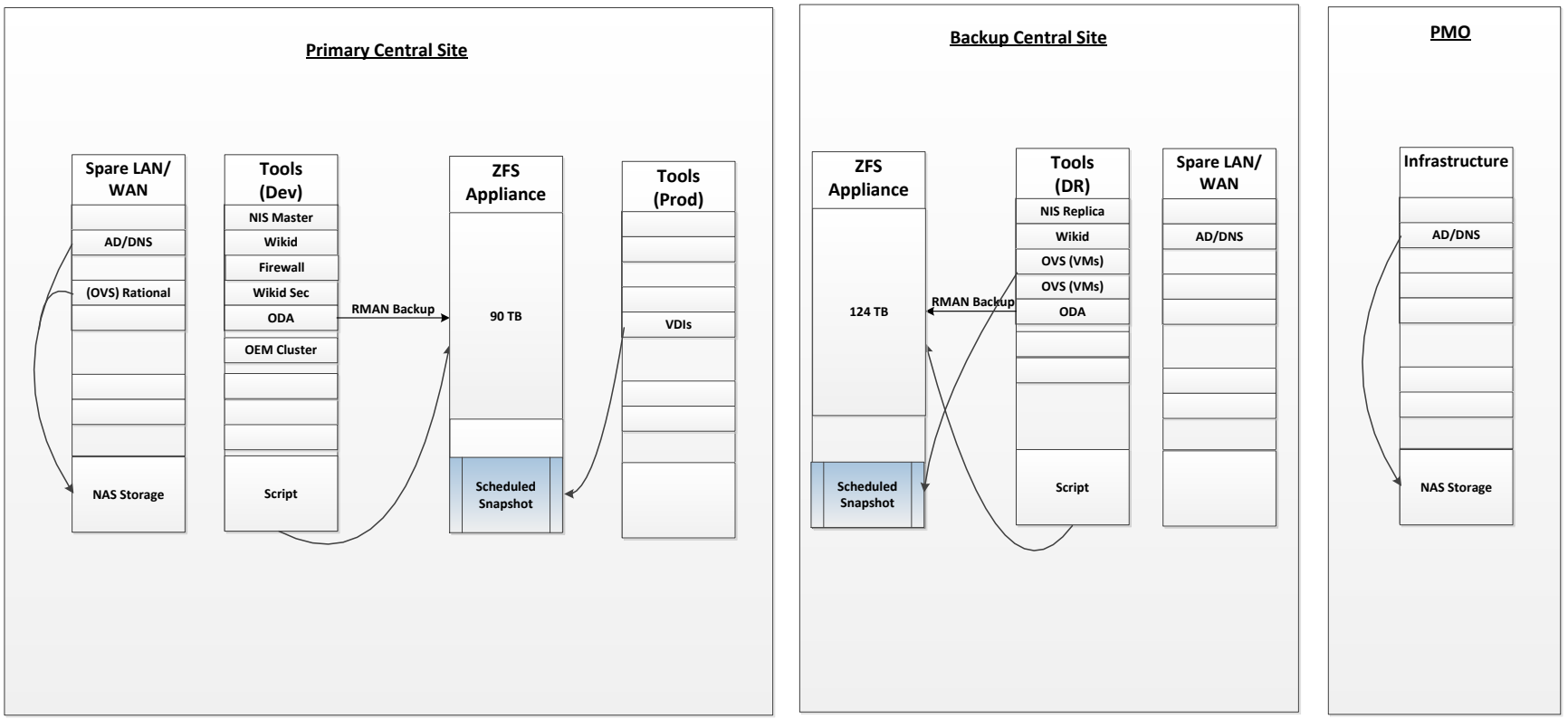


**Figure 5 Current Backup Architecture for Physical Servers and VDIs**

### 7.2. **RESTORATION**

Complete restorations for VDIs have already been successfully performed.

Restoration of physical servers will be time consuming, as each system will need to be re-installed and re-configured prior to restoring the important files from backup.

Only the components attached to the ZFS appliance can be restored automatically. All other environments require manual restoration.

### 7.3. **FUTURE SITUATION**

It is desired that all of the various backup mechanisms currently in place be replaced by an enterprise storage solution. The proposed future architecture for other backup is shown below.

## Other Backup Future

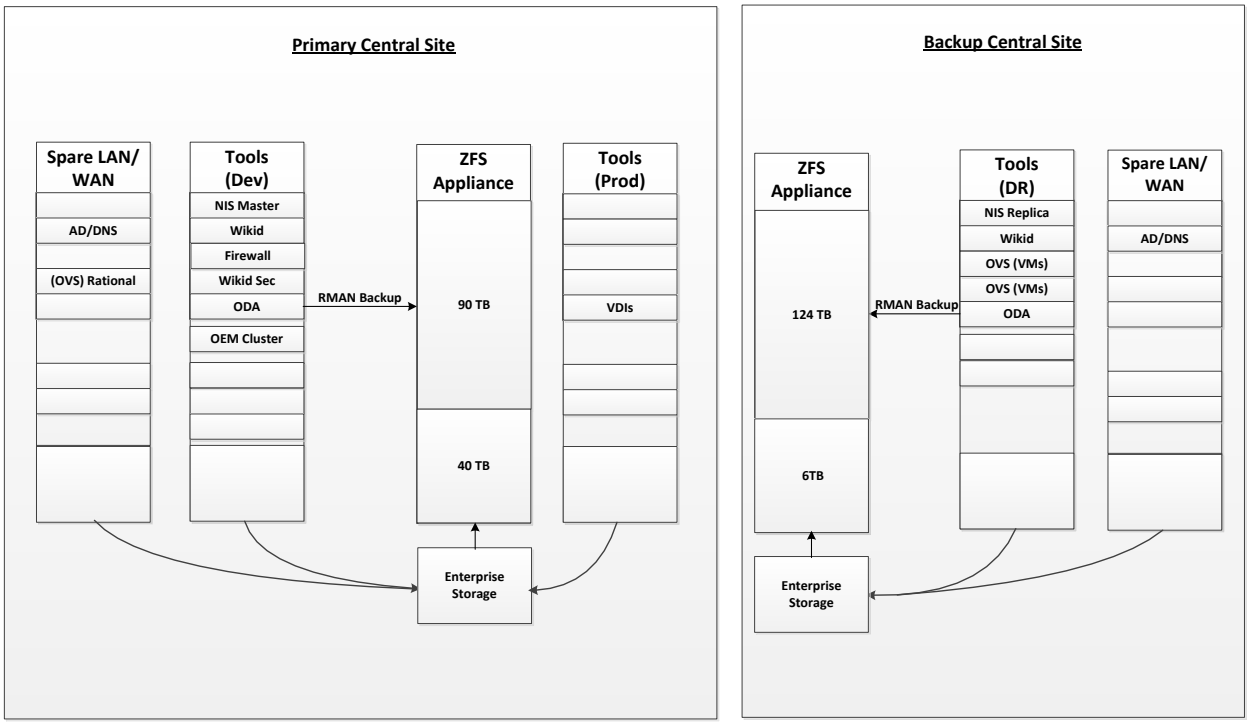


**Figure 6 Future Proposed Backup Architecture for Physical Servers and VDIs**

### 7.4. **CHALLENGES/GAPS**

a. There is no off-site backup of physical servers and VDIs today. The company recommends an enterprise storage solution and the implementation of the off-site replication. It is further recommended that there be replication between data centers and also backups be replicated to a 3rd party site. This will simulate the original design with tapes and off-site storage.

b. There are several physical servers spread across the various tools racks that are not backed up today (see Section 9, Servers Currently Not Backed Up). Licenses and hardware would need to be purchased to accommodate these using an enterprise solution.

c. A separate storage area has been carved out of the ZFS for snap shots of the Production VDIs. This set-aside storage subtracts from the overall storage available on the ZFS for storing everything else, which impacts how quickly it gets filled up. Our recommendation is to implement the VDI environment on a storage device allocated for NFS, and not to use the "backup to disk" device.

d. The time consuming restoration of physical servers could also be mitigated with the enterprise storage solution. The actual amount of time to restore can fluctuate greatly depending on different scenarios. Overall it is estimated that a failed server could be restored 80% faster using an enterprise solution.

e. Storage should be made available at the BCS in the Spare LAN/WAN rack for backup purposes.

f. The company does not understand how a snapshot backup is going to be used to re-image a Windows OS and application binaries. Enterprise class data protection solutions have special "bare-metal" utilities that perform this task. It will probably require a lot of scripting and special purpose work to enable the snapshot solution to support this requirement.

### 7.5. SUMMARY

Because it is not part of the Technical Infrastructure, the customer did not think that an enterprise backup solution was necessary for backing up physical servers and Windows-based tools.

The customer acknowledged that the ZFS appliance will continue to be used to backup of VDIs, and that the additional ZFS storage required because of this allocation will be dealt with by adding more storage capacity.

## 8. DOCUMENTATION AND VALIDATION

The following table details the status, as of the date on the cover, of the documentation for, and the validation of, the procedures for backing up and restoring the various items in the Technical Infrastructure. A link in a cell means a document for that procedure exists. Green in a cell means the procedure for that backup has been validated. When a green cell appears without a link, it means that an ad hoc procedure was used and that it was never documented.

| To Be Backed Up | Local Backup | Offsite Replication/Sync | Local Restoration | Offsite Restoration |
|---|---|---|---|---|
| Data | Data Guard (via RMAN) | Data Guard | DB Recovery | |
| vServers | ITOM-WI-001 | | | |
| VDIs | Manually Creating Snapshots | | | |
| Network equipment | ITOM-PS-002, ITOM-PD-003 | | ITOM-PD-003 | |
| Linux physical servers | | . | | |
| Windows physical servers | ITOM-WI-003 | ITOM-WI-004 | | |

**Table 2 Documentation and Validation**

## 9. BEST PRACTICES

The term "snapshot", as used by Oracle, has multiple meanings. When referring to a snapshot on disk, they are speaking of a conventional snapshot which consists of a file that contains a table of pointers. It has no real data, it is a file of metadata. When they talk about taking them to tape, they are referring to a "clone" or "business continuity volume," which is a bit-for-bit copy created by reading (and writing) the snapshot's source file system blocks, and not writing the snapshot table (or metadata) as it exists on disk. It should be relatively clear that storing a copy of snapshot metadata (without also copying the source file system) does precisely nothing in terms of providing a means of system recovery. Again, the "copy to tape operation" doesn't copy the snapshot to tape, it reads the local snapshot metadata, and writes the content of the source file system blocks to tape, effectively creating a clone.

Assuming the system is running 11G (although most concepts also apply to 12C), the relevant reference can be found here:

http://docs.oracle.com/cd/E11882_01/server.112/e10803/config_backuprec.htm#HABPT4929

Please note the guidance as to which method is appropriate for which business requirement in table 8.1. Of particular interest is their statement that neither ACFS nor ZFS snapshots are appropriate for database DR, backup and restore.

It's also important to understand that for Oracle (or for any RDBMS) there are in fact two things that need to be backed up; the system/server itself (aka the Operating System Environment, aka System State) and the database. Generally speaking, past practice was to back up (using RMAN) to a file system owned by the server or cluster, and then back up the system which would include a copy of the database and transaction logs in a known ACID state.

Current backup agents (e.g. NetBackup, Legato, Tivoli, etc.) include RMAN API integration which allows the Oracle DBA to back up the database directly to the backup application's media (e.g. disk, tape, etc.), eliminating the need to first write the DB backup to system disk.

The last key point to keep in mind is that generally speaking, snapshots are not application aware. Some methods do integrate with the application API and will quiesce the system and force the write cache to flush, but not all. So a snapshot, while great for preserving a file system's state at a specific point in time, is generally not regarded as a valid system backup. The primary exception (assuming API integration) is a VM, but the caveat of the source file system must be viable for the snapshot to be viable remains.

## 10. ENTERPRISE BACKUP RECOMMENDATION

Below is a table that details the options for an enterprise backup solution.

| Manufacturer | Product | HW/SW | Experience | Backs Up Everything? |
|---|---|---|---|---|
| Veritas (Symantec) | NetBackup 7.7 | Software | Yes | Yes |
| Veritas (Symantec) | 5300 Series | Appliance | Yes | Yes |
| IBM (TSM) | Spectrum Protect | Software | Yes | Yes |
| Acronis | Backup Advanced Suite | Software | No | Yes |
| EMC | Data Protection Suite | Software | Yes | Yes |

**Table 3 Enterprise Backup Solution Recommendations**

The solution Oracle recommends is by *Acronis*. Additional details about that solution can be found at: http://www.oracle.com/technetwork/server-storage/vm/ovm3-backup-recovery-1997244.pdf.

When implemented, this solution will perform all of the backups of non-engineered systems and the AD/DNS on the local ZFS appliance.

## 11. RETENTION PERIODS

The table below details the currently implemented retention periods.

| | Daily | Weekly | Monthly | Quarterly | Yearly |
|---|---|---|---|---|---|
| **Requirements** | **14 days** | **6 weeks** | **4 months** | **4 quarters** | **7 years** |
| Data (Exadata) | 6 days | 3 weeks | 1 month | | |
| vServers (Exalogic) | 6 days | 2 weeks | 1 month | | |
| Network | Until disk full | | | | |
| AD/DNS/Rational | 1 day | | | | |
| Tools | 6 days | 3 weeks | 1 month | | |

**Table 4 Current Retention Periods**

### 11.1. CHALLENGES/GAPS

The one day AD/DNS backup is a risk. Corruption must be caught within 24 hours and the backup system halted until the failed system can be restored. Should the file(s) get corrupted and not caught within 24 hours, the result is a complete loss of a usable backup. There will be nothing to restore from. This issue can be resolved with the recommended enterprise solution.

None of the retention periods above meet the requirements.

### 11.2. SUMMARY

The issue regarding the risky 1-day backup of AD/DNS was left unresolved.

## 12. SERVERS CURRENTLY NOT BACKED UP

The physical servers shown below, that are not currently backed up, fall into one of two categories:

1. Generic: servers such as a VDI OVS, have no specific configuration that would need to be backed up. If the server was completely lost, it could be replaced with another box running generic software and would not need to be restored from backup.

2. Not Backed Up: servers which are not generic, but are not being backed up by any solution.

| Server Name | Purpose | Environment |
|---|---|---|
| | RUEI - Data Collector 1 | PCS Development |
| | RUEI - Data Collector 1 | PCS Development |
| | OVS (3) | PCS Development |
| | OVS (4) | PCS Development |
| | DMZ UAT OVS | PCS Development |
| | OVS (11) | PCS Development |
| | OVS (12) | PCS Development |
| | OVS (13) | PCS Development |
| | OVS (14) | PCS Development |
| | OVS (15) | PCS Development |
| | OVS (16) | PCS Development |
| | OVS (17) | PCS Development |
| | OVS (18) | PCS Development |
| | OVS (19) | PCS Development |
| | OVS (20) | PCS Development |
| | Conversion Server | PCS Development |
| | ODA Head 1 | PCS Development |
| | ODA Head 2 | PCS Development |
| | DEV- Sun X3-2 Batch Processing 1 | PCS Development |
| | DEV- Sun X3-2 Batch Processing 2 | PCS Development |
| | DEV- Sun X3-2 Batch Processing 3 | PCS Development |
| | DR - Sun X4-2 Batch Processing 4 | BCS DR |
| | DR - Sun X4-2 Batch Processing 3 | BCS DR |
| | DR - OVS (3) [DMZ] | BCS DR |
| | DR - Sun X4-2 Batch Processing 2 | BCS DR |
| | DR - Sun X4-2 Batch Processing 1 | BCS DR |
| | DMZ OVS | BCS DR |
| | DR - Database Firewall 1 | BCS DR |
| | ODA Head 2 | BCS DR |
| | ODA Head 1 | BCS DR |

**Table 5 Physical Servers Not Currently Backed Up**

## 13. SIGNATURES

| | DOCUMENT APPROVAL HISTORY | |
|---|---|---|
| | Prepared By | Carl Weisman |
| | Reviewed By | |
| | Approved By | |

| APPROVAL DATE | APPROVED VERSION | APPROVER |
|---|---|---|
| | | |