# Backup Solution Testing on UCS for Small-Medium Range Customers (Disk to Tape) – Acronis Advanced Backup Software

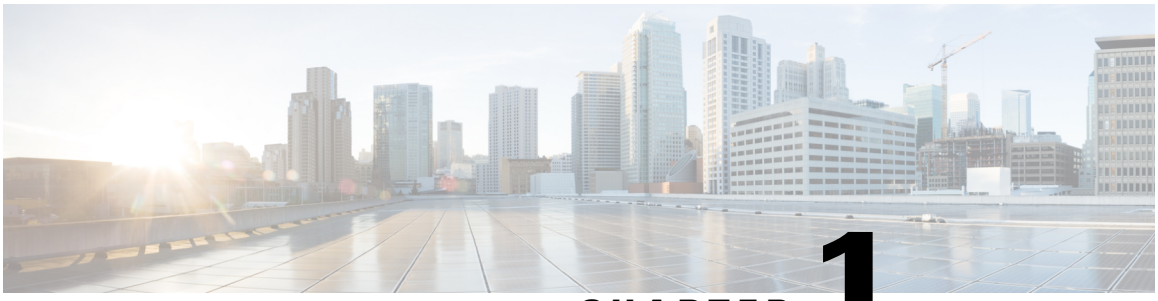
**First Published:** April 28, 2014

**Last Modified:** May 06, 2014

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-32151-01

# CONTENTS



CHAPTER 1

# Backup Solution Testing



## Overview

This program (Backup Testing - Backup to Disk and Replicate to Tape) validates data backup from the Windows and Linux operating systems on the Cisco UCS environment and the backup data stored in the Quantum LTO-5 Drives. The objective of Backup Testing is to verify the Backup and Restore of Data/Database, Entire Disks of Windows/Linux, Full Virtual machines, UCS Central applications by the backup software (Acronis Backup Software Advanced Edition) with the data repository models, which are covered in the Feature Tested section.

### Acronyms

| Acronym | Description |
|---|---|
| 10GbE | 10 Gigabit Ethernet |
| CIMC | Cisco Integrated Management Controller |
| CNA | Converged Network Adapter |
| DB | Database |
| HDD | Hard Disk Drive |
| JOS | Japanese Operating System |
| MS | Microsoft |
| OS | Operating System |
| PCI | Peripheral Component Interconnect |
| RAID | Redundant Array of Independent Disks |
| RHEL | Red Hat Enterprise Linux |

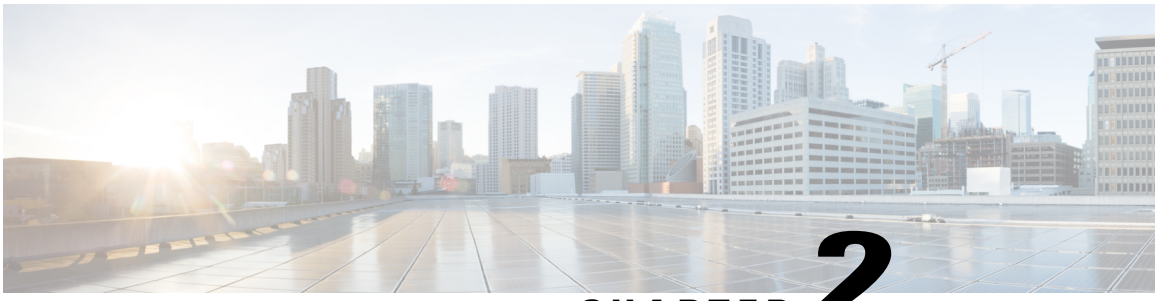
| Acronym | Description |
|---|---|
| SQL | Structured Query Language |
| UCS | Unified Computing System |
| VIC | Virtual Interface Card |
| VM | Virtual Machine |

# Backup Testing Strategy

The requirements gathered for Backup Testing (Backup to Disk and Replicate to Tape) are specific to the Japanese usage and market.

The following requirements are derived based on the inputs and prioritization given by Cisco Japan Solution Engineers:

- Virtual Machines are available on ESXi 5.5, which is installed in the Cisco UCS C Series Servers
  - Japanese Windows Server 2012 R2 installed directly on the Cisco UCS C Series Server for Disaster Recovery
  - Japanese RHEL 6.2 (x64 ) installed directly on the Cisco UCS C Series Server for Disaster Recovery
- Acronis Backup & Recovery 11.5 Advanced Version is used as Backup software.
- Acronis Backup & Recovery 11.5 Advanced Version installed on top of the WindowsServer2012R2 Japanese Operating System, which is installed on the local HDD of C Series Server. The Server Also Acts as AMS (Acronis Management System)
- Backup server is connected to Quantum LTO-5 Superloader 3 Drive by SAS connectivity using LSI 9286 CV-8e MegaRAID Controller Card .
- The internal RAID controller used on Cisco UCS C Series Server is LSI 9271 MegaRAID Controller Card.
- Backup data is stored in C Series Server local disk and then Replicated to Quantum LTO-5 Superloader 3 Drive using Acronis Backup & Recovery 11.5 .
- Backup the Full Virtual Machines from the ESXi 5.5 Server which is installed on UCS C Series server. Virtual Machines are installed with Windows Server or Linux Operating System.
- Data backup from the Windows 7 and RHEL 6.2 Japanese Operating Systems that are installed as Virtual machines. Data files include Microsoft Excel, Microsoft Word and PDF.
- Database backup from MSSQL Server2012 on the Windows Server 2012 R2 Japanese Operating System that is installed as a Virtual Machine.
- Select files from Windows or Linux operating system and schedule a backup job from AMS (Acronis Management Server ) to the managed Backup server.
- Backup of UCS Central, which is deployed as Virtual Machine on UCS C Series server.

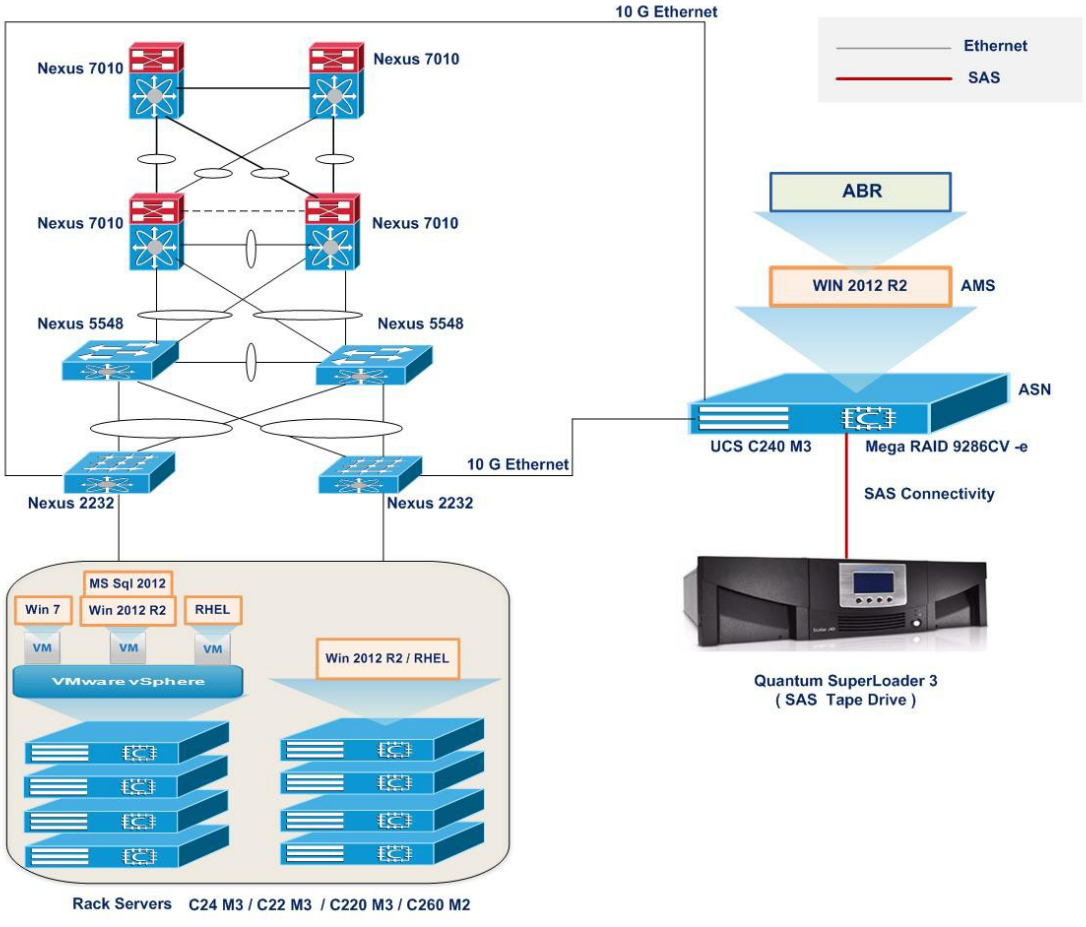


CHAPTER 2

# Test Topology and Environment Matrix

# Test Topology

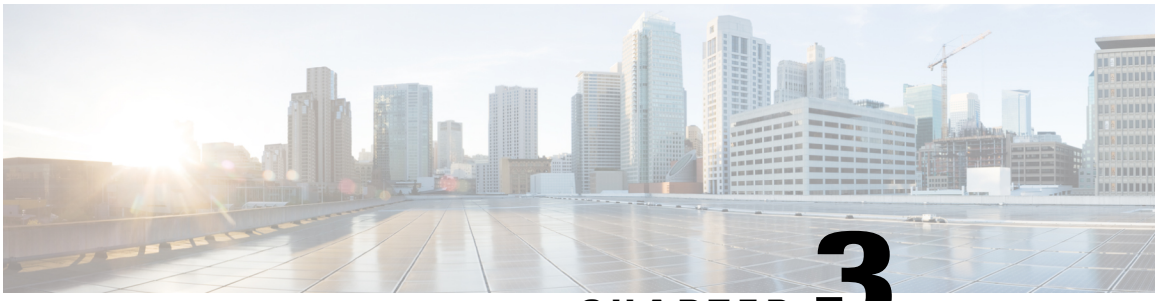
*Figure 1: Topology in Use*




# Environment Matrix

| Component | Version |
|---|---|
| **UCS** | |
| 1. Rack Servers | C240 M3, C220 M3, C24 M3, C260 M2 |
| 2. C Series Server CIMC | 1.5(4) 3 |
| **Infra** | |
| 1.Nexus 2232PP | 5.2(1)N1(6) |

| Component | Version |
|---|---|
| 2. Nexus 5548UP | 5.2(1)N1(6) |
| 3. Nexus 7010 | 6.2(2) |
| **Backup Software** | |
| Acronis Backup & Recovery | 11.5 |
| **Operating Systems** | |
| 1. Windows Server | Windows Server 2012 R2 x64 (Japanese) |
| 2. Windows OS | Windows 7 Enterprise SP1 x64 (Japanese) |
| 3. RHEL | Redhat Enterprise Linux 6.2 x64 (Japanese) |
| **Data Base** | |
| MS SQL server | Microsoft SQL Server 2012 R2 Enterprise x64 (Japanese) |
| **Hypervisor** | |
| ESXi | VMware ESXi 5.5 1331820 |
| **Tape Library** | |
| Quantum LTO-5 Superloader | V86.0 (0056.0h) |
| **PCI Adapter** | |
| Cisco P81E VIC | 1.5(4) 3 |



CHAPTER 3

# Implementation and Features Tested



## Design and Implementation

This program verifies and validates the functionality of Acronis Backup & Recovery 11.5 features on Cisco UCS Servers for Japanese environment.

Backup Server components (Server and Client) are installed on JOS and schedule backup from Cisco UCS C Series Server to the C Series Server.

The following activities were involved in the Implementation phase:

- Installed VMware ESXi 5.5 on the UCS C Series Servers that are configured to boot from Local HDD.
- Installed the Windows Server 2012 R2 Japanese operating system in the C Series Server on a Local HDD that is configured with RAID 5 (single parity). This C Series Server acts as a Backup Server and AMS (Acronis Management System), which is the Centralized Management console for taking the Backup and Restore of machines.
- In the C Series Server installed with ESXi 5.5, three virtual machines were created and installed with the following Japanese Operating Systems respectively:
  - Windows 7 Enterprise SP1 x64
  - Windows Server 2012 R2 x64
  - Redhat Enterprise Linux 6.2 x64
- 10 GbE connectivity established between C Series Server ( Cisco P81E VIC ) and Other C Series Server for backup data Read/Write operations through Nexus 7k.
- SAS connectivity between Backup Servers and Quantum Superloader using LSI 9286CV-8e MegaRAID Controller Card
- C Series Server installed with Windows Server 2012 R2 x64 Japanese Operating System and

  Acronis Backup & Recovery 11.5 Advanced Version installed on top of Japanese Operating System.

- Acronis Backup & Recovery 11.5 Agent for Core, Agent for Windows, Agent for Management Console are Installed on the Windows 7 and Windows 2012 Virtual Machines.
- Acronis Backup & Recovery 11.5 Agent is also installed on RHEL 6.2 Virtual Machines by installing the Required Packages such as (kernel, kernel-devel, and GCC ).
- Acronis Backup & Recovery 11.5 Agent for SQL is also installed on Top of the Windows Server 2012 Virtual Machine, and by adding the Required Privilege to the Acronis Agent
- Acronis Backup & Recovery 11.5 Agent for VMware vSphere ESXi enables backup and recovery of ESXi virtual machines without installing agents into the guest systems. The Agent for VMware vSPhere ESXi (Virtual Appliance ) is deployed directly to the VMware ESXi host.
- Cisco UCS Central is deployed as Virtual Machine on VMware ESXi 5.1, where backup of UCS Central is performed from the Acronis Backup & Recovery 11.5 and is able to restore the UCS Central at the active stage

# Features Tested

Data Backup was tested with the following backup methods:

### Full Backup

Full backup is the starting point for all other types of backup and contains all the data in the folders and files that are selected to be backed up. Because full backup stores all files and folders, frequent full backups resulting faster and simpler restore operations.

### Differential Backup

Differential backup contains all files that have changed since the last FULL backup. The advantage of a Differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if you perform the differential backup too many times, the size of the differential backup might grow to be larger than the baseline full backup.

### Incremental Backup

Incremental backup stores all files that have changed since the last FULL, DIFFERENTIAL, or INCREMENTAL backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup must be processed, which could result in a lengthy restore job.

### Archive protection

This option defines whether the archive will be protected with a password and whether the archive's content will be encrypted. This option is effective for both Windows and Linux Operating System

**Do not encrypt** - the archive will be protected with the password only

**AES 128** - the archive will be encrypted using the Advanced Encryption Standard (AES) algorithm with a 128-bit key

**AES 192** - the archive will be encrypted using the AES algorithm with a 192-bit key

**AES 256** - the archive will be encrypted using the AES algorithm with a 256-bit key.

The larger the key size, the longer it will take for the program to encrypt the archive and the more secure data will be. The encryption key is then encrypted with AES-256 using a SHA-256 hash of the password as a key. The password itself is not stored anywhere on the disk or in the backup file; the password hash is used for verification purposes. With this two-level security, the backup data is protected from any unauthorized access, but recovering a lost password is not possible.

### Backup priority

The Following Priority are mentioned while creating the Backup Plan

- **Low** - to minimize resources taken by the backup process, leaving more resources to other processes running on the machine
- **Normal** - to run the backup process with normal speed, allocating resources on a par with other processes
- **High** - to maximize the backup process speed by taking resources from other processes.

### Compression level

The option defines the level of compression applied to the data being backed up. This applies to both Windows & Linux Operating System. The optimal data compression level depends on the type of data being backed up.

- **None** - the data will be copied as is, without any compression. The resulting backup size will be maximal.
- **Normal** - recommended in most cases.
- **High** - the resulting backup size will typically be less than for the **Normal** level.
- **Maximum** - the data will be compressed as much as possible. The backup duration will be maximal. You may want to select maximum compression when backing up to removable media to reduce the number of blank disks required

### Disaster Recovery Plan

Disaster recovery plan (DRP) contains a list of backed up data items and detailed instructions that guide a user through a process of recovering these items from a backup.

A DRP is created after the first successful backup is performed by the backup plan. If the Send disaster recovery plans option is enabled, the DRP is sent by e-mail to the specified list of users. If the Save DRP as file option is enabled, the DRP is saved as a file to the specified location

If multiple machines are protected by a backup plan, then a separate DRP is created for each machine. You can specify a local folder (when connected directly to a managed machine), a network folder, an FTP or SFTP server as a location to save the DRPs.

### File-level backup snapshot

This option is effective only for file-level backup in Windows and Linux operating systems. This also defines whether to back up files one by one or by taking an instant data snapshot.

The default is Create snapshot if it is possible

- **Always create a snapshot**
  The snapshot enables backing up of all files including files opened for exclusive access. The files will be backed up at the same point in time. Choose this setting only if these factors are critical, that is, backing up files without a snapshot does not make sense. To use a snapshot, the backup plan has to run

under the account with the Administrator or Backup Operator privileges. If a snapshot cannot be taken, the backup will fail.

- **Create a snapshot if it is possible**
  Back up files directly if taking a snapshot is not possible.
- **Do not create a snapshot**
  Always back up files directly. Administrator or Backup Operator privileges are not required. Trying to back up files that are opened for exclusive access will result in a read error. Files in the backup may be not time-consistent.

### Volume Shadow Copy Service

These options are effective only for Windows operating systems.

The option defines whether a Volume Shadow Copy Service (VSS) provider has to notify VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications; in particular, completion of all database transactions at the moment of taking the data snapshot by Acronis Backup & Recovery 11.5.

### Bootable media

Bootable media is physical media (CD, DVD, USB flash drive or other removable media supported by a machine BIOS as a boot device) that boots on any PC-compatible machine and enables you to run Acronis Backup & Recovery 11.5 Agent either in a Linux-based environment or Windows Preinstallation Environment (WinPE), without the help of an operating system. Bootable media is most often used to:

- recover an operating system that cannot start
- access and back up the data that has survived in a corrupted system
- deploy an operating system on bare metal
- create basic or dynamic volumes on bare metal
- back up sector-by-sector a disk with an unsupported file system
- back up offline any data that cannot be backed up online because of restricted access, being permanently locked by the running applications or for any other reason.

### Microsoft SQL Server with single-pass backup

A single-pass backup operation creates an application-aware disk backup which enables browsing and recovery of the backed-up application data without recovering the entire disk or volume. The disk or volume can also be recovered as a whole. This means that a single solution and a single backup plan can be used for both the disaster recovery and data protection purposes. The application logs can be truncated after the backup, if necessary.

The single-pass backup functionality becomes available by installing Acronis Backup & Recovery 11.5 Agent for Microsoft SQL Server (single-pass).

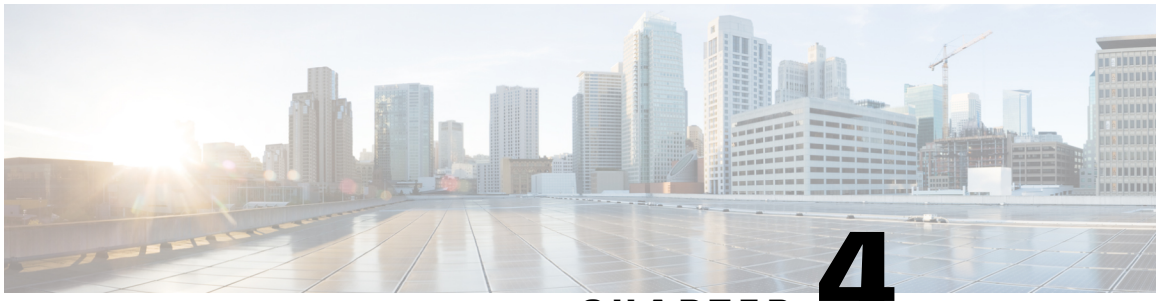
### Virtual Appliance for ESXi Host

Acronis believes that virtualization and transition to the cloud are not only a better way of doing computing, but also allow for achieving less downtimes and faster recoveries while reducing costs.

Acronis is firmly committed to helping its customers and channel partners get most of virtualization, and intend to set a new standard of backup and recovery in virtualized environments through:

- Reducing IT operating and maintenance costs to help business performance by providing technology that is easy to use and easy to implement.
- Minimizing overhead and getting most benefits from VMware vSphere environments by providing a backup and recovery solution specially designed for virtualized environments.
- Minimize risk of data loss by storing backups offsite in Acronis Cloud Storage.

Acronis Backup for VMware software could be installed directly on an ESX(i) host. Specify the desired ESX(i) server or vCenter access credentials. Set your Appliance (VM) name, choose the ESX(i) host and datastore as a target for deploying the Acronis Backup for VMware software.



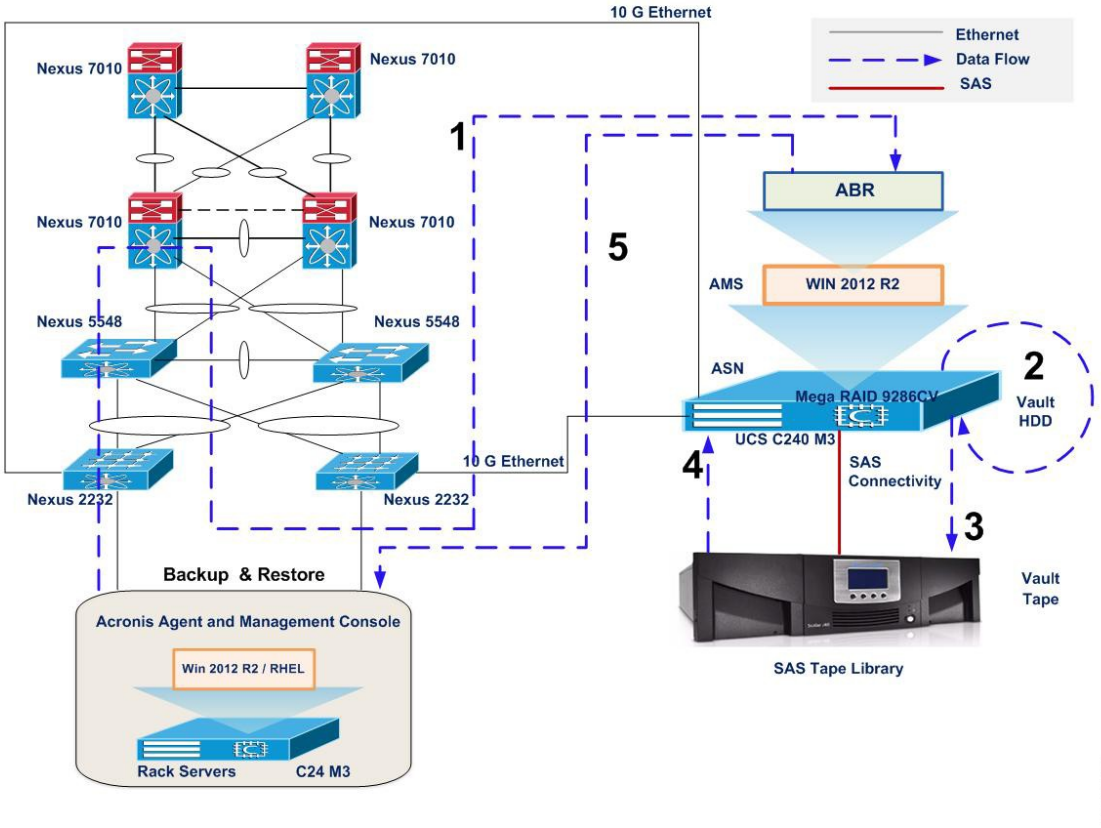
CHAPTER 4

# Test Scenario for UCS with Advanced Acronis 11.5

# Disaster Recovery for Same Hardware

## Backup Entire Disks of C Series Server to Disk and Replicate to Tape

*Figure 2: Topology in Use*




| Backup data flows: | | |
|---|---|---|
| **Step** | **From** | **To** |
| 1 | Backup of C Series Server(Entire Disks) | Backup Server |
| 2 | Backup Server | Local HDD of C Series Server |
| 3 | Local HDD of C Series Server | Quantum SuperLoader 3 |
| 4 | Quantum SuperLoader 3 | Backup Server |
| 5 | Backup Server | Restore of Entire Disks of C Series Server |

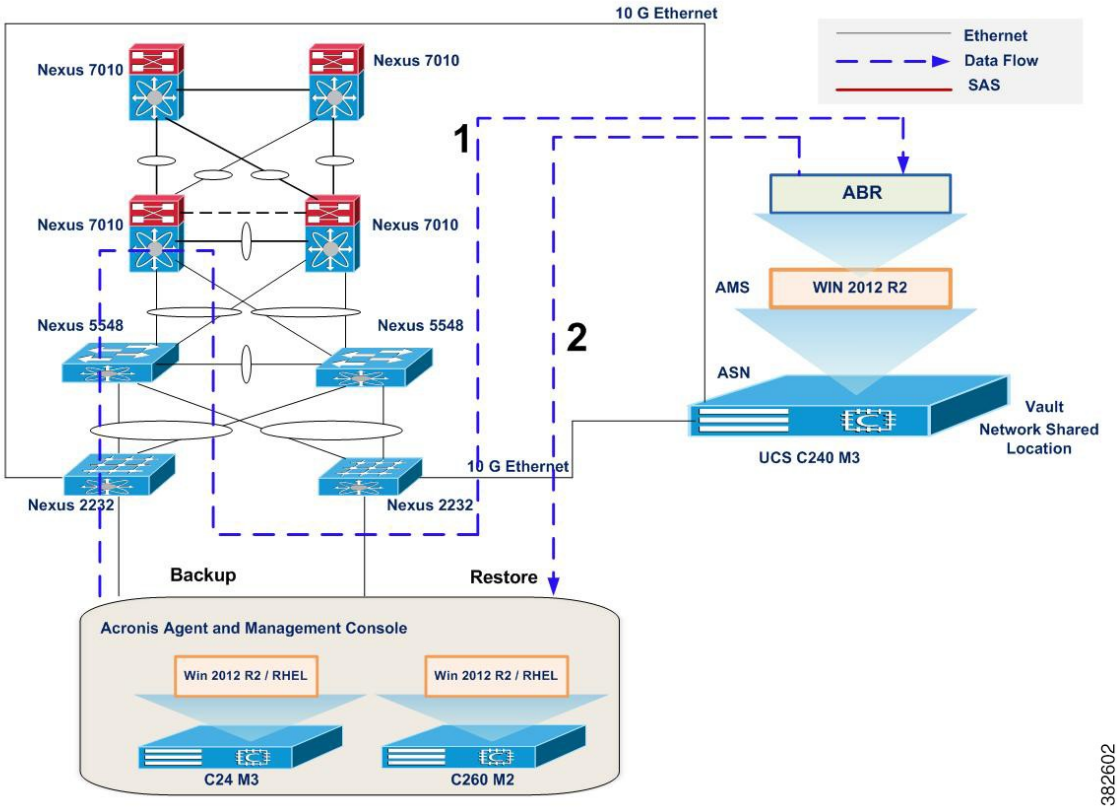
### Description

- Backup of Entire Disks from Windows 2012 R2 Japanese and RHEL 6.2 Japanese Operating System to C Series Server Local HDD and then Replicate the same to Quantum SuperLoader 3 using Acronis Advanced Server 11.5 software.
- Restore the Entire Disks from Disks/Tape to the Same hardware from Acronis Advanced Server 11.5 Recover Option

# Disaster Recovery for Different Hardware

### Backup Entire Disks of C Series Server to Disk and Replicate to Tape

***Figure 3: Topology in Use***



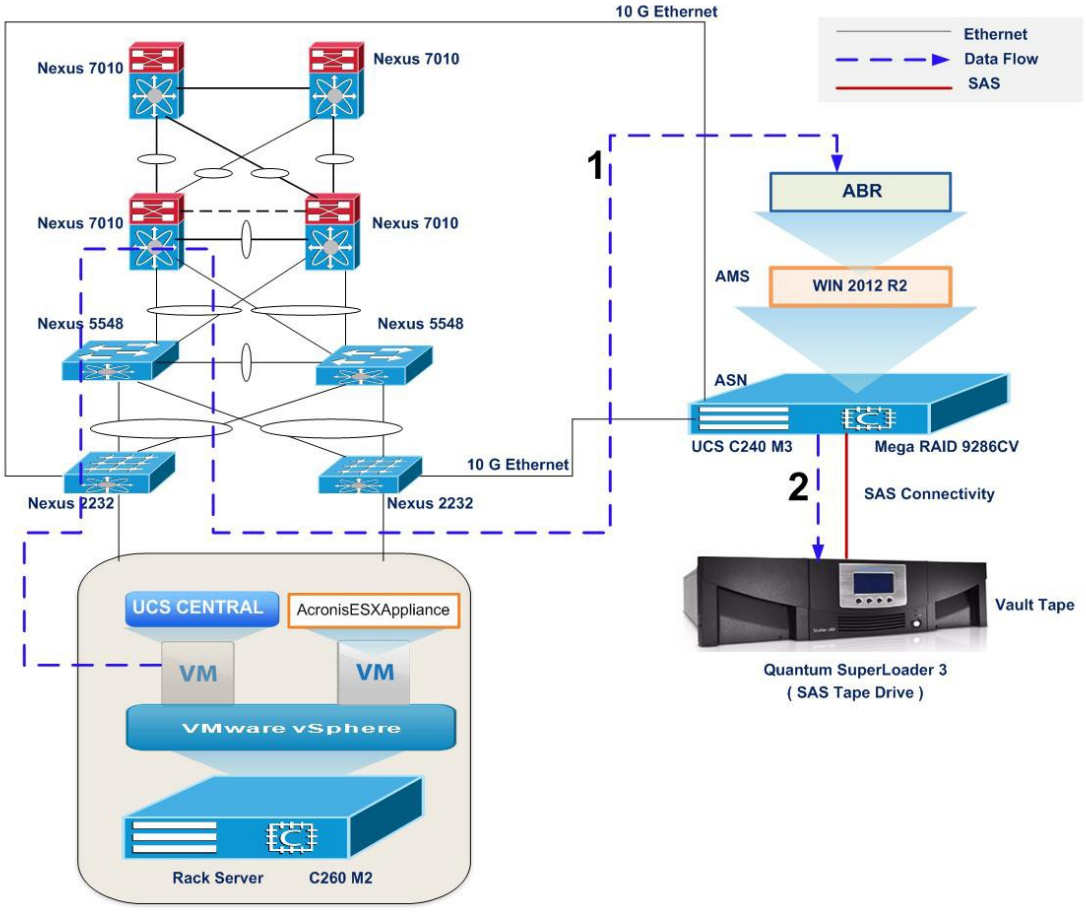

| Backup data flows: | | |
|---|---|---|
| **Step** | **From** | **To** |
| 1 | Backup of C Series Server(Entire Disks) | Network Folder Location |
| 2 | Network Folder Location | Restore of Entire Disks of C Series Server |

**Description**

1. Install the Required Agent and Bootable Media on the Machines to be Backedup.
2. Create the Bootable Media (ISO or CD/DVD) . Boot the Server using the media created (ISO or CD/DVD)
3. Perform Full Backup of Entire Disks and store the Archive to Network Location.
4. Boot the Media Created to the Different Hardware, and select Recover Option.
5. Select the Archive from the Network Location and Apply Raid/LVM to automatically assemble all lvm or raid volumes
6. Once Recover is Completed, Reboot the Server.

# UCS Central Backup

***Figure 4: Topology in Use***




| Backup data flows: | | |
|---|---|---|
| **Step** | **From** | **To** |

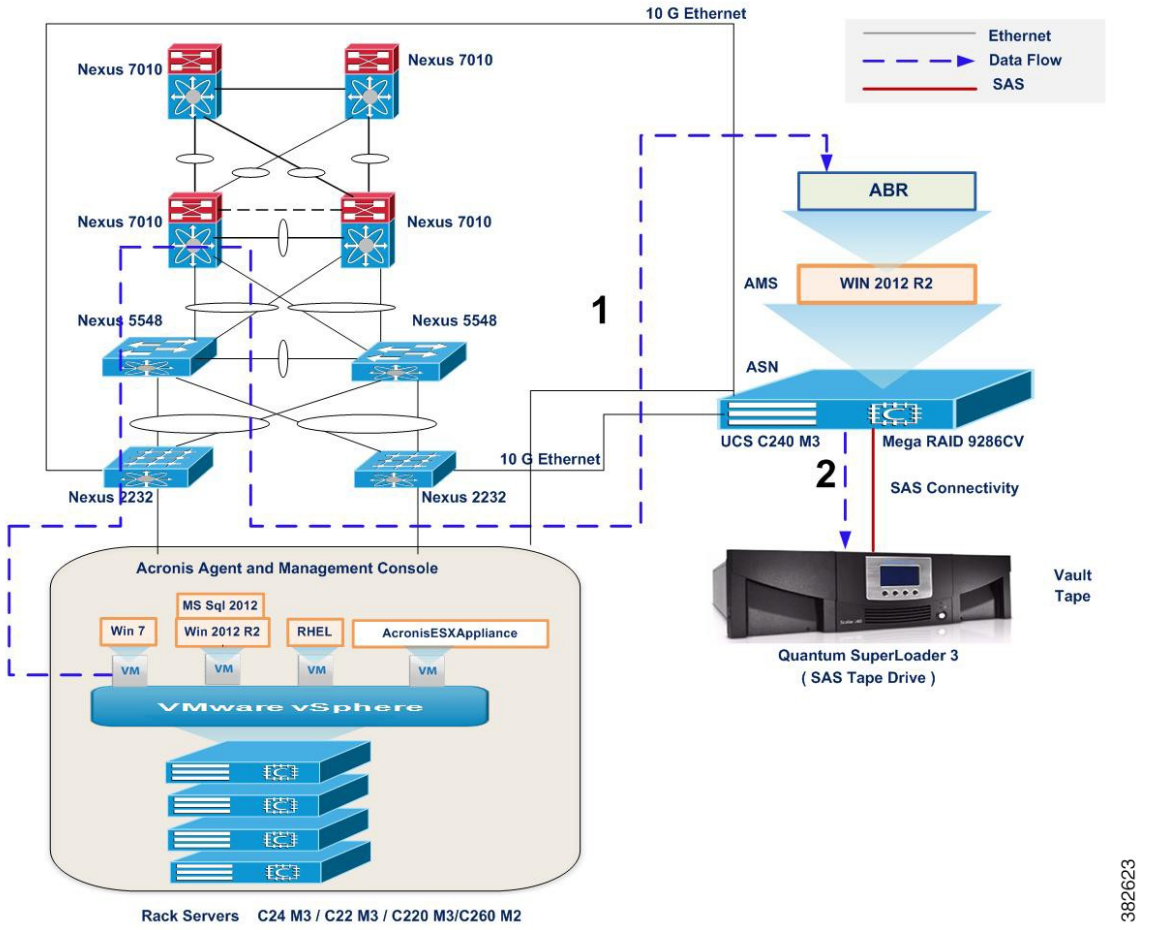
| Backup data flows: | | |
|---|---|---|
| 1 | UCS Central (VM) | Backup Server |
| 2 | Backup Server | Quantum SuperLoader 3 |

**Description**

- **1** · Backup the UCS Central VM from ESXi 5.1 host and restore it to the same ESXi host using Acronis Backup for Virtual Machine .

# VM Backup

***Figure 5: Topology in Use***



| Backup data flows: | | |
|---|---|---|
| **Step** | **From** | **To** |
| 1 | Virtual Machine | Backup Server |
| 2 | Backup Server | Quantum SuperLoader 3 |

**Description**

- Backup any Virtual Machine from ESXi 5.5 host and restore it to the same ESXi host using Acronis Backup for Virtual Machine .

**Issue :**

VM Version Type Changes after restoring the Virtual Machine as New Virtual Machine.

**Description:**

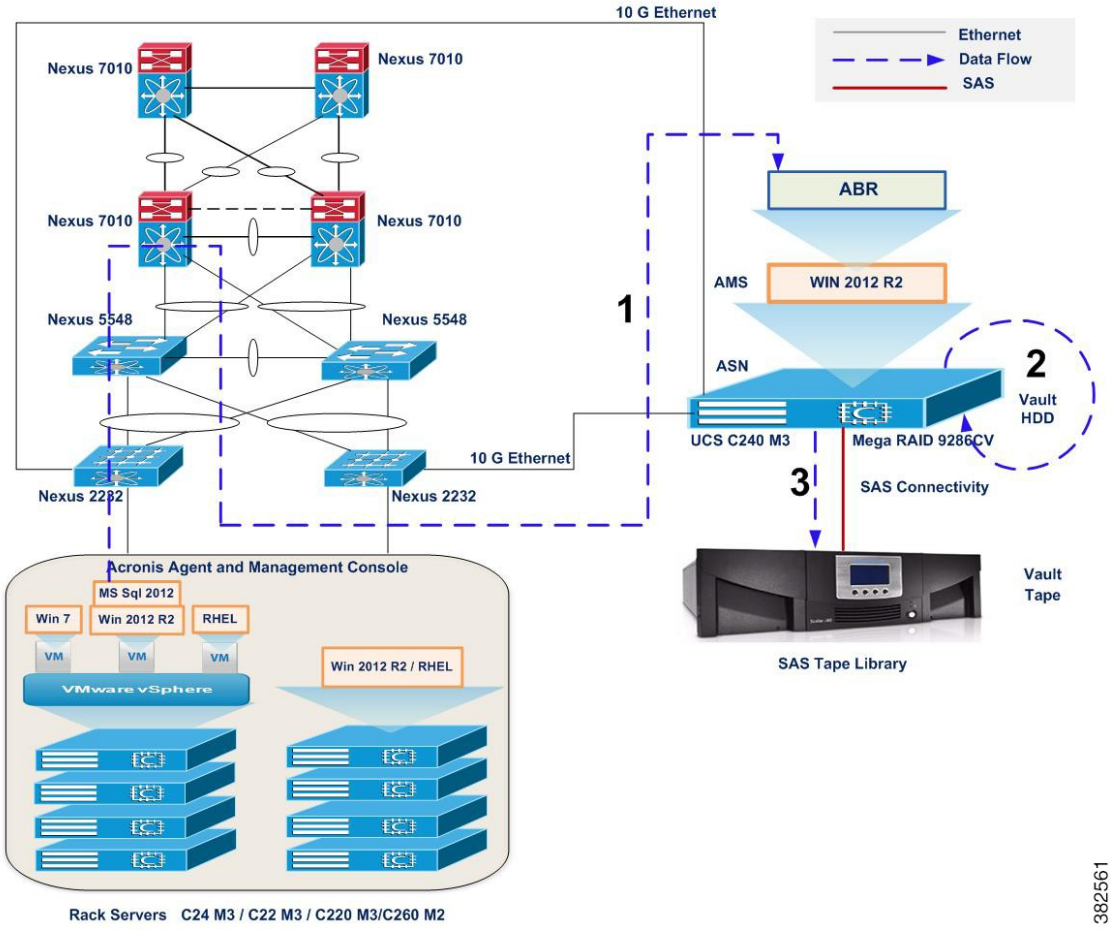
1. Select the Virtual Machine to be Backed up using Acronis Backup and Recovery 11.5 .
2. Run the Backup Job and Backup of Virtual Machine is Successful.
3. Select the Archive and create Recovery Plan.
4. Specify where to recover as " New Virtual Machine " in Recovery Plan.
5. Run the Recovery Job and the Restore of Virtual Machine is successful.
6. Restored Virtual Machine possess different VM Version.

**Workaround :**

Create a New Virtual Machine with the required version and attach the Disk to the newly created virtual Machine.

# SQL Backup

*Figure 6: Topology In Use*



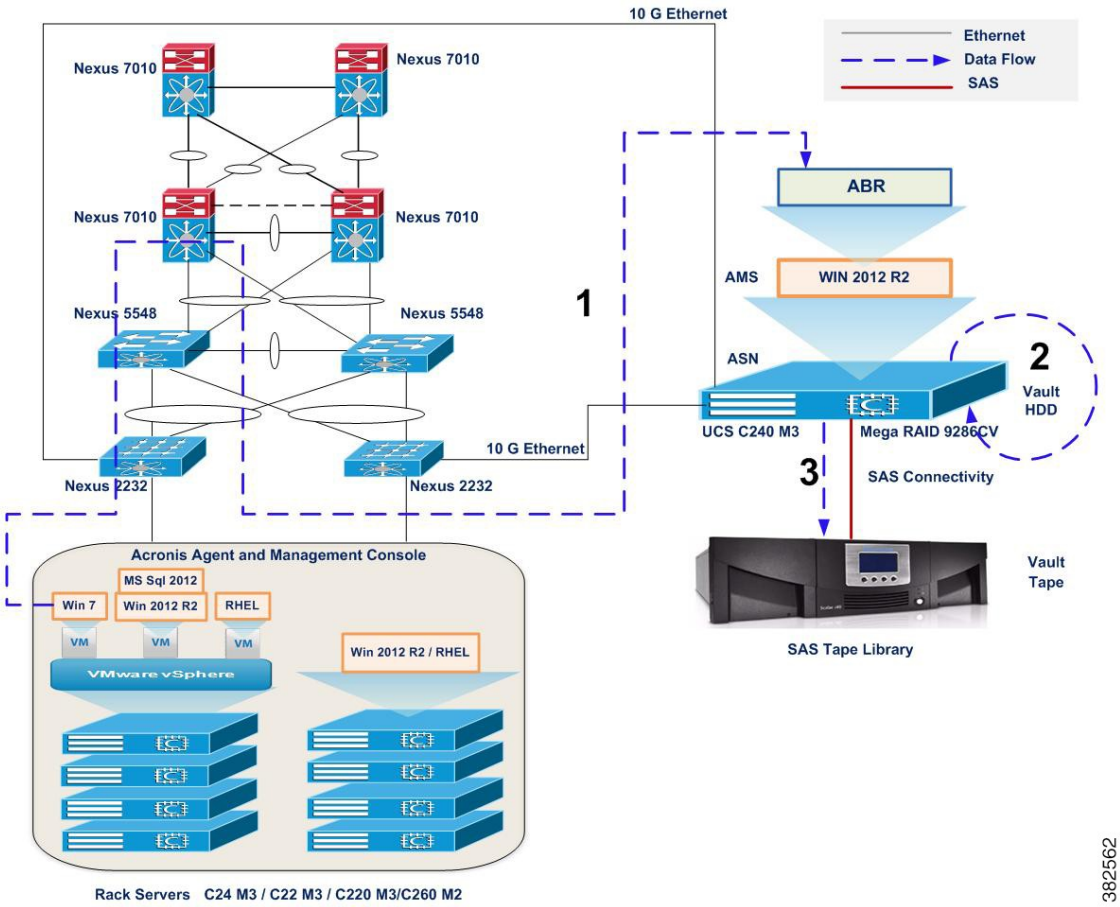

| Backup data flows: | | |
|---|---|---|
| **Step** | **From** | **To** |
| 1 | SQL Backup of C Series Server | C Series Backup Server |
| 2 | C Series Backup Server | Local HDD of C Series Server |
| 3 | Local HDD of C Series Server | Quantum SuperLoader 3 |
| 4 | Quantum SuperLoader 3 | C Series Backup Server |

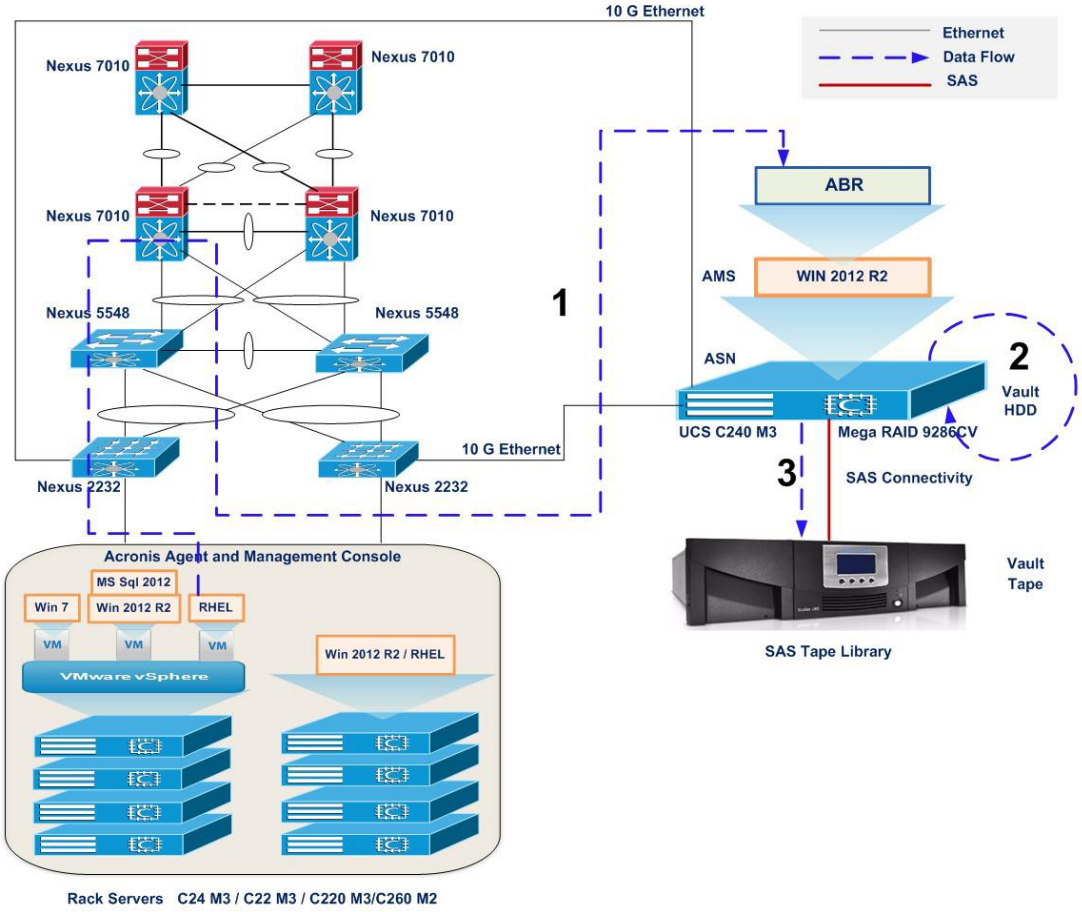
- Backup SQL Database using Acronis Single-Pass Backup for taking the Database on Windows Server 2012 R2 to C Series Server Local HDD and then Replicate the Database to Quantum SuperLoader 3

- Recover the Database either from Local HDD or Quantum SuperLoader 3 by using various Recover Option available on Acronis Advanced 11.5

# Windows File / Folders Backup

*Figure 7: Topology in Use*






| Backup data flows: | | |
|---|---|---|
| **Step** | **From** | **To** |
| 1 | Backup of C Series Server (Files & Folders) | Backup Server |
| 2 | Backup Server | Local HDD of C Series Server |
| 3 | Local HDD of C Series Server | Quantum SuperLoader 3 |
| 4 | Quantum SuperLoader 3 | Backup Server |
| 5 | Backup Server | Restore of Files/Folders of C Series Server |

### Description

- Backup of data files (Word,PDF, and Excel) from Windows7 and RHEL 6.2 Japanese Operating System to C Series Server Local HDD and then Replicate the same to Quantum SuperLoader 3 using Acronis Advanced Server 11.5 software.

- Recover the Files either from Local HDD or Quantum SuperLoader 3 by using various Recover Option available on Acronis Advanced 11.5

# Related Documentation

### Cisco Servers -Unified Computing

http://www.cisco.com/en/US/products/ps10265/index.htmhttp://www.cisco.com/en/US/products/ps10265/index.html

### LSI MegaRAID SAS 9286-8e

http://www.lsi.com/products/storagecomponents/Pages/MegaRAIDSAS9286-8e.aspx

### Acronis Backup & Recovery 11.5 Advanced Version for Windows

http://www.acronis.com/en-us/business/backup-advanced/windows-server/

### Acronis Backup & Recovery 11.5 Advanced Version for Linux

http://www.acronis.com/en-us/business/backup-advanced/linux-server/

### Acronis Backup & Recovery 11.5 Advanced Version for VMware

http://www.acronis.com/en-us/business/backup-advanced/vmware/