ılıılı cısco

Deployment Guide

Microsoft SQL Server 2012 Failover Cluster on Bare-Metal Microsoft Windows 2008 with Cisco UCS iSCSI-Based Storage Access: Deployment Guide



Contents

Executive Summary	3
Introduction	3
Small Computer Systems Interface over IP	3
Audience	4
Hardware and Software Requirements	4
Cisco Unified Computing System Overview Cisco Unified Computing System Components Microsoft Windows 2008 R2 SP1 Overview Microsoft SQL Server 2012 Overview	5 9 0 3
Design Topology1	5
Cisco UCS and iSCSI Storage Network	6 8
Microsoft Windows iSCSI Boot	0
Microsoft Windows iSCSI Solution Overview	
Microsoft SQL Server Failover Cluster Solution4	4
Physical and Logical Design 4 Installation of Microsoft Windows 2008 Failover Cluster Feature with iSCSI Software Initiator 4 Installation of Microsoft SQL Server 2012 Failover Cluster Feature with iSCSI Storage 5	-7
Conclusion	67
For More Information	67

Executive Summary

The document describes Microsoft SQL Server 2012 failover cluster deployment in the Cisco Unified Computing System[™] (Cisco UCS[®]) using the Small Computer System Interface over IP (iSCSI) protocol to communicate with storage devices. The document describes how to deploy a Microsoft SQL Server 2012 failover cluster on baremetal Microsoft Windows 2008 Release 2 (R2) with Service Pack 1 (SP1) with Cisco UCS iSCSI-based storage access. The deployment scenarios discussed in this document follow the Cisco UCS best practices and recommendations to help ensure that the systems are highly available and scalable and can be efficiently consolidated and centrally managed.

Introduction

A Microsoft SQL Server 2012 database on iSCSI storage offers a cost-effective solution for enterprise-level database deployments. An inexpensive yet reliable and robust storage solution, iSCSI-based storage appliances easily adapt to existing networking infrastructure for storage enclosure access. Cisco UCS can exploit the bandwidth available to provide scalable, enterprise-class storage access through the iSCSI protocol. Cisco UCS provides up to 80 Gbps of unified bandwidth for disk and network access for a single Cisco UCS 5108 Blade Server Chassis.

High availability is one of the primary requirements for enterprise-level database platforms because missioncritical applications cannot afford any downtime caused by unavailable databases at the network back end. Microsoft SQL Server 2012 integrates with the new Microsoft Windows 2008 failover cluster service to offer failover clustering, providing high availability for the database applications. Coupled with iSCSI storage at the system level, a clustering-enabled Microsoft SQL Server deployed on the Cisco UCS platform provides a complete back-end solution with optimal total cost of ownership (TCO) and high return on investment (ROI).

Small Computer Systems Interface over IP

Small Computer Systems Interface (SCSI) is a standard client-server protocol that is used to enable computers to communicate with storage devices. The iSCSI protocol transfers the SCSI packets over a TCP/IP (Ethernet) network. The most common implementation of iSCSI is over 1 or 10 Gigabit Ethernet. The iSCSI protocol provides an interoperable solution that uses the existing TCP/IP infrastructure to transport block-level storage requests. Using the iSCSI protocol, systems can connect to remote storage and use it as a physical disk even if the remote storage provider (target) actually uses virtual physical disks.

An iSCSI SAN typically consists of software or hardware initiators on the host connected to an isolated Ethernet network and storage resources. The storage resources are referred to as targets. The SCSI block commands are encapsulated into Ethernet packets for transmission over IP networks at both ends of the network by the iSCSI stack.

Advantages of iSCSI

Following are some of the main benefits of the iSCSI protocol compared to the SCSI protocol:

- iSCSI uses the existing TCP/IP network.
- iSCSI reduces total storage costs.
- iSCSI eliminates the distance limitation.
- iSCSI reduces complexity.
- iSCSI uses 10 Gigabit Ethernet.

Audience

The target audience for this guide consists of sales engineers, field consultants, professional services staff, IT managers, partner engineering staff, and customers who want to deploy Microsoft SQL Server on iSCSI.

Hardware and Software Requirements

This section provides information about hardware and software products used in this deployment model.

Cisco Unified Computing System Overview

Cisco UCS consists of a set of preintegrated data center components, including blade servers, adapters, fabric interconnects, and fabric extenders, that are integrated into a common embedded management system. This approach results in far fewer system components and improved manageability, greater operation efficiency, and more flexibility than other data center platforms.

Main Differentiating Technologies

Following are the main differentiating technologies that make Cisco UCS unique and advantageous compared to competing offerings. These technologies are discussed at a high level only, and discussion of other supporting technologies such as Fibre Channel over Ethernet (FCoE) is beyond the scope of this document.

Unified Fabric

Unified fabric can dramatically reduce the number of network adapters, blade-server switches, cables, and management touch points, bypassing all the network traffic to the parent fabric interconnects, where it can be prioritized, processed, and managed centrally. This approach improves performance, agility, and efficiency and dramatically reduces the number of devices that need to be powered, cooled, secured, and managed.

Embedded Multirole Management

Cisco UCS Manager is a centralized management application that is embedded in the fabric switch. Cisco UCS Manager controls all the Cisco UCS elements within a single redundant management domain. These elements include all aspects of system configuration and operation, eliminating the need to use multiple, separate element managers for each system component. Significant reduction in the number of management modules and consoles and in the number of agents resident on all the hardware (which must be separately managed and updated) is a critical feature of Cisco UCS. Cisco UCS Manager, using role-based access and visibility, helps enable cross-function communication efficiency, promoting collaboration among data center roles for increased productivity.

Cisco Extended Memory Technology

Significantly enhancing the available memory capacity of Cisco UCS servers, Cisco[®] Extended Memory Technology helps increase performance for demanding virtualization and large-data-set workloads. Data centers can now deploy very high virtual machine densities on individual servers and provide resident memory capacity for databases that need only two processors but can dramatically benefit from more memory. The high-memory dual in-line memory module (DIMM) slot count also lets users more cost-effectively scale this capacity using smaller, less costly DIMMs.

Dynamic Provisioning with Service Profiles

Cisco UCS Manager delivers service profiles, which contain abstracted server-state information, creating an environment in which everything unique about a server is stored in the fabric, and the physical server is simply another resource to be assigned. Cisco UCS Manager implements role-based and policy-based management

using service profiles and templates. These mechanisms fully provision one or many servers and their network connectivity in just a few minutes, rather than hours or days.

Cisco UCS Manager

Cisco UCS Manager is an embedded, unified manager that provides a single point of management for Cisco UCS. Cisco UCS Manager can be accessed through an intuitive GUI, a command-line interface (CLI), or the comprehensive open XML API. It manages the physical assets of the server and storage and LAN connectivity, and it is designed to simplify the management of virtual network connections through integration with the products of several major hypervisor vendors. It provides IT departments with the flexibility to allow administrators to manage the system as a whole, or to assign specific management functions to individuals based on their roles as managers of server, storage, or network hardware assets. It simplifies operations by automatically discovering all the components available on the system and enabling a stateless model for resource use.

The elements managed by Cisco UCS Manager include:

- Cisco UCS Integrated Management Controller (IMC) firmware
- RAID controller firmware and settings
- · BIOS firmware and settings, including server universal user IDs (UUIDs) and boot order
- Converged network adapter (CNA) firmware and settings, including MAC addresses and worldwide names (WWNs) and SAN boot settings
- Virtual port groups used by virtual machines, using Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) technology
- Interconnect configuration, including uplink and downlink definitions, MAC address and WWN pinning, VLANs, VSANs, quality of service (QoS), bandwidth allocations, Cisco Data Center VM-FEX settings, and EtherChannels to upstream LAN switches

Cisco Unified Computing System Components Figure 1 shows the Cisco UCS components.

Figure 1. Cisco UCS Components



Cisco UCS is designed from the foundation to be programmable and self-integrating. A server's entire hardware stack, ranging from server firmware and settings to network profiles, is configured through model-based management. With Cisco virtual interface cards (VICs), even the number and type of I/O interfaces is programmed dynamically, making every server ready to power any workload at any time.

With model-based management, administrators manipulate a model of a desired system configuration and associate a model's service profile with hardware resources, and the system configures itself to match the model. This automation accelerates provisioning and workload migration with accurate and rapid scalability. The result is increased IT staff productivity, improved compliance, and reduced risk of failure due to inconsistent configurations.

Cisco Fabric Extender Technology (FEX Technology) reduces the number of system components that need to be purchased, configured, managed, and maintained by condensing three network layers into one. It eliminates both blade server and hypervisor-based switches by connecting fabric interconnect ports directly to individual blade servers and virtual machines. Virtual networks are now managed exactly the same way that physical networks are, but enable massive scalability. This approach represents a radical simplification compared to traditional systems, reducing capital expenditures (CapEx) and operating expenses (OpEx) while increasing business agility, simplifying and accelerating deployment, and improving performance.

Cisco UCS Fabric Interconnects

Cisco UCS fabric interconnects create a unified network fabric throughout Cisco UCS. They provide uniform access to both networks and storage, eliminating the barriers to deployment of a fully virtualized environment based on a flexible, programmable pool of resources. Cisco fabric interconnects comprise a family of line-rate, low-latency, lossless 10 Gigabit Ethernet, IEEE Data Center Bridging (DCB), and FCoE interconnect switches. Based on the same switching technology as the Cisco Nexus[®] 5000 Series Switches, Cisco UCS 6200 Series Fabric Interconnects provide additional features and management capabilities that make them the central nervous system of Cisco UCS. The Cisco UCS Manager software runs inside the Cisco UCS fabric interconnects. The Cisco UCS 6200 Series Blade Servers and Cisco UCS blade server chassis. All chassis and all blades that are attached to interconnects are part of a single, highly available management domain. By supporting unified fabric, the Cisco UCS 6200 Series provides the flexibility to support LAN and SAN connectivity for all blades in its domain at configuration time. Typically deployed in redundant pairs, Cisco UCS fabric interconnects provide uniform access to both networks and storage, facilitating a fully virtualized environment.

Cisco UCS 6248UP 48-Port Fabric Interconnect

The Cisco UCS 6248UP 48-Port Fabric Interconnect is a one-rack-unit (1RU) 10 Gigabit Ethernet, IEEE DCB, and FCoE interconnect providing throughput of more than 1 terabit per second (Tbps) with low latency. It has 32 fixed Fibre Channel, 10 Gigabit Ethernet, IEEE DCB, and FCoE Enhanced Small Form-Factor Pluggable (SFP+) ports.

One expansion module slot can provide up to 16 additional Fibre Channel, 10 Gigabit Ethernet, IEEE DCB, and FCoE SFP+ ports.

Cisco UCS 6296UP 96-Port Fabric Interconnect

The Cisco UCS 6296UP 96-Port Fabric Interconnect is a 2RU 10 Gigabit Ethernet, FCoE, and native Fibre Channel switch offering up to 1920-Gbps throughput and up to 96 ports. The switch has 48 1/10-Gbps fixed Ethernet, FCoE, and Fibre Channel ports and three expansion slots.

One expansion module slot can provide up to 16 additional Fibre Channel, 10 Gigabit Ethernet, IEEE DCB, and FCoE SFP+ ports.

Cisco UCS 2200 Series Fabric Extenders

The Cisco UCS 2200 Series Fabric Extenders multiplex and forward all traffic from blade servers in a chassis to a parent Cisco UCS fabric interconnect over 10-Gbps unified fabric links. All traffic, even traffic between blades on the same chassis or virtual machines on the same blade, is forwarded to the parent interconnect, where network profiles are managed efficiently and effectively by the fabric interconnect. At the core of the Cisco UCS fabric extender are application-specific integrated circuit (ASIC) processors developed by Cisco that multiplex all traffic. Up to two fabric extenders can be placed in a blade chassis.

- The Cisco UCS 2204XP Fabric Extender has four 10 Gigabit Ethernet, FCoE-capable, SFP+ ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2204XP has sixteen 10 Gigabit Ethernet ports connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 80 Gbps of I/O to the chassis.
- The Cisco UCS 2208XP Fabric Extender has eight 10 Gigabit Ethernet, FCoE-capable, SFP+ ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2208XP has thirty-two 10 Gigabit

Ethernet ports connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 160 Gbps of I/O to the chassis.

Cisco UCS M81KR Virtual Interface Card

The Cisco UCS M81KR VIC is unique to the Cisco UCS blade system. This mezzanine adapter is designed based on a custom ASIC that is specifically intended for virtualized systems. It uses custom drivers for the virtualized host bus adapter (HBA) and the 10 Gigabit Ethernet network interface card (NIC). As is the case with the other Cisco CNAs, the Cisco UCS M81KR VIC encapsulates Fibre Channel traffic within 10 Gigabit Ethernet packets for delivery to the fabric extender and the fabric interconnect.

Cisco UCS Virtual Interface Card 1240

A Cisco innovation, the Cisco UCS VIC 1240 is a 4-port 10 Gigabit Ethernet, FCoE-capable modular LAN on motherboard (mLOM) designed exclusively for the M3 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional port expander, the Cisco UCS VIC 1240 capabilities can be expanded to eight ports of 10 Gigabit Ethernet.

Cisco UCS Virtual Interface Card 1280

A Cisco innovation, the Cisco UCS VIC 1280 is an 8-port 10 Gigabit Ethernet, FCoE-capable mezzanine card designed exclusively for Cisco UCS B-Series Blade Servers.

The Cisco UCS VIC 1240 and 1280 enable a policy-based, stateless, agile server infrastructure that can present up to 256 PCI Express (PCIe) standards-compliant interfaces to the host that can be dynamically configured as either NICs or HBAs.

Cisco UCS 5100 Series Blade Server Chassis

The Cisco UCS 5108 Blade Server Chassis is a 6RU blade chassis that accepts up to eight half-width Cisco UCS B-Series Blade Servers or up to four full-width Cisco UCS B-Series Blade Servers, or a combination of the two. The Cisco UCS 5108 can accept four redundant power supplies with automatic load sharing and failover and two Cisco UCS 2100 or 2200 Series Fabric Extenders. The chassis is managed by Cisco UCS chassis management controllers, which are mounted in the Cisco UCS fabric extenders and work in conjunction with Cisco UCS Manager to control the chassis and its components.

A single Cisco UCS managed domain can theoretically scale to up to 40 individual chassis and 320 blade servers. At this time, Cisco UCS supports up to 20 individual chassis and 160 blade servers.

Basing the I/O infrastructure on a 10-Gbps unified network fabric allows Cisco UCS to have a streamlined chassis with a simple yet comprehensive set of I/O options. The result is a chassis that has only five basic components:

- The physical chassis with passive midplane and active environmental monitoring circuitry
- Four power supply bays with power entry in the rear and hot-swappable power supply units accessible from the front panel
- Eight hot-swappable fan trays, each with two fans
- Two fabric extender slots accessible from the back panel
- Eight blade server slots accessible from the front panel

Cisco UCS B200 M2 Blade Servers

The Cisco UCS B200 M2 Blade Server is a half-slot, 2-socket blade server. The system uses two Intel Xeon processors p5600 series, up to 192 GB of double-data-rate-3 (DDR3) memory, two optional Small Form Factor

(SFF) SAS solid-state drives (SSDs, and a single CNA mezzanine slot for up to 20 Gbps of I/O throughput. The Cisco UCS B200 M2 Blade Server balances simplicity, performance, and density for production-level virtualization and other mainstream data center workloads.

Cisco UCS B250 M2 Extended Memory Blade Servers

The Cisco UCS B250 M2 Extended-Memory Blade Server is a full-slot, 2-socket blade server using Cisco Extended Memory Technology. The system supports two Intel Xeon processors 5600 series, up to 384 GB of DDR3 memory, two optional SFF SAS SSDs, and two CNA mezzanine slots for up to 40 Gbps of I/O throughput. The Cisco UCS B250 M2 blade server provides increased performance and capacity for demanding virtualization and large-data-set workloads, with greater memory capacity and throughput.

Cisco UCS B230 M2 Blade Servers

The Cisco UCS B230 M2 Blade Server is a full-slot, 2-socket blade server offering the performance and reliability of the Intel Xeon processor E7-2800 product family and up to 32 DIMM slots, which support up to 512 GB of memory. The Cisco UCS B230 M2 supports two SSDs and one CNA mezzanine slot for up to 20 Gbps of I/O throughput. The Cisco UCS B230 M2 Blade Server platform delivers outstanding performance, memory, and I/O capacity to meet the diverse needs of virtualized environments with advanced reliability and exceptional scalability for the most demanding applications.

Cisco UCS B440 M2 High-Performance Blade Servers

The Cisco UCS B440 M2 High-Performance Blade Server is a full-slot, 2-socket blade server offering the performance and reliability of the Intel Xeon processor E7-4800 product family and up to 512 GB of memory. The Cisco UCS B440 M2 supports four SFF SAS SSDs and two CNA mezzanine slots for up to 40 Gbps of I/O throughput. The Cisco UCS B440 M2 blade server extends Cisco UCS by offering increased levels of performance, scalability, and reliability for mission-critical workloads.

Cisco UCS B200 M3 Blade Servers

The Cisco UCS B200 M3 Blade Server delivers performance, versatility, and density without compromise. It addresses the broadest set of workloads, from IT and web infrastructure to distributed databases. Building on the success of the Cisco UCS B200 M2 Blade Server, the enterprise-class Cisco UCS B200 M3 Blade Server further extends the capabilities of the Cisco UCS portfolio in a half-width blade form factor. The Cisco UCS B200 M3 harnesses the power of the latest Intel Xeon processor E5-2600 product family, with up to 384 GB of RAM (using 16-GB DIMMs), two disk drives, and up to four ports of dual 10 Gigabit Ethernet throughput. In addition, Cisco UCS has the architectural advantage of not having to power and cool excess switches in each blade chassis. With a larger power budget per blade server, Cisco can design uncompromised expandability and capabilities in its blade servers, as evidenced by the new Cisco UCS B200 M3, with its leading memory slot and drive capacity.

Microsoft Windows 2008 R2 SP1 Overview

Microsoft Windows 2008 R2 is Microsoft's multipurpose next-generation operating system designed to increase reliability and flexibility. Microsoft Windows 2008 R2 SP1 introduces powerful next-generation tools, built-in virtualization technology, and security and server management enhancements to efficiently manage IT operations, reduce costs, and improve performance of business-critical systems. The main improvements offered in Microsoft Windows 2008 R2 SP1 are:

 Improved scalability and reliability: Microsoft Windows 2008 R2 SP1 is specifically designed to support increased workloads while using fewer resources.

- **Technology improvements:** Microsoft Windows 2008 R2 SP1 includes technology improvements designed with Microsoft Windows 7 enterprise users in mind, augmenting the network experience, security, and manageability.
- Improved management: Microsoft Windows 2008 R2 SP1 provides enhanced management consoles and automation for repetitive day-to-day administrative tasks.
- Improved web application platform: Microsoft Windows 2008 R2 SP1 provides the capability to deliver web-based multimedia experiences efficiently and effectively, with improved administration, diagnostic, development, and application tools and lower infrastructure costs.
- Microsoft Remote Desktop Services (RDS): Microsoft RDS enables users to access applications, data, and even an entire desktop running in the data center over the network. This capability provides both the features and the robustness of a proven solution, giving users flexible access to their data and applications.

Microsoft SQL Server 2012 Overview

Microsoft SQL Server is an enterprise-class relational database management system (RDBMS) that runs on the Microsoft Windows platform and provides a wide range of data management, data integration (including data quality), and business intelligence capabilities.

Some of the main features of Microsoft SQL Server 2012 are:

- High availability, including support for active multiple secondary databases, faster failover performance, fast setup, and integrated management
- ColumnStore Index, enabling the caching of query-critical data from the data warehouse in memory-based columnar format and delivering an average of 10 times the query performance of prior versions of Microsoft SQL Server
- Support for the Microsoft Windows server core to enable greater reliability and thorough cross-system security through a reduced surface area
- The new Microsoft Power View browser-based tool, along with enhancements to the Microsoft PowerPivot feature, providing rapid insight through self-service data exploration, visualization, and data mashup capabilities (users can collaborate and share these insights through Microsoft SharePoint)
- A new single business intelligence semantic model and data-quality services that help provide credible, consistent data
- Support for big data through bidirectional connectors for Hadoop along with enhancements for creation of massively scalable analytics and data warehouse solutions
- Cloud-ready connectivity built with features that support hybrid IT (integrating on-premises systems with public and private clouds)
- Expanded support for unstructured data and greater interoperability with PHP, Java, and Linux

Overview of Microsoft SQL Server 2012 Deployment Models on Cisco UCS This document describes two Microsoft SQL Server deployment models:

- <u>Microsoft SQL Server single-host deployment model</u>
- Microsoft SQL Server failover cluster deployment model

Microsoft SQL Server Single-Host Deployment Model

In the single-instance model, multiple applications are moved onto a single physical server with multiple Microsoft SQL Server instances. Each application is contained within its own Microsoft SQL Server instance. This model provides isolation of the Microsoft SQL Server instance binaries, allowing each application to be at a different patch level (major or minor version level). However, conflicts with the running application can potentially occur because system resources (mainly CPU, memory, and I/O) are shared, although tools such as the CPU affinity mask and maximum server memory settings can help provide resource isolation. Database system administration is isolated, but Microsoft Windows system administration shares the same host server. Each Microsoft SQL Server instance on the device can be enrolled within a Microsoft SQL Server control point for management. Another possible implementation is consolidation of several databases under a single Microsoft SQL Server instance to serve various applications. In this model, a single Microsoft SQL Server instance is shared across multiple applications, with each application having its own database.

The single-host deployment model is shown in Figure 2.



Figure 2. Microsoft SQL Server Single-Host Deployment Model

Microsoft SQL Server Failover Cluster Deployment Model

The Microsoft SQL Server failover cluster deployment model allows one Microsoft SQL Server to take over the tasks and responsibilities of another Microsoft SQL Server that has failed. This model helps ensure that users running mission-critical applications experience little or no downtime when such a failure occurs. Downtime can be very expensive, and the database administrator can help reduce it as much as possible. Microsoft SQL Server clustering is a high-availability technology for Microsoft SQL Server instances. It involves the sharing of server

resources between two or more nodes (or servers), which have one or more shared disks grouped into logical units called resource groups. The cluster service arbitrates ownership of the resource groups. A single node can own a resource group and its associated resources at any given time.

The Microsoft SQL Server failover cluster deployment model is shown in Figure 3. Two nodes that are members of the Microsoft Windows 2008 R2 SP1 failover cluster service are deployed on Microsoft Windows 2008 R2 SP1 server hosts on two separate Cisco UCS blades. Both Microsoft Windows 2008 R2 SP1 hosts are booted from a logical unit number (LUN) hosted on a NetApp FAS3270 with access through the iSCSI protocol. The quorum disk for the failover cluster is also accessed through the iSCSI protocol. The database data and log files are stored on separate LUNs carved out of the NetApp FAS3270 storage. These LUNs are accessed through the iSCSI initiator.

This design demonstrates the flexibility of storage access through the iSCSI protocol with a host-based iSCSI initiator. For high availability, at the physical level the clusters nodes are deployed on two different chassis, and at the software level they are configured with Microsoft Windows SQL Server failover clustering.



Figure 3. Microsoft SQL Server Failover Cluster Deployment Model

Storage Requirements for Microsoft SQL Server Database Deployment

Storage configuration is critical to any successful database deployment. As in any physical Microsoft SQL Server deployment, the storage should be sized properly to meet the database I/O requirements. The two important considerations for sizing the storage requirements are:

- Database size measured in GB
- Performance capacity measured by the number of I/O operations per second (IOPS) needed for the database to operate efficiently

To successfully design and deploy storage for a Microsoft SQL Server application, you need to understand the application's I/O characteristics and the Microsoft SQL Server I/O patterns. You need to consider parameters such as the read-to-write ratio of the application and typical I/O rates to configure the I/O characteristics of the application. The number of spindles and the speed should be configured with the maximum values to increase storage performance. RAID 1+0 provides better throughput for write-intensive applications. Place log files on RAID 1+0 (or RAID 1) disks for better performance and protection from hardware failures.

This validated solution uses the iSCSI protocol to access the primary database application storage.

Advantages of iSCSI Storage Implementation on the Microsoft Windows 2008 R2 SP1 Server Host The iSCSI protocol allows SCSI commands to be sent over a TCP/IP network. iSCSI uses standard IP network equipment such as Ethernet switches and standard NICs to send SCSI block commands encapsulated in IP packets.

iSCSI offers the following advantages:

- iSCSI uses the existing IP networks and components (NICs, switches, cables, etc.), and therefore a separate network is not required to create the SAN.
- An iSCSI SAN is cost effective compared to a Fibre Channel SAN.
- An iSCSI-based SAN can coexist with the current Fibre Channel-based SAN. This feature gives customers
 using Fibre Channel the flexibility to scale up their SANs by adding storage capacity using an iSCSI SAN.
- An iSCSI SAN does not have any distance limitation.
- iSCSI is easy to learn, deploy, and maintain because it uses common IP-based network components.
- iSCSI is well suited for implementation of SANs in virtual server environments because it supports software initiators that make such integration easier.
- iSCSI supports the same amount of bandwidth as IP networks and therefore can provide the high bandwidth required for virtual server environments.
- · iSCSI supports direct backup to tapes or disks even from virtual servers.

NetApp Storage Technologies and Benefits

NetApp solutions begin with NetApp Data ONTAP 8.0.1, the fundamental software platform that runs on all NetApp storage systems. NetApp Data ONTAP 8.0.1 is a highly optimized, scalable operating system that supports mixed network-attached storage (NAS) and SAN environments and a range of protocols, including Fibre Channel, iSCSI, FCoE, Network File System (NFS), and Common Internet File System (CIFS). Using the NetApp Data ONTAP 8.0.1 platform, the NetApp unified storage architecture offers the flexibility to manage, support, and scale business environments by using a single base of knowledge and a single set of tools. From the remote office to the data center, customers collect, distribute, and manage data from all locations and applications at the same time, scaling their investment by standardizing processes, reducing management time, and increasing availability. Figure 4 shows the NetApp unified storage architecture platform.





The NetApp storage hardware platform used in this solution is the NetApp FAS3270. The NetApp FAS3200 series is an excellent platform for Microsoft SQL Server 2012 deployments. NetApp storage is:

- Truly unified
- Highly efficient
- Extremely flexible

A variety of NetApp tools and enhancements are available to augment the storage platform. These tools assist in deployment, backup, recovery, replication, management, and data protection. This solution uses a subset of these tools and enhancements.

Design Topology

This section presents physical and logical high-level design considerations for Cisco UCS networking and computing with Microsoft Windows 2008 R2 SP1 on NetApp storage for Microsoft SQL Server 2012 failover cluster deployments.

Cisco UCS and iSCSI Storage Network

This section explains Cisco UCS iSCSI networking and computing design considerations when Microsoft SQL Server is deployed in a Microsoft Windows 2008 R2 SP1 server environment. In this design, the iSCSI traffic is isolated from the regular management and application data network using the same Cisco UCS infrastructure by defining logical VLAN networks to provide better data security. This design also reduces OpEx and CapEx compared to a topology in which a separate dedicated physical switch is deployed to handle iSCSI traffic.

Figure 5 presents a detailed view of the physical topology, identifying the various levels of the architecture and some of the main components of Cisco UCS in an iSCSI network design.





As shown in Figure 5 a pair of Cisco UCS 6248UP fabric interconnects carries both storage and network traffic from the blades with the help of a Cisco Nexus 5548UP Switch. Both the fabric interconnect and the Cisco Nexus 5548UP are clustered with the peer link between them to provide high availability. Two virtual PortChannels (vPCs) are configured to provide network and storage access paths for the blades to northbound switches. Each vPC has VLANs created for application network data, iSCSI storage data, and management data paths.

For more information about vPC configuration on the Cisco Nexus 5548UP Switch, see http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/configuration_guide_c07-543563.html.

Microsoft SQL Data Network and Storage Network vPC Mapping

Table 1 shows the Cisco Nexus 5548UP vPC configurations with the vPC domains and corresponding vPC names and IDs for Microsoft SQL Servers. To provide Layer 2 and 3 switching, a pair of Cisco Nexus 5548UP Switches with upstream switching are deployed, providing high availability to Cisco UCS in the event of failure, to handle management, application, and iSCSI storage data traffic. In the Cisco Nexus 5548UP topology, a single vPC feature is enabled to provide high availability, faster convergence in the event of a failure, and greater throughput.

vPC Domain	vPC Name	vPC ID
100	vPC-MS SQL 1	101
100	vPC-MS SQL 2	102
100	vPC-iSCSI Storage 1	103
100	vPC-iSCSI Storage 2	104

Table 1.	vPC Mapping
	vi C iviapping

In the vPC design table, a single vPC domain, Domain 100, is created across Cisco Nexus 5548UP member switches to define vPCs to carry specific network traffic. This topology defines four vPCs with IDs 101 through 104. vPC IDs 101 and 102 are defined for traffic from Cisco UCS fabric interconnects, and vPC IDs 103 and 104 are defined for traffic to NetApp storage. These vPCs are managed within the Cisco Nexus 5548UP, which connects Cisco UCS fabric interconnects and the NetApp storage system.

When configuring the Cisco Nexus 5548UP with vPCs, be sure that the status for all vPCs is "Up" for connected Ethernet ports by running the commands shown in Figure 6 from the CLI on the Cisco Nexus 5548UP Switch.

P 10.104.108.220 - PuTTY				🛃 10.104.108.221 - PuTTY						
http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/igpl-2.1.php rk2-n5548-af sh port-channel summary Flags: D - Down P - Up in port-channel (members) I - Individual H - Hot-standby (L&CP only) s - Suspended r - Module-removed S - Switched R - Routed					I - Indi	vidual ended ched	P Up in po H Hot-star c Module-r R Routed	ort-channel (ndby (LACP on		
U - Up	(port-cha	nnel)	Member Ports		Group	Port- Channel	Туре	Protocol	Member Port	3
roup Port- Channel	Туре	Protocol	Member Ports	,	1	Po1(SD) Po10(SD)	Eth Eth	NONE NONE		
00 Po100(SU) Eth	LACP	Eth1/3(P)	Eth1/4(P)	100	Po100 (SU)	Eth	LACP	Eth1/3(P)	Eth1/4(P)
01 Po101(SU) Eth	LACP	Eth1/13(P)		101	Po101 (SU)	Eth	LACP	Eth1/13(P)	
02 Po102 (SU) Eth	LACP	Eth1/19(P)		102	Po102 (SU)	Eth	LACP	Eth1/19(P)	
03 Po103 (SU) Eth	LACP	Eth1/14(P)		103	Po103 (SU)	Eth	LACP	Eth1/14(P)	
04 Po104(SU) Eth	LACP	Eth1/20(P)		104	Po104 (SU)	Eth	LACP	Eth1/20(P)	

Figure 6. PortChannel Status on Cisco Nexus 5548UP

Table 2 shows the vPC configuration details for Cisco UCS 6248UP Fabric Interconnects A and B with the required vPC IDs, VLAN IDs, and Ethernet uplink ports for a Microsoft SQL Server data network design.

Table 2. Fabric Interconnects A and B (Microsoft SQL Server Data Network)

vPC Name	vPC ID	LAN Uplink Ports	VLAN ID
vPC-MS SQL 1	101	Fabric Interconnect A (Eth 1/15 and 1/16)	108 (management) 109 (SQL network) 192 (iSCSI storage)
vPC-MS SQL 2	102	Fabric Interconnect B (Eth 1/15 and 1/16)	108 (management) 109 (SQL network) 192 (iSCSI storage)

On Cisco UCS Fabric Interconnect A, Ethernet uplink ports 15 and 16 are connected to Cisco Nexus 5548UP Application 1 (port 13) and Cisco Nexus 5548UP Application 2 (port 13), which are part of vPC ID 101 and have access to VLAN IDs 108, 109, 192, and 194. The same configuration is replicated for vPC ID 102 on Fabric Interconnect B, with ports 15 and 16 connected to port 14 of Cisco Nexus 5548UP Application 1 and Cisco Nexus 5548UP Application 2.

After configuring Cisco UCS 6248UP Fabric Interconnects A and B with vPCs, make sure that the status of all the PortChannels is "Enabled," as shown on the Cisco UCS Manager screen in Figure 7.

Figure 7. Uplink Interfaces and PortChannel Status

Equipment Servers LAN SAN VM Admin Filter: Al	LAN Uplinks VLANs Server Links MAC I Port Channels and Uplinks		ment 🛛 IP Identity Assig	nment	Qo5 Global Policies Faults Events FSM Pin Groups	
	Name		Administrative State	Ę	Name	Port
	Port Channels Fabric A			^		
🖻 - ಈ Port Channels 🚊 - ಈ Port-Channel 101 (Fabric A)) A A	Enabled Enabled	d		
	Eth Interface 1/16	A	1 Enabled			
) B B	Enabled Enabled			
	Eth Interface 1/16	B	1 Enabled			
	E Fabric A					
Uplink Interfaces					1	

On the Cisco Nexus 5548UP Switch, a separate vPC is created to access NetApp shared iSCSI storage. The vPC is created with the vPC name and corresponding vPC ID and required VLAN IDs, as shown in Table 3.

vPC Name	iSCSI Ports (Controllers A and B)	vPC ID	VLAN ID
vPC-iSCSI Storage 1	e1b and e1c (Controller A)	103	192
vPC-iSCSI Storage 2	e1b and e1c (Controller B)	104	192

Table 3. NetApp Storage

On NetApp Storage Controller A, Ethernet 10-Gbps port e1b is connected to Cisco Nexus 5548UP Application 1 (port 19), and Ethernet port e1c is connected to Cisco Nexus 5548UP Application 2 (port 19), which are part of vPC-iSCSI Storage 1 with vPC ID 103 that allows traffic from VLAN ID 192. On NetApp Storage Controller B, Ethernet 10-Gbps port e1b is connected to Cisco Nexus 5548UP Application 1 (port 20), and Ethernet port e1c is connected to Cisco Nexus 5548UP Application 1 (port 20), and Ethernet port e1c is connected to Cisco Nexus 5548UP Application 2 (port 20), which are part of vPC-iSCSI Storage 2 with vPC ID 104 that allows traffic from VLAN ID 192.

Cisco UCS Quality-of-Service System and Policy

Cisco UCS uses IEEE DCB to handle all traffic within Cisco UCS. This industry-standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. System classes determine how the DCB bandwidth in these virtual lanes is allocated across the entire Cisco UCS platform.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic, providing an assured level of traffic management even in an oversubscribed system. For example, you can configure the Fibre Channel Priority system class to determine the percentage of DCB bandwidth allocated to FCoE traffic.

Table 4 describes the system classes.

Table 4.System Classes

System Class	Description
Platinum priority Gold priority Silver priority Bronze priority	These classes set the quality of service (QoS) for all servers that include one of these system classes in the QoS definition in the service profile associated with the server. Each of these system classes manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.
Best-Effort priority	This class sets the QoS for the lane that is reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy to allow it to drop data packets if required.
Fibre Channel priority	This class sets the QoS for the lane that is reserved for FCoE traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy to help ensure that it never drops data packets.

QoS policies assign a system class to the outgoing traffic for a virtual NIC (vNIC) or virtual HBA (vHBA). You must include a QoS policy in a vNIC policy and then include that policy in a service profile to configure the vNIC.

To provide efficient network utilization and bandwidth control in a Microsoft SQL Server environment with Microsoft Windows 2008 R2 SP1 over an iSCSI network, QoS system classes and corresponding policies are defined for network traffic generated by iSCSI storage, Microsoft failover clusters, and the Microsoft SQL Server application in Cisco UCS as explained here:

- iSCSI storage traffic requires high bandwidth and a fast response time to access Microsoft SQL Server log data in the shared storage. To meet this requirement, a SQLLog QoS policy is created and defined with the Platinum class with the highest weight (bandwidth) and a maximum transmission unit (MTU) of 9000 for handling Microsoft SQL Server log transactions, which have a sequential I/O access pattern.
- To handle Microsoft SQL Server database data traffic, which have a more random I/O pattern and are less I/O intensive than log traffic, an **SQLDB** QoS policy is created with the Gold class with the second highest weight (bandwidth) and an MTU of 9000 to handle iSCSI packets.
- To handle Microsoft Windows cluster control data traffic across Microsoft SQL Server failover cluster nodes, a **MSSQLCluster** QoS class is created and defined with the third highest weight (bandwidth) on Cisco UCS.
- To handle Microsoft Windows bare-metal management and Microsoft SQL Server application data traffic from clients on the network that are not I/O intensive compared to Microsoft SQL Server database data and log traffic, an MSSQLAPP QoS class is created and defined with the fourth highest weight (bandwidth) on Cisco UCS.

Note: To apply QoS across the entire system, from Cisco UCS to the upstream switches (Cisco Nexus 5548UP Switches), you need to configure similar QoS classes and policy types with class-of-service (CoS) values that match the Cisco UCS QoS classes.

For more information, see the Cisco Nexus QoS guide at http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/qos/Cisco_Nexus_5000_Series_NX-OS_Quality_of_Service_Configuration_Guide_chapter3.html#con_1150612

Table 5 shows each QoS policy name with the corresponding priority, weight, and MTU value. These values are applied to static and dynamic vNICs in the Microsoft SQL Server deployment environment.

Policy Name	Priority	Weight (Percentage)	MTU
MSSQLLog	Platinum	10	9000
MSSQLData	Gold	9	9000
MSSQLCluster	Silver	8	9000
MSSQLAPP	Bronze	7	9000

Figure 8 shows Cisco UCS QoS system class and QoS policy configurations defined for static and dynamic vNICs for accessing a Microsoft SQL Server iSCSI network.

Figure 8. Cisco UCS QoS System Class and QoS Policy Configuration Window

Fault Summary	😌 🍥 🗳 New - 🔀 Options 🛛 🕢 Pending Activities 🛛 🔯 Exit							
2 10 7 2	>> 🗐 LAN 🖞 💭 LAN Cloud 🕴 🍟 QoS System Class							
Equipment Servers LAN SAN YM Admin	General Events F	SM						
Filter: All	Priority	Enabled	Co5	Packet Drop	Weight	Weight (%)	MTU	Multicast Optimized
* =	Platinum	V	5		10 💌	22	9000	-
B = LAN	Gold	V	4	V	9 🗸	20	9000	-
E Coud	Silver	V	2		8 🗸	18	9000	-
Fabric B	Bronze	V	1		7 🔻	15	normal	-
QoS System Class	Best Effort	M	Any	M	5 💌	11	normal	•
 ⊕-	Fibre Channel	N	3	Γ	5 💌	14	fc	N/A

Figure 9 shows how the class priorities are applied to the named QoS policies in Cisco UCS Manager.



Figure 9. Applying Priority Classes to QoS Policy in Cisco UCS Manager

Table 6 shows Cisco UCS and Cisco Nexus 5548UP QoS mapping, with Cisco UCS QoS policy configuration values matched with Cisco Nexus 5548UP QoS policy values to achieve end-to-end QoS.

On the Cisco Nexus 5548UP, a single policy-type map is defined with multiple class types, with Cisco UCS QoS matching configuration values that are applied at the global system level.

Cisco UCS QoS				Weight (Percentage)		
Policy Name	Priority	МТО	CoS	Class Type: Network QoS and QoS	Policy Type: Network QoS and QoS	
MSSQLLog	Platinum	9000	5	Network QoS: MTU 9000 and CoS 5 QoS: QoS group 5	Cisco UCS Nexus 5548UP QoS	
MSSQLData	Gold	9000	4	Network QoS: MTU 9000 and CoS 4 QoS: QoS group 4	Cisco UCS Nexus 5548UP QoS	
MSSQLCIuster	Silver	9000	2	Network QoS: MTU 9000 and CoS 2 QoS: QoS group 2	Cisco UCS Nexus 5548UP QoS	
MSSQLAPP	Bronze	9000	1	Network QoS: MTU 9000 and CoS 1 QoS: QoS group 1	Cisco UCS Nexus 5548UP QoS	

Table 6. Cisco UCS and Cisco Nexus 5548UP QoS Mapping

For more information about configuration details, see

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/qos/Cisco Nexus 5000 Series NX-OS_Quality_of_Service_Configuration_Guide_chapter3.html#con_1150612.

NetApp Storage Configuration Overview

This section discusses NetApp storage layout design details you should consider when you deploy a Microsoft SQL Server 2012 database using Microsoft Windows 2008 SP1 R2 on Cisco UCS in an iSCSI network environment.

Figure 10 shows a high-level storage design with a NetApp FAS3270 cluster storage system.

Figure 10. Design Overview for a NetApp Storage Cluster



The NetApp aggregation layer provides a large virtualized pool of storage capacity and disk IOPS to be used on demand by Microsoft Windows 2008 R2 SP1 on the aggregation layer. The aggregation-layer sizing is based on the storage requirements for Microsoft SQL Server data and log files to meet the storage capacity, performance, and snapshot backup requirements of an assumed workload. When sizing your environment, you need to perform the necessary planning to determine the exact storage configuration needed to meet your individual requirements. Aggregation-layer 0 (Aggr0) is defined for hosting root NetApp Flexible Volumes (FlexVols), which use the NetApp ONTAP operating system to handle NetApp storage configurations. For detailed NetApp storage command options, see http://now.netapp.com/NOW/public/knowledge/docs/ontap/rel732/pdfs/ontap/210-04499.pdf.

Table 7 shows the NetApp storage layout with volumes and LUNs created for various purposes.

		NetApp Storage Layo	ut
Aggregation and NetApp Controller	NetApp FlexVol	Flexible LUN	Comments
Aggr1 and Controller A	Boot_OS_VOL	MS_OS_LUN	iSCSI boot LUN for the Microsoft Windows host for node 1 of the failover cluster with a Cisco UCS B200 M3 blade server
Aggr1 and Controller A	MS_SQL_Cluster_VOL	MS_SQL_Cluster_LUN	LUN with Microsoft Windows-based software iSCSI initiator for storing failover cluster quorum data
Aggr1 and Controller A	MS_SQL_DB_VOL	MS_SQL_DB_LUN	LUN with Microsoft Windows–based software iSCSI initiator for storing the Microsoft SQL Server 2012 database file LUN
Aggr1 and Controller B	Boot_OS_VOL	MS_OS_LUN	iSCSI boot LUN for the Microsoft Windows host for node 2 of the failover cluster with a Cisco UCS B200 M3 blade server
Aggr1 and Controller B	MS_SQL_LOG_VOL	MS_SQL_LOG_LUN	LUN with Microsoft Windows–based software iSCSI initiator for storing the Microsoft SQL Server 2012 database log file LUN

Table 7.	NetApp Storage Layout with Volumes and LUNs
----------	---

Use the commands in this section to configure NetApp cluster storage systems on the storage controllers to implement the storage layout design described here. To run the following commands, from the CLI log into the storage controller using Secure Shell (SSH).

NetApp FAS3270HA (Controller A)

• The following command creates Aggr1 with a RAID group size of 10, 50 disks, and RAID_DP redundancy for hosting NetApp FlexVols and LUNs as shown in Table 7.

FAS3270HA-Controller A> aggr create aggr1 -t raid_dp -r 10 50

• The following commands create NetApp FlexVols on Aggr1 for hosting iSCSI LUNs, as shown in Table 7. These volumes are exposed to Microsoft Windows host and Microsoft SQL Server operations.

FAS3270HA-Controller A> vol create Boot_OS_VOL aggr1 50g
FAS3270HA-Controller A> vol create MS_SQL_DB_VOL aggr1 150g
FAS3270HA-Controller A> vol create MS_SQL_Cluster_VOL aggr1 150g

• The following commands create LUNs on NetApp FlexVols for hosting Microsoft SQL Server database and log files.

FAS3270HA-Controller A> lun create -s 40g -t windows /vol/Boot_OS_VOL/MS_OS_LUN

```
FAS3270HA-Controller A> lun create -s 100g -t windows
/vol/MS_SQL_DB_VOL/MS_SQL_DB_LUN
FAS3270HA-Controller A> lun create -s 100g -t windows
/vol/MS_SQL_Cluster_VOL/MS_SQL_Cluster_LUN
```

• The following commands create an initiator group (igroup) for mapping the Microsoft Windows host boot LUN and Microsoft SQL Server database data and log LUNs.

FAS3270HA-Controller A> igroup create -I -t windows SQLNODE1-Primary iqn.2012-01.com.windows:sqlnode1-Primary, iqn.2012-01.com.windows:sqlnode1-Secondary

The following commands map LUNs to specific igroups to access the Microsoft Windows host boot LUN and Microsoft SQL Server database data and log LUNs.

```
FAS3270HA-Controller A>
lun map /vol/Boot_OS_VOL/MS_OS_LUN SQLNODE1-Primary
FAS3270HA-Controller A>
lun map /vol/MS_SQL_DB_VOL/MS_SQL_DB_LUN SQLNODE1-Primary
FAS3270HA-Controller A>
lun map /vol/MS_SQL_Cluster_VOL/MS_SQL_Cluster_LUN SQLNODE1-Primary
```

After successfully running these commands, you can verify the storage configuration using the NetApp OnCommand System Manager, as shown in Figure 11.

Figure 11. Verification of Storage Configuration

Volumes 🙀 Create 🔡 Edit 🗙 Delete 🛛 🔖 Clone 👻 😁 Status 💌 🔕 Snapshot Copies 💌 🎯 Resize Name Aggregate Status Thin Provisioned MS_OS_LUN_vol oradata_A 😑 online No MS_SQL_Cluster_VOL oradata_A 😑 online No MS_SQL_DB_VOL oradata_A \varTheta online No LUNS LUN Management Initiator Groups 🚯 Create 🚺 Clone 📝 Edit 🗙 Delete | 🚳 Status 👻 Name Container Path MS_OS_LUN /vol/MS_OS_LUN_vol MS_SQL_Cluster_LUN /vol/MS_SQL_Cluster_VOL MS_SQL_DB_LUN /vol/MS_SQL_DB_VOL LUN Management **Initiator Groups** 🙀 Create 📝 Edit 🗙 Delete 🛛 😋 Refresh Name Type **Operating System** SQLNODE1-Primary **iSCSI** Windows Container Path Name MS_OS_LUN /vol/MS_OS_LUN_vol MS_SQL_DB_LUN /vol/MS_SQL_DB_VOL

NetApp FAS3270HA (Controller B)

MS_SQL_Cluster_LUN

 The following command creates Aggr1 with a RAID group size of 10, 50 disks, and RAID_DP redundancy for hosting NetApp FlexVols and LUNs as shown in Table 7.

/vol/MS_SQL_Cluster_VOL

FAS3270HA-Controller B> aggr create aggr1 -t raid_dp -r 10 50

• The following commands create NetApp FlexVols on Aggr1 for hosting iSCSI LUNs, as shown in Table 7. These volumes are exposed to Microsoft Windows host and Microsoft SQL Server operations.

FAS3270HA-Controller B> vol create Boot_OS_VOL aggr1 50g

FAS3270HA-Controller B> vol create MS_SQL_LOG_VOL aggr1 50g

 The following commands create LUNs on NetApp FlexVols for hosting Microsoft SQL Server database and log files.

```
FAS3270HA-Controller B>
lun create -s 30g -t windows /vol/Boot_OS_VOL/MS_OS_LUN
FAS3270HA-Controller B>
```

lun create -s 5g -t v windows /vol/MS_SQL_LOG_VOL/MS_SQL_LOG_LUN

 The following commands create an igroup for mapping the Microsoft Windows host boot LUN and Microsoft SQL Server database data and log LUNs.

```
FAS3270HA-Controller B> igroup create -I -t windows SQLNODE2-Primary iqn.2012-
01.com.windows:sqlnode2-Primary,iqn.2012-01.com.windows:sqlnode2-Secondary
```

 The following commands map LUNs to specific igroups to access the Microsoft Windows host boot LUN and Microsoft SQL Server database data and log LUNs.

```
FAS3270HA-Controller B>
lun map /vol/Boot_OS_VOL/MS_OS_LUN SQLNODE2-Primary
FAS3270HA-Controller B>
FAS3270HA-Controller B>
lun map vol/ MS_SQL_LOG_VOL/MS_SQL_LOG_LUN SQLNODE2-Primary
```

After successfully running these commands, you can verify the storage configuration using the NetApp Filter view, as shown in Figure 12.

Volumes

🙀 Create 🔡 Edit 🔾	🗙 Delete 🛛 🛅 Clone 👻	🖯 Status 👻 🗔 Sna	pshot Copies 💌 🎘 🦉 Resize
Name	Aggregate	Status	Thin Provisioned
MS_SQL_LOG_VOL	oradata_B	🥹 online	No
Boot_OS_VOL	oradata_B	😔 online	No

LUNs

LUN Management	Initiator Groups
🙀 Create 🔋 Clone	🛃 Edit 🗙 Delete 🛛 🚳
Name	Container Path
MS_OS_LUN	/vol/Boot_OS_VOL
MS_SQL_LOG_LUN	/vol/MS_SQL_LOG_VOL

LUN Management Initiator G	roups		
🙀 Create 🛛 Edit 🗙 Delete 🛛	😋 Refresh		
Name	Туре	Opera	ting System
SQLNODE2-Primary	iSCSI	Windo	WS
Name		Container Path	
MS_OS_LUN		/vol/Boot_OS_VOL	
MS_SQL_LOG_LUN		/vol/MS_SQL_LOG_	VOL

NetApp Multimode Virtual Interfaces

The NetApp multimode virtual interface (VIF) feature is enabled on NetApp storage systems on 10 Gigabit Ethernet ports for configuring the iSCSI target through which LUNs are exposed over the iSCSI protocol to host iSCSI initiators (Microsoft Windows hosts).

Figure 13 shows an iSCSI vPC-enabled network design on Cisco Nexus 5548UP and NetApp FAS3270HA Controllers A **a**nd B for accessing a Microsoft SQL Server data network.



Figure 13. iSCSI vPC Enabled on Cisco Nexus 5548UP

The vPC design layout for Cisco Nexus 5548UP Switches and corresponding NetApp cluster storage system multimode VIFs is as follows:

- Cisco Nexus 5548UP Application 1 and Cisco Nexus 5548UP Application 2 are part of the vPC domain and have two vPCs: vPC iSCSI Storage 1 and vPC iSCSI Storage 2, as described in the <u>Design Topology</u> section earlier in this document.
- vPC iSCSI Storage 1 has NetApp FAS3270HA (Controller A) 10 Gigabit Ethernet Interfaces e1b and e1c as member ports and is connected to Cisco Nexus 5548UP Application 1 and Cisco Nexus 5548UP Application 2 switches.
- vPC iSCSI Storage 2 has NetApp FAS3270HA (Controller B) 10 Gigabit Ethernet Interfaces e1b and e1c as member ports and is connected to Cisco Nexus 5548UP Application 1 and Cisco Nexus 5548UP Application 2 vPC switches.
- On NetApp FAS3270HA (Controller A), multilevel dynamic VIF, iSCSI A is created on 10 Gigabit Ethernet Interfaces e1b and e1c and has the MTU set to 9000 with jumbo frames enabled for accessing storage using the iSCSI protocol. VIF iSCSI A is configured with cluster failover enabled on the VIF, and the iSCSI B VIF IP address is set on NetApp FAS3270HA (Controller B).
- On NetApp FAS3270HA (Controller B), multilevel dynamic VIF iSCSI B is created on 10 Gigabit Ethernet Interfaces e1b and e1c and has the MTU set to 9000 with jumbo frames enabled for accessing storage using the iSCSI protocol. VIF iSCSI B is configured with cluster failover enabled on the VIF, and the iSCSI A VIF IP address is set on NetApp FAS3270HA (Controller A).
- On NetApp FAS3270HA (Controllers A and B), iSCSI is enabled on the e1b and e1c 10 Gigabit Ethernet interfaces for accessing storage through the iSCSI protocol from the Microsoft Windows 2008 R2 host-based software initiator.

Note: On the Cisco Nexus 5548UP upstream switch, make sure that the correct QoS class and MTU value and policy types are applied to the PortChannel ports (eth19 and eth 20). PortChannels are connected to the NetApp FAS3270HA (Controllers A and B), on the 10 Gigabit Ethernet interfaces (e1b and e1c), to allow network packets to be tagged from the Cisco Nexus 5548UP fabric. This step is needed because NetApp storage will not tag any network packets with MTU and QoS values.

The commands that follow show how to configure the CoS on the Cisco Nexus 5548UP for untagged packets originating from storage on the PortChannels.

Cisco Nexus 5548UP Application 1

Switch# Configure Terminal Switch(Conf)# Interface port channel 103 Switch(Conf-if)#untagged cos 5 Switch# sh policy-map type qos

Switch# Configure Terminal Switch(Conf)# Interface port channel 104 Switch(Conf-if)#untagged cos 4 Switch# sh policy-map type qos

Cisco Nexus 5548UP Application 2

Switch# Configure Terminal Switch(Conf)# Interface port channel 103 Switch(Conf-if)#untagged cos 5 Switch# sh policy-map type gos

Switch# Configure Terminal Switch(Conf)# Interface port channel 104 Switch(Conf-if)#untagged cos 4 Switch# sh policy-map type gos

For more information, see

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/qos/Cisco_Nexus_5000_Series_NXOS_Qua lity_of_Service_Configuration_Guide_chapter3.html#con_1150612.

NetApp VIF Configuration Details

The commands shown here are the NetApp CLI commands for configuring the multilevel dynamic VIF on NetApp FAS3270HA (Controllers A and B) cluster storage systems.

NetApp FAS3270HA (Controller A)

FAS3270HA-Controller A> iscsi start
FAS3270HA-Controller A > ifgrp create lacp iscsiA
FAS3270HA-Controller A > ifgrp add iscsiA ela elb
FAS3270HA-Controller A > ifconfig iscsiA mtusize 9000 192.191.1.2 netmask
255.255.255.0 partner iscsiB up

NetApp FAS3270HA (Controller B)

```
FAS3270HA-Controller B> iscsi start
FAS3270HA-Controller B > ifgrp create lacp iscsiA
FAS3270HA-Controller B > ifgrp add iscsiA ela elb
FAS3270HA-Controller B > ifconfig iscsiB mtusize 9000 192.191.1.4 netmask
255.255.255.0 partner iscsiA up
```

Make sure that the MTU is set to 9000 and that jumbo frames are enabled on the Cisco UCS static and dynamic vNICs and on the upstream Cisco Nexus 5548UP Switches.

Microsoft Windows iSCSI Boot

This section describes the Cisco UCS service profile design for deploying the Microsoft Windows iSCSI boot OS from the NetApp shared iSCSI target on the Cisco UCS B-Series server. In this deployment, the Cisco UCS 1240 or 1280 VIC is used for iSCSI SAN bootup of the Microsoft Windows OS from the NetApp iSCSI target.

The following steps show the basic configuration on the service profile to enable Microsoft Windows 2008 R2 SP1 iSCSI SAN bootup on the Cisco UCS B200 M3 Blade Server from the NetApp iSCSI target. For more information about the configuration steps for deploying Microsoft Windows iSCSI bootup, see the Cisco UCS CLI and GUI detailed configuration steps at

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configuration_Gui de_2_0.pdf.

 Create service profiles Chassis_Slot1_B200M3_SQLNode1 and Chassis_Slot6_B200M3_SQLNode2 and associate them with Cisco B200 M3 blades using the Cisco UCS 1240 or 1280 VIC to install Microsoft Windows 2008 R2 SP1 from the iSCSI target on NetApp FAS3270. Figure 14 shows the creation of these service profiles.



Figure 14. Creating Service Profiles

- On the Service Profiles tab for the newly created service profiles, create four static vNICs, iSCSI1, iSCSI2, iSCSI3, and iSCSI4, on Fabric A and Fabric B, respectively, with the MTU value set to 9000, without fabric failure and with network VLAN access to VLAN ID 192 (iSCSI storage), as shown in Figure 15.
- 3. To access Microsoft Windows for management and SQL applications by clients, create two separate static vNICs (vNIC1 and vNIC2) with VLAN ID 811, as shown in Figure 15.
- 4. For Microsoft Windows cluster control heartbeats across Microsoft SQL Server failover cluster nodes, create a separate static vNIC (vNIC3) with VLAN ID 193, as shown in Figure 15.

Figure 15. Creating Static vNICs on Fabric Interconnects



5. On the desired service profile, initially create one iSCSI vNIC, iSCSI-Primary, which is required to access the NetApp storage iSCSI target during iSCSI bootup to load the Microsoft Windows operating system over the iSCSI network. Make sure that the iSCSI vNIC iSCSI-Primary is overlaid on static vNIC iSCSI1, as shown in Figure 16.

A single iSCSI vNIC on the service profile is required only during the iSCSI installation period, because the Microsoft Windows OS requires the iSCSI NetApp target to be accessed over a single iSCSI path to detect the iSCSI LUN during installation.



Figure 16. iSCSI vNICs Overlaid on Static vNICs

For the Cisco UCS 1280 or 1240 VIC, make sure that the MAC address is marked "Derived" and that the correct VLAN ID (192) is chosen to access the NetApp iSCSI target during Microsoft Windows 2008 R2 SP1 server iSCSI bootup.

6. In Cisco UCS Manager, create a new iSCSI boot policy, **iSCSI-Boot**, with iSCSI vNIC **iSCSI-Primary** as a primary path during Microsoft Windows host iSCSI bootup. Figure 17 shows the boot policy configuration.

A single iSCSI vNIC defined in the **iSCSI-Boot** policy is required only during the iSCSI installation period, because the Microsoft Windows OS requires the iSCSI NetApp target to be accessed over a single iSCSI path to detect the iSCSI LUN during installation.

Warning					
Toelete	Name: i5 Description: ot on Boot Order Change: 1	7			
Show Policy Usage Rebo	Description:	7			
Rebo Enforce Warning	ot on Boot Order Change: J				
Varning Enforce	a series and a series of the				
Yarning	e vNIC/vHBA/iSCSI Name:	~			
The turns (avisses) (see and avi) does as					
The effective order of boot devices wi If Enforce vNIC/vHBA/iSCSI Name	is selected and the vNIC/vH	AN/Storage/iSCSI) is det IBA/iSCSI does not exist	, a config error will be	e reported.	
If it is not selected, the vNICs/vHBAs/ order is used.	SCSI are selected if they exi	st, otherwise the vNIC/\	HBA/iSCSI with the lo	west PCIe bus scan	
Local Devices 😵	Boot Order				
	🛨 🖃 🕰 Filter 👄 Ex	port 😹 Print			
vNICs 🛞	Name	1	Order	VNIC/VHBA/iSCSI VNIC	Туре
	CD-ROM	1			
vHBAs 😵	iscsi	2			

Figure 17. New iSCSI Boot Policy in Cisco UCS Manager

7. After the iSCSI boot policy is created, choose a newly created boot order policy for the desired service profile. For the chosen service profile on the Cisco UCS Manager Boot Order tab, assign **iSCSI-Primary** as the primary iSCSI vNIC with Microsoft Windows iSCSI boot parameters as shown in Table 8 and Figure 18.

If you have defined a single network subnet without any routing (Layer 2) iSCSI network for the Microsoft Windows OS iSCSI boot or to access the Microsoft SQL Server database over the iSCSI protocol, make sure to set the iSCSI target IP address as the default gateway in the iSCSI boot parameters.

iSCSI vNIC Name	iSCSI Initiator iSCSI Qualified Name (IQN)	Initiator IP Address Policy	Initiator IP Address	iSCSI Target IQN	iSCSI Port	iSCSI Target IP Address	LUN ID
iSCSI-Primary	iqn.2012- 01.com.window s:sqlnode1- primary	Static	192.191.1.2	992- 08.com.netapp: sn.1574125695	3260	192.191.1.2	0

Table 8. iSCSI Boot Parameters





Associate the service profile with the desired blade (Cisco UCS B200 M3 in this case). On Cisco UCS in the
associated service profile, launch the keyboard, video, and mouse (KVM) console. Through the virtual media
interface, map the Microsoft Windows 2008 R2 SP1 ISO image and install the operating system on the iSCSI
boot LUN exposed over the iSCSI network.

For more information about installing the OS in the iSCSI boot LUN, see http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html.

9. After the completion of the Microsoft Windows 2008 R2 SP1 iSCSI OS boot installation and bootup, access the KVM console for verification of the iSCSI-booted Microsoft Windows 2008 R2 SP1 OS. After the system is booted, define the secondary iSCSI vNIC **iSCSI-Secondary** in the service profile and iSCSI boot parameters to achieve redundancy in the event of failure during the iSCSI boot process. Figure 19 shows the final iSCSI vNIC and boot parameters settings needed for the Microsoft Windows 2008 R2 SP1 iSCSI OS boot. In Figure 19 you can see in the iSCSI boot properties window that the secondary iSCSI vNIC (**iSCSI-Secondary**) is configured and can boot if the primary iSCSI vNIC (**iSCSI-Primary**) fails.



Figure 19. iSCSI vNIC and Boot Parameter Settings

10. To configure the Microsoft Windows 2008 R2 SP1 iSCSI boot management IP address, access the Cisco UCS B200 M3 KVM console. Log in to the Microsoft Windows server, and to identify the Ethernet adapter connection interface that has been configured with VLAN ID 811 (management or application) access based on the MAC address, run the **ipconfig/all** command from the Microsoft Windows CLI. Figure 20 shows Ethernet adapters Local Area Connection 07 and Local Area Connection 05 selected for configuration.





 After identifying the Ethernet adapter interfaces, configure network redundancy using Cisco VIC network teaming software to create a virtual Ethernet adapter that is configured with the Microsoft Windows 2008 R2 SP1 management IP address.

Follow these steps to configure the Cisco VIC network teaming software:

- Copy the Cisco VIC network teaming software to the iSCSI-booted Microsoft Windows 2008 R2 SP1 host.
- b. Load the Cisco NIC teaming protocol driver.
- c. Create NIC teaming with active-active load balancing on the identified Ethernet interfaces to create a vNIC-teamed Ethernet interface.
- d. Configure the management IP address on the vNIC-teamed Ethernet interface.

Figure 21 shows the Cisco VIC network teaming and management IP address configuration details.





C:\NicTeaming\W2K8R2\x64>enictool.exe —1 Ethernet Adapters available to Team: Available Teams: 1. Local Area Connection 10 (Cisco NIC Teaming Miniport Driver #2)

Network Connections			
🔾 🔮 🔹 Control Panel 🔹	Network and Internet + Netv	work Connections 👻 👻 🌠	Search Network Connections
Organize Disable this network	device Diagnose this conne	ection Rename this connection >>	1 • F
Name *	Status	Device Name	Connectivity
Name *	Status Network	Device Name Cisco VIC Ethernet Interface	Connectivity No Internet access

With these steps, Microsoft Windows 2008 R2 SP1 installation is complete, with the iSCSI boot LUN configured on NetApp FAS3270.

Microsoft Windows iSCSI Solution Overview

This section provides an overview of iSCSI solution deployment with Cisco UCS. The solution builds a Microsoft Windows iSCSI infrastructure to deploy a Microsoft SQL Server 2012 failover cluster solution on a Microsoft Windows 2008 R2 SP1 bare-metal OS on Cisco UCS B-Series Blade Servers (Cisco UCS B200 M3) connected to NetApp iSCSI storage over an iSCSI network, as described in the section <u>Cisco UCS and Storage iSCSI Network</u>.

Physical and Logical Architecture

This section provides a physical and logical overview of iSCSI network architecture on Cisco UCS B-Series Blade Servers (Cisco UCS B200 M3) with Cisco VIC 1240 or 1280 adapters for deploying Microsoft Windows SQL Server with Microsoft Windows 2008 R2 SP1 using a native iSCSI software-based initiator to access shared NetApp storage over the iSCSI protocol.

Figure 22 shows the physical and logical architecture of the Cisco UCS configuration and provides an overview of the Microsoft Windows software-based iSCSI initiator configuration for deploying a Microsoft SQL Server 2012 failover cluster using Microsoft Windows 2008 R2 SP1.


Figure 22. Physical and Logical Architecture of Cisco UCS Configuration

Cisco UCS Service Profile Design

This section explains the network considerations for the Cisco UCS service profile for creating static vNICs to enable a software-based iSCSI software initiator in a Microsoft Windows 2008 R2 SP1 environment.

The following vNICs need to be created in the service profile for the Microsoft Windows 2008 R2 SP1 host to access the iSCSI storage target:

- Create two iSCSI vNICs, iSCSI-Primary and iSCSI-Secondary, which are overlaid on two static vNICs: iSCSI1 on Fabric A and iSCSI2 on Fabric B, respectively. See the <u>Microsoft Windows iSCSI Boot</u> for the implementation steps.
- Create two static vNICs, iSCSI1 on Fabric A and iSCSI3 on Fabric B, with VLAN ID 192, no fabric failover, and MSSQLLog QoS policy defined to handle Microsoft SQL Server 2012 database log iSCSI storage data network traffic.
- Create two static vNICs, iSCSI3 on Fabric A and iSCSI4 on Fabric B, with VLAN ID 192, no fabric failover, and MSSQLData QoS policy defined to handle Microsoft SQL Server 2012 database data iSCSI storage data network traffic.

- Create two static vNICs, vNIC1 on Fabric A and vNIC2 on Fabric B, with VLAN ID 809, fabric failover, and MSSQLAPP QoS policy defined to handle Microsoft Windows 2008 R2 SP1 management and Microsoft SQL Server 2012 application data network traffic.
- Create one static vNIC, vNIC3, on Fabric A, with VLAN ID 193, fabric failover, an MTU of 9000, and MSSQLCluster QoS policy defined to handle Microsoft cluster data network traffic from the Microsoft Windows 2008 R2 SP1 cluster nodes.

Table 9 lists the static vNICs with network properties created in the service profile.

vNIC	MAC Address	Fabric ID	Fabric Failover	VLAN ID	мти	Adapter Policy	QoS Policy
iSCSI1	0025:b501:0101	Fabric A	No	192	9000	Windows	MSSQLLog
iSCSI2	0025:b501:0102	Fabric B	No	192	9000	Windows	MSSQLLog
iSCSI3	0025:b501:0103	Fabric A	No	192	9000	Windows	MSSQLData
iSCSI4	0025:b501:0104	Fabric B	No	192	9000	Windows	MSSQLData
vNIC1	0025:b502:0201	Fabric A	Yes	809	9000	Windows	MSSQLApp
vNIC2	0025:b502:0202	Fabric B	Yes	809	9000	Windows	MSSQLApp
vNIC3	0025:b503:0101	Fabric A	Yes	193	1500	Windows	MSSQLCluster

 Table 9.
 Cisco UCS Service Profile Configuration

Microsoft Windows Host iSCSI Design

After booting the Microsoft Windows 2008 R2 SP1 OS through the iSCSI LUN on the Cisco UCS B200 M3 Blade Server, you need to assign the correct IP address to the corresponding Ethernet interface. You identify this address using the MAC address mapping from the Cisco UCS service profile vNIC setting for accessing Microsoft SQL Server 2012 database data and log iSCSI traffic, Microsoft Windows host management traffic, Microsoft SQL Server 2012 application traffic, and Microsoft Windows cluster traffic, as shown in Figure 23.



Figure 23. Mapping of Microsoft Windows NIC Adapters to Cisco UCS Static vNICs

Note the following Microsoft Windows 2008 R2 SP1 host logical iSCSI design considerations when deploying a Microsoft SQL Server 2012 failover cluster solution:

- Microsoft Windows 2008 R2 SP1 host management network and Microsoft SQL Server 2012
 application network traffic from clients is accessed through the Cisco vNIC-teamed Ethernet interface
 (Local Area Connection 10) with the MTU value set to 9000. The NIC-teamed Ethernet interface is
 enabled with active-active load balancing and is teamed on physical Ethernet interfaces Local Area
 Connection 5 and Local Area Connection 7, with Cisco UCS fabric failover enabled to achieve high
 availability and better network throughput.
- To access the Microsoft SQL Server 2012 database network traffic from the Microsoft Windows 2008 R2 SP1 host, a software-based iSCSI initiator is enabled with multipath on physical interfaces Local Area

Connection 0 and **Local Area Connection 3** with the MTU value set to 9000. iSCSI multipath is configured with active-active load-balancing policy to achieve high availability and better network throughput.

- To access the Microsoft SQL Server 2012 database log network traffic from the Microsoft Windows 2008 R2 SP1 host, a software-based iSCSI initiator is enabled with multipath on physical interfaces Local Area Connection 6 and Local Area Connection 2 with the MTU value set to 9000. iSCSI multipath is configured with active-active load-balancing policy to achieve high availability and better network throughput.
- To handle Microsoft 2008 Cluster network traffic across nodes, enable Ethernet interface Local Area Connection 8 with the MTU value set to 1500 and enable Cisco UCS fabric failure, to achieve high availability.

Also note that in scenarios in which multiple IP gateways are specified, you can route network packets to a specific gateway IP address by defining a lower metric value for a specific Ethernet interface that is set with the designated gateway. This setup provides additional control over the metric that is used for local routes.

In the configuration shown here, Microsoft Windows 2008 R2 SP1 host management network and Microsoft SQL Server 2012 application network traffic network packets are routed to the Cisco vNIC-teamed Ethernet interface (**Local Area Connection 10**) that is set with the appropriate gateway. To achieve this setup manually, set a lower metric value on this Ethernet interface (**Local Area Connection 10**), and on other Ethernet interfaces use the default settings, as shown in Figure 24.

COO 😰 - Control Panel - Network and Internet - Network C	onnections +	- 😂	Searc
Local Area Connection Network Microsoft Virtual Machine Bus Networ	Area Connection Status al Area Connection Properties orking Sharing ternet Protocol Version 4 (TCP/IP General You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings. Obtain an IP address automatice Advanced TCP/IP Settings IP Settings DNS WINS IP addresses IP addresses IP addresses IP addresses	Image setting Image setting <td< th=""><th>as of this</th></td<>	as of this
es	Add Default gateways: Gateway 10.101.110.1 Add Automatic metric	Metric Automatic	1

Figure 24. Lower Metric Value Setting on Ethernet Interface (Local Area Connection 10)

For more information, see http://support.microsoft.com/kb/299540.

To support end-to-end jumbo frames (MTU 9000) to carry the Microsoft SQL Server client, iSCSI, and cluster traffic from the Microsoft Windows 2008 R2 SP1 host, Cisco UCS, and NetApp storage, perform the following steps:

- 1. Configure MTU 9000 in the Cisco UCS QoS system with Platinum, Gold, Silver, and Bronze classes as shown in the section <u>Cisco UCS Quality-of-Service System and Policy</u>.
- 2. Configure MTU 9000 in the Jumbo field on the appropriate Ethernet interfaces (0, 10, 8, 6, 3, and 2 in this design) on the Microsoft Windows 2008 R2 SP1 host.
- 3. Configure NetApp iSCSI VIFs to enable the MTU 9000 value, as shown in the section <u>Microsoft SQL Data</u> <u>Network and Storage Network vPC Mapping</u>.
- On the Microsoft Windows 2008 R2 SP1 host, enable and configure the iSCSI software initiator and multipath I/O (MPIO) to access NetApp iSCSI targets.

For more information about configuring the iSCSI initiator in Microsoft Windows, see http://technet.microsoft.com/en-us/library/ee338476%28v=ws.10%29.

The following steps provide a high-level overview of the configuration of the Microsoft Windows 2008 R2 SP1 host iSCSI software initiator to access the NetApp iSCSI target:

 Discover the storage controller NetApp FAS3270HA Controller A VIF iscsiA (192.191.1.2) with the Microsoft Windows 2008 R2 SP1 host iSCSI initiator Interfaces (192.191.1.99 and 192.191.1.100), and discover the storage controller NetApp FAS3270HA Controller B VIF iscsiB (192.191.1.101 and 192.191.1.102) with the Microsoft Windows 2008 R2 SP1 host iSCSI software initiator, as shown in Figure 25.

rties							
Favorite Targe	ets Volumes and Devices	RADIUS Configuration					
Target portals The system will look for Targets on following portals: Refresh							
Port	Adapter	IP address					
3260	Default	Default					
3260	Default	Default					
To add a target portal, click Discover Portal.							
	the address above and	Remove					
	ok for Targets o Port 3260 3260 ortal, click Disco	Favorite Targets Volumes and Devices ok for Targets on following portals: Port Adapter 3260 Default 3260 Default ortal, click Discover Portal. et portal, select the address above and					

Figure 25. iSCSI Initiator Properties Showing Target IP Addresses

2. To enable iSCSI multipath, select the **Enable multi-path** check box in the target connection configuration for both controllers. Figure 26 shows multipath enabled.

Figure 26. Multipath Enabled for Target Connection

Connect To Target		
Target name:		
ign.1992-08.com.netapp:sn.1574125695 ation		
Add this connection to the list of Favorite Targets.	Advanced Settings	
This will make the system automatically attempt to restore the r connection every time this computer restarts.	General IPsec	
I Enable multi-path ect	Connect using	
Advanced OK Cancel	Local adapter: Microsoft iSCSI Initiator	•
	Initiator IP: 192.191.1.99	•
Name Status Ign.1992-08.com.netapp:sn.1574125695 Connected	Target portal IP: 192.191.1.2 / 3260	•
ign.1992-06.com.netapp:sn.157412695 Connected	General IPsec	
	· · ·	
	Local adapter: Microsoft iSCSI Initiator	-
	Initiator IP: 192.191.1.100	•
	Target portal IP: 192.191.1.2 / 3260	
To connect using advanced options, select a target and then Connect		
To completely disconnect a target, select the target and Disconnect Disconnect		
For target properties, including configuration of sessions, Properties		
For configuration of devices associated with a target, select		

ionnect To Target 🛛 🔀	×		
Target name: atik	ation		
iqn.1992-08.com.netapp:sn.1574126331			
Add this connection to the list of Favorite Targets. This will make the system automatically attempt to restore the connection every time this computer restarts.	General IPsec		
Enable multi-path	Connect using		
Advanced OK Cancel	Local adapter:	Microsoft iSCSI Initiator	•
	Initiator IP:	192.191.1.101	•
ign.1992-08.com.netapp:sn.1574125695 Connected ign.1992-08.com.netapp:sn.1574126331 Connected	Target portal IP:	192.191.1.4 / 3260	•
To connect using advanced options, select a target and then connect	Connect using Local adapter: Initiator IP:	Microsoft iSCSI Initiator	2
click Connect.	Target portal IP:	192.191.1.4 / 3260	2
To completely disconnect a target, select the target and then click Disconnect.	t		
For target properties, including configuration of sessions, select the target and click Properties.			
For configuration of devices associated with a target, select the target and then click Devices.			
the target and then click Devices.			

 In Microsoft Windows 2008 R2, log in to the iSCSI initiators to access NetApp targets; LUNS are automatically exposed for configuration. For a Microsoft SQL Server 2012 single-host installation, you use Disk 1 as the database file and Disk 2 as the log file, as shown in Figure 27. See the section <u>NetApp Storage</u> <u>Configuration Overview</u> for LUN creation and access details.





a. Under Disk Management, in Microsoft Windows 2008 R2, scan for new disks and format them. Create the NTFS file for storing Microsoft SQL Server 2012 database data and log files, as shown in Figure 28.

📕 Server Manager											
File Action View Help											
🗢 🔿 🖄 🖬 📓 🖬 🕄 🕯	9 BJ										
Server Manager (SQLNODE1) Roles	Disk Management Volume List + Graphical View										
Roles Gill Features Diagnostics	Volume		Type Basic	File System NTFS		(Boot, Page File, Crash Dump, Primary Partition)	Capacity 49.91 GB	Free Space 10.07 GB	% Free 20 %	Fault Tolerance No	Overhead 0%
Configuration	Cluster (G:)		Basic Basic			(Primary Partition) (Primary Partition)	5.00 GB 100.01 GB	4.95 GB 99.92 GB	99 % 100 %	No No	0% 0%
Windows Server Backup	MSSQLLog (L:)		Basic Basic			Primary Partition) (System, Active, Primary Partition)	100.00 GB 100 MB	99.91 GB 72 MB	100 % 72 %	No No	0% 0%
	50.01 GB Online aDisk 1 Basic 100.01 GB Online Basic 100.01 GB Online Colline	System 100 MB N Healthy (5 MSQLDab 100.01 Gr Healthy (f Healthy (f Luster 5.00 GB N Healthy (f	TFS System, System, ShTFS Primary Og (L:) ShTFS Primary (G:) ITFS	, Active, Prim) Partition)) Partition)	ary Partitic	(C:) 49.91 GB NTFS Healthy (Boot, Page File, Grash Dump, Primar	ry Partition)				

Figure 28. Scanning for New Devices on Microsoft Windows 2008 R2

4. Install Microsoft SQL Server on the Microsoft Windows 2008 R2 OS and create the database with the data and log files residing on the designated storage volumes. For more information about installing Microsoft SQL Server 2012, see <u>http://msdn.microsoft.com/en-us/library/bb500469%28v=sql.110%29.aspx</u>.

Microsoft SQL Server Failover Cluster Solution

This section provides a high-level physical and logical procedure for setting up a Microsoft SQL Server 2012 cluster failover deployment on a Microsoft Windows 2008 R2 SP1 host with a software-based iSCSI initiator on Cisco UCS to access NetApp shared iSCSI storage in an iSCSI network environment.

Failover clustering provides very good protection in the event of a hardware failure. Failover to an active node is fairly quick (between one and five minutes, depending on the state of the cluster and database). Failover clustering provides service availability but does not provide data redundancy such as database mirroring and log shipping. Data protection has to be provided at the storage level or in combination with other solutions.

Failover clustering provides host-level protection built on Microsoft Windows failover clustering. Cluster nodes typically are co-located within the same site or data center to provide local availability, but they also can be deployed regionally.

Physical and Logical Design

This section provides a high-level overview of the physical and logical infrastructure design considerations required to deploy a Microsoft SQL Server 2012 failover cluster on a Microsoft Windows 2008 R2 SP1 host based on an iSCSI software initiator on a Cisco UCS B200 M3 Blade Server.

This document describes Microsoft SQL Server 2012 failover clustering within the same site on a single Cisco UCS platform across two Cisco UCS B200 M3 Blade Servers mounted on separate Cisco UCS chassis for high availability and managed by a single Cisco UCS platform.

Figure 29 shows the physical and logical design of the Microsoft SQL Server 2012 failover cluster solution on a Microsoft Windows 2008 R2 SP1 host with an iSCSI software initiator.



Figure 29. Physical and Logical Design of Microsoft SQL Server 2012 Failover Cluster Solution

Perform the following steps to implement failover clustering on two Microsoft Windows 2008 R2 SP1 hosts **SQL Node1 and SQL Node2** using software-based iSCSI systems. These Microsoft Windows 2008 R2 SP1 nodes are part of a Microsoft Windows failover cluster, booted through the iSCSI target.

 To implement Microsoft server clustering and a Microsoft SQL Server 2012 failover cluster server on Microsoft Windows 2008 R2 SP1 hosts, you need to use two Cisco UCS B200 M3 blades (SQL Node1 and SQL Node2) in a dual chassis, as shown in Figure 29.

Define two service profiles with the required network infrastructure to install Microsoft Windows 2008 R2 SP1 iSCSI boot operating systems, which are clustered to host failover clustering. The design of the Microsoft Windows 2008 R2 SP1 iSCSI boot OS and iSCSI initiator for individual hosts is explained in the sections <u>Microsoft Windows iSCSI Boot</u> and <u>Microsoft Windows iSCSI Solution Overview</u>, respectively.

 To deploy Microsoft Windows 2008 failover cluster mode on Microsoft Windows 2008 R2 cluster nodes SQLNODE1 and SQLNODE2, attach eight static vNICs as shown in Figure 29.

a. Configure iSCSI interfaces with multipath on **Ethernet 6** and **Ethernet 2** local area connections Ethernet interfaces to access the iSCSI storage NetApp FAS3270HA Controller A VIF target, which hosts cluster LUNs

for Microsoft SQL Server database data files. The LUN is accessed through the Microsoft Windows 2008 R2 SP1 iSCSI software initiator.

b. Configure iSCSI interfaces with multipath on **Ethernet 0** and **Ethernet 3** local area connections Ethernet interfaces to access the iSCSI storage NetApp FAS3270HA Controller B VIF target, which hosts cluster LUNs for Microsoft SQL Server database Log files. The LUN is accessed through the Microsoft Windows 2008 R2 SP1 iSCSI software initiator.

c. Configure the Cisco NIC teaming virtual Ethernet interface on **Ethernet 5** and **Ethernet 7** local area connection Ethernet interfaces for internal and external clients to access the Microsoft SQL Server 2012 failover cluster server.

d. Configure the Microsoft cluster Ethernet interface on the **Ethernet 5** local area connection Ethernet interface for access cluster network communication across Microsoft SQL Server 2012 failover cluster servers.

 Perform the following steps to design the iSCSI NetApp storage target for deploying a Microsoft SQL Server 2012 failure cluster instance on Microsoft Windows 2008 R2 SP1 cluster nodes SQLNODE1 and SQLNODE2.

a. Microsoft Windows 2008 R2 SP1 cluster nodes **SQLNODE1** and **SQLNODE2** use the iSCSI software initiator configured with the **Ethernet 2** and **Ethernet 6** local area connection interfaces to access the NetApp cluster storage iSCSI target VIF (NetApp FAS3270HA Controller A **iscsiA** and **Ethernet 0** and **Ethernet 3** local area connection interfaces to access NetApp FAS3270HA Controller B **iscsiB**), with multipath enabled to access the Microsoft SQL Server 2012 database data and log LUNs. On NetApp storage systems (NetApp FAS3270HA Controllers A and B), provision cluster LUNs **MS_SQL_Cluster_LUN** for storing Microsoft cluster quorum data, and **MS_SQL_DB_LUN** and **MS_SQL_LOG_LUN** for storing shared Microsoft SQL Server 2012 failover cluster database data and log files. These LUNs are exposed through the iSCSI network on the Microsoft Windows 2008 R2 SP1 host, which is part of the Microsoft Windows server.

b. Make sure that you create igroups on both NetApp storage controllers, NetApp FAS3270HA Controller A and NetApp FAS3270HA Controller B, with both the **SQLNODE1** and **SQLNODE2** iSCSI initiator IQN names, and map **MS_SQL_Cluster_LUN**, **MS_SQL_DB_LUN** and **MS_SQL_LOG_LUN** to those IQNs as explained in the section <u>NetApp Storage Configuration Overview</u>.

c. After exposing NetApp storage LUNs to the Microsoft Windows 2008 R2 SP1 host **SQLNODE1** and **SQLNODE2** cluster nodes, scan for new disks in the disk manager and format the disk. Assign the same drive letter to both cluster nodes, as shown in Figure 30.

50	LNODE1			SQLNODE2				
Server Manager				En Server Manager				
File Action View Help				File Action View Help				
🗢 🔿 🔰 🖬 🔛 😹				🗢 🔿 🖄 📅 🚺 🖬 😰	e 😼			
Server Manager (VMSQLNODE1)	Disk Management	: Volume List + Graphical View		Server Manager (VMSQLNODE2)	Disk Management	Volume List + Graphical View		Actions
	Volume	Layout Type File System	Status	Roles Features	Volume	Layout Type File System	Status	Disk Mana
Production Configuration Sorrage Sorrage Sorrage Disk Management	(C:) ClusterQurom (G:) SQL Data DB (E:) SQL DB .og (F:)	Simple Basic NTFS Simple Basic NTFS Simple Basic NTFS Simple Basic NTFS	Healthy (S Healthy (P Healthy (P Healthy (P	Diagnostics Configuration Storage	(C:) ClusterQurom (G:) SQL Data DB (E:) SQL DB Log (F:)	Simple Basic NTFS Simple Basic NTFS Simple Basic NTFS Simple Basic NTFS	Healthy (System, Boot, Healthy (Primary Partitic Healthy (Primary Partitic Healthy (Primary Partitic	
	 ✓ Disk 1 Basic 100.01 GB 	SQL Data DB (E:) 100.01 GB \TF5			100.01 GB	SQL Data DB (E:) 100.01 GB NTFS	اد ام	
	Disk 2 Basic 5.00 GB	Healthy (Primary Partition) ClusterQurom (G:) 5.00 GB NTFS Healthy (Primary Partition)			Basic 5.00 GB	Healthy (Primary Partition) ClusterQurom (G:) 5.00 GB NTFS Healthy (Primary Partition)		
	Disk 3 Basic 100.01 GB	SQL DB Log (F:) 100.01 GB NTFS			100.01 GB	SQL DB Log (F;) 100.01 GB NTFS imary partition		

Figure 30. Scanning for New Disks and Assigning New Disks to Cluster Nodes

Installation of Microsoft Windows 2008 Failover Cluster Feature with iSCSI Software Initiator After configuration of the two Microsoft Windows 2008 R2 SP1 hosts, **SQLNODE1** and **SQLNODE2**, is complete, perform the following steps to deploy Microsoft Windows 2008 failover clustering:

- 1. Before installing the Microsoft failover clustering feature on Microsoft Windows 2008 R2 SP1 hosts **SQLNODE1** and **SQLNODE2**, verify that they are part of a Microsoft Active Directory domain.
- 2. Log in to individual Microsoft Windows 2008 R2 SP1 hosts **SQLNODE1** and **SQLNODE2** by selecting the domain controller with Admin credentials.
- Add the failover clustering feature on both Microsoft Windows 2008 R2 SP1 hosts: SQLNODE1 and SQLNODE2.
- 4. After installing the failover cluster feature on both Microsoft Windows 2008 R2 SP1 hosts, log in to either host (Microsoft Windows 2008 R2 SP1 SQLNODE1 or SQLNODE2) and launch the Failover Cluster Management console to validate clustering. Add Microsoft SQL Server hosts SQLNODE1 and SQLNODE2 with the fully qualified domain name in the Select Servers or a Cluster window, as shown in Figure 31.

Figure 31.	Adding	Microsoft	SQL	Server	Guest
------------	--------	-----------	-----	--------	-------

關 Failover Cluster Management		_ @ ×
File Action View Help		
Failover Cluster Management Failover Cluster Ma	inagement	Actions
NCm Create failover cluste	rs, validate hardware for potential failover clusters, and perform configuration changes to your failover clusters.	Failover Cluster Ma 🔺
102		Validate a Confi
	date a Configuration Wizard 🛛 🕺 🗙	
Overview 1	Select Servers or a Cluster	Manage a Cluste
A failover cluster 1000 physical cables a	R.	rs) are connected by View
Patron	You Begin To validate a set of servers, add the names of all the servers.	Holp
- Clusters Select	To test an existing cluster, add the name of the cluster or one of its nodes.	
* Managem Cluster		
I o begin to use I	Browse	Managing a cluster can
include migrating Confirm Validate a C Validat	Selected servers: SQLNODE1.tmesal.com Add	
Manage a C		
* More Info		
Eilover elu:		
Failover clu:		
Mcrosoft su		
	<previous next=""> Cancel</previous>	
		-

5. Select and add Microsoft Windows 2008 R2 SP1 hosts **SQLNODE1** and **SQLNODE2** and be sure to run all the tests to validate the cluster requirements, as shown in Figure 32.

Figure 32. Running Tests to Validate Cluster Requirements

Failover Cluster Management	Failover Cluster Management		Actions
Falover Guster Management	Create falover clusters, validate hardware Validate a Configuration Validate a Configuration Validate a Configuration Validate a Configuration Validate a Configuration To testing Option Configuration Validate a Configuration Testing Option Configuration Validate a Configuration Configuration Validate a Configuration Configuration Configuration Validate a Configuration Config	X 1) are connected by Managing a cluster can	Actions Failover Chaster Ma Valdate a Confi Create a Cluster New I hansge a Cluster New I help

Successful validation of the addition of Microsoft Windows hosts **SQLNODE1** and **SQLNODE2** to the cluster is shown in Figure 33.

If warning messages appear, they need to be documented, and associated risks and action plans need to be identified.

Figure 33. Failover Cluster Validation Report

The state Yew Yeb; Image: State Teste alove cluster Management Failover Cluster Management Failover Cluster Management Image: State Coverview State Coverview State State <th>👺 Failover Cluster Managemen</th> <th></th> <th>- 0 ×</th>	👺 Failover Cluster Managemen		- 0 ×
Failover Cluster Management Actions Failover Cluster Management Actions Cluster Summary a configuration Wizard a configuration Wizard Validate a Configuration Wizard x a connected by Manage a Cluster Ha Validate a Configuration Wizard x a connected by a connected by Validate a Configuration Wizard x a connected by a connected by Validate a Configuration Wizard x a connected by a connected by Validate a Configuration Wizard x a connected by a connected by Validation Testing has completed successfully. The configuration appears to be suitable for clustering, but split reed to reasond to For a connected by Validate a C Validation Cluster a connected by anaging a cluster connected by Validate a C Validation Summary go cluster kan a connected by anaging a cluster connected by Validation Validation Summary connected by the wizard, click View Report. Manage Configuration appears to be suitable to cluster suitable to clu	a state a state of the state of		
Pallover clusters, wildele haves for pornial fallower dusters, and perform configuration changes to your failower clusters.			
Create failower clusters, validate hardware for optential failower clusters, and perform configuration changes to your failower clusters. Vulcate a configuration witzard Cuter cluster Summary Cuter cluster Cute	📲 Failover Cluster Management	Failover Cluster Management	Actions
		Create fallover clusters, validate hardware for potential fallover clusters, and perform configuration changes to your failover clusters. Validate a Configuration Wizard Validate a Configuration Wizard Crusters Belore You Begin Select Servers or a Crusters Crusters Crusters Belore You Begin Crusters Cruster Cruster Crusters Cruster Crust	s) are connected by

6. Create a cluster and name it **MSSQL** with the cluster and IP address on the management VLAN (809) as shown in Figure 34.

Figure 34. Administering the Cluster

🐇 Failover Cluster Management				X
File Action View Help				
(= =) 🖬 🖬 🖛				
📲 Failover Cluster Management	Failover Cluster Management			Actions
		are for potential failover clusters, and perform configuration changes to your failover clusters.		Failover Cluster Ma 🔺
	Create failover clusters, validate hardw	ale to potential rational dealers, and ponem configuration analysis to your failower electrics.		Validate a Confi
			-	🖓 Create a Cluster
	* Overview Create Cluster Wiz	ard	×	Manage a Cluste
	A falover cluster physical cables a Access P	oint for Administering the Cluster	is) are connected by	View +
				Help
	Clusters Before You Begin	Type the name you want to use when administering the cluster.		
	* Managem Select Servers			
	To begin to use I Access Point for	Cluster Name: MSSQL One or more IR-vit addresses could not be configured at tomatically. For each natural to be used make	Managing a cluster can	
	include migrating Administering the Cluster	One or more IPv4 addresses could not be configured automatically. For each network to be used, make sure the network is selected, and then type an address.		
	Confirmation			
	Creating New Cluster	Networke Address		
	Manage a L Summary	192 191 1.0/24 Click here to type an address		
		R 10.104.108.0/24 10.104.108.240		
	* More Info			
	Falover clu:			
	Ealover clu:	Nore about the administrative Access Point for a cluster		
	Microsoft su	More about the administrative Access Form for a cluster		
		<previous next=""> Cancel</previous>		

Figure 35 shows cluster summary information prior to creation of the cluster for the **SQLNODE1** and **SQLNODE2** nodes.

Figure 35. Summary of the Created Cluster

🐺 Failover Cluster Management				_ 8 ×
File Action View Help				
📲 Failover Cluster Management	Failover Cluster Management			Actions
	200 Create fallovar chuslers, validate bardu	are for potential failover clusters, and perform configuration changes to your failover	chusters	Failover Cluster Ma 🔺
	Create failover clusters, validate hardw	are for potential ratiover disserve and perform configuration enanges to your ratiover	olasidas.	👹 Validate a Confi
				Create a Cluster
	* Overview 🙀 Create Cluster Wi	ard	X	📲 Manage a Cluste
	A failover cluster physical cables a Summary		ss) are connected by	View •
			2	Help
	Clusters Before You Begin	You have successfully completed the Create Cluster Wizard		
	Managem Select Servers	tiou have successibility completed the create cluster witzard		
	To begin to use 1. Access Point for		Managing a cluster can	
	include migrating Administering the Cluster	Create Cluster		
	Confirmation			
	Create a Ch. Creating New Cluster	Cluster: MSSQL		
	Manage a C Summary	Node: SQLNODE1.tmesql.com Node: SQLNODE2.tmesql.com		
		Node: SQLNODE2.tmesql.com Quorum: Node and Disk Majority (Cluster Disk 2)	2)	
	More Info	IP Address: 10.104.108.240	-	
		To view the report created by the wizard, click View Report. To close this wizard, click Finish.	View Report	
	Eailover clu			
	Ealover clu:			
	Mcrosoft su			
			Finish	

 To validate the Microsoft cluster installation, log in to either Microsoft Windows 2008 R2 SP1 host (SQLNODE1 or SQLNODE2) cluster node and launch the Failover Cluster Management console as shown in Figure 36.

🖥 Failover Cluster Management		- 8 ×			
File Action View Help					
🗢 🔿 🖄 🕅 🔛 📅					
Railover Cluster Management	Cluster MSSQL.tmesql.com	Actions			
E B Services and Applications		M55QL.tmesql.com			
I Nodes	Summary of Cluster MSSQL MSSQL MSSQL MSSQL MSSQL	🖓 Configure a Ser			
SQLNODEL SQLNODE2	MSSOL has 0 applications/services and 2 nodes	Mew Validation			
🛃 Storage	Name: MSSQL.tmssql.com Networks: Cluster Network 1, Cluster Network 2	🔐 Add Node			
Networks Cluster Network 1	Current Host Server: SQLNDDE1 Subnets; 21Pv4 and 01Pv6	🔎 Close Connection			
Cluster Network 2	Quorum Configuration: Node and Disk Majority (Cluster Disk 2)				
Cluster Events	Application Alert: <nore> Recent Cluster Events: None in the last 24 hours</nore>	View +			
	Necent cluster events. None in the last 24 hours	Refresh			
	Configure	Properties			
	Configure high availability for a specific service or application, add one or more servers (nodes), or migrate resource group settings from a sluster running Windows Server 2003	🕜 Help			
	Configure a Service or Application				
	Migrate Services and Applications				
	Nevigate to Storage to add disks				
	* Navigate				
	Services and Applications Nodes				
	Storage Networks				
	Cluster Events				
	Cluster Core Resources				
	^ More Information				
	Ealover clutter topics on the Web				
	Eloyer cluster communities on the Web				
	Microsoft surport page on the Web				
	1				
		11 44			

- 8. Log in to either Microsoft Windows 2008 R2 SP1 host (**SQLNODE1** or **SQLNODE2**) cluster node and choose the cluster witness disk for storing cluster information.
- 9. On the Failover Cluster Management console, select More Actions and then select the cluster name. In the Configure Cluster Quorum Wizard, under Quorum Configuration, choose Node and Disk Majority (recommended for the number of nodes used here) and select the MS_SQL_Cluster LUN disk drive as the witness disk if it is not been automatically identified, as shown in Figure 37.

Figure 37. Configuring MS SQL Cluster Quorum

File Action Vew Help Image: Selecter Management Imagement Imagement	
Palover Cluster Management 日報 MSSQL.tmesql.com Actions Actions MSSQL.tmesql.com MSSQL.tmesql.com	
B B MSSQLtmssqlcom	
E B MSSQLLmessLoom MSSQLLmess	
	ql.com 🔺
Summary of Clubter MSSCL	a Ser
Storage WIV MSSOL has O apolications/henrices and 2 nodes 🔢 Metworks 📓 Configure Cluster Quorum Wizard 🔀	ation
Add Node	
Current Host Ser Configure Storage Witness	nection
Nore Acti	ans +
Application Alert Recent Cluster E Before You Begin Select the storage volume that you want to assign as the disk witness.	•
Refersh Sete for a dage reand up you want a dage reand up you you want a dage reand up you you want a dage reand	
Configure Configure	;
Configure High av Worksson De Carolina Stature Norde Location Que High av Worksson De Carolina SQLNDB1 Avriatela Strange Server 2003 Q Helb	
Volume: (E) File System: NT_ 100.01 GB (99.9_	
✓ Configure Duster ✓ Magale Sarv Online SQLNODE1 Outputs Duster Volume: (G) File System: NT5 GB (98.7% free)	
Revirate to a Cluster Disk 3 (*) Online SQLNODE1 Available Storage	
Volume: (F) File System: NT_ 100.01 GB (99.9.	
Navigate	
Instance	
Date Ever	
Cluster Co	
More Infor	
Eakover duater topics on the Web	
Falover duster communities on the Web	
Misrosoft ausport page on the Web	

 On the Failover Cluster Management console, select More Actions and then select Networks. Under Networks, choose Cluster Network 2 and select the radio button Allow cluster network communication on this network. Figure 37 shows the configuration of cluster networks.

Figure 38. Configuring Cluster Network

tatus: Up luster Use: Internal		Subnets: 193.191.1.0/24 (IPv4) Cluster Network 2 Properties
		General
ame Network Connections	Status	Cluster Network 2
SQLNODE1 - Local Area Connection 6 Adapter: Cisco VIC Ethernet Interface #6 IP Address: 193.191.1.2	🕑 Up	Name: Cluster Network 2
 SQL00DE2 - Local Area Connection 3 Adapter: Cisco VIC Ethernet Interface #3 IP Address: 193.191.1.4 	🛞 Up	Allow cluster network communication on this network Allow clients to connect through this network Do not allow cluster network communication on this network
		Status: Up Subnets: 1921911.0/24
		Subnets: 133.191.1.0/24
	ame Network Connections SQLNODE1 - Local Area Connection 6 Adapter: Cisco VIC Ethernet Interface #6 IP Address: 193.191.1.2 SQLNODE2 - Local Area Connection 3 Adapter: Cisco VIC Ethernet Interface #3	ame Status Network Connections SQLNODE1 - Local Area Connection 6 Up Adapter: Cisco VIC Ethemet Interface #6 IP Address: 193.191.1.2 SQLNODE2 - Local Area Connection 3 SQLNODE2 - Local Area Connection 3 Adapter: Cisco VIC Ethemet Interface #3

Installation of Microsoft SQL Server 2012 Failover Cluster Feature with iSCSI Storage The following steps describe deployment of Microsoft SQL Server 2012 failure clustering on Microsoft Windows 2008 R2 SP1 hosts.

1. Log in to either Microsoft Windows 2008 R2 SP1 cluster node, **SQLNODE1** or **SQLNODE2**, to perform installation on Microsoft SQL Server 2012. This document uses the **SQLNODE1** cluster node.

a. Copy the Microsoft SQL Server 2012 binaries on the Microsoft Windows 2008 R2 SP1 host **SQLNODE1** cluster node for installation.

b. Log in to **SQLNODE1** with Admin credentials for installing Microsoft SQL Server 2012 software, launch the Microsoft SQL Server installation .exe file, and choose **New SQL Server failover cluster installation**, as shown in Figure 39.

🚼 SQL Server Installation Center	
Planning Installation	Wew SQL Server stand-alone installation or add features to an existing installation Launch a wizard to install SQL Server 2012 RCO in a non-clustered environment or to add features to an existing SQL Server 2012 RCO instance.
Maintenance Tools	New SQL Server failcver cluster installation Launch a wizard to instal a single-node SQL Server 2012 RCO failover cluster.
Resources Advanced	Add node to a SQL Server failover cluster
Options	Upgrade from SQL Server 2005, SQL Server 2003 or SQL Server 2008 R2 Launch a wizard to upgrade SQL Server 2005, SQL Server 2008 R2 to SQL Server 2018 R2 to SQL Server 2012 RCD.
SQL Server 2012	

Figure 39. Launch Microsoft SQL Server in Microsoft SQL Server Installation Center

c. Follow the installation steps in the wizard and provide license keys. Choose the Feature Selection option in the wizard and select appropriate features based on your requirements. For the Microsoft SQL Server binaries shared feature directory, provide the appropriate installation directory on the cluster node, **SQLNODE1**, as shown in Figure 40.

Feature Selection	o mstall.	
Setup Support Rules	Features	Feature description:
Souspaper New S Souspaper New S Feature Rule Feature Rule Instance Configuration Dick Space Requirements Clutter Resurce Group Clutter Resurce Group Clutter Resurce Group Clutter Resurce Configuration Database Ergne Configuration Enor Reporting Services Configuration Error Reporting Service	Instance Features Instance Features	Prerequisites for selected features: Aready installed:
	Select, All Unselect, All Shared Feature directory: C:\Program Hiss\Microsoft SQL Server\ Shared Feature directory (x86); C:\Program Files (x86)/Microsoft SQL Server\	

Figure 40. Selecting Evaluation Features to Install

d. In the Instance Configuration window of the wizard, enter **SQL2012** as the name of Microsoft SQL Server 2012 failover cluster, as shown in Figure 41.

Figure 41. Instance Configuration in Server Failover Cluster Wizard

o Support Rules udt Key	Specify a network name for t SQL Server Network Name:	he new SQL Server failover duster. This wil MS5QL2012	I be the name used to identify your failover clus	ter on the network.					
se Terms 5 Role ure Selection ure Rules	 Default instance Named instance: 	MSSQLSERVER							
ance Configuration pace Requirements er Resource Group er Disk Selection	Instance ID: MSSQL2012 Instance root directory: C:/Program Files//Nicosoft SQL Server/								
: Network Configuration Configuration ise Engine Configuration is Services Configuration ing Services Configuration leporting		C\Program Files\Microsoft SQL Server\MS C\Program Files\Microsoft SQL Server\MS C\Program Files\Microsoft SQL Server\MS is and features on this computer:	A511.MS5QL2012						
Installation Rules	Instance	Cluster Network Name	Features	Edition	Version	Instance ID			
to Install	VIM_SQLEXP		SQLEngine, SQLEngine\Replication	Express	10.50.1600.1	M5SQL10_50.VIM_5			
tion Progress te	<shared components=""></shared>	2	SSMS, Adv_SSMS, Conn, BC, IS		10.50.1600.1				

e. In the Cluster Disk Selection window, select **Cluster Disk 1** and **Cluster Disk 3** to store database data and log files. The Cluster Disk 2 resource is already reserved for cluster quorum storage, as shown in Figure 42.

Select shared cluster disk resource	es for your SQL Server failover clust	er.
Setup Support Rules Feature Selection Instance Configuration Disk Space Requirements	Specify the shared disks to b Analysis Services configuratio Cluster Disk 1 Cluster Disk 3	e included in the SQL Server resource cluster group. The first drive will be used as the default drive for all databases, but this can be changed on the Database Engine or IN DBDBS.
uster Resource Group uster Disk Selection uster Network Configuration uster Security Policy rver Configuration tabase Engine Configuration		
ror Reporting uster Installation Rules	Available shared disks:	
Ready to Install Installation Progress	Qualified Disk.	Message
nplete	Cluster Disk 1	
	Cluster Disk 2	The disk resource 'Cluster Disk 2' cannot be used because it is a cluster quorum drive.
	Cluster Disk 3	
		Refresh

Figure 42. Cluster Disk Selection to Store Database Data and Log Files

f. In the Cluster Network Configuration window, select the appropriate cluster network subnet from which the Microsoft SQL Server 2012 cluster IP address can be accessed by internal and external clients. This document uses Cluster Network 2, which is configured with the VLAN 809 management IP address, as shown in Figure 43.

Install a SQL Server Failover Clust Cluster Network Config						1 - Visconconscio.e	1.8.4.9.5.0.40.7.5.1.44T	eneralisti Schill and St. St.	_ 6 ×
Select network resources for your S		r.							275505555525
Setup Support Rules	Specify the network	settings for t	his failover cluster:						1.
Product Key	IP Type	DHCP	Address	Subnet Mask	Network.				
License Terms Feature Selection	IT IPv4	F		255.255.255.0	Cluster Network 1				
Instance Configuration	IPv4		10.104.108.241	255.255.255.0	Cluster Network 2				
Disk Space Requirements									
Cluster Resource Group									
Cluster Disk Selection									
Cluster Network Configuration									
Cluster Security Policy Server Configuration									
Database Engine Configuration									
Analysis Services Configuration									
Reporting Services Configuration									
Error Reporting									
Cluster Installation Rules									
Ready to Install									
Installation Progress									
Complete									
	1								
									Refresh
							< Back Ne	xt > Cancel	Help

Figure 43. Cluster Network Configuration in Server Failover Cluster Wizard

Cluster Network 1 is used to access Microsoft SQL Server 2012 database data and log file storage over the iSCSI network on the Microsoft Windows 2008 R2 **SQLNODE1** and **SQLNODE2** cluster nodes, as shown in Figure 44.



Figure 44. Summary of Cluster Network 1 and Cluster Network 2

g. In the Database Engine Configuration window, select the appropriate storage drive for storing Microsoft SQL Server 2012 user database data and log files. In this setup, the database data directory is set to E:\MSSQL_DATA, which is mapped to the disk created on NetApp iSCSI storage LUN **MS_SQL_DB_LUN**. The user database log directory is set to F:\MSSQL_LOG, which is mapped to the disk created on NetApp iSCSI storage LUN **MS_SQL_LOG_LUN**, as shown in Figure 45.

Install a SQL Server Failover Cluste Database Engine Config				_ 6 ×
Specify Database Engine authentical		d data directories.		15768/6425247
Setup Support Rules Product Key Ucense Tems Feature Selection Instance Configuration Disk Space Requirements Outser Network Configuration Outser Network Configuration Outser Security Policy Server Configuration Database Engine Configuration Analysis Services Configuration Error Reporting Outser Installation Rules Ready to Install Installation Progress Complete	System database directory: User database directory: User database log directory: Temp DB directory: Temp DB log directory:	ctories FILESTREAM E-1 E-1 E-1/MSSQL 10_S0.MSSQLSERVERI/MSSQL[Data E-1/MSSQL 10_S0.MSSQLSERVERI/MSSQL[Data E-1/MSSQL 10_S0.MSSQLSERVERI/MSSQL[Data E-1/MSSQL 10_S0.MSSQLSERVERI/MSSQL[Data E-1/MSSQL 10_S0.MSSQLSERVERI/MSSQL[Data]		
	1		<back next=""> Cancel</back>	Help

Figure 45. Database Engine Configuration Showing Database Directory and Log Directory

Figure 46 shows the two disks used for database data (E:) and log (F:) files, which are mapped to NetApp iSCSI storage LUNs **MS_SQL_DB_LUN** and **MS_SQL_LOG_LUN**, respectively.

File Action View Help																	
Server Manager (VMSQLNODE1)	Disk Management Volume List + Graphical View													Actions			
Roles	Volume			File System		us				0	apacity	Free Space	% Free	Fa			
B gal Peatures B gal Deposition Configuration Storage Windows Server Backup Bick Management	CusterQurom (C CusterQurom (C SQL DBU (H:) SQL DB Log (F:)	Simple :) Simple Simple	Basic Basic Basic Basic	NTFS NTFS CDFS NTFS	Heal Heal Heal Heal		Partition) Partition)	Active, Crash Di	mp, Primary Pa	artition) 40 5. 4. 10	0.00 GB .00 GB .08 GB .00.01 GB	15.87 GB 4.94 GB 0 MB	40 % 99 % 0 % 100 %	No No No No	More Actions	,	
	✓ Disk 0 Basic 40.00 GB Online	(C:) 40.00 GB Healthy (Boot, Page	File, Ac	tive, Crash Du	ump, Primary Parl	ttion)						-			
	Basic 100.01 GB Reserved	SQL Dat 100.01 G Healthy (BNTFS														
	Basic 5.00 GB Reserved	Cluster 5.00 GB M Healthy (NTFS														
	Basic 100.01 GB Reserved	SQL DB I 100.01 G Healthy (BNTFS														
	CD-ROM 0	-												-1	1		

Figure 46. Disks for Database Data and Log Files Mapped to NetApp iSCSI Storage

h. Figure 47 shows a summary of the configuration at the end of the Microsoft SQL Server 2012 failover cluster installation setup.

Figure 47. Summary of Configuration Details at the End of Failover Cluster Installation Setup

Ready to Install			
Verify the SQL Server 2012 RC0	edures to be installed.		
Setup Support Rules	Ready to install the SQL Server 2012 RCO failover duster:		
Product Key	E-Summery		
License Terms	Edition: Evaluation	-	
Setup Role	- Action: InstallFalloverCluster (Product Update)		
Feature Selection	E-Prerequisites		
	i Already installed:		
Feature Rules	- Windows PowerShell 2.0		
Instance Configuration	Microsoft .NET Framework 3.5		
Disk Space Requirements	🖻 To be installed from media:		
Cluster Resource Group	- Microsoft .NET Framework 4.0 (may require reboot)		
Cluster Disk Selection	Microsoft Visual Studio 2010 Shell		
	Microsoft Visual Studio Tools for Applications 3.0		
Cluster Network Configuration	E General Configuration		
Server Configuration			
Database Engine Configuration			
Analysis Services Configuration	- Full Text and Senantic Extractions for Search		
Reporting Services Configuration	· Data Quality Services		
	- Analysis Services		
Error Reporting	- Reporting Services - Native		
Ouster Installation Rules			
Ready to Install			
Installation Progress	Data Quality Client		
Complete			
comporto	- Client Tools Connectivity		
	- Integration Services		
	- Client Tools Backwards Competibility		
	Client Tools SDK		
	- Documentation Components		
	··· Management Tools - Basic		
	Management Tools - Complete		
	Distributed Replay Controller		
	Distributed Replay Client		
	Configuration file path:		
	C:\Program Files\Microsoft SOL Server\110\Setup Bootstrap\Log\20120316_085440\ConfigurationFile.ini		

i. Figure 48 shows completion of Microsoft SQL Server 2012 failover cluster installation on the cluster node **SQLNODE1**.

Complete		
Your 5QL Server 2012 RCO faile	ver cluster installation is complete with product updates.	
ietup Support Rules	Information about the Setup operation or possible next steps:	5.5.4.5.5.5
Product Key	Feature	Status
cense Terms	Management Tools - Complete	Surregard
stup Role	Client Tools Connectivity	Succeeded
ature Selection	Client Tools SDK	Succeeded
ature Rules	Client Tools Backwards Compatibility	Succeeded
ance Configuration	Management Tools - Basic	Succeeded
	SQL Server Data Tools	Succeeded
Space Requirements	Database Engine Services	Succeeded _
ter Resource Group	Q Data Quality Services	Succeeded
ter Disk Selection	V Full-Text and Semantic Extractions for Search	Succeeded
ter Network Configuration	SQL Server Replication	Succeeded
ver Configuration	Master Data Services	Succeeded Succeeded
abase Engine Configuration	Cistributed Replay Client	Succeeded
ysis Services Configuration	K character controlled	Jaccourd
orting Services Configuration	Detais:	
or Reporting	Details:	
ster Installation Rules	Viewing Product Documentation for SQL Server	
dy to Install		
allation Progress nplete		entation for SQL Sever have been installed. By default, the Help Viewer component uses the online library. After ionent to download documentation to your local computer. For more information, see Use Product nkID=224683&clcid=0x409>.
	Microsoft Update	
	For information about how to use Microsoft Update to identify upda	tes for SQL Server "Denali", see the Microsoft Update Web site: <u>http://go.microsoft.com/fwlink/?Linkld=108409</u> .
	Samples	
	Server "Denali", see the CodePlex Web site: http://go.microsoft.co	s part of SQL Server Setup. To install sample databases and sample code for non-Express editions of SQL m <u>/fwim///Link/d=182897</u> . To read about support for SQL Server sample databases and sample code for SQL
	Summary log file has been saved to the following location:	
	CAProgram Files/Microsoft SQL Server1110(Setup Bootstrap)Log(20120316	085440(Summary_VMSQLNCOE2_20120316_085440.bc

Figure 48. Completion of Microsoft SQL Server 2012 Failover Cluster Installation on SQLNODE1

j. To verify that Microsoft SQL Server 2012 failover cluster installation succeeded on the **SQLNODE1** cluster node, launch the Failover Cluster Management console and choose Services and Applications; verify that the **MSSQL2012** instance is added and that the cluster IP address and storage cluster disk status are listed as Online, as shown in Figure 49.

ster Management .tmesql.com SQL Server (MSSQLSERVER)	Becent Cluster Events: 🛕	Warning: Actions
Intrespicon Vices and Appleations SQU Server (MSGUE2 OLEVVER) des SQU SOLEL SQU NODEL SQU NODE2 SQU NODE2 Name Preferred Owner: SQU NODE2 Name Vices Mage Name MSGL2012 Name Vices Mage Current Owner: SQU NODE2 Name C		SQL Server (MSSQLSERVER) SQL Server (MSSQLSERVER) Bring this service or application on Take this service or application of Show the critical events for this at More this service or application to More this service or application Add a shared folder Add a shared folder Add a resoure Show Dependency Report View Delete Rename
Cluster Dirk 3 Volume: (F) Other Resources	Online File System: NTFS	Refresh Properties Heb
GMAnayas Services 은 SQL Server 순 SQL Server Agent	 ① Online ④ Online ④ Online 	Name: HS50,2012
		🗙 Delete
		Properties

Figure 49. Verifying the Storage Cluster Disk Status

k. To verify that the Microsoft SQL Server 2012 failover cluster instance is accessible on the **SQLNODE1** node, launch Microsoft SQL Server Management Studio and connect to the **MSSQL2012** instance and check the start status, as shown in Figure 50.

Figure 50. Verification of Microsoft SQL Server 2012 Failover Cluster Accessibility on SQLNODE1



 Perform the following steps to install Microsoft SQL Server 2012 failover clustering on Microsoft Windows 2008 R2 SP1 cluster host SQLNODE2 as a secondary node to join the primary failover cluster node installed on SQLNODE1.

a. Copy the Microsoft SQL Server 2012 binaries on the Microsoft Windows 2008 R2 **SQLNODE2** cluster node for installation.

b. Log in to **SQLNODE2** with Admin credentials for installing Microsoft SQL Server 2012 software. Launch the Microsoft SQL Server installation .exe file and choose the option **Add node to a Microsoft SQL Server failover cluster**, as shown in Figure 51.

Figure 51. Add Node to Microsoft SQL Server Failover Cluster in SQL Server Installation Center Wizard

🚼 SQL Server Installation Center	
Planning Installation Maintenance Tools Resources Advanced	New SQL Server stand-slone installation or add features to an existing installation Launch a wizard to install SQL Server 2012 RC0 in a non-clustered environment or to add features to an existing SQL Server 2012 RC0 instance. Image: Server failower cluster installation Launch a wizard to install a single node SQL Server 2012 RC0 failower cluster. Image: Add node to a SQL Server failower cluster Image: Launch a wizard to add a node to an existing SQL Server 2012 RC0 failower cluster.
Options	Upgrade from SQL Server 2005, SQL Server 2008 or SQL Server 2000 R2 Launch a wizard to upgrade SQL Server 2006, SQL Server 2008 or SQL Server 2008 R2 to SQL Server 2012 RC0.
SQL Server 2012	

c. In the Add a Failover Cluster Node window, below the **SQL Server instance name** field, select the **MSSQL2012** instance, which was created during the first step of Microsoft SQL Server 2012 failover cluster deployment, as shown in Figure 52.

Cluster Node Configu	ration				_ .
Add a node to an existing SQL S					NULLER CALLER
Setup Support Rules Cluster Node Configuration Cluster Network Configuration	SQL Server ins	itance name: MS	SQLSERVER		
Service Accounts			SQLNODE1		
Error Reporting Add Node Rules Ready to Add Node	Instance Name	Cluster Network Name	Features	Nodes	
Add Node Progress	M5SQLSERVER	M55QL2012	SQLEngine, SQL	YMSQUNODE2	
Complete	_				

Figure 52. Cluster Node Configuration in Failover Cluster Node Wizard

d. In the Cluster Network Configuration window of the wizard, **Cluster Network 2** is automatically selected as the configured IP address during Microsoft SQL Server 2012 failover cluster installation on **SQLNODE1**, as shown in Figure 53.

Figure 53. IP Address of Cluster Network 2

specify downline in addresses (and source (provid	isly-configured SQL Server failover cluster IP addresses are shown read-only a	Constants		
tup Support Rules	Specify the network settings for this failover duster:						
ster Node Configuration Ister Network Configuration	IP Type DHC	Address	5ubnet Mask	Subnet(s)	Network		
vice Accounts	П ІРу4 Г		255.255.255.0	192.191.1.0/24	Cluster Networ		
r Reporting Node Rules	IPv4	10.104.108.241	255.255.255.0	10.104.108.0/24	Cluster Networ		
dy to Add Node							
Node Progress							
plete							
					Mindows could not activate 🔀		

e. Figure 54 shows a summary of the configuration at the end of the installation process.

Figure 54. Summary of Cluster Network Configuration

۵ ۲

f. Figure 55 shows the completion of Microsoft SQL Server 2012 failover cluster installation on cluster node **SQLNODE2**.

Figure 55. Completion of Microsoft SQL Server 2012 Failover Cluster Installation on SQLNODE2

Your SQL Server 2012 RC0 fail	over cluster installation is complete with product updates.	
Setup Support Rules	Information about the Setup operation or possible next steps:	1.2.5.8.4.1
roduct Key	Feature	Status
icense Terms	Management Tools - Complete	Succeeded
etup Role	Client Tools Connectivity	Succeded
eature Selection	Client Tools SDK	Succeeded
sature Rules	Client Tools Backwards Compatibility	Succeeded
stance Configuration	Management Tools - Basic	Succeeded
	SQL Server Data Tools	Succeeded
isk Space Requirements	Database Engine Services	Succeeded
luster Resource Group	Q Data Quality Services	Succeeded
luster Disk Selection	Full-Text and Semantic Extractions for Search	Succeeded
luster Network Configuration	SQL Server Replication	Succeeded
erver Configuration	Master Data Services	Succeeded
atabase Engine Configuration	Distributed Replay Client	Succeeded
	Stributed Replay Controller	Succeeded
nalysis Services Configuration		
eporting Services Configuration	and the second	
rror Reporting	Details:	
luster Installation Rules	Viewing Product Documentation for SQL Server	
eady to Install		1
nstallation Progress		mentation for SQL Server have been installed. By default, the Help Viewer component uses the online library. After
omplete	Documentation for SQL Server. http://go.microsoft.com/fwlink/?l	pponent to download documentation to your local computer. For more information, see Use Product <u>LinkID=224683&clcid=0x409></u> .
	Microsoft Update	
	For information about how to use Microsoft Update to identify upd	ates for SOL Server "Denali", see the Microsoft Update Web site: http://go.microsoft.com/fwink/?LinkId=108409.
	Samples	
		as part of SQL Server Setup. To install sample databases and sample code for non-Express editions of SQL <u>om/Wink/Linkl=182687</u> . To read about support for SQL Server sample databases and sample code for SQL
	Summary log file has been saved to the following location:	
	C:\Program_Files\Microsoft_SOL_Server\110\Setup_Bootstrap\Log\20120316	0854401Summary VMSQLNODE2 20120316 085440.bt

g. Verify that nodes are added to the Microsoft SQL Server 2012 failover cluster on the Microsoft Windows 2008 R2 SP1 host **SQLNODE2** node. Launch the Failover Cluster Management console, and under Services and Applications verify that the **MSSQL2012** instance has been added, that the cluster IP address and storage cluster disks status are listed as "Online", and that under Nodes, both **SQLNODE1** and **SQLNODE2** are listed, as shown in Figure 56.

anagement SQL Server (MSSQL2012)		Recent Cluster Events: 🍌 Error 3 Warring 9	Actions
nd Applications even (MSSQ2012) NODEL NKOE2 Alets: <pre>Summary of SOL Server (MSSU Status: Online Alets: <pre><pre><pre><pre>Status: Online</pre></pre></pre></pre></pre>			SQL Server (MSSQL2012) Bring this service or application online Take this service or application offline Show the critical events for this ap Move this service or application to
r Network 1 Current Owner: VMSQLNODE1 r Network 2			Manage shares and storage
b Name	Status		Add a shared folder
Server Name			🛁 Add storage 🚰 Add a resource
	💿 Online 💿 Online		Show Dependency Report
Disk Drives			View
Volume: (E)	💿 Online File System: NTFS		🔀 Delete 🛒 Rename
E 📼 Cluster Disk 3	Tonline 🕥		G Refresh
Volume: (F)	File System: NTFS		Properties
Other Resources			🔣 Heb
SQL Server (MS5QL2012)	(Online		Cluster Disk 3
SQL Server Agent (MSSQL2012)	(Online		Bring this resource online
			Take this resource offline
			Remove from SQL Server (MSSQL2
			Show the critical events for this res
			Show Dependency Report
			More Actions
			Properties

Figure 56. Verify the Storage Cluster Disk Status and That Both Nodes Are Listed

 Perform the following steps to test failover of Microsoft SQL Server 2012 with the SQLNODE1 and SQLNODE2 cluster nodes.

a. Log in to the **SQLNODE1** cluster node, which currently manages and owns the **MSSQL2012 SQL** instance, as shown in Figure 57. Then shut down the node.

W Help		
Management SOL Servier (MSSOL 2012)	Recent Cluster Events: 🎪 Error 3, Warring: -	Actions
sql.com		SQL Server (MSSQL2012)
s and Applications Summary of SOL Server (MSSOL201	12)	🚓 Bring this service or application online
		🔹 Take this service or application offlir
GUNODEL Status: Unline		Show the critical events for this ap.
Alerts: <none> Preferred Owners: SQLNODE1.' SQLNODE2</none>		Move this service or application to .
ks Preferred Owners: SQLNODE1.' SQLNODE2 stor Network 1 Current Owner: SQLNODE1		Manage shares and storage
ster Network 2		Add a shared folder
Evonts Name	Status	Add storage
Server Name		
🖂 🌁 Name: MSSGL2012	(Online	Add a resource
FIP Address: 10.104.108.241	💽 Online	Show Dependency Report
Disk Drives		View
Cluster Disk 1	(Dnine	🔀 Delate
Volume: (E)	File System: NTFS	🛋 Rename
E 🖙 Cluster Disk 3	(Unline	Refresh
Volume: (F)	File System: NTFS	Properties
Other Resources		🚺 Help
SQL Server (MSSQL2012)	() Unline	Cluster Disk 3
SQL Server Agent (MSSQL2012)	(Online	🚱 Bring this resource online
		Take this resource offline
		Change drive letter
		🙀 Remove from SQL Server (MSSQL2.
		Show the critical events for this res
		Show Dependency Report
		More Actions
		Properties
	•	1 Help

Figure 57. SQLNODE1 Managing and Owning the Microsoft SQL Server 2012 Instance

b. After the shutdown of Microsoft Windows 2008 R2 node **SQLNODE1**, the Microsoft Windows failover cluster should be triggered automatically. Subsequently, the Microsoft SQL Server 2012 cluster resource will fail over to the secondary node, **SQLNODE2**. After the failover, **SQLNODE2** will become the current owner of the Microsoft SQL Server 2012 cluster, as shown in Figure 58.

ver Cluster Management				_ 8
ction View Help				
2 🖬 🛛 🖬				
ver Cluster Management	SQL Server (MSSQL2012)		Recent Cluster Events: 👍 Warning 11	Actions
MSSQL.tmesql.com				SQL Server (MSSQL
SQL Server (M55QL2012)	Summary of SQL Server (MSSQL2012)			🛟 Bring this servic
Nodes				🛟 Take this service
SQLNODE2	Status: Online			B Show the critical
Storage	Alerts: <none> Preferred Owners: ISQLNODE1, SQLNODE2</none>			Move this servic
Cluster Events	Current Owner: SQLNODE2			Manage shares
				Add a shared fol
	Name	Status		Add storage
	Server Name			Add a resource
	□ 🖳 Name: MSSQL2012	💽 Online		Show Dependen
	IP Address: 10.104.108.241	(Online		The second secon
	Disk Drives			
	E Cluster Disk 1	(Online		🔀 Delete
	E Cluster Disk 3	(Online		Rename
	Other Resources			Refresh
	A STATE OF A	O o r		Properties
	SQL Server (MSSQL2012) SQL Server Agent (MSSQL2012)	Online Online		Help
		() child		Name: M55QL2012
				Bring this resour
				Take this resour
				Show the critical
				Show Dependen
				More Actions
				🗙 Delete
				Properties
				Help

Figure 58. Owner of Microsoft SQL Server 2012 Cluster Is SQLNODE2 After Failover

Conclusion

Microsoft Windows 2008 R2 Enterprise x64 and Microsoft SQL Server 2012 x64 introduce many new features and enhancements. This guide presents the best practices to follow to get the best performance and reliability when deploying Microsoft SQL Server 2012 single-host and failover cluster database servers on bare metal with Microsoft Windows 2008 R2 SP1 using a host-based iSCSI initiator on NetApp iSCSI storage on Cisco UCS blade servers.

For More Information

See the following documents for additional information about implementation of Microsoft SQL Server 2012 on Microsoft Windows 2008 R2 SP1 with a NetApp iSCSI storage system on Cisco UCS B-Series Blade Servers:

- Microsoft SQL Server 2012 installation guide: <u>http://msdn.microsoft.com/en-us/library/bb500469%28v=sql.110%29.aspx</u>
- Cisco Nexus QoS switch configuration guide: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/qos/Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide chapter3.html#con 1150612 Cisco UCS hardware and software interoperability matrix: http://www.cisco.com/en/US/docs/unified_computing/ucs/interoperability/matrix/r hcl B rel2 0.pdf



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA