EMC MESSAGING AND COLLABORATION AS A SERVICE SOLUTION

Zimbra Collaboration Server, EMC Atmos, EMC Isilon, EMC VNX, EMC VPLEX, VMware vCloud Director

- Reduces storage costs by 40 percent
- Uses object and unified storage
- Includes federated storage access

Global Solutions Sales

Abstract

This white paper provides information about using EMC® and VMware technologies to create a messaging and collaboration as a service (MCaaS) platform that provides a multitenant solution, and the design considerations related to its implementation. The paper also provides information on how to integrate various components into this MCaaS infrastructure.

September 2013
Zimbra server components........................................................................................................ 25
Mailbox server ..................................................................................................................... 26
MTA (postfix) server .......................................................................................................... 26
LDAP server .......................................................................................................................... 27

Security.................................................................................................................................. 28
Overview ............................................................................................................................... 28
Integrating with a security solution ..................................................................................... 28
Using a vulnerability scanner .............................................................................................. 28
Lessons learned .................................................................................................................. 29
  Aggregating LUNs ........................................................................................................... 30
  Sizing the redo log ......................................................................................................... 30
  Configuring vCPU usage .............................................................................................. 30
  Installing and configuring IFS ..................................................................................... 30
  Disabling Zimbra anti-virus and anti-spam ............................................................... 31
  Generating random emails ......................................................................................... 31

Solution configuration ....................................................................................................... 32
Overview ............................................................................................................................... 32
Storage configuration ......................................................................................................... 32
  VNX configuration ........................................................................................................... 32
    Mailbox server disk layout .......................................................................................... 33
    Mailbox server storage layout and file system requirements .................................. 33
    MTA server storage layout and file system requirements ......................................... 34
    LDAP server storage layout and file system requirements ....................................... 35
  Storage pool ...................................................................................................................... 35
  VPLEX configuration ...................................................................................................... 36
  Atmos configuration ......................................................................................................... 37
  Isilon configuration ......................................................................................................... 37
    Configuring SmartConnect Advanced .................................................................. 38
    DNS configuration ....................................................................................................... 43
    Create NFS exports .................................................................................................... 43
  vSphere configuration .................................................................................................... 47
    VPLEX VASA provider ............................................................................................. 48
    vSphere Storage DRS ............................................................................................... 49
    vCloud Director configuration .................................................................................. 49
    VMware vShield Edge configuration ......................................................................... 51
    VMware vShield Load Balancer configuration ....................................................... 53

Solution integration ............................................................................................................ 54
Overview ............................................................................................................................... 54
Zimbra Server configuration ............................................................................................ 54
Atmos configuration .......................................................................................................... 57
  Creating Atmos tenants ............................................................................................... 57
  Replacing the Atmos web GUI (SSL) certificate ....................................................... 62
Executive summary

Business case

The challenge facing any service provider who wants to enter the messaging and collaboration “as a service” market is that there are competitors who have already-deployed solutions. By having deployed solutions and corresponding market share, these competitors have economies of scale in their solution and can offer them with aggressive price points to customers. Entering a relatively mature market that has low price points and low margins requires a price-competitive solution.

This type of market demands an architecture that:

- Supports a business plan with aggressive pricing
- Provides the recovery point objective (RPO) and recovery time objective (RTO) required by customers
- Scales up as customers purchase additional components for the solution

These challenges pose significant obstacles to developing the business case for the solution. In order to offer a price-competitive solution, costs must be kept as low as possible. Ideally, the solution should allow for an operational expenditure model with little to no capital expenditure investment.

The typical cost-per-GB of storage is high. Minimizing storage cost is usually done by purchasing a large array and fully populating it with drives, providing economic scaling. This requires a significant up-front investment and presents a potential liability, because it could take years to contract enough tenants to consume the array’s entire capacity.

What service providers need is a way to offer a price-competitive solution sized to be deployed with minimal up-front capital expenditure and able to grow through operational expenditure investments. Additionally, the cost of the solution must be profitable within the first twelve months.

The EMC® messaging and collaboration as a service (MCaaS) solution meets these requirements by using EMC and VMware technologies to minimize costs in the following ways:

- **Reducing up-front costs**—The MCaaS solution demonstrates a unique hybrid storage model that combines high-performance block with scale-out object storage to minimize cost-per-GB. It also meets service-level agreements (SLAs) for availability and reliability.

- **Maximizing resource utilization**—The MCaaS solution architecture maximizes the use of purchased equipment. The solution requires less up-front expenditure to deploy by enabling easy scalability as more customers adopt it.
The MCaaS solution is based on Zimbra Collaboration Server (ZCS), EMC Atmos®, EMC Isilon®, EMC VNX®, and EMC VPLEX® and provides cost savings through a scale-out architecture and effective resource utilization.

This solution provides messaging and collaboration services for:

- Organizations looking to move to a cloud-based mail and collaboration solution
- Organizations needing the ability to quickly scale up available mail and collaboration services due to acquisition or seasonal demands
- Distributed organizations looking for a centralized cloud-based mail and collaboration service offering

There are a couple of approaches that can be used to develop the solution’s storage architecture:

- **Monolithic**—Involves the up-front purchase of all equipment required for the next five years to support the solution.
- **Scale-out**—Involves building an architecture that is easily extensible through the integration of additional building blocks as the solution requires additional resources.

The scale-out approach minimizes the initial purchase and depreciation of equipment that will only be partially utilized in the beginning. As an example, even if you pay a premium of 20 percent for the hardware required for the scale-out solution, the return on investment (ROI) is much quicker than the monolithic method.

Figure 1 shows how a scale-out MCaaS architecture based on this solution would not only be profitable almost immediately but would continue to be more profitable than a monolithic architecture, which takes 38 months to generate any profit at all.

This solution implements the concepts of a scale-out architecture by using either Atmos or Isilon as a cost-effective and scalable object, or file, store in combination with EMC VPLEX, which enables the seamless addition of EMC VNX arrays to the storage fabric on an as-needed basis.
The combination of ZCS with Atmos or Isilon and VNX storage provides an optimal collaboration infrastructure. Storage, compute, and network layers maintain high availability, while EMC's building-block sizing approach achieves predictable performance and a repeatable storage design.

**Key results**

Key results confirmed during testing of this solution include:

- A building-block modular solution enables you to add it to an existing system or create a new one.
- Scalability enables you to add components as required so you can purchase only what you need at the time.
- Storage costs are reduced by up to 40 percent because you can buy the types of storage you need based on capacity requirements.
- Object and unified storage enables you to maximize resource utilization.
- Federated storage access enables you to easily add additional capacity as needed.
Introduction

Purpose
This white paper describes the design, implementation, and validation of an EMC MCaaS solution based on ZCS. The paper describes how the solution uses the features and strengths of VMware vCloud Director for resource allocation, Atmos or Isilon for mailbox storage, VNX for operating system (OS) storage, and EMC VPLEX for storage federation.

This multitenant email and collaboration solution has been developed in a modular fashion to enable you to easily size the physical infrastructure needed to support a given user base for your customers. The solution is a hybrid combination of high-speed block storage and scalable object or file storage in a virtualized multitenant environment based on modular building blocks of 5,000 users.

This white paper details three sample tenants of 5,000, 10,000, and 15,000 users.

Scope
This white paper:

- Describes the technologies, hardware and software components, and architecture used in the solution
- Validates the integration of the solution’s components and provides guidelines about how this type of solution can be built and integrated into your environment
- Outlines the configuration of the storage, virtualization, and ZCS for the use cases
- Validates services for users to demonstrate solution scalability and provide best practices for use
- Describes how to configure key components that are not documented in their respective product documentation
- Documents the installation of ZCS and recommends best practices for deploying it in a vCloud Director virtualized environment
- Discusses how to integrate this solution with the industry security best practices around configuration and identity and certification management
- Details non-standard configuration aspects that are essential to the solution

Procedures and configurations for implementing the solution may vary, depending on customer requirements.

For this white paper, the service provider or enterprise components are co-located within one geographic data center environment.

Note: The solution does not have to be co-located, but due to time constraints, we were unable to implement all of the additional components that would be necessary to address the challenges of locating the components in different geographic locations.

1 In this white paper, “we” refers to the EMC Solutions engineering team that validated the solution.
This white paper contributes to, but does not replace, other operational elements, such as systems integration, customization, run books, maintenance, and support. If you need operational guidance outside the scope of this white paper, contact your EMC Global Services and VMware Services representatives.

**Audience**

This white paper is intended for EMC employees, partners, and customers, including service providers, IT planners, system architects and administrators, and any others involved in evaluating, acquiring, managing, operating, or designing a MCaaS infrastructure environment using EMC and VMware technologies.

We assume that you have some familiarity with the concepts and operations related to messaging and virtualization technologies and their use in cloud and data center infrastructures.

**Terminology**

Table 1 defines some of the key terms used in this paper.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOB</td>
<td>Binary Large Object. A generic term for an arbitrary chunk of data.</td>
</tr>
<tr>
<td>Building block</td>
<td>A mailbox server building block represents the amount of storage and server resources required to support a specific number of ZCS users. The amount of required resources is derived from a specific user profile type, mailbox size, and disk requirements.</td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Message Access Protocol</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LMTP</td>
<td>Local Mail Transfer Protocol</td>
</tr>
<tr>
<td>POP</td>
<td>Post Office Protocol</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>Tenant</td>
<td>A customer of compute or storage services. A service provider has multiple tenants within their MCaaS infrastructure. A service provider “Tenant” maps to an Atmos ‘Subtenant.”</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>ZCS</td>
<td>Zimbra Collaboration Server</td>
</tr>
</tbody>
</table>
## Technology overview

### Overview

This section provides an overview of the primary technologies used in this solution:

- Zimbra Collaboration Server
- VMware vCloud Director
- EMC Atmos
- EMC Isilon
- EMC VNX
- EMC VPLEX

### Zimbra Collaboration Server

ZCS is a next generation email, calendar, and collaboration solution that is optimized for VMware. ZCS provides an open platform designed for virtualization and portability across private and public clouds, making it simpler to manage and more cost-effective to scale. With the most innovative web application available, ZCS boosts end-user productivity on any device or desktop—any time, any place—at lower costs compared to other providers. Versions of ZCS include a network edition, an open-source edition, and a prepackaged virtual appliance.

For information on how to configure ZCS, refer to the *Zimbra Collaboration Server Administrator's Guide*.

### VMware vCloud Director

VMware vCloud Director enables customers to build secure, multitenant, hybrid clouds by pooling infrastructure resources into virtual data centers and enabling those resources to be consumed on demand by tenants or users.

Key features of vCloud Director include:

- Virtual data centers
- Multitenant environments
- vCloud networking and security technologies
- Infrastructure service catalog
- Self-service portal
- VMware vCloud API and Open Virtualization Format
- Automation and orchestration

VNX block storage can be directly integrated through VMware vSphere into a vCloud Director environment. However, for Atmos, a Linux Installable File System (IFS) driver is used to enable access to the Atmos file system from the guest operating systems.
Figure 2 shows an overview of vCloud Director.

Figure 2. vCloud Director architecture

For more information on how to configure vCloud Director, refer to the *VMware vCloud Director Administrator’s Guide*.

**EMC Atmos**

EMC Atmos is an object-based cloud storage platform that stores, archives, and accesses unstructured content at scale. Atmos provides the essential building blocks that allow enterprises and service providers to transform to private, hybrid, and public cloud storage.

Key features of Atmos include:

- **Single system**—Efficiently store, manage, and aggregate distributed big data across locations through a single administrative interface. Gain a common view and central management.

- **Seamless scalability**—Add capacity, applications, locations, or tenants to your cloud with zero need to develop or reconfigure. Reduce administration time and ensure availability.

- **Value-based automation**—Use customizable metadata to apply “set-it-and-forget-it” policies to automate data placement and lifecycle, protection methods, and efficiency. Gain support for managing big data at scale.

- **Easy storage access**—Provide flexible access across networks and platforms for traditional applications, web applications, Microsoft Windows, Linux, and mobile devices. Allow users and applications instant access to data from any device.

- **Storage as a service**—Enable enterprises and service providers to meter capacity, bandwidth, and usage across tenants. Enable users to self-manage and access storage.
EMC Isilon

EMC Isilon is a scale-out network-attached storage (NAS) platform. With Isilon you can easily add more nodes to an Isilon cluster to increase capacity and performance. For example, you can scale capacity from a minimum three-node cluster with 18 terabytes capacity, to a 144-node cluster with over 20 petabytes within a single cluster, while greatly simplifying storage and data management.

The EMC Isilon OneFS® operating system combines the three functions of traditional storage architectures—file system, volume manager, and data protection—into one unified software layer, creating a single intelligent file system that spans all nodes within a storage system. OneFS has been designed to simplify administration activities and maintain this simplicity as the overall system scales.

Isilon provides several flexible product lines that can be used in an Isilon cluster:

- **S-Series nodes**—Provides the best performance for high-transactional and IOPS-intensive applications.
- **X-Series nodes**—Provides the right balance between large capacity and high-performance storage.
- **NL-Series nodes**—Provides cost-effective and highly scalable near-line storage.

Isilon can be accessed through various protocols, such as Common Internet File System (CIFS), Network File System (NFS), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Hadoop Distributed File System (HDFS) for Hadoop MapReduce jobs.

Isilon OneFS supports software models to handle additional enterprise-class features such as disaster recovery, quota management, and snapshots. OneFS supports the following features:

- **InsightIQ® (Data Management)**—A powerful, yet simple analytics platform.
- **SmartPools® (Data Management)**—A single file system for multiple tiers.
- **SmartQuotas™ (Data Management)**—Enables you to control and limit storage use, easily provision a single pool of Isilon scale-out storage, and present more storage capacity to applications and users. With SmartQuotas, you can seamlessly partition storage into segments at the cluster, directory, subdirectory, group, and user levels through quota and through provisioning assignments and policies.
- **SmartConnect™ (Data Access)**—Supplies policy-based load balancing with failover.
- **SnapshotIQ™ (Data Protection)**—Supplies simple, scalable, and flexible data protection.
- **Isilon for vCenter (Data Management)**—Manages Isilon functions from vCenter.
- **SyncIQ® (Data Replication)**—Supplies fast and flexible file-based asynchronous replication.

**Note:** Atmos is not a customer-installable product. Documentation on Atmos administration is provided as part of installation services.
- **SmartLock® (Data Retention)**—Supplies policy-based retention and protection against accidental deletion.

- **Aspera for Isilon (High-Performance Content Delivery)**—Supplies high-performance wide area file and content delivery.

Isilon enables you to define protection policies at the file level. This enables you to define less protection for the temporary data and to use the space for protecting important files.

For the purposes of this solution, NFS was used to access the Isilon storage from the mail transfer agent (MTA) guests.

**EMC VNX**

EMC VNX series is high-performing unified storage providing simplicity and efficiency, optimized for virtual applications. With VNX, you achieve higher levels of performance, protection, compliance, and ease of management.

- **Unified**—Uses a single platform for file and block data services. Centralized management makes administration simple. Data efficiency services reduce capacity requirements up to 50 percent.

  **Note:** In this solution, only block data services were used.

- **Optimized**—Uses VMware and Hyper-V integration optimized for virtual applications. Triples the speed of virtualized Microsoft SQL Server and Oracle workloads and starts up to 1,000 virtual desktops in less than eight minutes.

- **High Performance**—Provides high-bandwidth configurations that are ideal for data warehousing.

**EMC VPLEX**

EMC VPLEX implements a distributed virtualization layer to simplify and manage geographically distributed Fibre Channel (FC) based storage area networks (SANs) by providing:

- **Mobility**—Move applications, virtual machines, and data in and between data centers without impacting users.

- **Availability**—Increase your application availability and get non-stop data access by mirroring data across locations.

- **Collaboration**—Access data across multiple data centers simultaneously. Deliver instant data access to support remote users in real time.

- **Federated AccessAnywhere**—With Federated AccessAnywhere cache coherency technology, enjoy a consistent view of data that is presented, shared, accessed, or relocated between VPLEX clusters.

- **Scale-out cluster architecture**—Start small and grow with predictable service levels on a foundation of scalable, highly available processor engines.

In this solution, VPLEX is implemented between the virtualization layer (vSphere) and the physical layer (VNX) to simplify the management of local storage and to enable the improvement of the solution’s availability by adding storage hosted at a remote data center.

For more information about how to configure VPLEX, refer to the *EMC VPLEX Administration Guide*.
Messaging and collaboration as a service

Overview

MCaaS uses cloud infrastructure to provide collaboration services through a shared rather than dedicated infrastructure. Service providers can offer MCaaS to customers who want a flexible, on-demand messaging infrastructure without the need to purchase, configure, or maintain it themselves.

Much like an electric power utility, in which users consume and pay for power without needing to understand or maintain the component devices and infrastructure required to provide the service, in a MCaaS environment, customers can draw on the elastic resources that cloud infrastructure delivers and pay only for what they need.

A MCaaS environment typically consists of:

- Collaboration software
- Secure multitenant storage
- Virtualized multitenant environment

Challenges

This solution focused on two of the most significant challenges in deploying a cloud-based messaging solution:

- Storage costs
- Secure multitenant access

To minimize storage costs in the solution, we separated the high-speed block storage and message storage requirements. The workloads demanding higher IOPS were placed on a small high-speed block storage infrastructure, while the larger storage requirements for messages were placed on an object storage infrastructure. We were able to minimize the size and corresponding cost of the high-performance block-storage array while still providing adequate storage capacity and redundancy.

We addressed the secure multitenant access requirement by using vCloud Director to provide a multitenant-capable secure virtual data center (vDC) environment. In our solution, we deployed a separate vDC for each of the tenants we created.

This solution approaches the challenges of sizing elastic cloud-based workloads by sizing the infrastructure using building blocks.

Collaboration software

For this solution, we chose ZCS because it is built and designed for public and private cloud deployments. This capability, in conjunction with its open-source roots, makes it an ideal solution for organizations that prefer open-source solutions as well as those which require supported software.

Secure multitenant storage

Any public cloud-based solution must have a storage infrastructure that provides secure multitenancy. In this solution, two different types of storage arrays are used. An EMC VNX5100 array is used to provide block storage for higher IOPS workloads. Either an Atmos cloud storage platform or an Isilon scale-out NAS system is used to store all emails and attachments.
In the solution, each tenant's storage is isolated. With the Atmos cloud storage platform, this is done through the creation of a unique “tenant” for each tenant. Similarly, with the Isilon NAS platform, tenant separation is enforced through the creation of tenant-specific folders. In the case of the VNX storage array, this is accomplished through the virtualization capabilities of the platform and the creation of separate LUNs on the array.

This solution uses vCloud Director to build secure multitenant private or public clouds by pooling infrastructure resources into vDCs and exposing them to tenants through web-based portals or program interfaces. By building the solution’s virtualized environment with vSphere and vCloud Director, you can deliver virtual data center environments that are secure and flexible.

As with any public-cloud offering, the efficiency of the underlying compute, network, and storage infrastructures is critical. Virtualizing as many of these resources as possible provides the best opportunity to maximize their utilization. In addition, as secure multitenancy is enforced between vDCs, it is possible for you to enable tenant access, or even tenant administration, of the environment.
Solution architecture

Overview
This section provides a description of the solution architecture, including the hardware and software used.

ZCS architecture
ZCS is designed to provide an end-to-end mail solution that is scalable and highly reliable. The messaging architecture is built with well-known open-system technology and standards, and is composed of a mail server application and a client interface.

Core advantages
ZCS architecture includes the following core advantages:

- Open source integrations: Linux, Jetty, Postfix, MySQL, and OpenLDAP.
- Industry-standard open protocols: SMTP, LMTP, SOAP, XML, IMAP, and POP.
- Modern technology design: Java, JavaScript thin client, and DHTML.
- Horizontal and vertical scalability:
  - Each mailbox server can be scaled horizontally by adding more datastores.
  - Each mailbox server can be scaled vertically by adding more CPU and memory resources to the virtual machines and by using advanced storage array technologies such as thin provisioning.
- High availability support: For cluster integration to provide high availability, Zimbra can use VMware vSphere HA clustering.
- Browser-based client interface: Zimbra Web Client gives users easy access to all the Zimbra features.
- Administration console to manage accounts and servers.

Zimbra application packages
ZCS includes but is not limited to the following application packages:

- Zimbra Core—Includes the libraries, utilities, monitoring tools, and basic configuration files.
- Zimbra LDAP—ZCS uses OpenLDAP software, an open source LDAP directory server. User authentication is provided through OpenLDAP. Each account on the Zimbra Store has a unique mailbox ID that is the primary point of reference to identify the account. The OpenLDAP schema has been customized for ZCS.
- Zimbra Store (Zimbra server)—Includes the components for the mailbox server, including Jetty, which is the servlet container in which the Zimbra software runs. The Zimbra mailbox server includes the following components:
  - Datastore—A MySQL database.
  - Message store—The location where all email message contents and file attachments reside.
  - Index store—Index and search technology provided through Lucene; index files are maintained for each mailbox.
• **Zimbra MTA**—Postfix is the open source MTA that receives email through SMTP and routes each message to the appropriate Zimbra mailbox server using Local Mail Transfer Protocol (LMTP). Zimbra MTA also includes the anti-virus and anti-spam components.

• **Zimbra SNMP**—Installing the Zimbra SNMP package is optional. If you choose to install Zimbra SNMP for monitoring, the package should be run on every Zimbra server.

• **Zimbra Logger**—Installing the Zimbra Logger package is optional. It can be installed on one mailbox server. The Zimbra Logger installs tools for syslog aggregation and reporting. If you do not install the Logger, the server statistics section of the administration console is not displayed.

• **Zimbra Convertd**—The Zimbra Convertd package is installed on the Zimbra Store server. Only one Zimbra Convertd package needs to be present in the Zimbra environment.

• **Zimbra Aspell**—Installing the Zimbra Aspell package is optional. Aspell is the open source spell checker used on the Zimbra Web Client. When Zimbra Aspell is installed, the Zimbra Apache package is also installed.

• **Zimbra Proxy**—Installing the Zimbra Proxy is optional. Use of an IMAP/POP proxy server allows mail retrieval for a domain to be split across multiple Zimbra servers on a per user basis. The Zimbra Proxy package can be installed with the Zimbra LDAP, the Zimbra MTA, the Zimbra mailbox server, or on its own server.

• **Zimbra Memcached**—Memcached is a separate package from Zimbra Proxy and is automatically selected when the Zimbra Proxy package is installed. One server must run Zimbra Memcached when the proxy is in use. All installed Zimbra proxies can use a single memcached server.

• **Zimbra Archiving**—The Zimbra Archiving and Discovery feature is an optional feature for Zimbra Network Edition. Archiving and Discovery offers the ability to store and search all messages that were delivered to or sent by Zimbra. This package includes the cross-mailbox search function, which can be used for both live and archive mailbox searches. Using Archiving and Discovery can trigger additional mailbox license usage.

For a complete list and details about all the available application packages, refer to the Zimbra website.

---

**Zimbra mailbox server architecture**

The Zimbra mailbox server is a dedicated server that manages all mailbox content, including messages, contacts, calendar, briefcase files, and attachments.

Messages are received from Zimbra MTA and are passed through any filters that have been created. Messages are then indexed and deposited into the correct mailbox.

In addition to content management, the Zimbra mailbox server has dedicated volumes for backup and log files. Each Zimbra mailbox server in the system can see only its own storage volumes. Zimbra mailbox servers cannot see, read, or write to another server. In a Zimbra single-server environment, all services are installed on one server, and during installation, the computer is configured to partition the disk to accommodate each of the services.
In a Zimbra multiserver environment, the LDAP, Proxy, and MTA services can be installed on separate servers.

The mailbox server includes the following volumes:

- **Message store (BLOB store):** By default, mail message files are located in `/opt/zimbra/store`
- **Message database:** MySQL database files are located in `/opt/zimbra/db`
- **Redo log:** All message-related activities (including content) are logged in `/opt/zimbra/redolog`
- **Index store:** Index files are located in `/opt/zimbra/index`
- **Backup area:** Full and incremental backups are located in `/opt/zimbra/backup`
- **Log files:** Each component in Zimbra has log files. Local logs are located in `/opt/zimbra/log`

Figure 3 shows the Zimbra mailbox server architecture.

Figure 3.  Zimbra mailbox server architecture

For more information about mailbox server design, refer to Configuring Zimbra server.
The following architectural overview provides a high-level logical view of the environment.

This solution includes several tenants. Each of the tenants was created in a vDC with a suitable number of virtual CPUs, depending on the size of the tenant and availability requirements.

The tenants and sizes are:
- Pluto—5,000 users
- Mercury—10,000 users
- Saturn—15,000 users

Incoming emails are stored directly on either an Atmos or Isilon array, while logs, database indices, and the database are stored on a VNX that is accessed through VPLEX. Only one VNX array is used for this solution.

Figure 4 shows a high-level logical overview of the components included in the solution.

**Figure 4.** Logical architecture of solution components
Figure 5 shows the layout of the physical environment for the solution.

Table 2 lists the hardware resources used in this solution.

Table 2. Hardware resources

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Quantity</th>
<th>Configuration</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC VNX5100</td>
<td>1</td>
<td>VNX Block</td>
<td>• Unified storage is not needed for this solution.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For testing this solution, a VNX5700 configured as a VNX5100 was used.</td>
</tr>
<tr>
<td>EMC Atmos</td>
<td>4</td>
<td>WS2-60</td>
<td></td>
</tr>
<tr>
<td>EMC Isilon</td>
<td>3</td>
<td>NL-Series</td>
<td>Three-node cluster</td>
</tr>
<tr>
<td>EMC VPLEX</td>
<td>1</td>
<td>VPLEX Local</td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td>7</td>
<td>Each with two quad-core 2.54 GHz CPUs and 96 GB of RAM</td>
<td></td>
</tr>
<tr>
<td>LAN switches</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAN switches</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Appendix provides the detailed bill of materials for these components.
Table 3 lists the software resources used in this solution.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere</td>
<td>5.1</td>
</tr>
<tr>
<td>VMware vCloud Suite</td>
<td>5.1</td>
</tr>
<tr>
<td>Zimbra Collaboration Suite</td>
<td>Network Edition 8.0</td>
</tr>
<tr>
<td>EMC Atmos CE</td>
<td>2.1</td>
</tr>
<tr>
<td>EMC Atmos Installable File System</td>
<td>2.1</td>
</tr>
<tr>
<td>EMC Isilon OneFS</td>
<td>7.0.1.5</td>
</tr>
<tr>
<td>EMC FLARE®</td>
<td>5.32.0.5.201</td>
</tr>
<tr>
<td>EMC VPLEX</td>
<td>5.1.0.04.00.04 (firmware)</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux</td>
<td>6.3</td>
</tr>
<tr>
<td>Microsoft Windows Server</td>
<td>2008 R2</td>
</tr>
</tbody>
</table>
**Design considerations**

### Overview

This section contains design considerations, sizing requirements, and best practice recommendations for deploying ZCS in a vCloud-based environment using either Atmos or Isilon, as well as a VNX for storage.

### Sizing and configuring storage

Sizing and configuring a solution for ZCS can be a complicated process. Properly configuring and sizing each solution component guarantees smooth ZCS operation and the best user experience.

**Building block**

We chose to simplify the sizing, configuration, and scalability of a large Zimbra environment by defining a unit of measure—a building block. The building block represents the amount of storage and server resources required to support a specific number of ZCS users. The amount of required resources is derived from a specific user profile type, mailbox size, and disk requirements. Using the building block approach simplifies the design and implementation of ZCS. Once the initial building block is designed, it can be reproduced easily to support the required number of users in any enterprise, based on email environment requirements.

The building-block approach is a common best practice for creating a standalone mailbox server. Servers that are divided into building blocks can simplify server sizing during initial deployment. They also create a reproducible solution using virtual machines with predictable performance patterns.

The building block used in this solution consists of a typical 5,000-user profile on a single virtualized Zimbra mailbox server. You can use similar building blocks for other Zimbra components: LDAP, MTA, and mailbox server. Using this approach, the Zimbra environment can scale to any multiple of 5,000 mailboxes with predictable performance and ease of deployment.

For our scenarios of 5,000, 10,000, and 15,000 users, we deployed a cluster of seven VMware vSphere ESXi hosts.

Table 4 shows the virtual machines we deployed into the ESXi hosts.

<table>
<thead>
<tr>
<th>Virtual machine</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>2/tenant</td>
<td>Running in Multi-Master Replication (MMR) mode</td>
</tr>
<tr>
<td>MTA</td>
<td>2-3/tenant</td>
<td>For load balancing and redundancy through a software load balancer</td>
</tr>
<tr>
<td>Mailbox server</td>
<td>2-3/tenant</td>
<td>Each hosting 5,000 heavy user mailboxes</td>
</tr>
</tbody>
</table>

The building block for mailbox server configuration is more complex than for other Zimbra components, because it involves more parts, such as multiple volumes with different characteristics, user profile type, mailbox size, and disk requirements.
### Designing a building block

To design a building block:

1. Collect the user profile and requirements.
2. Design the building block.
3. Deploy the building block and validate its design.

### Task 1: Collecting the user profile and requirements

To collect the user requirements from the customer, ask the questions listed in Table 5.

#### Table 5. Building block user requirements questionnaire

<table>
<thead>
<tr>
<th>No.</th>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>What is the total number of mailboxes in your environment?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>How many are active mailboxes (what is the concurrency)?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>What is the average message size?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>What is the total number of messages sent and received per user per day?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>What is the mailbox quota per user (MB)?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>What percentage of messages has attachments?</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>What is the average attachment size (KB)?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>What is the average mailbox utilization percentage of quota?</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>What percentage of total users will be using webmail versus POP, IMAP, mobile, or Microsoft Outlook?</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>What is the message delivery peak period in minutes?</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Will you be using Zimbra anti-spam and anti-virus features on Zimbra MTAs?</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Will attachment indexing be used?</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Will the dumpster be enabled?</td>
<td></td>
</tr>
</tbody>
</table>

Accurate answers to these questions are essential for properly sizing your Zimbra servers and storage. Zimbra Professional Services can assist with sizing the mailbox server and storage and will enter the answers into a Zimbra sizing worksheet.

**Note:** The Zimbra sizing worksheet is used only by Zimbra Professional Services.
**Task 2: Designing the building block**

This task involves designing a building block that meets the requirements collected in Task 1. The building block includes storage and server resources.

We used VMware best practices and recommendations to develop our storage architecture. For more information, refer to Storage configuration.

**Task 3: Deploying the building block and validating its design**

After you deploy the building block, the next step is to validate the design using the Zimbra LoadGen testing tool.

**Note:** The LoadGen tool is available only from Zimbra Professional Services.

For details on how we validated the building block design for this solution, refer to Solution validation.

**Zimbra server components**

Using a multinode configuration, we installed and configured the server components, as shown in Table 6, for each 5,000-user building block.

**Table 6. Zimbra server components**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Modules installed and configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox</td>
<td>Installed two servers for load distribution</td>
<td>zimbra-core&lt;br&gt;zimbra-logger&lt;br&gt;zimbra-snmp&lt;br&gt;zimbra-store&lt;br&gt;zimbra-apache&lt;br&gt;zimbra-spell&lt;br&gt;zimbra-convertd&lt;br&gt;zimbra-archiving</td>
</tr>
<tr>
<td>server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTA server</td>
<td>Installed two servers for redundancy and load balancing</td>
<td>zimbra-core&lt;br&gt;zimbra-mta&lt;br&gt;zimbra-proxy</td>
</tr>
<tr>
<td></td>
<td>(We turned off anti-virus and anti-spam because large-scale mail environments usually deploy purpose-built appliances to handle those workloads.)</td>
<td></td>
</tr>
<tr>
<td>LDAP server</td>
<td>Installed two servers in MMR mode</td>
<td>zimbra-core&lt;br&gt;zimbra-ldap&lt;br&gt;zimbra-snmp</td>
</tr>
</tbody>
</table>
**Mailbox server**

We configured the Zimbra mailbox server, as shown in Table 7, for a single 5,000-user building block.

**Table 7. Mailbox server configuration**

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of virtual machines</td>
<td>2 (for load distribution)</td>
</tr>
<tr>
<td>Processor</td>
<td>4 x 2 GHz vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>16 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>Refer to Mailbox server storage layout and file system requirements</td>
</tr>
<tr>
<td>Network</td>
<td>Standard port group</td>
</tr>
<tr>
<td>Mount points</td>
<td>/boot – 500 MB</td>
</tr>
<tr>
<td></td>
<td>swap – 10 GB</td>
</tr>
<tr>
<td></td>
<td>/ – 40 GB</td>
</tr>
<tr>
<td></td>
<td>/opt/zimbra</td>
</tr>
<tr>
<td></td>
<td>/opt/zimbra/backup – on Atmos or Isilon</td>
</tr>
<tr>
<td></td>
<td>/mnt/mauifs – on Atmos</td>
</tr>
<tr>
<td></td>
<td>/opt/zimbra/store1 – on Isilon</td>
</tr>
</tbody>
</table>

**MTA (postfix) server**

We configured the Zimbra MTA server as shown in Table 8.

**Table 8. MTA server configuration**

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of virtual machines</td>
<td>2</td>
</tr>
<tr>
<td>Processor</td>
<td>2 x 2 GHz vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>Refer to MTA server storage layout and file system requirements</td>
</tr>
<tr>
<td>Network</td>
<td>Standard port group</td>
</tr>
<tr>
<td>Mount points</td>
<td>/boot – 500 MB</td>
</tr>
<tr>
<td></td>
<td>swap – 10 GB</td>
</tr>
<tr>
<td></td>
<td>/ – 40 GB</td>
</tr>
<tr>
<td></td>
<td>/opt/zimbra – 10 GB</td>
</tr>
<tr>
<td>Anti-virus and anti-spam</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
**LDAP server**

We configured the Zimbra LDAP (OpenLDAP v3.0) server as shown in Table 9.

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of virtual machines</td>
<td>2</td>
</tr>
<tr>
<td>Processor</td>
<td>2 x 2 GHz vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>Refer to <a href="#">LDAP server storage layout and file system requirements</a></td>
</tr>
<tr>
<td>Network</td>
<td>Standard port group</td>
</tr>
<tr>
<td>Mount points</td>
<td>/boot – 500 MB</td>
</tr>
<tr>
<td></td>
<td>swap – 10 GB</td>
</tr>
<tr>
<td></td>
<td>/ – 40 GB</td>
</tr>
<tr>
<td></td>
<td>/opt/zimbra</td>
</tr>
</tbody>
</table>
Security

Overview

One of the basic tenets of this solution is to ensure that it is implemented not only according to security best practices, but it is also integrated with other EMC security-related solution offerings.

Integrating with a security solution

The “as a service” solution described in the Proven Solutions Guide *EMC Integration of PKI and Authentication Services for Securing Virtualized Environments* deals with the configuration of servers, storage, networking, and security hardware and software components, and provides a resource for you to achieve compliance.

The security solution enables service providers to further enhance a hardened security baseline across hardware and software stacks. In addition, it describes the challenges of securing authentication to further harden the environment through:

- Integration with a public key infrastructure (PKI) to enable stronger authentication and non-repudiation
- Integration with a centralized authentication directory service to enable a centralized point of administration and policy enforcement

We integrated the MCaaS solution with the security solution, with the exception of VPLEX, due to time constraints during testing. All other EMC and VMware components were fully integrated with the central PKI and authentication directory services.

Using a pre-existing virtualized infrastructure security solution in this way eases the configuration and development work you have to do in order to meet customer security requirements, particularly for those customers demanding PCI DSS or other standard compliance.

Using a vulnerability scanner

All environments should be built on top of security best practices. You must ensure that vendor-specific security recommendations are followed. This can be more difficult to do when a software application is made available as a set of pre-built and integrated software components. There is less flexibility in ensuring that the latest versions of software packages, particularly open source software packages, are included.

In the absence of any specific vendor recommendations to mitigate risks, industry best practice guides and resources should also be considered. For example:

- *Center for Internet Security: Security Benchmarks*
- *Department Information Systems Agency (DISA): Security Technical Implementation Guides (STIGs)*
- *National Institute of Standards and Technology (NIST): Computer Security Resource Center – Special Publications*

Note: This is not a complete list of security resources.

Once you install the vendor’s software—for example, in this solution, we installed ZCS—EMC recommends that you use a vulnerability scanner to review the configuration of the systems and look for published vulnerabilities. The reference
for these vulnerabilities is the Common Vulnerability and Exposures (CVE) database, which is a dictionary of publicly known information security vulnerabilities and exposures. Security scanners use a database of CVEs to determine if there are any known vulnerabilities present on a system.

The limitation with vulnerability scanners is that any vulnerabilities they report may be false positives. False positives are reported when the mechanism to test for a vulnerability does not provide exact version and response characteristics. If it is not possible to create an exact test for just the vulnerable software, then the scanning tool may report that a system or software package has vulnerabilities that, in fact, it does not.

As shown in Figure 6, both the **High** and **Medium** warnings discovered by the Security Assistant software were false positives related to the versions of OpenSSL and Python installed on the server.

![Figure 6. Example of false positives with vulnerability scanner software](image)

You must thoroughly review all the results of the security scanning software.

To provide additional protection to the Zimbra instances running in the solution, we also deployed IP tables within the OS and vShield firewalls within each vDC to limit network traffic.

**Lessons learned**

During implementation of the solution we learned important lessons about the following areas:

- Aggregating LUNs
- Sizing the redo log
- Configuring vCPU usage
- Installing and configuring IFS
- Disabling Zimbra anti-virus and anti-spam
- Generating random emails
Aggregating LUNs

During the implementation of the vCloud Director environment, we found that it was better to aggregate the storage into two LUNs—one for higher IOPS workloads, and the other for the Active Directory and templates of the various virtual machines.

Depending on the back-end storage, when using Storage DRS (SDRS), it is sufficient to use fewer larger LUNs. Additional images, templates, media, and so on can reside on additional lower-tier LUNs. vCloud Director sometimes has difficulty correctly allocating storage capacity from a storage profile, so it must use SDRS to balance the usage. For this solution all the storage was fully provisioned. No “thin” provisioning was used.

Sizing the redo log

It is difficult to make specific sizing recommendations for any given environment. Instead, EMC recommends that you develop detailed use case requirements and engage with professional services to detail exact sizing requirements for your environments. The configuration detailed in this white paper should be used only for general guidance. However, one specific suggestion is to ensure that your redo log is adequately sized.

During the load testing done in the development of this solution, the most significant issue we encountered was filling up the redo log. This occurs due to the way in which the redo log is used by Zimbra. Instead of the redo log containing only transactional information, all data is included in the redo log. This, of course, includes all email messages and their attachments, not just their meta data. Therefore, the redo log requires more space than in a typical database deployment.

The active redo log and the archived redo logs must be on the same file system, because when the active redo log is rolled (archived), it is renamed and moved to the archive directory. The archived redo logs remain there until the next backup job runs; then the archived redo logs are incorporated into that backup job. This means that the redo log file system must be large enough to hold all sent and received emails between each backup job.

Configuring vCPU usage

The vCPU configurations and workloads for the 5k and 10k users’ sizes are the same. This is due to the availability requirements inherent in providing the 5k user building block and not because of its computational requirements. Going from 10k to 15k users involves adding two additional vCPUs: one each for an additional mailbox and MTA server.

Installing and configuring IFS

We implemented the solution with IFS on the Linux guest OS to access Atmos. The IFS installation and configuration was done as part of the Atmos installation performed by EMC Service. Here is a general overview of what was done:

- The default /mnt/mauifs for IFS mount point was used.
- The backup mount point (/opt/zimbra/backup) is a symlink to a directory on /mnt/mauifs/xxxx. Production environments should use alternative storage locations.
- Each Mailbox server points to a directory under /mnt/mauifs that is unique to the Atmos subtenant associated with that tenant.
• There are OS tuning options that should be made during IFS installation. These improve the performance of the IFS-accessible storage. Ensure that they are made during the EMC Service installation of Atmos and the IFS agents.

Disabling Zimbra anti-virus and anti-spam
For this solution, we disabled Zimbra's anti-virus and anti-spam modules as most service providers use dedicated hardware appliances to perform those operations. While true for most service providers, enterprise Zimbra customers do use some ASAV capability primarily for outbound messages. Disabling the modules improved the performance of the Zimbra MTAs.

Generating random emails
To validate this solution, we used the open source toolkit Postal from Russell Coker's Documents to generate random emails. We configured it to:

• Generate messages sized between 10 KB and 512 KB of random data.
• Configure five threads, on the mail generating system, dedicated to sending messages.
• Each connection to the MTA was enabled to send up to three messages per connection.
• Two hundred messages a minute were sent for each postal instance.
• Approximately 50 percent of the messages were sent over Secure Socket Layer (SSL) while the rest were sent unencrypted.
• The configuration was stressed by sending emails to and from all the tenant environments simultaneously to simulate internal and external email delivery within and between the tenant environments.
• We used instances running inside each tenant environment (on LDAP servers) that generated over 50 MB/minute of email per instance of Postal. When including all six running LDAP servers, this generated over 300 MB/minute of email, over 18 GB/hour, almost 0.5 TB/day.
Solution configuration

Overview

This section describes how we configured all the system components to work with ZCS.

Storage configuration

Storage configuration directly affects the performance of a Zimbra implementation. This is critical when considering a hybrid solution that uses block and object storage in a highly virtualized environment. Properly sizing both types of storage is essential, as it is for any application's performance. Zimbra, like other messaging and collaboration systems, is an I/O bound application. Storage must be designed to work optimally with the Zimbra application. To do this, you must identify Zimbra’s I/O characteristics, I/O patterns, and read/write ratios.

Zimbra mailbox servers are read/write intensive. Even with RAM and cache appropriately configured on the virtual machines, the message store generates a large amount of disk activity.

This solution used the high-speed block storage capabilities of VNX for:

- A MySQL instance that runs on each message store server and stores metadata (folders, flags, tags, and so on)
- A Lucene search index managed by the Java mailbox process

The BLOB message store managed by the Java mailbox process was stored on the Atmos object store or Isilon cluster.

Because the MySQL instance and the Lucene index generate the most random I/O, they should be serviced by a fast block-storage disk subsystem.

The solution included VPLEX to provide federation of the block storage subsystem in addition to the ability to easily use EMC RecoverPoint in future versions.

VNX configuration

For the storage pool, we configured two LUNs. Each 4.05 TB LUN was spread evenly across the disks. This pool consisted of 32 SAS drives configured as RAID 1/0.

The storage pool hosts all of the tenant virtual machines and Zimbra components. The mail stores are located in Atmos or Isilon.

For each virtual disk or VMDK created, we configured a mount point and then created a file system on the mounted partition. Each VMDK configured for a mailbox server must provide enough performance and capacity to meet user requirements.
Mailbox server disk layout
For this solution, we configured themount points shown in Table 10. This is a
typical layout for a larger deployment.

Table 10. Mailbox server disk layout

<table>
<thead>
<tr>
<th>Volume</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zimbra mount point directory</td>
<td>Anchor for the rest of LUNs; root partition for Zimbra application</td>
<td>/opt/zimbra</td>
</tr>
<tr>
<td>Data store</td>
<td>MySQL database files location (metadata)</td>
<td>/opt/zimbra/db</td>
</tr>
<tr>
<td>Message store (BLOB store)</td>
<td>Default mail message files location (messages, attachments)</td>
<td>/opt/zimbra/store</td>
</tr>
<tr>
<td>Index store</td>
<td>Message index partition for fast user searches</td>
<td>/opt/zimbra/index</td>
</tr>
<tr>
<td>Redo logs</td>
<td>MySQL database log files</td>
<td>/opt/zimbra/redolog</td>
</tr>
<tr>
<td>Log files</td>
<td>General Zimbra log files</td>
<td>/opt/zimbra/log</td>
</tr>
<tr>
<td>Atmos message store</td>
<td>Mail messages and attachments</td>
<td>/opt/zimbra/storeX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/mnt/mauifs/zimbra-msXX</td>
</tr>
<tr>
<td>Backup data</td>
<td>Zimbra backups/archived redo logs—consider backup and other storage options for production implementations</td>
<td>/opt/zimbra/backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>symlink pointed to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/mnt/mauifs/backup/zimbra-msXX</td>
</tr>
</tbody>
</table>

Mailbox server storage layout and file system requirements
We identified the file system requirements, as shown in Table 11.

Table 11. Mailbox server file system requirements

<table>
<thead>
<tr>
<th>Variable</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>User data (store)</td>
<td>10,000 GB user data (10,000 users with 1 GB each)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Database size is determined by message pointers, indexing requirements, calendar data, contact (appointment) data, and so on. IMAP users also use more database.</td>
</tr>
<tr>
<td>MySQL data (database)</td>
<td>500 GB (5% of user data: 0.05 x 10,000 users)</td>
</tr>
<tr>
<td>Zimbra redo log</td>
<td>400 GB (per sizing guidelines)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In typical Zimbra installations, a redo log would be much smaller. However, as this solution does not use Hierarchical Storage Management (HSM) and moves incoming mail directly to either Atmos or Isilon storage, extra space is allocated to handle any backlogs.</td>
</tr>
<tr>
<td>Variable</td>
<td>Requirement</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Indices</td>
<td>2,500 GB (25% of user data: 0.25 x 10,000)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The size is based on attachment indexing being on. Most enterprise customers turn it off. This saves on performance and capacity. With indexing off, the size would not be greater than 5% to 8%. However, language makes a difference, you should double the index estimate for Japanese, Korean, and Chinese characters, that is, 25% would equal 50%, and 8% would equal 16%.</td>
</tr>
<tr>
<td>Zimbra system logs</td>
<td>10 GB</td>
</tr>
<tr>
<td>Zimbra mount point</td>
<td>30 GB</td>
</tr>
</tbody>
</table>

Following Zimbra general sizing guidelines, we defined storage layout for each mailbox server based on a 1 GB mailbox size for each of 5,000 users, as shown in Table 12.

**Table 12. Mailbox server storage layout**

<table>
<thead>
<tr>
<th>Mount point</th>
<th>Size and type</th>
<th>File system</th>
<th>IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>50 GB VXFS (10 GB swap)</td>
<td>Ext3</td>
<td>Low</td>
</tr>
<tr>
<td>/opt/zimbra</td>
<td>30 GB</td>
<td>Ext3</td>
<td>Medium</td>
</tr>
<tr>
<td>/opt/zimbra/db</td>
<td>250 GB</td>
<td>Ext3</td>
<td>High</td>
</tr>
<tr>
<td>/opt/zimbra/redolog</td>
<td>200 GB</td>
<td>Ext3</td>
<td>High/Write</td>
</tr>
<tr>
<td>/opt/zimbra/index (message</td>
<td>1,250 GB</td>
<td>Ext3</td>
<td>High/Write Read</td>
</tr>
<tr>
<td>and attachment)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/opt/zimbra/log (Zimbra system</td>
<td>10 GB VXFS</td>
<td>Ext3</td>
<td>Medium/Write</td>
</tr>
<tr>
<td>logs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/mnt/mauifs/zimbra-msXX (mail store)</td>
<td>Atmos or Isilon</td>
<td>IFS or OneFS</td>
<td></td>
</tr>
<tr>
<td>/mnt/mauifs/backup/zimbra-msXX</td>
<td>Atmos or Isilon</td>
<td>IFS or OneFS</td>
<td></td>
</tr>
<tr>
<td>(backup data)</td>
<td></td>
<td></td>
<td>Medium</td>
</tr>
</tbody>
</table>

**MTA server storage layout and file system requirements**

Following Zimbra general sizing guidelines, we defined storage layout for the MTA server, as shown in Table 13.

**Table 13. MTA server storage layout**

<table>
<thead>
<tr>
<th>Mount point</th>
<th>Size and type</th>
<th>File system</th>
<th>IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>50 GB VXFS</td>
<td>Ext3</td>
<td>Low</td>
</tr>
<tr>
<td>/opt/zimbra</td>
<td>30 GB VXFS</td>
<td>Ext3</td>
<td>Medium</td>
</tr>
<tr>
<td>/opt/zimbra/log</td>
<td>10 GB VXFS</td>
<td>Ext3</td>
<td>Medium</td>
</tr>
<tr>
<td>/opt/zimbra/data</td>
<td>40 GB VXFS</td>
<td>Ext3</td>
<td>High</td>
</tr>
</tbody>
</table>
LDAP server storage layout and file system requirements

Following Zimbra general sizing guidelines, we defined storage layout for the LDAP server, as shown in Table 14.

Table 14. LDAP server storage layout

<table>
<thead>
<tr>
<th>Mount point</th>
<th>Size and type</th>
<th>File system</th>
<th>IOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>50 GB VXFS (10 GB swap)</td>
<td>Ext3</td>
<td>Low</td>
</tr>
<tr>
<td>/opt/zimbra</td>
<td>30 GB VXFS</td>
<td>Ext3</td>
<td>Medium</td>
</tr>
<tr>
<td>/opt/zimbra/log</td>
<td>10 GB VXFS</td>
<td>Ext3</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Storage pool

Figure 7 shows the ZaaS vCD Tenant Pool that we configured for vCloud Director in the VNX storage pool. We presented these LUNs to the VPLEX.

Figure 7. Storage pool
Figure 8 shows the disks that make up the storage pool.

**Figure 8. Storage pool disks**

We used 32 600 GB SAS drives for the storage pool. The disks were configured as RAID 1/0. We kept the disks to the VNX recommended 4+4 configuration for optimal performance and striping.

**Figure 9 shows the virtual volumes being presented to the hosts in a storage view. Storage views are used in VPLEX to mask virtual volumes to the host bus adapters (HBAs).**
Figure 10 shows the masked virtual volumes.

Figure 10. Masked virtual volumes

We used an additional two RAID 6 LUNs in the test environment. These LUNs hosted the vCloud Director catalog items and the virtual machines that were not vital to the performance of the Zimbra application. Virtual machines, such as Windows DCs, were used for tenant Active Directory integration in our solution and also for the security scanner virtual machine that was used to scan for environment vulnerabilities.

The Atmos system is installed by EMC Service based on your requirements and specifications. This includes the configuration of the IFS agents on the Zimbra mail stores as discussed earlier in Installing and configuring IFS. The only customer Atmos configuration, which was performed during the development of this solution, was the creation of tenants and subtenants. The steps involved in configuring these in Atmos are detailed in Solution integration.

The final Atmos configuration that includes the tenants we created for testing appears in the Atmos System Administration Console, as shown in Figure 11.

Figure 11. Atmos configuration with tenants

The EMC Isilon is a customer installable product. However, the setup and initialization of the Isilon array is outside the scope of this document.

This solution uses NFSv4 exports to connect the Zimbra mail stores to the Isilon storage. By default NFSv4 is not enabled.

For this solution we created three NFS exports and mounted them directly on each respective mail store.
We chose not to use quotas in this deployment. However, that is an option and should be considered during the sizing of the production Zimbra environment.

**Configuring SmartConnect Advanced**

EMC Isilon SmartConnect software allows IT managers to meet the demands of an always-on, 24x7 world by providing the highest levels of performance and data availability. With intelligent, automatic client connection load balancing and failover capabilities, SmartConnect simplifies and optimizes scale-out storage performance and data availability.

For NFS environments, SmartConnect provides automated failover and failback and automated rebalance across the cluster in the event of a failure or for ensuring performance. This delivers industry-leading levels of high availability and optimized performance for Isilon scale-out storage solutions.

The following section details the configuration steps that were followed to configure the Isilon nodes into the environment.

1. From **Cluster Management**, on **Network Configuration**, click **Add subnet**, as shown in Figure 12.

![Figure 12. Cluster Management](image)

2. Edit the Subnet Settings with the following details, as shown in Figure 13:
   a. Type the name.
   b. Type the netmask.
   c. Select the MTU.
   d. Type the gateway address.
   e. Type the SmartConnect service IP address.
3. Edit the IP Address Pool Settings with the following details, as shown in Figure 14:
   a. Type the pool name.
   b. Select the access zone.
   c. Add the new IP address range as required.
4. Edit the SmartConnect Settings with the following details, as shown in Figure 15:
   a. Type the zone name.
   b. Select the connection policy.
   c. Select the SmartConnect service subnet.
   d. Select the IP allocation method.
   e. Select the rebalance policy.
   f. Select the IP failover policy.

![SmartConnect Settings](image)

Figure 15. SmartConnect Settings

5. Edit the IP Address Pool Members with the required network interfaces, as shown in Figure 16.

By default, LACP is enabled but needs to be configured on the switch side in order to function.
6. After configuring SmartConnect, the configured settings are displayed on the Network Configuration screen, as shown in Figure 17.
7. Configure DNS by selecting **Edit** from the **Network Configuration** dashboard, as shown in Figure 18.

![Network Configuration Dashboard](image1.png)

**Figure 18. Network Configuration**

8. Add the domain name servers, as shown in Figure 19.

![Configure DNS](image2.png)

**Figure 19. Configure DNS**

9. After configuring DNS, the configured settings are displayed on the Network Configuration screen, as shown in Figure 20.

![DNS Settings](image3.png)

**Figure 20. DNS Settings**
DNS configuration

For SmartConnect to function correctly, create a delegation record on the DNS server, as shown in Figure 21.

Create NFS exports

Create a new directory for each of the NFS exports. To create a new directory, navigate to File System Management and select Add Directory from File System Explorer. Then specify the directory details, as shown in Figure 22.
For this solution we used NFSv4, which is not enabled by default. To enable NFSv4, navigate to Protocols > UNIX Sharing (NFS) > NFS Settings, select the Enabled button for NFSv4 Support, and enter the NFSv4 Domain, as shown in Figure 23. Then click Save.

Figure 23. NFS Service Settings

To create an NFS Export, navigate to Protocols > UNIX Sharing (NFS) > NFS Exports, click Add an export, and enter the appropriate information in the fields. Then click Save.

The following details are required for client access, as shown in Figure 24:

- Clients
- Root Clients
- Directory Paths
UNIX Sharing (NFS)
Manage existing NFS exports or create new exports as you need them to allow clients to access content stored on Isilon clusters.

**Figure 24. Add an NFS Export**
Figure 25 shows the NFS exports we created for this solution.

**Figure 25. Exported file systems**

Figure 26 shows one of the NFS exports we mounted on a mail store.

**Figure 26. Mounted NFS Export**
Figure 27 shows the Zimbra mail store volumes.

To ensure high availability and balanced performance, we configured a vSphere cluster from seven blade servers, each equipped with two quad-core processors and 96 GB of system memory. We configured HA and DRS on the VMware cluster. We did not configure the layout of the virtual machines on the blades as this was managed by vCloud Director.

We configured vSphere as shown in Figure 28.
**VPLEX VASA provider**

VPLEX is included in the solution to provide increased integration for virtual environments and provide easy management of both the virtualized server and storage environments directly from vSphere through integration with vSphere Storage APIs for Storage Awareness (VASA) and vSphere API for Array Integration (VAAI).

The VPLEX VASA provider is a virtual machine that is packaged as an Open Virtualization Format Archive (OVA) file. After you deploy and configure the VPLEX VASA provider vAPP, you must add the VPLEX VASA provider into the vCenter, as shown in Figure 29.

![VPLEX VASA provider](image)

**Figure 29. VPLEX VASA provider**

For details about how to install and configure the VPLEX VASA provider, refer to the VPLEX procedure generator, which is available from [EMC Online Support](#).

Figure 30 shows vCenter recognizing the datastore as a VPLEX Local Non-Distributed Volume. The VPLEX VASA provider also enables VMware users to have visibility into the storage configuration, health status, and functional capabilities of VPLEX.
vSphere Storage DRS

Figure 30 also shows that we enabled vSphere Storage DRS. vSphere Storage DRS provides smart virtual machine placement and load balancing mechanisms based on I/O and space utilization. To take full advantage of this feature, we set the automation policy to “fully automatic,” set the utilized space threshold to 50 percent, and set I/O latency to 15 ms. This means that storage movement will be forced when datastore storage utilization is above 50 percent or I/O latency is above 15 ms.

We wanted to deploy Zimbra in a vCloud Director-based environment to use the native multitenant capabilities of the program. vCloud Director sees the vSphere storage profiles as datastores. All of the tenant organization vDCs, except ZaaS, are built using the allocation pool model.

In the allocation pool model, only a percentage of the resources you allocate are committed to the organization vDC. You can specify the percentage, which enables you to overcommit resources.

Figure 31 shows the datastore clusters and their characteristics as seen by vCloud Director.

The VPLEX performance datastore cluster is the combination of the LUNs we built on the VNX storage pool. This datastore was used to host all of the Zimbra virtual machines for the three tenants deployed in this solution.
The VPLEX virtual machine store datastore was used to host:

- vCloud Director catalog items and the virtual machines not vital to the performance of the Zimbra application
- Virtual machines, such as the Windows DCs, used for tenant Active Directory integration in our solution
- The security scanner virtual machine used to scan the environment for vulnerabilities

As shown in Figure 32, each tenant is contained within their own vCloud Director organization—one for each of the organizations included in our solution. The additional organization, ZaaS, was created to house the service provider virtual machine catalog items and ISO images used to build out the tenants.

![Image of vCloud Director interface with organizations](image1)

**Figure 32. Tenants**

Figure 33 shows the organization vDCs that we created for each of the tenants. These represent the pool of resources allocated to each of the tenants. As stated previously, all of the tenant Org vDCs, except ZaaS, are built using the allocation pool model.

![Image of vCloud Director interface with Organization vDCs](image2)

**Figure 33. Organization vDCs for tenants**
Figure 34 shows the virtual machine templates that we added to the public catalog. These were used for the various tenant components.

![Virtual machine templates](image)

**Figure 34. Virtual machine templates**

Figure 35 shows a complete deployment of the Pluto tenant for a 5,000-user environment.

![Pluto tenant deployment](image)

**Figure 35. Pluto tenant deployment**

The tenants are walled off using VMware vShield Edge gateways in our solution to ensure separation and isolation between tenants. Some network traffic was necessary for the solution to function. In our design, we used three gateways:

- **Admin**—Enabled local communication between the virtual machines and also enabled remote access through an NAT and a firewall rule that we set up.

- **External**—Used for the MTAs. This enabled the MTAs to send and receive emails and client connections.
- **Storage**—Used to give the mail store servers access to the Atmos array or Isilon cluster. This enabled us to mount an Atmos store using IFS or Isilon NFSv4 export.

The gateways for the Pluto environment are shown in Figure 36.

Figure 36. vShield Edge gateways

Figure 37 shows how each of the internal routed networks are walled off by the Edge gateways.

Figure 37. Internal routed networks
As shown in Figure 38, to distribute load equally across the various components of the solution, we configured a load balancer on the external Edge gateways.

To ensure proper Zimbra functionality, configure the ports shown in Figure 39 on the load balancer.

---

**VMware vShield Load Balancer configuration**

**Figure 38. Configuring pool servers on the load balancer**

**Figure 39. Configuring virtual server ports on the load balancer**
Solution integration

Overview

This section details the steps used to configure the solution where the respective product installation or administrative guides do not capture sufficient detail.

Zimbra Server configuration

Several aspects of Zimbra need to be configured in a way that is unique to this solution. Procedures that are performed either by EMC or VMware Service or are well detailed in product literature are not included here.

To configure Zimbra to use Atmos or Isilon as the Primary Message Volume:

1. Log in to the Zimbra admin console.
2. Select Configure > Servers.
3. Select a mailbox server from the list, as shown in Figure 40.
4. Select Volumes, as shown in Figure 41.

Figure 40. Mailbox servers

Figure 41. Volumes
5. To create a new volume, click **Add**, as shown in Figure 42.

![Figure 42. Add a new volume](image)

6. In the **Add New Volume** dialog box, type the Atmos IFS or Isilon NFXv4 mount directory in **Volume Root Path**, as shown in Figure 43, and then click **OK**.

![Figure 43. Volume root path](image)

7. In the **Volumes** window, click **Save**.
8. Select **message 1** from the **Current primary message volume** list, as shown in Figure 44.

![Figure 44. Current primary message volume](image1)

9. Select **Atmos** or **Isilon** from the **Current secondary message volume** list, as shown in Figure 45, and then click **Save**.

![Figure 45. Current secondary message volume](image2)
Atmos is not a customer-installable product; therefore, the EMC Professional Services of a certified third party must perform the system installation.

**Note:** This solution uses secure IFS to connect the Zimbra MTAs to the Atmos storage. If this feature is required and EMC recommends it, then the feature must be enabled during the installation process.

### Creating Atmos tenants

To create a tenant in Atmos:

1. Log in to the Atmos System Administration Console as an administrator.

2. In the navigation pane, expand **Tenant Management**, and then click **Create Tenant**, as shown in Figure 46.

![System Administration Console](image)

*Figure 46. Create tenant*

3. Under **Create Tenant**, select **Local** or **Remote** from the list for **Authentication Source**:
   
   - To use Atmos managed user accounts, select **Local**.
   - To select external LDAP/AD user accounts, select **Remote**.

   All administrators for this tenant use the same **Authentication Source**.

4. If **Remote** was selected in the previous step, select the appropriate option from the list for **Authentication Address**, as shown in Figure 47.
5. Type the **Tenant Name**.

6. Select the appropriate option from the list for **UID Shared Secret Store Provider**, as shown in Figure 48:
   a. For large environments that require an external LDAP server for optimum performance, select **LDAP**.
   b. For smaller or lab environments, select **LockBox**.

7. If you selected **LockBox** in the previous step, in the **Key Provider Confirmation** dialog box, click **OK**.

8. To create the new tenant, click **Submit**.
To configure the newly created tenant:

1. Under **Tenant Management**, in the **Tenant List**, click the tenant name, as shown in Figure 49.

2. Under **Tenant Information**, copy and paste the **Tenant ID** to Notepad or another location, and then click **Add Tenant Admin**.

   The tenant ID is used to access the Atmos storage.

3. Under **Add New Admin**, type the local or remote **User Name** as determined by the **Authentication Source**.

   **Note:** An admin user, local or remote, may only be associated with a single tenant, as shown in Figure 50.

4. For local authentication, if the username does not exist, you can add a new user. In the **Add new user** dialog box, click **Add**.

5. Under **Add New Admin**, complete all user fields, including password if you are using local authentication, password confirmation, email address, mobile number, and phone number, as shown in Figure 51, and then click **Save**.

   The email address will be used for password recovery purposes only.
Atmos best practices recommend that you always create and use a subtenant rather than storing data at the tenant level.

To create a subtenant in Atmos:

1. Log out of the Atmos admin console as the Atmos system administrator, then log in as the tenant administrator.
2. In the navigation pane, expand **Tenant Management**, and then click **Tenant Dashboard**.
3. Under the **Subtenant List**, to create a new subtenant, click **Add**, as shown in Figure 52.

4. Under **Create Subtenant**, select the appropriate option from **Authentication Source**.
5. Type the **Subtenant Name** and then click **Create**.
Note: The subtenant name is only required to be unique within a tenant.

6. In the Tenant Dashboard window, under Subtenant List, click the newly created subtenant.

7. Under Subtenant Information, copy and paste the Subtenant ID to Notepad or another location, as shown in Figure 53.

![Subtenant Information](image)

Figure 53. Subtenant information

The combined tenant ID and subtenant ID are used to access the Atmos storage.

It is usually not necessary to create a subtenant-level administrator.

Policy specification

Policy specification is used to implement your data integrity requirements, as shown in Figure 54. Atmos documentation, support, and EMC Professional Services can help design a policy that meets your data requirements.
Figure 54. Sample default policy

Replacing the Atmos web GUI (SSL) certificate

To generate and install an SSL certificate for Atmos:

1. In Microsoft Active Directory Certificate Services, click Request a certificate.
2. In the Request a Certificate window, click Advanced certificate request.
3. In the Advanced Certificate Request window, click Create and submit a request to this CA.
4. In the Web Access Confirmation dialog box, click Yes.
5. Select the appropriate certificate template from the list under Certificate Template, as shown in Figure 55.
Note: Because the built-in Web Server template does not allow the private key to be exported, you must create another template if you enable this option.

6. In Identifying Information for Offline Template, type the required information, including name, email address, company, department, city, state, and country/region.

7. In Key Options, use security best practices to select options.

8. Select Mark keys as exportable, as shown in Figure 56.

![Figure 56. Mark keys as exportable](image)

9. If required, add Subject Alternative Name (SAN) details in Attributes, as shown in Figure 57, for example:

   SAN: dns=atmos1.drm.lab.esg.local&dns=10.110.46.11&dns=atmos1-is1-001

![Figure 57. SAN attributes](image)

10. Click Submit.

11. In the Web Access Confirmation dialog box, click Yes.

12. In the Certificate Issued window, click Install this certificate.

13. When the certificate is installed, in your system where the certificate was generated, start the Certificate Manager GUI.
14. Under **Certificates** - **Current User**, expand **Personal**, click **Certificates**, then right-click the certificate and select **All Tasks > Export**, as shown in Figure 58.

15. The **Certificate Export Wizard** opens. To continue, click **Next**.

16. To ensure that the private key is exported and managed according to your organization’s best practices, in the **Export Private Key** window, select **Yes**, export the private key.

17. In the **Export File Format** window, under **Personal Information Exchange - PKCS #12 (.PFX)**, select **Include all certificates in the certification path if possible**, as shown in Figure 59.
This automatically includes the root CA and any intermediate certificates. Click **Next**.

18. Follow industry best practices and set a password to protect the private key. In the **Password** window, type and confirm a password, then click **Next**.

19. In the **File to Export** window, type the name of the file you want to export in the PFX format, as shown in Figure 60. This file contains the private key, server certificate, root CA certificate, and any intermediate certificates. Click **Next**.

![Figure 60. Export certificate](image)

20. In the **Completing the Certificate Export Wizard** window, click **Finish**. A confirmation message is displayed.

After the certificate is exported, convert the file and import it to Atmos:

1. Using OpenSSL on any Windows or Linux system, convert the exported PFX file to the PEM format.

   For example, to convert `atmos1.pfx` to `atmos1.pem`, type:
   ```
   openssl.exe pkcs12 -in atmos1.pfx -out atmos1.pem
   ```

2. Type the **Import Password** used to export the private key. Verify the password: **MAC verified OK**.

3. Type the PEM pass phrase to protect the private key in the new file.

4. Type the PEM pass phrase again to encrypt the private key in the new file.
5. Verify there were no errors, as shown in Figure 61.

![Figure 61. Verifying pass phrase for PEM file](image)

6. Exit the OpenSSL window.

7. Log in to the Atmos admin console as the administrator.

8. In the navigation pane, expand **System Management ➔ Configuration ➔ Security.** Then click **SSL,** as shown in Figure 62.

![Figure 62. System dashboard](image)

9. In **Update Management GUI SSL Certificate,** locate and select the same PEM file for each of the following fields, as shown in Figure 63:
   - Certificate Key File
   - Server Certificate File
   - Certificate of Trusted Root CA
   - Certificate Chain of CAs
10. Click **Submit**.
11. Log out and reload the GUI to verify the new certificate is installed.
12. In the **Certificate** dialog box, on the **Details** tab, verify that the SAN parameter (if used) matches your requirements, as shown in Figure 64. Then click **OK**.

![Figure 63. Adding the PEM file](image)

![Figure 64. SAN parameter](image)
13. In the Certificate dialog box, on the Certification Path tab, verify the certificate chain, as shown in Figure 65. Then click OK.

![Certificate chain](image)

**Figure 65. Certificate chain**

**Configuring Atmos Secure LDAP**

This section details how to configure the Atmos components of the solution to use Secure LDAP against an Active Directory server. Secure LDAP uses SSL to encrypt user credentials and passwords while they are transmitted across the network.

To configure Atmos to use Secure LDAP:

1. To create a new administrator user, log into Atmos as SecureAdmin.
3. In Assign System Admin Role, select Remote for Authentication Source, and then click Assign.
4. For Remote Address, click Add, as shown in Figure 66.

![Add remote address](image)

**Figure 66. Add remote address**
5. In **Remote LDAP Configuration**, configure remote LDAP for secure LDAP/SSL, as shown in Figure 67 and Table 15.

![Remote LDAP Configuration](image)

**Figure 67.** Remote LDAP

**Note:** Some of your data may not match the example values shown.

**Table 15.** Sample data for configuring remote LDAP for secure LDAP/SSL

<table>
<thead>
<tr>
<th>Field</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Name</td>
<td>Usually set to “short” Active Directory domain name, as it must be manually entered by administrators when logging in</td>
</tr>
<tr>
<td>Bind DN</td>
<td>LDAP DN path for AD User created to access LDAP on AD domain</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Password for bind user</td>
</tr>
<tr>
<td>Server Name</td>
<td>IP address or DNS name of AD domain</td>
</tr>
<tr>
<td>LDAP Debug Level</td>
<td>0 - for no debug logging</td>
</tr>
<tr>
<td>Protocol</td>
<td>Idaps – for LDAP over SSL</td>
</tr>
<tr>
<td>Port Number</td>
<td>636 for LDAPs</td>
</tr>
<tr>
<td>LDAP Timeout</td>
<td>Example, 5,000 ms</td>
</tr>
<tr>
<td>User Search Path</td>
<td>LDAP DN path for AD Users</td>
</tr>
<tr>
<td>Field</td>
<td>Data</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Group Search Path</td>
<td>LDAP DN path for AD Groups</td>
</tr>
<tr>
<td>User Object Class</td>
<td>User – LDAP object class for users</td>
</tr>
<tr>
<td>User ID Attribute</td>
<td>sAMAccountName – LDAP attribute to match Atmos username with sAMAccountName to match the AD username</td>
</tr>
<tr>
<td>Group Object Class</td>
<td>Group – LDAP object class for groups</td>
</tr>
<tr>
<td>Group Member Attribute</td>
<td>Member – LDAP attribute to test group membership against</td>
</tr>
</tbody>
</table>

6. Use the newly added remote authentication source to create a remotely authenticated admin user. In **Assign System Admin Role**, click **Assign**, as shown in Figure 68.

![Figure 68. Create remotely authenticated admin user](image)

7. Log in to Atmos using remote authentication. When logging in, users must change **Auth Type** to **Remote** and manually specify the **Auth Address**, which will be the same as the **Remote Address**, as shown in Figure 69.

![Figure 69. Login information](image)
Solution validation

Overview
This section discusses how we validated the solution to ensure that the components were sized correctly. This provided an infrastructure capable of supporting 30,000 users. Details on the tool used during testing and detailed test results are included.

Notes
Benchmark results are highly dependent on workload, specific application requirements, and system design and implementation. Relative system performance will vary as a result of these and other factors. Therefore, this workload should not be used as a substitute for a specific customer application benchmark when critical capacity planning and/or product evaluation decisions are contemplated.

All performance data contained in this report was obtained in a rigorously controlled environment. Results obtained in other operating environments may vary significantly.

EMC Corporation does not warrant or represent that a user can or will achieve similar performance expressed in transactions per minute.

Test environment and workloads
We validated the solution environment through the use of an SMTP-based load generator called Postal. This is an open source tool capable of generating random emails and delivering them through SMTP, SMTP (TLS/SSL), or LMTP.

An additional testing tool that can test other aspects of a Zimbra solution is available from Zimbra Professional Services.

Test procedures
The Postal configuration used to load-test the environment was configured as follows:

- Messages of random size containing between 10 KB and 512 KB were generated
- Each Postal server contained five threads that sent messages simultaneously
- Each connection to the MTA could send up to three messages
- On average, 200 messages a minute were sent per instance
- Six Postal servers were deployed using the two LDAP servers in each environment. These servers were used simultaneously to generate over 50 MB/minute per instance of email to six MTAs
- Messages were sent over a 50/50 mix of SSL and clear text
- Emails were sent to and through all three environments simultaneously to simulate internal and external email delivery within and between environments
- MTAs delivered email to the internal mail server or to the external MTAs
- With all LDAP servers running, this generated over 300 MB per minute of email, which is over 18 GB per hour and almost 0.5 TB per day

We followed industry best practice recommendations for the configuration of the compute, network, and storage environments.
The configuration used in validating this solution consisted of only four Gen2 Atmos nodes. Because these have only 1 Gb Ethernet interfaces, channel bonding was implemented to combine three 1 Gb Ethernet ports on each of the four Atmos nodes to improve the network throughput. Gen3 Atmos nodes come with two 10 Gb Ethernet ports, so this should be less of an issue. In addition, any production configuration should consist of at least eight nodes based on Atmos recommendations.

EMC recommends that configurations are validated by the Atmos team prior to purchase.

Test results

Once configured, the solution was load tested by Postal for approximately one week.

Atmos test results

Of the performance metrics pulled from the environment over that time, only the Atmos network reported values close to saturation.

Figure 70 shows the load on the Ethernet interfaces of the Atmos cluster.

![Network load on atmos1 cluster](image)

Figure 70 also shows a seven-day record of incoming and outgoing network load testing. The interesting data in this graph are the green peaks, which are due to the Zimbra daily backup processing of the redo logs. This is a significant processing requirement and is quite high, mainly due to the load being generated by Postal.
The peak of 58 MB is near saturation for a single 1 Gb Ethernet link. While Postal is introducing 300 MB per minute of email (or 300 MB * 8/60 = 40 Kb per second), Atmos creates two synchronous replica copies of each object it stores. This replication traffic is sent through the external network interfaces to the other Atmos nodes and accounts for the balance of network traffic. In addition, Postal was running during the backup/redo log processing.

Based on our testing, the use of an eight-node Atmos environment should be considered minimal and scaled up accordingly, based on the number of users planned for the environment.

Figure 71 shows the CPU load on the atmos1 cluster. Typically, utilization is quite reasonable with only one CPU hitting 50+ percent utilization during load testing.

![Figure 71. CPU load on atmos1 cluster](image)

Figure 77 shows the load across the entire cluster. At an average CPU load of 10 processes, the system was able to handle the requested load.

**Isilon test results**

EMC Isilon InsightIQ software provides powerful performance monitoring and reporting tools to help you maximize the performance of your EMC Isilon scale-out storage system. InsightIQ includes innovative, advanced analytics to optimize applications, correlate workflow and network events, and accurately forecast future storage needs.
As shown in Figure 72, the generated load contributed toward a maximum CPU load of ~25%. This demonstrates that the Isilon was able to handle the workload with ease and that CPU constraint was not an issue.

Figure 72.  
**CPU usage**

Figure 73 shows the external network throughput captured by the Isilon. Of the available 30 Gb/s bandwidth in our Isilon configuration, we noticed an average load of ~180 Mb/s. The network spike of ~1.2 Gb/s captured by InsightIQ occurred during a backup operation performed by Zimbra.

Figure 73.  
**Network throughput**

In our test deployment we also configured the Isilon as a backup target. However, we recommend that customers consider backup and other storage options for backup retention in production implementations. The test results show that when using the 10 GE interfaces on the Isilon array, a network bottleneck is not an area of concern.

Figure 74 shows combined live network throughput.

Figure 74.  
**Live network throughput**
Figure 75 shows the total disk throughput in MBs. The average load is around 250 Mb/s, with the spike of up to ~1.5 Gb/s during a backup. This shows that the Isilon was successfully able to keep up with the load.

![Disk Throughput](image1)

**Figure 75. Disk throughput**

Figure 76 shows the average disk IOPS performed by the cluster. During testing we observed an average peak of ~3800 IOPS. Our solution consists of three NL400 nodes that can support a maximum of ~9600 IOPS (number of drives x 100 IOPS). Therefore, our cluster was well below the maximum supported IOPS threshold at around 40 percent.

![Disk IOPS](image2)

**Figure 76. Disk IOPS**

**VNX test results**

Of the performance metrics pulled from the environment during the Postal testing the VNX array was never fully saturated. The following graphs provide additional details. These results were generated while the VNX was configured with the Atmos array; however similar results were generated when the Isilon array was used for mail binary large object (BLOB) storage.

Figure 77 shows the load across the entire cluster.
Figure 77. Process load across entire cluster

Figure 78 shows the utilization of the various Zimbra disks served by the VNX storage array. The disks are:

- SCSI0:3 = /opt/zimbra/db
- SCSI0:4 = /opt/zimbra/index
- SCSI0:5 = /opt/zimbra/redolog

There was high read (1,000 KB/s) and write (1,736 KB/s) utilization on the index partition and high write (1,477 KB/s) on the database, while the redo log partition only consumed medium write (796 KB/s) bandwidth.

The report shown in Figure 78 was generated from data captured when the system delivered email directly to Atmos storage as the primary message store.
Figure 78. Zimbra disk performance

Figure 79 shows the virtual machine and server utilization. The average CPU utilization was 36.1 percent, and the virtual machine utilization was 63.7 percent.

Figure 79. Virtual machine and server utilization
Conclusion

Summary

This EMC MCaaS solution provides you with a modular hybrid block and object storage solution based on ZCS and either EMC Atmos or EMC Isilon BLOB storage. This solution also:

• Enables you to provide robust email and collaboration services
• Provides a reference implementation for delivering messaging and collaboration services that use your existing orchestration and portal infrastructure
• Provides the elastic, cost-effective, and multitenant email and collaboration capabilities that customers demand

Findings

Key results confirmed during testing of this solution include:

• A building-block modular solution enables you to add it to an existing system or create a new one
• Scalability enables you to add components as required so you can purchase only what you need at the time
• Storage costs are reduced by up to 40 percent because you can buy the types of storage you need based on capacity requirements
• Object and unified storage enables you to maximize resource utilization
• Federated storage access enables you to easily add additional capacity as needed
References

**EMC documentation**

For additional information, see the documents listed below. EMC documents are available on the [EMC Online Support](https://www.emc.com) website.

- *EMC Compute as a Service White Paper*
- *EMC Compute as a Service: Design Principles and Consideration for Deployment White Paper*
- *EMC Design Principles and Considerations for Configuring VMware vShield in Service Provider Environments White Paper*
- *EMC Storage Design and Data Protection for Zimbra Collaboration Server White Paper*
- *EMC Integration of PKI and Authentication Services for Securing Virtualized Environments Proven Solution Guide*
- *EMC VPLEX Administration Guide*

**Other documentation**

For additional information, see the documents on the [VMware](https://www.vmware.com) or [Zimbra](https://www.zimbra.com) website related to the products listed below.

- VMware vCloud Director
- VMware vSphere
- Zimbra Collaboration Server
MCaaS can be deployed in many different configurations depending on service provider and customer requirements. A baseline configuration for 30,000 users is provided below. It was built on the assumptions used throughout this white paper. Any combination of the 5,000-, 10,000-, and 15,000-user building blocks described in this white paper can be used to reach 30,000 users.

EMC recommends that service providers interested in deploying this solution engage consulting services to ensure that the environment is sized appropriately for the anticipated workloads. Consulting support is specifically recommended to determine Zimbra and Atmos configurations.

Table 16 shows the configuration for 30,000 users.

**Table 16. 30,000-user baseline configuration**

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Product ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Atmos software 120 TB</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>COS-SW-ENTL</td>
<td>Atmos SW License Key</td>
</tr>
<tr>
<td>120</td>
<td>COS-SW-SOL</td>
<td>Atmos SW Base 1 TB (1-500 TB)</td>
</tr>
<tr>
<td>1</td>
<td>SAMBA GPLV3</td>
<td>SAMBA GPLV3 Toolset various products</td>
</tr>
<tr>
<td>1</td>
<td>OMSA-TOOL-SET</td>
<td>GPLV3 DELL OMSA Toolset various products</td>
</tr>
<tr>
<td>1</td>
<td>M-PRESW-009</td>
<td>Premium Software Support Includes months 1-60</td>
</tr>
<tr>
<td><strong>Atmos hardware WS2-120 4N</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>BDX20K-RACKT</td>
<td>RACK 40UT 2DROP HAPW MFG QTY1 G1</td>
</tr>
<tr>
<td>8</td>
<td>BDX20K-DAE-HT</td>
<td>DAE 15 1T SATA 7.2K HAPW MFG QTY1 G1</td>
</tr>
<tr>
<td>2</td>
<td>A-PW40U-US</td>
<td>CBLE PWR L6-30A US QTY2 G2</td>
</tr>
<tr>
<td>2</td>
<td>BDX20K-SW-HT</td>
<td>SWCH 1GBE 24P HAPW MFG QTY1 G1</td>
</tr>
<tr>
<td>4</td>
<td>A-S-DP-1GHT</td>
<td>SVR 1U 1GBE HAPW MFG QTY2 G2</td>
</tr>
<tr>
<td>2</td>
<td>M-PREHW-001</td>
<td>Premium hardware support Includes months 37-60</td>
</tr>
<tr>
<td>2</td>
<td>WU-PREHW-001</td>
<td>Premium hardware support - WARR UPG</td>
</tr>
<tr>
<td><strong>VNX 5100 - Zimbra Performance Module</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>VNX51D156015F</td>
<td>VNX5100 DPE; 15x3.5 DRV-FLD INST 6X600</td>
</tr>
<tr>
<td>4</td>
<td>V31-DAE-N-15</td>
<td>3U DAE with 15 x 3.5-inch drive slots</td>
</tr>
<tr>
<td>66</td>
<td>V3-VS15-600</td>
<td>600 GB 15K SAS disk drive</td>
</tr>
<tr>
<td>1</td>
<td>VNXFCSFPS</td>
<td>Additional 8 G FC SFP for VNX5100/5300</td>
</tr>
<tr>
<td>1</td>
<td>VNX51-KIT</td>
<td>Documentation kit for VNX5100</td>
</tr>
<tr>
<td>1</td>
<td>VNXSPSAS</td>
<td>Second optional SPS for VNX5100/5300</td>
</tr>
<tr>
<td>Quantity</td>
<td>Product ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>456-103-617</td>
<td>DPA Replication Analysis: VNX5100 (Block)</td>
</tr>
<tr>
<td>1</td>
<td>456-005-702</td>
<td>Replication Manager: VNX5100</td>
</tr>
<tr>
<td>1</td>
<td>ESRS-GW-200</td>
<td>EMC Secure Remote Support Gateway Client</td>
</tr>
<tr>
<td>1</td>
<td>UNIB-V51</td>
<td>Unisphere Block and VNX OE VNX5100</td>
</tr>
<tr>
<td>1</td>
<td>PPAK-V51</td>
<td>Total Protection Pack for VNX5100</td>
</tr>
<tr>
<td>1</td>
<td>PS-PKG-LEBD</td>
<td>VNX - Basic Install-Implement Block BoE Complete: YES</td>
</tr>
<tr>
<td>1</td>
<td>PS-PKG-IMLPB</td>
<td>VNX - SnapView SnapSure Implement BoE Complete: YES</td>
</tr>
<tr>
<td>1</td>
<td>PS-PKG-IMRPB</td>
<td>VNX Block - MirrorView Implement BoE Complete: YES</td>
</tr>
<tr>
<td>2</td>
<td>PS-BAS-ADDAE</td>
<td>Rack and stack of up to 2 DAE BoE Complete: YES</td>
</tr>
<tr>
<td>1</td>
<td>M-PREHW-001</td>
<td>Premium hardware support Includes months 37-60</td>
</tr>
<tr>
<td>1</td>
<td>M-PRESW-001</td>
<td>Premium software support Includes months 1-60</td>
</tr>
<tr>
<td>1</td>
<td>M-PRESW-011</td>
<td>Premium software support - Platform/ELM Includes months 1-60</td>
</tr>
<tr>
<td>1</td>
<td>WU-PREHW-001</td>
<td>Premium hardware support - WARR UPG</td>
</tr>
</tbody>
</table>

**VPLEX**

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Product ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VS2-02-RACK</td>
<td>VPLEX VS2 Single Config Rack (Titan)</td>
</tr>
<tr>
<td>1</td>
<td>VS2-ENG-BASE</td>
<td>VPLEX VS2 Base Engine</td>
</tr>
<tr>
<td>1</td>
<td>VS2-PW40U-US</td>
<td>30A 1PH L6-30P N.AMER; Japan</td>
</tr>
<tr>
<td>1</td>
<td>VS2-SERVER</td>
<td>VPLEX VS2 Management Server</td>
</tr>
<tr>
<td>1</td>
<td>VS2-FM8GFC</td>
<td>8 Gb FC front-end I/O modules</td>
</tr>
<tr>
<td>1</td>
<td>ESRS-GW-200</td>
<td>EMC Secure Remote Support Gateway Client</td>
</tr>
<tr>
<td>1</td>
<td>PP-SE-VPLEX</td>
<td>PowerPath SE for VPLEX</td>
</tr>
<tr>
<td>1</td>
<td>VS-LOC-PBASE</td>
<td>VPLEX Local Base (Incl. 10 TB)</td>
</tr>
<tr>
<td>1</td>
<td>VS-OS-GPL3</td>
<td>NP ASSY VPLEX; OS GPLV3 SW; No charge</td>
</tr>
<tr>
<td>1</td>
<td>VS-OS-NONGPL3</td>
<td>NP VPLEX; OS NON GPLV3 SW; No charge</td>
</tr>
<tr>
<td>1</td>
<td>VS-GSN-PBASE</td>
<td>VPLEX GeoSynchrony Base (Incl. 10 TB)</td>
</tr>
<tr>
<td>7</td>
<td>VS-GSN-T2LIC</td>
<td>VPLEX GeoSynchrony 1 TB (15-25TB)</td>
</tr>
<tr>
<td>1</td>
<td>PS-BAS-VPLEX</td>
<td>EMC Design and Imp. for V-PLEX QS BoE Complete : YES</td>
</tr>
</tbody>
</table>
### Table 17. Isilon three-node baseline configuration

<table>
<thead>
<tr>
<th>Product ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pool 1 cluster</strong></td>
<td></td>
</tr>
<tr>
<td>NL400 node</td>
<td>36 TB HDD, 24 GB, 4 x 1 GE</td>
</tr>
<tr>
<td>Nodes</td>
<td>3</td>
</tr>
<tr>
<td>OneFS</td>
<td>7.0, +2:1</td>
</tr>
<tr>
<td>Switch</td>
<td>Mellanox IS5022 (eight-port)</td>
</tr>
<tr>
<td><strong>Pool 1 data on HDD</strong></td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>72 GB</td>
</tr>
<tr>
<td>CPUs</td>
<td>6</td>
</tr>
<tr>
<td>Cores</td>
<td>24</td>
</tr>
<tr>
<td>Raw HDD</td>
<td>108 TB</td>
</tr>
<tr>
<td>Usable HDD</td>
<td>64.9 TB</td>
</tr>
<tr>
<td>Number of HDD drives</td>
<td>108</td>
</tr>
<tr>
<td>Usable HDD at 80% utilization</td>
<td>52 TB</td>
</tr>
<tr>
<td>Protection overhead</td>
<td>33.3%</td>
</tr>
</tbody>
</table>