Hybrid Cloud Solution: Deploy and Scale an E-Business Application with Cisco Intercloud Fabric for Business Whitepaper
Contents

Goal of This Document.................................................................4
Audience.......................................................................................4
Introduction..................................................................................4
Cisco Intercloud Fabric Overview..................................................5
  Intercloud Fabric Director..........................................................5
  Cisco Prime Network Services Controller.................................6
  Secure Cloud Extension............................................................6
E-Business Application Overview..................................................7
System Components .....................................................................8
Application Deployment and Cisco Intercloud Fabric Architecture......9
  Design Requirements ................................................................9
  Network Design........................................................................10
  Application Deployment Across Hybrid Cloud............................12
Implementation and Configuration Details.......................................14
  Enterprise Environment Overview..............................................14
  Cisco Intercloud Fabric Deployment..........................................15
  E-Commerce Application Implementation....................................21
  Application Scaling....................................................................28
Conclusion ....................................................................................37
For More Information ..................................................................37

Figures

Figure 1. Cisco Intercloud Fabric Architecture ................................5
Figure 2. osCommerce Sample Website .........................................8
Figure 3. osCommerce Deployment Overview ................................9
Figure 4. Application Network Design..........................................10
Figure 5. Cisco Intercloud Fabric Data Center Network Configuration 11
Figure 6. Application Deployment Across Hybrid Cloud..................12
Figure 7. Intercloud Fabric Director: Cloud Virtual Machine Catalog Item .13
Figure 8. Topology Overview .......................................................14
Figure 9. Cisco Intercloud Fabric for Business Licensing................15
Figure 10. Cisco Intercloud Fabric Infrastructure Setup ..................16
Figure 11. Confirmation Summary ..............................................16
Figure 12. Cisco Intercloud Fabric Infrastructure Policies ................18
Figure 13. Cisco Intercloud Fabric Tunnel Profile..........................19
Figure 14. Port Groups in VMware vSphere Distributed Switch .......20
Figure 15. Cisco Intercloud Fabric Setup.....................................20
Figure 16. osCommerce New Installation ......................................23
Figure 17. osCommerce Database Parameters .............................24
Figure 18. osCommerce Web Server Settings ........................................... 25
Figure 19. osCommerce Online Store Settings ....................................... 25
Figure 20. osCommerce Installation Finished .......................................... 26
Figure 21. osCommerce Online Store ...................................................... 26
Figure 22. osCommerce Administration Tool ......................................... 27
Figure 23. Customer Cart .................................................................. 27
Figure 24. osCommerce Web Server Migration to Public Cloud ............. 29
Figure 25. Migrate VM to Cloud ............................................................ 29
Figure 26. Migrate VM to Cloud Parameters ......................................... 30
Figure 27. Deploy New osCommerce Web Servers
 in Public Cloud (AWS) ........................................................................ 30
Figure 28. Cisco Intercloud Fabric Policies .......................................... 31
Figure 29. Creating a Virtual Data Center .............................................. 32
Figure 30. Uploading an Image ............................................................... 32
Figure 31. Image Uploaded to Cisco Intercloud Fabric .......................... 33
Figure 32. Creating a Template ............................................................... 33
Figure 33. Create Template Parameters ............................................... 34
Figure 34. Adding a Catalog to a Template ............................................ 35
Figure 35. Service Request Creation ...................................................... 36
Figure 36. osCommerce Web Server Deployed in AWS ....................... 36

Tables
Table 1. Firewall Ports for Cisco Intercloud Fabric Communication......... 11
Table 2. Application Environment .......................................................... 21
Table 3. Database Server Details ............................................................ 24
Table 4. Web Server Details ................................................................ 25
Table 5. osCommerce Deployment Details ........................................... 28
Table 6. DNS Records ......................................................................... 28
Goal of This Document

This document describes the architecture and design details for deploying and scaling an e-business application using Cisco Intercloud Fabric™ for Business. With Cisco Intercloud Fabric for Business, you can extend your data center or private cloud to the public cloud, allowing you to acquire the added capacity you need with no boundary between your internal cloud and external clouds.

This document discusses deployment of an open-source reference application, osCommerce Online Merchant, in a VMware-based internal data center. It also discusses how to scale this application transparently using resources in Amazon Web Services (AWS).

Audience

The audience for this document includes sales engineers, field consultants, professional services staff, IT managers, partner engineers, and customers who want to take advantage of an infrastructure that is designed to scale on demand while maintaining consistent security and control policies.

Introduction

Industry trends indicate a growing movement among organizations to use hybrid cloud designs for acquiring additional on-demand computing and storage resources, thereby eliminating the need to build for peak capacity within their own data centers. Public clouds do not require the initial capital investments necessary to build out a company’s own private data center, and a public cloud can better service a company’s need for elasticity by providing essentially unlimited pay-as-you-grow expansion. Although hybrid cloud models are conceptually and financially attractive, customers are often reluctant to place their applications in the public cloud, away from their own premises. When an application or part of an application is deployed in the public cloud, companies want to help ensure not only that the transition from private data center to hybrid model is operationally feasible, but also that data access and control is carried over to this new architecture.

Cisco Intercloud Fabric facilitates secure hybrid cloud creation, giving customers the capability to scale their applications securely and conveniently. Using the Cisco® solution, customers can access additional computing power while extending their security, quality of service (QoS), and other control policies to the public cloud. Cisco Intercloud Fabric also allows customers to place workloads across heterogeneous environments in multiple provider clouds.

Some of the main benefits of the Cisco Intercloud Fabric solution are:

- Single point of management and control for virtual workloads across multiple provider clouds
- Choice of cloud providers and products, such as AWS, Microsoft Azure, and multiple intercloud fabric provider–based clouds
- Highly secure and scalable connectivity to extend private clouds to service provider clouds
- Capability to enforce consistent network and workload policies throughout the hybrid cloud
- Workload mobility to and from service provider clouds for virtual workloads

The solution architecture provides the following two product configurations to address enterprise and service provider customers:

- Cisco Intercloud Fabric for Business
- Cisco Intercloud Fabric for Providers
Cisco Intercloud Fabric for Business is intended for enterprise customers who want to be able to transparently extend their private clouds into provider cloud environments. Cisco Intercloud Fabric for Providers is intended for provider-managed cloud environments, to allow the service provider’s enterprise customers to transparently extend their private cloud environments into the provider's cloud.

This document focuses on an enterprise customer deployment model in an e-commerce environment and therefore discusses only Cisco Intercloud Fabric for Business.

**Cisco Intercloud Fabric Overview**

Cisco Intercloud Fabric is deployed as a set of virtual machines (VMs) in both private and provider clouds. The solution consists of the following components, shown in Figure 1:

- **Intercloud Fabric Virtual Machine**: This virtual machine contains the Intercloud Fabric Director (ICFD) feature and Cisco Prime™ Network Services Controller (NSC; abbreviated PNSC in figures in this document).
- **Secure Cloud Extension**: This component contains the Intercloud Fabric Extender (ICX) and Intercloud Fabric Switch (ICS) features.

**Figure 1.** Cisco Intercloud Fabric Architecture

Intercloud Fabric Director

The Intercloud Fabric Director feature is the single point of management and consumption for hybrid cloud solutions for both end users and IT administrators. It offers a single console so that end users and IT administrators can provision workloads and associated policies. Intercloud Fabric Director also exposes northbound APIs that allows customers to programmatically manage their workloads in the hybrid cloud environment or integrate with other cloud management platforms.
Cisco Prime Network Services Controller
Cisco Prime NSC software is a major element of many Cisco enterprise networking solutions, including Cisco Intercloud Fabric. Through a single pane, you can automate virtual network management to make configuration changes quickly and consistently. Cisco Prime NSC supports greater scalability along with standardization and adherence to policies in complex environments. In a Cisco Intercloud Fabric environment, Intercloud Fabric Director communicates with Cisco Prime NSC using Cisco Prime NSC’s northbound API, and customers and IT staff do not need to access Cisco Prime NSC directly to create or deploy workloads.

Secure Cloud Extension
The Secure Cloud Extension component forms the basis for the core switching and services infrastructure in the Cisco Intercloud Fabric solution. The Secure Cloud Extension provides the following features:

- Secure Layer 2 network extension from a private cloud to the provider cloud
- Advanced switching features for applications running in the provider cloud
- Support for services such as zone-based firewalls and routing in the provider cloud

The Secure Cloud Extension consists of several components working together to provide these functions. The private cloud is connected to the provider cloud through a highly secure tunnel that is established between a pair of virtual appliances: the Intercloud Fabric Extender and the Intercloud Fabric Switch. The Intercloud Fabric Extender runs in the private cloud, and the Intercloud Fabric Switch runs in the provider cloud, and these appliances can be deployed in a high-availability pair to provide redundancy. Virtual services can also be deployed in this environment to provide firewall and routing support in the provider cloud.

Intercloud Fabric Extender
The Intercloud Fabric Extender is a virtual machine that runs in the private cloud and provides the following functions:

- Establishes a secure site-to-site tunnel to interconnect with the intercloud fabric switch in the provider cloud
- Interacts with the virtual switch at the private cloud

Intercloud Fabric Switch
The Intercloud Fabric Switch is a virtual machine that runs in the provider cloud and provides the following functions:

- Runs the virtual Ethernet module (VEM) to provide Cisco Nexus® 1000V Switch functions in the cloud
- Establishes a secure tunnel to connect the VEM with the Intercloud Fabric Extender
- Establishes secure tunnels to connect all the cloud virtual machines
- Monitors and reports statistics of virtual machines in the cloud
- Monitors and reports any component failures in the cloud to Cisco Prime NSC

The embedded VEM in the Intercloud Fabric Switch is responsible for the following:

- Communicates with the virtual supervisor module (VSM) function that runs at the private cloud to retrieve virtual machine–specific network policies such as port profiles
- Switches the network traffic between cloud virtual machines
- Switches the network traffic between cloud virtual machines and the private cloud network
- Applies network policies and collects and reports VEM-related statistics

Intercloud Fabric Agent
The Intercloud Fabric Agent (ICA) feature provides a network overlay to the virtual machines in the cloud. The agent is deployed in the provider cloud as a secure tunnel driver that runs within the cloud virtual machines. The agent provides following functions:
- Establishes a secure tunnel to connect cloud virtual machines to the Intercloud Fabric Switch
- Collects secure overlay-related statistics

E-Business Application Overview
Designing a data center to meet continually changing e-commerce application requirements is a challenge. Although several factors influence the capacity planning decisions, the following two factors make capacity planning almost unmanageable:
- Unpredictable seasonal increases in customer load: for example, increased load during the holiday season
- Unexpected product success, resulting in unforeseen increased customer demand

Although not optimal, an increase in seasonable demand can be managed by overprovisioning the computing and storage resources to handle the projected load spikes. Unanticipated customer demand due to factors such as product success, however, requires IT department to not only acquire but also configure and deploy computing and storage resources in a very short amount of time, making the deployment financially stressful and operationally error prone.

Both of these aspects of e-commerce make an e-business application an excellent candidate for a hybrid cloud environment. An e-business application can be deployed in the internal data center with adequate resources to support typical customer demand. For occasional (seasonal or otherwise) and unexpected load spikes, one or more tiers of the application can be deployed (or burst) in the public cloud. To make this solution operationally viable, Cisco Intercloud Fabric can provide transparent communication among the various application tiers.

To demonstrate the applicability of Cisco Intercloud Fabric in an e-commerce environment, the osCommerce Online Merchant application was configured and deployed across private and public clouds (Figure 2). osCommerce is an open-source e-business application that provides customers with the features and tools required to set up an e-commerce site in a short amount of time. osCommerce contains both a catalog front end and an Administration tool back end that can be installed and configured through a web-based installation procedure. osCommerce is designed with the PHP web scripting language and uses the MySQL database server to store data. Although osCommerce can be installed on any web server that has PHP installed and has access to a database server, a typical installation includes:
- A CentOS server running Apache and PHP modules acting as a web front end and catalog server
- A second CentOS server running the MySQL database and used as an authentication and data source

The use of two server tiers enables the use of various options for deploying the application in the hybrid cloud environment. The validated scenario is discussed later in this document.
Figure 2. osCommerce Sample Website

System Components

The Cisco Intercloud Fabric solution can be deployed on a wide variety of data center and cloud configurations. The supported configurations and versions are listed in the Cisco Intercloud Fabric release notes:


This document covers the validation using the following data center, cloud, and application configurations:

- Cisco Intercloud Fabric for Business Release 2.2.1
- VMware vSphere-based private cloud
  - VMware vSphere 5.5 Update 2
  - VMware vSphere Distributed Switch (VDS)
  - Cisco Unified Computing System™ (Cisco UCS®) blade servers
- Amazon Web Services (AWS) as the public cloud
- osCommerce e-business application
  - CentOS 6.4 64-bit system with Apache and PHP (front end)
  - CentOS 6.4 64-bit system with MySQL database (back end)

Figure 3 shows the high-level architecture of the application deployment. In this design, the application servers are deployed in two different network segments (VLANs). A Cisco router (physical or virtual) provides the routing between the two application tiers. The back-end MySQL servers are deployed only internally, and the front-end Apache and PHP servers are deployed in both the private and public clouds. Cisco Intercloud Fabric is configured to securely extend the front-end network segment across the two clouds.
Figure 3. osCommerce Deployment Overview

Application Deployment and Cisco Intercloud Fabric Architecture

This section discusses the deployment requirements and the resulting design decisions for the application deployment.

Design Requirements

To successfully deploy the e-business application in a hybrid cloud environment, the following design requirements were considered crucial:

- One or more application tiers should be partially or completely deployed in the public cloud.
- The application should be accessed only from the enterprise data center, and any cloud virtual machines (deployed for increased capacity) must not be accessed directly from the public cloud.
- Data and authentication services should stay in the private data center but should be easily and immediately accessible from all the local and remote application virtual machines.
- Any new virtual machine in the cloud should be deployed without the need to move large amounts of data across the clouds.
- The workload on a server running in the private data center should be easily migrated to the cloud and back if capacity in the private data center becomes a concern.

These application demands require the following technical capabilities:

- Capability to position appropriate virtual machine templates in the public cloud
- Automatic virtual machine format conversion when virtual machines are migrated to and from the cloud
- Secure tunneling between the private and public cloud environments
- Capability to maintain IP addresses and gateway settings
- Routing between various VLANs across both clouds

The upcoming sections of this document describe a Cisco Intercloud Fabric design to support the e-business application.

**Network Design**

The e-business application, osCommerce, is deployed in two tiers: the front-end Apache and PHP server and the back-end MySQL database server. To deploy this application in the private data center, the network configuration shown in Figure 4 is used.

**Figure 4.** Application Network Design

![Application Network Design](image)

The front-end and back-end servers are placed in two different VLANs (101 and 103 in the example in Figure 4) to isolate the application tiers. The communication between the two tiers is enabled by routing. A firewall can optionally be deployed to further enhance the security of the database servers. To deploy Cisco Intercloud Fabric in this setup, an additional management VLAN (11) is used to host the management interfaces of the fabric components, as shown in Figure 5.
This management address space on VLAN 11 is also used as the tunnel source for the Intercloud Fabric Extender, and therefore the WAN router or firewall should be configured to apply Network Address Translation (NAT) to the management addresses to achieve a public routable IP address.

In addition, to establish successful communication between the fabric extender and the Intercloud Fabric Switch, the ports listed in Table 1 should be opened on the firewall. These ports are listed in the Cisco Intercloud Fabric release notes as well:


**Table 1.** Firewall Ports for Cisco Intercloud Fabric Communication

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>843</td>
<td>Adobe Flash</td>
</tr>
<tr>
<td>6644 and 6646</td>
<td>TCP and User Datagram Protocol (UDP)</td>
</tr>
</tbody>
</table>
Application Deployment Across Hybrid Cloud
This section describes the deployment of the application across the hybrid cloud and the operation of the application after it is deployed.

Deploying the Application-Tier
Data and authentication servers (MySQL back-end servers) are configured to stay in the private data center. Therefore, an Intercloud Fabric Extender trunk is configured to carry VLAN 101 only. The front-end Apache and PHP server will be deployed in both private and public clouds, and hence VLAN 101 is configured to be extended to the public cloud. Because traffic will enter only through the private data center, the solution requires only a Layer 2 extension of VLAN 101 to the public cloud (Figure 6).

In this configuration, front-end servers deployed in the cloud will access the MySQL database server using the Cisco Intercloud Fabric link. These cloud virtual machines will have their default gateway set to the router in the enterprise data center, hence enabling routing between all the virtual machines.

To load-balance customer traffic onto multiple front-end servers, a load balancer can also be deployed.

Note: For test purposes, you can avoid a load balancer installation by accessing the front-end server URLs directly.

Figure 6. Application Deployment Across Hybrid Cloud

Creating a Virtual Machine Template in the Cloud
Intercloud Fabric Director gives customers several ways to deploy a virtual machine in the cloud. One of the most common methods is to create a virtual machine template and then upload this template to the public cloud. When the template resides in the public cloud, new virtual machines can be easily deployed so that customers don't need to upload large amounts of data from their private data centers to the cloud. Because the template is uploaded using Intercloud Fabric Director, the director performs the appropriate conversion to the cloud virtual machine format and exposes the new template as a catalog item available in the director’s GUI, as shown in Figure 7.
Migrating the Virtual Machine to the Cloud

In addition to providing the capability to deploy a virtual machine in the cloud directly, Intercloud Fabric Director allows customers to move an existing virtual machine from their private cloud to the public cloud. In case of the e-business application under discussion in this document, this feature is useful when:

- Migrating a CPU-intensive virtual machine to the cloud to free local data center resources
- Migrating all the virtual machines in the Apache and PHP tier to the cloud in the future and letting customers access the application from the cloud

During migration, the director copies and repackages the virtual machine and brings up the virtual machine in the cloud. By default, the local data center virtual machine is shut down after the migration is complete, but this behavior can be modified if needed.

Application Operation

When an application is deployed using the configuration parameters discussed here, application servers are positioned in the customer data center so that the end users can access the application directly through the customer data center.

When the load on the existing front-end Apache and PHP servers increases, the application administrator logs into the Intercloud Fabric Director and deploys additional front-end servers using the predeployed template in the public cloud. The Intercloud Fabric Extender and Intercloud Fabric Switch provide secure Layer 2 extension, enabling communication between the front-end and back-end servers using the router in the data center. If the administrator wants to free the resources in the local data center, the administrator can migrate all the front-end virtual machines to the cloud. When the application computing requirements go down, the additional servers configured in the cloud can be deleted.

The director provides a single GUI for managing the resources in both the private and public clouds.
Implementation and Configuration Details

This section discusses the implementation and design details configured during the validation phase of this project. This document does not include explicit details like those found in a configuration guide for deployment; instead, it provides guidance about deployment considerations and best practices, along with links to documentation for installation, configuration, and troubleshooting.

Enterprise Environment Overview

Figure 8 shows the topology of the enterprise environment.

Figure 8. Topology Overview

The enterprise environment supports the validation of the Cisco Intercloud Fabric solution. The environment consists of VMware vSphere deployed as the hypervisor, Cisco Nexus 9000 Series Switches, Cisco Nexus fabric extenders, and Cisco UCS C-Series Rack Servers and B-Series Blade Servers along with IP-based storage connected in a highly available modular design. VMware VDS is used to provide Layer 2 connectivity between the various LAN segments in the enterprise data center.

The environment also consists of an Microsoft Active Directory (AD) server and a Domain Name System (DNS) server to support the solution. The Microsoft DNS server is also configured as a load balancer to load-balance the web servers of the osCommerce application.

As mentioned earlier, the osCommerce application is intended to be accessed from the enterprise, and users will not access the application directly from the cloud. The necessary routing and the firewall services are performed at the enterprise data center. The network gateways for cloud virtual machines are configured to use the enterprise’s aggregation routers.
Cisco Intercloud Fabric Deployment

This section provides an overview of the Cisco Intercloud Fabric implementation in the enterprise environment described in the preceding section.

You deploy the fabric using the Open Virtualization Archive (OVA) image downloaded from Cisco to the VMware environment. The OVA image installs the Intercloud Fabric Director and Cisco Prime NSC.

The following parameters must be provided in the Properties pane during the OVA deployment:

- Cisco Intercloud Fabric hostname
- Intercloud Fabric Director hostname
- Cisco Intercloud Fabric, Intercloud Fabric Director, and Cisco Prime NSC admin or root password
- Cisco Intercloud Fabric host static IP address
- Intercloud Fabric Director static IP address
- Cisco Prime NSC static IP address
- Cisco Intercloud Fabric, Intercloud Fabric Director, and Cisco Prime NSC IP subnet mask
- Cisco Intercloud Fabric, Intercloud Fabric Director, and Cisco Prime NSC IP gateway
- Cisco Intercloud Fabric, Intercloud Fabric Director, and Cisco Prime NSC domain name
- Cisco Intercloud Fabric, Intercloud Fabric Director, and Cisco Prime NSC DNS server IP address
- Syslog server IP address (optional)
- Cisco Intercloud Fabric, Intercloud Fabric Director, and Cisco Prime NSC Network Time Protocol (NTP) server IP address
- Time zone

Before you configure the Intercloud Fabric Director after the OVA deployment, you must obtain a license. To install a permanent Cisco Intercloud Fabric license, you must upload the Cisco Intercloud Fabric Base license file. The license count varies depending on the cloud provider and is enforced during virtual machine provisioning and migration.

To install the license, log in to the Intercloud Fabric Director web interface as admin and choose Administration > License (Figure 9).

Figure 9. Cisco Intercloud Fabric for Business Licensing

After the license is installed, use the following procedure to install Cisco Intercloud Fabric infrastructure components.
Choose Intercloud > Infrastructure. On the Infrastructure tab, click the Setup button.

The setup wizard registers Cisco Prime NSC, uploads the infrastructure bundle to Cisco Prime NSC, and installs the Intercloud Fabric VSM (lcfVSM) file using Cisco Prime NSC (Figure 10).

**Figure 10.** Cisco Intercloud Fabric Infrastructure Setup

The deployment process is automated and can be monitored by viewing the corresponding service request created within the Intercloud Fabric Director (Figure 11).

**Figure 11.** Confirmation Summary
Creating an Intercloud Fabric Cloud

An Intercloud Fabric Cloud (IcfCloud) creates secure connections between a private cloud and a provider cloud. An Intercloud Fabric Cloud includes two virtual gateways: one on the private cloud and one on the provider cloud. The gateway on the private cloud is referred to as the Intercloud Fabric Extender, and the gateway on the provider cloud is referred to as the Intercloud Fabric Switch. A secure Layer 4 tunnel connects the gateways, thereby extending the Layer 2 private cloud network into the provider cloud.

In this solution, AWS is used as the public cloud. You must meet the following prerequisites before you can create an Intercloud Fabric Cloud:

- You must have an account in the provider cloud (AWS).
- You must have credentials for the cloud provider, such as an access key and access ID for AWS.
- You should have completed the installation of Cisco Intercloud Fabric infrastructure components such as Cisco Prime NSC and the Intercloud Fabric VSM.

The enterprise administrator also needs to configure the IP addresses and VLAN ranges used to configure the management of the secure link and any services to be deployed in the service provider cloud.

Separate VLANs and IP network segments can be used for the management of the Cisco Intercloud Fabric components and the optional Intercloud Fabric Cloud tunnel interface. The fabric administrator has the option, during Intercloud Fabric Cloud deployment, to use the default settings, with the same network and the same IP address space for both the tunnel network and the management network for the Cisco Intercloud Fabric components.

In this validation environment, the default option was used, with the same VLAN (VLAN 11) used for the management and tunnel interfaces.

In the IcfCloud deployment wizard, you can also specify the configuration of MAC address pools for virtual machines that may either be instantiated or migrated to the service provider cloud, tunnel profile configuration settings for specifying tunnel encryption algorithms, protocols, and rekey settings. You can also specify IP groups, used to protect public-facing interfaces of virtual machines that are deployed in the service provider cloud. And you can specify additional services such as firewall (Intercloud Fabric Firewall) and routing (Intercloud Fabric Router) services, used to secure and provide local routing, and NAT services for virtual machines deployed in the cloud.

Intercloud Fabric Cloud creation includes the following workflow:

1. Create Cisco Intercloud Fabric infrastructure policies, profiles, and pools such as a management IP address pool for the Intercloud Fabric Extender, a tunnel IP address pool for the Intercloud Fabric Extender, a management IP address pool for the Intercloud Fabric Switch, an interface IP address pool for services, and an IP address pool for virtual machines in the cloud.
2. Create port profiles for the DVS in the private cloud.
3. Create management and data port profiles for the Cisco Virtual Security Gateway (VSG) for the fabric.
4. Create the Intercloud Fabric Cloud using the wizard.
Creating Cisco Intercloud Fabric Infrastructure Policies

Add a MAC address pool to allocate a group of MAC addresses to a virtual private cloud.

Add an IP group, which protects cloud resources by helping ensure that only the ports required for Cisco Intercloud Fabric are open to the public interface of the cloud virtual machines in an Intercloud Fabric Cloud and that access is allowed only from IP addresses in the IP group.

Figure 12 shows the policies that need to be configured from Intercloud Fabric Director.

**Figure 12.** Cisco Intercloud Fabric Infrastructure Policies

![Cisco Intercloud Fabric Infrastructure Policies](image)

Configuring a Tunnel Profile

A tunnel profile pairs a connection parameter policy with a key policy to help ensure secure communications for specific tunnel ports. After you configure tunnel profiles, you can apply them to tunnels between the following elements:

- Intercloud Fabric Extender and Intercloud Fabric Switch
- Intercloud Fabric Switch and cloud virtual machine

A site-to-site tunnel profile is used for tunnels between the Intercloud Fabric Extender and Intercloud Fabric Switch. The access tunnel profile is used for tunnels between the Intercloud Fabric Switch and cloud virtual machines.

Figure 13 shows the configuration of the tunnel profile. The communication protocol selected for the tunnel is TCP, with HTTPS disabled, and the encryption algorithm used is AES-128-CBC.
Figure 13. Cisco Intercloud Fabric Tunnel Profile

Configuring Port Profiles and Port Groups
VMware VDS is used in the validation environment. In VMware vCenter, you need to create the port groups that need to be associated with the virtual network interface cards (vNICs) of Cisco Intercloud Fabric, Intercloud Fabric Extender, and Cisco Prime NSC virtual machines.

The setup here uses the default installation of Cisco Intercloud Fabric, and the management vNIC is used to provide the management access to the Intercloud Fabric Extender and connectivity to the Cisco Prime NSC, Intercloud Fabric VSM, and enterprise servers such as DNS and NTP servers. The same vNIC is also used to provide a secure tunnel connection to the Intercloud Fabric Switch; hence, a common port group is used to provide management and tunnel access.

The enterprise data trunk vNIC on the Intercloud Fabric Extender is used as an uplink to send or receive traffic over the secure tunnel. It must be associated with the trunk port group. The trunk port group must contain all the VLANs that must be extended to the provider cloud. In this case, the web server VLAN (101) is being extended to the public cloud (AWS). Promiscuous mode for the port group associated with the data trunk vNIC needs to be enabled because VDS is used in the private cloud.

Figure 14 shows the settings.
Setting Up an Intercloud Fabric Cloud

To set up the Intercloud Fabric Cloud, log in to Cisco Intercloud Fabric. Choose Intercloud > IcfCloud and click the Setup button.

Fill in the required fields and click Submit. The Intercloud Fabric Cloud creation process runs in the background and can be monitored from Organizations > Service Requests within the Intercloud Fabric Director GUI.

Provide the account credentials for the AWS cloud. After the credentials have been validated, select the MAC address pool, tunnel profile, and IP address group as part of the network configuration.

Complete the fields shown in Figure 15 for Secure Cloud Extension and Intercloud Extender Placement.

Figure 14. Port Groups in VMware vSphere Distributed Switch

Figure 15. Cisco Intercloud Fabric Setup
You can monitor the deployment process for successful completion by viewing the corresponding service request created within Intercloud Fabric Director.

E-Commerce Application Implementation
osCommerce Online Merchant is an e-commerce and online store-management software program. It is available as free software under the GNU General Public License. The osCommerce application was used for this validation because of its simplicity of deployment.

Note: The osCommerce application has been selected as a sample e-commerce application only. The validation and test processes don’t suggest or guarantee any application-specific details. Application validation and setup are outside the scope of this document.

Environment
osCommerce can be installed on any web server that has PHP installed and has access to a database server. Options include shared servers, dedicated servers, cloud instances, and local installations running on Linux, UNIX, BSD, Mac OS X, and Microsoft Windows operating systems.

This validation test used dedicated virtual servers for the front end and back end with multiple web servers accessing a single database server (Table 2).

Table 2. Application Environment

<table>
<thead>
<tr>
<th>Application</th>
<th>osCommerce 2.3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server</td>
<td>Apache 2.2.15 (UNIX)</td>
</tr>
<tr>
<td></td>
<td>PHP 5</td>
</tr>
<tr>
<td>Database server</td>
<td>MySQL 5.1.73</td>
</tr>
<tr>
<td>Operating system</td>
<td>CentOS 6.4 64-bit</td>
</tr>
</tbody>
</table>

Web Servers
The test uses two CentOS 6.4 64-bit virtual machines as web servers. Apache 2.2.15 with PHP 5 is installed on the web servers. The web server must either support PHP as a module or allow execution of CGI scripts. For performance reasons, FastCGI is recommended over CGI.

The latest Apache and PHP packages can be installed using YUM from public repositories:

```
# yum install httpd php php-mysql php-gd php-imap php-ldap php-odbc php-pear php-xml php-xmllpc phpmyadmin
```

After the packages have been installed, start the Apache web server using the following command:

```
# service httpd start
```

Disable the SELinux feature on the web server to allow Apache to make remote connections to the database server. SELinux is a Linux kernel security module that provides a mechanism for supporting access control security policies. By default, SELinux prevents Apache from accessing the database from a remote server.

```
#/usr/sbin/setsebool -P httpd_can_network_connect=1
```

The initial deployment includes a single web server and a database server. The second web server is deployed by cloning the first web server.
Database Server

The environment consists of one database server that can be accessed by multiple front-end web servers and that can be scaled up or down based on need. The intention of this validated solution is to demonstrate that Cisco Intercloud Fabric can enable dynamic deployment of distributed e-commerce applications in a hybrid cloud environment that includes a private cloud and one or more public clouds. It also demonstrates that, with the Cisco solution, web servers can be deployed in multiple cloud environments and still have access to the database server deployed in the enterprise data center or private cloud while maintaining security.

The osCommerce application stores information about customers, payments, orders, etc. in the database server. The database server needs to be accessed by the web servers to enable customers log in and make purchase transactions.

In the validation environment, MySQL is deployed on a CentOS 6.4 64-bit virtual machine. To install MySQL, enter the following command:

```
# yum install mysql mysql-server
```

After the MySQL packages are installed on the database server, complete the initial configuration, setting the root password and the management of default users, by using the following command:

```
# mysql_secure_installation
```

Create a database to be used by osCommerce as follows:

```
# mysql -u root -p
mysql> CREATE DATABASE osCommdb;
mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'PASSWORD' WITH GRANT OPTION;
mysql> FLUSH PRIVILEGES;
mysql> exit
```

osCommerce Installation and Configuration

osCommerce is a web-based solution that needs its relevant files to exist on the web server. You can copy the files to the web server by extracting the download package to a computer and uploading the contents to the web server through FTP, or by copying the download package to the web server directly and extracting the contents there.

The following procedure directly downloads the package to a web server:

```
# cd /tmp
# wget http://www.oscommerce.com/files/oscommerce-2.3.4.zip
# unzip oscommerce-2.3.4.zip
```

Move the package folder to the web server’s root directory:

```
# mv oscommerce-2.3.4 /var/www/html/
```

You need to set the appropriate permissions for the web installation. For you to do so, the web server must be able to write to the following files during the installation procedure:

`catalog/includes/configure.php`
`catalog/admin/includes/configure.php`
After the installation procedure has completed successfully, you need to remove the web server write permission from these files.

Use the following commands to change file permissions directly on the server:

```
#chmod 777 /var/www/html/oscommerce-2.3.4/catalog/includes/configure.php
#chmod 777 /var/www/html/oscommerce-2.3.4/catalog/admin/includes/configure.php
```

Additionally, to add SELinux overrides, use the following command:

```
#chcon -R -t httpd_sys_content_rw_t /var/www/html/oscommerce-2.3.4/
```

Installation Procedure

The web-based installation procedure configures the online store and imports the configuration data into the database. This process is necessary to create a fully functional online store and to enable an administrator to manage the online store through the Administration tool.

You can use the configuration values provided by default, but you may need to change them depending on the environment of the web server.

Installing a New Online Store

The web-based installation procedure starts automatically when the online store is accessed through a web browser. To do this, enter the web address of the osCommerce installation in your browser:

```
http://www.oscomm-web.icf.local/ oscommerce-2.3.4/catalog
```

osCommerce automatically detects whether the installation process has been completed and redirects you to the installation procedure if it has not yet been performed (Figure 16).

*Figure 16. osCommerce New Installation*
Click Start to enter the database connection parameters to successfully connect to the database server, import the database table structure, and import the required data (Figure 17 and Table 3).

**Figure 17.** osCommerce Database Parameters

![osCommerce Database Parameters](image)

**Table 3.** Database Server Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server address</td>
<td>The address of the database server in the form of a hostname or IP address</td>
<td>10.1.3.1</td>
</tr>
<tr>
<td>Username</td>
<td>The username used to connect to the database server</td>
<td>Root</td>
</tr>
<tr>
<td>Password</td>
<td>The password that is used together with the username to connect to the database server</td>
<td>******</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database in which to place the data</td>
<td>osCommdb</td>
</tr>
</tbody>
</table>

The installation procedure verifies the values entered before you can proceed to the next step. Verify that the correct username, password, and database name are listed.

The next step is to set the web server parameters to successfully serve the online store to users. Verify the web server web address and the web server root directory (Figure 18 and Table 4).
Figure 18. osCommerce Web Server Settings

Table 4. Web Server Details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server address</td>
<td>The web address for the online store</td>
<td><a href="http://oscommerce-web.icf.local/oscommerce-2.3.4/catalog/">http://oscommerce-web.icf.local/oscommerce-2.3.4/catalog/</a></td>
</tr>
<tr>
<td>Root directory</td>
<td>The directory in which the online store is installed on the web server</td>
<td>/var/www/html/oscommerce-2.3.4/catalog/</td>
</tr>
</tbody>
</table>

Click Continue to go to the next step. Fill in the web store details (Figure 19). This step sets the store owner and administrator for the online store. Be sure to note the administrator username and password because these are used to log in and to access the Administration tool.

Figure 19. osCommerce Online Store Settings
The last step in the installation procedure stores the database server and web server parameters in the configuration file on the web server. After you have successfully saved the configuration file, the installation procedure is finalized, and the online store is ready for use (Figure 20).

**Figure 20. osCommerce Installation Finished**

After the installation succeeds, you can access the online store (Figure 21) directly from this link: [http://oscomm-web.icf.local/oscommerce-2.3.4/catalog/index.php](http://oscomm-web.icf.local/oscommerce-2.3.4/catalog/index.php).

You can access the Administration tool (Figure 22) from this link: [http://oscomm-web.icf.local/oscommerce-2.3.4/catalog/admin/login.php](http://oscomm-web.icf.local/oscommerce-2.3.4/catalog/admin/login.php).

**Figure 21. osCommerce Online Store**
Customers can access the osCommerce website and browse the store contents after the store owner has installed and set up the store. They can purchase items in the store by creating a user account or as a guest by providing information for purchasing the items electronically.

In Figure 23, a user has logged in to the store’s portal and added items to the cart. The test discussed in this document verified the same information later, after the application was scaled, by following the procedure described in rest of this document. The same user credentials were used to log in to the application accessing the new web servers deployed in the public cloud (AWS), the authentication was successful, and the cart items remained in the user account.
Deployment Details
The osCommerce application is deployed in the enterprise private cloud on two web servers and a database server, with the enterprise private cloud extended to the AWS public cloud. Table 5 summarizes the details of the deployment.

Table 5. osCommerce Deployment Details

<table>
<thead>
<tr>
<th>osCommerce application URL</th>
<th><a href="http://oscomm-web.icf.local">http://oscomm-web.icf.local</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server 1</td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>Web server 2</td>
<td>10.1.1.2</td>
</tr>
<tr>
<td>Database server</td>
<td>10.1.3.1</td>
</tr>
<tr>
<td>Active Directory and DNS</td>
<td>10.1.1.50, 10.1.1.51</td>
</tr>
<tr>
<td>Microsoft DNS–based load balancer</td>
<td>10.1.1.50</td>
</tr>
<tr>
<td>Domain name</td>
<td>icf.local</td>
</tr>
</tbody>
</table>

The osCommerce application web servers are load-balanced using the Microsoft DNS server, which provides a simple method for load balancing the client use of web servers. The enterprise can use any advanced dedicated load balancers; the test here used Microsoft DNS because of its simplicity.

Microsoft DNS is configured for round-robin local balancing. DNS A host records are created to resolve the pool's fully qualified domain name (FQDN) to the IP addresses of all the servers in the pool (Table 6). New web servers can be added to the pool as they are deployed.

Table 6. DNS Records

<table>
<thead>
<tr>
<th>FQDN</th>
<th>Type</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oscomm-web.icf.local</td>
<td>Host (A)</td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>Oscomm-web.icf.local</td>
<td>Host (A)</td>
<td>10.1.1.2</td>
</tr>
<tr>
<td>Oscomm-web.icf.local</td>
<td>Host (A)</td>
<td>&lt;New Server IP Address&gt;</td>
</tr>
</tbody>
</table>

The first DNS client that queries the server to resolve this host's name receives the list in default order. When a second client sends a subsequent query to resolve this name, the list is rotated.

Application Scaling
With Cisco Intercloud Fabric, the enterprise can dynamically and transparently use the resources in the cloud for the e-commerce application to support additional customer demand, to scale out, and to scale back. Increased demand, for example, may be generated by holiday or other seasonal purchases, or it may be the result of maintenance activities, etc.

The enterprise can use the resources in the public cloud through the hybrid cloud. By using virtual machine templates created by Cisco Intercloud Fabric, additional web servers can be deployed in the public cloud to serve the osCommerce application. Alternatively, enterprise users can migrate the existing web servers deployed in the private cloud to the public cloud as is, without making any additional configuration changes to the migrated virtual machines.
Migrating Existing Web Servers to the Public Cloud (AWS)

In this test scenario, one of the web servers was migrated to the public cloud using Cisco Intercloud Fabric. The persistent information within the application, including users and store-related details, was verified to be intact after the migration (Figure 24).

Figure 24.  osCommerce Web Server Migration to Public Cloud

Initially, the enterprise data center deployed two web servers and a database server. One of the web servers was migrated to AWS using Cisco Intercloud Fabric, and after the migration the web server was fully functioning, with connectivity to the database server on the enterprise side.

Because the web server that was migrated to the cloud already existed, after the migration is complete, users can use the server immediately without the need to make any additional configuration changes.

Figure 25 shows how to migrate a virtual machine. Choose **Intercloud > Compute**. Select a virtual machine from the list, and click the **Migrate VM to Cloud** button.

Figure 25.  Migrate VM to Cloud

In the dialog box, complete the required fields. Enter the name of the target virtual machine, select the virtual data center (VDC), and select the OS version. Then click **Proceed** to complete the migration (Figure 26).
Migrated virtual machines can remain in the enterprise and left in a powered-off state, or the user or administrator can choose to remove them completely.

Deploying New Web Servers in the Public Cloud (AWS)
The quickest way to add new front-end servers to the application to meet immediate demand is to deploy additional web servers in the public cloud (Figure 27). This approach eliminates the time consumed in moving data from the enterprise data center to the public cloud during a migration.

New web servers in the public cloud can be deployed using Cisco Intercloud Fabric templates. These servers can be used in the application immediately after their deployment.

The only additional task required after the new servers are deployed is to add the IP addresses for the new web servers to the DNS A host records pool.

Deployment of virtual machines using Cisco Intercloud Fabric includes the following workflow:

1. Create policies.
2. Create a virtual data center.
3. Upload an image.
4. Create a template.
5. Add a catalog to the template.
6. Create a service request.

**Note:** All of these tasks can be preexecuted, and the web server template can be made available in the catalog so that enterprise users can initiate the deployment of servers instantly on a self-service basis.

Creating Policies
Cisco Intercloud Fabric provides self-service virtual machine provisioning from a pool of assigned resources using predefined policies set by administrators. A policy is a group of rules that determine where and how a new virtual machine is provisioned.

Cisco Intercloud Fabric requires you to set up the following policies to provision virtual machines (Figure 28):

- **Network:** The network policy includes resources such as network settings, Dynamic Host Configuration Protocol (DHCP) or static IP, and the option to add multiple vNICs for virtual machines provisioned using this policy.
- **System:** System policy defines system-specific information such as the template to use, the time zone, and operating system-specific information. It defines the naming policy of instantiated virtual machines.
- **Computing:** Computing policy is used only for the private cloud VDC to identify hypervisor targets for placement during migration operations from the provider cloud to the enterprise.

All virtual machines were configured with one network interface. For the virtual machines created by the enterprise administrator using the vCenter, the IP addresses was assigned manually. For the virtual machines instantiated by Intercloud Fabric Director in the provider cloud, the IP address was assigned from a static IP pool configured in the Intercloud Fabric Director.

Figure 28. Cisco Intercloud Fabric Policies

Creating a Virtual Data Center
A VDC is an environment that combines virtual resources, operation details, rules, and policies to manage specific group requirements.

A group or organization can manage multiple VDCs, images, templates, and policies. Organizations can allocate quotas and assign resource limits for individual groups at the VDC level. You can also define approvers specific to a VDC. The approver for a particular VDC must approve the request from users for virtual machine provisioning.

A virtual machine that is provisioned using a service request can be associated with a VDC. When you are creating a service request, you can choose the VDC on which this virtual machine is provisioned. You can view a list of
VDCs that are available for a particular group and choose the required VDC when provisioning virtual machines (Figure 29).

**Figure 29.** Creating a Virtual Data Center

![Creating a Virtual Data Center](image)

Uploading an Image

To upload an image, log in to Cisco Intercloud Fabric and choose Intercloud > Compute.

In the Compute window, open the Enterprise Template tab and click the Upload Image button. Complete the required fields for Image Upload in the wizard (Figure 30).

**Figure 30.** Uploading an Image

![Uploading an Image](image)

The image appears in Cisco Intercloud Fabric after the upload is complete (Figure 31).
Creating a Template

After the image is uploaded to Cisco Intercloud Fabric, you need to create a template.

Log in to Cisco Intercloud Fabric. Choose Intercloud > Compute. On the Enterprise Templates tab, select the image and click the Create Template in Cloud button (Figure 32).

Figure 32. Creating a Template
To complete the Create Template in Cloud procedure, fill in the required fields (Figure 33).

**Figure 33.** Create Template Parameters

Adding a Catalog to the Template

Users can self-provision virtual machines using predefined catalog items. Catalog items are created by the system administrator. Catalog items define parameters such as the cloud name and group name to which the virtual machine is bound.

You need to add a catalog to the template after the image is uploaded and the template is created based on the uploaded image.

Log in to Cisco Intercloud Fabric. Choose **Policies > Catalogs**. On the **Catalog** tab, select the template and click the **Add** button. Click **Submit** and complete the required fields for Create Catalog (Figure 34).
Creating a Service Request

To provision a virtual machine, you must first create a service request. After an administrator or a relevant user approves the service request, the virtual machine is provisioned. Virtual machines can be immediately approved, or they can be scheduled for approval within a maximum of 90 days from the original request.

To create a service request, log in to Cisco Intercloud Fabric. Choose Organizations > Service Requests. On the Service Request tab, click Create Request. In the Create Request dialog box, complete the required fields.

Select the catalog, select the VDC in which the virtual machine needs to be deployed, and select the virtual machine networks to which the virtual machine should be connected.

Figure 35 shows a summary of a service request for deploying a virtual machine. In this example, the virtual machine is osCommerce Web Server.
You can monitor this task from Organizations > Service Requests. After the task succeeds, a new osCommerce Web Server will be deployed in AWS and can be accessed by users (Figure 36).

After the new servers are deployed in to the public cloud (AWS), existing users will be able to log in to the osCommerce online store accessing the new web servers. The users will have access to all the information pertaining to them because the information related to authentication and to the online store is stored in the database server.
Conclusion

Cisco Intercloud Fabric for Business facilitates creation of a secure hybrid cloud, enabling customers to scale applications securely and conveniently. Using Cisco Intercloud Fabric, customers can access additional computing power while maintaining security and control of their applications.

Cisco Intercloud Fabric is very well suited for e-business applications, allowing customers to place complete or partial front-end application tiers in the public cloud while maintaining access to internal authentication and database servers.

In addition, the Intercloud Fabric Director feature allows virtual machine templates to be uploaded to the cloud for immediate application server deployment. The director also provides the capability to migrate customer workloads between private and public clouds.

For More Information

- Cisco Intercloud Fabric 2.2.1 Release Notes:
- Cisco Intercloud Fabric getting-started guide:
- osCommerce Online Merchant installation procedure:
  [http://library.oscommerce.com/Online&en&oscom_2_3&getting_started&new_installation](http://library.oscommerce.com/Online&en&oscom_2_3&getting_started&new_installation)