FUJITSU Cloud Service S5
Configuring a Server Load Balancer

This guide describes the options and process for adding and configuring a Server Load Balancer (SLB) Virtual Appliance, within a FUJITSU Cloud Service S5 Virtual System (VSYS)

About the SLB

An SLB is a virtual software load balancer that provides the ability to balance requests, maintain sessions and monitor both failures and continuous service. It can be added to any vSYS, with each instance taking the space of 1 VM (be it a Virtual server or SLB) of a maximum 20 that can be added per vSYS. A SLB can be added to each vSYS network segment (DMZ, Secure1, Secure2) but can only load balance VMs within that segment.

Updates to the SLB software are advertised within the portal, and are installed by the end customer. In the event of a problem, the customer has up to a week in which to regress the update and roll back to the previous version of the appliance.

Each SLB has a virtual IP address and associated load balancing rules assigned to it.

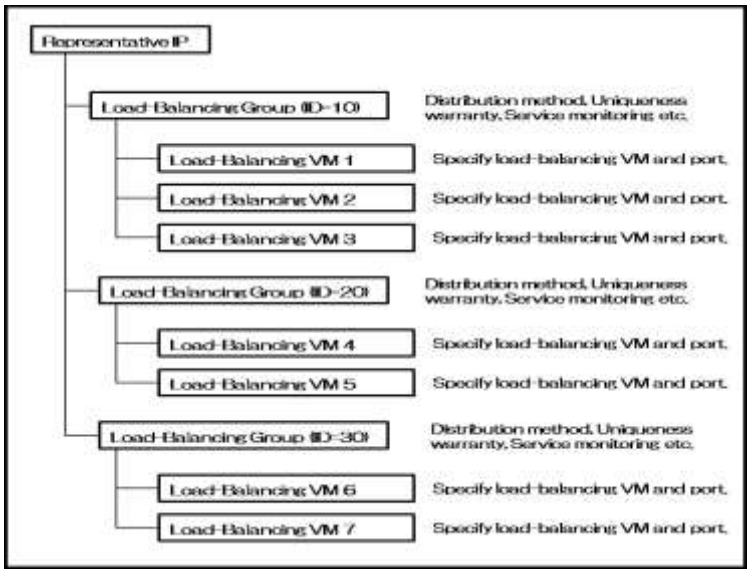


Fig. 1 - Structure of Load Balancing Rules

The load balancing rules allow the following options to be configured:

■ Load balancing method
Allows the method for determining how requests are distributed across VMs to be changed.

■ Consistency preservation method
Consistency preservation is used to help direct subsequent requests, to the same VM that processed the initial request. This allows the method for tracking and performing this to be changed.

■ Health checking
Monitors the running status of the VMs.

ISN007452

- Error corrections on load balanced VMs.
  - Reset connections : The system resets a TCP connection and informs the User, in the event of an error.
  - Automatic integration: Select whether to automatically reinstate VM's that have recovered from a failure.

- Error page setting

Users can specify the error page that is displayed in response to HTTP requests that occur, when ALL load balancer VMs are:

  - Under Maintenance
  - Have Failed
  - Have exceeded the maximum number of connections

- SSL Server Certificate and Intermediate CA Certificate registration

Register SSL Server Certificate and Intermediate CA Certificate for SSL (HTTPS) communication.

SLBS can be added when either creating or modifying an existing configuration via the normal drag and drop procedure. Each SLB must be given a unique name within that virtual system, which can be changed later if required.

The following points should be noted when choosing to add a SLB:

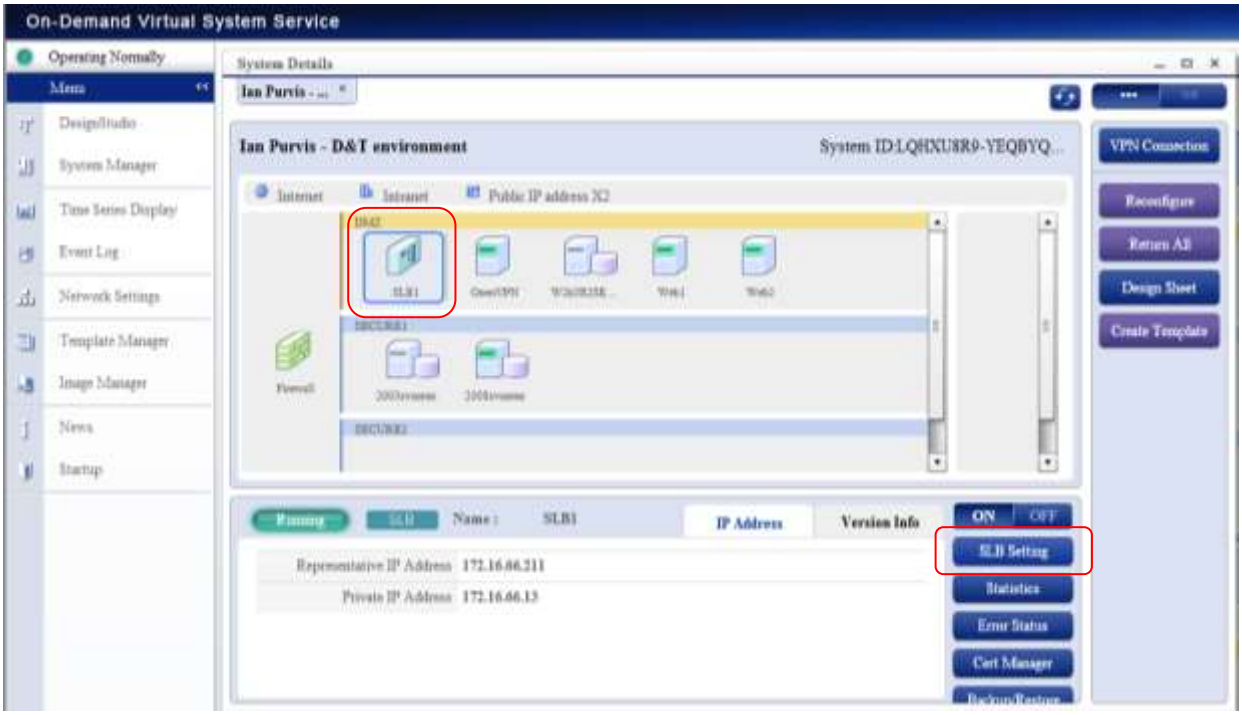
- Duplicated VMs in the same load balance group are not allowed even though the service port is different.
- Users can specify Error Page Setting, Certificate Registration and Intermediate CA Certificate Registration after a load balance group is created and the group setting is complete.
- Users can only specify Error Page Setting when [HTTP], [HTTPS] or [HTTP+HTTPS] is selected as the group setting protocol.
- Users can only specify Certificate Registration and Intermediate CA Certificate Registration when [HTTPS] or [HTTP+HTTPS] is selected as the group setting protocol.
- Users can only register a single Certificate File per SLB.
- Before a SLB can be deleted, it must be in stopped state.

Basic SLB Configuration

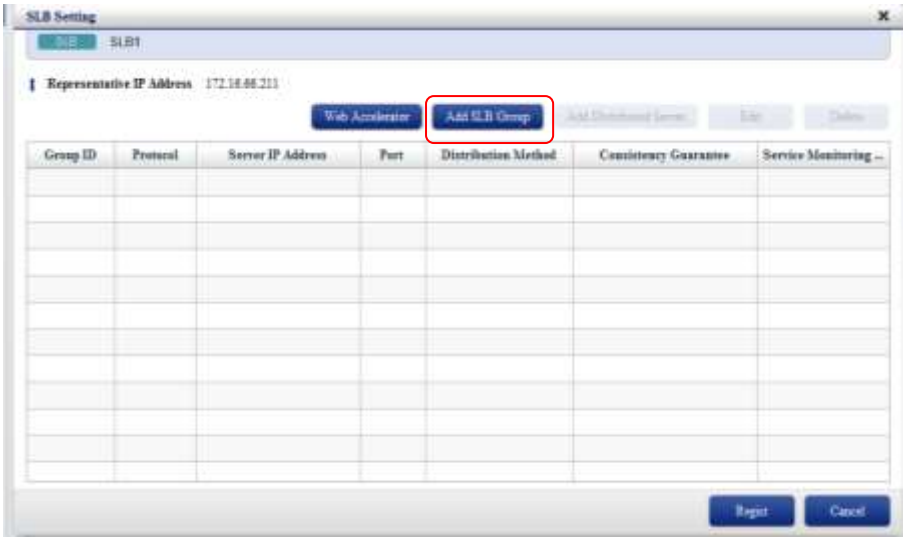
The vSYS Firewall will need to be configured in accordance with any SLB requirements to allow communication on the specific protocol and ports. For example, the below firewalls are necessary to allow HTTP and HTTPS traffic from the Internet, through the firewall and to a SLB on the DMZ network segment.

Firewall configuration is outside the scope of this guide

1. Within 'System Manager | System Details', highlight the appropriate SLB icon and select 'SLB Setting' button

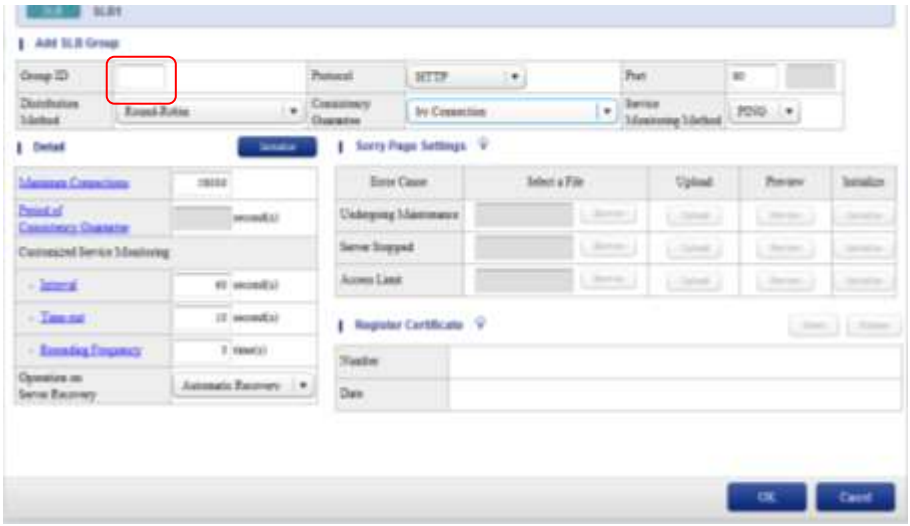


2. In the resulting window, click 'Add SLB Group'



3. Supply a Group ID

Item	Available setting	Description
Group ID	Any Number between [1-99999].	A unique identifier. Rules are applied incrementally by group ID (lowest first). IDs should not be consecutive and should allow intervals between IDs to allow new rules to be inserted later if required. Users cannot assign the same ID to different groups.



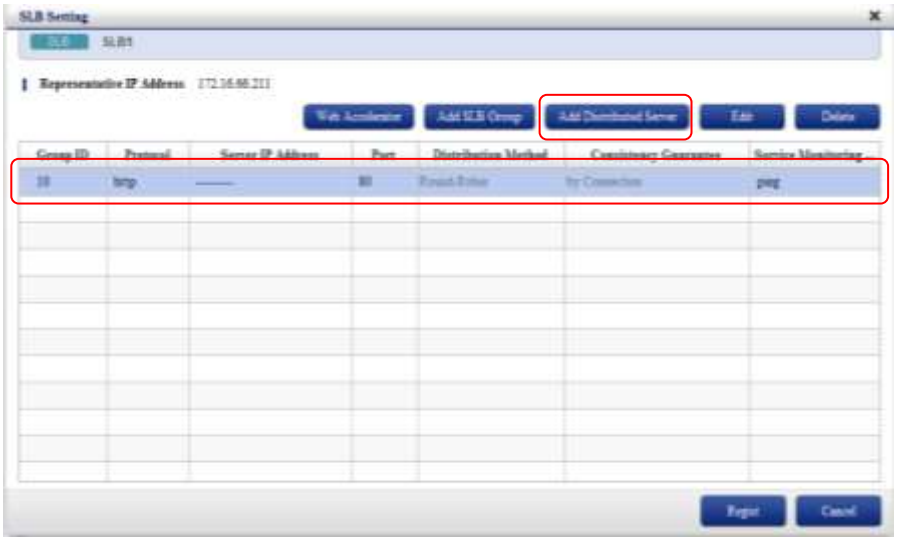
4. Please review and configure the following options at this point, according to your requirements.

Item	Available setting	Description
Distribution Method	Select either [Round-Robin] or [Minimum Connection Number].	Round-Robin : The SLB forwards requests sequentially and ignores the amount of load on each VM. Minimum Connection Number: The SLB forwards requests preferentially to the VMs that have fewer connections.

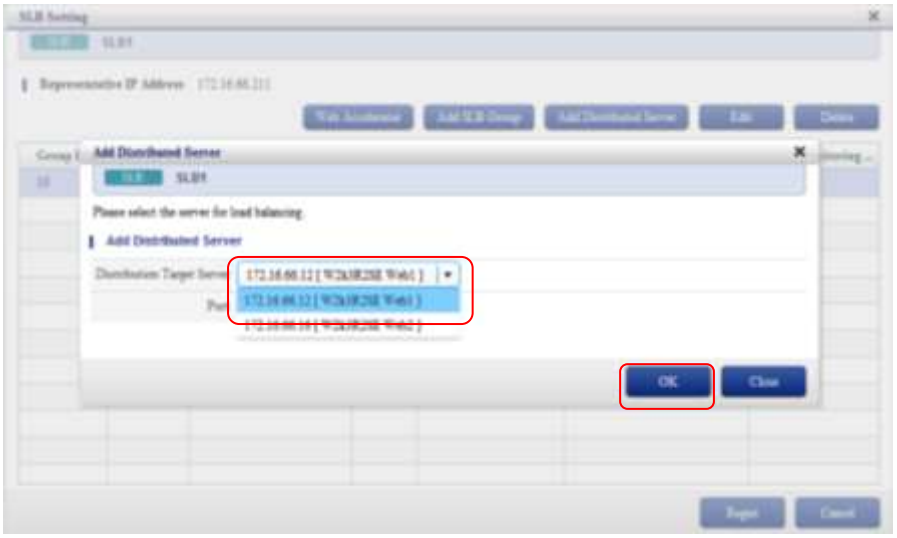
Service Monitoring Method	Select from either [TCP] or [PING].	Select the method of monitoring the load balancer VMs. TCP : Checks whether load balancer VMs can perform a 3-way handshake in TCP (connection in TCP is able to establish correctly). Then disconnects with a FIN command after connection is established. If users select [UDP] for the protocol, this method is not available. PING : Checks the response from the server by sending ICMP (PING).
Period of Consistency Guarantee	Number between [1-604800]	Configure time to preserve a session (sec). It is enabled when selecting the 'Type' (except [per connection]) option at the [Connection Preservation] setting. For TCP connections, the request is sent to the same server until this time has elapsed. Default: 90
Customize Service Monitoring		If service monitoring parameters are set higher than necessary, false positives may occur.
Interval	Number between [1-99999]	Configure the interval to monitor VMs (sec). Default: 60
Time Out	Number between [1-99]	Configure the time out for packets to detect a failure on VMs (sec). Default: 10
Resending Frequency	Number between [0-99999]	Configure the number of retry packets to send. If it is set to 0, retry packets will not be sent. Default: 3
Operation on Server recovery	[Automatic Recovery] or [Manual Recovery]	Configure whether to reassign to a load balance group automatically or manually after VMs are restored.

5. When complete, click 'Ok', followed by 'Yes'.

6. Highlight the new group and click the 'Add Distributed Server' button which is now no longer grayed out.



7. Select the first desired server to be added to the load balancer from the drop down box and click 'Ok', answering 'Yes' to the warning message.



8. Repeat steps 4 to 5 for each additional server to add to the group. Note: you can only select Servers from the same network segment as the SLB

9. Click 'Regist' button to implement the changes when all required servers are added.

10. Click ' Yes', followed by 'No' to complete.

Changing the SLB Protocol

The SLB is capable of distributing requests using 4 protocols. These are:

- HTTP – For distributing standard Web Based Traffic between 2 or more servers. E.g. Standard Web Site
- HTTPS –For distributing secure Web Based Traffic between 2 or more servers. E.g. Secure Web Site dealing with financial transactions
- TCP- For distributing TCP requests from clients on a specific port between 2 or more servers e.g. Application Servers
- UDP – For distributing UDP requests from clients on a specific port between 2 or more servers e.g. Application Servers

The following table provides an overview to the Protocol related configuration options:

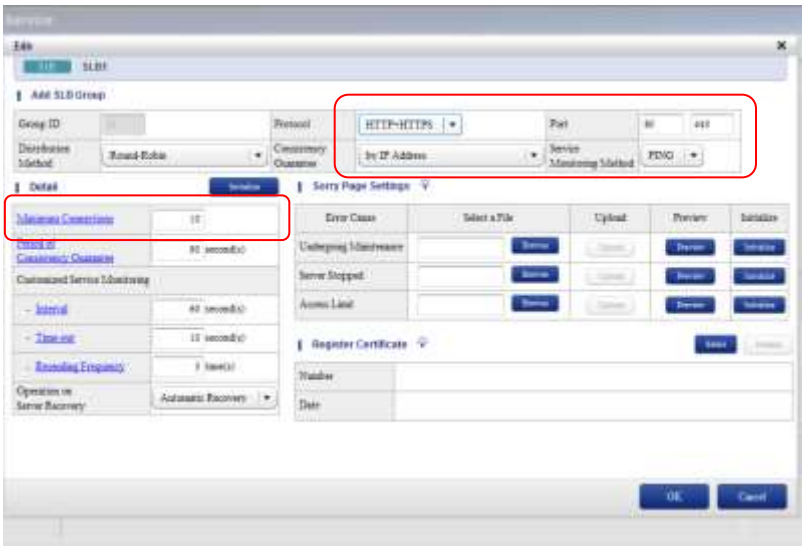
Item	Available setting	Description
Protocol	Select from [HTTP], [HTTPS], [HTTP + HTTPS], [UDP] or [TCP].	Select the protocol for distribution.
Port	Specify the port.	If Users select [HTTP], [HTTPS], [UDP], or [TCP] for the protocol, they specify one distribution port. If Users select [HTTP + HTTPS] they specify two distribution ports. If users select [HTTP+HTTPS], the same consistency preservation is applied to both HTTP and HTTPS communication. If Users select [HTTP] and [HTTPS] for different groups, different consistency preservation methods are applied.
Consistency Preservation	Select from [By Connection] [By IP Address] [By Cookie] [By Cookie-URL] [Cookie Client ID Insertion Method] [Cookie Server ID Insertion Method].	By Connection : TCP communication is forwarded to the same VM while a connection is established. If Users select [HTTP + HTTPS] for the protocol, this method is not available. By IP Address : The session is maintained based on client's source IP Address.

		By Cookie: The session is maintained based on the Cookie information specified by ServletAPI2.2. This method does not reference URL information. Cookie information specified by load balancing VMs should be unique among different VMs during periods of consistency preservation. If Users select [UDP] or [TCP], this method is not available. **By Cookie-URL:** The session is maintained based on the Cookie or URL information specified by ServletAPI2.2. Server applications use JavaServletAPI2.2 or better to create Cookie information [JSESSIONID=], or insert [jsessionid=] into the URL then notify the client. Firstly cookie information then URL information is referenced. Both Cookie and URL information should be unique among different VMs during periods of consistency preservation. If Users select [UDP] or [TCP], this method is not available. **[Cookie Information Example]** Set-Cookie: JSESSIONID=1234; **[URL Information Example]** http://www.test.com/index .html;jsessionid=1234 **Cookie Client ID Insertion Method:** SLB inserts a client ID (any value) into the cookie and the session is maintained by the relationship between the inserted client ID and the distributed VM. If users select [HTTP + HTTPS], [UDP] or [TCP] for the protocol, this method is not available. **Cookie Server ID Insertion Method:** SLB inserts the value processed from the IP Address / Port Number of VMs into the cookie (fixed value for each VM) and maintains the session. If Users select [HTTP+HTTPS], [UDP], or [TCP] for the protocol, this method is not available. Cookie client ID insertion based: SLB inserts client ID (any value) into the cookie, then session is maintained by the relationship between inserted client ID and distributed VM. If users select [HTTP+HTTPS], [UDP], or [TCP] for the protocol, this method is not available.

Max. Connection	Number between [1-58000] or [1-10000]	Maximum number of connections a SLB can handle. [HTTP], [UDP] or [TCP]: 1-58000 (Default: 58000) [HTTPS] or [HTTP+HTTPS]: 1-10000 (Default: 10000)

Specifying a Protocol of HTTP and / or HTTPS

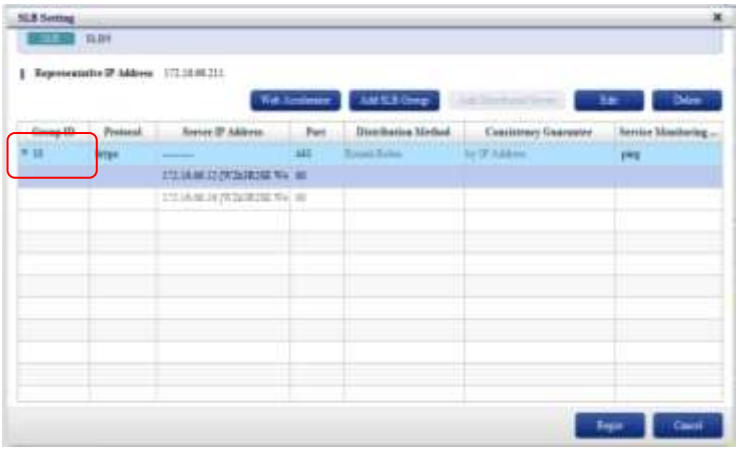
1. This is configured by editing the SLB group and changing the drop down box to either HTTP+HTTPS or HTTPS



2. If HTTP+HTTPS is specified then Ports 80 and 443 should be specified as above. If HTTPS is specified only, then port 443 should be configured as below:

3. Maximum Connections should also be between 1 and 10000 if HTTPS is set using either options.
4. To complete the protocol configuration, click 'Ok', 'Yes

5. Within the 'SLB Setting' screen, click the right facing arrow under GroupID, to show the member distribution servers.



6. Select each server in turn, click 'Edit' and allocate the server to the ports it will process

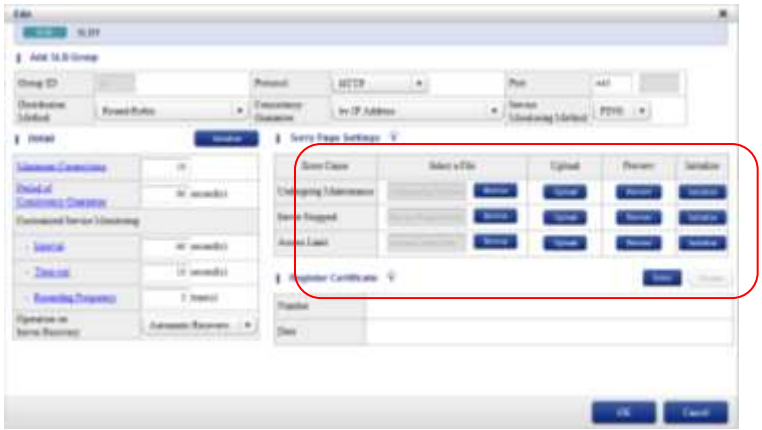
   If HTTPS is specified, then at least one server must be configured to handle port 443, likewise if HTTP is specified, one server must be configured for port 80. If HTTP+HTTP is selected, then both ports 80 & 443 should be specified

7. Click 'Ok' when ports are all set
8. Click 'Register', then 'Yes' to implement the changes.

Sorry Page Settings

The 'Sorry Page Settings' are available for configuration after a SLB Group has been registered. This allows the default web page for the following scenarios to be changed:

- Undergoing Maintenance: Web Page to display when all servers in group are in maintenance mode
- Server stopped: Web Page to display when all servers in group are powered off
- Access Limit: Message to display to requests, in access to the maximum number of connections that has been configured.



For each sorry page to override:

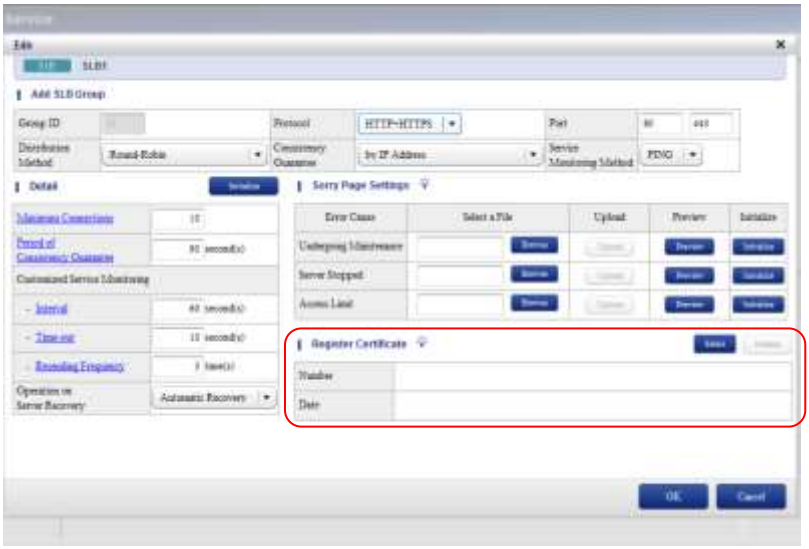
1. Click 'Browse' and locate the required HTML file
2. Click 'Upload' and 'Ok' for each.
   The Update button will become grayed out when successful, and browse box will become clear again.
3. To restore the default webpage, click 'Initialise'
4. Clicking 'Preview', will open a Browser showing the HTML file you have uploaded.
5. Commit changes by pressing 'Ok', then 'Regist' to exit

Sorry Page Settings		Configure a response page to show clients when HTTP requests cannot be distributed to targets by the load balancer. The page is in HTML format without any link to external files such as image files or style sheets.
Under Maintenance.	Upload HTML file.	Upload a response page when the status of all the targets is under maintenance or migrating to maintenance.
Server is Down.	Upload HTML file.	Upload a response page when the status of all the targets except the one with maintenance mode or migrating to maintenance is down.
Exceed Access Limits	Upload HTML file.	Upload a response page when requests exceed the maximum connection limit.

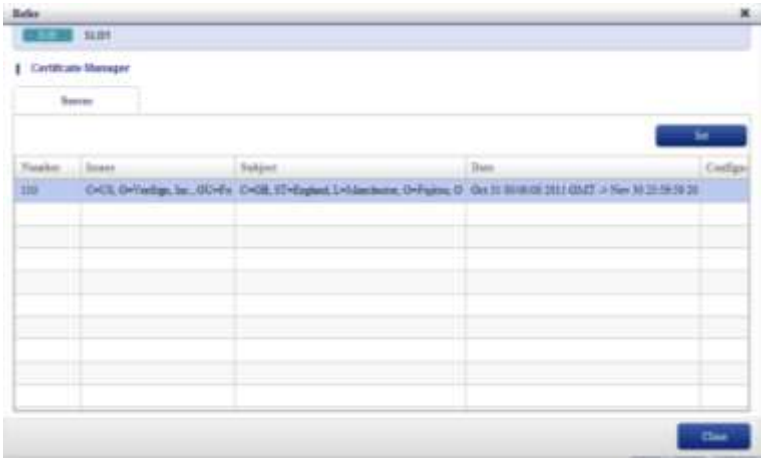
Certificate Registration

The Register Certificate Configuration options shown below, becomes available if protocol HTTP or HTTP+HTTPS are specified and the SLB has been configured to use certificates using Cert Manager (See SLB Certifcate Management)

1. Under 'Register' Certificate click 'Select'



2. Highlight the server certificate (see SLB Certificate Management) and click 'Set', answering 'Yes', then 'Ok'.



3. Click 'Close', 'Ok', 'Yes' & 'Register' to implement the changes and exit

SLB Certificate Management

A SSL certificate is required if the SLB is to load balance HTTPS requests. This requires each of the following sections to be performed:

Generate a CSR file

This section explains how to create a CSR file to be used by the third party certificate provider e.g. Verisign, when issuing a Server certificate.

The SLB configuration requires both the SSL server certificate and intermediate CA certificate from the certificate provider.

CSR file creation can be performed on any machine and does not have to be done inside a FUJITSU Cloud Service S5 VM.

> It is imperative that the private key created below, is kept in a safe and secure location. Please backup the private key and passphrase to media, other than the local hard disk, and place strict control over it.

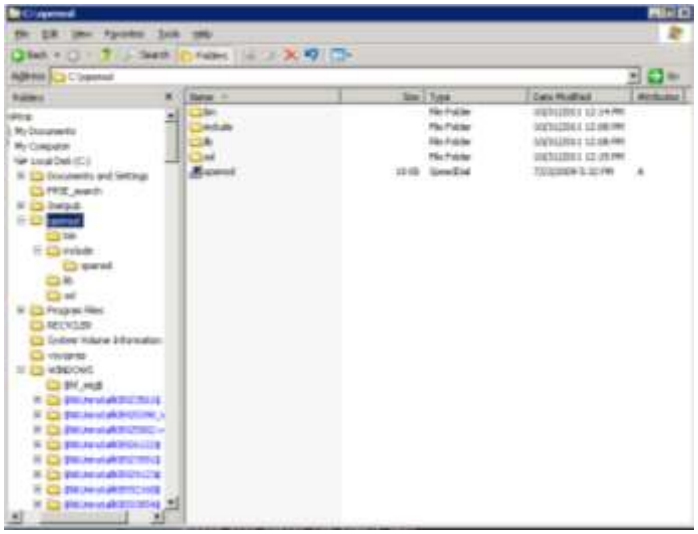
Generation Method with OpenSSL

1. Download the appropriate version of OpenSSL suited for your environment.
   For Windows, this can be downloaded from http://code.google.com/p/openssl-for-windows/downloads/list.

(The following instructions were performed using openssl-0.9.8k_Win32.zip on Windows 2003 Server.)

2. Unzip the downloaded file and copy the folder to the root of C:.

3. Rename the copied folder 'openssl'.
4. Within c:\openssl, create a folder called 'ssl'.



5. Copy the file c:\openssl\openssl to c:\openssl\ssl
6. Open a command prompt and change location to c:\openssl\bin

Note: The file names in the below instructions are an example only and can be changed to suit your environment

7. Use the following OpenSSL command to generate a pseudo random number to be used in the creation of the private key.

```
C:\openssl\bin> openssl md5 * > slb.rand
```

8. Create the private key file (slb.key) from the created pseudo random number file (slb.rand) using the following command. In the following example, encryption scheme is triple DES, with a 2048 bit private key.

```
C:\openssl\bin> openssl genrsa -rand slb.rand -des3 2048 > slb.key
```

9. Enter any passphrase to protect the private key (Enter same phrase twice).

```
Enter pass phrase:
Verifying - Enter pass phrase:
```

* Up to 20 letters of one-byte alphanumeric characters and [!"#$%&()=~|-^\@[;:]/ .,{`}*+_ ><] are available for passphrase.
* Passphrase is required for certificate registration. Please set a passphrase.

10. Use the following command to create the CSR file (slb.csr) from the generated private key file (slb.key).

```
C:\openssl\bin> openssl req -new -key slb.key -out slb.csr
```

11. When prompted to enter the passphrase of the private key, enter the passphrase specified at step 9.

```
Enter pass phrase for slb.key:
```

12. You will then be prompted with a serious of questions, which should be answered according to your environment.

    The following is shown as an example:

    [Country Name] Enter half-width capital letters (2 words) which represent the country code.

```
Country Name (2 letter code) : GB
Organization Name (eg, company): Fujitsu
Locality Name (eg, city) : Manchester
Organizational Unit Name (eg, section) []: TFS
```

    [Common Name] Enter the URL for your website. Note: IP address is not allowed
    Example: In case of <https://www.sample.co.uk/> -> Enter <www.sample.co.uk>

```
Common Name (eg, your name or your server's hostname) []: www.sample.co.uk
```

    The rest are unnecessary items and should be skipped by pushing [Enter] key without entering any value.

```
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

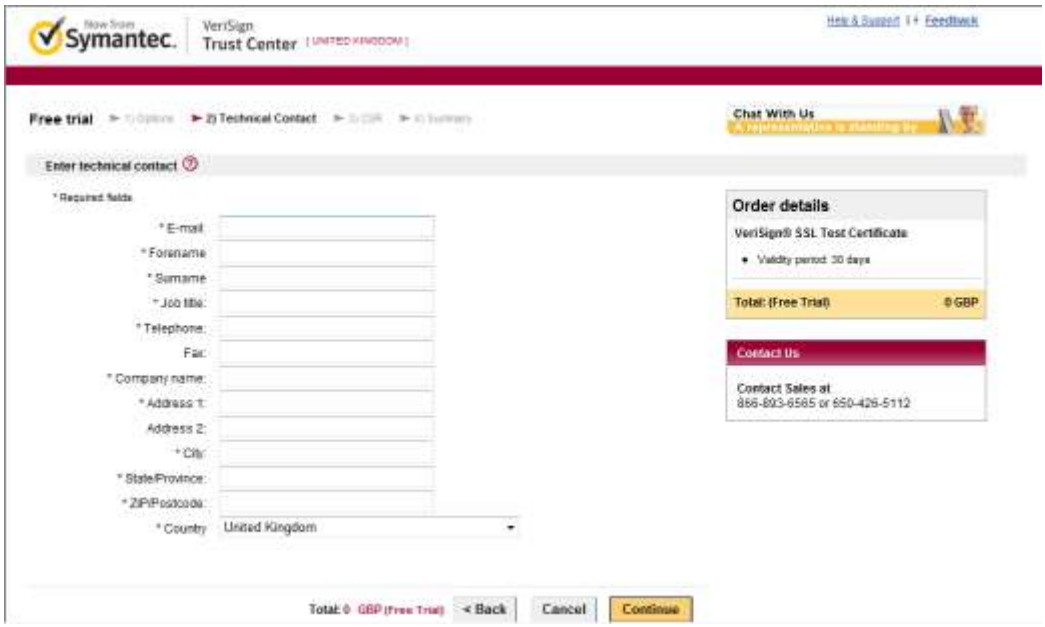
    CSR file (slb.csr) is generated and saved in c:\openssl\bin.

```
# cat sample.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICtDCCAZwCAQAwbzELMAkGA1UEBhMCS1AxDjAMBgNVBAgTBVRva3lvMQ4wDAYD
VQQHEwVUb2t5bzEVMBMGA1UEChMMRnVqaXRzdSBMdGQuMQ8wDQYDVQQLEwZTQU1Q
TEUxGDAWBgNVBAMTD3d3dy5zYW1sZS5jby5qcDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAOTI8gdUn8wt8PzxY08lXvJL7/lgkm0K1ulFHwJ13aST+nxn
mz6WiGji+BlAxkatL9tK23dEERKGyxk7BEtTecgZxZ4hGeZWMaooSYZPDQLJ1rci
5PsDBubhhJwWxpVis7Hw8/Ex9HwmSc+13dSS5RH8EzjlVfZ/dWUcIdgzzy8zCHLV
mwokRdSi+sOEcNrxXTp2lRiz22SIC34A7b+gKnMmv5moVObO0r15UYOXf+sKdoSN
/i+ZRnoz2hB1iYaXThpBV7dyBwPgaSgoCn1g98oXkhjRAI9/oN3aLUnU7++9EwOO
H1J/SJmTTlut2UPKd+yWDi4gfnyMla0gx0Y+nrcCAwEAAaAAMA0GCSqGSIb3DQCB
BQUAA4IBAQCH93UgfDNapEsVu91YTZ+KH9GAVIF1ikNAQuJREYG2kNPFd2uWxKIr
aVsknJyKpxgqwbnxAeWVwwdzcKVvu17UCvzBbZbWrV6cndscqV4XoxS5dweyfsTn
rDXntej4bR9QOvr9iQ5WzMHOxTEoWSUjuOaV9ZMQSTfzMy9SRC9XWc9R3Mbzi0tg
yB9ZwUJjBDqUW9Ecs+gnrnnPW4jJgWz89yF+4l9lOW9YVdm6SOQmAUkR5sJz0rxlD
6wkYPxxPKzv4OCmIeXjCWjRa/zCFQx22vMyzuOOLMcr611+npNN928AVJC3KrTzj
71MHWTXkFOpFhlYV7GtE4wl3e+YIwMSw
-----END CERTIFICATE REQUEST-----
```

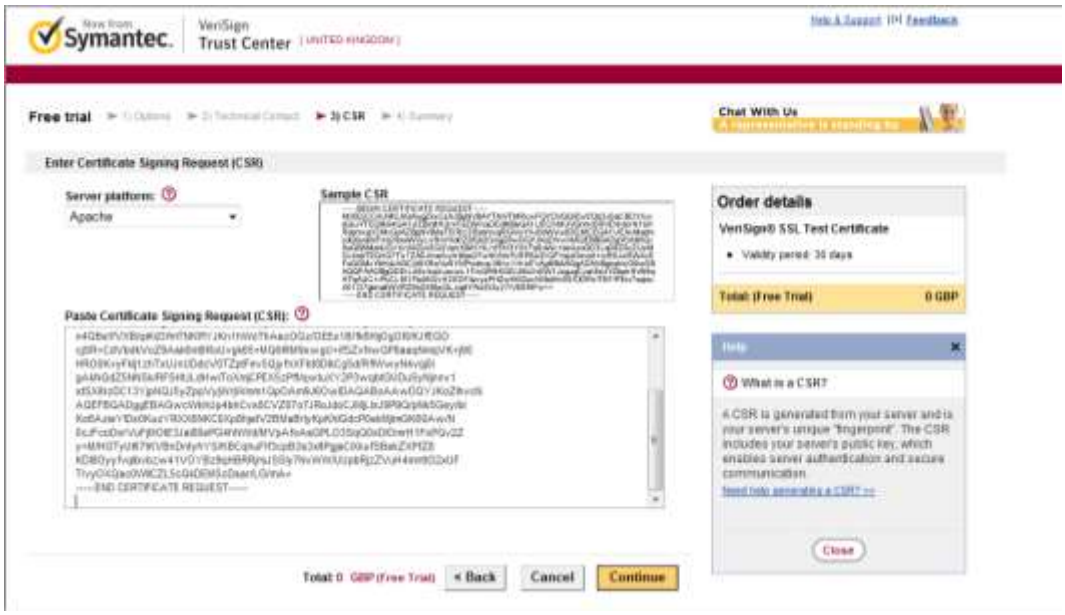
Obtain Server Certificate from CA

You should now obtain the server certificate from your CA. The following steps show how to obtain a trial test certificate from Verisign:

1. Go to http://www.verisign.co.uk/ssl/free-trial/
2. Select 'Get Free trial' under 'Option 2 - VeriSign® SSL Test Certificate'
3. Click 'Continue'



4. Complete your details and click 'Continue'
5. Specify server platform as 'Apache' and paste in contents of csr file (SLB.csr) and click 'Continue'



6. Tick 'I Accept….' and then 'Submit'
7. You will receive an email from support@verisign.co.uk containing your server certificate and links to root and intermediate certificates

8. Copy the certificate (example as shown below) from the end of the email and paste into notepad, saving it as c:\openvpn\bin\server.csr

-----BEGIN CERTIFICATE-----
MIIGLjCCBRagAwIBAgIQQyDbyFDAxJE+9k30/qrKezANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwOTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNl
cnZlciBDQSAtIEcyMB4XDTExMTAzMTAwMDAwMFoXDTExMTEzMDIzNTk1OVowggEB
MQswCQYDVQQGEwJHQjEQMA4GA1UECBMHRW5nbGFuZDETMBEGA1UEBxQKTWFuY2hl
c3RlcjEQMA4GA1UEChQHRnVqaXRzdTEMMAoGA1UECxQDVFNEMTwwOgYDVQQLFDNU
ZXJtcyBvZiB1c2UgYXQgd3d3LnZlcmlzaWduLmNvLnVrL2Nwcy90ZXN0Y2EgKGMp
MDUxIjAgBgNVBAsTGUF1dGhlbnRpY2F0ZWQgYnkgVmVyaVNpZ24xJzAlBgNVBAsT
Hk1lbWJlciwgVmVyaVNpZ24gVHJ1c3QgTmV0d29yazEgMB4GA1UEAxQXZmdjcC5k
eW5kbnMtYXQtd29yay5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDVAeVlIlBqPRhgQ8f3EIqgkSj/rK0hIb9xo+NXEGd9JEKfgYF5/9VcH+qIp3d+
ZM0o8hgkqfWFahOECxw4bP84QTHUH9+ToeKM6A5H8ol8QY5yNJH4J1Vt2RWhn0Cy
TqYFGhS+CTrn4xDohEz3HCBT6J9Jm83BA/xpqo2apUr6P3QdE7Qq/IWQiPXOFPFQ
mdQN1xXRNmm0V6/ICPJ+dcVu3wMiQKDI39F8hbDI3i+qPSKACQ1B1nk01KT9EVIe
0kt0fCJOheaMI8RfnM9+3+rC25djY/fCpu0ZQO5LI2Oee/XG1JeI3MMLXdiOk1An
nJmmlXKNauNaabVCk4Cb0no7AgMBAAGjggHTMIIBzzAJBgNVHRMEAjAAMAsGA1Ud
DwQEAwIFoDBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSVHJpYWwtRzItY3Js
LnZlcmlzaWduLmNvbS9TVlJUcmlhbEcyLmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG
+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nw
cy90ZXN0Y2EwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQY
MBaAFCgXE4q91qK13AYst7aO2hBmYG7lMHQGCCsGAQUFBwEBBGgwZjAkBggrBgEF
BQcwAYYYaHR0cDovL29jc3AudmVyaXNpZ24uY29tMD4GCCsGAQUFBzAChjJodHRw
Oi8vU1ZSVHJpYWwtRzItYWlhLnZlcmlzaWduLmNvbS9TVlJUcmlhbEcyLmNlcjBu
BggrBgEFBQcBDARiMGChXqBcMFowWDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIa
BBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5j
b20vdnNsb2dvMS5naWYwDQYJKoZIhvcNAQEFBQADggEBAC7hXVU9S3RoGccRxA/a
IIi+diLxd9qI9Tk7O0ihopHAoVlBEG+XFO/OR4JDxrgIIOooVRRCzN3vFzdzzOKA
zred8Ix2u83SQngw6yMtyi3wW8G/P6s0Hvz+IARy1WfXHxSj75CInZaxWMhPtzjE
0QkHLnKAPlrq7LotPSCu5XJxcHDWIAC30EzLkNjkCP44lAvimYMd1TAHUrkwoZVv
RVKHp8dwI2gm0LDUPk2ZLDzxOmkg4Co1thchjmGKSNeOX/a1qdpazs/idQ+cR2bR
M8PsPyDkfb5MDshIcIcLB80SEwO44NwPVQAqf1ykeskhqR6MHwlxyUv5bQ3rJdis
MNM=
-----END CERTIFICATE-----

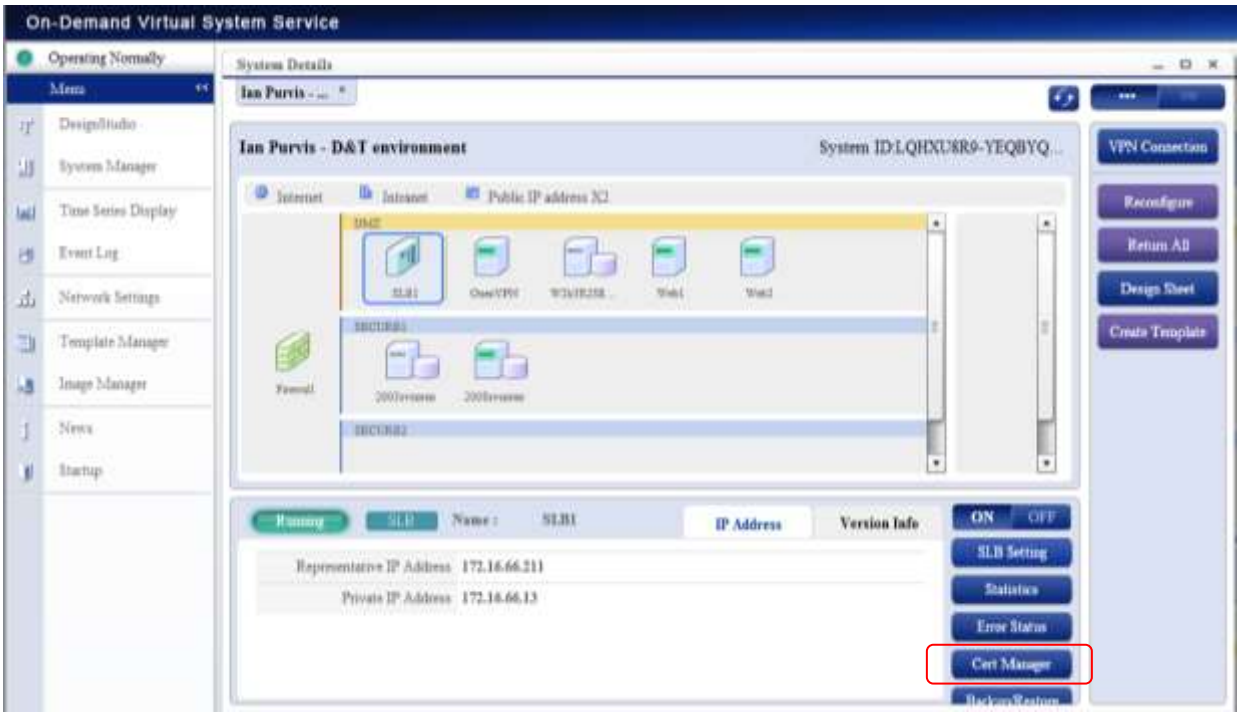
9. Follow the link in step 2 of the email, copy and paste the intermediate certificate into the file c:\openvpn\bin\intermediate.csr
10. Run the command

```
C:\openssl\bin>openssl pkcs12 -export -in server.csr -inkey slb.key -certfile intermediate.csr -out slb.pfx
```

11. Enter pass phrase for slb.key specified earlier:
12. Enter Export Password:
    Re-enter password to Verifying it
13. Slb.pfx is created in c:\openssl\bin

Uploading Certificate to SLB

1. Within System Manager, highlight the SLB and select the 'Cert Manager' button



2. In the resulting window, select the 'CA' tab
3. Click 'Register', then enter a 3 digit number greater than or equal to 100, browse to the intermediate file called intermediate.csr

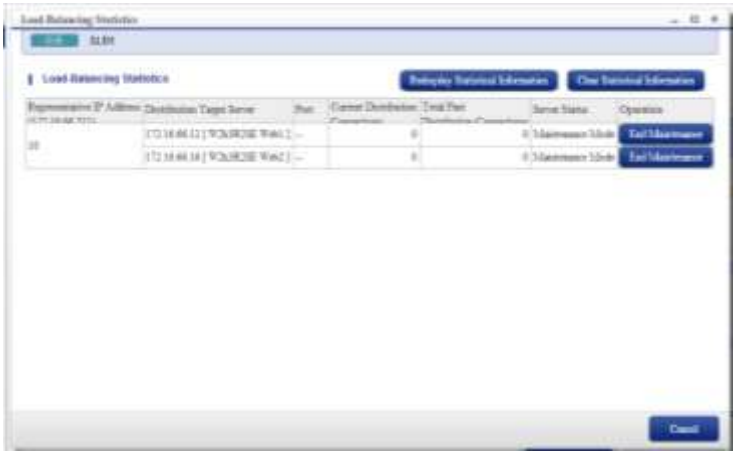
4. Click 'Register' and 'Ok' to message dialogue
5. Click Server tab, enter a 3 digit number greater than 100 and browse for slb.pfx created earlier.
6. Enter the password specified earlier and click 'Registr"

7. Click 'Ok' to success dialog box and then 'Close'

Placing Load Balanced Servers into Maintenance Mode

Users can switch VMs in load balance groups to Maintenance Mode (detach from the group) or recover from Maintenance Mode (reassign to the group).
Users can select to either 'Migrate to Maintenance Mode Immediately' or 'Specify the Session Monitoring Period of Time to Migrate to Maintenance Mode'. If Users choose the latter, the switch occurs after the period of time specified by Users between 1 and 120 minutes.

1. From 'System Manager | System Details' menu, select the 'Statistics' Button.
2. Click 'Start Maintenance' button alongside each server in the group to view maintenance mode options.
3. Click 'Ok' to put the server into maintenance mode straight away, or select option two and specify the delay required in minutes and then click 'Ok'. Click 'Ok' to commit.
4. Select to remove a server from maintenance mode, click 'End Maintenance'.



Status Messages of a VM under an SLB:

■ In Operation
VMs have been assigned to a load balance group. Traffic will be distributed between VMs.

■ Migrating to Maintenance
Users have started the operation to migrate VMs to Maintenance Mode. Traffic is preserved and if the session is being preserved, new traffic is sent to the same VM. If not, it will be distributed to another VM. A VM is migrated to maintenance mode after a period of time specified by the user.

■ Under Maintenance
The operation to migrate a VM or recover a VM configured as "Manual Recovery" has been started. Current traffic will be disconnected and new connections will not be accepted.

■ Out of Service
A failure has been detected on a VM and been detached from a load balancer. Current traffic will be disconnected regardless of the preservation of a session and new traffic will not be accepted.

The 'Statistics' screen also shows the number of connections that each VM in the load balance group is processing, as well as the total number of connections that have been processed. Users can also clear the information and the total number of connections processed after the clearance is shown.

Error Status

The 'Error Status' button displays the number of error responses in a certain time period and the total amount of error responses of each load balance group. Users can also clear the information and the total number of error responses processed after the clearance is shown.

The following items are displayed:

■ Number of Connections
The number of received connections. Resent SYN packets are not included.

■ Error (Under Maintenance)
The number of error responses if all VMs in a load balancer group are Under Maintenance or Migrating to Maintenance Mode.

■ Error (While Server is Down)
The number of error responses if all VMs in a load balancer group (except the ones Under Maintenance or Migrating to Maintenance Mode) are down.

■ Error (Access limits)
The number of error responses when the number of connections exceed the maximum limit.

Backup and Restore

The configuration of a SLB is backed up and restored within the portal, in the same way as a VM.

Contact

FUJITSU Cloud Service S5 Team
FUJITSU
E-mail: GlobalCloud@us.fujitsu.com
Website: us.fujitsu.com