What You Make Possible
Application Load Balancing

Jeff Ostermiller
Content Programs

7 Educational Tracks
• Borderless Networks
  • Network Infrastructure & Systems
  • Security
  • Mobility
• DC & Virtualization
• Collaboration
• Video
• Service Provider
• BYOD
• Cloud

Sub-Programs
• Certifications

Additional Programs:
• IT Management
• IT Executive Symposium
• Cisco-on-Cisco Case studies
• Public Sector General Session
• Collaboration User Group
• CCIE Practical Exam
• Architecture Town Halls
• Cisco Developers Network
• Product and Solution Sessions

Experiential Learning:
• Technical Solutions Clinic
• Meet the Engineer
• Walk-In Self Paced Labs
• Table Topics
ACE Deployment in an Application Environment
BRKAPP-2020
Agenda

- Load Balancing Today’s Web Application
  - Benefits of Traffic Management
  - Introduction to ACE
  - Design Considerations
  - Probes, Persistence, Predictors
  - Server Offload

- Templatized Configuration

- Linking VMware VCenter manager to the ANM 5.1

- Deploying VMware View w/Cisco ACE

- Microsoft Deployments
  - ACE for Microsoft Exchange 2010
  - ACE for Microsoft SharePoint 2010

- ACE Support for IPv6
Load Balancing Today’s Web Applications

What are the Challenges?

- Virtual Data Center introduces new challenges for load balancers and application management
  - Transition to Virtual Machines (VMs) using Vmware and Microsoft Hyper-V technology
  - Servers that used to be stand-alone are now VMs
  - Virtual data center requires orchestration of the application, VM server and switching infrastructure
Application Delivery Controller

- Benefits of Traffic Management - Why application delivery Controller:
  - Availability
  - Scalability
  - Performance
  - Security

- The Cisco Application Control Engine (ACE) provides validated solutions for Microsoft applications

Cisco ACE 4710
0.5 – 4Gbps

Cisco ACE30 Module
4–16 Gbps

Cisco vACE
Design Considerations

One Armed Mode
- Load Balancers not inline
- Allows direct server access
- Requires Source NAT, PBR, or RISE

Routed Mode
- Easy to deploy
- Requires at least two IP subnets
- Servers in dedicated IP subnet

Bridged Mode
- Easy migration for servers
- Requires one IP subnets
- Recommend for non-LB traffic
Introduction to ACE Load Balancer

- Cisco ACE provides many advanced load balancing feature which can be applied to meet challengers with deploying today's applications

1. Access-control (permit or deny a request)
2. Management traffic
3. TCP normalization/connection parameters
4. Server load balancing
5. Fix-ups/application inspection
6. Source NAT
7. Destination NAT
Virtual Context Setup

- Virtual contexts are virtualized ACEs. Each virtual context has independent configuration and dedicated resources assigned. One context can pull resources from another.

Virtual Virtualization of Microsoft Exchange 2010

A separate virtual machine for each of the roles: Two Client Access Server, Hub Transport, Four Mailbox in a DAG (Database Availability Group)
Basic Load Balancing for ERP Applications

- **Predictors**
  - How can you balance the connections?

- **Probes**
  - Is the server active? How can you check?

- **Persistence**
  - How do you keep the client connected to the same server?
Health Probes
SAP Enterprise Portal

SAP Library
SAP Library contains the complete documentation for SAP Web Application Server.

Web Services Navigator
Web Services Navigator is a tool that gives you a short overview of a specific Web service based on its WSDL, and enables you to test your Web service by creating and sending a client request to the real end point.

System Information

UDDI Client

/index.html
/lirj/portal
Health Checks

Watch the Expected Status Code

ACE/dc\# telnet 169.145.90.16 50100
Trying 169.145.90.16...
Connected to 169.145.90.16.
Escape character is '^]'.
GET /nwa HTTP/1.1
Host: 169.145.90.16

HTTP/1.1 302 Found
server: SAP NetWeaver / AS Java 7.1
content-type: text/html
location:
http://169.145.90.116/webdynpro/dispatcher/sap.com/tc~lm~itsam~co~ui~nwa~localnavigation~wd/NWAApp
# Probe Defaults

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Min Time</th>
<th>Max Time</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>Time between successful probes</td>
<td>2</td>
<td>65535</td>
<td>120</td>
</tr>
<tr>
<td>FailDetect</td>
<td>Number of failed probes before marking as failed</td>
<td>1</td>
<td>65535</td>
<td>3</td>
</tr>
<tr>
<td>PassDetect Interval</td>
<td>Time to send a probe when a server is marked as failed</td>
<td>2</td>
<td>65535</td>
<td>300</td>
</tr>
<tr>
<td>PassDetect Count</td>
<td>Number of successful probes before marking the server as passed</td>
<td>1</td>
<td>65535</td>
<td>3</td>
</tr>
<tr>
<td>Open</td>
<td>time for a successful 3-way handshake</td>
<td>1</td>
<td>65535</td>
<td>10</td>
</tr>
<tr>
<td>Receive</td>
<td>time for getting a response, ie. send a GET, wait for a reply</td>
<td>1</td>
<td>65535</td>
<td>10</td>
</tr>
</tbody>
</table>
To configure a real server to remain in the OPERATIONAL state unless all probes associated with it fail (AND logic), use the fail-on-all command in real server host configuration mode.

```plaintext
probe http BasicHTTP_02-probe-1
  interval 5
  passdetect interval 5
  request method get url /index.htm
  expect status 200 499
  open 10

probe scripted SQL_USER
  interval 5
  passdetect interval 10
  script SQL_PROBE SQL_User Success 0

serverfarm host BasicHTTP_02
  failaction purge

probe BasicHTTP_02-probe-1
probe SQL_USER
rserver 192.168.11.1 80
  inservice
rserver 192.168.11.2 80
  inservice
rserver 192.168.11.3 80
  inservice
```
Predictors - Application Response

- Load balancing based on server response time; response time calculated over a configured number of samples and supports the following options:

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN to SYN-ACK</td>
<td>Time between SYN send from ACE to SYN-ACK received from the server</td>
</tr>
<tr>
<td>SYN to Close</td>
<td>Time between SYN send from ACE to FIN/RST received from the server</td>
</tr>
<tr>
<td>Application Request to Response</td>
<td>Time between HTTP request send from ACE to HTTP response received from the server</td>
</tr>
</tbody>
</table>
Predictors - Application Response

- Measures the response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request.

---+---------------------+------+------------+----------+----------+---------
rservr: TCP80-SF
172.16.29.10:0    8    OPERATIONAL  0    239287    32
[Real Server] Predictor (1)

Response Type: App-Req-To-Resp
Response Samples: 8
Weight Connection: ✓

serverfarm TCP80-SF
predictor response app-req-to-responserserver SERVER1
inservice
rservr SERVER2
inservice

---+---------------------+------+------------+----------+----------+---------
real weight state current total failures
rservr: TCP80-SF
172.16.29.10:0  8 OPERATIONAL  0  239287  32
max-conns : - , out-of-rotation count : -
min-conns : -
conn-rate-limit : - , out-of-rotation count : -
bandwidth-rate-limit : - , out-of-rotation count : -
retcode out-of-rotation count : -
average response time (usecs) : 228
# Session Persistence Methods

## How to Uniquely Identify a Client…

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Cookie</th>
<th>SSL ID</th>
<th>HTTP Redirect</th>
<th>RDP</th>
<th>SIP</th>
<th>GPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Does It Work</td>
<td>Client= its SRC IP</td>
<td>client = a cookie value</td>
<td>client = SSL session ID</td>
<td>LB Redirects to Specific (V)Server</td>
<td>SD, Session Directory, Routing Token = server IP + Port</td>
<td>Client = Session Call-ID</td>
</tr>
<tr>
<td>Variation</td>
<td>Full IP Masked IP</td>
<td>Static Dynamic Insert</td>
<td>Full SSID Offset</td>
<td></td>
<td></td>
<td>custom</td>
</tr>
<tr>
<td>Info Stored on</td>
<td>LB</td>
<td>LB</td>
<td>LB</td>
<td>Client</td>
<td>LB</td>
<td>LB</td>
</tr>
<tr>
<td>Good For</td>
<td>Simplicity</td>
<td>Flexibility</td>
<td>No Cookie support</td>
<td>No State on LB</td>
<td>Recovering Disconnected WTS sessions</td>
<td>SIP-specific stickiness</td>
</tr>
<tr>
<td>Caveats</td>
<td>Proxies</td>
<td>HTTP only Clear Test</td>
<td>SSL v3 Renegotiation</td>
<td>HTTP only Absolute URLs Bookmarks</td>
<td>No Token, needs to fall back to source IP</td>
<td></td>
</tr>
</tbody>
</table>
Session Persistence

- When customers visit an e-commerce site, they usually start out by browsing the site.
- Depending on the application, the site may require that the client become "stuck" to one server once the connection is established, or the application may not require this until the client starts to build a shopping cart.
- This is known as stickiness or session persistence.
- Prior to ACE 4.X, sticky connections require a resource class to be configured. If your forget ANM will send you the following message.
Basic ERP Web Load Balancing

Persistence Options

- Configuration shows two different sticky options; HTTP Cookie insert and source IP sticky
Basic ERP Web Load Balancing

Persistence Options

- Configuration shows two different sticky options; HTTP Cookie and source IP sticky

```plaintext
sticky http-cookie ILIKECOOKIES
    cookie insert
    timeout 720
    serverfarm HTTP-SF

sticky ip-netmask 255.255.240.0 address source
    serverfarm HTTPS-SF

policy-map type loadbalance first-match WEB-PM
    class class-default
        sticky-serverfarm

policy-map type loadbalance first-match TCP80-PM
    class class-default
        sticky-serverfarm
```

© 2012 Cisco and/or its affiliates. All rights reserved.
Basic ERP Web Load Balancing

Create new rule

Click View then Edit to modify

What are you looking for?

What do you want to do when you find it?

© 2012 Cisco and/or its affiliates. All rights reserved.
Basic ERP Web Load Balancing

```plaintext
sticky http-cookie ILIKECOOKIES COOKIESTICKY
  cookie insert browser-expire
  serverfarm TCP80-SF
!
policy-map type loadbalance first-match HTTP-PM
  class class-default
    sticky-serverfarm COOKIESTICKY
policy-map multi-match LOADBALANCE
  class HTTP-CM
    loadbalance vip inservice
    loadbalance policy HTTP-PM
interface vlan 2
  ip address 10.10.119.55 255.255.255.0
  access-group input EVERYONE
  service-policy input LOADBALANCE
  service-policy input REMOTE-MGMT
```
Basic ERP Web Load Balancing

class-map match-all TCP80-CM
  2 match virtual-address 10.10.119.112 tcp eq 80
rserver host SERVER1
  ip address 10.10.119.1
  inservice
rserver host SERVER2
  ip address 10.10.119.222
  inservice
probe tcp TCP80-PROBE
  interval 10
  port 80
  passdetect interval 10
  passdetect count 3
probe http HTTP-PROBE
  interval 20
  passdetect interval 5
  request method get url /index.html
  expect status 200 499

serverfarm TCP80-SF
  probe TCP80-PROBE
  probe HTTP-PROBE
  predictor leastconns slowstart 200
rserver SERVER1
  inservice
rserver SERVER2
  inservice
sticky http-cookie ILIKECOOKIES COOKIESTICKY
  cookie insert browser-expire
serverfarm TCP80-SF

policy-map type loadbalance first-match HTTP-PM
   class class-default
      sticky-serverfarm COOKIESTICKY
policy-map multi-match LOADBALANCE HTTP-CM
   loadbalance vip inservice
   loadbalance policy HTTP-PM
interface vlan 2
  ip address 10.10.119.55 255.255.255.0
  access-group input EVERYONE
  service-policy input LOADBALANCE
  service-policy input REMOTE-MGMT
no shutdown
Basic ERP Web Load Balancing

Simple or Complex?

Select *NEW

New Options Dynamically Appear

Increase Header Max Parse Length Case-Insensitive
URL Parsing (Advanced Mode)

How to look for the data

What are you looking for?
Cookies
Directories?
Headers?

Now you found it, now what?

Now for the Regex Expression

© 2012 Cisco and/or its affiliates. All rights reserved.
Basic ERP Web Load Balancing

Where's the Cookie?

Default Header Parse Length 2K

parameter-map type http INSENSITIVE
case-insensitive
persistence-rebalance
set header-maxparse-len 8192
policy-map multi-match LOADBALANCE
class HTTP-CM
loadbalance vip inservice
loadbalance policy SAP-PM
appl-parameter http advanced-options INSENSITIVE

switch/SAP-Datacentre# show stats http
+------------------------------------------+
| HTTP statistics                        |
+------------------------------------------+
| LB parse result msgs sent : 151        |
| Inspect parse result msgs : 0          |
| TCP fin/rst msgs sent : 8              |
| SSL fin/rst msgs sent : 18             |
| Drain msgs sent : 118                  |
| Reuse msgs sent : 0                    |
| Reproxed requests : 0                  |
| Headers inserted : 254                 |
| HTTP chunks : 37                       |
| HTTP unproxy conns : 14                |
| Whitespace append : 0                  |
| Response entries recycled : 110        |
| Header insert errors : 0               |
| Static parse errors : 0                |
| Invalid path errors : 0                |
| TCP data msgs sent : 152               |
| SSL data msgs sent : 495               |
| Bounced fin/rst msgs sent: 8           |
| Unproxy msgs sent : 14                 |
| Particles read : 1718                  |
| HTTP requests : 156                    |
| Headers removed : 0                    |
| HTTP redirects : 0                     |
| Pipelined requests : 0                 |
| Pipeline flushes : 0                   |
| Second pass parsing : 0                |
| Analysis errors : 0                    |
| Max parse len errors : 3               |
| Resource errors : 0                    |
| Bad HTTP version errors : 0            |

© 2012 Cisco and/or its affiliates. All rights reserved.
URL Parsing

class-map type http loadbala match-any URL-MATCHING
    2 match http url .*

class-map type http loadbala match-any URL-IMAGE
    2 match http url /image/.*

class-map match-all HTTP-CM
    2 match virtual-address 172.16.1.73 tcp eq 80

serverfarm IMAGE-SF
    probe IMAGE-PROBE
    rserver IMAGE1 inservice
    rserver IMAGE2 inservice

serverfarm WEB-SF
    probe WEB-PROBE
    rserver SERVER1 inservice
    rserver SERVER2 inservice

sticky http-cookie IMAGE-COOKIES IMAGECOOKIE
    cookie insert browser-expire
    serverfarm IMAGE-SF backup WEB-SF

sticky http-cookie WEB-COOKIES WEBCOOKIE
    cookie insert browser-expire
    serverfarm WEB-SF

! policy-map type loadbala first-match HTTP-PM
    class URL-IMAGE
        sticky-serverfarm IMAGE-COOKIE
    class URL-MATCHING
        sticky-serverfarm WEB-COOKIE

policy-map multi-match L4
    class HTTP-CM
        loadbalance vip inservice
        loadbalance policy HTTP-PM
        appl-para http advanced-option INSENSITIVE

© 2012 Cisco and/or its affiliates. All rights reserved.
Server Offloading
SSL Server Offload

- To terminate or initiate HTTPS connections with ACE, the virtual context must have at least one SSL proxy service. An SSL proxy contains the certificate and key information needed to terminate HTTPS connections from the client or initiate them to the servers.

- ANM (Application Network Manager) provides you with a guided setup to import an SSL key pair into the ACE.
Sample SSL Key/Cert Pair

- ACE shipped with a default RSA 1024 bit. Certificate is based on this key pair
- The sample certificate and key are named `cisco-sample-cert` and `cisco-sample-key`
- You can view the sample SSL key and cert

- The sample SSL key and cert files can be exported using the ‘crypto export’ command
HTTP to HTTPS Redirect via the GUI

More Manual via Device manager than I want... Think Templates, more to come in the next section

---

appropriate template

Do you need to redirect HTTP to HTTPS?

%H = Domain Name


%P = Path

Description: Generic Secure Webserver with redirect

Appropriate template

What are you going to redirect them to?
Basic SSL Load Balancing

Redirecting Clients to Use SSL

```bash
rserver redirect REDIRECT
    webhost-redirection https://%h%p 302
    inservice

serverfarm redirect REDIRECT-SF
    rserver REDIRECT
    inservice

! class-map match-all HTTP
    2 match virtual-address 172.16.1.73 tcp eq 80

policy-map type loadbalance first-match REDIRECT-PM
    class class-default
        serverfarm REDIRECT-SF

! policy-map multi-match LOADBALANCE
    class HTTP
        loadbalance vip inservice
        loadbalance policy REDIRECT-PM
```

http://www.cisco.com/go/ace

https://www.cisco.com/go/ace
SSL Server Offload Configuration

- In order to configure SSL, you need to add the following to a L3 / L4 class map:
  - `parameter-map type ssl`
  - `ssl-proxy service`
  - `policy-map`

- `parameter-map` is used to define parameters for SSL connections (e.g., SSL version, cipher suites, close protocol behavior)

- `ssl-proxy` is used to define the certificates and keys to be used in SSL connections
SSL Packet Flow with ACE

Client

---

SYN (tcp—443)
SYN SYN/ACK ACK
SSL Handshake

HTTPS—GET index.html
Accept-Encoding: gzip, deflate
HTTPS—Response

---

Server

TCP Flow

HTTP—GET index.html
HTTP—200 Ok Response
index.html

---

ssl-proxy service CLIENT-SSL
  key mykey.pem
cert mycert.pem

! serverfarm WEB-PROTOCOLS
  rserver SERVER1 81
     inservice
  rserver SERVER2 81
     inservice
  probe HTTP-GET

! policy-map type loadbalance first-mat SSL-PM
  class class-default
    serverfarm WEB-PROTOCOLS
  ! policy-map multi-match L4
    class HTTPS-CM
      loadbalance vip inservice
      loadbalance policy SSL-PM
      loadbalance vip icmp-reply
    ssl-proxy server CLIENT-SSL

class-map match-all HTTPS-CM
  2 match virtual-address 172.16.1.73 tcp eq 443

© 2012 Cisco and/or its affiliates. All rights reserved.
Basic SSL Offload Example

rserver host SERVER1
ip address 192.168.1.1
inservice
rserver host SERVER2
ip address 192.168.1.2
inservice

probe http HTTP-GET
interval 5
port 81
passdetect interval 3
request method get url /secure/index.html
expect status 200 200

parameter-map type ssl CLIENT_PARAM
cipher RSA_WITH_RC4_128_MD5 priority 2
cipher RSA_WITH_AES_128_CBC_SHA priority 3
cipher RSA_WITH_AES_256_CBC_SHA priority 5
session-cache timeout 600
ssl-proxy service CLIENT-SSL
key mykey.pem
cert mycert.pem
ssl advanced-options CLIENT_PARAM

class-map match-all HTTPS-CM
2 match virtual-address 172.16.1.73 tcp eq 443

serverfarm WEB-PROTOCOLS
pro rserver SERVER1 81
inservice
rserver SERVER2 81
inservice

! sticky http-cookie WEBCOOKIE STICKYCOOKIE
cookie insert
serverfarm WEB-PROTOCOLS

! policy-map type load first-match SSL-PM
class class-default
sticky-serverfarm STICKYCOOKIE
policy-map multi-match L4
class HTTPS-CM
loadbalance vip inservice
loadbalance policy SSL-PM
loadbalance vip icmp-reply
ssl-proxy server CLIENT-SSL
Standardization with Templates
Why Templates

- Standardization
- Simplify
- Best Practices
- Customization
- Portability of rules

http://developer.cisco.com/web/anm/application-templates
Template Considerations

- Templates do not know all local configuration
- Configure Reals first with names then use Templates
- Templates are for multiple devices so must be abstracted
  - Examples DR, QA, Test, Production
Working with Templates

Templates do not know all local configuration. Configure Reals first with names then use Templates. Templates are for multiple devices so must be abstracted.

Examples DR, QA, Test, Production
Microsoft Exchange Template Code

```xml
<template xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  applicationType="Microsoft Exchange 2010" version="1.1"
  xsi:noNamespaceSchemaLocation="file:application_template_v2.xsd"
  description="MS Exchange Template" showInGuidedSetup="true">
  <Input>
    <Group name="service" type="group" displayString="Application Configuration">
      <Variable name="name" type="name" displayString="Application Config Name:" perm="ace_vip"/>
      <Variable name="fqdn" type="string" displayString="Exchange FQDN:" perm="ace_vip" default="%N"/>
      <Variable name="vip" type="ipaddresswithprefix" displayString="Exchange VIP Address:" perm="ace_vip"/>
    </Group>
    <Array name="realss" displayString="IP Addresses of Real Servers that are in the Client Access Array (CAS)" perm="ace_vip">
      <Variable name="ipAddr" displayString="" type="ipaddress" perm="ace_vip"/>
    </Array>
    <Variable name="secure" type="boolean" displayString="Secure communication between Load Balancer and Servers:" perm="ace_vip"/>
    <If test="(!$secure) = false">
      <Label name="warning" type="warning" displayString="Be sure to configure your CAS server to enable http/>
    </If>
  </Input>
</template>
```
Microsoft Exchange Template User View

http://developer.cisco.com/web/anm/application-templates
ACE in a Virtualized Environment
Enabling a New Server in a VM Environment

- ANM 5.x VCenter plug-in lets Sysadmins **activate, suspend, configure and monitor rservers**

---

**Diagram:**

- ACE Load Balancer
- ESX Cluster
  - Application servers
  - VM1
  - VM2
  - VM3
- SLB Team
- Sysadmin
ANM 5.2 Plug-in for VMware VCenter

activate, suspend, configure and monitor rservers
Deploying VMware View 4.6 with Cisco ACE
Why Add a Cisco ACE?

- **Scalability**: Larger deployments require multiple Security Servers or multiple Connection Servers
  - Cisco ACE balances client connections across available connection servers
  - VMware rates a single View Connection Server at 1,500 concurrent non-tunneled connections, and 30% less if tunneled

- **Fault Tolerance**
  - Cisco ACE detects the failure of View components, and directs traffic around the failure

- **Performance**
  - Reduce CPU usage on Connection Servers by offloading HTTPS cryptography
VMware View Deployment with Cisco ACE

General Types of View Deployments

- **LAN Direct Deployment**
  - Display protocol does not pass through the View Connection Server

- **LAN Tunneled Deployment**
  - Display protocol Traffic is encapsulated in HTTPS and passes through the View Connection Server

- **Secure (DMZ) Tunneled Deployment**
  - Display protocol Traffic is encapsulated in HTTPS and passes through the View Security Server
  - View Security Server does not participate in Active Directory, and can be safely placed in DMZ
VMware View Deployment with Cisco ACE

LAN Tunneled Deployment w/ACE

- More Secure – All traffic encapsulated in SSL. Virtual Desktop IP Addresses do not need to be reachable by clients
- Offload Benefit – SSL cryptography offloaded by Cisco ACE, reducing CPU utilization on Connection Servers
- Recommended for LAN deployments on secure networks. Connection Servers participate in Active Directory and should not be exposed to the Internet
VMware View Deployment with Cisco ACE
Secure Tunneled Deployment (DMZ)

1. HTTP(S) – Authentication & Desktop Selection
2. AJP/JMS Authentication
3. RDP Over HTTPS
4. RDP Un-Tunneled By Security Server

* Client RDP connection is tunneled over HTTPS to Security Server

Active Directory Server
vCenter
Connection Server
ESX Cluster Containing Virtual Desktops
VMware View Deployment with Cisco ACE

Secure Tunneled Deployment (DMZ) w/ACE

- Most Secure – All traffic encapsulated in SSL. No public exposure of Connection Servers
- Requires careful planning, since Security Servers depend on their paired Connection Server

1a. Authentication
1b. Authentication Decrypted
1c. Authentication Proxied

2a. RDP
2b. RDP Decrypted
2c. RDP Brokered
VMware View Deployment with Cisco ACE

Configuring Secure Tunneled Deployment

Connection Servers
- No specific configuration required

Security Servers
- Create locked.properties file on each security server as shown in earlier slide
- Restart VMware Security Server windows service after placing locked.properties file

Cisco ACE
- Configure VIP listening on TCP/443
  - Configure each security server as an rs nauseum port 80 (and add to serverfarm)
  - Configure an HTTP probe on serverfarm, to check health of connection servers
  - Configure leastconns predictor on VIP, with slowstart
  - Configure SSL proxy on VIP
  - Configure Source IP sticky on VIP (default timeout of 24 hours is ideal)
  - Configure redirect to HTTPS for HTTP requests
VMware View Deployment with Cisco ACE

- Whenever the connection servers are behind a Cisco ACE which is terminating SSL, the “Require SSL” option **MUST** be un-checked

- The probes configured on the Cisco ACE **MUST** match this setting. If the box is checked, use HTTPS probes, if the box is un-checked, use HTTP probes
VMware View Deployment with Cisco ACE

- Connection server settings are not global, rather per-server
- The external URL MUST be set to an FQDN which is resolvable by clients
- When connection servers sit behind a Cisco ACE, the external URL should be set to an FQDN which resolves to the VIP address
- Pay attention to protocol and port! Make sure it matches what is configured on the Cisco ACE VIP
- Direct connection should only be used in LAN environments where the virtual desktops and clients have routes to each other
VMware View Deployment with Cisco ACE

probe http VIEW-ACE-PROBE
  interval 5
  passdetect interval 5
  request method get url /favicon.ico
  expect status 200 200
  open 1
rserv redirect VIEW_REDIRECT
  webhost-redirection https://%h%p 302
  inservice
serverfarm host VIEW-SF
  predictor leastconns slowstart 300
  probe VIEW-ACE-PROBE
  rserver CONNECTION_SERV1 80
    inservice
  rserver CONNECTION_SERV2 80
    inservice
sticky ip-netmask 255.255.255.255 address source VIEW-STICKY
  replicate sticky
serverfarm VIEW-SF
VMware View Deployment with Cisco ACE

class-map match-any VIEW-REDIRECT-CM
  2 match virtual-address 30.30.30.10 tcp eq www

class-map match-any VIEW-HTTPS-CM
  2 match virtual-address 30.30.30.10 tcp eq https

policy-map type loadbalance http first-match VIEW-HTTPS-PM
  class class-default
    sticky-serverfarm VIEW-STICKY

policy-map type loadbalance http first-match VIEW-REDIRECT
  class class-default
    serverfarm VIEW-REDIRECT

policy-map multi-match VIEW-HTTPS
  class VIEW-HTTPS-CM
    loadbalance vip inservice
    loadbalance policy VIEW-HTTPS-PM
    ssl-proxy server VIEW-SSL

class VIEW-REDIRECT-CM
  loadbalance vip inservice
  loadbalance policy VIEW-REDIRECT
Load Balancing Microsoft Exchange
Outlook Web Access 2010 Example
Application Solutions Validated with ACE

Comprehensive set of validated ACE solutions

This design guide presents an end-to-end solution architecture that demonstrates how enterprises can virtualize their Exchange 2010 environment on Cisco Unified Computing System

Exchange 2010
ACE Load Balancing OWA

- Exchange 2010:
  All client access goes through Client Access Servers, likely more than 8 servers needed to support load

- Network Architecture
  Session persistence for user sessions involving multiple flows
  - Source-IP-based stickiness
  - HTTP-based cookie persistence
    (ACE-inserted, server)
Understanding Exchange Architecture

Exchange 2007

- Exchange Components
  - WS
  - OWA
  - UM
  - Transport Agents
  - Mailbox Agents
  - Sync

- Outlook / MAPI clients
- Entourage

- Middle Tier
- Biz Logic

- Mailbox
  - MAPI RPC
  - DAV
  - Store

Exchange 2010

- Exchange Components
  - WS
  - OWA
  - UM
  - Transport Agents
  - Mailbox Agents
  - Sync

- Outlook / MAPI clients
- Entourage

- Middle Tier
- Biz Logic

- Mailbox
  - MAPI RPC
  - DAV
  - Store

- Exchange Core Biz Logic

© 2012 Cisco and/or its affiliates. All rights reserved. Cisco Public
Exchange 2010 Middle Tier

- New services in Exchange Server 2010 that reside on CAS
  
  Restrict all Outlook data access to a single common path by migrating Mailbox and Directory endpoints to CAS

- What it handles:
  
  Outlook data connections go to **RPC Client Access Service** on CAS instead of connecting to Mailbox servers

  **Address Book Service** on CAS replaces DSProxy interface, handles all Outlook Directory connections

  Public folder connections connect directly to the Mailbox server, but through RPC Client Access Service running on backend
Exchange 2010
ACE Load Balancing Outlook Anywhere

ACE can provide the following benefits:

- Additional Data Centre Security using ACL
- Load balancing using the HTTP header-value "MSRPC"
- Session persistence based on SOURCE-IP or http-header Authorization
- SSL termination
- Health monitoring check Client Access Server status
RPC over HTTP

- Access Exchange from an Outlook Client
  - If you use RPC over HTTP, you can use Outlook to access Exchange Server over the Internet
  - The HTTP session terminates at a server running Internet Information Services (IIS) that has the RPC over HTTP Proxy networking component installed
  - RPC over HTTP turns a Web request into an RPC request. Outlook sends the RPC request inside an HTTP tunnel. The actual RPC request does not change between the Outlook client and the Exchange server
Outlook Anywhere Over HTTP

- If ACE can use the User-Agent: MSRPC HTTP header to detect RPC over HTTP
- This enables you to use the same VIP for OWA and Outlook Anywhere, therefore saving address space
- ACE can use the Basic Authorization header for session persistence. This eliminates you having to use SOURCE-IP stickiness

RPC_IN_DATA /rpc/rpcproxy.dll?exch-ace-tme.com:6004 HTTP/1.1
Accept: application/rpc
User-Agent: MSRPC
Host: exch-ace-tme.com
Content-Length: 1073741824
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
Authorization: Basic Q0xJRU5UXG1kaXR0bWVyOmZvbw==

When using NTLM, the default authorization type, hash value will change. Therefore you cannot use the Authorization header for session persistence. You will need to use source-ip stickiness.
Microsoft Exchange Template User View

http://developer.cisco.com/web/anm/application-templates
Microsoft Exchange Template User View

**Base Name in Config**

- VIP: WWW.CISCO.COM or REGEX %H

**VIP**

- 10.1.1.1
- 10.1.1.2
- 10.1.1.3

**Do you need end to end SSL?**

- No

---

© 2012 Cisco and/or its affiliates. All rights reserved.
Microsoft Exchange Template User View cont.

- Secure communication between Load Balancer and Servers:
  - Be sure to configure your CAS server to enable http
    - Key Type: PEM
    - SSL Key: Choose File sample-key.pem
    - SSL Certificate: Choose File sample-cert.pem
  - CertKey
  - Passphrase:
  - Use IP Sticky for MSRPC Connections to Servers:
    - Check box
  - Do not use IP Sticky if a large percentage of the clients access via a superproxy.

- SSL Certs
- Which ACE
- Outlook Anywhere
- More info to follow
Microsoft Exchange Template User View cont.

Network Configuration

- Load Balancer (Device:Virtual/Context): 660-195.3.Admin

Client VLANs:
- All VLANs
- 511
- 650
- 110
- 510

Enable Source NAT:

Deploy or Stage

Deploy Template

Deployed and Named

© 2012 Cisco and/or its affiliates. All rights reserved.
GUI Versus CLI Comparison

dc1-ace1/Admin# show run filter vips
Generating configuration....

probe https OWA-probe-1
  interval 60
  passtime 2
  passdetect count 2
  ssl version all
  request method get url /exchweb/bin/auth/owalogon.asp
  expect status 400 404
  open 10

rserver host CAS1
  ip address 192.168.200.15
  inservice

rserver host CAS2
  ip address 192.168.200.16
  inservice

rserver redirect OWA http
  webhost-redirection https://%H/owa 302
  inservice

serverfarm host OWA
  failaction purge
  predictor leastconns
  probe OWA-probe-1
  rserver CAS1 80
  inservice
  rserver CAS2 80
  inservice

serverfarm host OWA-others
  failaction purge
  predictor leastconns
  rserver CAS1
  inservice
  rserver CAS2
  inservice

serverfarm redirect OWA_redir
  failaction purge
  rserver OWA_http
  inservice
  sticky http-cookie sessionid OWA-OutlookSession
  replicate sticky
  serverfarm OWA
  sticky http-header Authorization OWA-OutlookRPC
  replicate sticky

serverfarm OWA

ssl-proxy service OWA-termination
  key OWA-sample-key.pem
  cert OWA-sample-cert.pem

class-map type http loadbalance match-any OWA-cond
  description RPC
  2 match http header User-Agent header-value "MSRPC"
  class-map match-all OWA_http
  2 match virtual-address 10.87.121.119 tcp eq www
  class-map match-all OWA_https
  2 match virtual-address 10.87.121.119 tcp eq https
  class-map match-all OWA_other
  2 match virtual-address 10.87.121.119 any

policy-map type loadbalance first-match OWA_http-17slb
  class class-default

serverfarm OWA_redir

policy-map type loadbalance first-match OWA_https-17slb
  class OWA-cond
  sticky-serverfarm OWA-OutlookRPC
  class class-default
  sticky-serverfarm OWA-OutlookSession

policy-map type loadbalance first-match OWA_other-17slb
  class class-default

serverfarm OWA-others

policy-map multi-match vips
  class OWA_http
    loadbalance vip inservice
    loadbalance policy OWA_http-17slb
  class OWA_https
    loadbalance vip inservice
    loadbalance policy OWA_https-17slb
  class OWA_ssl
    loadbalance vip inservice
    loadbalance policy OWA_other-17slb
  class OWA_vips
    loadbalance vip inservice
    loadbalance policy OWA_vips-17slb

serverfarm OWA

OWA ACE Base Configuration

rserver host CAS1
  ip address 192.168.1.11
  inservice
rserver host CAS2
  ip address 192.168.1.12
  inservice

access-list everyone line 10 extended permit ip any any

! class-map type management match-any REMOTE-ACCESS
  description REMOTE-ACCESS-traffic-match
  2 match protocol ssh any
  3 match protocol icmp any
  4 match protocol https any

! policy-map type management first-match REMOTE-MGN
  class REMOTE-ACCESS
    permit

! interface vlan 2
  description CLIENT_VLAN
  ip address 172.16.20.254 255.255.255.0
  access-group input everyone
  service-policy input REMOTE-MGN
interface vlan 3
  description SERVER_VLAN
  ip address 10.1.1.254 255.255.255.0
  access-group input everyone
  service-policy input REMOTE-MGN
crypto csr-params SSL_PARAMS
  country US
  state CA
  organization-name SJC
  organization-unit DC
  common-name owa.sjc.com
  serial-number 1
  email administrator@sjc.com

ssl-proxy service OWA-SSL
  key owa.pem
  cert owa.pem

probe http HTTP-GET
  interval 10
  passdetect interval 10
  request meth get url /iisstart.htm
  expect status 200 202
!
probe icmp PING
  interval 3
!
serverfarm CAS
  probe HTTP-GET
  probe PING
  rserver CAS1 80
    inservice
  rserver CAS2 80
    inservice

class-map match-all OWA-SSL-CM
  2 match virtual-addr 172.16.11.190 tcp eq 443
!
sticky http-cookie Cookie OWA-STICKY
  cookie insert browser-expire
  replicate sticky
  serverfarm CAS
!
policy-map type loadbalan first-ma OWA-SSL-PM
  class class-default
  sticky-serverfarm OWA-STICKY
!
policy-map multi-match LOADBALANCE
  class OWA-SSL-CM
    loadbalance vip inservice
    loadbalance policy OWA-SSL-PM
    loadbalance vip icmp-reply active
    ssl-proxy server OWA-SSL
!
interface vlan 2
  description CLIENT_VLAN
  ip address 172.16.20.254 255.255.255.0
  access-group input everyone
  service-policy input REMOTE-MGN
  service-policy input LOADBALANCE
Initial HTTP to HTTPS Redirect

ACE redirects clients initial request from http-to-https
Combined Outlook Anywhere and OWA ACE Configuration

class-map match-all OWA-OUTLOOKANYWHERE-SSL
  2 match virtual-addr 172.16.11.190 tcp eq 443
!
sticky http-cookie Cookie OWA-STICKY
  cookie insert browser-expire
  replicate sticky
  serverfarm CAS-80
sticky http-header Authorization CAS-RPC-HTTP
  serverfarm CAS-80
!
policy-map type loadbalan first-ma OWA-OUTLOOKANYWHERE
match OUTLOOK_ANYWHERE http header User-Agent header-value "MSRPC"
  sticky-serverfarm CAS-RPC-HTTP
  class class-default
  sticky-serverfarm OWA-STICKY
Optional Information for OWA

- Use Microsoft Cookie instead of ACE cookie for HTTP session persistence across the CAS servers

  ```
  sticky http-cookie sessionid exchange-sticky-sessionid-grp
  timeout 20
  serverfarm CAS
  ```

- Additional health monitoring probe that you could add to check the availability of Exchange

  ```
  probe http http-probe
  interval 60
  passdetect interval 60
  passdetect count 2
  request method get url /exchweb/bin/auth/owalogon.asp
  expect status 401 401

  probe https https-probe
  interval 60
  passdetect interval 60
  passdetect count 2
  request method get url /owa/auth/login.aspx
  expect status 401 401
  ```
Optional Information for OWA

- Using HTTP Compression for OWA to compress the following objects:
  - JavaScript
  - GIF files
  - CSS

  ```
  parameter-map type http CompressObjects
  persistence-rebalance
  compress mimetype "text/css"
  compress mimetype "images/gif"
  compress mimetype "application/x-javascript"
  ```

  ```
  policy-map type loadbalance first-match OWA-OutlookAnywhere
  match OUTLOOK_ANYWHERE http header User-Agent header-value "MSRPC"
  sticky-serverfarm CAS-RPC-HTTP
  class class-default
  compress default-method gzip
  sticky-serverfarm OWA-STICKY
  ```

  ```
  policy-map multi-match Exchange2007
  class VIP-HTTPS-OWA-OutlookAnywhere
  loadbalance vip inservice
  loadbalance policy OWA-OutlookAnywhere
  appl-parameter http advanced-options CompressObjects
  ssl-proxy server exch-ace-tme.com
  ```
Optional Information for OWA

- Use the show service-policy detail to view compression ratio

ACE# show service-policy Exchange2007 detail

class: VIP-HTTPS-OWA-OutlookAnywhere
ssl-proxy server: exch-ace-tme.com
VIP Address: Protocol: Port:
10.10.10.100 tcp eq 443
loadbalance:
  L7 loadbalance policy: OWA-OutlookAnywhere
  Persistence Rebalance: ENABLED
  curr conns : 0 , hit count : 26
  dropped conns : 0
  L7 loadbalance policy : OWA-OutlookAnywhere
  class/match : OUTLOOK_ANYWHERE
  LB action :
    sticky group: CAS-RPC-HTTP
    primary serverfarm: CAS-80
    state:UP
  compression : off
  class/match : class-default
  LB action :
    sticky group: OWA-STICKY
    primary serverfarm: CAS-80
    state:UP
    backup serverfarm : -
    hit count : 397
    dropped conns : 0
  compression : on
  compression:
    bytes_in : 1600177
    bytes_out : 576628
Compression ratio : 63.96%  
Shows compression ratio
Microsoft SharePoint 2010 with ACE
What is Microsoft SharePoint Server 2010?

- Microsoft SharePoint Server 2010 is a portal-based collaboration platform for creating, managing and sharing documents and Web services.

- SharePoint 2010 enables users to create "SharePoint Portals" that include shared workspaces, applications, blogs, wikis and other documents accessible through a Web browser.
Logical Architecture

- A SharePoint 2010 Serverfarm is a 3 Tier Architecture, which consists of:
  - Web Front End Server(s)
  - Application Server(s)
  - Database Server(s)
- The Web Server role provides Web content to clients.
- The Application Server role provides SharePoint 2010 services such as search queries, Office Web Applications and crawling and indexing content.
- The Database Server stores Content and Configuration information.
ACE Load Balancing SharePoint 2010
Web Front End Servers

ACE can provide the following benefits:

- Additional Data Centre Security using ACL
- Layer 4/7 load balancing between Clients and SharePoint WFE servers with session persistence based upon HTTP Cookie insertion
- SSL termination
- Health monitoring (Including In-Band) for guaranteed service availability
ACE Load Balancing Services

- SSL Termination for Portal Traffic
- L4 Load Balancing for Application Traffic
- In-Band & OOB WFE Server Health Checking
- Session Persistence maintained with HTTP Cookie Insertion
SharePoint 2010 Portal ACE Configuration

probe http msSharePoint01-probe-1
  interval 5
  passdetect interval 30
  expect status 401 401
  open 15

rserver host WFE01
  ip address 192.168.11.1
  inservice
rserver host WFE02
  ip address 192.168.11.2
  inservice

serverfarm host msSharePoint01-80
  failaction purge
  predictor leastconns
  probe msSharePoint01-probe-1
  inband-health check remove 100 reset 500 resume-service 300
  rserver WFE01 80
    inservice
  rserver WFE02 80
    inservice

parameter-map type http msSharePoint01-http
  persistence-rebalance
  set content-maxparse-length 8192

OOB Health Checking for Failed WFE Servers

In-Band Health Checking for Failed HTTP Connections

Required for Cookie Insertion on HTTP 1.1 Persistent Connections
SharePoint 2010 Portal ACE Configuration

sticky http-cookie SPLB-Port msSharePoint01-WFE-Portal
  cookie insert browser-expire
  replicate sticky
  serverfarm msSharePoint01-80
sticky http-cookie SPLB-WFE msSharePoint01-WFE-Apps
  cookie insert browser-expire
  replicate sticky
  serverfarm msSharePoint01

policy-map type loadbalance first-match msSharePoint01_https-17slb
  class class-default
    compress default-method deflate
    sticky-serverfarm msSharePoint01-WFE-Portal
policy-map type loadbalance first-match msSharePoint01_other-17slb
  class class-default
    compress default-method deflate
    sticky-serverfarm msSharePoint01-WFE-Apps
Simplifying All of the Above with ANM Application Templates

Only Required to Provide:

- VIP IP
- WFE Server IP Addresses
- SSL Cert/Key Location
- NAT Required?

ANM Does the rest!
Simplifying All of the Above with ANM Templates

Application Type: Microsoft SharePoint 2010

Application Configuration

- **Application Config Name:** msSharePoint01
- **VIP Address:** 192.168.10.101
- **SharePoint Application Servers:**
  - 192.168.11.1
  - 192.168.11.2
  - 192.168.11.3
- **SSL Offload Port:** 80
- **Key Type:** PEM
- **SSL Key:** /Users/whitear/Desktop/m
- **SSL Certificate:** /Users/whitear/Desktop/m
- **Cert/Key Password:**
- **Enable Compression:**

MS Sharepoint

Client
SSL Termination
Server
ACE Configuration Created by ANM Template

access-list vip-acl-1 remark Created to permit IP traffic to VIP.
access-list vip-acl-1 line 10 extended permit ip any host 192.168.10.100

probe http msSharePoint01-probe-1
  interval 5
  passdetect interval 30
  expect status 401 401
  open 15

probe icmp msSharePoint01-probe-2
  interval 2
  passdetect interval 60

rserver host 192.168.11.1
  ip address 192.168.11.1
  inservice

rserver host 192.168.11.2
  ip address 192.168.11.2
  inservice

rserver host 192.168.11.3
  ip address 192.168.11.3
  inservice
ACE Configuration Created by ANM Template

serverfarm host msSharePoint01
  failaction purge
  predictor leastconns
  probe msSharePoint01-probe-2
  inband-health check remove 100 reset 500 resume-service 300
  rserver 192.168.11.1
    inservice
  rserver 192.168.11.2
    inservice
  rserver 192.168.11.3
    inservice
serverfarm host msSharePoint01-80
  failaction purge
  predictor leastconns
  probe msSharePoint01-probe-1
  inband-health check remove 100 reset 500 resume-service 300
  rserver 192.168.11.1 80
    inservice
  rserver 192.168.11.2 80
    inservice
  rserver 192.168.11.3 80
    inservice

  parameter-map type http msSharePoint01-http_params
  persistence-rebalance
  set content-maxparse-length 8192
ACE Configuration Created by ANM Template

sticky http-cookie SPLB-Port msSharePoint01-WFE-Portal
  cookie insert browser-expire
  replicate sticky
  serverfarm msSharePoint01-80
sticky http-cookie SPLB-WFE msSharePoint01-WFE-Apps
  cookie insert browser-expire
  replicate sticky
  serverfarm msSharePoint01

ssl-proxy service msSharePoint01-termination
  key msSharePoint01-msExch02key.pem
cert msSharePoint01-msExch02cert.pem

class-map match-all msSharePoint01_https
  2 match virtual-address 192.168.10.100 tcp eq https
class-map match-all msSharePoint01_other
  2 match virtual-address 192.168.10.100 any

policy-map type loadbalance first-match msSharePoint01_https-17slb
  class class-default
    compress default-method deflate
    sticky-serverfarm msSharePoint01-WFE-Portal

policy-map type loadbalance first-match msSharePoint01_other-17slb
  class class-default
    compress default-method deflate
    sticky-serverfarm msSharePoint01-WFE-Apps
ACE Configuration Created by ANM Template

```plaintext
policy-map multi-match int10
  class msSharePoint01_https
    loadbalance vip inservice
    loadbalance policy msSharePoint01_https-l7slb
    appl-parameter http advanced-options msSharePoint01-http_params
    ssl-proxy server msSharePoint01-termination
  class msSharePoint01_other
    loadbalance vip inservice
    loadbalance policy msSharePoint01_other-l7slb
    loadbalance vip icmp-reply active

interface vlan 10
  access-group input vip-acl-1
  service-policy input int10
```
IPv6 Options
IPv6 Load Balancing Deployment Modes

**True Dual Stack Support**
- IPv6 Client Network
- IPv6 Virtual Servers
- IPv6 Real Servers

**Dual Stack**
Supports End-to-End IPv4 and IPv6 Virtual servers and Real servers

**IPv6-to-IPv4 Translation**
Supports Translation from IPv6 Virtual Server to IPv4 Real servers and vice versa

**SLB64 and SLB46 Support**
- IPv6 Client Network
- IPv6 Virtual Servers
- IPv4 Real Servers

For IPv6 to IPv4 translation or IPv4 to IPv6, Source NAT is required
ACE Release A5(1.0) Provides IPv6 Support

- **Dual Stack**
  - IPv4-to-IPv4 and IPv6-to-IPv6
  - HTTP and DNS inspection for native IPv6-IPv6 traffic

- **Translation**
  - SLB64, SLB46 for all the Layer4 load balancing, which do not need payload modifications or pinholing
  - NAT64, NAT46 for all TCP, UDP protocols, which do not need payload modifications or pinholing
  - SLB64 and SLB46 support L7 loadbalancing for HTTP and SSL protocols.
  - No DNS64 or DNS46 support on ACE

- **Mixed v4 & v6 rservr support**
- **Duplicate Address Discovery**
- **Neighbor Discovery**
- **ICMPv6**
- **Application Awareness**
  - HTTP, HTTPS and DNS
- **OCSP Support for Authenticating SSL Offloaded Sessions**
  - IPv6 and IPv4 support
Recommended Reading
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com
Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: https://www.facebook.com/ciscoliveus
  - Twitter: https://twitter.com/#!/CiscoLive
  - LinkedIn Group: http://linkd.in/CiscoLI