

TESTING & INTEGRATION GROUP

SOLUTION GUIDE

AppDirector Load balancing IBM Websphere SIP Servers

INTRODUCTION	2
RADWARE'S APPDIRECTOR	2
IBM'S WEBSHERE SIP SERVER	3
SOLUTION DETAILS	5
SOFTWARE AND HARDWARE	5
TESTED NETWORK OVERVIEW	6
CONFIGURATION	7
RADWARE DEVICES	7
<i>APPDIRECTOR ACTIVE CONFIGURATION</i>	7
<i>APPDIRECTOR BACKUP CONFIGURATION</i>	9
<i>IBM WEBSHERE SERVER-1</i>	10
<i>IBM WEBSHERE SERVER-2</i>	10
APPENDIX	11
<i>HEALTH MONITORING WITH SIP OPTIONS</i>	11
TECHNICAL SUPPORT	12

TECHNICAL SOLUTION GUIDE

AUTHOR: Elad Kurzweil

DATE: Wednesday, January 17, 2007

Version: 1.0

Introduction

The success of large scale service oriented organizations (such as, finance and banking, Insurance, E-com and Service Portals) is measured by their ability to provide a wide variety of services and online applications and introduce a large number of new services which will increase their revenue stream, while still maintaining a friendly user experience and lowering expenses. Therefore, optimizing IT infrastructure and application servers are a major priority for such organizations.

IBM's Websphere SIP servers allow organization to achieve such goal by effectively operating multiple applications. WebSphere Application Servers provide an extremely efficient infrastructure allowing for a capable e-business application deployment environment and providing additional valuable application services and capabilities such as transaction management, security, clustering, performance, availability, connectivity and scalability. The SIP (Session Initiation Protocol) components in WebSphere Application Server is an additional added value to productivity as it allows organizations to run a highly converged HTTP and SIP applications with seamless failover provided by the Proxy Server.

However, the advantages provided by IBM's Websphere SIP servers may also be a disadvantage to the network if the traffic is not controlled correctly. Utilizing Radware's AppDirector ensures that the traffic is managed correctly and all servers are utilized efficiently therefore handling Load balancing, reducing failures at any end point and allowing for greater scalability. AppDirector eliminates bottlenecks, failures and downtime from servers while constantly protecting data traffic from security violations as well. Therefore, when utilizing Radware's AppDirector, organizations promise to deliver not only an optimized solution but also a reliable and a secured one as well. In summary, the combined solution of IBM's Websphere SIP servers along with Radware's AppDirector results in a smart and reliable network application infrastructure. This allows organizations to provide efficient, reliable and secured services to their customers and employees.

Radware's AppDirector

Radware AppDirector is an intelligent application delivery controller for the data center that provides scalability and application-level security for IT infrastructure optimization, fault tolerance and redundancy.

AppDirector combines the power of Radware's Multi-Gigabit Application Switching hardware with APSolute OS Application-Smart Networking to ensure local and global server availability, accelerated application performance and safeguard applications with integrated intrusion prevention and denial of service protection for fast, reliable, secure application delivery.

AppDirector uses advanced Layer 4-7 policies and granular application intelligence for end-to-end application-smart networking, aligning server infrastructure operations with application front end requirements to eliminate traffic surges, server bottlenecks, connectivity disconnects and downtime for assured application access, full application continuity and redundancy. AppDirector enables fine tuning of network behavior at all critical points, end-to-end, based on granular application-specific classification of packets to optimize traffic flows for a wide range of enterprise web applications such as CRM, ERP, and other IP-based applications including support for VoIP, streaming media, and secure LDAP applications.

With AppDirector's fully integrated intrusion prevention and Denial of Service protection data center applications and server resources are insulated against application level attacks. The ability to control multi-step SSL processing provides enhanced security of HTTP, FTP, SMTP and SIP over SSL.

AppDirector lets you get the most out of your IT investments by maximizing the utilization of server infrastructure resources and enabling seamless consolidation and high scalability. Make your network adaptive and more responsive to your dynamic application and business needs with AppDirector's fully integrated traffic classification and flow management, health monitoring and failure bypassing, traffic redirection, bandwidth management, intrusion prevention and DoS protection.

For more information, please visit: <http://www.radware.com>

IBM's WebSphere SIP Server

WebSphere Application Server Version 6.1 delivers rich SIP functionality throughout its infrastructure.

Session Initiation Protocol (SIP) has grown considerably since it first became an IETF standard in 1999. SIP was originally intended purely for video and audio but has now grown to become the control protocol for many interactive services, particularly in the peer-to-peer realm. SIP, and the standards surrounding SIP, provide the mechanisms to look up, negotiate, and manage connections to peers on any network over any other protocol.

Using version 6.1, you can write applications using the SIP Servlet 1.0 specification, which was introduced to allow enterprise applications to use SIP and to support SIP-predominant applications in the Java EE environment.

WebSphere Application Server also provides tooling for the development environment and high performing Edge Components to handle distributed application environments. The SIP components in WebSphere Application Server have a tight integration with the existing HTTP servlet and portlet work, with which you can write a highly converged HTTP and SIP application with seamless failover provided by the Proxy Server.

In WebSphere Application Server, the Web container and SIP container are converged and are able to share session management, security and other attributes. In this model, an application that includes SIP servlets, HTTP servlets, and portlets can seamlessly interact, regardless of the protocol.

High availability, offered by the Network Deployment version of WebSphere Application Server, of the converged applications is made possible because of the tight integration of HTTP and SIP in the base application server.

In front of a clustered application sits the Proxy server, managing the traffic and workload of the SIP and HTTP traffic to the Container. This Proxy Server is a stateless SIP proxy and a HTTP reverse proxy together, which uses the unified clustering framework and high availability manager services of the ND package to seamlessly monitor the health of the servers and failover work, when necessary. The Proxy server also can act as a stand alone Stateless SIP proxy in front of the SIP Container in the application server when no HTTP traffic is present.

With the converged proxy and converged container, session failover is done with affinity to the application, allowing the HTTP and SIP sessions to be tied together automatically. Having the SIP and HTTP Sessions automatically tied together from the container to the Proxy is another way the WebSphere Application Server 6.1 solution excels in converged environments.

For the SIP function in the Proxy server, it is important to understand that it is stateless. The SIP RFC defines two types of Proxy Servers, one stateful and one stateless. Normally, a SIP Proxy is a stateful instance and stateless proxies are specified as such. A stateful proxy participates in the call flows as we had seen in example from the SIP Overview. A stateful proxy can be implemented using SIP Servlets as a basic example was shown in the SIP Servlet section.

The stateless SIP proxy functionality in the Proxy server allows the Proxy to handle the workload, routing, and session affinity needs of the SIP container with less complexity. Being stateless, the Proxy server can be fronted by a Load. If a Proxy Server fails, the affinity is to the container and not to the proxy itself so there is one less potential failure along the message flow.

For more information, please visit: <http://www-306.ibm.com/software/websphere/>

Solution Details

The solution documented below allows for building a scalable highly-available cluster of SIP servers. IBM Websphere SIP servers are serving the SIP calls and registration with user database synchronization between the servers.

AppDirector Layer 7 persistency is implemented to guarantee the client persistent redirection to the same WebSphere server.

Radware's AppDirector further offers HA and scalability of the solution through the distribution of user requests between the IBM SIP servers. Health monitoring is done via SIP UDP port 5060 and can be done with advanced proprietary Radware SIP UDP/TCP OPTIONS mechanism.

Important Notes:

- **Activating CallID persistency saves resources and optimizes system behavior. However, CallID Persistency is not mandatory because the IBM WebSphere SIP servers are synchronizing through the backend user database**
- **A Loopback address should be added to IBM Websphere SIP Servers holding the AppDirector Farm 1.1.1.200 IP.**
- **Health Monitoring is provided using SIP protocol checks.**
- **With further configuration, the AppDirector may provide a global solution with many WebSphere server locations.**

Software and Hardware

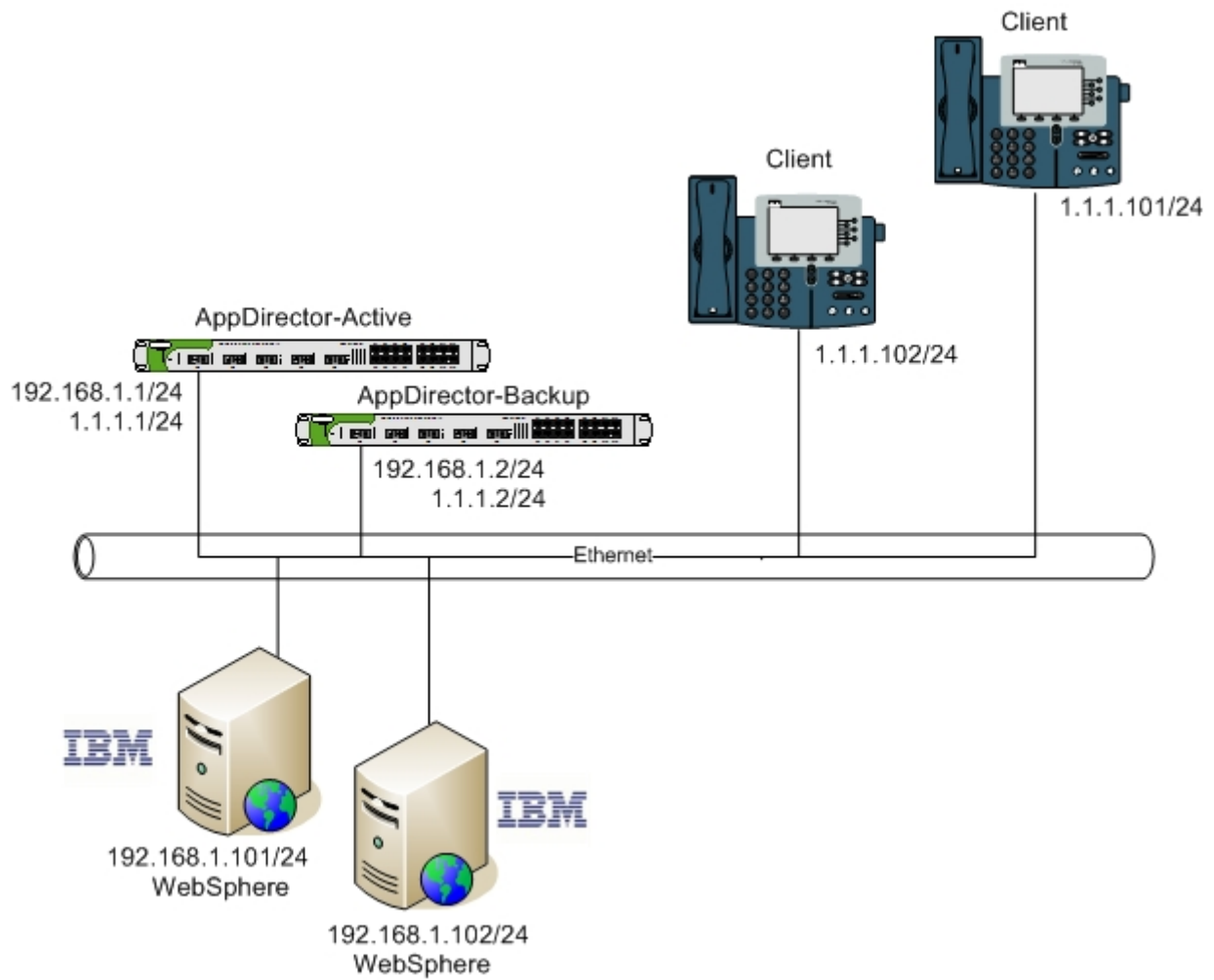
The following is a list of hardware and Multimedia software tested to verify the interoperability of the presented solution:

Radware's Appdirector v.1.00.2

SIP Clients: Linksys PAP2, Cisco 7960G, Polycom IP500

Application Server : IBM WebSphere 6.1 with SIP Envelope

Tested network overview



Network Diagram

Configuration

Radware Devices

APPDIRECTOR ACTIVE CONFIGURATION

Network Configuration

- Create IP 1.1.1.1 on port 17
- Create IP 192.168.1.1 on port 17

Farm Configuration

- Create Farm named "IBM.SIP" in **AppDirector -> Farms -> Farm Table** with these parameters (for the AppXcel appliances using HTTPS mode)
 - o Farm Name – IBM.SIP
 - o Session mode – Server per session
 - o Connectivity checks – No Checks
 - o Leave all other fields as default

Servers Configuration

- Create Server named "IBM.SIP.Server.1" and attach it to Farm "IBM.SIP" in **AppDirector -> Servers -> Server Table** with these parameters
 - o Farm Name – IBM.SIP
 - o Server Address – 192.168.1.101
 - o Type – Local Triangulation
 - o Leave all other fields as default
- Create Server named "IBM.SIP.Server.2" and attach it to Farm "IBM.SIP" in **AppDirector -> Servers -> Server Table** with these parameters
 - o Farm Name – IBM.SIP
 - o Server Address – 192.168.1.102
 - o Type – Local Triangulation
 - o Leave all other fields as default

Layer 4 Policy Configuration

- Create L4 Policy for SIP Traffic named "SIP.Traffic" in **AppDirector -> Servers -> Server Table** with these parameters
 - o Virtual IP – 1.1.1.200
 - o L4 Protocol – UDP
 - o L4 Port – 5060
 - o Application - SIP
 - o L4 Policy Name – SIP.Traffic
 - o Farm Name – IBM.SIP
 - o Leave all other fields as default

Layer 7 Configuration

- Create L7 Text match session ID persistency (Header mode) in **AppDirector -> L7 Server Persistency -> Text Match** with these parameters
 - o Farm Name – IBM.SIP
 - o L4 Protocol - UDP
 - o Persistency Identifier – Call-ID
 - o Lookup mode – Header
 - o Learning Direction – Both Directions
 - o Identifier Match - Exact
 - o Persistent L7 Switching mode – First Request
 - o Leave all other fields as default

AppDirector Health Monitoring

NOTE: In this paper the SIP UDP port 5060 has been verified, the customer can use Radware SIP UDP/TCP OPTIONS module for deeper SIP checks. Please refer to the [Appendix](#) in this paper for instructions how to configure the SIP UDP/TCP OPTIONS module.

- Enable Health Monitoring in **Health Monitoring -> Global Parameters**

- Create a Check for SIP UDP on server 192.168.1.101 in **Health Monitoring -> Check Table**
 - o Check name – IBM.Server.1.SIP.UDP.Check
 - o Method – UDP
 - o Dest IP – 192.168.1.101
 - o Dest Port – 5060

- Create a Check for SIP UDP on server 192.168.1.102 in **Health Monitoring -> Check Table**
 - o Check name – IBM.Server.2.SIP.UDP.Check
 - o Method – UDP
 - o Dest IP – 192.168.1.102
 - o Dest Port – 5060

- Bind the SIP check IBM.Server.1.SIP.UDP.Check to Server IBM.SIP – 192.168.1.101 in **Health Monitoring -> Binding Table**
- Bind the SIP check IBM.Server.2.SIP.UDP.Check to Server IBM.SIP – 192.168.1.102 in **Health Monitoring -> Binding Table**

VRRP Configuration

- Enable VRRP in **AppDirector -> Redundancy -> Global Configuration**
 - o IP Redundancy Admin Status – VRRP
 - o Interface Grouping – Enable
 - o ARP with interface grouping – Send
 - o VLAN Redundancy – Active
 - o Backup Fake ARP – Enable
 - o Backup Interface Grouping – Enable

- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - o IF Index – 17
 - o VR ID – 1
 - o Priority – 255 (Highest number is Active device)
 - o Primary IP – 192.168.1.1
 - o Leave all other options as default

- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - o IF Index – 17
 - o VR ID – 2
 - o Priority – 255 (Highest number is Active device)
 - o Primary IP – 1.1.1.1
 - o Leave all other options as default

Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP -> Associated IP Addresses**

- o IF Index – 17, VR ID – 1, Associated IP 192.168.1.1
- o IF Index – 17, VR ID – 2, Associated IP 1.1.1.1
- o IF Index – 17, VR ID – 2, Associated IP 1.1.1.200

APPDIRECTOR BACKUP CONFIGURATION

Network Configuration

- Create IP 1.1.1.2 on port 17
- Create IP 192.168.1.2 on port 17

- Copy all configuration from the Active AppDirector device

Redundancy

- Work with the APSolute Insite wizard to copy and convert the Active AppDirector configuration choosing the redundancy mode VRRP or Proprietary.

VRRP Configuration

- Enable VRRP in **AppDirector -> Redundancy -> Global Configuration**
 - o IP Redundancy Admin Status – VRRP
 - o Interface Grouping – Enable
 - o ARP with interface grouping – Send
 - o VLAN Redundancy – Active
 - o Backup Fake ARP – Enable
 - o Backup Interface Grouping – Enable

- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - o IF Index – 17
 - o VR ID – 1
 - o Priority – 100 (Low number is Backup device)
 - o Primary IP – 192.168.1.1
 - o Leave all other options as default

- Create Virtual Router interfaces in **AppDirector -> Redundancy -> VRRP -> VR Table**
 - o IF Index – 17
 - o VR ID – 2
 - o Priority – 100 (Low number is Backup device)
 - o Primary IP – 1.1.1.1
 - o Leave all other options as default

- Create Associated IP Addresses in **AppDirector -> Redundancy -> VRRP -> IP Addresses**
 - o IF Index – 17, VR ID – 1, Associated IP 192.168.1.1
 - o IF Index – 17, VR ID – 2, Associated IP 1.1.1.1
 - o IF Index – 17, VR ID – 2, Associated IP 1.1.1.200

IBM WEBSHERE SERVER-1

- Create IP 192.168.1.101 on network interface
- Add loopback interface with IP 1.1.1.200 (AppDirector VIP)
- Create Default GW to 192.168.1.1
- If using Radware proprietary SIP Health monitoring engine there is a need to add registered user to the IBM SIP Server. By adding the user, Radware SIP Health Monitoring can use the OPTIONS command to verify that the user Exist.

IBM WEBSHERE SERVER-2

- Create IP 192.168.1.102 on network interface
- Add loopback interface with IP 1.1.1.200 (AppDirector VIP)
- Create Default GW to 192.168.1.1
- If using Radware proprietary SIP Health monitoring engine there is a need to add registered user to the IBM SIP Server. By adding the user, Radware SIP Health Monitoring can use the OPTIONS command to verify that the user Exist.

Appendix

HEALTH MONITORING WITH SIP OPTIONS

- Create a Check for SIP on server 192.168.1.101 in **Health Monitoring** -> **Check Table**
 - Check name – IBM.Server.1.SIP.UDP.Check
 - Method – SIP UDP
 - Dest IP – 192.168.1.101
 - Dest Port – 5060
 - Arguments –
 - Request URI – aa@radware.com
 - From – bb@radware.com
 - Max Forward – 0
 - Leave all other fields as default

- Create a Check for SIP on server 192.168.1.102 in **Health Monitoring** -> **Check Table**
 - Check name – IBM.Server.2.SIP.UDP.Check
 - Method – SIP UDP
 - Dest IP – 192.168.1.102
 - Dest Port – 5060
 - Arguments –
 - Request URI – aa@radware.com
 - From – bb@radware.com
 - Max Forward – 0
 - Leave all other fields as default

Technical Support

Radware offers technical support for all of its products through the Radware Certainty Support Program. Please refer to your Certainty Support contract, or the Radware Certainty Support Guide available at:

<http://www.radware.com/content/support/supportprogram/default.asp>.

For more information, please contact your Radware Sales representative or:

U.S. and Americas: (866) 234-5763

International: +972(3) 766-8666