**Introduction:**

AVA Consulting is a Premier Consulting providing Enterprise solutions on designing Microsoft Technologies. AVA follows Microsoft standard frameworks and proven methodologies in designing and implementing the Infrastructure solutions.

AVA has successfully performed Enterprise Infrastructure transformations including both Desktop transformations and Server transformations. AVA has proven track record of quality and delivery methodologies and provide value to its customers by reducing the Operations costs and increase the revenue.

## 1 AVA Solution for HYDRA

**Solution Description:**

HYDRA DNS infrastructure has potential security issues which provide external entities to gain control over the infrastructure and access the application data or the servers. AVA performed critical analysis of HYDRA infrastructure and produced the report which requires infrastructure should be redesigned.

HYDRA organization hosts their infrastructure in New South Wales. There are 2 major sites connected with high speed networks, the infrastructure is hosted on Microsoft infrastructure servers. The Headquarters is in Sydney followed by Secondary site in Melbourne.

HYDRA existing Microsoft infrastructure is operational on Windows Server 2008 R2 with single Active Directory Forest and having multiple domain controllers configured across the physical sites. HYDRA existing environment has critical Security issues with respect to their Domain Naming System and require redesigning their Domain Naming System and ensure HYDRA security policies are met.

HYDRA is engaging AVA, a Microsoft Premier Consulting firm to perform the DNS restructuring which involves placing the DNS servers in DMZ zone and route the internal DNS server requests to DMZ DNS server instead of public ISP servers.

### Hybrid Cloud:

AVA will perform DNS infrastructure on HYDRA’s existing virtual environment and ensure the following

- Virtualization reduces the physical server foot print
• Faster restoration of Server and reduced downtime
• Reducing Operation and Management cost.
• Centralized administration ability for managing server resources and Auditing

HYDRA Existing Data Center:

Existing HYDRA Data Center is hosted in Sydney and managed by 3rd party vendor. HYDRA has 2 offices (Sydney and Melbourne) each of the sites are hosted on specific datacenters and connected with high speed networks.

HYDRA DNS infrastructure is designed to have local Namespace and the public name space is managed by ISP. Both branches are connected with IP VPN to Sydney datacenter. Below table shows the existing servers and Network infrastructure for both Datacenters.

<table>
<thead>
<tr>
<th>Server Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerConnect 8024F x 2</td>
<td></td>
</tr>
<tr>
<td>PowerConnect 5548 x 2</td>
<td></td>
</tr>
<tr>
<td>PowerConnect M1000e x 2</td>
<td></td>
</tr>
<tr>
<td>Microsoft Hyper-V x 4</td>
<td></td>
</tr>
<tr>
<td>Application Servers x 4</td>
<td></td>
</tr>
<tr>
<td>SAN x 4</td>
<td></td>
</tr>
<tr>
<td>HP OpenView Server x 1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Microsoft Infrastructure Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Domain Controller</td>
<td>Virtual</td>
</tr>
<tr>
<td>Additional Domain Controller</td>
<td>Virtual</td>
</tr>
<tr>
<td>Microsoft Exchange Server</td>
<td>Virtual</td>
</tr>
<tr>
<td>Microsoft System Center Virtual Machine Manager</td>
<td>virtual</td>
</tr>
<tr>
<td>Microsoft System Center Operations Manager</td>
<td>Virtual</td>
</tr>
<tr>
<td>Microsoft System Center Configuration Manager</td>
<td>virtual</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>Virtual</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Virtual</td>
</tr>
<tr>
<td>Certificate Server</td>
<td>Virtual</td>
</tr>
<tr>
<td>File Server</td>
<td>Physical</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS Namespace</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Hydra.local</td>
</tr>
<tr>
<td>Global</td>
<td>Hydra.com</td>
</tr>
</tbody>
</table>
Solution Diagram:

Sydney DataCenter

ISP

Network Backbone

Site Connectivity to Melbourne DC

PowerConnect 8024F

PowerConnect 5548

PowerEdge M1000e

1x10GbE

4x 10GbE TwinAx

4x 10GbE TwinAx

1x10GbE

1x10GbE

PowerConnect 8024F

PowerConnect 5548

PowerEdge M1000e

SAN Storage replication

Hybrid Cloud

Application Server

DC, AIO, Exchange, SCVMM

HP Open View Monitoring

SCCM, SCOM

DataBases
Requirement Understanding:

Following are the requirement gathering performed after performing infrastructure analysis and discussing with Architectural group.
1. Data center hosting are performed by 3rd party vendors
2. Server Maintenance are performed by 3rd party vendors including Server Patch Management
3. Networking operations including Firewall ports provisioning, subnet infrastructure are performed by 3rd party vendor.
4. Storage provisioning are performed by 3rd party vendor
5. DR procedures are managed by 3rd party vendor
6. IP Re-addressing for DNS server is performed by AVA
7. DNS infrastructure designing is performed by AVA
8. DNS Implementation is performed by AVA
9. DNS impact analysis is performed by AVA
10. DNS tests are performed by AVA
11. Public Namespace is managed by ISP
12. Private Namespace is hosted by HYDRA
13. Privileges to logon to DNS Servers / Domain Controllers are provisioned by HYDRA

**DNS Design Considerations:**

AVA has the following design for restructuring the DNS infrastructure for HYDRA.

a) DNS Server IP will be configured with private Internet Protocol address
b) DNS server will be staged in Demilitarized zone and rely on Root Hints for name resolution.
c) Clients will be pointing to intranet DNS server and any request for public namespace will be managed by DMZ DNS servers
d) Inbound and Outbound Firewall ports should be managed by HYDRA for DNS requests
e) IP Address range should be configured that fall under valid range and should be Static IP address
f) DMZ DNS server will not be configured with forwarders, rather rely on root hints for name resolution
g) Disable Caching on the DMZ DNS servers which prevents possible DNS Cache poisoning
h) Re-configure clients DNS IP Address with DNS Server which has new IP address configured.
i) Configure Secondary Zone for the HYDRA.Local name space.

**Installation Pre-requisites:**

AVA assumes that following are provisioned by HYDRA respectively

a) Provision of Virtual Servers which includes Hardware, Network and Memory is configured by HYDRA professionals.
b) Installation and Configuration of the Windows Server 2008 R2 in DMZ network (Full edition) Operating System is performed by AVA consultants
c) Network devices and ports are configured by HYDRA engineers and ensure the firewall ports are opened for DNS Servers communications between Production and DMZ sites.
d) Remote Monitoring for the servers are provisioned and desired firewall ports are enabled for AVA consultants to access the servers on different farms

e) Ensure the patching of the servers are compliant with the HYDRA standards and performed by HYDRA Operations team

f) Ensure the auditing of the servers is performed prior installing of the Domain Controllers.

g) Ensure all the relevant applications (eg: Anti-virus ) are installed and configured on the server which will be configured as DNS server.

Assumptions:
- This document will not provide detail step-step visual information about the configuration of DNS server in DMZ environment.
- This document will provide best practices to restructure the DNS infrastructure.

Installation Steps:
Following are the installation steps for restructuring DNS infrastructure on the HYDRA Data Center

1) On the DNS server that will be configured on the DMZ, follow the below steps
   a) The Server to configure as DNS, ensure the static IP address is configured
   b) Proper privileges to launch the Server Manager
   c) Ensure the firewall ports specified in Step 3 are configured appropriately ( PortQry tool can be use to verify the ports )
   d) Account to install the DNS server role and configure the role accordingly
   e) This DNS server will not be hosting any zones
   f) DNS server will not be configured with Forwarders and rely on Root Hints for name resolution

2) Logon to Intranet DNS server which is managing Hydra.local namespace. The user should have privileges to modify the DNS server properties. This operation can be done physically logging on to the server or through remote DNS server MMC.

3) On the Intranet DNS server Check the basic networking connectivity on the Server and ensure the server is opened for the following Ports

<table>
<thead>
<tr>
<th>Protocol and Port</th>
<th>AD and AD DS Usage</th>
<th>Type of traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP and UDP 53</td>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
<td>DNS</td>
</tr>
<tr>
<td>UDP 138</td>
<td>DFS, Group Policy</td>
<td>DFSN, NetLogon, NetBIOS Datagram Service</td>
</tr>
<tr>
<td>UDP 67 and UDP 2535</td>
<td>DHCP</td>
<td>DHCP, MADCAP</td>
</tr>
<tr>
<td>Protocol</td>
<td>Port</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UDP 137</td>
<td></td>
<td>User and Computer Authentication,</td>
</tr>
<tr>
<td>TCP 139</td>
<td></td>
<td>User and Computer Authentication, Replication</td>
</tr>
</tbody>
</table>

4) Ensure the Domain Controller / DNS Server is configured with Static IP address. Validate the subnet mask and Default gateway configured on the server – Strictly no multi home networks

5) Ensure the IPv4 Static address is configured on the DNS Server interface and configure with valid range.

6) Ensure the binding order of the working interface is always configured in the highest order

7) DNS Cache locking is configured as per HYDRA requirement, by default it is set to 90%

8) Ensure the Forwarding timeout is set to 6 seconds

9) Ensure the DNS host file on the DNS server should be empty

10) Ensure the Primary DNS server IP is configured to itself

11) Ensure the DNS server Scavenging is configured and set automatic scavenging ( default 7 days )

12) Ensure that only desired DNS server is set for scavenging and disable scavenging on secondary DNS servers

13) Ensure the recursion timeout must be greater than the forwarding timeout

14) Remove the ISP IPAddress from DNS forwarder list and point to DMZ DNS server Ipaddress to forward the requests

15) Test the reverse lookup behavior

16) Test the name resolution from client operating system, and any applications which are requesting for External name space ( Hydra.local or Microsoft.com )

17) Use Wireshark / Netmon sniffer utilities to analyze the response time. This includes thorough understanding the client NIC adapter, MTU size, RSS response times.
18) Apply the required server hardening and the Group policies to manage DNS infrastructure.

This document provides design consideration of restructuring DNS infrastructure and the best practices.