radware

Alteon Application Switch optimizing the delivery of VMware Horizon 6.2

Contents

Introduction

Implementing VMware Horizon in an organization introduces a new set of challenges for IT, pushing its infrastructure to the limit and challenging its current administration policies. VMware Horizon requires that an organization meet SLA commitments and provide QoE assurances. The inability to comply with these requirements will result in user frustration and loss of user productivity.

This guide presents a standardized integration solution in which Radware's load balancing and acceleration product, Alteon, is set up in front of a VMware Horizon environment to ensure its availability and performance in order to meet SLA and QoE requirements.

Alteon Next Generation ADC

Alteon NG is Radware's next generation application delivery controller (ADC) and the only load balancer that guarantees application SLA. It provides advanced, end-to-end local and global load balancing capabilities for all Web, cloud, and mobile based applications. The Alteon NG load balancer combines best-of-breed application delivery plus advanced services to companies with key application infrastructure challenges affecting Web applications such as heavier, more complex Web content; mobility, and BYOD, and the migration to the cloud.

Alteon NG: Complete Application SLA Assurance

The Alteon next generation (NG) ADC solution is the industry's only ADC built from the ground up to ensure application SLA at all times. It innovatively leverages several next-generation services that are not available in any other ADC on the market:

- Alteon NG is architecturally designed to ensure application SLA by delivering full resource isolation between different applications, while eliminating resources from being maxed-out.

- Alteon NG incorporates application performance monitoring (APM) capabilities that provide full visibility into application SLA that can be broken down by application, transaction, or location.

- Alteon NG integrates FastView, the industry's most advanced Web performance optimization (WPO) technology, which accelerates application response for higher conversion rates, revenues, and productivity.

- Alteon NG is part of unique attack mitigation architecture, allowing accurate detection and mitigation of the most advanced cyber-attacks.

Architecturally Designed to Ensure Application SLA

Alteon NG enables companies to flexibly allocate a separate virtual ADC (vADC) instance per application, service, or department. Each vADC instance is fully isolated from neighboring instances and has independent CPU cores, memory, network stack, management control, and operating system versions. As a result, the Alteon ADC ensures complete fault isolation and predictable application SLA for all delivered Web applications at all times. In addition, next-

generation services can be quickly and safely enabled without impacting the performance of other service applications.

Alteon NG is designed to dynamically scale when necessary. It can scale up on-demand, meaning you can add more throughput, services, and vADCs with no hardware modifications. It can also scale out-of-the-box on demand by leveraging an external, extensible resource pool (such as server infrastructure) for computational intensive NG services. As a result, Alteon NG allows for cost-effective consolidation, eliminating the purchase of additional ADC units. It provides easy, fast provisioning of additional vADC instances with no service interruption at a fraction of the cost of buying a physical ADC.

Full Application SLA Visibility with Radware's Application Performance Monitoring (APM)

Radware's Application Performance Monitoring (APM) module provides real-time tracking of application SLA by measuring real-user transactions, including real errors. Embedded in Alteon NG, Radware's APM is an out-of-the box solution that does not require synthetic transaction scripting or additional installation, thereby reducing deployment time and costs. Radware's APM intuitively tracks SLA by location, user, and application and transaction type, to expedite root cause analysis. In addition, it provides historical reports based on user-defined SLA that feature granular analysis allowing the measurement of the delay per transaction phase, including data center time, network latency, and browser rendering time.

FastView™ Web Performance Optimization (WPO)

Radware's FastView™ technology, part of Alteon NG, is the most advanced application acceleration technology in the industry. By adding Web performance optimization (WPO) capabilities on top of the standard application acceleration features, it accelerates application response time up to 40%. FastView acceleration treatments are optimized according to each user, end-user device, and browser, with specific optimization for mobile devices. As a result, FastView increases conversion rates and revenues and also improves productivity and customer loyalty.

In addition, FastView™ automatically optimizes new applications, new application versions, and new application modules, reducing manual code optimization while letting you focus on core business competence.

Unique Attack Mitigation Architecture

A key component of Radware's Attack Mitigation Network (AMN), Alteon NG delivers the best Web application security coverage. It leverages a unique Defense Messaging mechanism that efficiently mitigates attacks by signaling attack information to Radware's DefensePipe cloud service and DefensePro, a data center attack mitigator located at the network perimeter.

The integration of advanced Web Application Firewall (WAF) capabilities, such as a unique out-of-path WAF deployment mode and auto-policy generation features, enable risk free implementation. In addition, full instance isolation and resource reservation ensures ADC

resources. Even when WAF policies are updated, there is no impact on application availability and performance. This results in a secured Web application with guaranteed SLA. Finally, Alteon NG features a built-in authentication gateway that provides single sign-on (SSO) capabilities by supporting RADIUS, Active Directory, LDAP, and RSA SecurID, and simplifies the user experience without compromising application security.

Complete Layer 4-7 Feature Set

Alteon NG delivers a complete set of Layer 4-7 services to ensure the availability, performance, and security of mission-critical applications in the local and cloud data centers. These extend to traffic redirection, content modification, persistency, redundancy, advanced health monitoring, and global server load balancing (GSLB). In addition, Alteon NG integrates advanced modules such as bandwidth management and link load balancing, reducing data center footprint and simplifying deployment.

Shaped to Deliver Applications

With Radware's AppShape™ technology, Alteon ADC benefits from reduced deployment time of application delivery services by 85%, while guaranteeing maximum value for each business critical application in terms of availability, performance and security. AppShape offers configuration templates and wizards for leading business applications. AppShape allows application delivery services to be fully managed and operated from an application-centric view, including operational screens, logs and compliance – resulting in simplified and efficient application management in the ADC. Furthermore AppShape's reporting capabilities help organizations with capacity planning tasks by providing per application trends analysis and resources utilization reports.

VMware Horizon

VMware Horizon delivers rich, personalized virtual desktops as a managed service from a virtualization platform, built to deliver the entire desktop, including the operating system, applications, and data. With VMware Horizon, desktop administrators virtualize the operating system, applications, and user data and deliver modern desktops to end-users. VMware Horizon provides centralized automated management of these components for increased control and cost savings. It improves business agility while providing a flexible high performance desktop experience for end-users across a variety of network conditions.

VMWare Horizon brings the agility and availability of cloud computing to the desktop and applications. Built on VMware vSphere, Horizon delivers desktops from a single integrated platform as part of your cloud services. You can dynamically allocate resources to enable highly responsive and available environment to end-users. You can scale up and down desktop services on demand to quickly meet changing business needs and proactively protect against planned and unplanned downtime. You can run your desktops as business critical services for your workforce.

VMware Horizon increases control of desktops, applications and data by delivering and managing them as centralized services. A single, powerful administrative console provides oversight of desktop services while enabling IT to execute previously cumbersome tasks such

as provisioning, updates, and patches, with a few mouse clicks. You can manage desktop components separately for greater flexibility in provisioning, updates, and delivery. You can easily apply policies and quickly enable and disable users, all from a centralized console for optimal business response. Horizon frees up time from maintenance for technology innovation.

Radware Alteon and VMware Horizon Server Architecture

Figure 1 – Tested Example Configuration
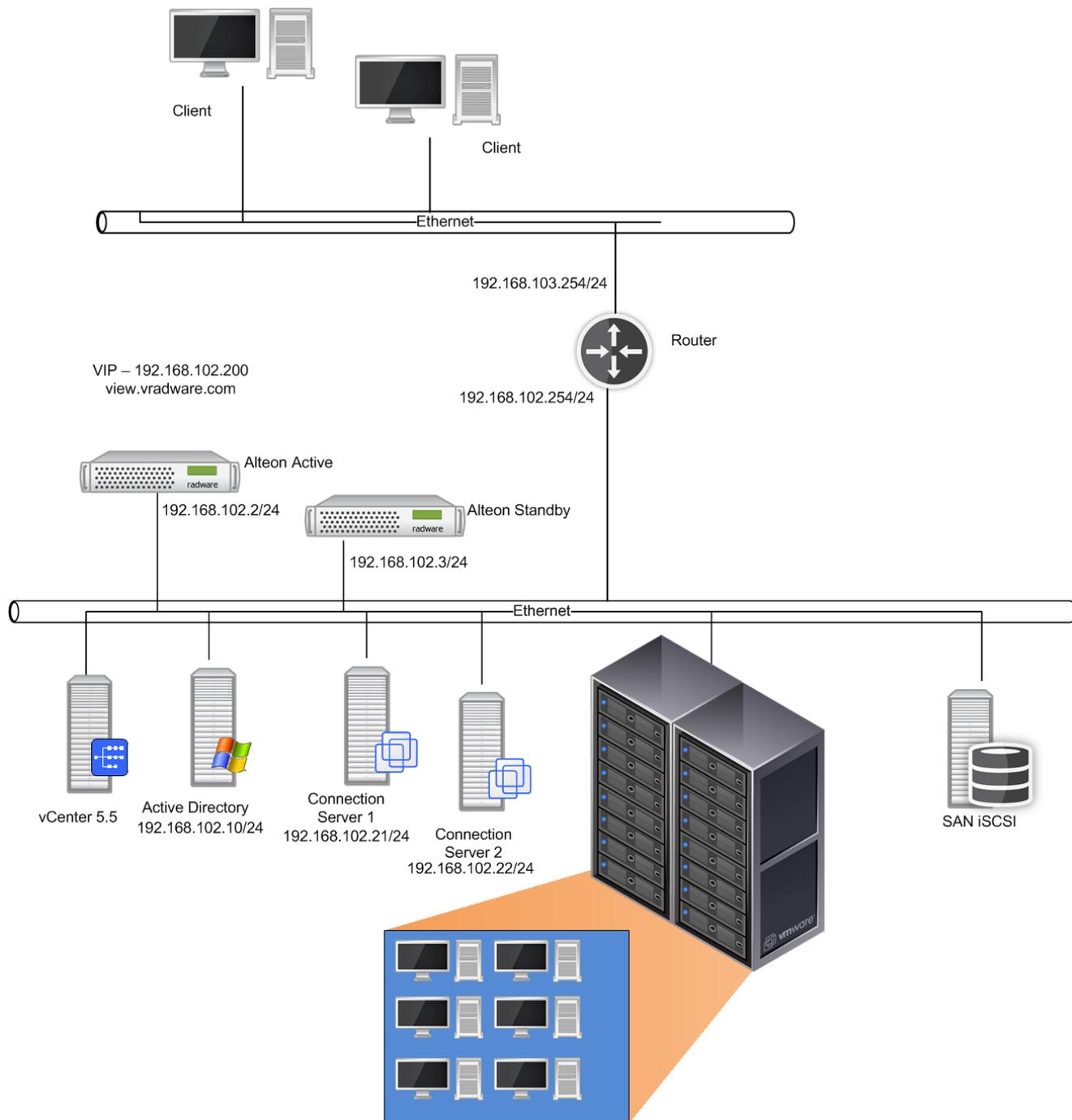
Prerequisites

Important Implementation Notes

- Throughout this guide, reference is made to the "Radware" pre-configured certificate, but you can import a certificate or create a new certificate in Alteon. For more information on exporting, importing, or creating a certificate, see the *Alteon Application Switch Operating System Application Guide*.

- The VMware Horizon SSL Certificate must be installed on all connection servers and on the Alteons:

  - The certificate must include inside the server's certificate (DNS field) the connection servers' names and VIP names. For example: `VIP – view.vradware.com and connection servers con1.vradware.com, con2.vradware.com, con1 and con2`. If you have Wildcard certificate, use `*.vradware.com`.

  - The common name should be the VIP name, for example: `view.vradware.com`

- VMware Horizon can work in the following ways:

  - **Blast Secure Gateway** – All traffic (PCoIP and login) on port 443 (secure) goes through the connection servers (proxy mode).

  - **PCoIP Secure Gateway mode** – All PCoIP traffic goes on port 4172 through the connection servers (proxy mode).

  - If only **use Secure Tunnel Connection** is selected – Login goes through the connection servers (443 secure), and PCoIP traffic goes directly from the client to the selected VM.

- **VERY IMPORTANT** - If you are using **PCoIP Secure Gateway mode** - Change all load balancing on ports 4172, 443, and 8443 to use source IP persistency (the Layer 7 configuration does not work).

- Persistency is performed by using Layer 7 the AppShapes script for VMware services – HTTPS Secure Tunnel and/or Blast Secure Gateway.

- The default Aging time for a session is 600 minutes, which can be changed inside the connection servers and inside the Alteon AppShapes script.

Software and Hardware

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

- Microsoft Windows 2008 R2 x64bits

- Radware Alteon version 30.0.2

- VMware Horizon Connection, Agent, Composer and client v.6.2

- VMware vCenter 5.5

Configuration

Alteon Active Configuration

Network Configuration

```
/c/sys/mmgmt
      dhcp disabled
      addr 192.168.101.2
      mask 255.255.255.0
      broad 192.168.101.255
      gw 192.168.101.254
      ena
/c/sys/access
      tnet ena
/c/port 1
      pvid 102
/c/l2/vlan 1
      learn ena
      def 0
/c/l2/vlan 2
      dis
      learn ena
      def 2
/c/l2/vlan 102
      ena
      name "LAN"
      learn ena
      def 1
/c/l2/stg 1/clear
/c/l2/stg 1/add 1 2 102
/c/sys/access/sshd/ena
/c/sys/access/sshd/sshv1 dis
/c/sys/access/sshd/on
/c/l3/if 1
      ena
      ipver v4
      addr 192.168.102.2
      vlan 102
/c/l3/gw 1
      dis
```

```
      ipver v4
      addr 192.168.102.254
```

Sync Configuration

```
/c/slb/sync
      pips e
      certs e
/c/slb/sync/peer 1
      ena
      addr 192.168.102.3
```

PIP Configuration

```
/c/slb/pip/type port
/c/slb/pip/add 192.168.102.201 1
```

Compression Configuration

```
/c/slb/accel/compress
      on
/c/slb/accel/compress/comppol 1
      minsize 1
      ena
```

Health Monitoring Configuration

```
/c/slb/advhc/health VMware_Horizon HTTP
      ssl enabled
/c/slb/advhc/health VMware_Horizon HTTP/http
      host "view.vradware.com"
      path "/broker/xml"
      response 403 incl "clientlaunch-default"
```

AppShapes Configuration

```
/c/slb/appshape/script 5
      ena
      name "VMwareView62"
      import text
when INIT {
    set ::timeout 36000
}
when HTTP_REQUEST {
    if { [HTTP::cookie exists "JSESSIONID"] == 1 } {
        set found [persist lookup usid [string range [HTTP::cookie
value "JSESSIONID"] 0 31] any virtual server]
        if {$found != ""} {
```

```
                    group select [LB::server group] server $found
            }
      } else {
            set sjsess [string first "tunnel?" [HTTP::uri]]
            if {$sjsess != -1} {
                  set found [persist lookup usid [string range [HTTP::uri]
[expr $sjsess + 7] end] any virtual server]
                  if {$found != ""} {
                        group select [LB::server group] server $found
                        HTTP::disable
                  }
            }
      }
}
when HTTP_RESPONSE {
      if {[HTTP::status] == 101} {
            if {[HTTP::header value Connection] == "Upgrade"} {
                  HTTP::disable
                  return
            }
      }
      if { [HTTP::cookie exists "JSESSIONID"] == 1 } {
            persist add usid [HTTP::cookie value "JSESSIONID"] any virtual
$::timeout
      } else {
            HTTP::collect
      }
}
when HTTP_RESPONSE_DATA {
      set connection_id_start [HTTP::payload find "<connection-id>"]
      if {$connection_id_start != -1} {
            set connection_id_start [expr $connection_id_start + 15]
            set connection_id_end [HTTP::payload find "</connection-id>"]
            persist add usid [HTTP::payload $connection_id_start [expr
$connection_id_end - $connection_id_start]] any virtual $::timeout
      }
}
-----END
```

Alteon Process Directions
```
/c/slb/port 1
      client ena
```

```
        server ena
        proxy ena
```

SLB Configuration
```
/c/slb
        on
/c/slb/adv
        direct ena
        vstat ena
        submac "ena"
/c/slb/sync
        pips e
        certs e
/c/slb/sync/peer 1
        ena
        addr 192.168.102.3
/c/slb/real 1
        ena
        ipver v4
        rip 192.168.102.21
        name "Horizon.1"
/c/slb/real 2
        ena
        ipver v4
        rip 192.168.102.22
        name "Horizon.2"
/c/slb/group 1
        ipver v4
        metric roundrobin
        health VMware_Horizon
        add 1
        add 2
        name "Horizon.group"
/c/slb/group 2
        ipver v4
        add 1
        add 2
/c/slb/group 3
        ipver v4
        metric roundrobin
        add 1
```

```
      add 2
      name "TCP.4172"
/c/slb/group 4
      ipver v4
      metric roundrobin
      add 1
      add 2
      name "TCP.8443"
/c/slb/pip/type port
/c/slb/pip/add 192.168.102.201 1
/c/slb/port "1"
      client ena
      server ena
      proxy ena
/c/slb/port "2"
      client ena
      server ena
      proxy ena
/c/slb/virt 1
      ena
      ipver v4
      vip 192.168.102.200
      vname "Horizon.service"
/c/slb/virt 1/service 443 https
      group 1
      rport 443
      dbind forceproxy
/c/slb/virt 1/service 443 https/ssl
      srvrcert cert 1
      sslpol 1
/c/slb/virt 1/service 443 https/appshape
      add 1 5
/c/slb/virt 1/service 4172 basic-slb
      group 3
      rport 4172
      pbind clientip norport
/c/slb/virt 1/service 8443 https
      group 4
      rport 8443
      dbind forceproxy
```

```
/c/slb/virt 1/service 8443 https/ssl
     srvrcert cert 1
     sslpol 1
/c/slb/virt 1/service 8443 https/appshape
     add 1 5
/c/l3/hamode vrrp
/c/slb/gslb
     off
     hostlk ena
/c/sys/access/https/cert WebManagementCert
/c/sys/access/https/https e
```

SSL Configuration

```
/c/slb/ssl/certs/key 1
/c/slb/ssl/certs/import key "1" text
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9609515F8314EB7B
```

```
wvPpTwEGLuFC0CDTy6jKAHRqqAIFggyswp+I+sFul60aqCyV/ouAp8xCb5/8RqZJ
TEb60/6ZNwznrdSgzVjlAoDHpI4Qgw71CXnKMNbCeBdOlBh/NSikCTvKSlv0m1R3
eckI4dQnlxXQCQXGrMjSCjwke/XfzaNUH7yQ5mLeKhsq4GizJXIwZWx/836YLzwU
azHg4b+seyYDnddjf4e+H3odKz8nmqaabtFnulQsRPjo/XWJcy5ZKRrbMEHJh37p
jKpUEJye0bAeYoir96mlQbs5BpzHATA8yLHuTRp8kBJjs7BTM3HurzwoXg7sPn69
y0Gp0WEN17rYvml5yshuUgutHC6Sr7wSE3oh349ZXoBeXash/I1FbU30ZRUgU2rV
tXOpyXldG25fCKGA1GAWHO+aqv0w0zZyDQntFKCThMzltirTcT1wOh2vB5T+ooXT
bGFcusdqQI3BLIb7nKYeFlTgMlfgh6Y0KkFlr2iP1r3Os54rdbd0AJulLNrZ21JK
KYZka2MwB++/JJHEuodt5CIt/C9uSu9WAgFiw12wiCii7lCVtAF7c+MtvioojBQG
Prpfi4ABAOKjq2TPdyqBkdvQHPMhqMJtGROTJMHDS/JflVHOtg4soboUghS5Uov+
uABsYXOXj9QQ55rV/sy5fH19j/1IN+Nqwroc0JEoS+m/6+IX1vA1vR/2J34db7SI
ui/XhTqj2TPVP56kIVIE0k5yZKYUr5kXM5xD2DAm0bTaq7qgodP8oUHS+qokIyGo
6Py2rcz28gCIMbC7yP9ztzbL5S5Njpsvs7B9kTBJ90I3SL0Wi2hw3DJbHo6VlxPV
zy1je4RrdDa96g5Mek2RPVgrqvOs2RMDjW+CuOKzZHlH8XCm4SXhx5poqdp1U4D+
kQjb1KGCjb3eib1zNvBZ8ulS5osyNBKp6aEoUQn6pVBycGQx+YjwEEXb/sPX2A3S
xNm2IfKpHDbqrI5eroF3qxQa1+jQ5iKz9Cr5o5b6lJg3sMmRFGIEPgNQEIhA3abz
68dNXq5ZzVAsy+WZ5UCLTF/Ih5iVwoJT11XWFu6ioHBfJWjcnyQhPii/CxH3vY19
HzNcUQKWehBqKkV7SrJ3Ad3Vx2/DCWzB4qOgN5QBzehgAlw4r4LzMb0hhi2U5BfT
wxkfo9v21ngSKB05zh7ABzFO12VrIsYs0IUgak4xMCPvXzQHLowFtekRpHlh7nSz
FcbCyCu/VsCrmGF5VTgVWgrtXtzOUrCfn3pCpvhPd9U2tG/WGkUa0H1V1Qx3WR4c
Pakimt59Jas/EY8DMZ2FE3SUST2L8yCjvdo2/+HGqgPP22wTJQ7KZqGHf5V1GscD
xQwqAP4kiZdE116/sIRUR19ShtTd8DCm0QMGyfF2hX4EivRuON86tfqaIUzR4LCL
```

LPOk6tJZoLiqyv0Dlv0cv00jmZcrPJ/h5vftVXWrvhLiF7n20tzhEvkcBfdxQkZq
bjg1gaESh1edW/yf9VR24zDS66lKRzXZOr1XUF5FccMS863LADPpF7jK4MjU0A9g
S/ybZ9tDOFkT/CYsJI95MTGqUoXjbNpudmei/SsdN0ciSrfUPBZ9OA==
-----END RSA PRIVATE KEY-----

/c/slb/ssl/certs/cert 1
/c/slb/ssl/certs/import cert "1" text
-----BEGIN CERTIFICATE-----
MIIGBDCCBOygAwIBAgIKYUqgwgAAAAAABDANBgkqhkiG9w0BAQUFADBKMRMwEQYK
CZImiZPyLGQBGRYDY29tMRgwFgYKCZImiZPyLGQBGRYIdnJhZHdhcmUxGTAXBgNV
BAMTEHZyYWR3YXJlLUNFUlQtQ0EwHhcNMTUxMDI3MTQwNDI3WhcNMTcxMDI3MTQx
NDI3WjAcMRowGAYDVQQDExF2aWV3LnZyYWR3YXJlLmNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBANDS9rd1Lh/58WSWJSPx4J+Te42S2EfNH20g1OLk
JpVpqCgcvd8XSaz6nx4GZikTPaZKcqsH/v6vFiXLVs6HPxm0ksQ+93kYd5Bz7CqV
XbAz01XLIchGn7B/WaLs0ST44zaYWzxV2QdOByOENSXtZCvBki05lR0ezGiTsS4f
OmTCkk8Z7JVvITksm1KvF7H7hXbzMOapEVpkzed9Nl3KRwJEffog9NPMB6srjns5
shL6mSe8VYo2sX4apEXeyfNSMlw7zYvslJeP2ygvlaRec0H5S0oVJ6gaRW1jpqmG
cG/NuKmw9fX+Ygf0BNPs+/Cld+Eoq4Q2aweSOOWKV42bdckCAwEAAaOCAxgwggMU
MD0GCSsGAQQBgjcVBwQwMC4GJisGAQQBgjcVCIaV2y6G9/NEhf2JJIWfsS+GhYRm
gUfypwWHyZAdAgFlAgEBMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAO
BgNVHQ8BAf8EBAMCBPAwJwYJKwYBBAGCNxUKBBowGDAKBggrBgEFBQcDATAKBggr
BgEFBQcDAjAdBgNVHQ4EFgQU1DZLz5Nv60Stoybv+FBCFjP60tgwgaUGA1UdEQSB
nTCBmoIRY29uMS52cmFkd2FyZS5jb22CBGNvbjGCEWNvbjIudnJhZHdhcmUuY29t
ggRjb24yghF2aWV3LnZyYWR3YXJlLmNvbYIEdmlld4IRc2VjMS52cmFkd2FyZS5j
b22CEXNlYzIudnJhZHdhcmUuY29tggRzZWMxggRzZWMyghNzZWN1cmUudnJhZHdh
cmUuY29tggZzZWN1cmUwHwYDVR0jBBgwFoAUpMB2QmTghtBJ0pGhX7QJ7Gv5RZIw
gcwGA1UdHwSBxDCBwTCBvqCBu6CBuIaBtWxkYXA6Ly8vQ049dnJhZHdhcmUtQ0VS
VC1DQSxDTj1jZXJ0LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPXZyYWR3YXJlLERDPWNvbT9j
ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz
dHJpYnV0aW9uUG9pbnQwgcMGCCsGAQUFBwEBBIG2MIGzMIGwBggrBgEFBQcwAoaB
o2xkYXA6Ly8vQ049dnJhZHdhcmUtQ0VSVC1DQSxDTj1BSUEsQ049UHVibGljJTIw
S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz12
cmFkd2FyZSxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNl
cnRpZmljYXRpb25BdXRob3JpdHkwDQYJKoZIhvcNAQEFBQADggEBAAoDLG/cguXR
yM+1py27bQhwr6i7bGBxuYsJTb0pU3q7cebNEU+Ln465qX4/ZN89fBWQQZDHh6Id
hULueHTUh0w4Tl/V373XNupQm5IWeODxbulIJFh3sH3K4Fc635MlthT08S8W2/jd
wwyclQohWIWe8QhKGCNpSKshItf+ipytbGVNYroOEFqVNu6zlGEofiGbZDJZY3wT
V0wX0H/rULlD1ecIgIPjT3hMbh+D00PbBduIt5WzN5EEi8dMeHPeY3z+cJtSzMyE

```
Ik6IPBf3NF8KjC3OpF6mVaMR/HFjzIRP9kBlbOK82Vq0bMg7VRwSQiHNg1rySV0o
ETuf+dvsaeY=
-----END CERTIFICATE-----


/c/slb/ssl
      on
/c/slb/ssl/sslpol 1
      name "Horizon.view"
      convert disabled
      ena
/c/slb/ssl/sslpol 1/backend
      ssl enabled
      cipher "high"
```

VRRP Configuration
```
/c/l3/vrrp/vr 102
      ena
      ipver v4
      vrid 102
      if 1
      prio 250
      addr 192.168.102.1
/c/l3/vrrp/vr 103
      ena
      ipver v4
      vrid 103
      if 1
      prio 250
      addr 192.168.102.201
/c/l3/vrrp/vr 104
      ena
      ipver v4
      vrid 104
      if 1
      prio 250
      addr 192.168.102.200
/c/l3/vrrp/group
      ena
      ipver v4
      vrid 254
```

```
        if 1
        share dis
```

Alteon Standby Configuration

Network Configuration
```
/c/port 1
        pvid 102
/c/l2/vlan 1
        learn ena
        def 0
/c/l2/vlan 102
        ena
        name "LAN"
        learn ena
        def 1
/c/l2/stg 1/clear
/c/l2/stg 1/add 1 2 102
/c/sys/access/sshd/ena
/c/sys/access/sshd/sshv1 dis
/c/sys/access/sshd/on
/c/l3/if 1
        ena
        ipver v4
        addr 192.168.102.3
        vlan 102
/c/l3/gw 1
        ena
        ipver v4
        addr 192.168.102.254
```

Sync Configuration
```
/c/slb/sync
        pips e
        certs e
/c/slb/sync/peer 1
        ena
        addr 192.168.102.2
```

VRRP Configuration
```
/c/l3/vrrp/vr 102
        ena
```

```
        ipver v4
        vrid 102
        if 1
        prio 250
        addr 192.168.102.1
/c/l3/vrrp/vr 103
        ena
        ipver v4
        vrid 103
        if 1
        prio 250
        addr 192.168.102.201
/c/l3/vrrp/vr 104
        ena
        ipver v4
        vrid 104
        if 1
        prio 250
        addr 192.168.102.200
/c/l3/vrrp/group
        ena
        ipver v4
        vrid 254
        if 1
        share dis
```

VMware Horizon Connection servers (connection 1)

-       IP Address – 192.168.102.21/24
-       DG – 192.168.102.254

VMware Horizon Connection servers (connection 2)

–   IP Address – 192.168.102.22/24
–   DG – 192.168.102.254

VMware Horizon Connection Servers

Configure VMware Horizon Connection global settings

Go to the **View Configuration > Servers > Connection servers** tab and edit each connection server, add the External URL name 'https://view.mycomapny.com:443' (this will be the name that the clients are pointing to)
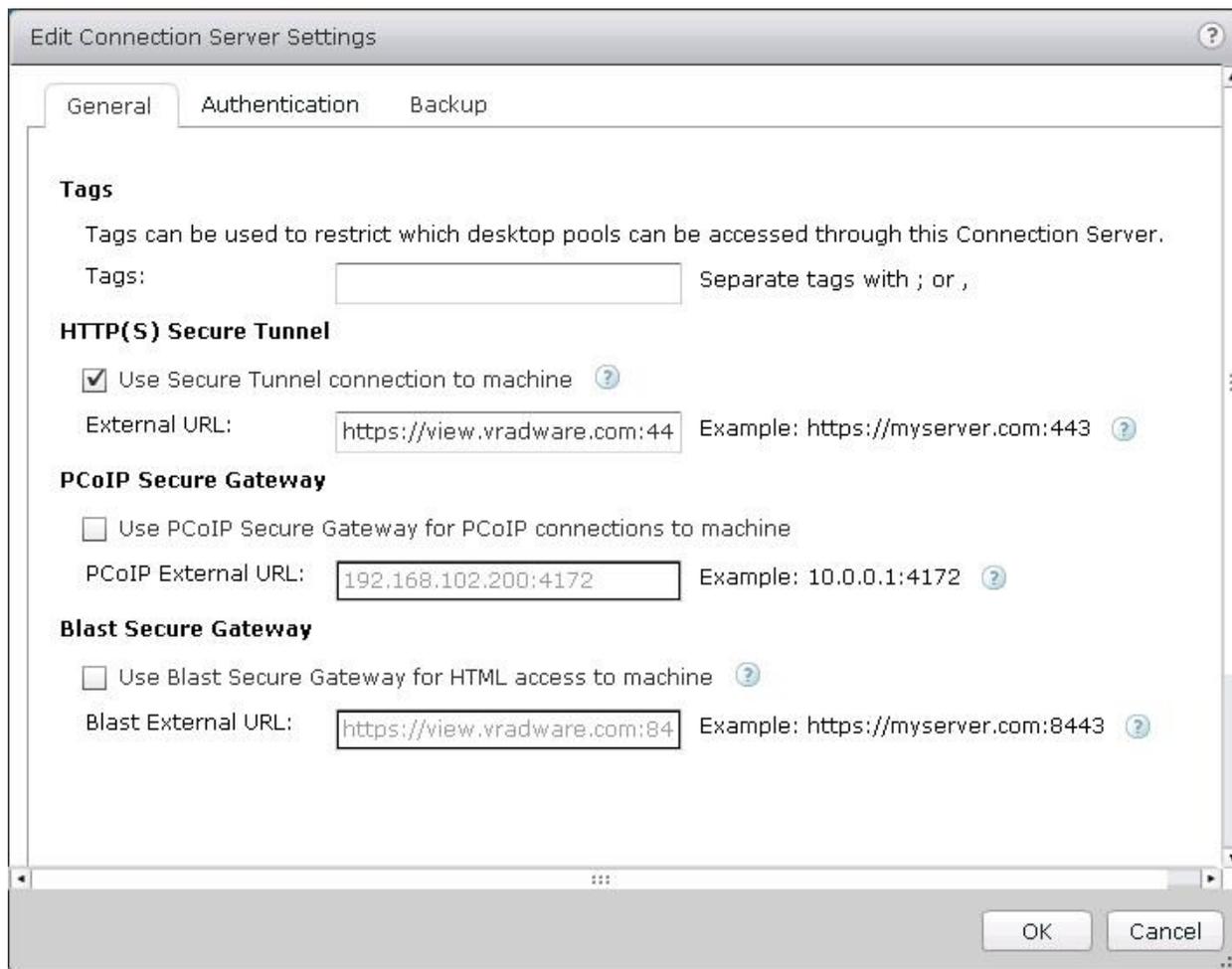
Technical Support

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

North America

Radware Inc.

575 Corporate Drive

Mahwah, NJ 07430

Tel: +1-888-234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.

Tel Aviv 69710, Israel

Tel: 972 3 766 8666