Horizon Air 15.3.2 Access Point Setup

July 2015

vmware

Revision History

Date	Version	Description
08/05/2015	1.0	Initial release

© 2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

This page intentionally left blank.

1 Overview

This document describes the process for setting up Access Point, which is a new solution replacing the existing Remote Access Manager (dtRAM) in DaaS deployments. Access Point is a VMware developed End-User Computing (EUC) appliance that acts as a specialized gateway (or reverse proxy) that manages access to enterprise EUC products deployed in a private or public cloud. It consolidates functionality that was previously implemented in various enterprise EUC products, and simplifies deployments for customers who use multiple EUC products within their environments.

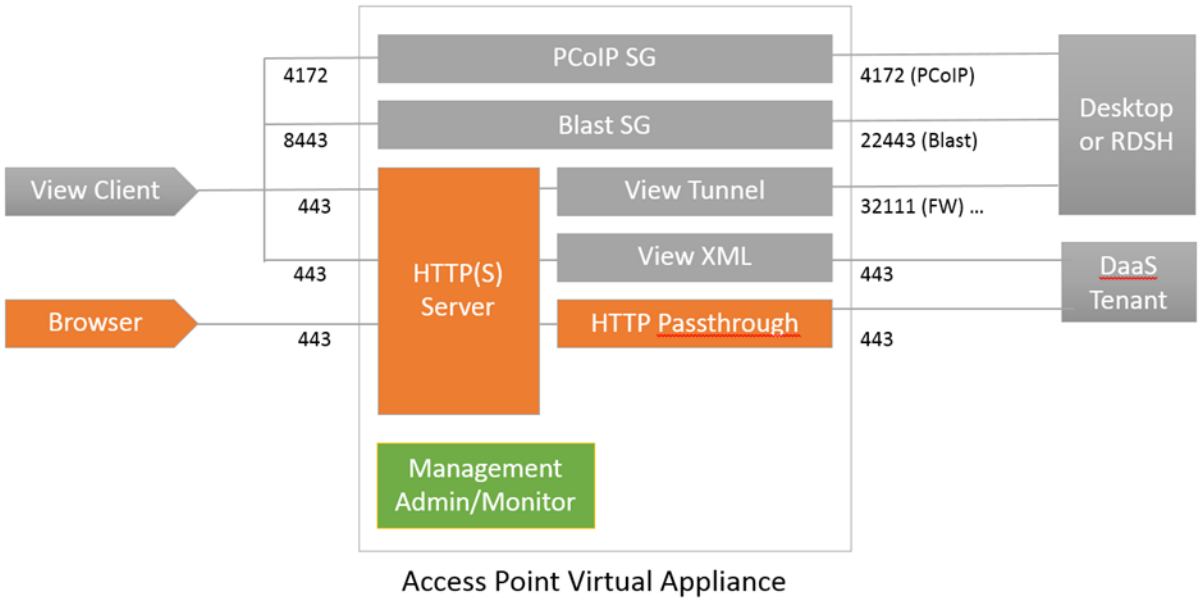
The following are advantages of migrating to Access Point:

- Customers who migrate to Access Point can reduce their firewall open ports to 443, 4172 and 8443.
- Access Point will properly handle SSL certificates for HTML Access (Blast) so that a certificate will no longer be required on the virtual desktop.

  Note: For internal access not via Access Point, desktops will still need to have SSL certificates.

1.1 High-Level Architecture

The diagram below shows the high-level architecture of Access Point configured in a DaaS deployment.



1.2 Basic Functionality

The basic functionality of Access Point is as follows.

- The client makes a connection to the reverse proxy, and when the response comes back, the client intercepts it.
- The connection can be established by either a browser or the Horizon client.
- Once a virtual desktop session is established, the PCoIP SG, Blast SG, or View Tunnel may be used for the virtual desktop traffic, depending on what protocol the user has selected. The tunnel is used for the RDP protocol as well as USB connections.

Access Point used in a Horizon DaaS deployment has the following characteristics:

- There will be no authentication (at least for the first release). This responsibility will remain within the Tenant Appliance.
- All communication will be proxied through Access Point if the end-user is accessing the solution from outside of the corporate network. This includes:
    - All View specific protocol handling (XMLAPI, PCoIP, etc)
    - Any Tenant Appliance communication

1.3 Access Point vs. dtRAM

The main differences between the existing dtRAM and Access Point are outlined in the table below.

dtRAM	Access Point
Tenant appliance sits in front of the dtRAM and controls its operations	Access Point appliance sits in front of the tenant appliance so that the tenant does not know it exists. The tenant requires software changes to accommodate this new architectural shift.
Does not make use of a PSG (or BSG or Tunnel) gateway that is installed	Makes use of a PSG (or BSG or Tunnel) gateway that is installed
Needs to use a wide range of ports for PCoIP etc. from the client and requires customers to open all of these ports to allow access	All PCoIP traffic can come in on the standard port (4172). Other single ports are used for BSG and Tunnel.
BSD-based and uses "pf" to forward traffic	Linux appliance with built-in proxying capabilities
Supports HA clustering	HA clustering is possible if you choose to configure load balancers (see example in Appendix A)
Supports geographically dispersed datacenters	Does not support geographically dispersed datacenters in the first release
Has security weaknesses because it can only validate traffic based on source IP address	Uses deep protocol inspection techniques to ensure that traffic from the client is properly validated before it is passed on to the virtual desktops

1.4 Performance

The following are some considerations regarding Access Point performance.

- **Capacity –** Access Point has been tested with as many as 2,000 concurrent sessions, but the number of sessions your system can handle depends on the amount of data being sent and received (for example, video content).
- **Monitoring–** Access Point does not currently have an internal monitoring tool, but you are able to obtain usage information using vCloud Director monitoring of the tenant appliance.
- **Rebooting –** Performing a reboot operation for Access Point disconnects all active users. The user's desktop session remains active, but the user will need to reestablish the connection to regain access to the desktop. If Access Points are deployed in a load balanced configuration with multiple Access Points, then any active or new users will be able to immediately reconnect via the load balancer and the connection will be handled by another Access Point while one is rebooting.
- **High Availability / Failover –** HA clustering is possible if you choose to configure load balancers (see example in Appendix A).

2 Set Up Access Point

Note: You cannot deploy an Access Point VM from a vSphere Windows client. You must deploy it from the vSphere web client.

1. Download the latest version of the Access Point OVA file.
2. Determine the IP addresses (DNS/Netmask/Gateway) for the required networks, as described below.

Configuration	Networks	
3 NIC **(Recommended configuration)**	**Internet (NIC 1)**	Any network with internet access
	Management (NIC 2)	This can be your 169 network. Since this does not have its own DNS or Gateway, you can enter any numbers for DNS and set the netmask to 255.255.255.0
	Backend (NIC 3)	Network that the Tenant uses for desktops
2 NIC	**Internet (NIC 1)**	Network the Tenant is on
	Management (NIC 2)	This can be your 169 network. Since this does not have its own DNS or Gateway, you can enter any numbers for DNS and set the netmask to 255.255.255.0
1 NIC	**Internet (NIC 1)**	Network that the Tenant is on

Note: If NIC 2 is present, then the administration server (port 9443) that provides the REST APIs will only listen on that NIC. This server is accessed by the "apsetup.sh" script used in Step 5 below. If NIC 2 is not present, then that administration server listens on all of the interfaces.

3. In the vSphere web client, follow the normal method for deploying a template. In the "Customize template" step, enter information as shown below.

   Note: The fields below may not all appear, depending on your configuration, and may also appear in a different order than that shown below.

Heading	Field	Value
Networking Properties	External IP Address	Enter the physical IP address of NIC 1. **Note: If user access is via a NAT address, do <u>not</u> enter that address here.**
	DNS server addresses	Enter IP of the DNS that the Access Point will use to resolve Hostnames.

	Management network IP Address	If configuration is 3 NIC or 2 NIC, enter Management Network IP from the previous step.
	Backend network IP Address	If configuration is 3 NIC, enter Backend Network IP from the previous step.
Password Options	Password for the root user of this VM	Enter initial password for root user.
	Password for the admin user, which enables REST API access	Enter password to be used for REST API Admin user.
System Properties	Locale to use for localized messages	en_us
	Syslog server URL	Leave blank
Horizon Properties	Horizon server URL	Leave blank
	Horizon server thumbprints	Leave blank

4. When you have finished the deployment process, power on the VM and wait for the login screen to appear on the console.
5. On the tenant appliance, run the following command:

   ```
   sudo /usr/local/desktone/scripts/apsetup.sh
   ```

6. Enter the requested information for the Access Point appliance:

Prompt	**Value**
Admin Password:	Password for the admin user of the Access Point.
Management IP:	This is the same address you entered above for Management network IP Address.
External IP:	The IP address for NIC 1 or the NAT IP address of NIC 1.
External Hostname [*xx.xx.xx.xx*]:	[Default hostname in brackets]
External PCoIP Port [4172]:	Default PCoIP Port shown in brackets: [4172]
External HTML Access Port [8443]:	Default HTML Access Port in brackets: [8443]
External Tunnel Port [443]:	Default Tunnel Port in brackets: [443]

7. The response status returned will indicate whether the configuration was successful.

Response status	Result
200	Configuration successful
400	Invalid input
401	Password incorrect. Confirm that password matches admin password configured during OVA deployment.
000	One of the following: • Network connection failure. Confirm that IP address matches management IP address configured during OVA deployment. • REST API password does not meet password criteria.

8. If dtRAM was in use on this environment previously, set the **element.allocator.ram.use** policy to false and remove the associated NAT and firewall rules.

9. Configure NAT and firewall rules to allow access to the Access Point appliance through Internet network.

   Note: When using an edge gateway load balancer the NAT for ports 80 and 443 are not required. These ports are forwarded automatically.

Port	Usage
4172/tcp, 4172/udp	PCoIP desktop access protocol
8443/tcp	HTML desktop access protocol
443/tcp	Secure web portal access
80/tcp	Insecure web portal access (will be redirected to 443)

Appendix A – Example of Load Balancer Configuration

Note: The following is an example of the process for configuring a load balancer. The settings you use will be different.

1. Choose an external IP to use for NAT (for example, 1.2.3.4).
2. Choose three external ports per Access Point for NAT (for example, [41721, 8443, 4431], [41722, 8444, 4432]).
3. Log in to the vCloud Director interface as an Organization Administrator.
4. Navigate to Edge Gateway Services:
   a. Click Administration in the top menu.
   b. Click Virtual Datacenters in the Administration pane to the left.
   c. Click the Virtual Datacenter name in the pane on the right.
   d. The pane on the right has a row of tabs along the top. Click the Edge Gateways tab.
   e. In the list of Edge Gateways, click one to select it.
   f. Right-click the Edge Gateway and click Edge Gateway Services.
5. Configure DNAT:
   a. On the Edge Gateway Services page, click the NAT tab.
   b. Configure as shown below.

Applied On	Type	Original IP	Original Port	Translated IP	Translated Port	Protocol
external	DNAT	1.2.3.4	41721	192.168.0.10	4172	TCP & UDP
external	DNAT	1.2.3.4	8443	192.168.0.10	8443	TCP
external	DNAT	1.2.3.4	4431	192.168.0.10	443	TCP
external	DNAT	1.2.3.4	41722	192.168.0.11	4172	TCP & UDP
external	DNAT	1.2.3.4	8444	192.168.0.11	8443	TCP
external	DNAT	1.2.3.4	4432	192.168.0.11	443	TCP

6. Configure Firewall:
   a. On the Edge Gateway Services page, click the Firewall tab.
   b. Configure as shown below.

Name	Source	Destination	Protocol	Action
ap1-pcoip	any:any	1.2.3.4:41721	TCP & UDP	Allow
ap1-blast	any:any	1.2.3.4:8443	TCP	Allow
ap1-tunnel	any:any	1.2.3.4:4431	TCP	Allow
ap2-pcoip	any:any	1.2.3.4:41722	TCP & UDP	Allow
ap2-blast	any:any	1.2.3.4:8444	TCP	Allow
ap2-tunnel	any:any	1.2.3.4:4432	TCP	Allow

7. Configure load balancer pool servers:
    a. On the Load Balancer tab, click **Pool Servers** and click **Add**.
    b. On the Name & Description tab, type a name and optionally a description for the pool server.
    c. Click **Next**.
    d. On the Configure Service tab:
        - Click **Enable** for HTTP and HTTPS services.
        - Select IP Hash for the balancing method for both services.
        - For default ports, enter the following:
            - HTTP – Port 80
            - HTTPS – Port 443
    e. Click **Next**.
    f. On the Configure Health-Check tab:
        - For HTTP and HTTPS, enter Monitor Ports.
        - For HTTPS, change Mode to TCP.
        - In the **URI for HTTP service** field, enter **/favicon.ico**
    g. Click **Next**.
    h. On the Manage Members tab, add each Access point as a member, described below.
        1) Click **Add**.
        2) In the Add Member dialog:
            - Enter the IP address of the Internet AP interface, as defined when you deployed the OVA.
            - For both HTTP and HTTPS, enter 80 for Port and 443 for Monitor Port.
        3) Click **OK**.
8. Configure load balancer virtual server:
    a. On the Load Balancer tab, click **Virtual Servers** and **click Add**.
    b. Enter a name and description for the virtual server.
    c. Select an external network from the Applied on drop-down menu.
    d. Enter the external IP address of the virtual server.
    e. From the drop-down menu, select the pool you created earlier.
    f. In Services, select **Enable** for HTTP and HTTPS.
    g. For Persistence Method, enter **No persistence** for HTTP and HTTPS.
    h. Click **Enabled** to enable the virtual server.
    i. Click **OK**.