Horizon Air 15.3.2 DaaS Agent Installation and Upgrade

July 2015

Revision History

Date	Version	Description
07/21/2015	1.0	Initial release

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

Overview

This document describes the process for Horizon Air customers to install VMware DaaS Agent 15.3.2. It is required that all tenants be running DaaS platform 15.3.2 before you begin the process described below.

- If you are performing a fresh install of DaaS Platform 15.3.2, use the instructions below under New Install to perform the DaaS Agent installation.
- If you are upgrading to DaaS Platform 15.3.2, follow the instructions below under Upgrade.

Note: Once the tenant appliances are upgraded to DaaS platform 15.3.2, the DaaS 15.3.2 agent is required in order to create new RDSH Remote Application Pools in the Horizon Air administration console.

New Install

Install the DaaS Agent using one of the methods described below.

Install Manually

1. Download the **DaaSAgent_15.3.2.msi** file.

   Note: This version of the DaaS Agent file is only compatible with DaaS platform version 15.3.2.

2. Install DaaS Agent by copying the file onto your VM and running the install.
3. On any VM where the SSL certificate is not already installed, do the following.

   a. Log in to the Enterprise Center and select pool management ► patterns.

   b. On the Pattern Management page, select Download the Horizon DaaS SSL certificate.

   c. Save the cacert.pem file to the DaaS agent's cert directory (typically C:\Program Files (x86)\VMware\VMware DaaS Agent\cert). This file contains the public certificate of the DaaS internal Certificate Authority.

   Note the following:

   - Existing desktop VMs that are running a previous version of the DaaS Agent will continue to function without any changes. However, to ensure secure communication, the agent should be updated to the current version as soon as possible.
   - Once the agent is updated on any existing desktop VMs, the cacert.pem file must be placed on those VMs in the cert directory.
   - It is not necessary to back up the cacert.pem file on the DaaS agent system. The cacert.pem file is contained on the service provider and tenant appliances and will be backed up as part of the service provider appliance backups. If the cacert.pem file is lost from the agent system it can be downloaded again from the Enterprise Center.

   For troubleshooting information regarding this download, see the Enterprise Center help.

4. The DaaS Agent must be configured to point at the tenant appliances. This can be done 1 of 2 ways:

   ○ DaaS Agent Discovery: The tenant appliance addresses can be automatically discovered by the DaaS Agent via DHCP by utilizing option code 74. For more information, see instructions in the Configure Tenant Discovery for DaaS Agent section below.

   ○ Update of DaaS Agent configuration file: The tenant appliance addresses can be manually updated in the DaaS Agent configuration file. Open the file C:\Program Files (x86)\DaaS Agent\service\MonitorAgent.ini with a text editor like notepad (note: on 32-bit systems the path will be exclude the "(x86)"). Remove the semi-colon on the line containing the parameter `standby_address` and provide a comma separated list of the tenant appliance IP addresses. A restart of the DaaS Agent Windows service is required after making this change.

Install Via GPO Policy

To install the DaaS Agent on all VMs for all Tenants, you typically use a domain controller with a GPO policy.

See http://support.microsoft.com/kb/816102 for a detailed reference.

Note the following:

- If the SSL Certificate is not already installed, it must be installed on all VMs when the DaaS Agent is installed. This can also be done by GPO policy.
- The DaaS Agent upgrade process does not persist the monitoragent.ini settings. If you are not using DHCP tenant address discovery, then you must update the agent configuration in the monitoragent.ini file via GPO policy as well.

Upgrade

Once the tenant appliances are upgraded to DaaS 15.3.2, DaaS Agent 15.3.2 is required in order to create new RDSH Remote Application Pools in the Horizon Air Console.

When the Tenant appliances have been upgraded, update the DaaS Agent using one of the methods described below.

Update Via GPO Policy

To update the DaaS Agent on all VMs for all upgraded Tenants, you typically use a domain controller with a GPO policy.

See http://support.microsoft.com/kb/816102 for a detailed reference.

Note the following:

- If the SSL Certificate is not already installed, it must be installed on all VMs when the DaaS Agent is updated. This can also be done by GPO policy.
- The DaaS Agent upgrade process does not persist the monitoragent.ini settings. If you are not using DHCP tenant address discovery, then you must update the agent configuration in the monitoragent.ini file via GPO policy as well.

Update Manually

1. Download the **DaaSAgent_15.3.2.msi** file.

   Note: This version of the DaaS Agent file is only compatible with DaaS platform version 15.3.2.

2. Install DaaS Agent by copying the file onto your VM and running the install.
3. Confirm that tenant discovery has been configured. If it has not, this can be done 1 of 2 ways:
   - **DaaS Agent Discovery (recommended):** The tenant appliance addresses can be automatically discovered by the DaaS Agent via DHCP by utilizing option code 74. For more information, see instructions in the Configure Tenant Discovery for DaaS Agent section below.
   - **Update of DaaS Agent configuration file:** The tenant appliance addresses can be manually updated in the DaaS Agent configuration file. Open the file C:\Program Files (x86)\DaaS Agent\service\MonitorAgent.ini with a text editor like notepad (note: on 32-bit systems the path will be exclude the "(x86)"). Remove the semi-colon on the line containing the parameter `standby_address` and provide a comma separated list of the tenant appliance IP addresses. A restart of the DaaS Agent Windows service is required after making this change.

Configure Tenant Discovery for DaaS Agent

A DHCP helper/relay is required to deliver the DHCP requests over the VPN tunnel to the tenant network. This can be done directly on the switches to which the hosts are attached; if this is not possible, a small Linux appliance can be configured in the tenant to perform this function.

- Configure the DHCP scope for the desktop subnet, starting at x.x.x.30.
- Configure DHCP option code 74 (IRC Chat) to point to the two IPs allocated for the tenant appliances. For example, if you are using a Windows server to provide DHCP service:
    1) Open the DHCP configuration client from Control Panel > Administrative Tools.
    2) Right-click Server Options and select **Configure Options** from the pop-up menu.
    3) If you have defined limited address scopes, you can confine the options configuration to a particular scope. Click on the scope and right-click on **Scope Options** to configure the 074 option code for that scope only. Configuration is the same as for the whole DHCP server.
    4) Scroll down to the 074 option for Internet Relay Chat (IRC) and check the box.
    5) Add IP addresses for tenant appliances.