Technical white paper

HPDM & Microsoft Azure Cloud Deployment Guide

HP Device Manager 4.7 SP3

Table of contents

Overview

HP Device Manager (HPDM) is a device management tool capable of working in many different complicated environments. If you configure your firewall, you can deploy HPDM in a cloud and use it to manage HP devices. This document covers deploying HPDM in Microsoft® Azure.

Note:
Make sure your Azure account has the necessary privileges, and that you have created your Azure workspace before deploying HPDM. For more information of creating an Azure account, contact Microsoft.

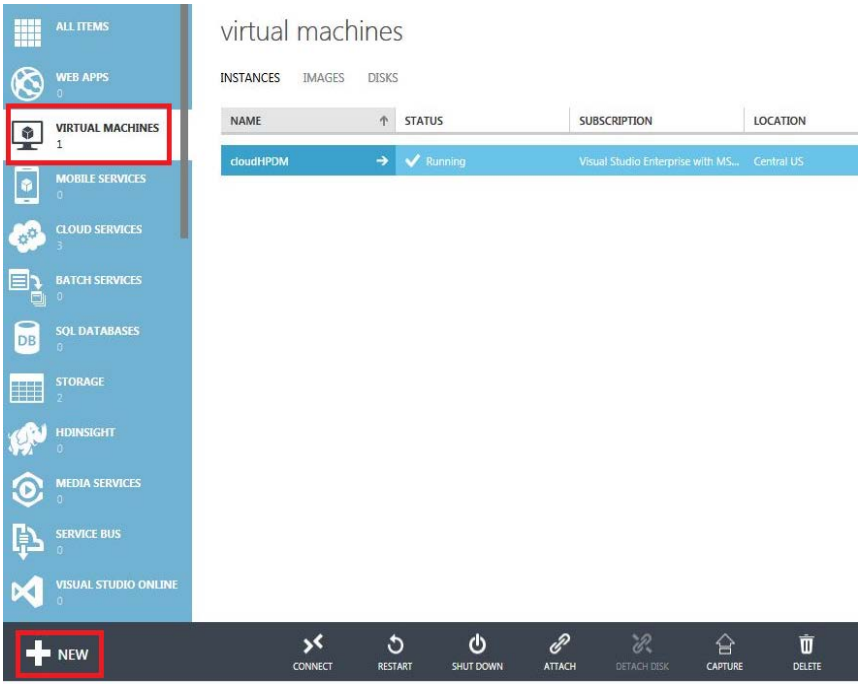
Deploying HPDM on Azure

To deploy HPDM in Azure and manage HP devices:

1. Create virtual machines in your Azure workspace.
2. Install HPDM.
3. Configure the firewall.

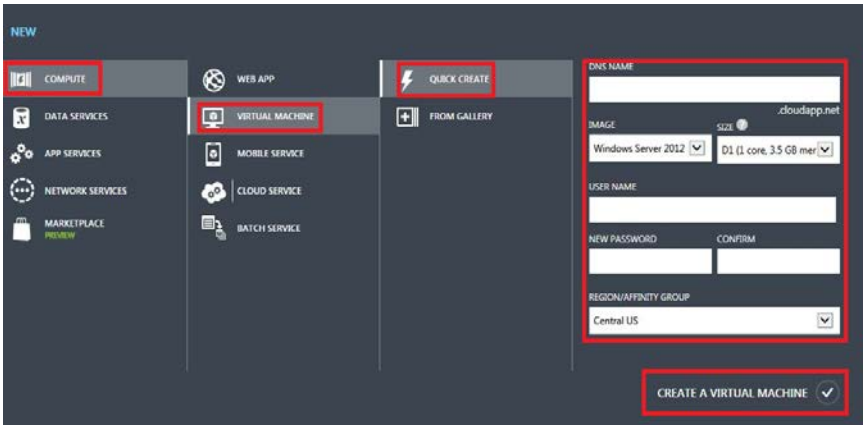
Creating virtual machines in your Azure workspace

1. Go to https://manage.windowsazure.com and log on using your Azure account.
2. In the VIRTUAL MACHINES tab, select **NEW**.

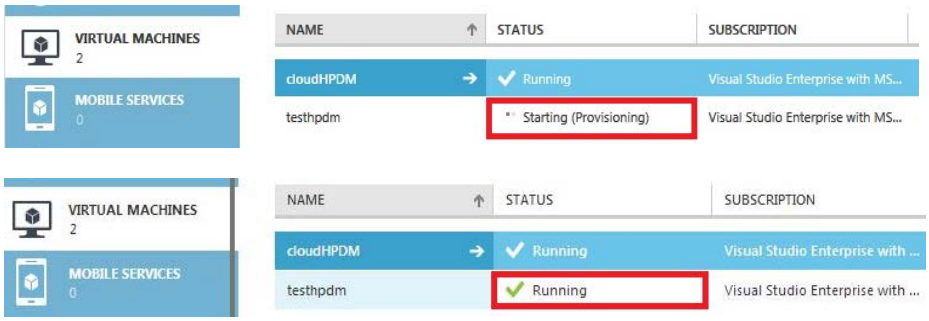


3. Select **COMPUTE**, select **VIRTUAL MACHINE**, select **QUICK CREATE**, and then enter your information in the resulting boxes.

4. Select **CREATE A VIRTUAL MACHINE**.

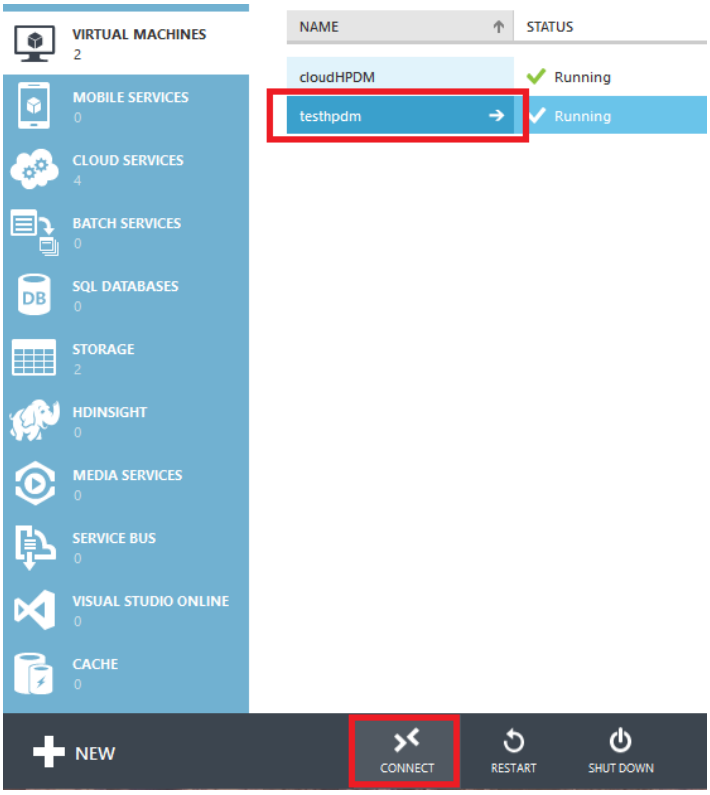


When the virtual machine status changes from Starting (Provisioning) to Running, you can install HPDM.



Installing HPDM and HPDM Embedded HTTPS server

1. Select the virtual machine you created in Creating virtual machines in your Azure workspace, and then select **CONNECT**.



2. Save the RDP file your local system, and then use it to connect.
3. Upload the HPDM package to the virtual machine, and then install it. For instructions on installing HPDM, see the HP Device Manager 4.7 white paper *Installation and Update*.

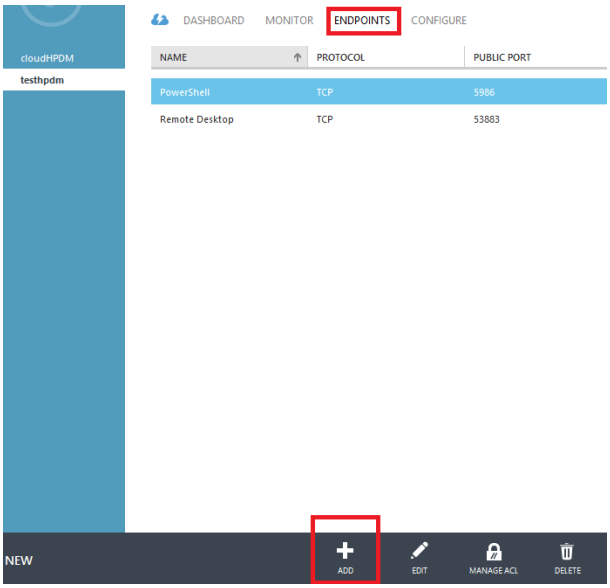
4. Optionally, upload the installation package of HPDM Embedded HTTPS Server to the virtual machine, and then install it. For instructions on installing HTTPS server, see the HP Device Manager 4.7 white paper *HPDM Embedded HTTPS Server Deployment Guide*.

Configuring the firewall rules

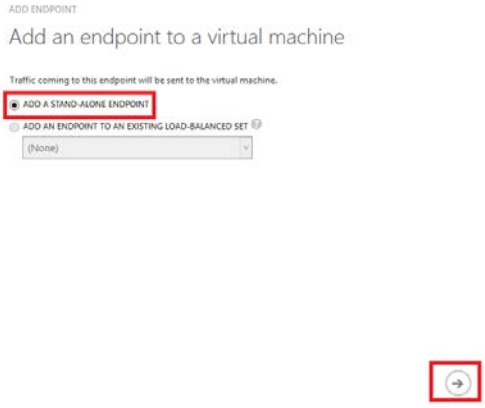
By default, a virtual machine created in Azure is protected by the endpoint firewall. You must map the ports corresponding to HPDM to manage your device over the Internet.

To add a port to your firewall:

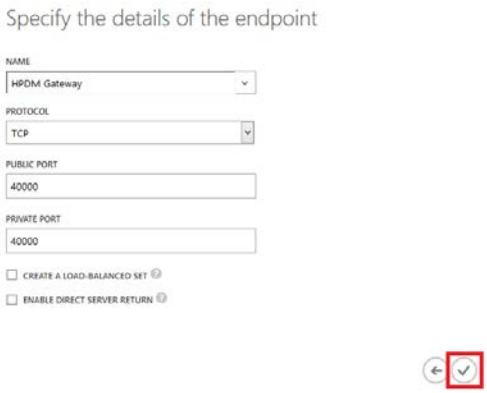
1. Select a virtual machine with HPDM installed to open the virtual machine properties page.
2. In the ENDPOINTS tab, select **ADD**.



A. In the dialog that appears, select **ADD A STAND-ALONE ENDPOINT**, and then click the right arrow in the lower right-hand corner.



B. Select the **NAME** of your HPDM component, select the **PROTOCOL** it uses, and then enter the **PUBLIC PORT** and the **PRIVATE PORT** that it uses.



C. Select the checkmark.

Repeat this procedure for every port that HPDM uses in your production environment. For more information about which ports HPDM uses, see the HP Device Manager 4.7 white paper *Deployment Guide*.

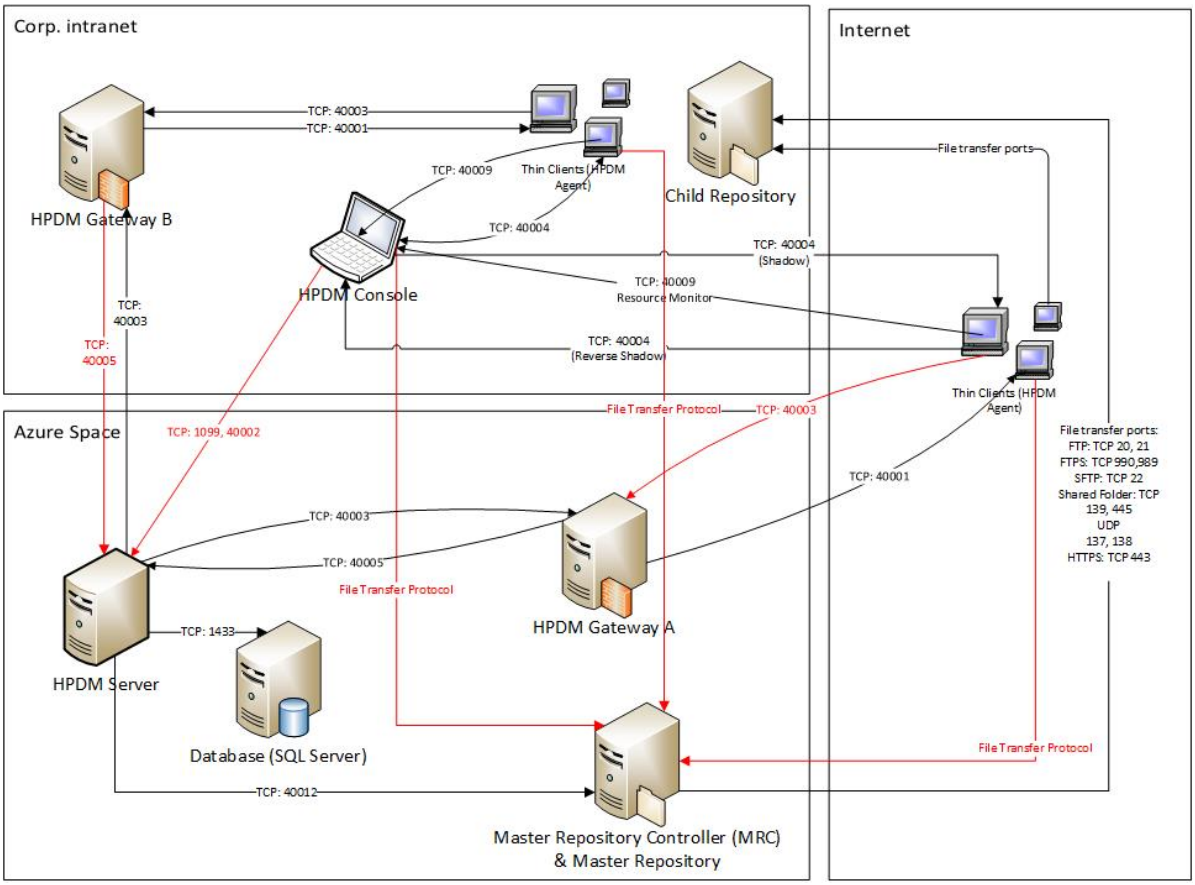
Sample scenario

Production environments are complex, diversified, and flexible. Use the following example to better understand port configuration in the cloud. This is a typical model with detailed configurations for reference.

Note

There might be firewalls between Internet/Intranet and Azure. Make sure that you have completed the procedure in Configuring the firewall rules to allow communication between your devices and the cloud.

Figure 1. Typical topography



All ports in red in Figure 1 must be added to the endpoint firewall.

Table 1. Enpoints rule in Azure

Name	Protocol	Public Port	Private Port
HPDM Gateway B to HPDM Server	TCP	40005	40005
HPDM Console to HPDM Server	TCP	1099	1099
HPDM Console to HPDM Server	TCP	40002	40002
HPDM Agent to Master Repository Controller	TCP/UDP	File Transfer Port	File Transfer Port
HPDM Console to Master Repository Controller	TCP/UDP	File Transfer Port	File Transfer Port
HPDM Agent to HPDM Gateway A	TCP	40003	40003

For more information

To read more about HP Device Manager, go to hp.com/go/hpdm.

Sign up for updates
hp.com/go/getupdated

Second Edition: August 2016

First Edition: October 2015