

Microsoft Dynamics® GP

Microsoft Dynamics GP 2013 on Windows Azure

White Paper

A guide to planning, deploying and managing Microsoft Dynamics GP 2013 on Windows Azure Infrastructure Services.

Date: December 2013

C:\Users\jmikkels\Pictures\prev_MS_rgb_Dynamics_Blk.jpg

Table of Contents

[Introduction 4](#_Toc363816075)

[Checklist 4](#_Toc363816076)

[What’s in this guide 5](#_Toc363816077)

[Part 1: Windows Azure Account 6](#_Toc363816078)

[Sign up for a Windows Azure Account 6](#_Toc363816079)

[Create a Subscription 8](#_Toc363816080)

[Sign up for a Windows Azure Support Plan 8](#_Toc363816081)

[Part 2: Planning 10](#_Toc363816082)

[Licensing 10](#_Toc363816083)

[Microsoft License Mobility through Software Assurance 10](#_Toc363816084)

[Microsoft Dynamics GP 2013 11](#_Toc363816085)

[Remote Desktop Services (RDS) 11](#_Toc363816086)

[Microsoft SQL Server 11](#_Toc363816087)

[Other Licensing Considerations – Windows Azure Billing / Cost Allocation 11](#_Toc363816088)

[Legal 12](#_Toc363816089)

[Security 12](#_Toc363816090)

[Privacy 12](#_Toc363816091)

[Compliance 12](#_Toc363816092)

[Microsoft Dynamics GP Components 13](#_Toc363816093)

[Deployment Models 14](#_Toc363816094)

[Extend Corporate Network 14](#_Toc363816095)

[Dedicated Private Virtual Network 15](#_Toc363816096)

[System Requirements 15](#_Toc363816097)

[High Availability and Disaster Recovery (HADR) 17](#_Toc363816098)

[Availability Set 17](#_Toc363816099)

[SQL Server HADR 18](#_Toc363816100)

[Redundant Storage 18](#_Toc363816101)

[Host O/S Maintenance 18](#_Toc363816102)

[Part 3: Deploy Microsoft Dynamics GP 19](#_Toc363816103)

[Creating an Affinity Group 19](#_Toc363816104)

[Creating a Virtual Network 20](#_Toc363816105)

[Creating Virtual Machines 20](#_Toc363816106)

[Configuring Active Directory 22](#_Toc363816107)

[Configuring Microsoft SQL Server 23](#_Toc363816108)

[Installing Microsoft Dynamics GP Desktop Client and Creating Databases 26](#_Toc363816109)

[Configuring Microsoft SQL Server Reporting Services 27](#_Toc363816110)

[Configuring the Tenant Services Server 28](#_Toc363816111)

[Configuring the Web Client Web Server 29](#_Toc363816112)

[Configuring the Web Client Session Host Server 29](#_Toc363816113)

[Configuring Remote Desktop Services 30](#_Toc363816114)

[Configuring SharePoint Server 36](#_Toc363816115)

[Configuring a Management Reporter Server 37](#_Toc363816116)

[Part 4: Maintenance 38](#_Toc363816117)

[Database Maintenance and Backups 38](#_Toc363816118)

[Data Disk 38](#_Toc363816119)

[Backup Directly to Blob Storage 38](#_Toc363816120)

[Managing Virtual Machines 39](#_Toc363816121)

[Updating Microsoft Dynamics GP 40](#_Toc363816122)

[Part 5: Troubleshooting and Technical Support 41](#_Toc363816123)

[Troubleshooting 41](#_Toc363816124)

[Contacting Billing and Technical Support 42](#_Toc363816125)

[Windows Azure 42](#_Toc363816126)

[Microsoft Dynamics GP 43](#_Toc363816127)

# Introduction

This guide provides information for deploying Microsoft Dynamics GP 2013 on Windows Azure Infrastructure Services (WAIS). WAIS provides the infrastructure you need to provide customers with dependable, secure ERP deployments in the cloud, backed by Microsoft for a full-stack offering.

Flexibility and familiarity make WAIS an ideal platform for Microsoft Dynamics GP 2013. Microsoft Dynamics GP 2013 for deploying in the cloud is exactly the same one that you are used to selling and deploying every day. Since WAIS is a Virtual Machine environment, the process of deploying and managing Microsoft Dynamics GP on WAIS should be very familiar to you already. Your knowledge and previous experience deploying Microsoft Dynamics GP on-premise or as a hosted service will be beneficial when deploying on WAIS. You have flexibility with respect to the license model you choose to package with your Windows Azure offering to customers. And because the product is constant, customers can be reassured that they can move off of (or onto) the cloud seamlessly.

The following WAIS features are used as building blocks when you create a Microsoft Dynamics GP environment.

1. Virtual Machines – The virtual machines are the Windows Servers that host the Microsoft Dynamics GP components and other pre-requisite software.
2. Virtual Network – A virtual network provides a network in the cloud for cross-machine communication.
3. Storage Account – A storage account stores the data disks and the virtual machine VHD files.
4. Affinity Group – An affinity group keeps the storage accounts and virtual machines in the same cluster of the data center for optimal performance.

How you will configure the WAIS features will be based on the needs of the Microsoft Dynamics GP deployment. For example, how many virtual machines are required, the network configuration for cross-machine communication, and disk configuration for storing data must be configured in Windows Azure to support the Microsoft Dynamics GP installation. After the Windows Azure environment is set up and configured, the Microsoft Dynamics GP components and required pre-requisite software can be installed on the virtual machines in much the same way as they would be on virtual machines in on-premise or hosted environments.

## Checklist

The following checklist provides an overview of the steps for deploying Microsoft Dynamics GP on Windows Azure.

|  |  |
| --- | --- |
| Step | For more information, see… |
| Sign up for a Windows Azure account | [Sign up for a Windows Azure Account](#_Chapter_1:_Sign) <https://account.windowsazure.com/Home/Index> |
| Create subscription | [Create a Subscription](#_Create_a_Subscription) |
| Determine deployment configuration | [Deployment Models](#_Deployment_Models) |
| Create Affinity Group | [Creating an Affinity Group](#_Chapter_1:_Create)  <http://msdn.microsoft.com/en-us/library/windowsazure/hh531560.aspx> |
| Create Virtual Network | [Creating a Virtual Network](#_Chapter_2:_Create_1)  <http://msdn.microsoft.com/en-us/library/windowsazure/jj156007.aspx> |
| Create Virtual Machines | [Creating Virtual Machines](#_Chapter_3:_Create)  <http://www.windowsazure.com/en-us/manage/windows/tutorials/virtual-machine-from-gallery/> |
| Deploy Microsoft Dynamics GP | [Part 3, Deploy Microsoft Dynamics GP](#_Part_3:_Deploy) |
| Create backup and scheduled maintenance procedures | [Database Maintenance and Backups](#_Chapter_1:_Database) |
| Maintain virtual machines | [Managing Virtual Machines](#_Chapter_2:_Virtual) |
| Update Microsoft Dynamics GP | [Updating Dynamics GP](#_Chapter_3:_Updating) |

## 

## What’s in this guide

This document provides guidelines for deploying Microsoft Dynamics GP on Windows Azure. Microsoft Dynamics GP on Windows Azure assumes that the Microsoft Dynamics GP 2013 product is being used. The information contained in this guide is intended to be used along with the main product documentation for Microsoft Dynamics GP 2013. The guide is divided into the following parts:

* [Part 1, Windows Azure Account](#_Part_1:_Windows) contains information on signing up for a Windows Azure Account and creating a subscription.
* [Part 2, Planning](#_Part_2:_Planning_1) contains information on planning your deployment, including licensing, common deployment configurations, and server sizing.
* [Part 3, Deploy Microsoft Dynamics GP](#_Part_3:_Deploy) describes how to set up the Windows Azure services for Microsoft Dynamics GP and install Microsoft Dynamics GP on the Windows Azure services.
* [Part 4, Maintenance](#_Part_4:_Maintenance) contains information about maintaining the Microsoft Dynamics GP deployment, including upgrading to the newest releases.
* [Part 5, Troubleshooting and Technical Support](#_Part_5:_Troubleshooting_1) contains information on troubleshooting and getting technical support for issues with Microsoft Dynamics GP on Windows Azure.

# Part 1: Windows Azure Account

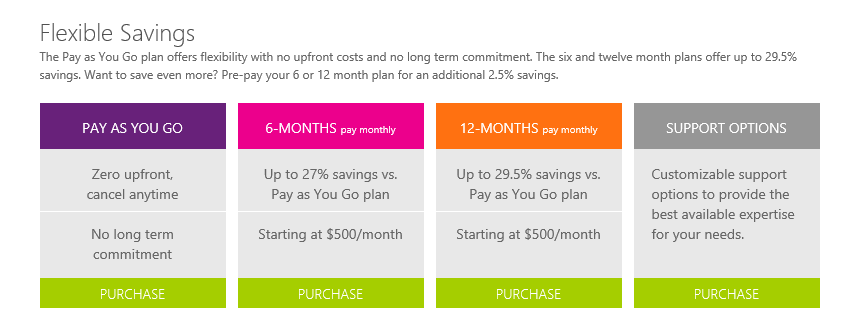
This part contains information about signing up for a Windows Azure Account and creating a subscription. It contains the following sections:

* [Sign up for a Windows Azure Account](#_Chapter_1:_Sign) provides directions for signing up for a Windows Azure Account.
* [Create a Subscription](#_Create_a_Subscription) provides directions for creating one or more subscriptions for the Windows Azure Account.
* [Sign up for a Windows Azure Support Plan](#_Part_2:_Planning) provides information for signing up for a Windows Azure support plan.

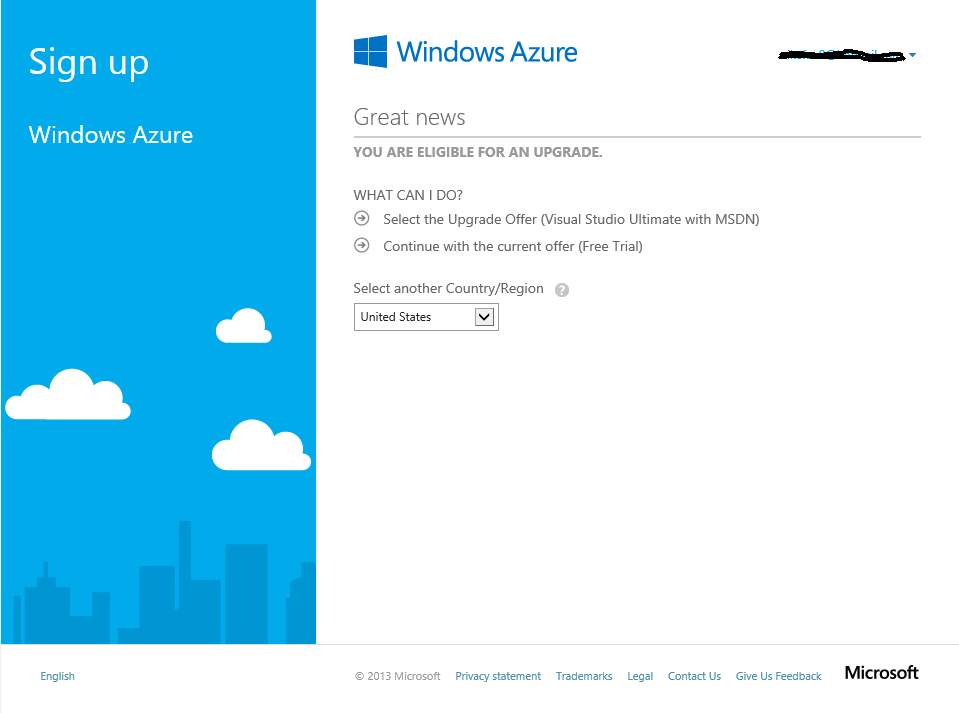
## Sign up for a Windows Azure Account

You will need to sign up for a Windows Azure Account before creating any of the service components. Use these steps to create a Windows Azure Account.

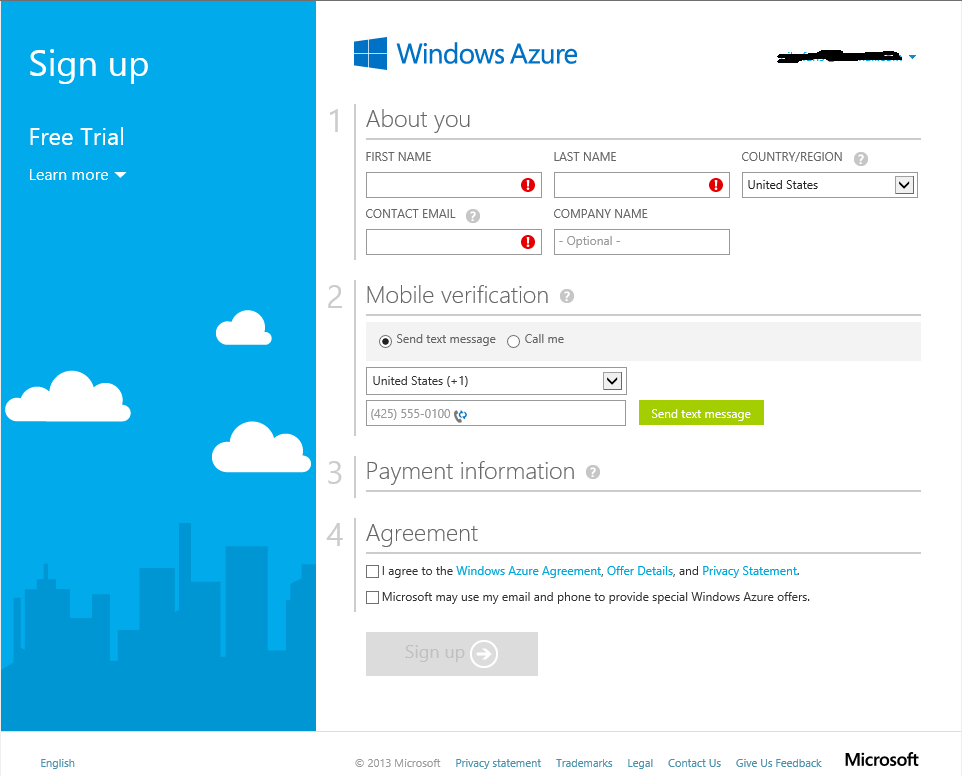
1. Go to <http://www.windowsazure.com/en-us/pricing/free-trial/>
2. Choose to create a new account using either the free trial or purchase option. If you select the purchase option, you will have the option of selecting from a 6 or 12 month commitment plan or a Pay-as-You-Go plan.



1. Log in using the Microsoft Account that will be the owner of the Windows Azure account. Sign up for a Microsoft Account if needed.
2. Assuming that the Microsoft Account is not already the owner of a Windows Azure account, a wizard window will open and walk you through the process of setting up a new account.
3. The first window will display information about creating a Windows Azure account. The information will be specific to the type of account being created. Select your country/region from the drop-down and click the arrow to continue.



1. Verify or provide the information about you.
2. Provide a telephone number to verify your account. You can select to have a text message sent or receive a telephone call.
3. Provide the credit card that will be billed on a monthly basis, the billing address information and the account information. Click **Next** to continue. The account is created at this point.



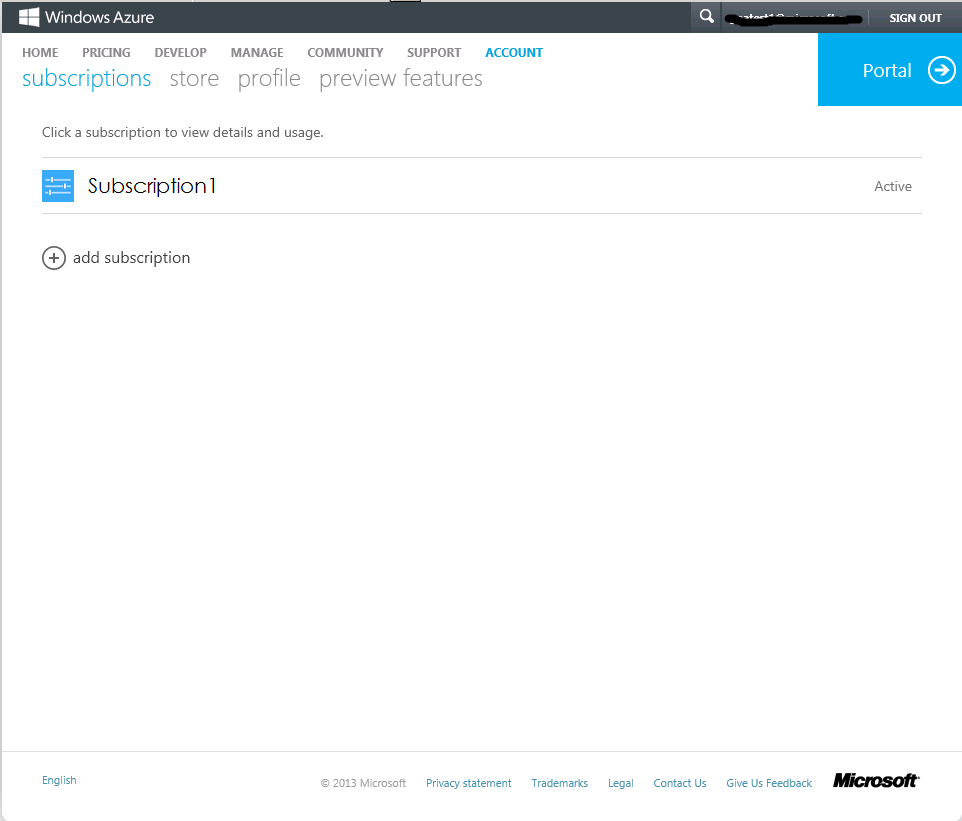
1. After the account is created, the Account home page is displayed. Select Account Center to create a subscription and manage your account. Select Management Portal to manage your Windows Azure services and applications.

## Create a Subscription

You will create one or more subscriptions for the Windows Azure account. A subscription is a grouping of Windows Azure services and applications, including the virtual machines discussed earlier. The subscription provides a way to control the access to and the use of the Windows Azure subscribed service. On the account billing, the resource usage of Windows Azure services for each subscription is reported separately. In a situation where you will have multiple Microsoft Dynamics GP deployments, you may decide to use a separate subscription for each deployment in order to track expenses related to each deployment. All of the Microsoft Dynamics GP components for a single deployment need to be deployed to the same subscription however. You can set up different administrators for each subscription as required. See [Overview of Subscription Management](http://msdn.microsoft.com/en-us/library/windowsazure/hh531793.aspx)[[1]](#footnote-1) for additional information.

Use the following steps to create a subscription.

1. Sign in to the [Azure account management portal](https://account.windowsazure.com/Home/Index)[[2]](#footnote-2).
2. Click Account Center to manage the account.
3. Click to add a subscription.



1. Click a subscription offer from the available list to create the subscription.

Note: You can rename the subscription after it has been created.

## Sign up for a Windows Azure Support Plan

Windows Azure support plans provide technical and billing support for Windows Azure. The Windows Azure support plans offer flexible support options that will allow you to select the right level of support for your Windows Azure deployment. The support options range from support services included with your Windows Azure Account at no charge to Premier support services offered under Cloud Vantage Services. Information on the available support plans and purchasing a plan can be found on the [Windows Azure Support](http://www.windowsazure.com/en-us/support/plans/)[[3]](#footnote-3) page. Technical and billing support for Microsoft Dynamics GP will continue to be offered using the existing programs. Refer to the [Microsoft Dynamics GP](#_Microsoft_Dynamics_GP_1) support section in Part 5 of this document for additional information.

# Part 2: Planning

Planning your Windows Azure deployment of Microsoft Dynamics GP includes making decisions about which Microsoft Dynamics GP components to deploy, what configuration to use, and what the system requirements are for those components. These are decisions that must be made in all Microsoft Dynamics GP deployments. This part of the document covers the special considerations that impact these decisions when deploying on Windows Azure. This part contains the following sections.

* [Licensing](#_Licensing) provides information on licensing Microsoft Dynamics GP and the required software on Windows Azure.
* [Legal](#_Licensing) provides information on protecting Customer data deployed on Windows Azure.
* [Microsoft Dynamics GP Components](#_Microsoft_Dynamics_GP) provides information about the Microsoft Dynamics GP components that can be deployed on Windows Azure.
* [Deployment Models](#_Deployment_Models) describes the two common configurations that are used when deploying Microsoft Dynamics GP on Windows Azure.
* [System Requirements](#_Chapter_2:_System) provides sizing recommendations for the virtual machine instance sizes that are available in Windows Azure.
* [High Availability and Disaster Recovery (HADR)](#_High_Availability_and) provides information on setting up the Windows Azure environment for high availability and disaster recovery.

## Licensing

Licensing the various components of the Microsoft Dynamics GP 2013 solution is an important consideration in all deployment types. For deployments on Windows Azure, you will want to evaluate the special licensing terms specific to Windows Azure and the impact that these decisions have on the overall cost of providing the hosted solution.

All Microsoft software installed in the Windows Azure Virtual Machine environment must be properly licensed. Windows Azure Virtual Machines include by default a license for use of Windows Server in the Windows Azure environment. Certain Windows Azure Virtual Machine offerings may also include additional Microsoft software on a per-hour or evaluation basis. [Click here](http://www.windowsazure.com/en-us/pricing/licensing-faq/)[[4]](#footnote-4) to view additional common FAQs regarding licensing on Windows Azure Virtual Machines.

### Microsoft License Mobility through Software Assurance

License Mobility through Software Assurance gives Microsoft Volume Licensing customers the flexibility to deploy eligible server applications with active Software Assurance on Windows Azure. With this Software Assurance benefit, there is no need to purchase new licenses and no associated mobility fees so, you can easily deploy existing licenses on the Windows Azure cloud platform.

With License Mobility through Software Assurance, you can:

* Deploy certain server application licenses purchased under your Volume Licensing agreement in Windows Azure data centers.
* Extend the value of your server application licenses by deploying them on-premises or in the cloud.
* Take advantage of the low cost computing infrastructure for changing business priorities.

More program benefit details and information can be found [here](http://www.windowsazure.com/en-us/pricing/license-mobility/)[[5]](#footnote-5).

For information about Microsoft’s License Mobility program see: <http://www.microsoft.com/licensing/software-assurance/license-mobility.aspx>

### Microsoft Dynamics GP 2013

Use the Microsoft Dynamics NAV 2013 and Microsoft Dynamics GP 2013 Pricing and Licensing page on Partner Source to learn more about the Perpetual Licensing and Service Provider License agreement (SPLA) licensing programs – both of which are supported for on-Azure deployments.

Consult the [Microsoft Dynamics NAV 2013 and Microsoft Dynamics GP 2013 Licensing Guide](https://mbs.microsoft.com/partnersource/pricing/announcements/MSDNAVGP2013LicensingGuide.htm)[[6]](#footnote-6) to improve your understanding of how to license Microsoft Dynamics GP 2013.

### Remote Desktop Services (RDS)

Remote Desktop Services (RDS) Subscriber Access Licenses (SALs) purchased through the Microsoft Service Provider Licensing Agreement (SPLA) may be used to deliver graphical user interface functionality for applications on Windows Azure virtual machines. RDS Client Access Licenses (CALs) purchased through other Volume Licensing programs including the Enterprise Agreement may not be used with Windows Azure virtual machines. To read more about licensing RDS with Windows Azure Virtual Machines, see: <http://www.windowsazure.com/en-us/pricing/licensing-faq/> and [Product Use Rights (PUR) document](http://www.microsoft.com/licensing/about-licensing/product-licensing.aspx)[[7]](#footnote-7).

### Microsoft SQL Server

There are three ways to license Microsoft SQL Server in Windows Azure Virtual Machines:

1. Install or upload your own SQL Server image using the license mobility benefits under Software Assurance.
2. Obtain the SQL Server image from the image gallery and pay the per-hour rate of SQL Server in Windows Azure Virtual Machines.
3. Hosted solution for SQL Server Standard Edition licensed as Subscriber Access Licenses (SAL) through SPLA.

Partners will want to carefully evaluate each of these options for Microsoft SQL Server as the cost models are very different. The deployment model you choose to employ and the number of users that will be supported are key factors in this decision.

### Other Licensing Considerations – Windows Azure Billing / Cost Allocation

For many Partners determining how to bill Customers for monthly, consumption-based charges from Windows Azure will represent a new challenge.

To learn what billing information is available, Partners should review the [Understand Your Bill for Windows Azure](http://www.windowsazure.com/en-us/support/understand-your-bill/)[[8]](#footnote-8) section on the Windows Azure Portal. These pages provide an overview of the Windows Azure billing process, links to sample invoices and a description of the daily usage data file that can be exported and analyzed.

Windows Azure billing is done monthly at the Account level. Charges for various services are grouped and reported at the Subscription level. To simplify the cost allocation exercised, Partners supporting multiple Customer deployments may wish to segregate each Customer’s services to individual subscriptions.

Note:

Please note that this whitepaper does not supersede or replace any of the legal documentation covering use rights for Microsoft products and does not constitute a commitment of licensing program availability.  For current product use rights and licensing program availability for products licensed through Volume Licensing (including SPLA), please refer to <http://www.microsoft.com/licensing/>. For current product use rights and licensing program availability for products licensed through Order Central, please refer to <https://mbs.microsoft.com/partnersource/pricing/>.

## Legal

Together with Microsoft, Partners must work together to protect Customer data and provide guidance to Customers when it comes to security, privacy, and compliance practices.

Microsoft runs Windows Azure services with common operational practices and features across multiple geographies and jurisdictions. However, it is ultimately up to Partners and Customers to determine if Microsoft services satisfy their regulatory needs.

To help provide Partners and Customers with up to date information the Windows Azure [Trust Center](http://www.windowsazure.com/en-us/support/trust-center/)[[9]](#footnote-9) provides detailed information on security, privacy, and compliance topics for Windows Azure customers.

### Security

This topic provides an overview of the provisions Microsoft is taking to provide a secure environment within geographically dispersed datacenters. Among the extensive list of Security-related resources, the [**Standard Response to Request for Information: Security and Privacy**](http://go.microsoft.com/fwlink/?linkid=293448&clcid=0x409)**[[10]](#footnote-10)** outlines how Windows Azure meets the suggested principals and mapped them to the International Standards Organization (ISO) 27001:2005 and ISO 27002. This standardized response empowers Partners and Customers with in-depth information to evaluate different offerings in the market place today.

### Privacy

Includes links to multiple resources that describe Privacy practices of the Windows Azure environment. It includes a link to the [Windows Azure Privacy Statement](http://go.microsoft.com/fwlink/p/?linkid=131004&clcid=0x409)[[11]](#footnote-11) an overview of privacy terms and a discussion of the location of Customer data, E.U. Data Protection Directive.

### Compliance

This topic provides resources to help Partners and Customers comply with the specific laws and regulations applicable to their unique industry and use scenario.

## Microsoft Dynamics GP Components

This section provides information about the Microsoft Dynamics GP components that can be deployed on Windows Azure. How you license Windows Server will determine how you deploy some of the Microsoft Dynamics GP components on Windows Azure. The Microsoft Dynamics GP components that require Remote Desktop Services (RDS) for end-user access over the Internet can be deployed on Windows Azure only if you are using a Subscriber Access License (SAL) purchased through the Microsoft Service Provider License Agreement (SPLA). You can use Remote Desktop for Administration to run these components for administrative purposes. User access to applications using remote desktop, will be limited to a maximum of 2 administrator users using Remote Desktop for Administration. Refer to the following list for component availability.

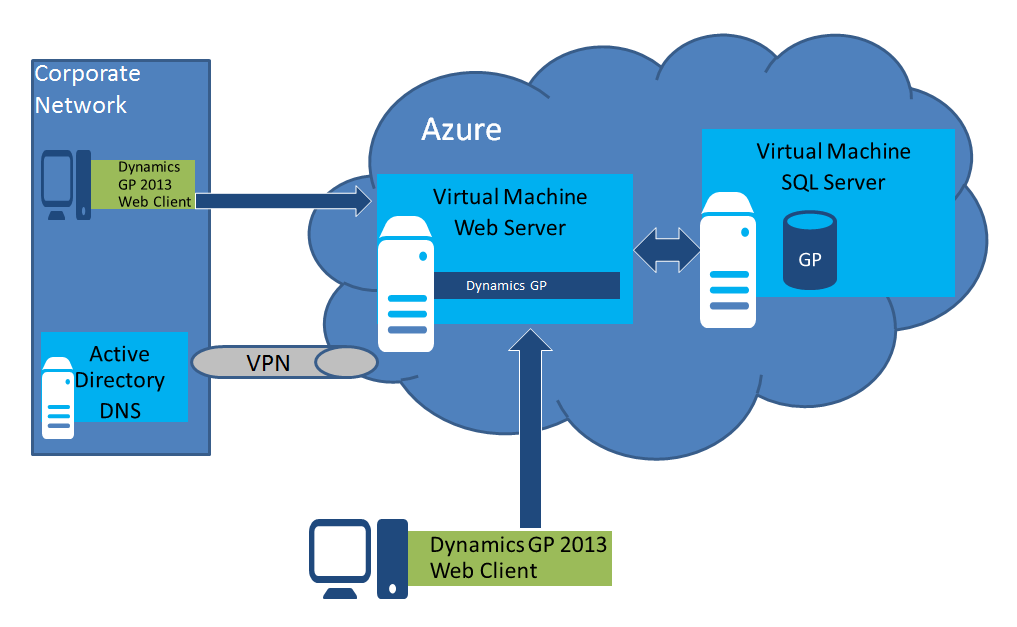
|  |  |
| --- | --- |
| Component | Availability |
| Microsoft Dynamics GP databases | Yes |
| Microsoft Dynamics GP client | Limited[[12]](#footnote-12) |
| Microsoft Dynamics GP web client | Yes |
| eConnect | Limited[[13]](#footnote-13) |
| Workflow | Yes |
| Business Portal | Yes |
| SQL Server Reporting Services Reports | Yes |
| Excel Reports | Limited[[14]](#footnote-14) |
| Integration Manager | Limited[[15]](#footnote-15) |
| Analysis Cubes | Limited[[16]](#footnote-16) |
| Management Reporter | Limited[[17]](#footnote-17) |
| FRx | No |
| ISV Solutions | Limited[[18]](#footnote-18) |

## Deployment Models

The deployment models for Microsoft Dynamics GP on Windows Azure are the same models available for on-premise and hosted environments. The models range from a single-machine deployment joined to your corporate network, to a scale out multitenant hosting deployment using a private virtual network in Windows Azure. The difference in these models on Windows Azure when comparing with an on-premise installation is the setup of the environment, (machines, network configuration, etc.). The machine configurations, like single-machine and scale-out, available for deploying Microsoft Dynamics GP on-premise are also available for deploying in Windows Azure. They can be used in both of the network configurations discussed below. In both of these network configuration models, all of the Microsoft Dynamics GP components, with the exception of some ISV products that integrate using Web Services for Microsoft Dynamics GP, are installed to one or more virtual machines in Windows Azure. For performance reasons you will want to avoid installing some of the Microsoft Dynamics GP components to your on-premise network and some to virtual machines in Windows Azure.

### Extend Corporate Network

This model allows you to extend your corporate network with a network of resources hosted in Windows Azure. In this model you create secure site-to-site connectivity between your on-premises network and a Windows Azure Virtual Network. The Windows Azure Virtual Network becomes an extension of your corporate network, with access to on-premise resources such as directory services and DNS (Domain Name System). The Microsoft Dynamics GP components are installed to virtual machines on the virtual network in Windows Azure. The quantity and configuration of these virtual machines is based on your deployment needs, much like deploying to computers on your corporate network. The following diagram shows a simple Microsoft Dynamics GP Web Client deployment on a Windows Azure Virtual Network connected to an on-premise network.

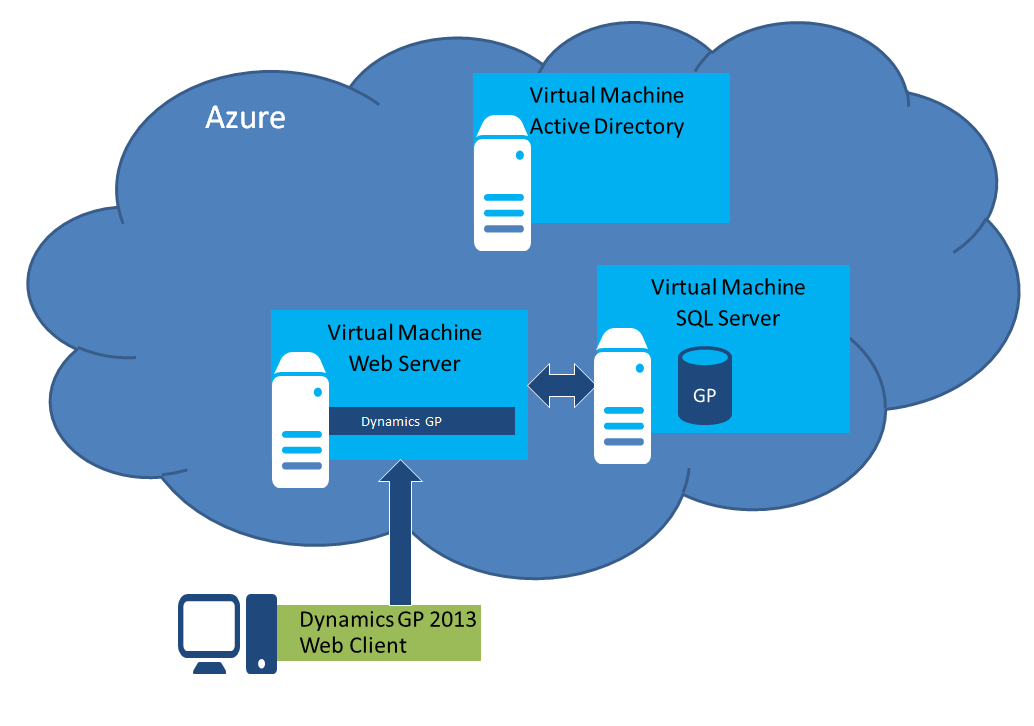


In this diagram the VPN (Virtual Private Network) represents the secure site-to-site connectivity between the Windows Azure Virtual Network and the corporate network. The virtual network is configured to use the DNS services on the corporate network for name resolution of the Windows Azure Virtual Machines. The Web Server and SQL Server virtual machines are joined to the corporate network domain for directory services, including the authentication of Microsoft Dynamics GP users. If additional server roles are required for the Microsoft Dynamics GP deployment, additional virtual machines would be added to the virtual network in Windows Azure and joined to the corporate network domain.

An additional option in this model is to add a read-only domain controller, with local DNS, to the Windows Azure Virtual Network to improve latency for name resolution and user authentication.

### Dedicated Private Virtual Network

In this model a Windows Azure Virtual Network is created that is fully contained within Windows Azure. It is not connected to an on-premise network. All of the Microsoft Dynamics GP and required infrastructure components are installed on virtual machines on the virtual network. Unless a single machine configuration is being used, you will need to add an Active Directory domain controller with DNS to the virtual network. The virtual network will be configured to use the domain’s DNS system for name resolution of machines on the virtual network. The quantity and configuration of the virtual machines is based on your deployment needs, much like deploying to computers on your corporate network. The following diagram shows a simple Microsoft Dynamics GP Web Client deployment on a dedicated private Windows Azure Virtual Network.



In this diagram the Windows Azure Virtual Network contains an Active Directory domain controller with DNS. The virtual network is configured to use the DNS services on the domain controller for name resolution of the Windows Azure Virtual Machines. The Web Server and SQL Server virtual machines are joined to the domain in Windows Azure for directory services, including the authentication of Microsoft Dynamics GP users. If additional server roles are required for the Microsoft Dynamics GP deployment, additional virtual machines would be added to the virtual network in Windows Azure and joined to the domain in Windows Azure.

## System Requirements

The system requirements for deploying on Windows Azure are the same as deploying Microsoft Dynamics GP on-premise or in other data centers. The virtual machines in Windows Azure have a standard processor and memory configuration that is based on the instance size. The instance sizes range from an A0 standard instance to an A7 memory intensive instance. You can scale the instance size up or down as usage patterns change. You can also add additional instances to scale out as demand increases. The following table contains the compute instance sizes for Windows Azure Virtual Machines at the time this guide was created. Refer to the [Pricing Details](http://www.windowsazure.com/en-us/pricing/details/)[[19]](#footnote-19) page for the latest instance sizes and pricing.

Standard Instances

| Compute Instance Name | Virtual Cores | RAM |
| --- | --- | --- |
| Extra Small (A0) | Shared | 768 MB |
| Small (A1) | 1 | 1.75 GB |
| Medium (A2) | 2 | 3.5 GB |
| Large (A3) | 4 | 7 GB |
| Extra Large (A4) | 8 | 14 GB |

Memory Intensive Instances

| Compute Instance Name | Virtual Cores | RAM |
| --- | --- | --- |
| A6 | 4 | 28 GB |
| A7 | 8 | 56 GB |

Use the published [Microsoft Dynamics GP 2013 system requirements](http://technet.microsoft.com/en-us/library/jj673201(v=gp.20).aspx)[[20]](#footnote-20) when determining the compute instance size required for each of the virtual machine instances in your configuration. The table below maps out the published system requirements to the Windows Azure Virtual Machine instance sizes at the time this guide was created. In each server configuration you will be able to start with a specific size and then increase or decrease the instance size as needed. You may also add additional virtual machine instances for those Microsoft Dynamics GP servers that can be scaled out. These guidelines should serve as a starting point and be adjusted based on your individual configuration.

|  |  |
| --- | --- |
| Servers | Instance Size |
| Microsoft SQL Server | * Profile 1 – A1 * Profile 2 – A2 * Profile 3– A3 * Profile 4 – A4 |
| Remote Desktop Services Server | * Up to 15 users - A2 * Up to 30 users – A3 * Up to 60 users – A4 |
| Web Server (web client) | Single Machine   * Up to 25 users – A2 * Up to 60 users – A3 * Up to 120 users – A4   Scale Out   * A2 |
| Session Host Server (web client) | * Up to 25 users – A2 * Up to 60 users – A3 * Up to 120 users – A4 |
| Web Server (Web Services, Workflow, BP, SQL Reporting Services) | A2 (A3 if deploying multiple applications on single server) |
| Application Server (Management Reporter services) | A2 |

\* The “up to … users” recommendations are based on concurrent users.

There is a 20 core limit by default on a Windows Azure subscription. If your subscription is going to require a total of more than 20 cores, you will need to open a quota increase ticket with Microsoft Support [here](http://www.microsoft.com/windowsazure/support/). A core is equal to a single small Virtual Machine instance. A medium Virtual Machine instance is equal to 2 cores, a large instance equals 4 cores, etc.

Example:

If you have 1 large, 2 medium and 1 small Virtual Machine instances in your subscription, the total cores for the subscription is 9.

| Compute Instance Size | Cores |
| --- | --- |
| Small (A1) | 1 |
| Medium (A2) | 2 |
| Medium (A2) | 2 |
| Large (A3) | 4 |

Total 9

## High Availability and Disaster Recovery (HADR)

While the Windows Azure Infrastructure Services are designed to provide a high availability and fault tolerant platform for applications, there are considerations you as the administrator need to plan for in order to best utilize these capabilities. The Windows Azure high availability mechanisms protect the high availability of the Virtual Machines (VMs), not specifically the applications which run on these VMs. It is up to you as the administrator to use these mechanisms when implementing the application in order to meet the HADR capabilities you require. The following sections contain information on the high availability mechanisms available in Windows Azure to use with your Dynamics GP deployment.

### Availability Set

An availability set in Windows Azure is a configuration option available when load balancing multiple VMs that places the VMs in different fault and update domains. The result is that the application is still available even if there is a failure or planned update to a VM instance that takes it off-line for a period of time. The fault domain protects against unplanned failures by creating the VMs in a different “rack” of servers, resulting in them being on different physical hardware and serviced by different networking components. The update domain protects against downtime from planned updates to the host operating system by placing the VMs on host machines configured with different maintenance schedules.

An availability set requires that the application is installed on multiple VMs that have been configured as a load balanced cloud service. Not all of the Dynamics GP components can be deployed in this configuration however, the following Dynamics GP application components support being deployed on a load balanced cloud service.

1. Web Client Web Server (Only possible if using a scale out deployment with separate Session Host servers or if each of the servers runtime service is configured for a unique port.)
2. Web Services for Microsoft Dynamics GP
3. SQL Server Reporting Services
4. Tenant Services (Requires the Tenant Services be configured for load balancing in your DNS configuration.)
5. Business Portal
6. Workflow

Refer to the article [Manage the High Availability of Virtual Machines](http://www.windowsazure.com/en-us/manage/windows/common-tasks/manage-vm-availability/)[[21]](#footnote-21) for additional information.

### SQL Server HADR

There are a number of different HADR technologies in the SQL Server product that are supported in Windows Azure. These include the following.

* AlwaysOn Availability Groups
* Database Mirroring
* Log Shipping
* Backup and Restore with Windows Azure Blob Storage Service

These technologies can be used independently or together to provide the high availability and disaster recovery required. When used with Microsoft Dynamics GP, the AlwaysOn and Database Mirroring technologies provide failover capabilities for the Dynamics GP databases. The Log Shipping and Backup and Restore with Windows Azure Blob Storage Service provide recovery capabilities for the Dynamics GP databases. Refer to the article [High Availability and Disaster Recovery for SQL Server in Windows Azure Virtual Machines](http://msdn.microsoft.com/library/windowsazure/jj870962.aspx)[[22]](#footnote-22) for additional information.

### Redundant Storage

The redundant storage mechanism of Windows Azure provides for multiple copies of the VM’s VHD files and the data disks that store data such as the Dynamics GP databases. The first redundant story mechanism is locally redundant storage (LRS), which maintains three copies of the account data within the primary data center. The second mechanism is geo redundant storage (GRS, also known as geo-replication), which replicates the account data to a secondary data center. These redundant copies are done automatically by the platform. You do need to be aware that for the Windows Azure data disks used to store the Dynamics GP databases, if GRS is enabled the data and log files for a database need to be placed on the same disk.

### Host O/S Maintenance

Since you are the administrator of your VMs, you are in control of applying updates to the operating system of the VM. You however are not in control of the updates applied to the host operating system. The host operating system is updated at least quarterly and updates are performed by the platform as outlined in the article [Windows Azure Host OS Updates](http://msdn.microsoft.com/en-us/library/windowsazure/hh543978.aspx)[[23]](#footnote-23). The process of applying an update to the host operating system shuts down and restarts all of the VM instances on the machine. The Dynamics GP components that are deployed using an availability set will continue to function as expected using the VM instance in a different update domain than the one being updated. The Dynamics GP components that are not deployed using an availability set will be off-line for the period of time it takes to update the host OS and restart the VM instance. In addition, any user processes running on your VM instance at the time of the host OS update will be terminated. In order to best plan for this scenario and to keep user sessions from being terminated abnormally, a notification of an upcoming host OS update is sent 2-3 days prior to the Microsoft Account that is the owner of the Windows Azure subscription. The updates are typically scheduled for non-business hours in the given region. You will need to handle this update in the same way you handle an update to your VM instance, which would include informing users of the maintenance time and keeping users out of Dynamics GP during the update period.

# Part 3: Deploy Microsoft Dynamics GP

The deployment of Microsoft Dynamics GP on Windows Azure is very similar to an on-premise deployment. The setup of the network and virtual machines in Windows Azure is where the deployment of Microsoft Dynamics GP on Windows Azure is the most different from on-premise deployments. You will use the Windows Azure Management Portal or PowerShell for most of the setup actions. These include setting up a virtual network, creating virtual machines, and configuring the virtual machines through Remote Desktop for Administration. After setting up the environment, you will install the Microsoft Dynamics GP components on the virtual machines that are acting as the SQL Server, Web Server, Session Host machines, and so on. This part contains the following sections.

* [Creating an Affinity Group](#_Creating_an_Affinity) provides direction for creating an affinity group in Windows Azure.
* [Creating a Virtual Network](#_Creating_a_Virtual) provides directions for setting up a virtual network in Windows Azure.
* [Creating Virtual Machines](#_Creating_Virtual_Machines) provides directions for creating a virtual machine instance in Windows Azure.
* [Configuring Active Directory](#_Configuring_Active_Directory) provides information about configuring Active Directory on a Windows Azure Virtual Machine.
* [Configuring Microsoft SQL Server](#_Configuring_Microsoft_SQL) provides directions for configuring SQL Server on a Windows Azure Virtual Machine for use with Microsoft Dynamics GP.
* [Configuring Microsoft SQL Server Reporting Services](#_Chapter_6:_Configure_1) provides direction for configuring SQL Server Reporting Services on a Windows Azure Virtual Machine for use with Microsoft Dynamics GP.
* [Configuring the Tenant Services Server](#_Configuring_the_Tenant) provides direction for configuring a Windows Azure Virtual Machine as a host for Tenant Services. Tenant Services is an optional Microsoft Dynamics GP component required only if you are installing Microsoft Dynamics GP for use by multiple customer organizations (tenants).
* [Configuring the Web Client Web Server](#_Configuring_the_Web) provides directions for configuring a Web Server on a Windows Azure Virtual Machine for use with Microsoft Dynamics GP web client.
* [Configuring the Web Client Session Host Server](#_Chapter_7:_Configure) provides directions for configuring a Windows Azure Virtual Machine as a Microsoft Dynamics GP Web Client session host.
* [Configuring Remote Desktop Services](#_Configuring_Remote_Desktop) provides directions for configuring Remote Desktop Services on a Windows Azure Virtual Machine for use with Microsoft Dynamics GP.
* [Configuring SharePoint Server](#_Configuring_SharePoint_Server) provides directions for configuring a SharePoint Server on a Windows Azure Virtual Machine for use with Microsoft Dynamics GP.
* [Configuring a Management Reporter Server](#_Configuring_a_Management) provides directions for configuring a Windows Azure Virtual Machine for use with Management Reporter.

## Creating an Affinity Group

An affinity group keeps the Windows Azure Virtual Machines and storage within the same cluster of a single data center for the best performance. An affinity group is required to create a Windows Azure Virtual Network. Refer to the [How to Create an Affinity Group](http://msdn.microsoft.com/en-us/library/windowsazure/hh531560.aspx)[[24]](#footnote-24) article for directions about creating an affinity group.

## Creating a Virtual Network

A Windows Azure Virtual Network must be created in your subscription so that you can create and run the Windows Azure Virtual Machine instances. The Windows Azure Virtual Network may be connected to a physical network for site-to-site connectivity, it could also be set up as a dedicated private network in the cloud. The virtual machines serve as the Windows Server hosts for the Microsoft Dynamics GP components deployed on the virtual network you create.

Before setting up your virtual network, you will need to determine the design that will best meet your deployment scenario. Things to consider include whether you will be joining this network to another network, the address ranges for the network and how domain name resolution (DNS) will be handled. In the current Windows Azure release, it may be difficult to make changes to the virtual network after virtual machines have been deployed. Refer to the [Windows Azure Virtual Network](http://msdn.microsoft.com/en-us/library/windowsazure/jj156007.aspx)[[25]](#footnote-25) and [Windows Azure Name Resolution Overview](http://msdn.microsoft.com/en-us/library/windowsazure/jj156088.aspx)[[26]](#footnote-26) articles for design considerations.

When deploying Microsoft Dynamics GP on Windows Azure, you have two options. You can create a private virtual network that is fully-contained within Windows Azure, or you can create a virtual network in Windows Azure that is connected to your existing physical network. In either case, all of the Microsoft Dynamics GP components will be deployed to virtual machine instances on the Windows Azure Virtual Network. You may want to connect to an existing network to leverage Active Directory services for user authentication or other on-premise resources. The decision of whether or not to connect the virtual network to your physical network will determine how you configure name resolution (DSN) for the virtual network. The virtual network and name resolution articles above provide the type of name resolution that is required or recommended for each of the scenarios. When creating a private virtual network with multiple virtual machines, you will need to create a domain controller for authentication and name resolution (DNS). The virtual network will need to be configured to use the domain controller’s IP address for DNS. This means that you must modify the DNS setting for the virtual network after creating the domain controller virtual machine on the virtual network.

You create a virtual network by using the Windows Azure Management Portal or by creating and importing a network configuration file. Refer to the article [Create a Virtual Network in Windows Azure](http://www.windowsazure.com/en-us/manage/services/networking/create-a-virtual-network/)[[27]](#footnote-27) for information about creating a virtual network using the Windows Azure Management Portal. Refer to the article [Configuring a Virtual Network Using Network Configuration Files](http://msdn.microsoft.com/en-us/library/windowsazure/jj156097.aspx)[[28]](#footnote-28) for information about using the network configuration file.

## Creating Virtual Machines

All of the Microsoft Dynamics GP components, along with the required software like Microsoft SQL Server and Microsoft SQL Server Reporting Services, will be installed on Windows Server virtual machine instances in Windows Azure. Depending on your deployment needs, you will use one or more virtual machine instances. For example, you may have a SQL Server virtual machine, a Web Server virtual machine and an Active Directory virtual machine.

A virtual machine instance can be created from a VHD template image available in the Windows Azure platform image gallery or from an image or VHD disk you created and uploaded. You also have the ability to capture a configured virtual machine instance as a template image for creating additional virtual machine instances. Refer to the article [Virtual Machines](http://msdn.microsoft.com/en-us/library/windowsazure/jj156003.aspx)[[29]](#footnote-29) for additional information.

Follow the steps in the article [Create a Virtual Machine](http://www.windowsazure.com/en-us/manage/windows/tutorials/virtual-machine-from-gallery/)[[30]](#footnote-30) to create the virtual machines. Use the following guidelines when creating the virtual machine instances for Microsoft Dynamics GP. The remaining sections in this part provide information that applies to the virtual machine configuration for each of the server roles used in Microsoft Dynamics GP.

1. Use a unique name that identifies the virtual machine. (Example: GPSQLServer)
2. Select the virtual machine instance size based on the information provided in the [System Requirements](#_Chapter_2:_System) section.
3. Enter a name and password for the virtual machine’s administrator account.
4. Indicate whether the virtual machine will be a standalone virtual machine or whether it will be connected with other virtual machines to provide load balancing and high availability.

Standalone Virtual Machine

Selecting the “Create a new cloud service” option for the Cloud Service field will create a new cloud service for the virtual machine using the DNS name provided in the cloud service DNS name field. The cloud service, along with endpoints created on the virtual machine, provide external communication to the virtual machine. Communication from machines not on the virtual network is considered external communication. You can use this option to set up a virtual machine for any of the server roles in your Microsoft Dynamics GP deployment. You will also use this option to set up the first virtual machine in a load-balanced configuration.

Connect to existing Virtual Machine

Selecting an existing cloud service name in the Cloud Service drop down will configure this virtual machine to work with an existing virtual machine for load balancing. When selecting this option, all virtual machines connected together will be load balanced by a single cloud service using the DNS name provided. You can use this option for virtual machines that serve the following roles in your Microsoft Dynamics GP deployment.

1. Web Client Web Server (Only possible if using a scale out deployment with separate Session Host servers.)
2. Web Services for Microsoft Dynamics GP
3. SQL Server Reporting Services
4. Tenant Services (Requires the Tenant Services be configured for external communication.)
5. Business Portal
6. Workflow
7. If you have selected to create a new cloud service, provide the DNS name that will be used for external communication to the virtual machine. The name will be in the format of \*.cloudapp.net. If you selected an existing cloud service, the DNS name for the cloud service will default in and can’t be changed. If you will be using a domain name other than the provided **cloudapp.net** DNS name, you will need to create a CNAME record to map your custom domain name to the DNS name selected during the creation of the virtual machine. Another alternative is to add an A record to the virtual IP address of the virtual machine. Refer to the article [Configuring a custom domain name for a Windows Azure cloud service or storage account](http://www.windowsazure.com/en-us/develop/net/common-tasks/custom-dns/)[[31]](#footnote-31) for additional information.
8. If you are an administrator for more than one Windows Azure Subscription, select the subscription you want the virtual machine created in.
9. Select the virtual network and subnet to put the VM in. All of the virtual machines used in a single Microsoft Dynamics GP deployment must be created on the same virtual network.
10. Select to have a storage account automatically created or select and existing storage account for the virtual machine’s VHD file.
11. If you are connecting multiple virtual machines together in a cloud service to perform an action like load balancing, provide the name for an availability set. The availability set can be created with the first virtual machine created in a cloud service. Select the existing availability set for each additional virtual machine being added to the cloud service. The availability set ensures that the virtual machine instances are created in different fault and update domains. Using this option provides further protection against a single point of failure, such as a failing network switch, that could affect the entire cloud service.
12. Add any endpoint you know will be required for the virtual machine. Endpoints can also be added as needed after the creation of the virtual machine.

## Configuring Active Directory

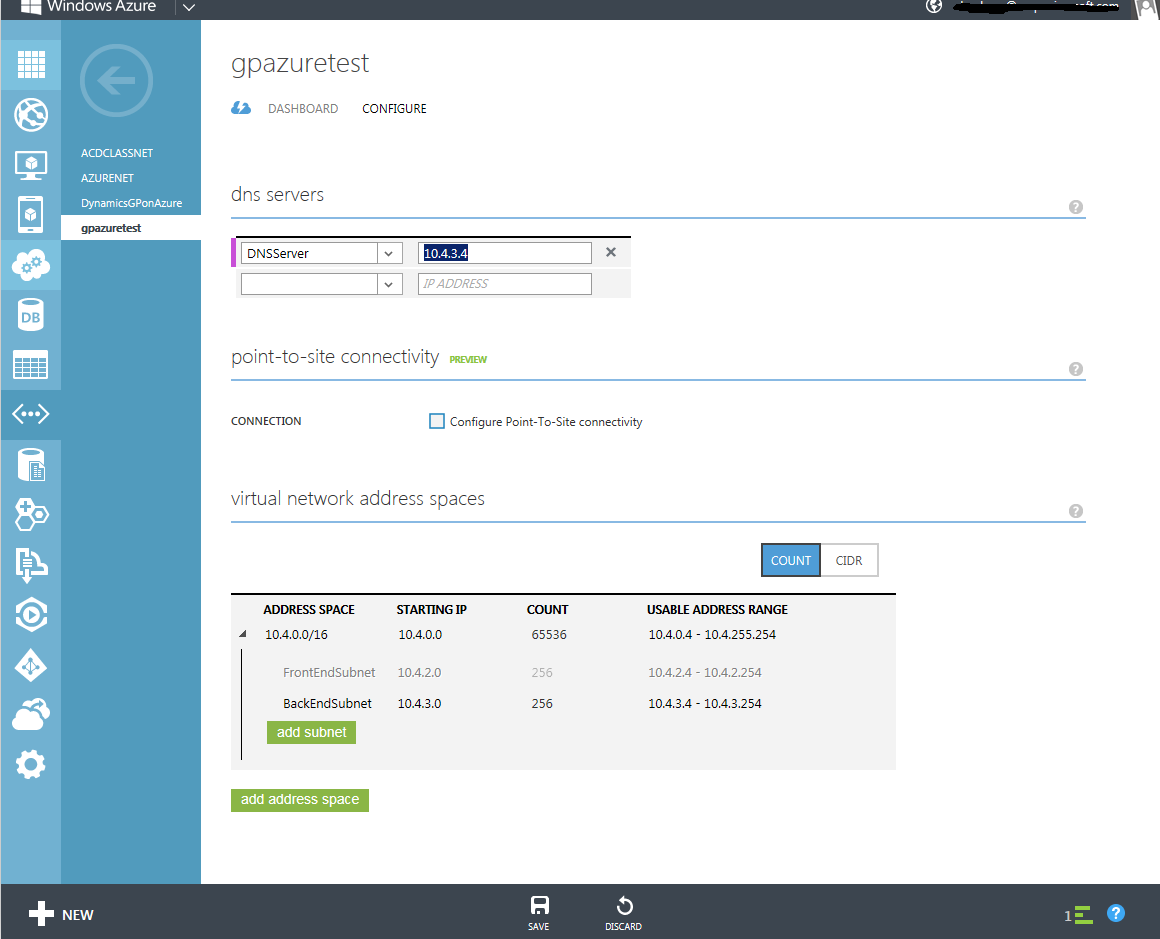
In a Microsoft Dynamics GP deployment on Windows Azure, users are authenticated as Windows accounts in order to be granted access to the application. In deployment scenarios where there are multiple virtual machines serving different roles within the deployment, using Active Directory to authenticate users across the machines is recommended. The configuration of your virtual network will determine how you configure Active Directory. The requirements for deploying Active Directory on a Windows Azure Virtual Machine differ very little from on-premise deployments, but there are a few differences that you will need to be aware of. Refer to [Guidelines for Deploying Windows Server Active Directory on Windows Azure Virtual Machines](http://msdn.microsoft.com/en-us/library/windowsazure/jj156090.aspx)[[32]](#footnote-32) for additional information.

In an environment where you have configured a private virtual network in Windows Azure, you will need to set up the first virtual machine as an Active Directory domain controller. Follow the steps in the article [Install Active Directory forest in the Windows Azure network](http://www.windowsazure.com/en-us/manage/services/networking/active-directory-forest/)[[33]](#footnote-33) for directions on setting up Active Directory in a private Windows Azure Virtual Network. You may also choose to deploy additional domain controllers for improved availability and performance if needed.

In an environment where you have connected the Windows Azure Virtual Network to your on-premise network, you may choose to configure a virtual machine as an additional Active Directory domain controller for your on-premise forest. This can improve the availability and performance of Active Directory. Follow the steps in the article [Install a Replica Active Directory Domain Controller in Windows Azure Virtual Networks](http://www.windowsazure.com/en-us/manage/services/networking/replica-domain-controller/)[[34]](#footnote-34) for directions about using a Windows Azure Virtual Machine as an additional domain controller for your on-premise Active Directory forest.

If you will be using the Active Directory domain controller virtual machine for name resolution (DNS) on the Windows Azure Virtual Network that it is deployed on, you will need to modify the configuration of the existing Windows Azure Virtual Network after the domain controller is set up. Use the following steps to configure the Windows Azure Virtual Network to use the domain controller virtual machine for DNS.

1. In the Windows Azure Management Portal, select the virtual network you created. Click the **Configure** tab.
2. Enter the name and Internal IP address of the Domain Controller virtual machine. (The internal IP address can be found on the dashboard page of the virtual machine.)



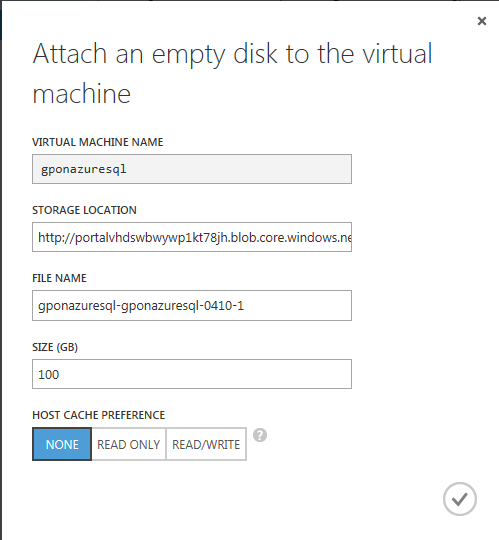
1. Save the changes using the **SAVE** option on the bottom of the page.

## 

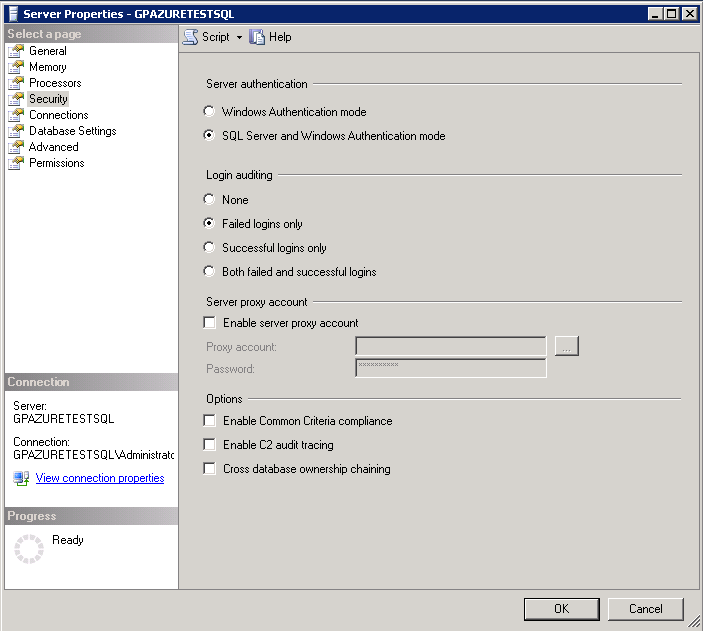
## Configuring Microsoft SQL Server

All Microsoft Dynamics GP deployments require a Microsoft SQL Server to manage the databases that contain the business data. When deploying on Windows Azure, a Microsoft SQL Server installation on a Windows Azure Virtual Machine will be used. Microsoft Dynamics GP does not support using Windows Azure’s SQL Database feature that provides a database-as-a-service. Use the following steps when creating the Windows Azure Virtual Machine to host the Microsoft SQL Server. Refer to the [Performance Considerations for SQL Server in Windows Azure Virtual Machines](http://msdn.microsoft.com/en-us/library/windowsazure/dn248436.aspx)[[35]](#footnote-35) white paper for the latest information.

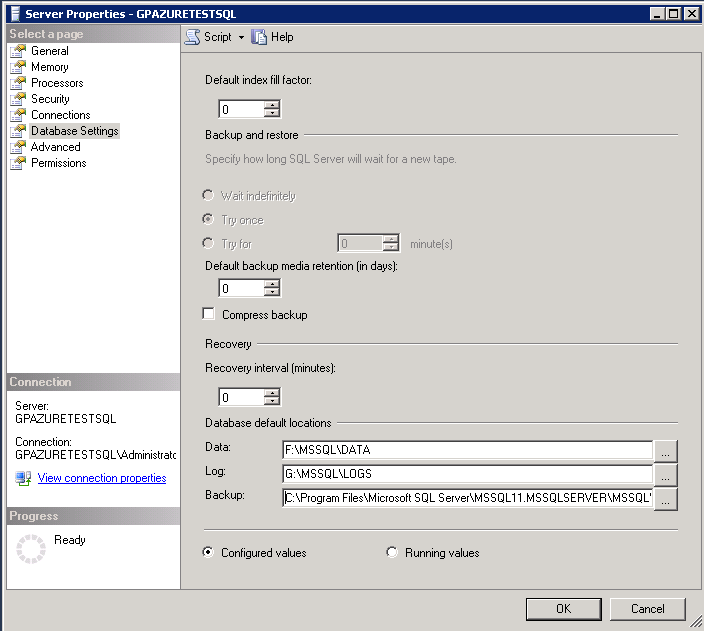
1. Create the virtual machine using a Windows Server 2008 R2 or Windows Server 2012 image template. If you choose to create a virtual machine using an image from the Image Gallery with Microsoft SQL Server already installed (Microsoft SQL Server 2012 SP1 Enterprise or Microsoft SQL Server 2012 SP1 Standard), you will have additional steps to perform after the virtual machine is created to configure Microsoft SQL Server for use with Microsoft Dynamics GP.
2. Attach at least one data disk to the virtual machine. The data disk stores the SQL Server data and log files. You may also want to create a second data disk for SQL backups. (Repeat the following steps for each disk you want added.) If you are using Geo Redundant Storage (GRS) for the data disks, make sure and place the data and log files for the databases on the same disk. The recommended host cache configuration of the data disk will depend on the total number of concurrent Dynamics GP users accessing the data disk and the size of the data disk. Setting the “HOST CACHE PREFERENCE” to read only will cache the disk to the local machine’s disks and may improve performance in configurations with fewer than approximately 250 concurrent users. The maximum size of the data disk in order to use the read only cache setting is 640 GB, so if your data disk is larger than this you will need to set the “HOST CACHE PREFERENCE” to none.
   1. In the Windows Azure Management Portal, select the virtual machine you created. On the bottom of the screen, click **Attach** and then click **Attach Empty Disk**.
   2. Provide the size for the data disk.
   3. If you will have fewer than approximately 250 concurrent Dynamics GP users accessing the data disk and the data disk is less than 640 GB, set “HOST CACHE PREFERENCE” to **READ ONLY**. If you will have more than 250 concurrent GP users or the data disk is larger than 640GB then set “HOST CACHE PREFERENCE” to **NONE**.



1. In the Windows Azure Management Portal, select the virtual machine. On the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Open Disk Management to initialize and format the data disks that were attached.
   2. Join the virtual machine to the domain.
   3. Create the following folder structure at the root of the data disk.
      1. Data – MSSQL\DATA
      2. Log – MSSQL\LOGS
   4. Install Microsoft SQL Server using the recommended settings in the [Microsoft Dynamics GP installation manual](http://www.microsoft.com/en-us/download/details.aspx?id=34669)[[36]](#footnote-36). (Skip this step if you used a virtual machine image with Microsoft SQL Server already installed.)
   5. Open SQL Server Management Studio and make the following changes:
      1. Right-click on the SQL Server and choose to view the properties.
         1. Select the Security page and verify that the Server Authentication is set to SQL Server and Windows Authentication mode. If it is not, then choose that setting.



* + - 1. Select the Database Settings tab and change the Database default locations to the folders that you created in the data disks you attached to the virtual machine.



* + - 1. Click **OK** to save settings. (Restart SQL Server for the settings to take effect.)
    1. Create a new SQL Server Login with sysadmin privileges, or as an alternative enable the ‘sa’ account to use when setting up Dynamics GP. If enabling the ‘sa’ account, enter a password for the account. (This step only needs to be done if you didn’t perform it during the SQL Server installation, or if the virtual machine was created from the Image Gallery.)
  1. Verify there is sufficient disk space on the C: drive. There must be at least 1 GB of free space available.
  2. Note whether the Reporting Services, Analysis Services, Full-text Search Services, and Integration Services are installed and running on the image. If you won’t be using any of these services on this server, stop the services and change them to manual or disabled.
  3. Use Windows Explorer to assign Full Control permissions to the MSSQL\DATA folder for the “NT Service\MSSQLSERVER” account if this permission hasn’t already been granted. Verify security settings to be sure correct permissions are set.
  4. Use Windows Explorer to assign Full Control permissions to the MSSQL\LOGS folder for the “NT Service\MSSQLSERVER” account if this permission hasn’t already been granted. Also assign the same permissions as are assigned by SQL Server to the “NT Service\SQLSERVERAGENT” and “NT Service\MSSQLFDLauncher” accounts if they haven’t already been granted.
  5. Add an inbound rule to allow access to the SQL Server (default port 1433) to the virtual machine’s firewall.

In order to further protect the SQL Server from unauthorized access, you may want to consider removing the endpoint on the host virtual machine for the remote desktop connection. Removing this public endpoint will require that all virtual machine administration for the SQL Server is done from another machine within the virtual network.

### Installing Microsoft Dynamics GP Desktop Client and Creating Databases

When you create the Microsoft Dynamics GP databases will depend on whether you are in a single tenant or multitenant deployment environment. In a single tenant deployment, the databases are typically created after Microsoft SQL Server and Microsoft SQL Server Reporting Services have been installed and configured. In a multi-tenant model, the databases are typically created as part of provisioning each new customer. A program called Microsoft Dynamics GP Utilities, which is installed with the Microsoft Dynamics GP Desktop Client, is used to create the databases.

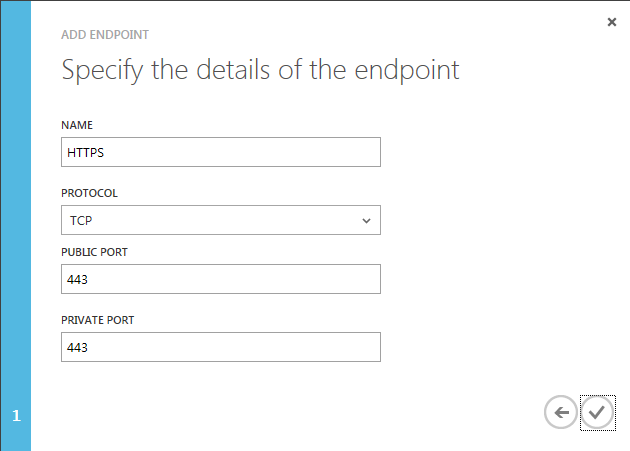
The installation of the Microsoft Dynamics GP desktop client used to create the databases can be on the SQL Server virtual machine or another virtual machine depending on your configuration. It is recommend that you install on another virtual machine, such as the Microsoft Dynamics GP web client’s session host or the Remote Desktop for Administration server, in order to keep the SQL Server virtual machine as clean as possible with sufficient operating system disk space. Use the following steps to install the Microsoft Dynamics GP desktop client, create the databases, and deploy the Business Intelligence Reports.

1. Install the Microsoft Dynamics GP Desktop Client using the directions in the [installation manual](http://www.microsoft.com/en-us/download/details.aspx?id=34669)[[37]](#footnote-37).
2. Use Microsoft Dynamics GP Utilities in the desktop client installation to create the Microsoft Dynamics GP databases. Make sure and select to create the databases on the data disk attached to the SQL Server virtual machine instead of the operating system disk. If you are using Geo Redundant Storage (GRS) for the data disk, make sure and place the data and log files on the same disk.
3. You can select to deploy the SQL and Excel reports for the database in Microsoft Dynamics GP Utilities or use the Reporting Tools Setup window within Microsoft Dynamics GP. If you plan to allow client computers that are not on the network to access the SQL Reports, make sure and use the public URL to SQL Server Reporting Services during the deployment.

## Configuring Microsoft SQL Server Reporting Services

If you will be using SQL Server Reporting Services reports for your Microsoft Dynamics GP deployment on Windows Azure, you must install Microsoft SQL Server Reporting Services on a virtual machine instance. How users will be accessing the SQL reports will determine whether you install SQL Server Reporting Services on the same server as the SQL Server database engine or a different server. If users will be accessing reports from client computers that are not connected to the virtual network, it is recommended that you deploy SQL Server Reporting Services to a different virtual server than the SQL Server database engine. Use the following steps to create a Windows Azure Virtual Machine to host Microsoft SQL Server Reporting Services. Refer to the [SQL Server Business Intelligence in Windows Azure Virtual Machines](http://msdn.microsoft.com/en-us/library/windowsazure/jj992719.aspx)[[38]](#footnote-38) page for the latest information.

1. Create the virtual machine using a Windows Server 2008 R2 or Windows Server 2012 image template. If you choose to create a virtual machine using an image from the Image Gallery with Microsoft SQL Server already installed (Microsoft SQL Server 2012 SP1 Enterprise or Microsoft SQL Server 2012 SP1 Standard), you will have additional steps after the virtual machine is created to configure Microsoft SQL Server Reporting Services for use with Microsoft Dynamics GP.
2. In the Windows Azure Management Portal, select the virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. Install Microsoft SQL Server Reporting Services using the recommended settings in the [Dynamics GP installation manual](http://www.microsoft.com/en-us/download/details.aspx?id=34669)[[39]](#footnote-39). (Skip this step if you used an image with Microsoft SQL Server already installed.)
   3. Use the Reporting Services Configuration Manager to configure SQL Server Reporting Services. If users will be accessing the reports over the internet, it is recommended that you configure reporting services for SSL (Secure Sockets Layer). Refer to article [Configure SSL Connections on a Native Mode Report Server](http://technet.microsoft.com/en-us/library/ms345223(v=sql.110).aspx)[[40]](#footnote-40) for additional information.
   4. Follow the setup instructions in the Microsoft Dynamics GP System Setup Guide on the Microsoft Dynamics GP 2013 installation media to configure SQL Server Reporting Services for use with Microsoft Dynamics GP.
   5. Add an inbound rule to allow access to the SQL Server Reporting Services port to the virtual machines firewall.
3. If users will be accessing the SQL reports from client computers not connected to the virtual network, add a public endpoint for the virtual machine.
   1. In the Windows Azure Management Portal, select the virtual machine. Click the **ENDPOINT** tab.
   2. On the bottom of the screen, click **Add Endpoint.**
   3. **Select to add a standalone endpoint if the virtual machine is not load balanced with another virtual machine. If you want to load balance the same endpoint as another virtual machine in the same cloud service, select to “Add an endpoint to an existing load-balanced set”.**
   4. **Add an endpoint for the SQL Server Reporting Services port (typically 443).**



If you will be setting up multiple SQL Server Reporting Services virtual machine instances as load balanced, create additional virtual machine instances using these same steps. When creating the virtual machine, choose to join the cloud service created when setting up the first SQL Server Reporting Services virtual machine.

## Configuring the Tenant Services Server

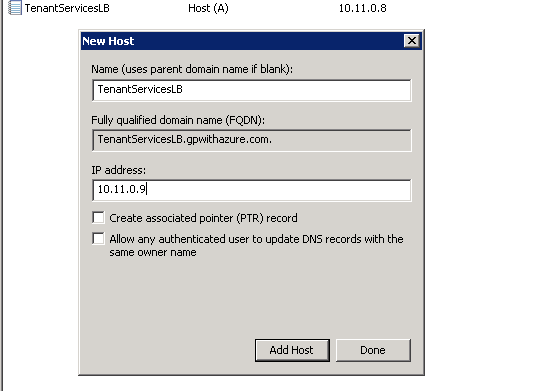
If you will be deploying Microsoft Dynamics GP for use by multiple customer organizations (tenants), you will need to install Tenant Services on a virtual machine in Windows Azure. The Tenant Services can be installed on a virtual machine that is running other Microsoft Dynamics GP components, or the Tenant Services can be installed on a dedicated virtual machine. Use the following steps when creating a dedicated Windows Azure Virtual Machine to host Microsoft Dynamics GP Tenant Services. Refer to the TSInstallAdminGuide.pdf on the Microsoft Dynamics GP 2013 installation media for information about preparing the server for Tenant Services.

1. Create the virtual machine using a Windows Server 2008 R2 or Windows Server 2012 image template.
2. In the Windows Azure Management Portal, select the virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. Install the Dynamics GP Tenant Services using the instructions in the TSInstallAdminGuide.pdf on the Microsoft Dynamics GP 2013 installation media.

If you will be setting up multiple Tenant Services virtual machine instances as load balanced, create additional virtual machine instances using these same steps. When creating the virtual machine, choose to join the cloud service created when setting up the first Tenant Services virtual machine. There are two options for configuring the load balanced endpoint for the Tenant Service.

1. The recommended approach is to keep all communications to the Tenant Services within the Windows Azure Virtual Network. In order to load balance this communication, you will need to add new a A record in your internal DNS for each of the Tenant Service virtual machines using a load balanced name and the internal IP address of the virtual machine. The Tenant Services URL used by other applications will be the load balanced name you used for the A records added to your DNS. Refer to the [Configuring DNS load balancing](http://technet.microsoft.com/en-us/library/cc787484(v=WS.10).aspx)[[41]](#footnote-41) article for additional information.

Example: In this example, two new A records with a FQDN of TenantServicesLB.gpwithazure.com that are mapped to the internal IP addresses of the two virtual machines that I installed Tenant Services on are added to DNS. (10.11.0.8 and 10.11.0.9) When I then use an address such as <http://TenantServicesLB.gpwithazure.com/>..., DNS will use a round robin approach to distributing communications to the tenant services.



1. The other option is to use the load balanced public fully qualified domain name of the cloud service created by Windows Azure. This requires however that you expose the endpoint publicly which isn’t necessary and in most scenarios not recommended. The Tenant Services URL used by other applications will be the fully qualified domain name of the cloud service. Create a virtual machine endpoint for both the Tenant Services Discovery Service and Tenant Services Management Service ports using the following steps.
2. In the Windows Azure Management Portal, select the virtual machine. Click the **ENDPOINT** tab.
3. On the bottom of the screen, click **Add Endpoint.**
4. **Add an endpoint for the Tenant Services Discovery Service (typically 48630).**
5. **Add an endpoint for the Tenant Services Management Service (typically 48631).**

## 

## Configuring the Web Client Web Server

If you will be deploying the Microsoft Dynamics GP Web Client, you must install the web server components on a Windows Azure Virtual Machine with Internet Information Services (IIS) installed. The Microsoft Dynamics GP Web Client can be installed in a single machine or scale out deployment configuration. In a single machine configuration, the Session Server components will also be installed on the web server instead of on a separate session host. Use the following steps along with the [Microsoft Dynamics GP Web Client Installation and Administration Guide](http://www.microsoft.com/en-pk/download/details.aspx?id=34672)[[42]](#footnote-42) to set up the Windows Azure Virtual Machine as a web server.

1. Create the virtual machine using a Windows Server 2008 R2 or Windows Server 2012 image template.
2. In the Windows Azure Management Portal, select the virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. Import the security certificate to the computer’s personal store.
   3. Install Internet Information Services (IIS) and ASP.NET by adding the Web Server (IIS) role. Make sure and select the ASP.NET and Windows Authentication features on Windows Server 2008 R2 and the ASP.NET 4.5, Windows Authentication, and HTTP Activation features on Windows Server 2012.
   4. Create a new web site or configure the default web site for SSL.
   5. Add an inbound rule for the IIS web site’s port to the virtual machines Windows firewall.
   6. Install Microsoft Dynamics GP Web Client using the instructions in the [Microsoft Dynamics GP Web Client Installation and Administration Guide](http://www.microsoft.com/en-pk/download/details.aspx?id=34672)[[43]](#footnote-43).
3. Add a public endpoint for the web site’s port.
   1. In the Windows Azure Management Portal, select the virtual machine, and then click the **ENDPOINT** tab.
   2. On the bottom of the screen, click **Add Endpoint.**
   3. **Add an endpoint for the IIS web site’s port (typically 443).**
   4. **If you have installed the Session Server feature on this server, add an endpoint for the runtime service’s port.**

If you will be setting up multiple Web Server virtual machine instances as load balanced, create additional virtual machine instances using these same steps. When creating the virtual machine, choose to join to the cloud service created when setting up the first Web Server virtual machine.

## Configuring the Web Client Session Host Server

If you will be deploying the Microsoft Dynamics GP web client using a scale out deployment, then you will need to add one or more Windows Azure Virtual Machines as session hosts. In a scale out deployment of the web client, the Session Central service running on the web server will be responsible for load balancing the session host servers. This requires that each session host virtual machine instance be configured as a standalone virtual machine. Use the following steps along with the [Microsoft Dynamics GP Web Client Installation and Administration Guide](http://www.microsoft.com/en-pk/download/details.aspx?id=34672) to set up the Windows Azure Virtual Machine as a session host.

1. Create the virtual machine using a Windows Server 2008 R2 or Windows Server 2012 image template.
2. In the Windows Azure Management Portal, select the virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. Import the security certificate to the computer’s personal store.
   3. Install Microsoft Dynamics GP Web Client per the instructions in the [Microsoft Dynamics GP Web Client Installation and Administration Guide](http://www.microsoft.com/en-pk/download/details.aspx?id=34672). (Note: Make sure and install the GP Web Resource Cache for improved performance.)
3. Add a public endpoint for the runtime service’s port.
   1. In the Windows Azure Management Portal, select the virtual machine, and then click the **ENDPOINT** tab.
   2. On the bottom of the screen, click **Add Endpoint.**
   3. **Add an endpoint for the runtime service’s port.**

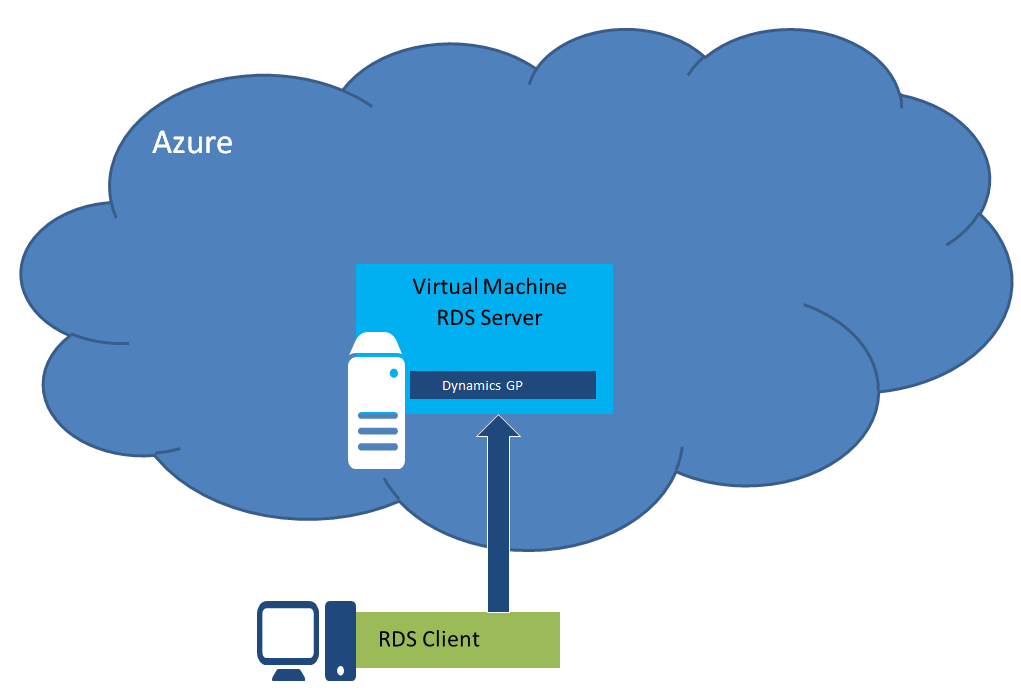
## Configuring Remote Desktop Services

If you will be deploying any of the Microsoft Dynamics GP components that require Remote Desktop Services (RDS) for user access, you will need to add one or more Windows Azure Virtual Machines as RDS servers. There are many options for the configuration of the RDS servers, it is recommended that the RD Gateway service is used and the Microsoft Dynamics GP application component is published as a remote app to provide the most secure access. At the time this guide was published, you need to have purchased Subscription Access Licenses (SALs) using the Microsoft Service Provider License Agreement (SPLA) in order to use RDS on Windows Azure. Refer to the [Product Use Rights (PUR) document](http://www.microsoft.com/licensing/about-licensing/product-licensing.aspx)[[44]](#footnote-44) for the latest information.

In planning your RDS server configuration, you need to determine the number of virtual machines that will be required. If you will require more than one RDS server, you will likely be setting up a load balanced RDS Server farm using two or more Windows Azure Virtual Machines. The following are a few examples of a Windows Azure virtual machine configuration for RDS Servers.

Single Machine

A single machine configuration consists of one virtual machine with all of the required RDS role services installed on it. These services would typically consist of RD Connection Broker, RD Session Host, RD Gateway, RD Web Access and RD Licensing. A single machine configuration doesn’t offer any redundancy, the result is that if the virtual machine is unavailable for any reason users will not have access to the application.

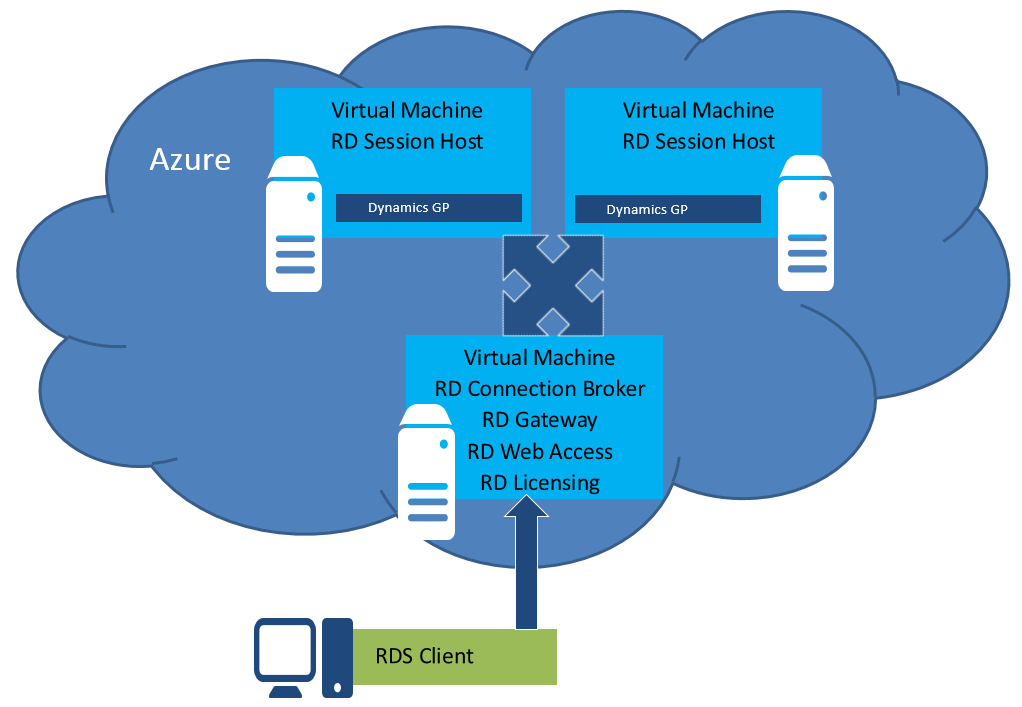


Use the following steps to set up a single Windows Azure Virtual Machine as a RDS server host.

1. Create the virtual machine using a Windows Server 2008 R2 or Windows Server 2012 image template or upload a custom image.
2. In the Windows Azure Management Portal, select the virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. If you already have a security certificate you will be using for the RD Gateway, then import the security certificate to the computer’s personal store.
   3. Open server manager and add the Remote Desktop Services role and role services.
   4. Configure Remote Desktop Services. (i.e. Configure certificates, Create Session Collection, etc.)
   5. Install the Microsoft Dynamics GP components that require RDS to access by using the directions provided in the [[Microsoft Dynamics GP installation manual](http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx)[[45]](#footnote-45)](http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx).
   6. Configure the Microsoft Dynamics GP application component as a RemoteApp.
3. Add a public endpoint for the RD Gateway and RD Web Access ports.
   1. In the management portal, select the virtual machine, and click the ENDPOINT tab.
   2. On the bottom of the screen, click **Add Endpoint.**
   3. **Add an endpoint for the RD Gateway port and RD Web Access port if used. (Port 443 by default.)**

Load Balanced Session Hosts

A load balanced session host configuration consists of two or more virtual machines configured as stand-alone cloud services. In this configuration, the RD Gateway, RD Connection Broker, RD Licensing and RD Web Access role services are installed to a single stand-alone virtual machine and are not configured for high availability. The RD Session Host role service is installed on one or more stand-alone virtual machines. The RD Connection Broker on the virtual machines is load balancing user sessions on one or more virtual machines with the RD Session Host role service installed. A load balanced session hosts configuration only offers redundancy for the RD Session Hosts, the result is that if the virtual machine hosting the other role services is unavailable for any reason users will not have access to the application.



Use the following steps to set up two or more Windows Azure Virtual Machines as RDS Server farm hosts.

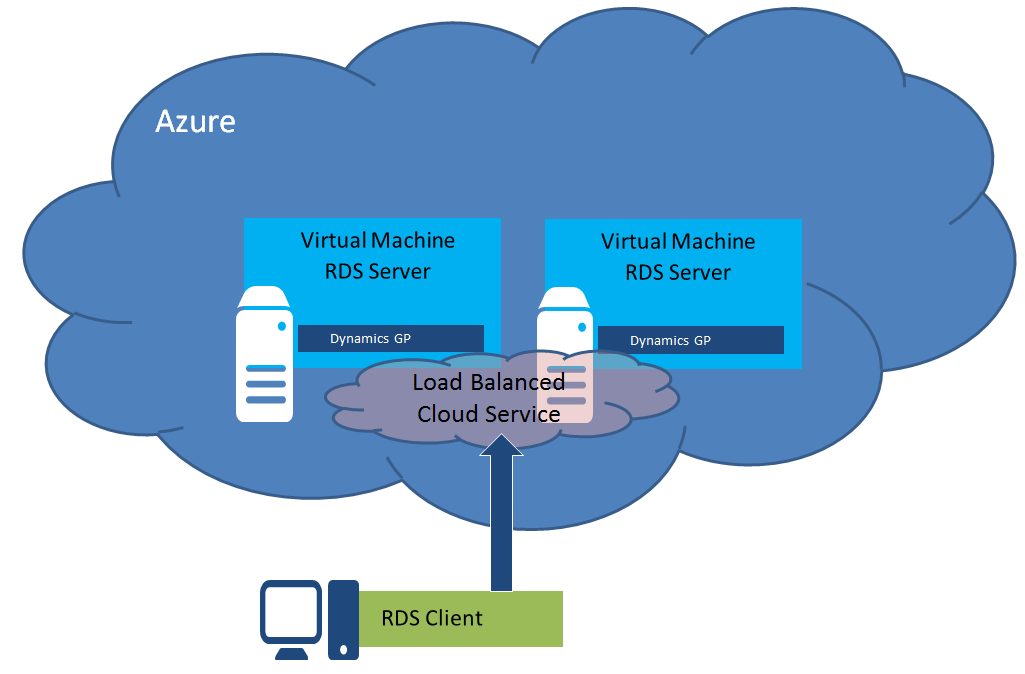
1. Create the virtual machines using a Windows Server 2008 R2 or Windows Server 2012 image template or custom image.
2. In the Windows Azure Management Portal, select the virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. If you already have a security certificate you will be using with the RD Gateway, then import the security certificate to the computer’s personal store.
   3. Open server manager and add the Remote Desktop Services role and role services.
   4. Configure Remote Desktop Services. (i.e. Configure certificates, Create Session Collection, etc.)
   5. Additional configuration for the RD Session Host.
      1. Install the Microsoft Dynamics GP components that require RDS to access by using the directions provided in the [[Microsoft Dynamics GP installation manual](http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx)[[46]](#footnote-46)](http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx).
      2. Configure the Microsoft Dynamics GP application component as a RemoteApp.
3. Add a public endpoint for the RD Gateway and RD Web Access ports.
   1. In the management portal, select the virtual machine, and click the ENDPOINT tab.
   2. On the bottom of the screen, click **Add Endpoint.**
   3. **Add an endpoint for the RD Gateway port and RD Web Access port if used. (Port 443 by default.)**

**Repeat the steps above for each of the virtual machines.**

High Availability Server Farm

A high availability server farm configuration consists of multiple virtual machines with the RDS role services configured for high availability. This configuration provides for redundant virtual machines that are load balanced so that users may continue to access the application as long as one of the servers hosting the role service is available. There are a number of possible configurations for this environment, the following are two possible configurations.

The first configuration example has all of the RDS role services deployed on two or more virtual machines connected together as a load balanced cloud service in Windows Azure. This provides a single public virtual IP address for load balanced user access to the RD Gateway and RD Web Access role services. Each machine also has an internal IP address for the RD Connection Broker and RD Session Host communications. In this configuration, all of the RDS role services are installed on each of the virtual machines. The RD Connection Broker is configured for high availability and will use a SQL Server database for session information. The RD Connection Broker is distributing the user sessions across the RD Session Host virtual machines.



Use the following steps to set up a high availability RDS server farm on load balanced Windows Azure Virtual Machines.

1. Create the virtual machines using a Windows Server 2008 R2 or Windows Server 2012 image template or a custom image. (Select to connect the 2nd and all additional virtual machines to the first virtual machine.)
2. In the Windows Azure Management Portal, select the first virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. If you already have a security certificate you will be using with the RD Gateway, then import the security certificate to the computer’s personal store.
   3. Open server manager and add the Remote Desktop Services role and role services.
   4. Configure Remote Desktop Services. (i.e. Configure certificates, Create Session Collection, Configure RD Connection Broker for high availability, etc.)

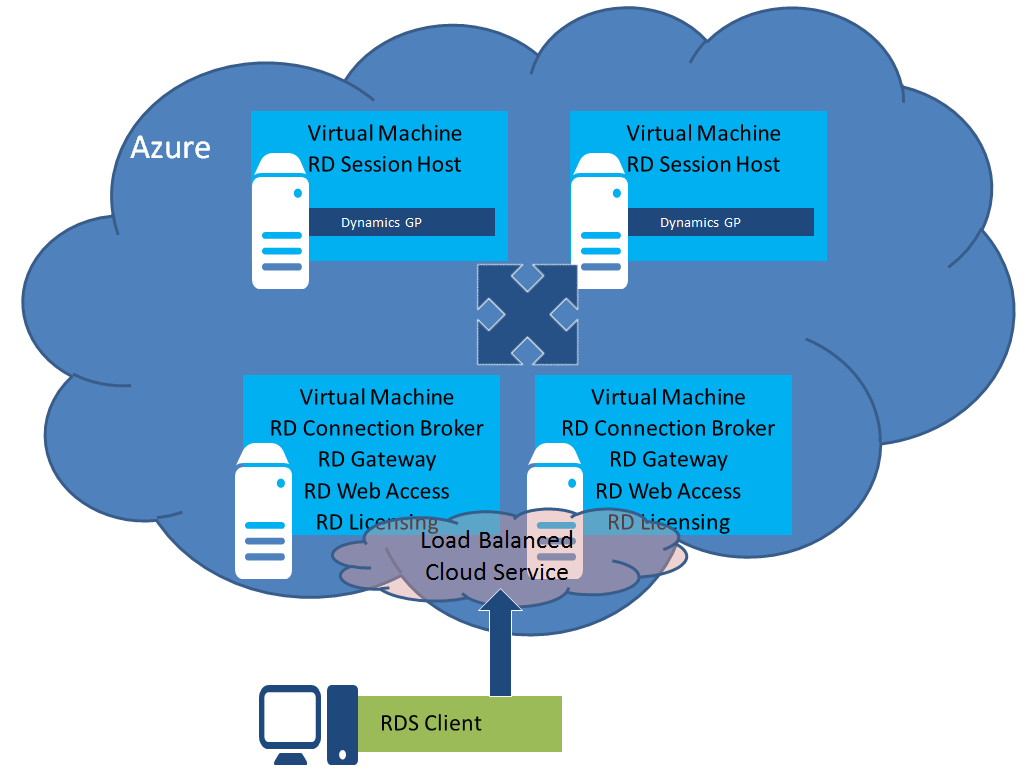
Note: When configuring the RD Connection Broker for high availability you will provide a load balanced address for the RD Connection Broker, it is suggested you don’t use the same domain name as the load balanced cloud service.

* 1. Install the Microsoft Dynamics GP components that require RDS to access by using the directions provided in the [[Microsoft Dynamics GP installation manual](http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx)[[47]](#footnote-47)](http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx).
  2. Configure the Microsoft Dynamics GP application component as a RemoteApp.

1. Add a public endpoint for the RD Gateway and RD Web Access ports.
   1. In the management portal, select the virtual machine, and click the ENDPOINT tab.
   2. On the bottom of the screen, click **Add Endpoint.**
   3. **Add an endpoint for the RD Gateway port and RD Web Access port if used. (Port 443 by default.)**
2. **Add an A record on your internal DNS for the RD Connection Broker load balanced address you provided during the setup of RD Connection Broker for high availability and the internal IP address of the virtual machine.**

**Repeat the steps above for each of the virtual machines.**

The second example has the RDS role services split up between two or more virtual machines connected together as a load balanced cloud service and two or more machines configured as stand-alone cloud services. This configuration is typically used in a deployment when you have a large number of application users that require many RD Session Hosts. The virtual machines that have the RD Gateway, RD Connection Broker, RD Licensing and RD Web Access role services installed will be connected together as a load balanced cloud service in Windows Azure. The RD Session Host role services are installed on virtual machines set up as stand-alone cloud services. The RD Connection Broker is distributing the user sessions across the RD Session Host virtual machines.



Use the following steps to set up a high availability RDS server farm on load balanced Windows Azure Virtual Machines.

1. Create the virtual machines using a Windows Server 2008 R2 or Windows Server 2012 image template or custom image. (Select to connect the 2nd and all additional virtual machines to the first virtual machine.)
2. In the Windows Azure Management Portal, select the first virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. If you already have a security certificate you will be using with the RD Gateway, then import the security certificate to the computer’s personal store.
   3. Open server manager and add the following Remote Desktop Services roles and role services to the server.
      1. RD Connection Broker
      2. RD Gateway
      3. RD Web Access
      4. RD Licensing
   4. Configure the installed services.
      1. Configure certificates for RD Gateway, RD Web Access and RD Connection Broker as needed.
      2. Configure RD Connection Broker for high availability.

Note: When configuring the RD Connection Broker for high availability you will provide a load balanced address for the RD Connection Broker, it is suggested you don’t use the same domain name as the load balanced cloud service.

1. Add a public endpoint for the RD Gateway and RD Web Access ports.
   1. In the management portal, select the virtual machine, and click the ENDPOINT tab.
   2. On the bottom of the screen, click **Add Endpoint.**
   3. **Add an endpoint for the RD Gateway port and RD Web Access port if used. (Port 443 by default.)**
2. **Add an A record on your internal DNS for the RD Connection Broker load balanced address you provided during the setup of RD Connection Broker for high availability and the internal IP address of the virtual machine.**

**Repeat the steps above for each of the virtual machines that will be configured with the high availability role services.**

Use the following steps to set up two or more Windows Azure Virtual Machines as stand-alone RD Session Host servers.

1. Create the virtual machines using a Windows Server 2008 R2 or Windows Server 2012 image template or custom image.
2. In the Windows Azure Management Portal, select the first virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. If you already have a security certificate you will be using with the RD Gateway, then import the security certificate to the computer’s personal store.
   3. Open server manager and add the RD Session Host role service.
   4. Install the Microsoft Dynamics GP components that require RDS to access by using the directions provided in the [[Microsoft Dynamics GP installation manual](http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx)[[48]](#footnote-48)](http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx).
   5. Configure the Microsoft Dynamics GP application component as a RemoteApp.

**Repeat the steps above for each of the virtual machines.**

## Configuring SharePoint Server

If you will be deploying Business Portal for Microsoft Dynamics GP or Workflow for Microsoft Dynamics GP, you will need to add one or more Windows Azure Virtual Machines with Microsoft SharePoint. Refer to the [SharePoint Deployment on Windows Azure Virtual Machines](http://www.windowsazure.com/en-us/manage/windows/other-resources/sharepoint-on-azure/)[[49]](#footnote-49) documentation for additional information. Use the following steps to set up the Windows Azure Virtual Machine with Microsoft SharePoint.

1. Create the virtual machine using a Windows Server 2008 R2 or Windows Server 2012 image template.
2. In the Windows Azure Management Portal, select the virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. Install and configure Microsoft SharePoint Foundation or Microsoft SharePoint Server using the directions provided in the [Business Portal](http://www.microsoft.com/en-us/download/details.aspx?id=13041)[[50]](#footnote-50) and [Workflow](http://www.microsoft.com/en-us/download/details.aspx?id=36071)[[51]](#footnote-51) installation manuals.
   3. Add an inbound rule for the SharePoint port to the virtual machines Windows firewall.
   4. Install Business Portal for Dynamics GP and/or Workflow for Dynamics GP using the installation manuals.
3. Add a public endpoint for the SharePoint port.
   1. In the Windows Azure Management Portal, select the virtual machine, and then click the **ENDPOINT** tab.
   2. On the bottom of the screen, click **Add Endpoint.**
   3. **Add an endpoint for the SharePoint port.**

## Configuring a Management Reporter Server

If you will be deploying Management Reporter for use with Microsoft Dynamics GP, you will need to install Management Reporter on a virtual machine in Windows Azure. The Management Reporter server components can be installed on the same machine as other Microsoft Dynamics GP server components or installed on a dedicated virtual machine. The Report Designer and Desktop Viewer client components will need to be installed on the Remote Desktop for Administration server so that end-users will be able to access them. If you will be using the Report Designer and Desktop Viewer client only for administrative purposes, they can be installed on the same virtual machine as the server components. Use the following steps when creating the Windows Azure Virtual Machine to host Management Reporter. Refer to the [Management Reporter Installation Guide](http://www.microsoft.com/en-us/download/details.aspx?id=5916)[[52]](#footnote-52) and [Management Reporter Integration Guide for Microsoft Dynamics GP](http://download.microsoft.com/download/7/8/A/78A3710A-9D72-4908-B302-CD54B5130096/DynGPDataProvInstGuide_ENUS.pdf)[[53]](#footnote-53) for additional information.

1. Create the virtual machine using a Windows Server 2008 R2 or Windows Server 2012 image template.
2. In the Windows Azure Management Portal, select the virtual machine. At the bottom of the screen, click **Connect. This will open a remote desktop connection to the virtual machine.**
   1. Join the virtual machine to the domain.
   2. Install and configure the Management Reporter Server using the instructions in the [Management Reporter Installation Guide](http://www.microsoft.com/en-us/download/details.aspx?id=5916).
   3. If you will be using the Management Reporter Client components on this server, follow the installation instructions in the [Management Reporter Installation Guide](http://www.microsoft.com/en-us/download/details.aspx?id=5916). If you will be using them on another server, open a remote desktop connection to that virtual machine and perform the installation.

# Part 4: Maintenance

Even though the Windows Azure platform is built to provide high availability and fault tolerance, there is still maintenance and backup procedures you will need to put in place for Microsoft Dynamics GP. The maintenance procedures will make sure that your Microsoft Dynamics GP system is at the most recent version, running correctly and with the best performance. The backup procedures will provide periodic backups of mission-critical data. This part contains the following sections.

* [Database Maintenance and Backups](#_Database_Maintenance_and) provides recommendations for creating scheduled database maintenance and backup processes.
* [Managing Virtual Machines](#_Managing_Virtual_Machines) provides information about changing the size, monitoring and patching the Windows Azure Virtual Machines.
* [Updating Microsoft Dynamics GP](#_Updating_Microsoft_Dynamics) provides information about updating the Microsoft Dynamics GP components to the latest release.

## Database Maintenance and Backups

The database maintenance and backup strategy to implement on Windows Azure will follow the same recommendations as an on-premise deployment. The recommendations include scheduled database maintenance tasks designed to keep the database running optimally and a database backup routine that allows recovery to a previous point in time, avoiding costly re-work. The frequency of the maintenance and backup procedures is determined based on your database activity and re-work tolerance.

The key difference in building your maintenance and backup procedures on Windows Azure versus on-premise is where the database backups will be stored. The recommended storage location for the database backups for a Windows Azure deployment is in Windows Azure blob storage. Windows Azure blob storage provides a number of safeguards for the data. The first is locally redundant storage (LRS). LRS maintains three copies of the account data within the primary data center. The second is g**eo-redundant storage (GRS),** which replicates the account data to a secondary data center in the same region. GRS functionality is implemented through a feature called geo-replication, which is turned on for a storage account by default, but can be turned off if you don’t want to use it. Refer to the [Windows Azure Storage](http://www.windowsazure.com/en-us/manage/services/storage/)[[54]](#footnote-54) page for information on creating and managing storage accounts. There are two options for creating backups in Windows Azure blob storage.

### Data Disk

A new empty data disk can be attached to the Windows Azure Virtual Machine that will be used to store the backup files. The data disk will be visible like any other local disk when setting up your maintenance plan. Select this disk as the backup file location when following the directions in the article [Microsoft Dynamics GP Database Maintenance](https://mbs.microsoft.com/Cms/Templates/document/General.aspx?NRMODE=Published&NRNODEGUID=%7b44C2D373-35BC-45E9-A86D-8A0E6E7C4B68%7d&NRORIGINALURL=%2fcustomersource%2fdocumentation%2fhowtodocuments%2fmsd_gpslinfodatabasemaintenanceplans%2ehtm%3fprintpage%3dfalse%26sid%3d32fkbo0uqxlevuxjp1hdidqm%26stext%3dDynamics%2520GP%2520database%2520backup&NRCACHEHINT=Guest&sid=32fkbo0uqxlevuxjp1hdidqm&printpage=false&stext=Dynamics%20GP%20database%20backup) for setting up a Microsoft Dynamics GP maintenance plan using the SQL Server Maintenance Plan Wizard.

### Backup Directly to Blob Storage

New functionality in Microsoft SQL Server 2012 SP1 CU2 provides the ability to backup directly to blob storage in Windows Azure. The number of data disks that can be attached is limited based on the virtual machine instance size, so using this approach will not require the use of a data disk attached to the virtual machine. There are currently a few restrictions on using this option from within SQL Server Management Studio. Refer to the article [SQL Server Backup and Restore with Windows Azure Blob Storage Service](http://msdn.microsoft.com/en-us/library/jj919148.aspx)[[55]](#footnote-55) for additional information.

## Managing Virtual Machines

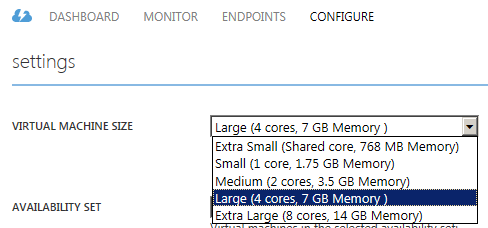
Windows Azure monitors the health of the hardware and network that the virtual machine instance is running on. It will automatically move the VHD when there is a failure. Windows Azure does not force operating system updates to running virtual machine instances. After the Windows Azure Virtual Machine instances are deployed, you are responsible for patching, configuring and maintaining the operating system and other software within your virtual machine instance.

Because a Windows Azure virtual machine instance is a Hyper-V image, you can use the same processes and tools to manage the virtual machine as you would on-premise. You are in complete control of the monitoring and patching process and are able to use familiar tools like Microsoft System Center and Windows Update to keep the operating system and other software running properly.

It is recommended that you use published best practices information when determining the approach to take for managing the Windows Azure Virtual Machines. The virtual machines containing the Microsoft Dynamics GP components should be set up to have updates applied during pre-determined maintenance windows to avoid service interruptions for users. By default the virtual machine instances created from the Windows Azure Platform Image Gallery are configured with Windows Update set to automatically install important Windows updates during a maintenance window configured for 3:00 AM on the virtual machine’s clock. It is recommended you evaluate this setting to verify that it fits into your desired maintenance process and adjust accordingly.

You may also want to change the virtual machine instance size as usage patterns change. Follow these steps to change the size of a virtual machine instance.

1. In the Windows Azure Management Portal, select the virtual machine, and then click the **CONFIGURE** tab.
2. Select the desired size from the Virtual Machine Size drop-down.



1. On the bottom of the screen, click **Save.**

Changing the size of a virtual machine will result in a re-deployment of the virtual machine. You will want to perform this procedure when no users are logged in and using Microsoft Dynamics GP or other software on the virtual machine.

## Updating Microsoft Dynamics GP

Updating Microsoft Dynamics GP on Windows Azure uses the same process as on-premise deployments. The Microsoft Dynamics GP product documentation and download site provides step-by-step instructions for performing the update. The following is a high-level checklist of the update process for Microsoft Dynamics GP.

1. Review the latest upgrade documentation and plan your upgrade.
2. Download the update from PartnerSource or CustomerSource.
3. Place the downloaded files in a share accessible by the virtual machines with Microsoft Dynamics GP components installed.
4. Make a backup of the Microsoft Dynamics GP databases.
5. Install the update onto each virtual machine that is running the Microsoft Dynamics GP Desktop Client installation.
6. Run Microsoft Dynamics GP Utilities to upgrade the databases.
7. Install updates to the remaining Microsoft Dynamics GP components.
8. Verify the update for each additional component.

# Part 5: Troubleshooting and Technical Support

This part contains information about troubleshooting and accessing technical support if unexpected application behavior occurs. It contains the following sections:

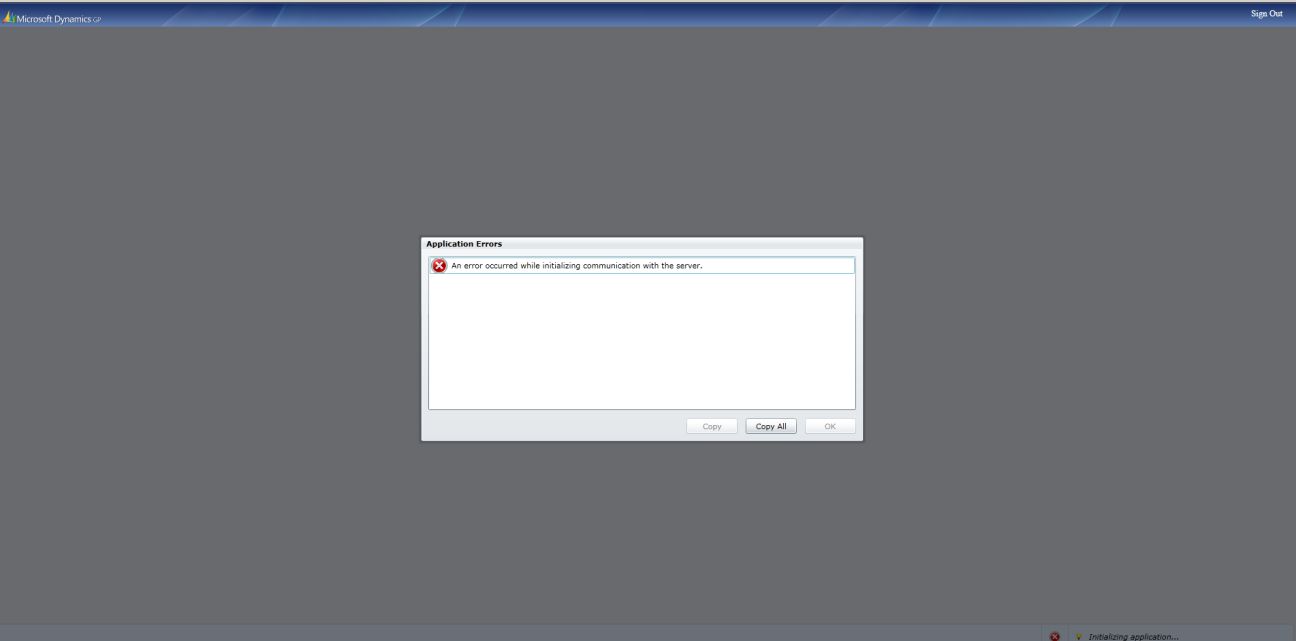
* [Troubleshooting](#_Chapter_1:_Troubleshooting) provides information on troubleshooting a Microsoft Dynamics GP on Windows Azure deployment.
* [Contacting Technical Support](#_Chapter_2:_Contacting) provides information on accessing Microsoft technical support.

## Troubleshooting

Troubleshooting Microsoft Dynamics GP on Windows Azure typically involves the same techniques that you would use for any Microsoft Dynamics GP deployment. The Microsoft Dynamics GP product documentation will serve as a good reference for identifying and resolving application issues. When troubleshooting on Windows Azure, you will need to account for unique communication errors that you may not have to consider in an on-premise deployment.

Depending on the virtual network configuration and where users will be accessing Microsoft Dynamics GP from, you may see issues related to communications not reaching the intended destination. When Microsoft Dynamics GP is deployed on-premise, the name resolution and communication routing from the user’s client computer to the Microsoft Dynamics GP servers is handled by your internal DNS and network configuration. Unless all users will be accessing Microsoft Dynamics GP from an on-premise network connected to the Windows Azure Virtual Network, the communication from the user’s client computer to Microsoft Dynamics GP in Windows Azure is handled by public DNS records and virtual machine endpoints.

An example of this type of issue is a user getting the following error when attempting to access the Microsoft Dynamics GP Web Client.



When you suspect that the error could be a communications issue, you will want to start by verifying that the virtual machine is running and accessible using the Windows Azure Management Portal. If the virtual machine is running and accessible, verify the following configuration settings are set correctly.

1. If you are using a custom domain name, verify that an A or CNAME record exists in DNS.
2. Verify that an endpoint has been created for the virtual machine if communication is originating from an external network.
3. If using SSL, verify that the custom domain name being used is covered by the security certificate.
4. Verify that there are appropriate inbound and outbound rules configured on the virtual machine’s Windows firewall for the TCP port that is being used.
5. Verify the TCP port being used is not blocked by a client-side firewall or proxy.

## Contacting Billing and Technical Support

If you need to contact Microsoft Support with technical or licensing (operations) questions, you need to be aware that there is different contact information for Microsoft Dynamics GP and Windows Azure. In order to expedite resolution of the issue you need to identify the type of question or issue you have in order to use the appropriate contact information. Use the information below to best identify which support organization to contact.

### Windows Azure

The following are examples of Windows Azure questions or issues. If you are experiencing any of the following types of issues you will want to contact Windows Azure support.

1. Billing questions for Windows Azure services.
2. Errors in the Windows Azure Management Portal.
3. Errors running Windows Azure PowerShell cmdlets.
4. Unable to open a remote desktop connection to a Windows Azure Virtual Machine.

If you have a billing-related question, open the [Windows Azure support option page](http://www.windowsazure.com/en-us/support/contact/)[[56]](#footnote-56) and select the **technical and billing support** option. You will need to log in using your Microsoft Account. Windows Azure billing support is provided at no cost.

If your question is about using Windows Azure, you have the following options for obtaining technical support. Refer to the [Windows Azure Support Plan](http://www.windowsazure.com/en-us/support/plans/)[[57]](#footnote-57) page for available plans and pricing information.

1. Online Forums – Open the [Forums page](http://www.windowsazure.com/en-us/support/forums/)[[58]](#footnote-58) to obtain assistance with your questions from the Windows Azure community.
2. Service Dashboard - Open the [Windows Azure support option page](http://www.windowsazure.com/en-us/support/contact/)[[59]](#footnote-59) and select the **Service dashboard** option to get the current health status of the Windows Azure platform and services.
3. Assisted Technical Support - Open the [Windows Azure support option page](http://www.windowsazure.com/en-us/support/contact/), If you are an existing Account holder – sign in using your Microsoft Account and create a support ticket.
4. If you have subscriptions that are not active, please contact [Microsoft Support](http://support.microsoft.com/)[[60]](#footnote-60).

### Microsoft Dynamics GP

The following are examples of Microsoft Dynamics GP questions or issues. If you are experiencing any of the following types of issues you will want to contact Microsoft Dynamics GP support.

1. Microsoft Dynamics GP licensing questions.
2. Errors while using Microsoft Dynamics GP.
3. Errors accessing Microsoft Dynamics GP on a server that is running and accessible using a remote desktop connection. Example: Get an error attempting to access the web client on the Web Server, but are able to open a remote desktop connection to the Web Server.

If your question is a licensing related question, contact the Dynamics Regional Operations Centers (ROCs). The Regional Operations Centers can be contacted on-line using the PartnerSource [Ordering](https://mbs.microsoft.com/partnersource/ordering/)[[61]](#footnote-61) or [Operations](https://mbs.microsoft.com/partnersource/GlobalOperationsSupportPage.htm)[[62]](#footnote-62) pages.

If your question or issue is about using Microsoft Dynamics GP, you have the following options for obtaining technical support.

1. Self-help Technical Support – Log onto [PartnerSource](https://mbs.microsoft.com/partnersource/default)[[63]](#footnote-63), click Support and then Knowledge Base to search for articles on your question or issue.
2. Assisted Technical Support - Log onto [PartnerSource](https://mbs.microsoft.com/partnersource/default), click Support and then New Technical Support Request to create a request to speak with a support engineer.
3. Partner Network – Access the **Get Support** page on the [Microsoft Partner Network (MPN)](https://mspartner.microsoft.com/en/us/Pages/Support/get-support.aspx)[[64]](#footnote-64).



1. <http://msdn.microsoft.com/en-us/library/windowsazure/hh531793.aspx> [↑](#footnote-ref-1)
2. <https://account.windowsazure.com/Home/Index> [↑](#footnote-ref-2)
3. <http://www.windowsazure.com/en-us/support/plans/> [↑](#footnote-ref-3)
4. <http://www.windowsazure.com/en-us/pricing/licensing-faq/> [↑](#footnote-ref-4)
5. <http://www.windowsazure.com/en-us/pricing/license-mobility/> [↑](#footnote-ref-5)
6. <https://mbs.microsoft.com/partnersource/pricing/announcements/MSDNAVGP2013LicensingGuide.htm> [↑](#footnote-ref-6)
7. <http://www.microsoft.com/licensing/about-licensing/product-licensing.aspx> [↑](#footnote-ref-7)
8. <http://www.windowsazure.com/en-us/support/understand-your-bill/> [↑](#footnote-ref-8)
9. <http://www.windowsazure.com/en-us/support/trust-center/> [↑](#footnote-ref-9)
10. <http://www.microsoft.com/en-us/download/details.aspx?id=26647> [↑](#footnote-ref-10)
11. <http://www.windowsazure.com/en-us/support/legal/privacy-statement/> [↑](#footnote-ref-11)
12. The Microsoft Dynamics GP desktop client can be used for end-user access through Remote Desktop Services if you have a Subscriber Access License. The Microsoft Dynamics GP desktop client can be used for administrative purposes with Remote Desktop for Administration. [↑](#footnote-ref-12)
13. If the application that is using eConnect requires Remote Desktop Services for end-user access, then a Subscriber Access License is required. If access is for administrators only, then Remote Desktop for Administration can be used. [↑](#footnote-ref-13)
14. Excel reports connect directly to the Microsoft Dynamics GP databases. Because the SQL Server is not exposed to the Internet, the Excel reports must be run from a computer connected to the Windows Azure Virtual Network. This means that Microsoft Excel to be run on a Remote Desktop Services server or from a computer on the network connected to the Windows Azure Virtual Network. [↑](#footnote-ref-14)
15. Integration Manager can be used for end-user access through Remote Desktop Services if you have a Subscriber Access License. Integration Manager can be used for administrative purposes with Remote Desktop for Administration. [↑](#footnote-ref-15)
16. Analysis Cubes reports connect directly to the Microsoft Dynamics GP databases. Because the SQL Server is not exposed to the Internet, the Analysis Cubes reports must be run from a computer connected to the Windows Azure Virtual Network. [↑](#footnote-ref-16)
17. The Management Reporter report designer and desktop viewer can be used for end-user access with a Subscriber Access License for Remote Desktop Services. The Management Reporter report designer and desktop viewer can be used for administrative purposes with Remote Desktop for Administration. The Web Viewer can be used by all end-users to view reports. [↑](#footnote-ref-17)
18. ISV products must be evaluated on a product-by-product basis. [↑](#footnote-ref-18)
19. <http://www.windowsazure.com/en-us/pricing/overview/?fb=en-us> [↑](#footnote-ref-19)
20. <http://technet.microsoft.com/en-us/library/jj673201(v=gp.20).aspx> [↑](#footnote-ref-20)
21. <http://www.windowsazure.com/en-us/manage/windows/common-tasks/manage-vm-availability/> [↑](#footnote-ref-21)
22. <http://msdn.microsoft.com/library/windowsazure/jj870962.aspx> [↑](#footnote-ref-22)
23. <http://msdn.microsoft.com/en-us/library/windowsazure/hh543978.aspx> [↑](#footnote-ref-23)
24. <http://msdn.microsoft.com/en-us/library/windowsazure/hh531560.aspx> [↑](#footnote-ref-24)
25. <http://msdn.microsoft.com/en-us/library/windowsazure/jj156007.aspx> [↑](#footnote-ref-25)
26. <http://msdn.microsoft.com/en-us/library/windowsazure/jj156088.aspx> [↑](#footnote-ref-26)
27. <http://www.windowsazure.com/en-us/manage/services/networking/create-a-virtual-network/> [↑](#footnote-ref-27)
28. <http://msdn.microsoft.com/en-us/library/windowsazure/jj156097.aspx> [↑](#footnote-ref-28)
29. <http://msdn.microsoft.com/en-us/library/windowsazure/jj156003.aspx> [↑](#footnote-ref-29)
30. <http://www.windowsazure.com/en-us/manage/windows/tutorials/virtual-machine-from-gallery/> [↑](#footnote-ref-30)
31. <http://www.windowsazure.com/en-us/develop/net/common-tasks/custom-dns/> [↑](#footnote-ref-31)
32. <http://msdn.microsoft.com/en-us/library/windowsazure/jj156090.aspx> [↑](#footnote-ref-32)
33. <http://www.windowsazure.com/en-us/manage/services/networking/active-directory-forest/> [↑](#footnote-ref-33)
34. <http://www.windowsazure.com/en-us/manage/services/networking/replica-domain-controller/> [↑](#footnote-ref-34)
35. <http://msdn.microsoft.com/en-us/library/windowsazure/dn248436.aspx> [↑](#footnote-ref-35)
36. <http://www.microsoft.com/en-us/download/details.aspx?id=34669> [↑](#footnote-ref-36)
37. <http://www.microsoft.com/en-us/download/details.aspx?id=34669> [↑](#footnote-ref-37)
38. <http://msdn.microsoft.com/en-us/library/windowsazure/jj992719.aspx> [↑](#footnote-ref-38)
39. <http://www.microsoft.com/en-us/download/details.aspx?id=34669> [↑](#footnote-ref-39)
40. <http://technet.microsoft.com/en-us/library/ms345223(v=sql.110).aspx> [↑](#footnote-ref-40)
41. <http://technet.microsoft.com/en-us/library/cc787484(v=WS.10).aspx> [↑](#footnote-ref-41)
42. <http://www.microsoft.com/en-pk/download/details.aspx?id=34672> [↑](#footnote-ref-42)
43. <http://www.microsoft.com/en-pk/download/details.aspx?id=34672> [↑](#footnote-ref-43)
44. <http://www.microsoft.com/licensing/about-licensing/product-licensing.aspx> [↑](#footnote-ref-44)
45. <http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx> [↑](#footnote-ref-45)
46. <http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx> [↑](#footnote-ref-46)
47. <http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx> [↑](#footnote-ref-47)
48. <http://technet.microsoft.com/en-us/library/jj673202(v=gp.30).aspx> [↑](#footnote-ref-48)
49. <http://www.windowsazure.com/en-us/manage/windows/other-resources/sharepoint-on-azure/> [↑](#footnote-ref-49)
50. <http://www.microsoft.com/en-us/download/details.aspx?id=13041> [↑](#footnote-ref-50)
51. <http://www.microsoft.com/en-us/download/details.aspx?id=36071> [↑](#footnote-ref-51)
52. <http://www.microsoft.com/en-us/download/details.aspx?id=5916> [↑](#footnote-ref-52)
53. <http://download.microsoft.com/download/7/8/A/78A3710A-9D72-4908-B302-CD54B5130096/DynGPDataProvInstGuide_ENUS.pdf> [↑](#footnote-ref-53)
54. <http://www.windowsazure.com/en-us/manage/services/storage/> [↑](#footnote-ref-54)
55. <http://msdn.microsoft.com/en-us/library/jj919148.aspx> [↑](#footnote-ref-55)
56. <http://www.windowsazure.com/en-us/support/contact/> [↑](#footnote-ref-56)
57. <http://www.windowsazure.com/en-us/support/plans/> [↑](#footnote-ref-57)
58. <http://www.windowsazure.com/en-us/support/forums/> [↑](#footnote-ref-58)
59. <http://www.windowsazure.com/en-us/support/contact/> [↑](#footnote-ref-59)
60. <http://support.microsoft.com/> [↑](#footnote-ref-60)
61. <https://mbs.microsoft.com/partnersource/ordering/> [↑](#footnote-ref-61)
62. <https://mbs.microsoft.com/partnersource/GlobalOperationsSupportPage.htm> [↑](#footnote-ref-62)
63. <https://mbs.microsoft.com/partnersource> [↑](#footnote-ref-63)
64. <https://mspartner.microsoft.com/en/us/Pages/Support/get-support.aspx> [↑](#footnote-ref-64)