Guardian Instance Setup Document

Version 2.0

# Contents

[Contents 2](#_Toc422833025)

[Prerequisites 4](#_Toc422833026)

[Technology Stack 6](#_Toc422833027)

[System/ Cloud Role Configurations 7](#_Toc422833028)

[Setting up Infrastructure 8](#_Toc422833029)

[Cloud Service (For Portal, Services and Worker Role) 8](#_Toc422833030)

[Azure Storage 8](#_Toc422833031)

[Azure SQL Server Creation 8](#_Toc422833032)

[Event Hub Creation 8](#_Toc422833033)

[Deployment 9](#_Toc422833034)

[Pre-Deployment Steps 9](#_Toc422833035)

[Configuration Changes 9](#_Toc422833036)

[ServiceConfiguration Keys 9](#_Toc422833037)

[GConfig Keys 12](#_Toc422833038)

[Constants Fields 12](#_Toc422833039)

[Deployment Steps 13](#_Toc422833040)

[Post-Deployment Steps 13](#_Toc422833041)

[ Setup Groups and Sub Groups/ Circles 13](#_Toc422833042)

[Technical Validations 13](#_Toc422833043)

[Functional Validations 13](#_Toc422833044)

[Publishing Apps to App store 14](#_Toc422833045)

[Windows App Store 14](#_Toc422833046)

[Google Play Store 14](#_Toc422833047)

[Apple Store 14](#_Toc422833048)

[APPENDIX A - **HOW TO: Create Cloud Services** 15](#_Toc422833049)

[APPENDIX B - **HOW TO: Create Azure Storage Account** 16](#_Toc422833050)

[APPENDIX C - **HOW TO: Create Azure SQL Database** 19](#_Toc422833051)

[APPENDIX D - **HOW TO: Create Event Hubs** 21](#_Toc422833052)

[APPENDIX E - **HOW TO: Upload Certificates** 22](#_Toc422833053)

[APPENDIX F - **HOW TO: Deploy Cloud Service** 23](#_Toc422833054)

[APPENDIX G - **HOW TO: Upgrade Database** 25](#_Toc422833055)

[APPENDIX H - **HOW TO: Auto Scale-up and Scale-down setup** 26](#_Toc422833056)

[APPENDIX I - **HOW TO Generate Different Keys** 28](#_Toc422833057)

# Prerequisites

1. Procure Microsoft Azure Cloud Subscription
   1. <https://manage.windowsazure.com> (or)
   2. <https://portal.azure.com>
2. Create domains for below in the nearest region/ data center to the user base
   1. Guardian Portal
   2. Guardian Service
   3. Guardian Worker Role
3. Procure two separate certificates(both .cer and .pfx files) for Portal and Service domains
4. Procure Licenses for the below

|  |  |
| --- | --- |
|  |  |
| Azure Subscription | <http://www.windowsazure.com>  Pay-as-you-use - **~400$ for Small Instance** |
| SMS | VFirst  <http://www.vfirst.com/#connect>  Prepaid/ Pay-as-you-use  Charge per SMS(India) – 0.15-0.2 INR based on the bulk purchase/ usage |
| Email | <https://sendgrid.com>  Pay-as-you-use - Free account - 400 emails/ day  $10 account – 40,000 emails/ month |
| Bing Map | <https://www.bingmapsportal.com/Application> |
| Live Authentication | <https://account.live.com/developers/applications/index> |
| ~~Google Search API~~  ~~[Optional]~~ | [~~https://console.developers.google.com~~](https://console.developers.google.com)  [~~https://developers.google.com/places/webservice/usage~~](https://developers.google.com/places/webservice/usage) |
| Google Authentication++ | <https://developers.google.com/web/> |
| 2 SSL certificates  [Optional] – Can be self-signed certs, if data is not HBI | <http://www.digicert.com>  <https://www.digicert.com/welcome/ssl-plus.htm>  139-175$/ year |
| WP Publisher Account | <https://dev.windows.com/en-us/programs/join> - 20$  <https://appdev.microsoft.com/StorePortals/en-US/Account/Signup/SelectAccountType> |
| Android Publisher Account | <https://play.google.com/apps/publish/signup/> - 25$ |
| iOS Publisher Account | <https://developer.apple.com/programs/enroll/> - 99$/ year |

\* - These services are free as of now/ as per the thresholds

++ - This feature is yet to be implemented

1. Create Page for the App in Facebook and create an app. Make a note of App ID which will be used in Devices(WP/Android/iOS) configurations in code
2. Detailed steps of procuring licenses are listed in the below document



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Component** | **Role Size** | **No. of Instances** | **Pricing** | **Recommended Size**  **For medium user base** | **Recommended Size**  **For large user base** | **Comments** |
| Guardian Portal | Medium/ A2 | 1 | $119 | A2 – 2 Instances | A2 – 3 Instances | Based on size of user base, instances should be increased on need basis(Auto scaling) |
| Guardian Services | Medium/ A2 | 2 | $238 | A2 – 2 Instances | A2 – 3 Instances |
| Message Broadcaster | Small/ A1 | 1 | $60 | A2 – 1 Instances | A2 – 1 Instances |  |
| Azure SQL Database | S0 | 2GB | $15 | S2 | S3 | For large user base, recommended to go to Premium tiers |
| Storage + Transactions | 10GB |  | $10 |  |  |  |
| Event Hubs |  |  | In preview |  |  |  |
| SMS+Email |  |  | Based on usage |  |  |  |
| **Total** |  |  | $442 per Month |  |  |  |

# Technology Stack

* .NET 4.5
* Azure SDK 2.5
* Devices Tech Stack
  + Windows Phone 8 - XAML
  + Android(Kitkat – Jellybean) - Java 7
  + iOS(4-6) - Object C
* Microsoft Azure Cloud
  + Web Roles
  + Worker Roles
  + Event Hubs
  + Azure Storage – Tables, Blobs
  + SQL Azure
* Windows Live Authentication aka Microsoft Account
* BING Maps
* Bing Search API
* Facebook App
* AutoMapper

**Tools:**

* SSMS
* Azure Powershell
* Azure Storage Explorer

# System/ Cloud Role Configurations

|  |  |  |
| --- | --- | --- |
| **Component** | **Name** | **Role Size** |
| Guardian Portal | https://<PortalDomain>.cloudapp.net | Cloud Service / Medium |
| Guardian Services | https://<ServiceDomain>.cloudapp.net | Cloud Service / Medium |
| Message Broadcaster | https://<PortalDomain>.cloudapp.net | Cloud Service / Medium |
| Azure SQL Database | Guardian |  |
| Storage + Transactions | GuardianStorage<Name>  GuardianDiagnostics<Name> |  |
| Event Hubs | Guardian<Name>EventHub |  |

Referred to as: Table 1.0

# Setting up Infrastructure

## Cloud Service (For Portal, Services and Worker Role)

* Create three Cloud Services for Guardian Portal, Guardian Services and Guardian Worker as per the **Table 1.0**
* Select the appropriate configurations and region/ data center
* Upload respective certificates to Portal and Service Cloud Services

For detailed steps on How to create Cloud Services and Upload certificates, see **APPENDIX A** and **APPENDIX E**

## Azure Storage

In Azure Management Portal, create two Storage accounts for Guardian Storage and Diagnostics. Provide the names as per the **Table 1.0**

Make note of the Storage Keys.

For detailed step-by-step instructions to create Storage Account and obtain keys, refer **APPENDIX B**

## Azure SQL Server Creation

In Azure Management Portal, create a Database. Provide the name for the Database as per the **Table 1.0**

Make note of the SQL Connection String

For detailed step-by-step instructions to create Database and SQL Database Server and obtain Connection String, refer **APPENDIX C**

## Event Hub Creation

In Azure Management Portal, create Event Hub under Service Bus. Provide the name for the Event Hub as per the **Table 1.0**

Make note of the Event Hub Connection String

For detailed step-by-step instructions to create Event Hubs, see **APPENDIX D**

# Deployment

## Pre-Deployment Steps

## Configuration Changes

Before setting up as the new instance/deployment to the Azure environment, following changes in the configuration files need to be done.

Configure with new key values in files.

#### a. ServiceConfiguration.cscfg

(Following files are available under **HOST\SOS.AzurePortalHost , HOST\SOS.AzureServiceHost and HOST\SOS.AzureWorkerRoleHost)**

#### b. gconfig.js

(File is located at project **Web\Scripts\js**)

#### c. Config.cs

(File is located in **Phone\UtilityClasses**)

### ServiceConfiguration Keys



QueueConnection = DefaultEndpointsProtocol=https;AccountName= GuardianStorage<Name>;AccountKey= XXXXXXXXXXX<Replace with Primary Access Key of Storage account>

TableConnection = DefaultEndpointsProtocol=https;AccountName= GuardianStorage<Name>;AccountKey=XXXXXXXXXXX<Replace with Primary Access Key of Storage account>

BlobConnection = DefaultEndpointsProtocol=https;AccountName= GuardianStorage<Name>;AccountKey= XXXXXXXXXXX<Replace with Primary Access Key of Storage account>

AzureSQLConnectionString = <ADO.NET SQL Connection String>

Management Portal🡪SQL Databases🡪Dashboard🡪Show Connection strings

EventHubConnectionString = <Event Hub Connection String>

EventHubName = LiveLocations

SMSDefaultFromnumber = <Provide the Name SMS provider supplies>

GuardianPortalUri = https://guardianportal<Name>.cloudapp.net

ClientSecret = <LiveAuth Client Secret>,<LiveAuth Client Secret>

\*Two times need to mention the same Client Secret Key

\* Refer Appendix I

BingKey = <Refer Appendix I>

LiveAppUri = guardianportal<Name>.cloudapp.net

RandomNumberDigits = 5

SMSPostGap = 15

FacebookPostGap = 15

EmailPostGap = 15

SendSms = True

UseEventHubs = True

SMSServiceUserID = XXXXXXX

SMSServicePassword = XXXXXXX

sendGridUserID = XXXXXXX

sendGridPassword = XXXXXXX

#### **Other operational configurations:**

SubGroupAllocationIntervalInMinutes = 5

BroadcastRunIntervalInSeconds = 60

ArchiveTimeGapInMinutes = 240

ArchiveRunIntervalInMinutes = 10

TinyServiceUri = http://tinyurl.com/api-create.php

#### **Communication Message Configurations:**

SMSMessage = {name} ({phone}) needs urgent help at {address}. Track at {tinyuri}

SMSSafeMessage = {name} is safe now.

EmailSubject = Guardian SOS: {name} needs urgent help!

EmailMessage = Hello, &lt;br&gt; &lt;br&gt; {name} (Mobile No {phone}) needs urgent help at {address}. Track at {tinyuri} and help urgently. &lt;br&gt;&lt;br&gt; Thanks,&lt;br&gt;Guardian Team&lt;br&gt;&lt;br&gt;&lt;br&gt;\*\*This email is sent from an unmonitored alias. If you can’t provide help, try reaching appropriate authorities for help.\*\*&lt;br&gt;

EmailSafeSubject = Guardian SOS: {name} is safe now!

EmailSafeMessage = Hello, &lt;br&gt; &lt;br&gt; {name} (Mobile No {phone}) is safe now. &lt;br&gt; &lt;br&gt; Thanks,&lt;br&gt; Guardian Team &lt;br&gt; &lt;br&gt; &lt;br&gt;\*\*This email is sent from an unmonitored alias. If you can’t provide help, try reaching appropriate authorities for help.\*\*&lt;br&gt;

FacebookSubject = Guardian SOS: {name} needs urgent help!

FacebookSafeSubject = Guardian SOS: {name} is safe now!

FacebookMessage = {name} (Mobile No {phone}) needs urgent help at {address}. Track at {tinyuri} and help urgently.

FacebookSafeMessage = {name} is safe now.

PhoneValidationSMS = Please enter {0} verification code to create your Profile for phone number ending with {1}

PhoneReValidationSMS = Please enter {0} verification code to create your Profile for phone number ending with {1}

EmailGroupValidationSubj = Activate your Group validation for Guardian

EmailGroupValidationMsgTmp = Hi, &lt;br&gt; &lt;br&gt;Please click the below link to validate your Guardian group association. &lt;br&gt; &lt;br&gt; Validation Link: https://GuardianPortal<Name>.cloudapp.net/verification.aspx?key={0}&amp;pr={1}&amp;et=G &lt;br&gt; &lt;br&gt; Thanks,&lt;br&gt;-Guardian Team &lt;br&gt;\*\*This email is sent from an unmonitored alias.\*\*&lt;br&gt; &lt;br&gt;

EmailMarshalValidationMsgTmp = Hi, &lt;br&gt;&lt;br&gt;Please click the bollowing link to confirm yourself as Guardian group marshal. &lt;br&gt;&lt;br&gt; Validation Link: https://GuardianPortal<Name>.cloudapp.net/verification.aspx?key={0}&amp;pr={1}&amp;et=M &lt;br&gt;&lt;br&gt; Thanks,&lt;br&gt;-Guardian Team &lt;br&gt;\*\*This email is sent from an unmonitored alias.\*\*&lt;br&gt;&lt;br&gt;

EmailMarshalValidationSubj = Guardian marshal confirmation

BuddyNotificationSMSBody = {0}({1}) added you as a buddy in Guardian App. To unsubscribe, click {2}

BuddyNotificationEmailBody = Hi,&lt;br&gt; &lt;br&gt;{0}({1}) has added you as a buddy in Guardian for receiving SOS notifications and Tracking.&lt;br&gt;If you wish not to receive notifications for this user, click below link to unsubscribe &lt;br&gt; {2} &lt;br&gt;&lt;br&gt;Thanks, &lt;br&gt;-Guardian Team &lt;br&gt;\*\*This email is sent from an unmonitored alias.\*\*

BuddyNotificationEmailSubject = Buddy addition in Guardian for {0}({1})

UnRegisterNotificationEmailSubject = Profile unregistered in Guardian

UnRegisterNotificationEmailBody = Hi,&lt;br&gt; &lt;br&gt;You have unregistered yourself from Guardian App. We have ensured to delete your profile from our servers.&lt;br&gt;Please be informed that Guardian works best when you use it as a registered user. &lt;br&gt;&lt;br&gt;Thanks, &lt;br&gt;-Guardian Team &lt;br&gt;\*\*This email is sent from an unmonitored alias.\*\*

<Certificate name="PortalCert" thumbprint=<Get this from Azure portal for the created web portal> thumbprintAlgorithm="sha1</Certificates>

### Portal GConfig Keys

LiveClientID: "000000XXXXXXXX4A1",

MapCredentials: "AqtaE18u0YgWQjcXXXXXXXXXXXXXXXXXXXXXXXXX3LBPIVl6utemHKIzv",

For the above keys to generate, Please refer Appendix I.

PortalUrl: http://guardianportal<name>.cloudapp.net/default.aspx

### Apps Config Fields

~~public static string FBAppID = "8637XXXXX02300";~~

~~public static string FBAppSecret = "86a53aaa7XXXXXXXXXX2ccba91b3";~~

public const string LiveAuthClientId = "000000XXXXXX4A1";

For the above keys to generate, Please refer Appendix I.

public static string GuardianServiceUrl = "http://guardianservice<name>.cloudapp.net/";<Map to newly created web service URL>

public static string GuardianPortalUrl = "https://guardianportal<name>.cloudapp.net/";<Map to newly created web portal URL>

## Deployment Steps

**Cloud Services:**

Package the three projects from Host projects. You will get below two files

Package File - <Project Name>.cspkg

Configuration File - ServiceDefinition.cscfg

Upload via Azure Management Portal to respective Cloud Services

Alternatively, publish from Visual Studio 2013 with Azure SDK installed.

* Run the Projects and with the Option “Publish to Azure” complete the deployment to respective newly created Cloud services and Storages.

For detailed steps, see **APPENDIX F**

**Database**:

Use Database upgrade wizard to upgrade the Database using GuardianDatabase.dacpac file. For detailed steps, check **APPENDIX G**

## Post-Deployment Steps

### Setup Groups and Sub Groups/ Circles

Follow the below document to Create Groups, Sub Groups and their Admin User accounts



## Technical Validations

<TBD>

## Functional Validations

<TBD>

# Publishing Apps to App store

## Windows App Store



## Google Play Store

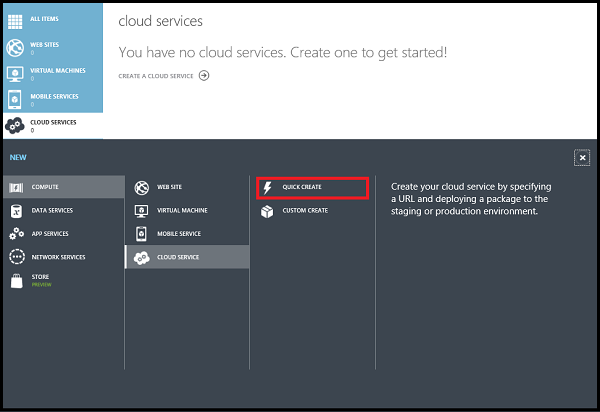


## Apple Store

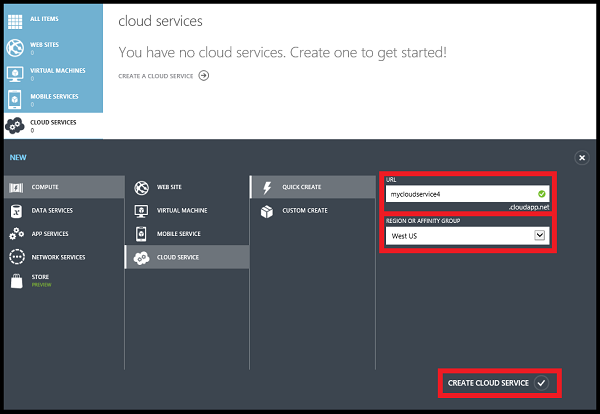


# APPENDIX A - **HOW TO: Create Cloud Services**

1. In the [Management Portal](http://manage.windowsazure.com/), click **New**>**Compute**>**Cloud Service**>**Quick Create**.

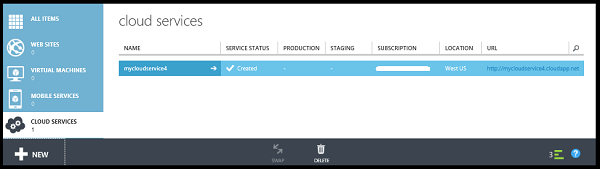


1. In **URL**, enter a subdomain name to use in the public URL for accessing your cloud service in production deployments. The URL format for production deployments is: http://myURL.cloudapp.net.
2. In **Region or Affinity Group**, select the geographic region or affinity group to deploy the cloud service to. Select an affinity group if you want to deploy your cloud service to the same location as other Azure services within a region.
3. Click **Create Cloud Service**.



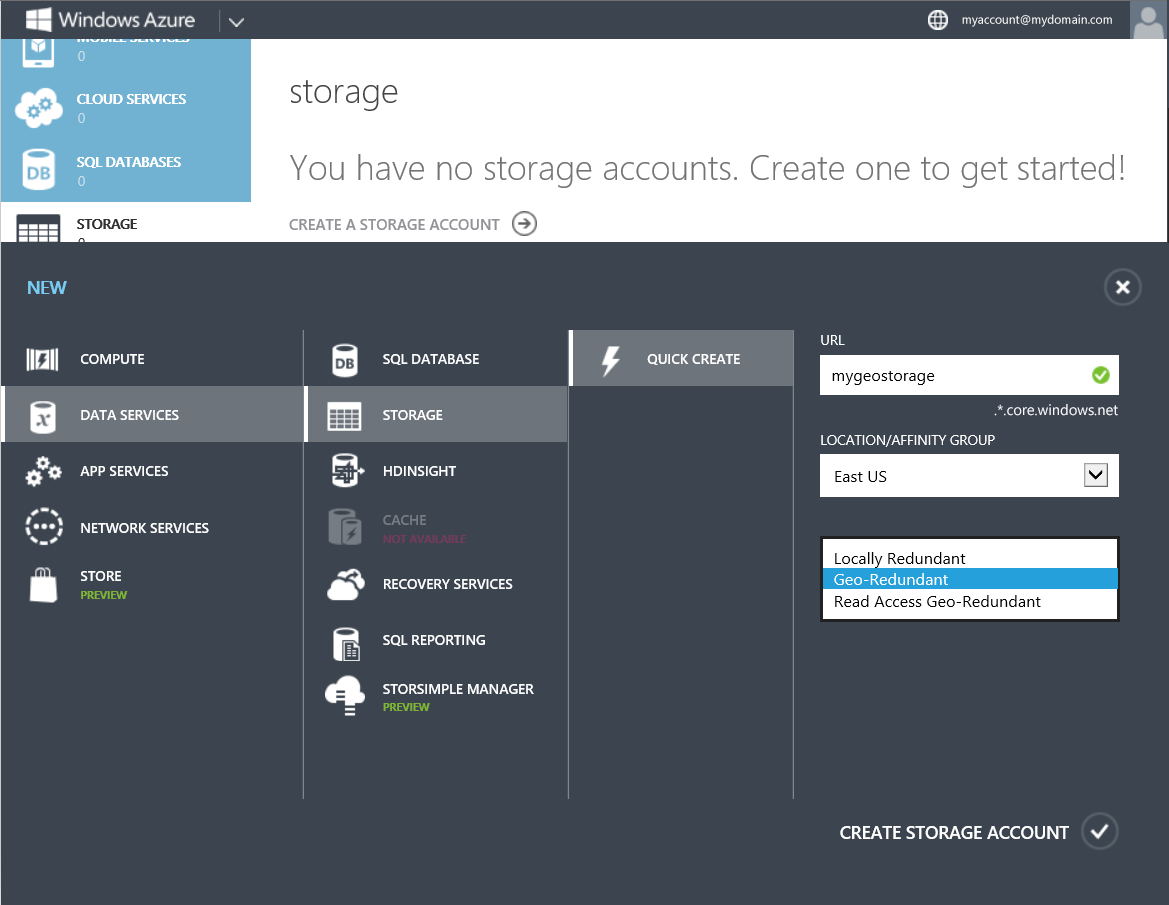
You can monitor the status of the process in the message area at the bottom of the window.

The **Cloud Services** area opens, with the new cloud service displayed. When the status changes to Created, cloud service creation has completed successfully.



# APPENDIX B - **HOW TO: Create Azure Storage Account**

1. Sign in to the [Management Portal](https://manage.windowsazure.com/).
2. Click **Create New**, click **Storage**, and then click **Quick Create**.



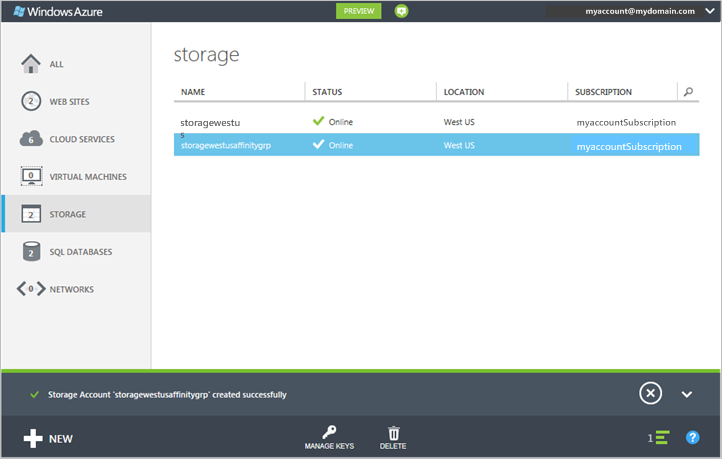
1. In **URL**, enter a name for your storage account. See [Storage account endpoints](http://azure.microsoft.com/en-in/documentation/articles/storage-create-storage-account/#account-endpoints) below for details about how this name will be used to address objects that you store in Azure Storage.
2. In **Location/Affinity Group**, select a location for your storage account that is close to you or to your customers. If data in your storage account will be accessed from another Azure service, such as an Azure virtual machine or cloud service, you may want to select an affinity group from the list to group your storage account in the same data center with other Azure services that you are using to improve performance and lower costs.

**Note:** Note that you must select an affinity group when your storage account is created; you cannot move an existing account to an affinity group.

For details about affinity groups, see [Service co-location with an affinity group](http://azure.microsoft.com/en-in/documentation/articles/storage-create-storage-account/#affinity-group) below.

1. If you have more than one Azure subscription, then the **Subscription** field is displayed. In **Subscription**, enter the Azure subscription that you want to use the storage account with. You can create up to five storage accounts for a subscription.
2. In **Replication**, select the desired level of replication for your storage account. The recommended replication option is Geo-Redundant replication, which provides maximum durability for your data. For more details on Azure Storage replication options, see [Storage account replication options](http://azure.microsoft.com/en-in/documentation/articles/storage-create-storage-account/#replication-options) below.
3. Click **Create Storage Account**.

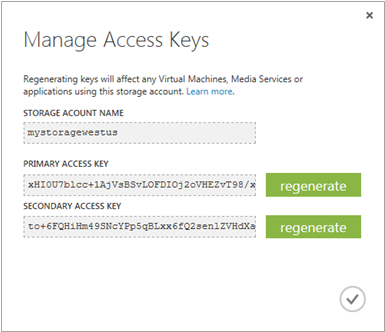
It may take a few minutes to create your storage account. To check the status, you can monitor the notifications at the bottom of the portal. After the storage account has been created, your new storage account has **Online** status and is ready for use.



You can use **Manage Keys** to copy a storage access key to use in a connection string. The connection string requires the storage account name and a key to use in authentication. For information about configuring connection strings to access Azure storage services, see [Configuring Connection Strings](http://msdn.microsoft.com/en-us/library/ee758697.aspx).

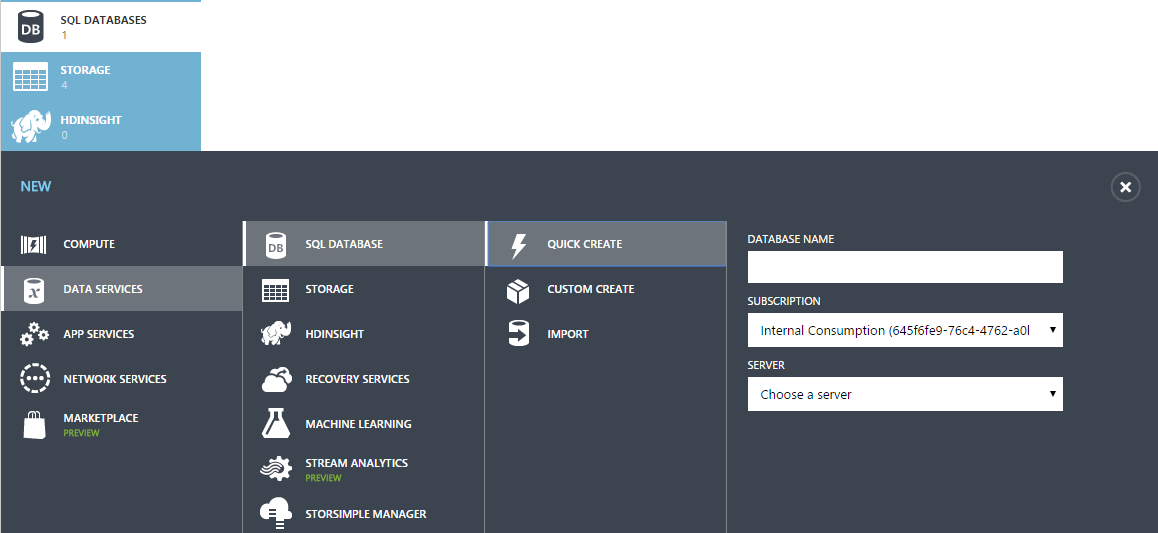
1. In the [Management Portal](http://manage.windowsazure.com/), click **Storage**, and then click the name of the storage account to open the dashboard.
2. Click **Manage Keys**.

**Manage Access Keys** opens.

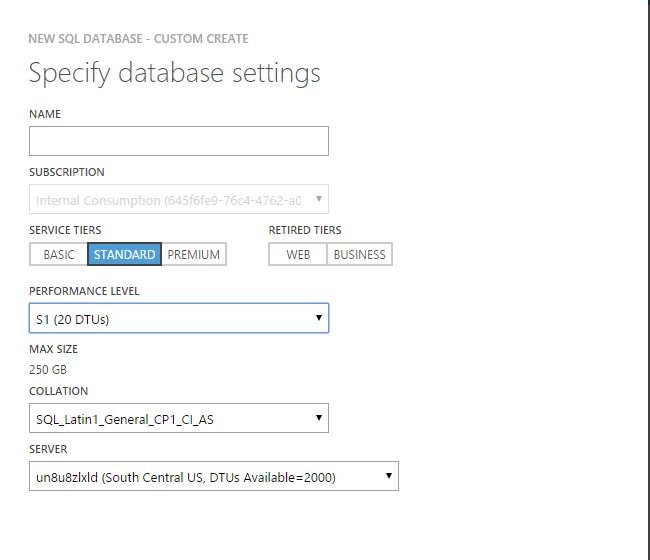


# APPENDIX C - **HOW TO: Create Azure SQL Database**

1. Sign in to the [Management Portal](https://manage.windowsazure.com/).
2. Click **Create New -> DATA SERVICES**, click **SQL Database**, and then click **Quick Create**.

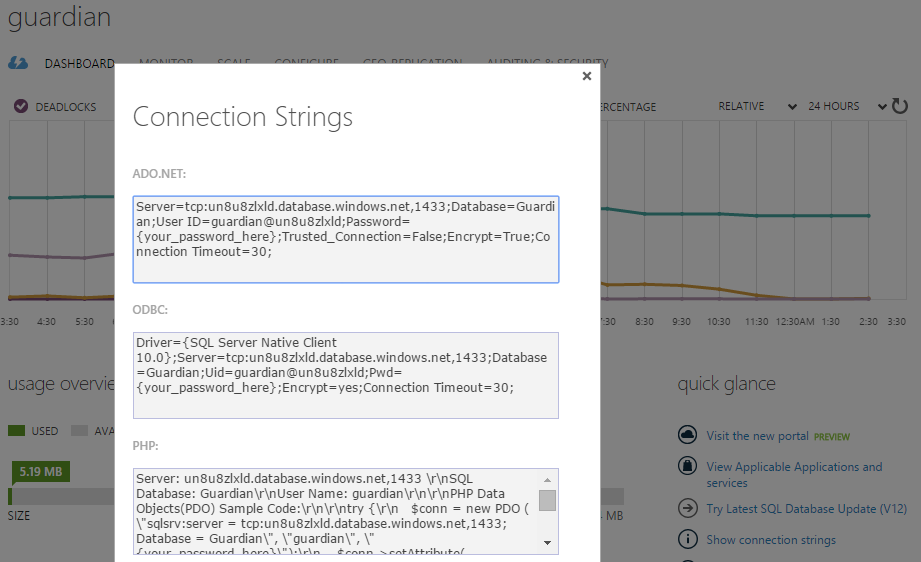


1. Provide Database Name
2. Select the Subscription
3. Select option to ‘Create new SQL Database Server’ for the ‘Server’ dropdown.
4. Select Standard - S0 or above Service Tier



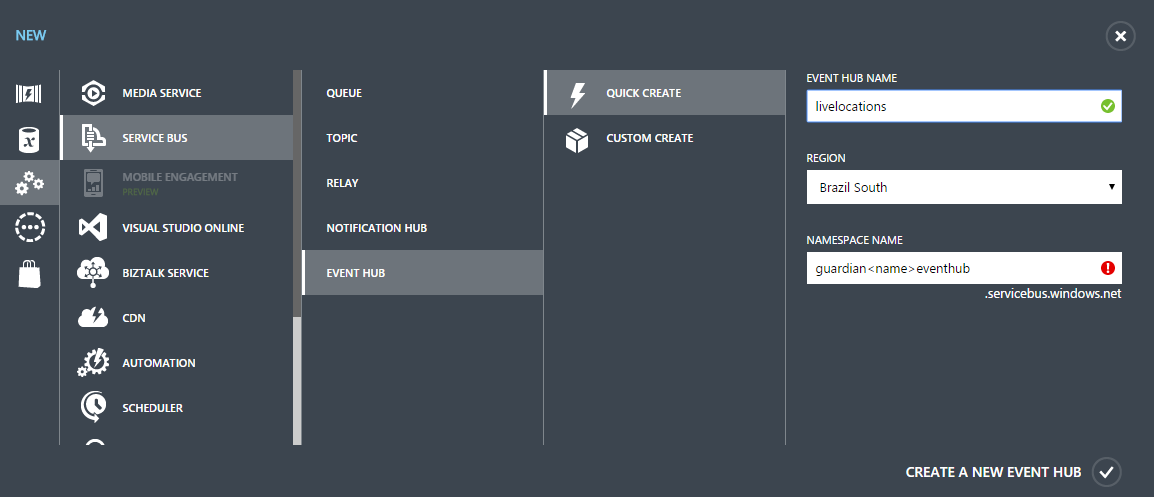
**ADO.NET Connection String:**

* Select the Database and click on ‘Dashboard’
* Click on Connection String(4th option under ‘quick glance’)
* Provide this connection string in Configuration Files

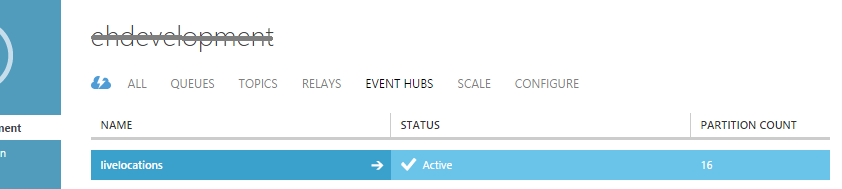


# APPENDIX D - **HOW TO: Create Event Hubs**

1. In the [Management Portal](http://manage.windowsazure.com/), click **Service Bus and then click on New**
2. Select Event Hub and click on ‘Quick Create’

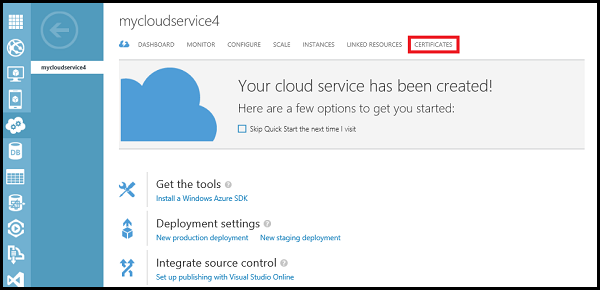


1. Provide ‘livelocations’ as the Event Hub Name
2. Select the appropriate region in Region dropdown
3. Provide name for Namespace as per Table 1.0
4. Click ‘Create A New Event Hub’
5. You will be able to see the below after creation is completed



# APPENDIX E - **HOW TO: Upload Certificates**

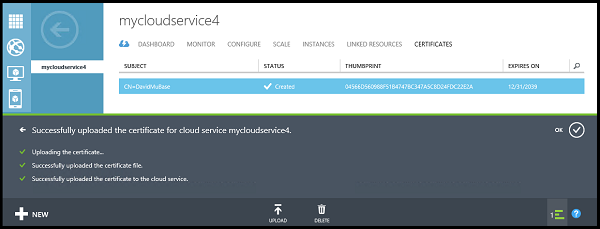
1. In the [Management Portal](http://manage.windowsazure.com/), click **Cloud Services**, click the name of the cloud service, and then click **Certificates**.



1. Click either **Upload a certificate** or **Upload**.
2. In **File**, use **Browse** to select the certificate (.pfx file).
3. In **Password**, enter the private key for the certificate.
4. Click **OK** (checkmark).



You can watch the progress of the upload in the message area, shown below. When the upload completes, the certificate is added to the table. In the message area, click OK to close the message.



# APPENDIX F - **HOW TO: Deploy Cloud Service**

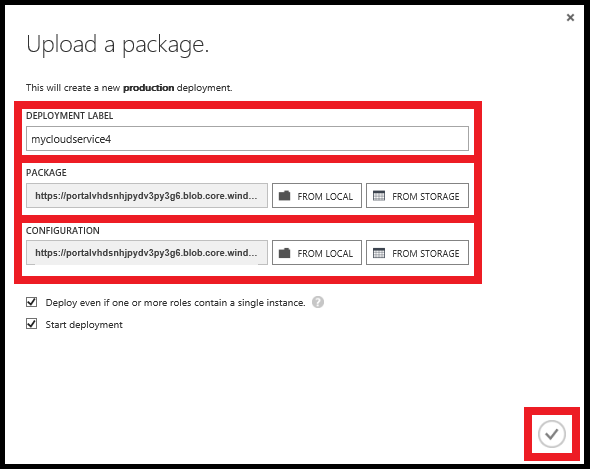
1. In the [Management Portal](http://manage.windowsazure.com/), click **Cloud Services**, click the name of the cloud service, and then click **Dashboard**.

The dashboard opens in the Production environment, you could at this point select Staging to deploy your application in the staging environment. For more information, see [Manage Deployments in Azure](http://msdn.microsoft.com/en-us/library/gg433027.aspx).

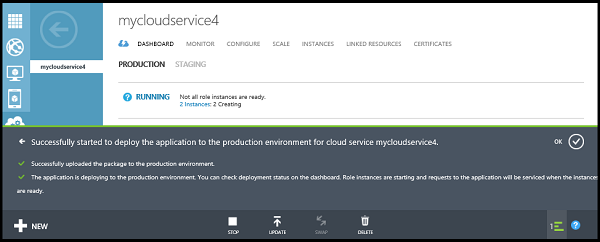
1. Click either **Upload a new production deployment** or **Upload**.
2. In **Deployment label**, enter a name for the new deployment - for example, MyCloudServicev4.
3. In **Package**, use **Browse** to select the service package file (.cspkg) to use.
4. In **Configuration**, use **Browse** to select the service configure file (.cscfg) to use.
5. If the cloud service will include any roles with only one instance, select the **Deploy even if one or more roles contain a single instance** check box to enable the deployment to proceed.

Azure can only guarantee 99.95 percent access to the cloud service during maintenance and service updates if every role has at least two instances. If needed, you can add additional role instances on the **Scale** page after you deploy the cloud service. For more information, see [Service Level Agreements](http://www.windowsazure.com/en-us/support/legal/sla/).

1. Click **OK** (checkmark) to begin the cloud service deployment.



You can monitor the status of the deployment in the message area. Click OK to hide the message.

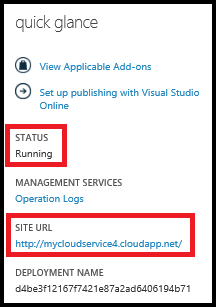


***To verify that deployment completed successfully***

1. Click **Dashboard**.

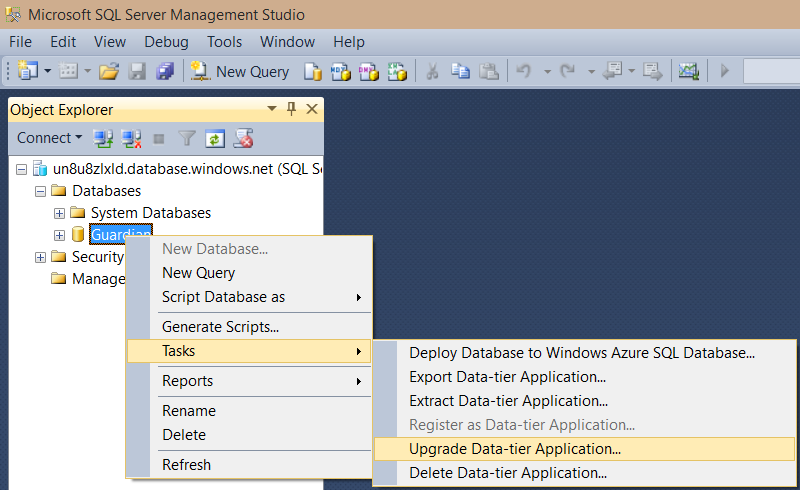
The status should show that the service is **Running**.

1. Under **quick glance**, click the site URL to open your cloud service in a web browser.



# APPENDIX G - **HOW TO: Upgrade Database**

1. Open SQL Server Management Studio
2. Connect to SQL Azure Database with User Name and Password
3. Right click the Database(if not already exist, create one) and select Tasks
4. Click on ‘Upgrade Data-tire application”

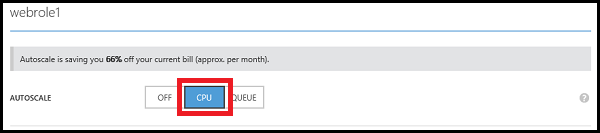


1. Select the GuardianDatabase.dacpac and follow the wizard by clicking ‘Next’ and finally ‘Finish’

For more details, refer: <https://msdn.microsoft.com/en-us/library/azure/jj156167.aspx>

# APPENDIX H - **HOW TO: Auto Scale-up and Scale-down setup**

1. In the [Management Portal](https://manage.windowsazure.com/), click **Cloud Services**, and then click the name of the cloud service to open the dashboard.
2. Click **Scale**.
3. Scroll to the section for the role or availability set, and then click **CPU**. This enables automatic scaling of your application based on the average percentage of CPU resources that it uses.



1. Each role or availability set has a slider for changing the number of instances that can be used. To set the maximum number of instances that can be used, drag the bar on the right to the right. To set the minimum number of instances that can be used, drag the bar on the left to the left.

**Note:** On the Scale page, **Instance** represents either a role instance or an instance of a Virtual Machine.



The maximum number of instances is limited by the cores that are available in the subscription. The colors of the slider represent the used and available cores in your subscription:

* Blue represents the maximum number of cores that the role can use.
* Dark grey represents the cores that are used by all roles and Virtual Machines in the subscription. When this value overlaps the cores used by the role, the color turns to dark blue.
* Light grey represents the cores that are available to use for scaling.
* Pink represents a change has been made that has not been saved.

1. A slider is used for specifying the range of average percentage of CPU usage. When the average percentage of CPU usage goes above the maximum setting, more role instances are created or Virtual Machines are turned on. When the average percentage of CPU usage goes below the minimum setting, role instances are deleted or Virtual Machines are turned off. To set the maximum average CPU percentage, drag the bar on the right to the right. To set the minimum average CPU percentage, drag the bar on the left to the left.



1. You can specify the number of instances to add or turn on each time your application is scaled up. To increase the number of instances that are created or turned on when your application is scaled up, drag the bar right. To decrease the number, drag the bar left.



1. Set the number of minutes to wait between the last scaling action and the next scale-up action. The last scaling action can be either scale-up or scale-down.

Up time

All instances are included when calculating the average percentage of CPU usage and the average is based on use over the previous hour. Depending on the number of instances that your application is using, it can take longer than the specified wait time for the scale action to occur if the wait time is set very low. The minimum time between scaling actions is five minutes. Scaling actions cannot occur if any of the instances are in a transitioning state.

1. You can also specify the number of instances to delete or turn off when your application is scaled down. To increase the number of instances that are deleted or turned off when your application is scaled down, drag the bar right. To decrease the number, drag the bar left.



If your application can have sudden increases in CPU usage, you must make sure that you have a sufficient minimum number of instances to handle them.

1. Set the number of minutes to wait between the last scaling action and the next scale-down action. The last scaling action can be either scale-up or scale-down.

Down time

1. Click **Save**. The scaling action can take up to five minutes to finish.

# APPENDIX I - **HOW TO Generate Different Keys**

Bing Key/ Map Credentials

Login to this URL with the live account credential and then create new key

<https://www.bingmapsportal.com/Application>

Click on the create new key link and then setup following fields

**Application name:** Guardian<name> <Provide new application name>

**Application URL:** https://guardian<name>.cloudapp.net <Map to Portal URL>

**Key type**: Basic <Select Basic Option>

**Application type** **:** / Other Public Mobile App <Select this Option>

Click on Create, it will generate new bing key as below

**Key:**AqtaE18u0YgWQjc1PIMudswXXXXXXXXXXXXXqgwndcBOInc3LBPIVl6utemHKIzv

Live Account Integration

For Client ID & ClientSecret

Login to this URL with the live account credential and then create new application

<https://account.live.com/developers/applications/index>

We have to fill the following settings before to get the keys

* [Basic Information](https://account.live.com/developers/applications/basicinfo/000000004C15475F?n=1)
* Application name:Guardian<Name>
* Default language:English (United States)
* Terms of service URL:https://guardian<name>.cloudapp.net/privacy.htm
* Privacy URL:https://guardian<name>.cloudapp.net/privacy.htm
* [API Settings](https://account.live.com/developers/applications/apisettings/000000004c15475f)
* Mobile or desktop client app:Yes
* Restrict JWT issuing:No
* Enhanced redirection security:Disabled
* Target domain:**guardian<name>.cloudapp.net**

(\*Target domain field is needed to setup with correct value, otherwise **LiveAuthID** won’t get generated)

* Redirect URLs:https://guardian<name>.cloudapp.net/default.aspx
* [App Settings](https://account.live.com/developers/applications/appsettings/000000004c15475f)
* It will generate Client ID and Client Secrete
* [Localization](https://account.live.com/developers/applications/localization/000000004c15475f)
* Language:
* English (United States)
* Application name:
* Guardian<name>

Sample of newly created account for reference

**Guardian<Name>**

* Basic Information

Application name:

Guardian<name>

Default language:

English (United States)

Application logo:

Image of a 48 x 48 logo.

Terms of service URL:

https://guardian<name>.cloudapp.net/privacy.htm

Privacy URL:

https://guardian<name>.cloudapp.net/privacy.htm

* API Settings

Mobile or desktop client app:

Yes

Restrict JWT issuing:

No

Enhanced redirection security:

Enabled

Target domain:

**Guardian<name>.cloudapp.net**

Redirect URLs:

https://guardian<name>.cloudapp.net/default.aspx

* App Settings

**Client ID:**

000000XXXXX594A1

**Client secret:**

zHe9pIdSXXXXXXXXXXXXHhsn-KNS

* Localization

Language:

English (United States)

Application name:

Guardian<name>

Facebook Integration - Obsolete

URL: <https://developers.facebook.com/>

Create facebook developer account that will generate these fields App ID and App Secret.

Sample of newly created FB account for reference

|  |  |
| --- | --- |
| https://fbcdn-photos-c-a.akamaihd.net/hphotos-ak-xft1/t39.2081-0/p128x128/851578_455087414601994_1601110696_n.png | Guar­d­i­a­n­<Name>  This app is in development mode |
| |  |  |  | | --- | --- | --- | | **App ID**  8637417XXXX300 | API Version  v2.3 | **App Secret**  86a53aaa7XXXXXXXXX8a3a02ccba91b3 | |

# APPENDIX J – **VFirst SMS Templates**

1 - {name} ({phone}) needs urgent help at {address}. Track at {tinyuri}

2 - {name} is safe now.

3 - {0}({1}) added you as a buddy in Guardian App. To unsubscribe, click {2}

4 - Please enter {0} verification code to create your Profile for phone number ending with {1}

# APPENDIX K – **Guidelines for Certificates and Custom Domain association**

References:

<https://azure.microsoft.com/en-us/documentation/articles/cloud-services-configure-ssl-certificate/>

<https://support.microsoft.com/en-us/kb/2990804>

Get an SSL certificate

To configure SSL for an application, you first need to get an SSL certificate that has been signed by a Certificate Authority (CA), a trusted third-party who issues certificates for this purpose. If you do not already have one, you will need to obtain one from a company that sells SSL certificates.

The certificate must meet the following requirements for SSL certificates in Azure:

* The certificate must contain a private key.
* The certificate must be created for key exchange, exportable to a Personal Information Exchange (.pfx) file.
* The certificate's subject name must match the domain used to access the cloud service. You cannot obtain an SSL certificate from a certificate authority (CA) for the cloudapp.net domain. You must acquire a custom domain name to use when access your service. When you request a certificate from a CA the certificate's subject name must match the custom domain name used to access your application. For example, if your custom domain name is **contoso.com** you would request a certificate from your CA for \***.contoso.com** or **www.contoso.com**.
* The certificate must use a minimum of 2048-bit encryption.

For test purposes, you can create and use a self-signed certificate. A self-signed certificate is not authenticated through a CA and can use the cloudapp.net domain as the website URL. For example, the task below uses a self-signed certificate in which the common name (CN) used in the certificate is **sslexample.cloudapp.net**. For details about how to create a self-signed certificate using IIS Manager, See [How to create a certificate for a role](http://msdn.microsoft.com/library/azure/gg432987.aspx).

Next, you must include information about the certificate in your service definition and service configuration files.

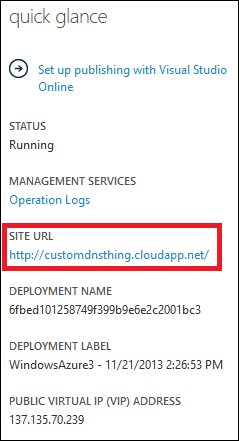
Associate a custom domain name with an Azure Cloud Service

When you create an application in Azure, Azure provides a subdomain on the cloudapp.net domain so your users can access your application on a URL like http://<myapp>.cloudapp.net. However, you can also expose your application on your own domain name, such as contoso.com.

Add a CNAME record for your custom domain

To create a CNAME record, you must add a new entry in the DNS table for your custom domain by using the tools provided by your registrar. Each registrar has a similar but slightly different method of specifying a CNAME record, but the concepts are the same.

1. Use one of these methods to find the **.cloudapp.net** domain name assigned to your cloud service.
   * Login to the [Azure Management Portal](https://manage.windowsazure.com/), select your cloud service, select **Dashboard**, and then find the **Site URL** entry in the **quick glance** section.



* + Install and configure [Azure Powershell](http://azure.microsoft.com/en-us/documentation/articles/install-configure-powershell/), and then use the following command:

**Get-AzureDeployment -ServiceName yourservicename | Select Url**

1. Save the domain name used in the URL returned by either method, as you will need it when creating a CNAME record.
2. Log on to your DNS registrar's website and go to the page for managing DNS. Look for links or areas of the site labeled as **Domain Name**, **DNS**, or **Name Server Management**.
3. Now find where you can select or enter CNAME's. You may have to select the record type from a drop down, or go to an advanced settings page. You should look for the words **CNAME**, **Alias**, or **Subdomains**.
4. You must also provide the domain or subdomain alias for the CNAME, such as **www** if you want to create an alias for **www.customdomain.com**. If you want to create an alias for the root domain, it may be listed as the '@' symbol in your registrar's DNS tools.
5. Then, you must provide a canonical host name, which is your application's **cloudapp.net** domain in this case.

For example, the following CNAME record forwards all traffic from www.contoso.com to contoso.cloudapp.net, the custom domain name of your deployed application:

**Alias/Host name/Subdomain** **Canonical domain**

www contoso.cloudapp.net

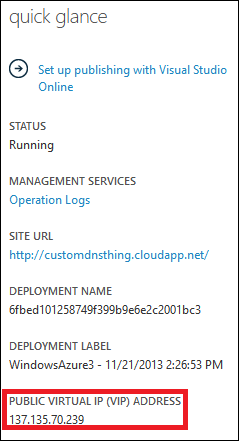
A visitor of **www.contoso.com** will never see the true host (contoso.cloudapp.net), so the forwarding process is invisible to the end user.

**Note** The example above only applies to traffic at the **www** subdomain. Since you cannot use wildcards with CNAME records, you must create one CNAME for each domain/subdomain. If you want to direct traffic from subdomains, such as \*.contoso.com, to your cloudapp.net address, you can configure a **URL Redirect** or **URL Forward** entry in your DNS settings, or create an A record.

Add an A record for your custom domain

To create an A record, you must first find the virtual IP address of your cloud service. Then add a new entry in the DNS table for your custom domain by using the tools provided by your registrar. Each registrar has a similar but slightly different method of specifying an A record, but the concepts are the same.

1. Use one of the following methods to get the IP address of your cloud service.
   * Login to the [Azure Management Portal](https://manage.windowsazure.com/), select your cloud service, select **Dashboard**, and then find the **Public Virtual IP (VIP) address** entry in the **quick glance** section.



* + Install and configure [Azure Powershell](http://azure.microsoft.com/en-us/documentation/articles/install-configure-powershell/), and then use the following command:

**get-azurevm -servicename yourservicename | get-azureendpoint> -VM | select Vip**

If you have multiple endpoints associated with your cloud service, you will receive multiple lines containing the IP address, but all should display the same address.

1. Save the IP address, as you will need it when creating an A record.
2. Log on to your DNS registrar's website and go to the page for managing DNS. Look for links or areas of the site labeled as **Domain Name**, **DNS**, or **Name Server Management**.
3. Now find where you can select or enter A record's. You may have to select the record type from a drop down, or go to an advanced settings page.
4. Select or enter the domain or subdomain that will use this A record. For example, select www if you want to create an alias for **www.customdomain.com**.   
   If you want to create a wildcard entry for all subdomains, enter '\*'. This will cover all sub-domains such as **mail.customdomain.com**, **login.customdomain.com**, and **www.customdomain.com**.If you want to create an A record for the root domain, it may be listed as the '@' symbol in your registrar's DNS tools
5. Enter the IP address of your cloud service in the provided field. This associates the domain entry used in the A record with the IP address of your cloud service deployment.

For example, the following A record forwards all traffic from contoso.com to 137.135.70.239, the IP address of your deployed application:

**Host name/Subdomain** **IP address**

@ 137.135.70.239

This example demonstrates creating an A record for the root domain. If you wish to create a wildcard entry to cover all subdomains, you would enter '\*' as the subdomain.