CMP/WAP Ops Guide  
Partial. Incomplete. Preview.

## Overview

CMP/WAP is a suite of software components which adds Azure VM management features to the WAP. There are two main components: the CMP worker service and the WAP extension. The WAP extension is further broken into two parts: the resource provider, and the WAP portal admin and tenant sites.  
  
Admin and tenant WAP users interact with the system through the admin and tenant sites which are seamlessly integrated with the WAP portal. The worker service carries out administrative operations with Azure and various other systems on behalf of requests from the WAP extension.

## Physical Architecture

 Physical Architecture: Express Configuration

 Physical Architecture: Enterprise Configuration

CMP Servers

|  |  |  |
| --- | --- | --- |
| Server | Function | Location |
| CMP Server | CMP HTTP Server + CMP Windows Service + Swivelseat | On premises (or Azure post GG) |
| CMP DB | CMP Database | Shares LAN with CMP Server |
| AFTS | AFTS + VHD Prep | Each data center which hosts migration sources |

Other Objects

|  |  |  |
| --- | --- | --- |
| Object | Functions | Location |
| MyCap | MyCapacity IIS + DB | On premises |
| Migration Sources | Hosts targeted to be migrated | On premises |
| Clouds | Target location for migrated hosts | Azure |

## Installation

There are two installer packages: one for the CMP worker service and one for the WAP extension. These are installed and configured separately.



## CMP Service Installation

### Certificate Installation

1. Choose an account on which the CMP worker service will run.
2. Log on to the CMP service host computer with the CMP worker service account.

Azure admin certificate

1. Obtain a .pfx file for a certificate which has admin access to each Azure subscription to be managed.
2. For ease of administration a single certificate can be given admin access to all Azure subscriptions to be managed.
3. For each certificate:
   1. Install certificate and key to the Current User : Personal : Certificates store
   2. Install certificate and key to the Local Computer : Personal : Certificates store

CMP Secret certificate

1. Obtain a single .pfx file for a certificate which will be used to encrypt secrets in config and DB tables.
2. For ease of administration It is allowable to use the Azure Admin certificate for this purpose. If you use the same certificate than you can skip this step.
3. Install certificate and key to the Current User : Personal : Certificates store
4. Install certificate and key to the Local Computer : Personal : Certificates store

### Worker Service Installation

1. Execute the installer file: CmpWorkerServiceInstaller.msi (TODO: Location)
2. Use the service management console to change the ‘CmpWorkerService’ Log On account to the chosen account.

### CMP Database Installation

1. Select a DB server or create an Azure SQL database.
2. Set DB server to allow SQL authentication (this is the only option for Azure SQL).
3. Record the credentials.
4. Install the DB from the installer file (TODO: Location)

### CMP ServiceBus Creation

1. Log on to the Azure Admin Portal.
2. Select an subscription which will be used to home the CMP service bus queue.
3. Create a ServiceBus Queue.
4. Record the queue connection string.

### Worker Service Configuration

#### Config File:

In this step you will edit the CmpWorkerService.exe.config file. Windows will not allow you to edit this in place, so you must move the file to a read/write directory to edit and then write it back to the operating directory when done editing.

1. Copy the config file (C:\Program Files (x86)\Microsoft\MSIT\CmpWorkerService\ CmpWorkerService.exe.config) to a read\write directory.
2. Edit the indicated calues
3. As an admin, copy the red\write CmpWorkerService.exe.config back to the C:\Program Files (x86)\Microsoft\MSIT\CmpWorkerService directory.

|  |  |  |
| --- | --- | --- |
| Key \ ConnectionString | Description | Sample |
| CMPContext | Connection string to access the CMP database. If you wish to encrypt the access password then refer to the ‘CMP Secret Management’ section below | Data Source=CmpWap;Initial Catalog=CMP;Persist Security Info=True;User ID=sa;Password=XXX;MultipleActiveResultSets=True |
| KryptoCert | Set to "LocalMachine,My,<Thumbprint>" where <Thumbprint> is the thumbprint of the CMP Secret certificate as installed above. | LocalMachine,My,339C80283637D69D9D9F0F5FE00970D93CB0A148 |
| DomainJoinAccount | Account creds used to domain join VMs. Set to "<domain>,<name>,<password>". If you wish to encrypt the account password then refer to the ‘CMP Secret Management’ section below | redmond,markwes,[KText]kdPXcqVzA9R3ZK3Z8kP8FcNQEaVz6GR5ptji8pEiD5TJRq/Vr7I7oX9lMlWJoMwEEE1msvtLJ8Fun2JrUDBgeQtjjz9j0Pj/vKqhqmsHDL4jG9L3YXzq2tu2qLS5uyAJdd5iD8RME0eGCV8TzjzqSUGC9P/t3cQa8DTx9EMxrrvJaSJWb3cbHNiFvP56jVKNnZHN9GE7lGv8ggKoQYOxI3J/gZUk6egxvPlSktURXZX6TlxeFJnPqEVJhNFUpFAa417W+dB5m1ERCC/psruhKs43XszSAIJHVVpyzDaVjZASDJxtLDFg8ikRzLpe9RcWwl4c2xFclgZdtF1SBg1sWQ==[/KText] |
| AUTOLOCALADMINUSERNAME | The local admin of the VMs to be created | 123User!! |
| AUTOLOCALADMINPASSWORD | The password of the local admin. If you wish to encrypt the account password then refer to the ‘CMP Secret Management’ section below | [KText]MpYWdBSk/LjqqZmFmZCls4fMVDJhHZC5TgJRqdUiSxI/oV1yq9SFi2q6bZvR0sxN83tCQn3Dxgja0IUvxkw1eXlgcFCaFOzwuTYhiAL9gNZXpLwW1QKuGkOFHVC5xopweUS3xdBFkOnR+JkUrXy4kU7gEKc9nhSM1KPOegQCFsEAfoQhbbjSYmq0eUxkcQIbTbKhWlBOGop9ny0N3XY/P5gP56hfPT0WdpwKLynUEYnSRTBMbigjnJ8+WZKzBzsyB1XSRJQZzkdXajY/EBgU3n1FD4MXH2X21wxZ7d9VCB2uCBGjWFIETHVtflVbBv7oNEBvM7IlmOw+BDsMPKFc/w==[/KText] |
| AUTOSUBNETNAME | The name of the Vnet subnet which will be accessed by the VMs. | TenantSubnet |
| CMPContextPassword | The KText encrypted password of the SQL auth account used to access the CMP database. Refer to the ‘CMP Secret Management’ section below. | [KText]aNVLpJUPQW0bosxnlW6tqzms1/Z3rylXz5sK+nXf6Jn7Bob9uF55FwIF4mjkdOGx2ZW0PQ8Mr1T87RabzI5vKrWFQFZ+4AXY+HR+jkRpLCVUjTiRE3Jxb8KNkibdc85NJIjJEKppXccNRS0K9kMlJ8RlyJPNaJOkaIobkZectcNNlSMEZZGk4ZP1Zy0CbJFxF6l7sAFQHdy6NgNEEm0nZLk3KwoaMTpwp+Lh5C36nLLq21K9A56cZ+hkZON2qMCSgiybn90g4mqAywsc4lY7SASJRFK0Vo5hGvVSTx5TdgMDhv39kHjTUtOuY647GgR0MTztf0aZf/fU4/JF2pagwg==[/KText] |
| Microsoft.ServiceBus.ConnectionString | The Azure ServiceBus connection string as created above. If you wish to encrypt the SharedSecretValue then refer to the ‘CMP Secret Management’ section below | Endpoint=sb://cmpdevsb.servicebus.windows.net/;SharedSecretIssuer=owner;SharedSecretValue=[KText]OdutotKGwGUcHrCAxaoPKv/MThop7dHLeJ8NXEJ4I685+7HhOPxIIiqzpg1COg5Py9X7TYdXGV2nf6lst4jRCBCkxph/tEV/IfLnJOqtI3vM7LIMXBUjcwc/FGYL5vpJDNp+aWTKd++Zs7TnWsBkWWHgRHmF7crMFnprqa5I2dffp6E0/diPZNBn7asOtyBGyQ3yQCrG4jy43QdJxrrD/Q723uXORu4N2YayLT+u7Sgq9ol3iPDi5oKlahTscDtnkWbU7tbwg13jbXH63JFjAgJs3VEu+cP7Y2d1qhGP+fYygPRk2W/IqIiJfWRa+LaiB+Q8R72mdFPKojcMPUDI1w==[/KText] |

#### Sample:

<?xml version="1.0" encoding="utf-8"?>

<configuration>

<configSections>

<section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework, Version=6.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermission="false"/>

<!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 --></configSections>

<connectionStrings>

<!-- CMP Wap Local -->

<add name="CMPContext" connectionString="Data Source=CmpWap;Initial Catalog=CMP;Persist Security Info=True;User ID=sa;Password=XXX;MultipleActiveResultSets=True"

providerName="System.Data.SqlClient" />

</connectionStrings>

<appSettings>

<add key="KryptoCert" value="LocalMachine,My,339C80283637D69D9D9F0F5FE00970D93CB0A148"/>

<add key="DomainJoinAccount" value="redmond,markwes,[KText]kdPXcqVzA9R3ZK3Z8kP8FcNQEaVz6GR5ptji8pEiD5TJRq/Vr7I7oX9lMlWJoMwEEE1msvtLJ8Fun2JrUDBgeQtjjz9j0Pj/vKqhqmsHDL4jG9L3YXzq2tu2qLS5uyAJdd5iD8RME0eGCV8TzjzqSUGC9P/t3cQa8DTx9EMxrrvJaSJWb3cbHNiFvP56jVKNnZHN9GE7lGv8ggKoQYOxI3J/gZUk6egxvPlSktURXZX6TlxeFJnPqEVJhNFUpFAa417W+dB5m1ERCC/psruhKs43XszSAIJHVVpyzDaVjZASDJxtLDFg8ikRzLpe9RcWwl4c2xFclgZdtF1SBg1sWQ==[/KText]"/>

<add key="ProcessVmsActive" value="T"/>

<add key="ClientSettingsProvider.ServiceUri" value=""/>

<add key="AUTOLOCALADMINUSERNAME" value="123User!!"/>

<add key="AUTOLOCALADMINPASSWORD" value="[KText]MpYWdBSk/LjqqZmFmZCls4fMVDJhHZC5TgJRqdUiSxI/oV1yq9SFi2q6bZvR0sxN83tCQn3Dxgja0IUvxkw1eXlgcFCaFOzwuTYhiAL9gNZXpLwW1QKuGkOFHVC5xopweUS3xdBFkOnR+JkUrXy4kU7gEKc9nhSM1KPOegQCFsEAfoQhbbjSYmq0eUxkcQIbTbKhWlBOGop9ny0N3XY/P5gP56hfPT0WdpwKLynUEYnSRTBMbigjnJ8+WZKzBzsyB1XSRJQZzkdXajY/EBgU3n1FD4MXH2X21wxZ7d9VCB2uCBGjWFIETHVtflVbBv7oNEBvM7IlmOw+BDsMPKFc/w==[/KText]"/>

<add key="AUTOSUBNETNAME" value="TenantSubnet"/>

<add key="DefaultStateTtlMinutes" value="120"/>

<add key="DefaultVmRebootDwellTimeMinutes" value="3"/>

<!-- CMP Wap -->

<add key="CMPContextPassword" value="[KText]aNVLpJUPQW0bosxnlW6tqzms1/Z3rylXz5sK+nXf6Jn7Bob9uF55FwIF4mjkdOGx2ZW0PQ8Mr1T87RabzI5vKrWFQFZ+4AXY+HR+jkRpLCVUjTiRE3Jxb8KNkibdc85NJIjJEKppXccNRS0K9kMlJ8RlyJPNaJOkaIobkZectcNNlSMEZZGk4ZP1Zy0CbJFxF6l7sAFQHdy6NgNEEm0nZLk3KwoaMTpwp+Lh5C36nLLq21K9A56cZ+hkZON2qMCSgiybn90g4mqAywsc4lY7SASJRFK0Vo5hGvVSTx5TdgMDhv39kHjTUtOuY647GgR0MTztf0aZf/fU4/JF2pagwg==[/KText]" />

<add key="Microsoft.ServiceBus.ConnectionString" value="Endpoint=sb://cmpdevsb.servicebus.windows.net/;SharedSecretIssuer=owner;SharedSecretValue=[KText]OdutotKGwGUcHrCAxaoPKv/MThop7dHLeJ8NXEJ4I685+7HhOPxIIiqzpg1COg5Py9X7TYdXGV2nf6lst4jRCBCkxph/tEV/IfLnJOqtI3vM7LIMXBUjcwc/FGYL5vpJDNp+aWTKd++Zs7TnWsBkWWHgRHmF7crMFnprqa5I2dffp6E0/diPZNBn7asOtyBGyQ3yQCrG4jy43QdJxrrD/Q723uXORu4N2YayLT+u7Sgq9ol3iPDi5oKlahTscDtnkWbU7tbwg13jbXH63JFjAgJs3VEu+cP7Y2d1qhGP+fYygPRk2W/IqIiJfWRa+LaiB+Q8R72mdFPKojcMPUDI1w==[/KText]" />

<add key="KCTFolderName" value="KCT0001830"/>

<add key="ApproverAlias" value="redmond\ITCMPDev"/>

</appSettings>

<startup>

<supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5.1"/>

</startup>

<entityFramework>

<defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">

<parameters>

<parameter value="v11.0"/>

</parameters>

</defaultConnectionFactory>

<providers>

<provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices, EntityFramework.SqlServer"/>

</providers>

</entityFramework>

<runtime>

<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">

<dependentAssembly>

<assemblyIdentity name="Microsoft.WindowsAzure.Storage" publicKeyToken="31bf3856ad364e35" culture="neutral"/>

<bindingRedirect oldVersion="0.0.0.0-3.0.3.0" newVersion="3.0.3.0"/>

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Data" publicKeyToken="b77a5c561934e089" culture="neutral"/>

<bindingRedirect oldVersion="0.0.0.0-4.0.0.0" newVersion="4.0.0.0"/>

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="Microsoft.Data.OData" publicKeyToken="31bf3856ad364e35" culture="neutral"/>

<bindingRedirect oldVersion="0.0.0.0-5.6.1.0" newVersion="5.6.1.0"/>

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral"/>

<bindingRedirect oldVersion="0.0.0.0-6.0.0.0" newVersion="6.0.0.0"/>

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="Microsoft.Data.Edm" publicKeyToken="31bf3856ad364e35" culture="neutral"/>

<bindingRedirect oldVersion="0.0.0.0-5.6.1.0" newVersion="5.6.1.0"/>

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="Microsoft.Data.Services.Client" publicKeyToken="31bf3856ad364e35" culture="neutral"/>

<bindingRedirect oldVersion="0.0.0.0-5.6.1.0" newVersion="5.6.1.0"/>

</dependentAssembly>

</assemblyBinding>

</runtime>

<system.serviceModel>

<bindings>

<basicHttpBinding>

<binding name="BasicHttpBinding\_IITSMTicketService">

<security mode="TransportCredentialOnly">

<transport clientCredentialType="Ntlm"/>

</security>

</binding>

</basicHttpBinding>

</bindings>

<client>

<!-- CMP Dev, test and UAT. Needs to run under an account that has perms to http://ITSMUAT. -->

<endpoint address="" binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding\_IITSMTicketService" contract="ITSMTicketServiceReference.IITSMTicketService" name="BasicHttpBinding\_IITSMTicketService"/>

<!-- CMP Prod. Needs to run under an account that has perms to http://ITSM.

<endpoint address="http://itsm/ITSMWebService2/ITSMTicketService.svc"

binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding\_IITSMTicketService"

contract="ITSMTicketServiceReference.IITSMTicketService" name="BasicHttpBinding\_IITSMTicketService" />-->

</client>

</system.serviceModel>

</configuration>

### Database Configuration:

#### Tables

The CMP database contains a number of tables, two of which must be edited for configuration:

1. CmpServiceUserAccounts
2. ServiceProviderAccounts

**Table:** CmpServiceUserAccounts

The CmpServiceUserAccounts table is used to store the credentials which must be supplied by clients of the CMP web service. The table is required for the enterprise CMP/WAP configuration, and is not used in the express CMP/WAP configuration.

Schema:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| ID | Int | 0 | Row unique ID, sequential |
| DisplayName | varchar | CmpServiceUser | Associated display name, just for reference, not used by CMP. |
| Name | varchar | CmpServiceUser | CMP service User Name |
| Password | varchar | [KText]u1wi7op….wqrjsoavPBng==[/KText] | Password. May be encrypted. See Ktext section. |
| Config | varchar | <config></config> | Required value: “<config></config>” |
| TagData | varchar | <tag></tag> | Required value: “<tag></tag>” |
| Domain | Varchar | CMP | Required value: “CMP” |
| AssociatedCorpAccountName | varchar | redmond\cmpmaster | Associated user account, just for reference, not used by CMP. |
| StatusCode | varchar | ACTIVE | Required value: ACTIVE |
| AccountTypeCode | varchar | SA | Required value: “SA” |
| IsActive | bit | 1 | Required value: 1 |

**Table:** ServiceProviderAccounts

The CmpServiceUserAccounts table is used to store details about the Azure subscriptions in which CMP manages VMs. Details of each Azure subscription are represented in a single row.

Schema:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| ID | Int | O | Row unique ID, sequential |
| Name | varchar | MarkWestMsftInternal | Associated name, just for reference, not used by CMP. |
| Description | varchar | MarkWestMsftInternal | Associated descriuption, just for reference, not used by CMP. |
| OwnerNamesCSV | varchar | markwes | Associated owner names, just for reference, not used by CMP. |
| Config | varchar | <config></config> | Required value: “<config></config>” |
| TagData | varchar | <tag></tag> | Required value: “<tag></tag>” |
| AccountType | varchar | AzureSubscription | Required value: “Required value: “<tag></tag>” |
| ExpirationDate | DateTime | NULL | Not used by CMP. |
| CertificateBlob | varchar | NULL | Not used by CMP. |
| CertificateThumbprint | varchar | 339C80283637D69D9D9F0F5FE00970D93CB0A148 | The thumbprint of the Azure subscription admin access certificate |
| AccountID | varchar | 26661eda-81ca-4307-b331-698118ad668e | The Azure subscription account ID |
| AccountPassword | varchar | NULL | Not used by CMP. |
| Active | bit | 1 | Required value: 1 |
| AzRegion | varchar | Central US | The exact name of the Azure region in which the Affinity Group was allocated. |
| AzAffinityGroup | varchar | ag2-usc | The name of the Affinity Group in which the Vnet was created |
| AzVNet | varchar | SDODev1VNET1ERUSC | The name of the Vnet in which the Subnet was created |
| AzSubnet | varchar | TenantSubnet | The name of the subnet on which VMs will network. |
| AzStorageContainerUrl | varchar | http://sg2uscer.blob.core.windows.net/vhds | The URL of the container in which VM VHDs will be stored. |
| ResourceGroup | varchar | Default | A CMP specific name used to group collections of Azure subscriptions into capacity pools. All rows which share the same ResourceGroup name will participate in the same capacity pool. |
| CoreCountMax | Int | 0 | Reserved |
| CoreCountCurrent | int | 0 | Reserved |

## WAP Extension Installation

Site + Resource Provider  
installer:

1. Install Microsoft.WindowsAzurePack.CmpWapExtension.Setup msi.
2. Run Register-ResourceProvider.ps1 in Admin Mode

If we plan to configure WAP extension RP(MgmtSvc-CmpWapExtension) to http/https in IIS

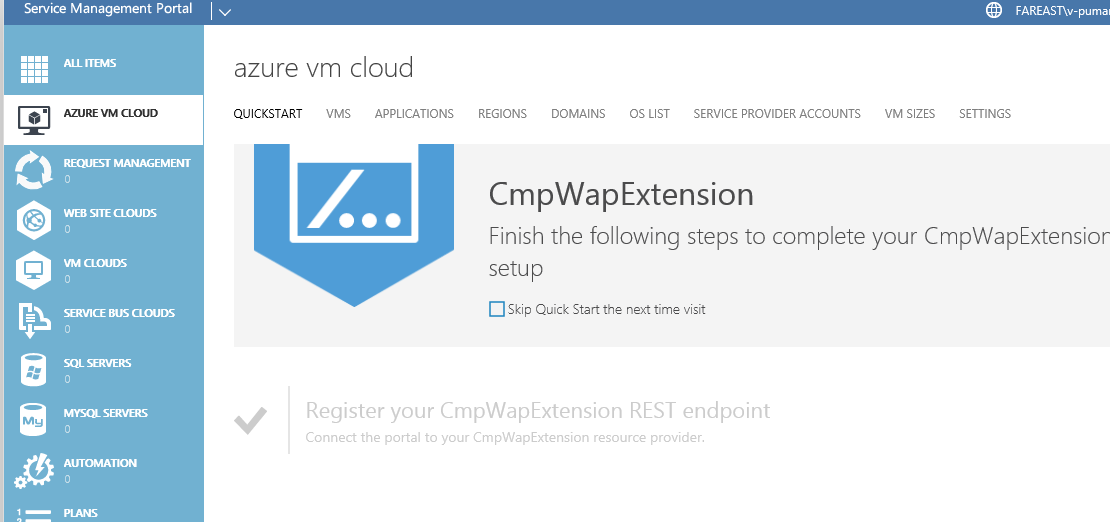
Need to modify the below section in powershell script accordingly

'AdminForwardingAddress' = "https://$hostName/admin";

'TenantForwardingAddress' = "https://$hostName/";

'NotificationForwardingAddress' = "https://$hostName/admin";

1. Browse Wap Admin site and click on **Azure VM CLOUD** RP and should be to see the below screen once the RP is registered successfully.



1. Now we want to give our tenants access to this resource provider. If we already have a plan and we just need to add this custom resource provider to that plan.

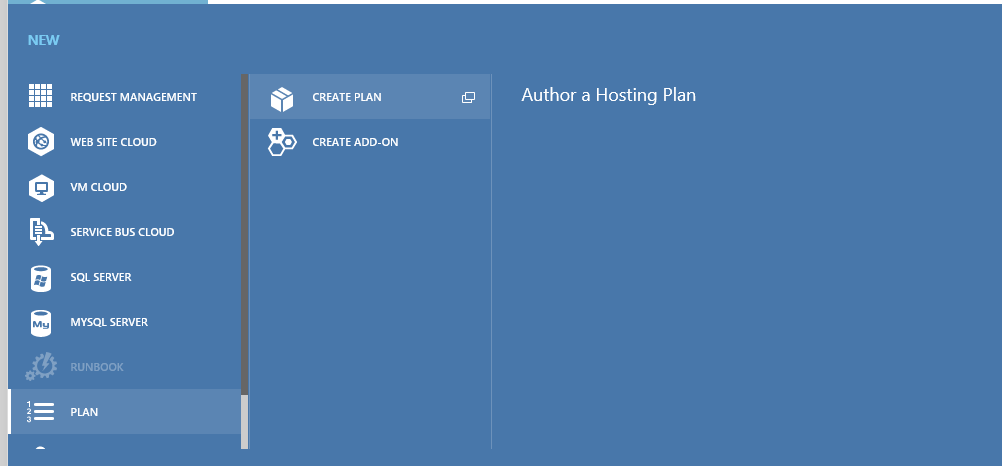
In the WAP Admin Portal, select one of your plans, and in the actions menu click on Add Service and select CmpWAPExtension as Service and click on the check mark to add the service to the plan.



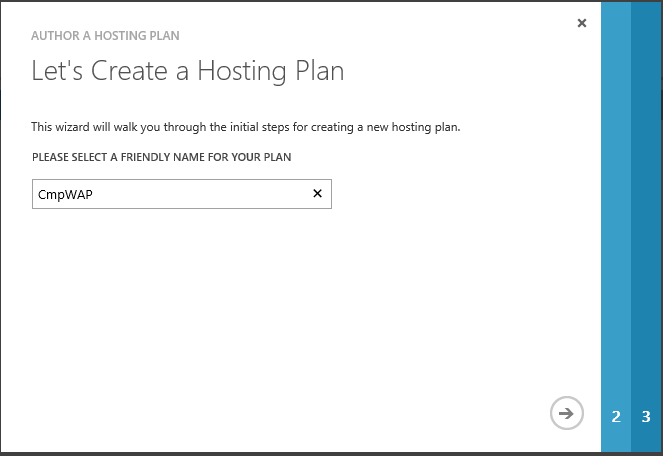
**Or**

1. If we want to create a new plan for new WAP RP

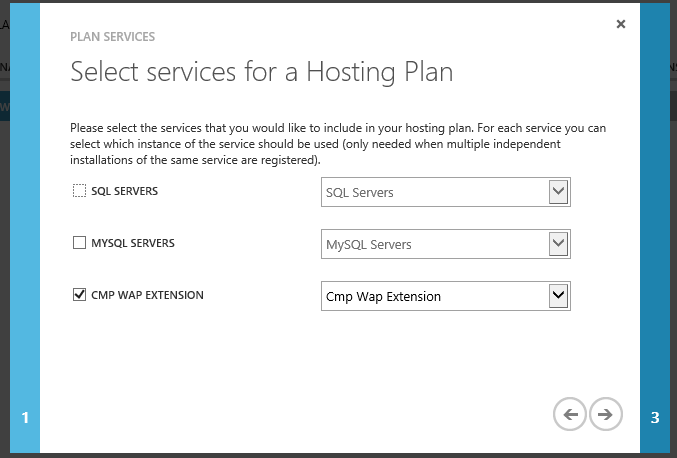
* Click on New Create Plan



* Give a FriendlyName



* Select CmpWapExtension



* Run Apppool of MgmtSvc-CmpWapExtension website under Service account which has access to AD(it should have permission to delete AD object).

Add the service account as admin in WAP using below command which needs to run in powershell(Admin mode)

**To Add Admin --WAP**

$connectionstring = 'Server=<wapservername>;Initial Catalog=Microsoft.MgmtSvc.Store;User ID=sa;Password=xxxxx'

Add-MgmtSvcAdminUser -ConnectionString $connectionstring -Principal 'Redmond\xxxxxx'

**To Fetch Admin List --WAP**

$connectionstring = 'Server=<wapservername>;Initial Catalog=Microsoft.MgmtSvc.Store;User ID=sa;Password=xxxxx'

Get-MgmtSvcAdminUser -ConnectionString $connectionstring

### Config File

#### Schema:

#### Description:

#### Sample:

<?xml version="1.0" encoding="utf-8"?>

<!--

For more information on how to configure your ASP.NET application, please visit

http://go.microsoft.com/fwlink/?LinkId=169433

-->

<configuration>

<configSections>

<!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468 -->

<section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFramework, Version=6.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" requirePermission="false" />

</configSections>

<connectionStrings>

<!-- CmpWap -->

<add name="CMPContext" connectionString="Data Source=cmpwap;Initial Catalog=CMP;Persist Security Info=True;User ID=sa;Password=XXX;MultipleActiveResultSets=True"

providerName="System.Data.SqlClient" />

<add name="MicrosoftMgmtSvcCmpContext" connectionString="Data Source=cmpwap;Initial Catalog=Microsoft.MgmtSvc.Cmp;Persist Security Info=True;User ID=sa;Password=123Mainau!;MultipleActiveResultSets=True"

providerName="System.Data.SqlClient" />

<add name="masterContext" connectionString="Data Source=thezephyr;Initial Catalog=master;Persist Security Info=True;User ID=sa;Password=123Mainau!;MultipleActiveResultSets=True"

providerName="System.Data.SqlClient" />

</connectionStrings>

<appSettings>

<!-- Following credentials are used for basic auth for CmpWapExtension resource provider. Its shown like this for this sample only.

Its always recommended not to store credentials in plain text in web.config.

Encrypt the credentials or config file -->

<add key="Username" value="admin" />

<add key="Password" value="pass@word1" />

<add key="CmpServiceUrl" value="https://cmpdevpubservice.cloudapp.net/Odata" />

<add key="MatchPattern" value="\*" />

<add key="DefaultTargetServiceProviderAccountID" value="0" />

<add key="DefaultTargetServiceProviderAccountGroup" value="Default" />

<add key="KryptoCert" value="LocalMachine,My,339C80283637D69D9D9F0F5FE00970D93CB0A148" />

<add key="CmpServiceCredentials" value="[KText]ArV8zwhjWZYi4Av0IOsjHniXAyp3Lp+y1KQM68T2ybGa/G6fV7CcklCSZmEekeX4/lDTkVrKtGKG+u8/5noRu4K+t1JrTe9wBBbNd+HjIGTBGKYcEuesUVfBaOl3VxJHoR6Ay8AdDiWJiVmCCVbmbcB4z33y+Rqn0jKnNkAESgWGP4I7hpdMebU/dWJq5d59QjqQmbcVa+n3izXSqo+NbmvuXD5zHadV7BYg+ph4rjX5+y58cCou+rF2SY9fhysZcaZnkQKwmUTWApc1RmM/SqwCPsp/InfSzQart84dShwUxLybXLqYmO/6SfqhPs+ifNJOWMexePnyxP5bIZZV/A==[/KText]" />

<add key="CMPContextPassword" value="[KText]aNVLpJUPQW0bosxnlW6tqzms1/Z3rylXz5sK+nXf6Jn7Bob9uF55FwIF4mjkdOGx2ZW0PQ8Mr1T87RabzI5vKrWFQFZ+4AXY+HR+jkRpLCVUjTiRE3Jxb8KNkibdc85NJIjJEKppXccNRS0K9kMlJ8RlyJPNaJOkaIobkZectcNNlSMEZZGk4ZP1Zy0CbJFxF6l7sAFQHdy6NgNEEm0nZLk3KwoaMTpwp+Lh5C36nLLq21K9A56cZ+hkZON2qMCSgiybn90g4mqAywsc4lY7SASJRFK0Vo5hGvVSTx5TdgMDhv39kHjTUtOuY647GgR0MTztf0aZf/fU4/JF2pagwg==[/KText]" />

</appSettings>

<!--

For a description of web.config changes see http://go.microsoft.com/fwlink/?LinkId=235367.

The following attributes can be set on the <httpRuntime> tag.

<system.Web>

<httpRuntime targetFramework="4.5.1" />

</system.Web>

-->

<system.web>

<compilation debug="true" targetFramework="4.5.1" />

<httpRuntime targetFramework="4.5" />

</system.web>

<system.webServer>

<validation validateIntegratedModeConfiguration="false" />

<handlers>

<remove name="ExtensionlessUrlHandler-ISAPI-4.0\_32bit" />

<remove name="ExtensionlessUrlHandler-ISAPI-4.0\_64bit" />

<remove name="ExtensionlessUrlHandler-Integrated-4.0" />

<add name="ExtensionlessUrlHandler-ISAPI-4.0\_32bit" path="\*." verb="GET,HEAD,POST,DEBUG,PUT,DELETE,PATCH,OPTIONS" modules="IsapiModule" scriptProcessor="%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet\_isapi.dll" preCondition="classicMode,runtimeVersionv4.0,bitness32" responseBufferLimit="0" />

<add name="ExtensionlessUrlHandler-ISAPI-4.0\_64bit" path="\*." verb="GET,HEAD,POST,DEBUG,PUT,DELETE,PATCH,OPTIONS" modules="IsapiModule" scriptProcessor="%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet\_isapi.dll" preCondition="classicMode,runtimeVersionv4.0,bitness64" responseBufferLimit="0" />

<add name="ExtensionlessUrlHandler-Integrated-4.0" path="\*." verb="GET,HEAD,POST,DEBUG,PUT,DELETE,PATCH,OPTIONS" type="System.Web.Handlers.TransferRequestHandler" preCondition="integratedMode,runtimeVersionv4.0" />

<remove name="OPTIONSVerbHandler" />

<remove name="TRACEVerbHandler" />

</handlers>

</system.webServer>

<runtime>

<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">

<dependentAssembly>

<assemblyIdentity name="System.Web.Helpers" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-2.0.0.0" newVersion="2.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Web.Mvc" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="1.0.0.0-4.0.0.0" newVersion="4.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Web.WebPages" publicKeyToken="31bf3856ad364e35" />

<bindingRedirect oldVersion="0.0.0.0-3.0.0.0" newVersion="3.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Web.Razor" publicKeyToken="31bf3856ad364e35" culture="neutral" />

<bindingRedirect oldVersion="0.0.0.0-3.0.0.0" newVersion="3.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Web.WebPages.Razor" publicKeyToken="31bf3856ad364e35" culture="neutral" />

<bindingRedirect oldVersion="0.0.0.0-3.0.0.0" newVersion="3.0.0.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="Microsoft.WindowsAzure.Storage" publicKeyToken="31bf3856ad364e35" culture="neutral" />

<bindingRedirect oldVersion="0.0.0.0-3.0.3.0" newVersion="3.0.3.0" />

</dependentAssembly>

<dependentAssembly>

<assemblyIdentity name="System.Data" publicKeyToken="b77a5c561934e089" culture="neutral" />

<bindingRedirect oldVersion="0.0.0.0-4.0.0.0" newVersion="4.0.0.0" />

</dependentAssembly>

</assemblyBinding>

</runtime>

<entityFramework>

<defaultConnectionFactory type="System.Data.Entity.Infrastructure.LocalDbConnectionFactory, EntityFramework">

<parameters>

<parameter value="v11.0" />

</parameters>

</defaultConnectionFactory>

<providers>

<provider invariantName="System.Data.SqlClient" type="System.Data.Entity.SqlServer.SqlProviderServices, EntityFramework.SqlServer" />

</providers>

</entityFramework>

</configuration>

### DB

## Secret Management

CMP requires access to a number of secrets in order to perform it’s functions. You may use the KTextEncryptor utility to create ciphertext for KText blocks.

|  |  |  |
| --- | --- | --- |
| Name | Source | Store |
| … | Request | DB |
| … | DB | DB |
| … | Config | Config |

**Encryption Model:**  
  
**Asymmetric crypto.**

* Encrypt: Clear->ToUTF8->RSACryptoServiceProvider->ToB64->Ciphertext
* Decrypt: FromB64->RSACryptoServiceProvider->FromUTF8->Cleartext
* Shared cert: .cer used by operators, .pfx used by cloud service.
* Encryption performed on premises with desktop tool.
* Decryption performed in cloud service.

#### Storage:

* Ciphertext is stored in a KText block. KText Block := [KText]<ciphertext>[/KText]
* A KText block may appear in any string.
* At config time the operator encrypts clear text and inserts the ciphertext into KText blocks.
* At config time the operator uses the KTextUtil tool to create KText blocks (see appendix)
* During runtime processing the blocks are removed and the ciphertext is resolved with the Cleartext. For example:  
    
     
    
  “The Secret is -> ‘[KText]W2r…hsdr==[/KText]’” would resolve to “The Secret is -> ‘Happiness’”

#### Configuration:

**App Settings**

|  |  |  |  |
| --- | --- | --- | --- |
| Setting | Location | Format | Description |
| KryptoCert | Key/Value | <StoreLocation>,<store>,<Thumb> | Specifies the cert to be used for decryption |
| <KText Block> | Value | [KText]<ciphertext>[/KText] | Ciphertext block inserted into any string value. |

<appSettings>

<add key="KryptoCert" value="LocalMachine, My, 345…148" />

<add key="DomainJoinAccount" value="redmond, superfly, [KText]1…ekw==[/KText]" />

<add key="CMPContextPassword" value="[KText]k7o6…0Ka==[/KText]" />

</appSettings>

**Connection Strings**

Special handling. Add connection string as usual to config file, blank out clear password:

<connectionStrings>

<add name="CMPContext" connectionString="Data Source=vp947thmuq.database.windows.net,1433;Initial Catalog=CMP;Persist Security Info=True;User ID=markw@vp947thmuq;Password=XXX;MultipleActiveResultSets=True;Encrypt=True"

providerName="System.Data.SqlClient" />

</connectionStrings>

Add a key to the AppSettings section named “<ConnectionSting.name>Password” with the ciphertext of the password in a KText block:

<appSettings>

<add key="CMPContextPassword" value="[KText]k7o…U0Ka ==[/KText]" />

</appSettings>

--------------------------------------------

### CmpAzureServiceWebRole

### Web.config

**App Settings**

|  |  |  |  |
| --- | --- | --- | --- |
| Setting | Location | Format | Description |
| KryptoCert | appSettings | <StoreLocation>,<store>,<Thumb> | Specifies the cert to be used for decryption |
| CMPContext | Connection String | <connectionString> | A standard SQL auth connection string with the password value replaced with ‘XXX’ |
| CMPContext | appSettings | <connectionString> | A standard SQL auth connection string with the password value replaced with ‘XXX’ (intentional duplicate) |
| CMPContextPassword | appSettings | [KText]<ciphertext>[/KText] | Ciphertext value of the CMPContext connection string password |
| CmpServiceUserName | appSettings | <username> | Basic Auth creds username used to access Cmp Web Service Interface |
| CmpServiceUserPassword | appSettings | [KText]<ciphertext>[/KText] | Basic Auth creds user password used to access Cmp Web Service Interface |

Sample Values

<configuration>

<connectionStrings>

<add name="CMPContext" connectionString="Data Source=x1wbwqfi4p.database.windows.net,1433;Initial Catalog=CmpUatDb;Persist Security Info=True;User ID=markw@x1wbwqfi4p;Password=XXX;MultipleActiveResultSets=True;Encrypt=True" providerName="System.Data.SqlClient" />

</connectionStrings>

<appSettings>

<add key="KryptoCert" value="LocalMachine,My,339C80283637D69D9D9F0F5FE00970D93CB0A148" />

<add key="CMPContext" value="Data Source=x1wbwqfi4p.database.windows.net,1433;Initial Catalog=CmpUatDb;Persist Security Info=True;User ID=markw@x1wbwqfi4p;Password=XXX;MultipleActiveResultSets=True;Encrypt=True" />

<add key="CMPContextPassword" value="[KText]aNVLpJUPQW0bosxnlW6tqzms1/Z3rylXz5sK+nXf6Jn7Bob9uF55FwIF4mjkdOGx2ZW0PQ8Mr1T87RabzI5vKrWFQFZ+4AXY+HR+jkRpLCVUjTiRE3Jxb8KNkibdc85NJIjJEKppXccNRS0K9kMlJ8RlyJPNaJOkaIobkZectcNNlSMEZZGk4ZP1Zy0CbJFxF6l7sAFQHdy6NgNEEm0nZLk3KwoaMTpwp+Lh5C36nLLq21K9A56cZ+hkZON2qMCSgiybn90g4mqAywsc4lY7SASJRFK0Vo5hGvVSTx5TdgMDhv39kHjTUtOuY647GgR0MTztf0aZf/fU4/JFyyyyy==[/KText]" />

<add key="CmpServiceUserName" value="CmpServiceUser" />

<add key="CmpServiceUserPassword" value="[KText]aNVLpJUPQW0bosxnlW6tqzms1/Z3rylXz5sK+nXf6Jn7Bob9uF55FwIF4mjkdOGx2ZW0PQ8Mr1T87RabzI5vKrWFQFZ+4AXY+HR+jkRpLCVUjTiRE3Jxb8KNkibdc85NJIjJEKppXccNRS0K9kMlJ8RlyJPNaJOkaIobkZectcNNlSMEZZGk4ZP1Zy0CbJFxF6l7sAFQHdy6NgNEEm0nZLk3KwoaMTpwp+Lh5C36nLLq21K9A56cZ+hkZON2qMCSgiybn90g4mqAywsc4lY7SASJRFK0Vo5hGvVSTx5TdgMDhv39kHjTUtOuY647GgR0MTztf0aZf/fU4/JFxxxxx==[/KText]" />

</appSettings>

</configuration>

--------------------------------------------

### CmpAzureWorkerWorkerRole

### App.config

**App Settings**

|  |  |  |  |
| --- | --- | --- | --- |
| Setting | Location | Format | Description |
| KryptoCert | appSettings | <StoreLocation>,<store>,<Thumb> | Specifies the cert to be used for decryption |
| CMPContext | Connection String | <connectionString> | A standard SQL auth connection string with the password value replaced with ‘XXX’ |
| DomainJoinAccount | appSettings | <domain>,<name>,[KText]<ciphertext>[/KText] | This account is used as the domain creds to join each new VM to the given domain. KText is the ciphertext value of the account password. |
| CmpWorker.DomainJoin.DomainName | appSettings | <domain> | This is the domain on which the CmpWorker service should reside. |
| CmpWorker.DomainJoin.UserName | appSettings | <account name> | This account is used as the domain creds to join the CmpWorker service to the given domain. |
| CmpWorker.DomainJoin.UserPassword | appSettings | [KText]<ciphertext>[/KText] | KText is the ciphertext value of the CmpWorker service domain join account password. |
| AUTOLOCALADMINUSERNAME | appSettings | <user name> | Local VM admin user of each new VM created |
| AUTOLOCALADMINPASSWORD | appSettings | [KText]<ciphertext>[/KText] | Ciphertext value of the local VM admin account password |
| CMPContextPassword | appSettings | [KText]<ciphertext>[/KText] | Ciphertext value of the CMPContext connection string password |
|  |  |  |  |

Sample Values

<configuration>

<configSections>

<connectionStrings>

<add name="CMPContext" connectionString="Data Source=x1wbwqfi4p.database.windows.net,1433;Initial Catalog=CmpUatDb;Persist Security Info=True;User ID=markw@x1wbwqfi4p;Password=XXX;MultipleActiveResultSets=True;Encrypt=True" providerName="System.Data.SqlClient" />

</connectionStrings>

<appSettings>

<add key="KryptoCert" value="LocalMachine,My,339C80283637D69D9D9F0F5FE00970D93CB0A148" />

<add key="DomainJoinAccount" value="redmond,markwes,[KText]kdPXcqVzA9R3ZK3Z8kP8FcNQEaVz6GR5ptji8pEiD5TJRq/Vr7I7oX9lMlWJoMwEEE1msvtLJ8Fun2JrUDBgeQtjjz9j0Pj/vKqhqmsHDL4jG9L3YXzq2tu2qLS5uyAJdd5iD8RME0eGCV8TzjzqSUGC9P/t3cQa8DTx9EMxrrvJaSJWb3cbHNiFvP56jVKNnZHN9GE7lGv8ggKoQYOxI3J/gZUk6egxvPlSktURXZX6TlxeFJnPqEVJhNFUpFAa417W+dB5m1ERCC/psruhKs43XszSAIJHVVpyzDaVjZASDJxtLDFg8ikRzLpe9RcWwl4c2xFclgZdtF1SBg1sWQ==[/KText]" />

<add key="CmpWorker.DomainJoin.DomainName" value="redmond.corp.microsoft.com" />

<add key="CmpWorker.DomainJoin.UserName" value="markwes" />

<add key="CmpWorker.DomainJoin.UserPassword" value="[KText]kdPXcqVzA9R3ZK3Z8kP8FcNQEaVz6GR5ptji8pEiD5TJRq/Vr7I7oX9lMlWJoMwEEE1msvtLJ8Fun2JrUDBgeQtjjz9j0Pj/vKqhqmsHDL4jG9L3YXzq2tu2qLS5uyAJdd5iD8RME0eGCV8TzjzqSUGC9P/t3cQa8DTx9EMxrrvJaSJWb3cbHNiFvP56jVKNnZHN9GE7lGv8ggKoQYOxI3J/gZUk6egxvPlSktURXZX6TlxeFJnPqEVJhNFUpFAa417W+dB5m1ERCC/psruhKs43XszSAIJHVVpyzDaVjZASDJxtLDFg8ikRzLpe9RcWwl4c2xFclgZdtF1SBg1sWQ==[/KText]" />

<add key="AUTOLOCALADMINUSERNAME" value="123User!!" />

<add key="AUTOLOCALADMINPASSWORD" value="[KText]MpYWdBSk/LjqqZmFmZCls4fMVDJhHZC5TgJRqdUiSxI/oV1yq9SFi2q6bZvR0sxN83tCQn3Dxgja0IUvxkw1eXlgcFCaFOzwuTYhiAL9gNZXpLwW1QKuGkOFHVC5xopweUS3xdBFkOnR+JkUrXy4kU7gEKc9nhSM1KPOegQCFsEAfoQhbbjSYmq0eUxkcQIbTbKhWlBOGop9ny0N3XY/P5gP56hfPT0WdpwKLynUEYnSRTBMbigjnJ8+WZKzBzsyB1XSRJQZzkdXajY/EBgU3n1FD4MXH2X21wxZ7d9VCB2uCBGjWFIETHVtflVbBv7oNEBvM7IlmOw+BDsMPKFc/w==[/KText]" />

<add key="CMPContextPassword" value="[KText]aNVLpJUPQW0bosxnlW6tqzms1/Z3rylXz5sK+nXf6Jn7Bob9uF55FwIF4mjkdOGx2ZW0PQ8Mr1T87RabzI5vKrWFQFZ+4AXY+HR+jkRpLCVUjTiRE3Jxb8KNkibdc85NJIjJEKppXccNRS0K9kMlJ8RlyJPNaJOkaIobkZectcNNlSMEZZGk4ZP1Zy0CbJFxF6l7sAFQHdy6NgNEEm0nZLk3KwoaMTpwp+Lh5C36nLLq21K9A56cZ+hkZON2qMCSgiybn90g4mqAywsc4lY7SASJRFK0Vo5hGvVSTx5TdgMDhv39kHjTUtOuY647GgR0MTztf0aZf/fU4/JF2pagwg==[/KText]" />

</appSettings>

</configuration>