1. Install **IIS Web Server** with all required features and management tools.
	1. Start Server Manager, run **Add roles and features** wizard and install following:

Roles:

* **Web Server IIS**

Web Server IIS Role features and services:

* **Web Server** -> **Security** -> **Windows Authentication**
* **Web Server** -> **Application Development** -> **ASP.NET 4.6**
1. Setup **Web Site**
	1. Create Folder **c:\inetpub\AMS**
	2. Copy Application files to **c:\inetpub\AMS**
	3. Open **IIS management console**. Select Server.
	4. Create Web Site. In **IIS Management Console** right click on **Sites** -> **Add Website…**
	5. Fill fields as shown:



* 1. Setup Web Site **Authentication**. Select site **AMS.**
* Double click **Authentication** icon.
* Disable all Authentication except **Windows Authentication**.



* Right Click **Windows Authentication** -> **Providers**
* Remove all providers and add **Negotiate:Kerberos.** Click **OK.**



* Right Click **Windows Authentication** -> **Advanced Settings…**
* Untick **Enable Kernel-mode authentication.**



* 1. Disable **Default Web Site**. Right click on it -> **Manage Web Site** -> **Stop**



* 1. Setup **Application Pool**. Click **Applications Pools** and right click **AMS** pool -> **Advanced Settings**
* Check that **Managed Pipeline Mode** is **Integrated**
* Checkthat **.NET CLR Version** is **4.0**
* Change **Start Mode** to **Always Running**
* Change **Pool Identity** to **LocalSystem**



* 1. Change **Windows Authentication Settings** for **AMS Web Site**. Select AMS site in left pane and double click **Configuration Editor**. 

In dropdown tree menu select **system.webServer** -> **security** -> **authentication** -> **windowsAuthentication**



Setup parameters as shown:



And сlick **Apply** on the right pane.

* 1. Disable all other pools. Right click on pool -> **Stop**.
1. Setup **Kerberos Authentication**
	1. Create **SPN** for web server account. Open **cmd** as user that haswrite access to web server AD account and run command:

**setspn -s HTTP/\_service\_URL\_ \_WEBSERVER\_HOSTNAME\_**

For example if service URL – **ams.asp.xaracloud.net** and Web Server Host Name **– ukbth05man00:**

**setspn -s HTTP/ams.asp.xaracloud.net ukbth05man00**

Check that SPN created successfully:

**C:\Users\asp360admin>setspn -l ukbth05man00**

**Registered ServicePrincipalNames for CN=UKBTH05MAN00,OU=Management Servers,OU=Member Servers,DC=asp,DC=xaracloud,DC=net:**

 **HTTP/ams.asp.xaracloud.net**

3.2 Enable **Delegation** for Web Server AD Account.



1. Create task in **Windows Task Scheduler**
	1. Start **Windows Task Scheduler**,right click on **Task Scheduler Library** -> **Create Task…**
	2. Enter task **Name** and **Description**. On **Security Options** pane tick **Run whether user is logged on or not**.
	3. Click **Change User or Group…** button and select AD account to run task. All created tasks will run as selected AD account. So, this account must have necessary permissions in **AD**, **DFS** shares and **Exchange Server**. 
	4. Click **Triggers** tab. Create new trigger. Tick **Repeat task every:** and select desired time interval (1 hour). Select **for a duration of:** Indefinitely. Tick **Stop task if it runt longer than** and select time interval (1 hour). 
	5. Click **Actions** tab and create Action **Start a program.**

**Program/Script**:

powershell.exe

**Add arguments (optional):**

Invoke-WebRequest -Uri 'http://ams.asp.xaracloud.net/tasks.aspx?StartTasks=true' -Method GET -UseDefaultCredentials



Click **OK** in **Edit Action** window.

* 1. Click **OK** in Create task window and enter account password. If message about required permissions for selected account appears (for example – **Log on as batch job**)**,**  then open **Local Security Policy** management tool and grant required rights. 
1. Install **Powershell Modules**.

Run powershell with admin privileges and execute:

Install-Module -Name PSAlphaFS

1. Add users of the service to management servers built in **Remote Management Users** group.