



Updated 12th May 2020

WorkSpaces Manager provides a full Amazon WorkSpaces management portal.

Product highlights:

- WorkSpaces Environment Management with optional application self-service feature for domain group-based application deployment.
- Task driven User & WorkSpaces provisioning.
- Automatic reboot schedule defined on a per WorkSpaces basis.
- Cost reporting and Cost Optimisation.
- Optional WorkSpaces Agent to report on Processor, Memory and Disk statistics

WorkSpaces Manager provides a full Amazon WorkSpaces management portal. Containing both a user self-service portal and administration portal administration of WorkSpaces in a simple to use browser-based portal. This removes the need to provide staff with access to the AWS console and provides easy searching across all WorkSpaces and User information.

The optional WorkSpaces Agent can be deployed by domain GPO to gather hourly metrics on Processor and Memory utilisation and available disk space for root and user drives.

The User portal can be extended to provide application self-service if the environment, provide group-based application deployment service such as Liquidware FlexApp, SCCM or similar products.

WorkSpaces Manager is deployed as an appliance from the AWS MarketPlace as an EC2 instance.

| | |
|------------------|---|
| Version | 2.0.0 |
| By | Nuven Consulting Limited |
| Categories | Application Development Infrastructure as Code |
| Operating System | Windows, Windows Server 2016 |
| Delivery Method | AWS MarketPlane \ Amazon Machine Image |

Installation & configuration guide for AWS MarketPlace subscription

Introduction

This guide has been authored by experts at Nuvens in order to provide information and guidance concerning the installation and configuration of WorkSpaces Manager.

Information in this document is subject to change without notice. No part of this publication may be reproduced in whole or in part, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any external use by any person or entity without the express prior written consent of Nuvens Consulting Ltd.

Contents

| | |
|--|----|
| Introduction | 2 |
| Software Requirements | 4 |
| WorkSpaces Portal requirements | 4 |
| Workspace Client Agent Requirements..... | 4 |
| Additional Requirements | 4 |
| Pre-requisites..... | 5 |
| AWS WorkSpaces Cost Optimizer | 5 |
| Active Directory Service Account..... | 6 |
| Installing the WorkSpaces Management Portal from AWS MarketPlace..... | 7 |
| Join your WorkSpaces Manager instance to your Active Directory Domain..... | 14 |
| First Time Setup | 14 |
| Installing the WorkSpaces Agent | 20 |
| High Availability | 25 |
| Database | 25 |
| User/Admin Portal | 25 |
| Securing the Portal and adding a friendly portal address | 29 |
| Portal address | 29 |
| SSL Certificate | 30 |

Software Requirements

WorkSpaces Manager is available as a standalone product and consists of three parts: the Management Portal, the Update Service and the optional Client WorkSpaces agent. The WorkSpaces Management Portal provides one central location where users can manage their own WorkSpace and administrators can provision, manage & monitor the WorkSpaces environment.

The requirements specified below are for deployments up to 500 users. For larger deployments and deploying as an HA cluster please contact support@nuvens.co.uk.

WorkSpaces Portal requirements

| Component | Requirements |
|---------------------|--|
| Platforms Support | Windows Server 2008 R2/2012/2012 R2/2016/2019. Only 64-bit versions where applicable are supported. Both physical and virtual instances are also supported. |
| Additional Software | <ul style="list-style-type: none">• Microsoft® .NET Framework 4.6.2 or higher• Microsoft SQL Server Express or higher All additional software is included with the Workspaces Manager installer |
| Browsers Supported | Chrome 22.x, Firefox 12.x, and Internet Explorer 9.x or higher versions of these browsers. If you are using Internet Explorer 9, disable enhanced security. |
| CPU | 2 CPUs 1 gigahertz (GHz) or faster |
| Memory | 4 GB RAM |
| Storage | 20Gb of additional storage is provisioned with the Appliance |

If the WorkSpaces Manager Portal is being used to provision user accounts in AD a service account will be required with delegated access to the OU's that accounts will be created in.

Workspace Client Agent Requirements

The WorkSpaces Client requires the following for installation:

| Component | Requirements |
|---------------------|---|
| Platforms Support | Windows 7/8.1/10, Windows Server 2008 R2/2012/2012 R2/2016/2019 |
| Additional Software | Microsoft® .NET Framework 4.6.2 or higher |
| Browsers Supported | Chrome 22.x, Firefox 12.x, and Internet Explorer 9.x or higher versions of these browsers. If you are using Internet Explorer 9, disable enhanced security. |
| CPU | 2 CPUs 1 gigahertz (GHz) or faster |
| Memory | 2 GB RAM |
| Storage | 50 MB available hard disk space |

Additional Requirements

WorkSpaces Manager requires Active Directory to deploy its client files to the desktop and point the user to its configuration file. Users also must use Active Directory to login to their physical or virtual desktops.

Pre-requisites

The following pre-requisites should be created before launching the appliance from the AWS Marketplace.

Not all pre-requisites are mandatory, please read each one to determine if it's required.

AWS WorkSpaces Cost Optimizer

This is not a mandatory requirement however we recommend that this is applied and run in “Dry Run Mode”.

This AWS service auto switches WorkSpaces between Hourly and Monthly Cost modes to ensure the WorkSpaces costs are optimized. Please refer to the link below for more details and deployment instructions.

Please ensure that you are in the correct region before deployment.

<https://aws.amazon.com/solutions/amazon-workspaces-cost-optimizer/>

After deploying the WorkSpaces cost optimiser please make a note of the S3 Bucket ARN created.

Active Directory Service Account

Not Mandatory

When creating the AD Service Account to support AWS WorkSpaces you will have already provided an account with permissions to create computer objects within AD to the OU specified at the time.

We recommend using the same service account and providing additional permissions to delete computer objects. Through the Management Portal when a WorkSpace is terminated the system will then be able to remove the orphaned computer object.

The AD service account is also used to create user accounts and add/remove users from AD groups if the application management option is used.

Using Active Directory Users and Computers, you can delegate the administration of an Organizational Unit to user or group that may not have the administration permissions otherwise.

To do this, follow these steps:

1. On your domain controller, click Start and point to Administrative Tools.
2. Click on Active Directory Users and Computers.
3. In Active Directory Users & Computers, select the OU to delegate administration.
4. Right click the OU and click on Delegate Control. This will start the delegation control wizard.
5. In select User Account window, click Add.
6. Find the correct User or group and double click.
7. Click OK.
8. In Tasks to Delegate window, choose the permissions to assign and click Next.
9. Review the summary and click Finish.

Delegate policy-related permissions on a domain, OU, or site using GPMC

<http://technet.microsoft.com/en-us/library/cc759064%28WS.10%29.aspx>

Delegating Administration of Account and Resource OUs

<http://technet.microsoft.com/en-us/library/cc784406%28WS.10%29.aspx>

Installing the WorkSpaces Management Portal from AWS Marketplace

Firstly, ensure that you are logged on to your AWS Console. Then go to the AWS Marketplace and search for 'Workspaces Manager Appliance'. Alternatively, click this [link](#) to take you there.

When found, select 'Continue to subscribe'.

The screenshot shows the AWS Marketplace product page for 'WorkSpaces Manager Appliance' by Nuvens. The page includes a search bar, navigation tabs (Overview, Pricing, Usage, Support, Reviews), and a 'Continue to Subscribe' button. The 'What's Included' section notes that the product includes both software packages described below. The 'Highlights' section lists: Advanced Search Functionality, Import and Manage WorkSpaces at scale, and Intelligent Cost Optimisation with realtime performance monitoring and remote access. The pricing information shows a typical total price of \$0.064/hr.

You now need to subscribe to the software. Select 'Accept Terms'.

The screenshot shows the subscription page for 'WorkSpaces Manager Appliance'. It features a 'Continue to Configuration' button with the text 'You must first review and accept terms.' Below this, there is a 'Subscribe' button and a section titled 'Terms and Conditions'. The 'Nuvens Offer' section contains a dark grey box with the text: 'By subscribing to this software, you agree to the pricing terms and the seller's end user license agreement (EULA). Your use of AWS services is subject to the AWS Customer Agreement.' An 'Accept Terms' button is located to the right of this text. Below the offer box, there is a note: 'The following table shows pricing information for the listed software components. You're charged separately for your use of each component.'

Now select 'Continue to Configuration'.

 **WorkSpaces Manager Appliance** Continue to Configuration

[< Product Detail](#) [Subscribe](#)

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

Nuvens Offer

You have subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). Your use of AWS services is subject to the [AWS Customer Agreement](#).

| Product | Effective date | Expiration date | Action |
|------------------------------|----------------|-----------------|------------------------------|
| WorkSpaces Manager Appliance | 8/13/2019 | N/A | Show Details |

Change your Region to the region that you want your WorkSpaces Manager appliance to reside. Then select 'Continue to Launch'.

 **WorkSpaces Manager Appliance** Continue to Launch

[< Product Detail](#) [Subscribe](#) [Configure](#)

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Fulfillment Option

WorkSpaces Manager Appliance

Software Version

3.0.0 (Nov 19, 2019)

Whats in This Version
WorkSpaces Manager Appliance
running on t2.medium
[Learn more](#)

Region

EU (Ireland)

Pricing information

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

| | |
|------------------------------|--------|
| WorkSpaces Manager Appliance | \$0/hr |
|------------------------------|--------|

BYOL
running on t2.medium

From 'Choose Action', select 'Launch CloudFormation'. Then select 'Launch'.

The screenshot shows the 'WorkSpaces Manager Appliance' configuration page. At the top, there is a navigation bar with links for '< Product Detail', 'Subscribe', 'Configure', and 'Launch'. The main heading is 'Launch this software'. Below this, a sub-heading reads 'Review your configuration and choose how you wish to launch the software.' The 'Configuration Details' section includes:

- Fulfillment Option:** WorkSpaces Manager Appliance (running on t2.medium)
- Software Version:** 3.0.0
- Region:** EU (Ireland)

A 'Usage Instructions' button is located below the configuration details. The 'Choose Action' section features a dropdown menu set to 'Launch CloudFormation' and a descriptive text: 'Choose this action to launch your configuration through the AWS CloudFormation console.' A prominent orange 'Launch' button is positioned at the bottom right of the configuration area.

On the next section, accept all entries and select 'Next'.

The screenshot displays the 'Create stack' wizard in the AWS CloudFormation console. The breadcrumb trail is 'CloudFormation > Stacks > Create stack'. The left sidebar shows the progress: Step 1 (Specify template), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review). The main content area is titled 'Create stack' and is divided into two sections:

- Prerequisite - Prepare template:** This section explains that every stack is based on a template (JSON or YAML). It offers three options: 'Template is ready' (selected), 'Use a sample template', and 'Create template in Designer'.
- Specify template:** This section explains that a template is a JSON or YAML file. It provides two options for the template source: 'Amazon S3 URL' (selected) and 'Upload a template file'. Under 'Amazon S3 URL', a text box contains the URL: 'https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/c4228857-4beb-449c-9339-4a454042e716.e7f63b72-cdbd-4364-86f1-2e2085f9c59'. Below this, the 'Amazon S3 template URL' is displayed as 'S3 URL: https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/c4228857-4beb-449c-9339-4a454042e716.e7f63b72-cdbd-4364-86f1-2e2085f9c59f/template'. A 'View in Designer' button is also present.

At the bottom right, there are 'Cancel' and 'Next' buttons.

You now specify your parameters for your stack configuration. Enter :

Stack Name: Your stack name. Call it something that is relevant for your own identification.

Instance Type: Leave a t2.medium as they should be sufficient to run WorkSpaces Manager. (Drop down list)

Key Name: You may have multiple key names under your IAM account for your own account. Select one – this will be used to provide you with the local administrator credentials to the WorkSpaces Manager EC2 instance further down the line. NOTE : You will need the associated key file to be able to decrypt the password later on. (Drop down list)

RDPLocation: Enter a CIDR from which both WorkSpaces and Admins will access WorkSpaces Manager. You can amend this later.

Subname: Select a Private subnet for your WorkSpaces Manager to reside. (Drop down list)

VPCName: Select the VPC that you wish to place the WorkSpaces Manager in. (Drop down list)

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name

NuvensWorkSpacesManagerStack

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

InstanceType
WebServer EC2 Instance type

t2.medium

KeyName
Name of an existing EC2 KeyPair to enable SSH access to the instance

MikeAPNuvensKeyPair

RDPLocation
IP CIDR from which WorkSpaces and Admins will access the WorkSpaces Manager. You can add rules later by modifying the created security groups e.g. 10.0.0.0/16

172.31.0.0/16

SubName
Name of an existing Private Subnet

subnet-435a3e0b (172.31.16.0/20) (Private Subnet 1)

VPCName
Name of an existing Private VPC to deploy to

vpc-6e8fd708 (172.31.0.0/16) (MikeDevAccountVPC)

Cancel Previous Next

You now configure your stack options.

Tags: You can tag the resources if you wish.

Permissions: Leave this blank as permissions will be created for you.

Advanced Options: Keep all options as default. You can enter an SNS Topic ARN to notify you of when the stack is created, but this isn't necessary. You will know when it's finished as the WorkSpaces Manager will appear as an EC2 instance in the console.

Then select 'Next'.

The screenshot shows the 'Configure stack options' step in the AWS CloudFormation console. The breadcrumb trail is 'CloudFormation > Stacks > Create stack'. The left sidebar shows four steps: Step 1 'Specify template', Step 2 'Specify stack details', Step 3 'Configure stack options' (which is the current step), and Step 4 'Review'. The main content area is titled 'Configure stack options' and contains two sections: 'Tags' and 'Permissions'. The 'Tags' section has a description: 'You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. [Learn more.](#)' It features two input fields labeled 'Key' and 'Value', and a 'Remove' button. Below these is an 'Add tag' button. The 'Permissions' section has a description: 'Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more.](#)' It includes a sub-section 'IAM role - optional' with the instruction 'Choose the IAM role for CloudFormation to use for all operations performed on the stack.' Below this is an 'IAM role name' dropdown menu with a 'Sample-role-name' placeholder and a 'Remove' button.

The screenshot shows the 'Advanced options' step in the AWS CloudFormation console. The breadcrumb trail is 'CloudFormation > Stacks > Create stack'. The left sidebar shows four steps: Step 1 'Specify template', Step 2 'Specify stack details', Step 3 'Configure stack options', and Step 4 'Review' (which is the current step). The main content area is titled 'Advanced options' and has a description: 'You can set additional options for your stack, like notification options and a stack policy. [Learn more.](#)' It contains four expandable sections: 'Stack policy' (with subtext 'Defines the resources that you want to protect from unintentional updates during a stack update.'), 'Rollback configuration' (with subtext 'Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. [Learn more.](#)'), 'Notification options', and 'Stack creation options'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next' (which is highlighted in orange).

You will now find yourself at the 'Review' screen. Scroll down to the bottom, select the acknowledgement and then select 'Create Stack'.

► Quick-create link

Capabilities

ⓘ The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more.](#)

I acknowledge that AWS CloudFormation might create IAM resources.

Cancel
Previous
Create change set
Create stack

You will now return to the stack status screen where you can see the progress of the WorkSpaces Manager stack.

CloudFormation > Stacks: NuvensWorkSpacesManagerStack

NuvensWorkSpacesManagerStack Delete Update Stack actions ▼ Create stack

Stack info | **Events** | Resources | Outputs | Parameters | Template | Change sets

Events

Q Search events

| Timestamp | Logical ID | Status | Status reason |
|------------------------------|------------------------------|--|----------------|
| 2019-08-15 12:58:09 UTC+0100 | NuvensWorkSpacesManagerStack | ⓘ CREATE_IN_PROGRESS | User Initiated |

You can view the tasks as they are being performed. When the stack creation is complete, the status will change from 'CREATE_IN_PROGRESS' to 'CREATE_COMPLETE'. The stack creation takes around 3-4 minutes to complete.

CloudFormation > Stacks: NuvensWorkSpacesManagerStack

NuvensWorkSpacesManagerStack Delete Update Stack actions ▼ Create stack

Stack info | **Events** | Resources | Outputs | Parameters | Template | Change sets

Events

Q Search events

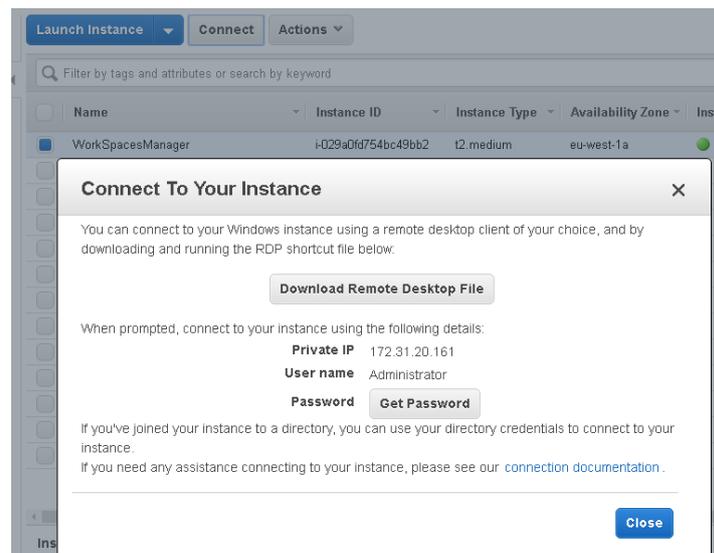
| Timestamp | Logical ID | Status | Status reason |
|------------------------------|------------------------------------|--|-----------------------------|
| 2019-08-15 15:00:38 UTC+0100 | EC2Instance | ⓘ CREATE_IN_PROGRESS | Resource creation Initiated |
| 2019-08-15 13:00:36 UTC+0100 | EC2Instance | ⓘ CREATE_IN_PROGRESS | - |
| 2019-08-15 13:00:34 UTC+0100 | InstanceProfile | ✔ CREATE_COMPLETE | - |
| 2019-08-15 12:58:43 UTC+0100 | WorkSpacesManagerS3Access | ✔ CREATE_COMPLETE | - |
| 2019-08-15 12:58:42 UTC+0100 | Pricing | ✔ CREATE_COMPLETE | - |
| 2019-08-15 12:58:42 UTC+0100 | WorkSpacesManagerCloudwatch Policy | ✔ CREATE_COMPLETE | - |

If you now view your EC2 instances in the region that you chose to install WorkSpaces Manager, you'll see the WorkSpaces Manager instance. Give this around 5-10 minutes for the Status Checks to finish and for local administrator password the auto generated.



| Name | Instance ID | Instance Type | Availability Zone | Instance State | Status Checks | Alarm Status | Public DNS (IPv4) |
|-------------------|---------------------|---------------|-------------------|----------------|-------------------|--------------|-------------------|
| WorkSpacesManager | i-029a0fd754bc49bb2 | t2.medium | eu-west-1a | running | 2/2 checks passed | None | |

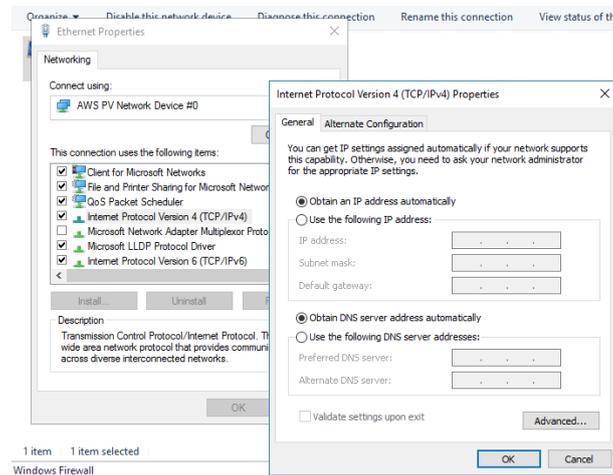
Now RDP to your instance using the Private IP assigned to the instance using the local administrator password and using the KeyName and associated keyfile that you specified in the Stack Details section above. If you cannot RDP to the instance, you need to be connecting from a device in the network CIDR that you specified in RDPLocation in Stack Details section above.



Join your WorkSpaces Manager instance to your Active Directory Domain

Connect to the WorkSpaces Manager instance and join it to your Active Directory domain. Once complete, you can now go to the next section on 'First Time Setup'.

PLEASE NOTE: You need to have your DHCP options set in AWS to be able to find your domain, or enter your DNS servers manually in the TCP/IPv4.



First Time Setup

Log on to the WorkSpaces Manager EC2 instance, go to Internet Explorer and browse to <http://localhost>.

From a browser, connect to the Private IP address of the WorkSpaces Manager portal instance from a device in the 'RDPLocation' CIDR range specified above in 'Specify Stack Details'. If you get this message, you can either enter your DOMAIN\USERNAME and password, or you can go to Internet Explorer > Internet Options and add the website address (e.g. <http://private-ip-of-your-instance>) to Trusted Sites or Local Intranet. You can also provide your portal with a friendly portal name address (e.g. <http://workspacesmanager.yourdomain>) which means that it will most likely be accepted from most\all browsers in your organisation without amending the Trusted Sites or Local Intranet settings. To give it a friendly name, see the section 'Securing the Portal and adding a friendly portal address'.

Sign in
<http://172.31.20.161>
Your connection to this site is not private

Username

Password

When you can successfully connect to the portal, you will be presented with a setup screen to enter information for

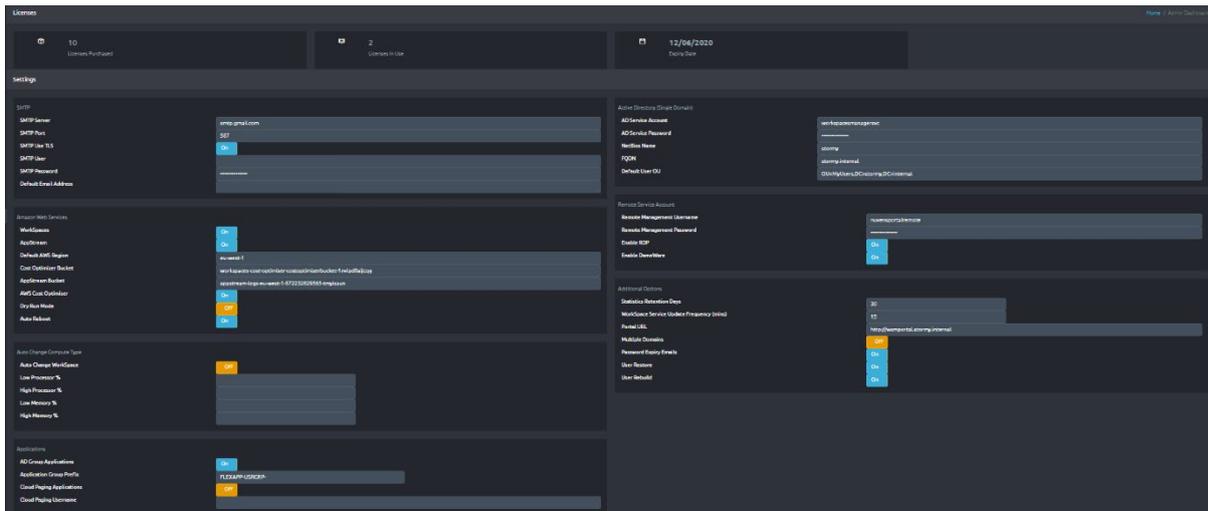
- License key
- AD Service account
- SMTP details
- Default AWS Region
- Other system settings.

The license key will have been sent via email when you registered on the AWS Marketplace.

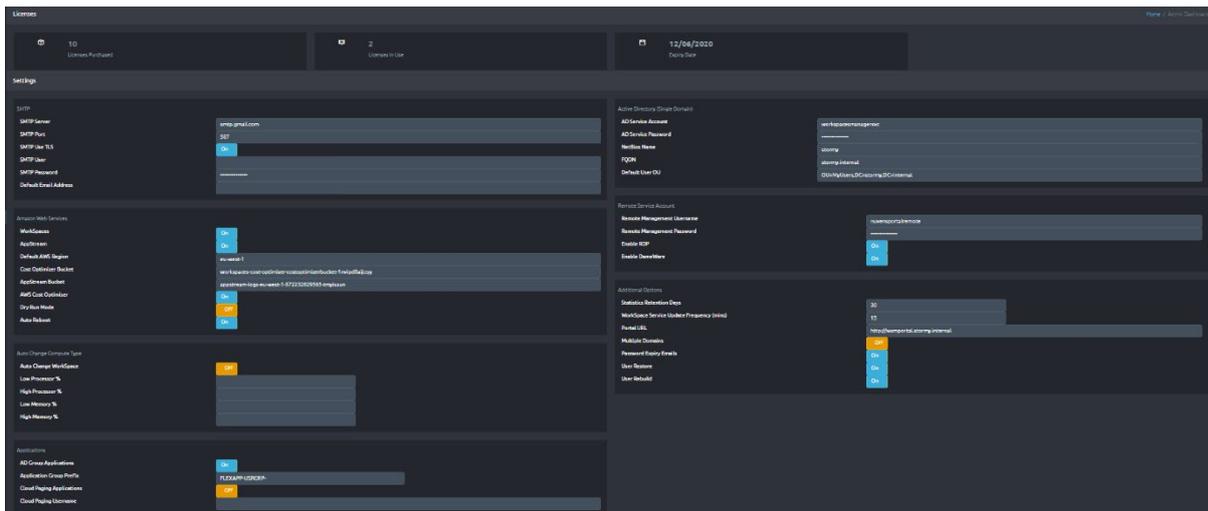
The screenshot shows a dark-themed setup interface with the following sections:

- License Key:** A text box containing the message: "The License Key will have been sent by email. It can also be obtained from your Nuvens account".
- SMTP:** Fields for SMTP Server, SMTP Port, SMTP Use TLS (toggle: OFF), SMTP User, SMTP Password, and Default Email Address.
- Active Directory:** Fields for AD Service Account, AD Service Password, NetBios Name, FQDN, Default User OU, and Password Expiry Emails (toggle: OFF).
- Amazon Web Services:** Fields for Default AWS Region, Cost Optimizer Bucket, and AWS Cost Optimiser (toggle: OFF). Toggles for Dry Run Mode and Auto Reboot are also present.
- Remote Service Account:** Fields for Remote Management Username and Remote Management Password.
- Additional Options:** Toggles for Enable Applications (OFF), Admin Group (text box), Enable RDP (OFF), and Enable DameWare (OFF).

This is an example of the Portal filled in.



Now press 'Save'. Please wait for up to 30 seconds for the next screen to appear. When it does, it will show the administration section of the portal on the License\Settings page. You can change settings in here where you see them.



Sections explained:

| Required to advance | |
|----------------------------------|--|
| License Key | This will be sent to you when you register the Portal on AWS Marketplace. |
| Active Directory (Single Domain) | <p>NOTE : If you have users in more than one domain, you can turn on the 'Multiple Domains' feature in the 'Additional Options' section. You can learn more in 'Section 9 – Mult-Domain Forest' of the WorkSpaces Manager User Guide.</p> <p>AD Service Account and password: When creating the AD Service Account to support AWS WorkSpaces you will have already provided an account with permissions to create computer objects within AD to the OU specified at the time. We recommend using the same service account and providing additional permissions to delete computer objects.</p> |

| | |
|--|--|
| | <p>NetBIOS name: NetBIOS name of the domain that your WorkSpaces will be joining.</p> <p>FQDN: Fully Qualified Domain Name of the domain that your WorkSpaces will be joining.</p> <p>Default User OU: If you create a user in the 'Add User' section of the Portal, this is where it will place that user. If you use the 'Import Template' then you can specify where you want the user(s) to be located per OU or by copying template users.</p> |
|--|--|

These can be filled in later

| |
|--|
| SMTP |
| <p>This enables you to send emails to users when their new Workspace is ready and/or if their password is to expire in two weeks' time. You could use AWS Simple Email Service to achieve this, or your own SMTP setup.</p> |
| Amazon Web Services |
| <p>Workspaces: Turns on the WorkSpaces Management function.</p> <p>AppStream: <i>In development and not available yet.</i> Turns on the AppStream Management function.</p> <p>Default AWS Region: This is the AWS Region that your Amazon WorkSpaces are hosted in. For example, Ireland will be eu-west-1. A full list of Regions can be located here.</p> <p>Cost Optimizer Bucket: This is the bucket name mentioned in the 'AWS WorkSpaces Cost Optimizer' section earlier on the document.</p> <p>AppStream Bucket: <i>In development and not available yet.</i> This is where you put in your S3 bucket for your AppStream Usage Reports.</p> <p>AWS Cost Optimiser: This enables the AWS Cost Optimiser.</p> <p>Dry Run Mode: Running the Cost Optimiser in Dry Run Mode will show you the changes that would have been made</p> <p>Auto Reboot: This gives the ability to set reboot times on WorkSpaces. Available once you've set up the Portal.</p> |

Auto Change Compute Type

You can opt for WorkSpaces Manager to automatically change compute type of a WorkSpace. This is useful if, for example, you had a user running heavy spreadsheets on a Standard WorkSpace and it would benefit them with being upgraded to a Performance WorkSpace.

Set Low and High Processor and Memory values (these are up to you). WorkSpaces Manager will also advise you of recommendations.

Applications

AD Group Applications: Enable this is you use software distribution on to your WorkSpaces from the likes of LiquidWare FlexApp. This allows users to add and remove applications available to them through the Self Service side of the WorkSpaces Manager Portal. You can change this to your own prefix when you've logged into the Portal. For example, your FlexApp groups could be prefixed 'FLEXAPP-USRGRP'.

Application Group Prefix:

As above, this is the prefix of your application distribution groups with whatever product you are using (FlexApp, SCCM, etc).

Cloud Paging Applications:

If you want to use Nument Cloudpaging applications with WorkSpaces, you can enable this feature on here.

Cloud Paging Username:

This is where you enter the account name that you use for Numecent Cloudpaging.

Additional Options

Statistics Retention Days:

If the WorkSpace Agent has been deployed to the WorkSpaces, it will be reporting back to the server key metric statistics periodically as defined in the Group Policy (see section below on 'Installing The WorkSpaces Agent'). In a large estate, this will create millions of rows within the database over a period of time. The number of days that are retained within the database can be specified here. If the number of days are too high on a large estate (e.g. 60) then it will have an impact on queries of statistics and also increased disk space usage. For smaller estates, you can set this to 30 days and monitor from there.

WorkSpace Service Update Frequency (mins):

This will automatically update the local database with up to date information on this period. 15 minutes is sufficient for most cases, but you wouldn't want to do this on, for example, a 1 minute period on a very large WorkSpaces and user estate. If you need to do a manual update for any reason, you can do this in the Update section of the portal.

Portal URL:

Enter your portal URL here.

Multiple Domains:

If you are using a multi-domain forest, you can add multiple domains that host your user accounts. Therefore, their WorkSpaces can be managed, searched and reported on.

Password Expiry Emails:

If this is chosen, users will receive a notification email two weeks prior to their password expiring. This can be turned on/off whenever and is not required to complete the Portal configuration at this stage.

User Restore:

Enables the Self-Service function for a user to restore their Workspace to a last known healthy state. Automatic snapshots for use when restoring a Workspace are scheduled every 12 hours. If the Workspace is healthy, snapshots of both the root volume and user volume are created around the same time. If the Workspace is unhealthy, these snapshots are not created. If needed, a user can restore a Workspace to its last known healthy state. This recreates both the root volume and user volume, based on the most recent snapshots of these volumes that were created when the Workspace was healthy.

User Rebuild:

Enables the Self-Service function for a user to rebuild their Workspace.

- The system is refreshed with the most recent image of the bundle that the Workspace was created from. Any applications that were installed, or system settings that were changed after the Workspace was created, are lost.
- The user volume (for Microsoft Windows, the D drive; for Linux, /home) is recreated from the most recent snapshot. The current contents of the user volume are overwritten.
Automatic snapshots for use when rebuilding a Workspace are scheduled every 12 hours. If the Workspace is healthy, a snapshot of the user volume is created. If the Workspace is unhealthy, the snapshot is not created.
- The primary elastic network interface is recreated. The Workspace receives a new private IP address.

Remote Services Account

This is an account that you configure to remote control user devices using Dameware, etc. This is the generic account that you connect with (which will be standard throughout your organisation). You can remote control a user's WorkSpaces by selecting 'Dameware' (if you've selected the 'Enable Dameware' option in 'Additional Options' and it downloads a connection file for you to run.

Enable RDP:

Enables the option for downloading an RDP file to connect to the user's Workspace from within the Portal.

Enable DameWare:

Enables the option for downloading an RDP file to connect to the user's Workspace from within the Portal.

A 60 day unlimited Workspace trial is available after which a monthly billing subscription will be started. The System only counts active WorkSpaces used within the last 30 days and can be cancelled at any time.

For any assistance with the License key or setting up the WorkSpaces Manager Appliance please contact support@nuvens.co.uk

Installing the WorkSpaces Agent

The WorkSpaces Manager agent collects Processor, Memory and disk utilisation on an hourly basis.

The Agent installer can be found in “D:\WorkSpaceAgent” on the appliance.

The Agent requires a registry key value to be present to locate the database on the appliance.

[HKEY_USERS\DEFAULT\Software\Nuvens]

"Portal"="http://DNS or IP address of your portal" (REG_SZ)

(If you are using SSL, use **https** in place of http)

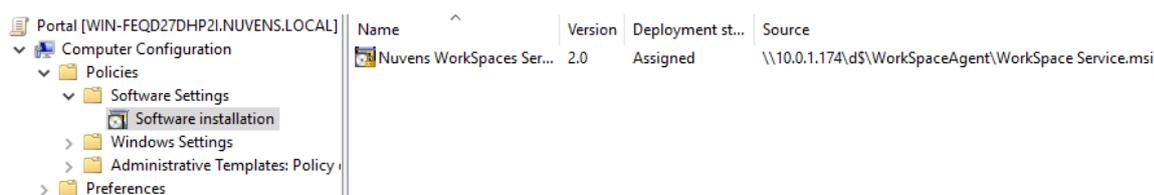
"Frequency" = "5" (REG_DWORD (32-bit))

(The value data is a numeric value of minutes (e.g. '5' where the Agent reports back to the database every 5 minutes with metrics. You can change this frequency to an increased value if you have a large estate as a lot of information will be stored in the database).

The best way to deploy the registry settings and the application is via a Group Policy or by using a distribution tool of your choice (such as Microsoft SCCM).

In Group Policy Manager Create a new Group policy on the OU containing the AWS WorkSpaces. Under Computer Configuration expand Policies:

- Expand Software Settings under Computer Configuration
- Right-click Software Installation, select the New context menu and then click on Package
- In the Open dialog type the full UNC path of the shared package you want to assign
- Click on the Open button
- Click on Assigned and then click OK (the package will be added to the right pane of the "Group Policy" window)



The required Registry values can be added on the same Group Policy

Under Computer Configuration expand Preferences: -

- Expand Windows Settings under Preferences
- Right-click Registry and create new registry item

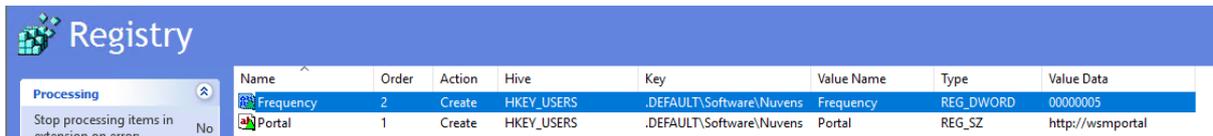
(a) Create the “Portal” registry value with the key

[HKEY_USERS\DEFAULT\Software\Nuvens]

- The value name is “Portal” of type REG_SZ.
- The value data is http (or https) and the IP address (or DNS address) of your WorkSpaces Manager appliance. (e.g. http://wsmportal).

(b) Create the “Frequency” registry value with the key [HKEY_USERS\DEFAULT\Software\Nuvens]

- The value name is “Frequency” of type REG_DWORD (32-bit)
- The value data is a numeric value of minutes (i.e. 5 where the agent reports back to the database every 5 minutes with metrics. You can change this frequency to an increased value if you have a large estate as a lot of information will be stored in the database).



The screenshot shows the Windows Registry Editor window titled "Registry". It displays a table of registry values. The table has columns for Name, Order, Action, Hive, Key, Value Name, Type, and Value Data. Two values are listed: "Frequency" and "Portal".

| Name | Order | Action | Hive | Key | Value Name | Type | Value Data |
|-----------|-------|--------|------------|--------------------------|------------|-----------|-----------------|
| Frequency | 2 | Create | HKEY_USERS | .DEFAULT\Software\Nuvens | Frequency | REG_DWORD | 00000005 |
| Portal | 1 | Create | HKEY_USERS | .DEFAULT\Software\Nuvens | Portal | REG_SZ | http://wsportal |

If you

The WorkSpaces Manager agent collects Processor, Memory and disk utilisation on an hourly basis.

The Agent installer can be found in "D:\WorkSpaceAgent" on the appliance.

The Agent requires a registry key value to be present to locate the database on the appliance.

[HKEY_USERS\DEFAULT\Software\Nuvens]

"Portal"="http://DNS or IP address of your portal" (REG_SZ)

(If you are using SSL, use https in place of http)

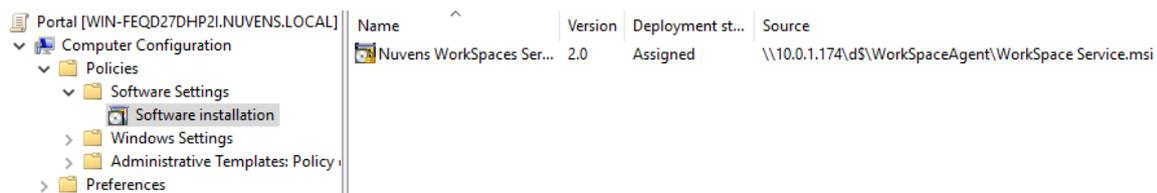
"Frequency" = "5" (REG_DWORD (32-bit))

(The value data is a numeric value of minutes (e.g. '5' where the Agent reports back to the database every 5 minutes with metrics. You can change this frequency to an increased value if you have a large estate as a lot of information will be stored in the database).

The best way to deploy the registry settings and the application is via a Group Policy or by using a distribution tool of your choice (such as Microsoft SCCM).

In Group Policy Manager Create a new Group policy on the OU containing the AWS WorkSpaces. Under Computer Configuration expand Policies:

- Expand Software Settings under Computer Configuration
- Right-click Software Installation, select the New context menu and then click on Package
- In the Open dialog type the full UNC path of the shared package you want to assign
- Click on the Open button
- Click on Assigned and then click OK (the package will be added to the right pane of the "Group Policy" window)



The required Registry values can be added on the same Group Policy

Under Computer Configuration expand Preferences: -

- Expand Windows Settings under Preferences
- Right-click Registry and create new registry item

(a) Create the "Portal" registry value with the key

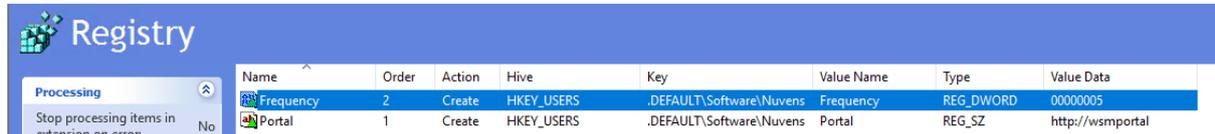
[HKEY_USERS\DEFAULT\Software\Nuvens]

- The value name is "Portal" of type REG_SZ.
- The value data is http (or https) and the IP address (or DNS address) of your WorkSpaces Manager appliance. (e.g. http://wsmportal).

(b) Create the “Frequency” registry value with the key

[HKEY_USERS\DEFAULT\Software\Nuvens]

- The value name is “Frequency” of type REG_DWORD (32-bit)
- The value data is a numeric value of minutes (i.e. 5 where the agent reports back to the database every 5 minutes with metrics. You can change this frequency to an increased value if you have a large estate as a lot of information will be stored in the database).



The screenshot shows the Windows Registry Editor window titled "Registry". On the left, there is a "Processing" pane with a "Stop processing items in extension on error" button and a "No" status. The main pane displays a table of registry values.

| Name | Order | Action | Hive | Key | Value Name | Type | Value Data |
|-----------|-------|--------|------------|--------------------------|------------|-----------|------------------|
| Frequency | 2 | Create | HKEY_USERS | .DEFAULT\Software\Nuvens | Frequency | REG_DWORD | 00000005 |
| Portal | 1 | Create | HKEY_USERS | .DEFAULT\Software\Nuvens | Portal | REG_SZ | http://wsmportal |

High Availability

The WorkSpaces Manager appliance is a single EC2 instance containing IIS & SQL Express. Providing you schedule a backup schedule for the EBS volumes associated with the appliance, recovery can be completed in under an hour.

Database

To achieve database HA we recommend on deploying AWS RDS Microsoft SQL Server into at least 2 Availability Zones.

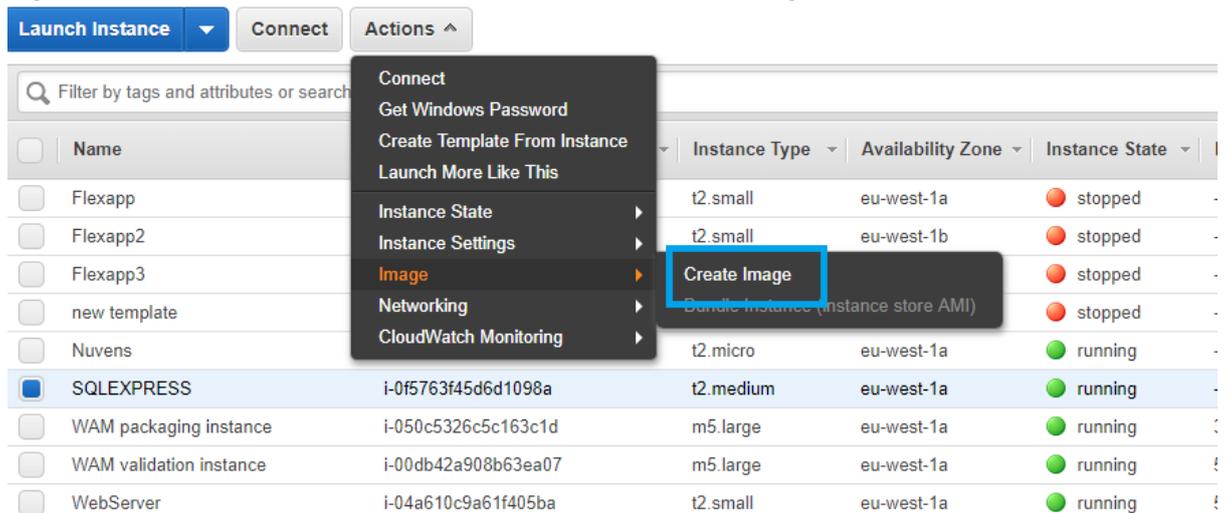
After deploying RDS you will need to do the following actions: -

- Change the registry key 'Portal' to point to the RDS database cluster endpoint.
- Edit the Web.Config in D:\Portal on the appliance from "127.0.0.1" to the RDS Cluster endpoint.
- Stop the 'PortalService' service on the appliance. Edit the service config file in "C:\Program Files (x86)\Nuvens Consulting Ltd\Nuvens AWS WorkSpaces Management Portal Service\PortalService.exe.config" and change the database connection string from "127.0.0.1" to the RDS Cluster endpoint. Then restart the appliance.

User/Admin Portal

There are several ways that HA can be provided for the Portal including Auto Scaling Groups. The simplest method is to make an Amazon Machine Image of your appliance.

1. Log into your Amazon Web Services EC2 site using your administrative credentials.
2. Right-click on the instance to make an AMI and select Create Image.

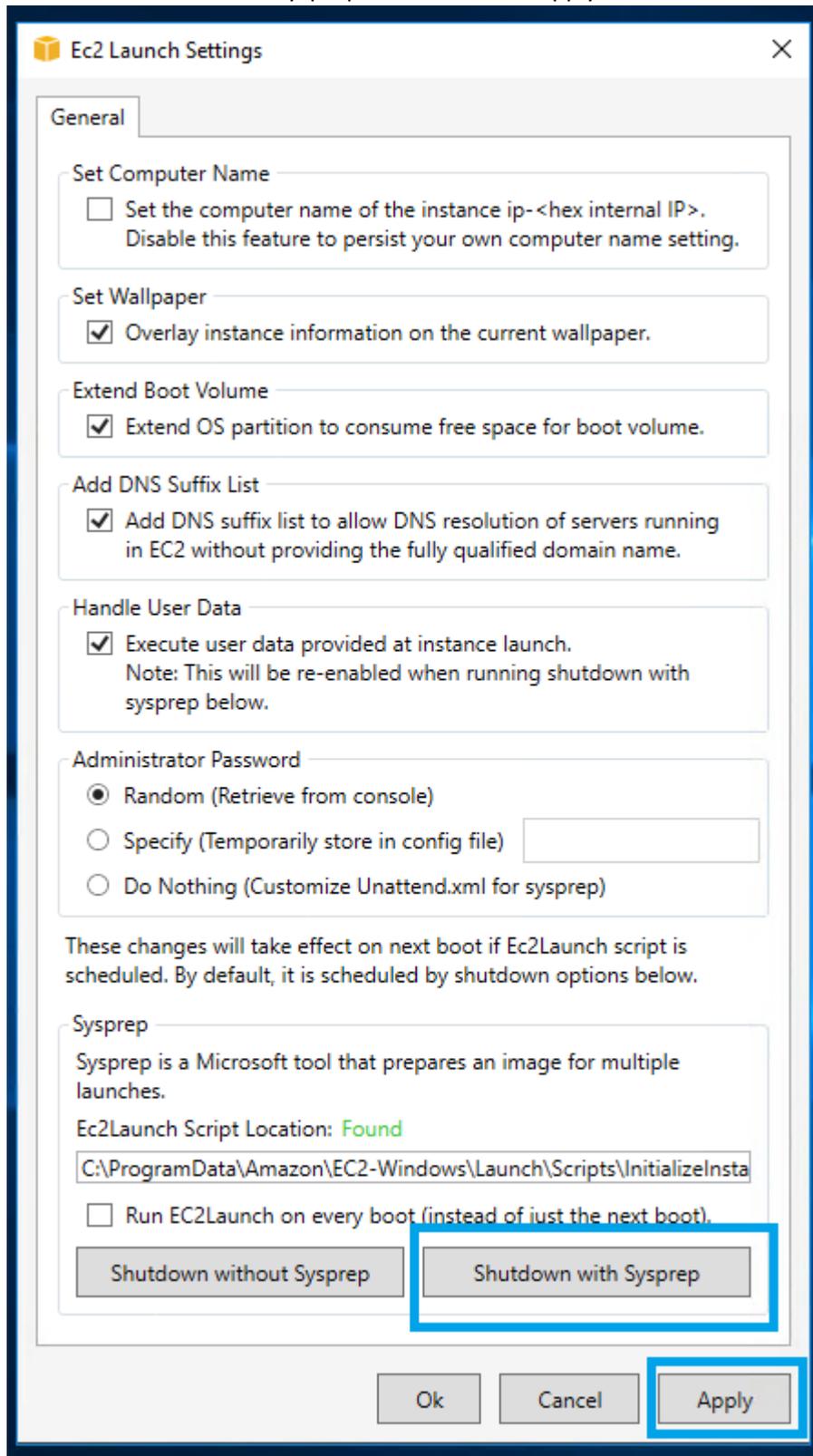


3. Name the Image and click Create Image

This will make a cloned image of your WorkSpaces Manager Instance. This can be kept as a backup.

To be able to deploy the image as another instance we need to first go through a process called SysPrep and create our deployable image.

1. Stop the original instance that the image was created from.
2. Launch the AMI just created as a new instance.
3. Once the instance is running connect via RDP.
4. Click the 'Windows' icon on the instance and start 'Ec2LaunchSettings'.
5. Click on 'Shutdown with Sysprep' and then click 'Apply'.



6. This will start a process of removing Windows user and system settings. Once it's complete the instance will be left in a stopped state.
7. The original appliance can now be started again.
8. The Sysprepped stopped image can now be imaged again to create our master appliance image. Once the AMI has been created you can terminate the source instance,

Now that we have created a master image this can be launched into an alternative Availability Zone in the Region. The same instructions as 'Installing the WorkSpaces Management Portal on AWS' can be used to launch the image however this time rather than installing from the Marketplace you will launch the instance from the AMI just created. If you are launching with domain joined configured and ensuring that you assign the 'WorkSpacesManager' Role, the instance will be available after about 30 minutes.

This has provided 2 instances in different AZ's configured to connect to HA RDS Microsoft SQL Server. However, we now need to create a single point of entry into the Portal.

1. From the AWS Console select 'EC2' Service then 'Target Groups'.
2. Click Create target group and provide a target group name before clicking 'Create'.

3. Register both WorkSpace Manager appliances with the target group

| Target group name | Port | Protocol | Target type | VPC |
|-------------------|------|----------|-------------|-----------------------|
| WorkSpaceManager | 80 | HTTP | instance | vpc-0b72b48baba3b00cd |

Target group: WorkSpaceManager

Description | **Targets** | Health checks | Monitoring | Tags

The load balancer starts routing requests to a newly registered target as soon as the registration process completes and the target passes the initial health checks. If demand on your targets decreases, you can deregister targets.

[Edit](#)

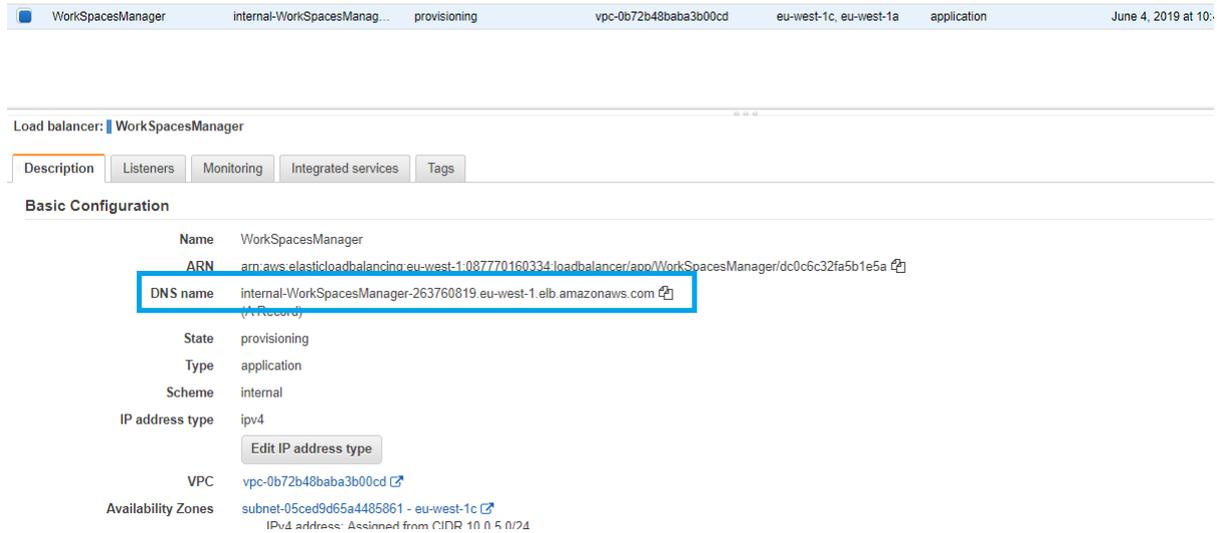
Registered targets

| Instance ID | Name | Port | Availability Zone |
|---------------------|---------------------|------|-------------------|
| i-08fc239002850311b | WorkSpaceManager-1c | 80 | eu-west-1c |
| i-0f5763f45d6d1098a | WorkSpaceManager-1a | 80 | eu-west-1a |

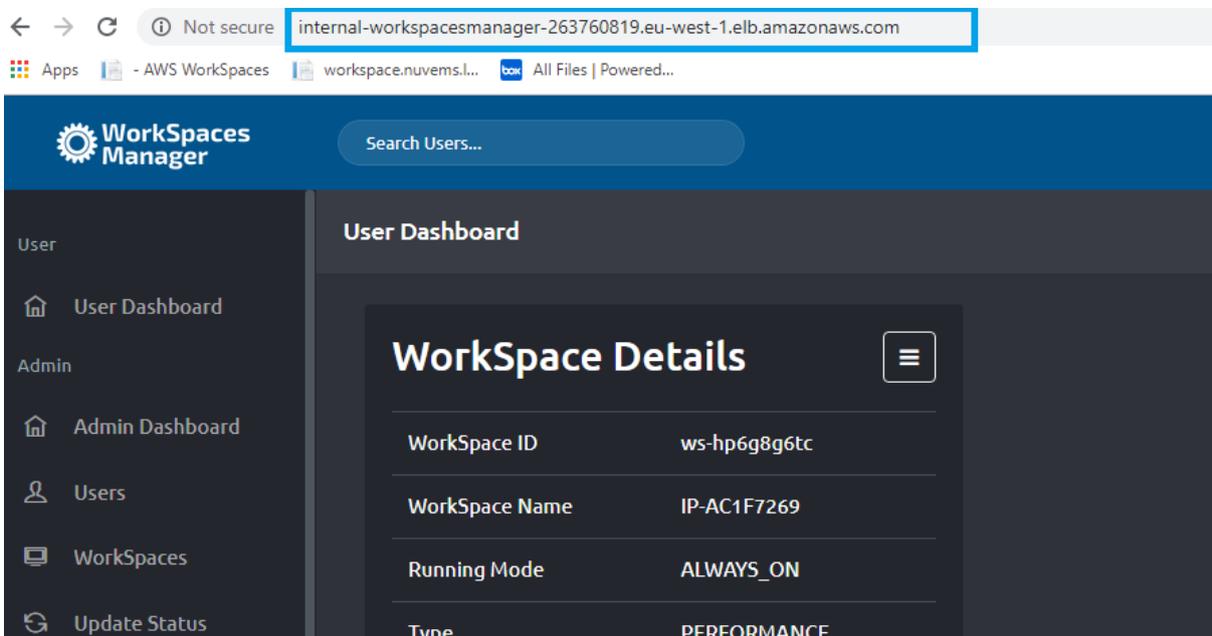
4. Next create an Application Load Balancer ensuring you select the Availability Zones that you used when creating the target group and the Scheme is set as 'Internal'.

5. On Step3: Configure Security Groups, create a new security allowing inbound HTTP from the private subnets.
6. On Step4: Configure Routing, select the target group we created above then click next and complete creation of the load balancer.

Once the load balancer has been created you can view the details of the load balancer including its DNS name.



The DNS name can be used to access the portal which will be load balanced across both instances



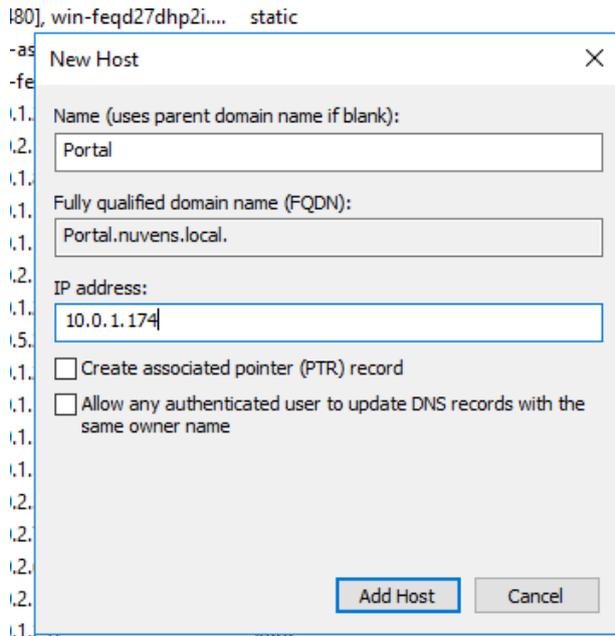
The portal is now in full HA mode load balanced across 2 AZ's with an HA database supporting it. However, the address is not very friendly. See 'Securing the Portal and adding a friendly portal address' below.

Securing the Portal and adding a friendly portal address

Portal address

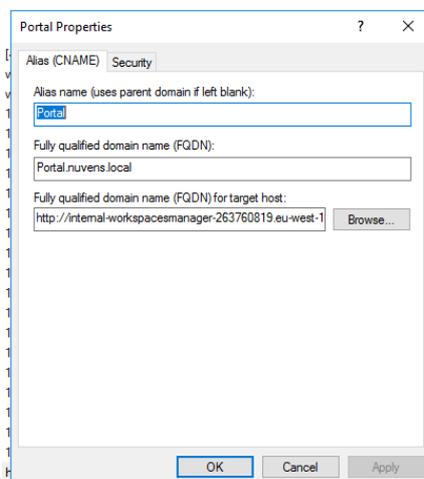
Rather than accessing the Portal via the IP address of the instance you can add a record to your DNS server.

From DNS manager add an A record to your domain referencing the IP address of the instance



This will now allow you to reference the portal in this scenario has <http://portal.nuvens.local>.

If you have configured load balancing then you will need to add a CNAME record and reference the DNS record of the load balancer which in this example would be:



SSL Certificate

Now that we have a friendly hostname we can associate an SSL certificate to encrypt traffic between the client browser and the host.

1. Select the Load Balancer previously created and click on listeners.
2. Add a listener for HTTPS port 443.
3. Create a Default action to forward to the target group.
4. Select the appropriate certificate from ACM.
5. Click 'Save'.

The screenshot shows the 'Add listener' configuration page in the AWS Management Console. At the top, there is a breadcrumb 'Listeners' and a page title 'WorkSpacesManager | Add listener'. A blue 'Save' button is visible in the top right corner. Below the header, a message states: 'Add a new listener. Each listener must include one action of type forward, redirect, fixed response.' The main section is titled 'WorkSpacesManager | Add listener' and contains the following configuration fields:

- Protocol : port**: A dropdown menu set to 'HTTPS' and a text input field containing '443'. Below this is the instruction: 'Select the protocol for connections from the client to your load balancer, and enter a port number from which to listen to for traffic.'
- Default action(s)**: A section with the instruction 'Indicate how this listener will route traffic that is not otherwise routed by a another rule.' It contains one action card titled '1. Forward to...' with a trash icon. The dropdown menu for this action is set to 'WorkSpaceManager' and has a blue checkmark. Below the action card is a '+ Add action' button.
- Security policy**: A dropdown menu set to 'ELBSecurityPolicy-2016-08' with a refresh icon.
- Default SSL certificate**: A dropdown menu set to 'From ACM (recommended)' and a text input field containing 'www.nuvens.info - 368d7643-dd63-4279-a590-850aceef98ce' with a refresh icon.