



Workspaces Manager- Installation guide

Updated 14th September for WorkSpaces Manager 4.7.0

Product highlights:

- WorkSpaces Environment Management with optional application self-service feature for domain group-based application deployment
- Task driven User & WorkSpaces provisioning
- Performance monitoring
- Multi-AWS Account
- Multi-Domain
- Automatic reboot schedule defined on a per WorkSpaces basis
- Cost reporting and Cost Optimisation.
- WorkSpaces Performance Monitor 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 WorkSpaces Performance Monitor 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, as well as logon\logoff\inactivity\disconnect times. See [Section 6](#) for instructions.

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

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

Version	4.7.0
By	Nuven Consulting Limited
Categories	Application Development Infrastructure as Code
Operating System	Windows, Windows Server 2019
Delivery Method	AWS Marketplace \ Amazon Machine Image

Revision History

Revision Date	Version	Changes
13/01/2021	1.0	Initial Document
22/01/2020	1.1	Added HA and single deployment diagrams in Section 7
08/02/2021	1.2	Amended supported browsers
15/02/2021	1.3	Added Fixed Tagging option to Options
18/02/2021	1.4	Upgraded to WSM version to 4.2.0
07/04/2021	1.5	Upgraded to WSM version to 4.3.0
06/05/2021	1.6	Added Annex for permissions of the service account
02/06/2021	1.7	Upgraded to WSM version to 4.4.0
15/06/2021	1.8	Upgraded to WSM version to 4.5.0
13/08/2021	1.9	Upgraded to WSM version to 4.6.0
14/09/2021	1.10	Upgraded to WSM version to 4.7.0

Contents

Revision History.....	2
1. Introduction.....	4
2. Software requirements.....	5
2.1 WorkSpaces Portal requirements.....	6
2.2 WorkSpaces Performance Monitor Agent requirements.....	6
2.3 Portal Requirements: AD Domain join.....	6
3. Prerequisites for the installation of the WorkSpaces Manager appliance.....	7
3.1 AWS WorkSpaces Cost Optimizer	7
3.2 Active Directory Service Account.....	7
4. Obtain a license for the WorkSpaces Manager appliance.....	9
5. Installing the WorkSpaces Management appliance from AWS Marketplace	11
5.1 Join your WorkSpaces Manager instance to your Active Directory Domain	17
5.2 First Time Setup.....	18
5.2.1 Licenses	19
5.2.2 SMTP.....	19
5.2.3 Remote Service Account	21
5.2.4 Auto Change Compute Type.....	21
5.2.5 Active Directory (Single\Multiple Domain Forest)	22
5.2.6 Amazon Web Services.....	25
5.2.7 Additional Options.....	27
5.2.8 Applications.....	31
6. Installing the WorkSpaces Performance Monitor Agent.....	35
7. High Availability.....	37
7.1 Database.....	37
7.2 User/Admin Portal.....	38
8. Securing the Portal and adding a friendly portal address.....	44
8.1 Portal address	44
8.2 SSL Certificate	45
Annex 1.....	46

1. Introduction

This guide has been authored by experts at Nuvens 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.

2. Software requirements

WorkSpaces Manager is available as a standalone product and consists of three parts: The Management Portal, the Update Service, and the WorkSpaces Performance Monitor 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.

Since the WorkSpaces Management Portal uses IIS with Single Sign-On, the appliance must be a member of the Active Directory Forest/Domain.

To deploy as an HA cluster, please refer to [Section 7](#) (High Availability) or contact support@nuvens.co.uk for assistance.

2.1 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 (minimum version)	Chrome 22.x, Firefox 12.x, Opera 12.x, Safari 5.1x, Microsoft Edge 88.x
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.

- See [Annex 1](#) for details

The WSM Portal also reports back to Nuvens the version in use so that we can better support customers.

2.2 WorkSpaces Performance Monitor Agent requirements

The WorkSpaces Performance Monitor Agent requires .NET 4.6.2 or higher pre-installed on the WorkSpaces themselves. If it is not installed, the agent will prompt for the installation. The installation is covered in [Section 6](#).

2.3 Portal Requirements: AD Domain join

WorkSpaces Manager Appliance must be joined to the AD Domain before starting the configuration, otherwise it will show an error when saving the configuration on first login.

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.

3. Prerequisites for the installation of the WorkSpaces Manager appliance

3.1 AWS WorkSpaces Cost Optimizer

Whilst this is not a mandatory requirement, we recommend that this is applied and initially run in "Dry Run" mode.

This AWS service auto-switches WorkSpaces between Hourly and Monthly Cost modes on a monthly basis to ensure the WorkSpaces costs are optimised. 'Dry Run' mode means that recommendations will be shown in the WorkSpaces Manager Portal, but the recommended changes will not be applied. 'Dry Run' mode can be turned off later in the WorkSpaces Manager portal as to enable this function.

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.

3.2 Active Directory Service Account

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.

- See [Annex 1](#) for details

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>

4. Obtain a license for the WorkSpaces Manager appliance

Go to the [AWS Marketplace](#) and search for 'Workspaces Manager' and select 'Nuvens' as the Vendor filter. Select the product below.

The screenshot shows the AWS Marketplace search results for 'workspaces'. The search bar contains 'workspaces' and shows 3 results. The left sidebar has a 'Vendors' filter with 'Nuvens (3)' selected. The main content area displays three products: 'WorkSpaces Manager Appliance' (Version 4, sold by Nuvens), 'WorkSpaces Manager' (sold by Nuvens Consulting Ltd, 3 AWS reviews), and 'WorkSpaces Cost Optimisation Assessment' (sold by Nuvens). The 'WorkSpaces Manager' product is highlighted with a red box.

Now, select 'Continue to Subscribe'.

The screenshot shows the product page for 'WorkSpaces Manager' by Nuvens Consulting Ltd. The page includes a 'Continue to Subscribe' button and a 'Save to list' button. The product description states: 'WorkSpaces Manager integrates between the user domain and AWS WorkSpaces to allow simple provisioning and management of WorkSpaces'. It also features 3 AWS reviews.

Product Overview

With Amazon WorkSpaces Manager, there is no need for an Admin to have any prior knowledge of using the AWS portal. Our simple to navigate, secure, internal console provides a one stop interface containing all the tools necessary to manage your WorkSpaces fleet

Advanced easy search functionality
Find a WorkSpace by user name, computer name, email address, IP address, directory, bundle, tags & more

Cost Optimisation Of WorkSpaces Fleet
Automatically Identify unused WorkSpaces for a defined time period and convert these to PAYG

Highlight Identify Orphaned WorkSpaces that are in existence but not tied to an AD user
Intelligent cost optimisation tool

Large Scale Migration Project
Import users in Bulk via Excel to deploy WorkSpaces at scale.
Full workflow of WorkSpaces creation from integrating with AD to customisation welcome email to users *
Integrate with O365 to create a mailbox as part of the workflow for WorkSpaces creation
Integrate with SCCM or Liquidware FlexApp for user self-service of applications

Highlights

- Simplify deployment and management of AWS WorkSpaces
- Reduce and manage WorkSpaces spend through Right-Sizing and pro-active monitoring
- Further secure your WorkSpaces platform with granular admin roles

5. Installing the WorkSpaces Management appliance 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 product page for 'WorkSpaces Manager Appliance' by Nuvens. The page includes a 'Continue to Subscribe' button, a 'Save to List' button, and a pricing box showing a typical total price of \$0.064/hr. Below the product details, there are tabs for Overview, Pricing, Usage, Support, and Reviews. The 'Product Overview' section is active, showing 'What's Included' and 'Highlights'.

WorkSpaces Manager Appliance
By: [Nuvens](#) Latest Version: 3.2.0
WorkSpaces Manager surcharges and automates your management of AWS WorkSpaces
Windows ☆☆☆☆☆ 0 AWS reviews
BYOL

Continue to Subscribe
Save to List
Typical Total Price
\$0.064/hr
Total pricing per instance for services hosted on c2.medium in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

Product Overview

What's Included
Note: Always ensure your operating system is current for your needs. This product includes both of the software packages described below:

WorkSpaces Manager Appliance
By: [Nuvens](#)

With Amazon WorkSpaces Manager, there is no need for an Admin to have any prior knowledge of using the AWS portal. Our simple to navigate, secure, internal

Highlights

- Advanced Search Functionality
- Import and Manage WorkSpaces at scale
- Intelligent Cost Optimisation with realtime performance monitoring and remote access

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

The screenshot shows the subscription page for 'WorkSpaces Manager Appliance'. It includes a 'Continue to Configuration' button and a note that the user must first review and accept terms. The page is titled 'Subscribe to this software' and includes a 'Terms and Conditions' section with a 'Nuvens Offer' and an 'Accept Terms' button.

WorkSpaces Manager Appliance
Continue to Configuration
You must first review and accept terms.

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

Subscribe to this software

To create a subscription, review the pricing information and accept the terms for this software.

Terms and Conditions

Nuvens Offer

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](#).

Accept Terms

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.

Delivery Method
WorkSpaces Manager Appliance

Software Version
4 (Jan 04, 2021)
Whats in This Version
WorkSpaces Manager Appliance
running on t5a.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 t5a.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'. Below this is a heading 'Launch this software' and a sub-heading 'Review your configuration and choose how you wish to launch the software.' The main content is divided into two sections: 'Configuration Details' and 'Choose Action'. In the 'Configuration Details' section, there are four rows of information: 'Fulfillment Option' (WorkSpaces Manager Appliance, running on t3a.medium), 'Software Version' (4), and 'Region' (EU (Ireland)). A 'Usage Instructions' button is located below this section. The 'Choose Action' section features a dropdown menu set to 'Launch CloudFormation' and a 'Launch' button. A descriptive text next to the dropdown states: 'Choose this action to launch your configuration through the AWS CloudFormation console.'

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

The screenshot shows the 'Create stack' wizard 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'. The main content area is titled 'Create stack' and is divided into two sections: 'Prerequisite - Prepare template' and 'Specify template'. In the 'Prerequisite' section, there are three radio buttons: 'Template is ready' (selected), 'Use a sample template', and 'Create template in Designer'. The 'Specify template' section includes a 'Template source' section with two radio buttons: 'Amazon S3 URL' (selected) and 'Upload a template file'. Below this is a text input field for the 'Amazon S3 URL' containing the URL 'https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/c4228857-4beb-449c-9339-4a454042e716.8732e2e9-3d75-4a24-beb2-ef2ad7b43c4f.template'. 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 t3a.medium (in a drop-down list) as they should be sufficient to run WorkSpaces Manager

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

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 (in a drop-down list)

VPCName: Select the VPC that you wish to place the WorkSpaces Manager in (in a 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

Enter a stack name

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

t3a.medium

KeyName

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

key-1234567890

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-43... (172.31.16.0/20) (Private Subnet 1)

VPCName

Name of an existing Private VPC to deploy to

vpc-6e8... (172.31.../16) (Private Subnet VPC)

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 is not necessary. You will know when it is finished as the WorkSpaces Manager will appear as an EC2 instance in the console

Then select 'Next'.

The screenshot shows the 'Configure stack options' screen in the AWS CloudFormation console. On the left, a navigation pane shows four steps: Step 1 (Specify template), Step 2 (Specify stack details), Step 3 (Configure stack options - currently selected), and Step 4 (Review). The main content area is titled 'Configure stack options' and contains two sections: 'Tags' and 'Permissions'. The 'Tags' section includes a table with columns for 'Key' and 'Value', and a 'Remove' button. Below the table is an 'Add tag' button. The 'Permissions' section includes a description and an 'IAM role - optional' section with a dropdown menu for 'IAM role name' and a 'Remove' button.

The screenshot shows the 'Advanced options' screen in the AWS CloudFormation console. The main content area is titled 'Advanced options' and includes a description and four expandable sections: 'Stack policy', 'Rollback configuration', 'Notification options', and 'Stack creation options'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

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

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

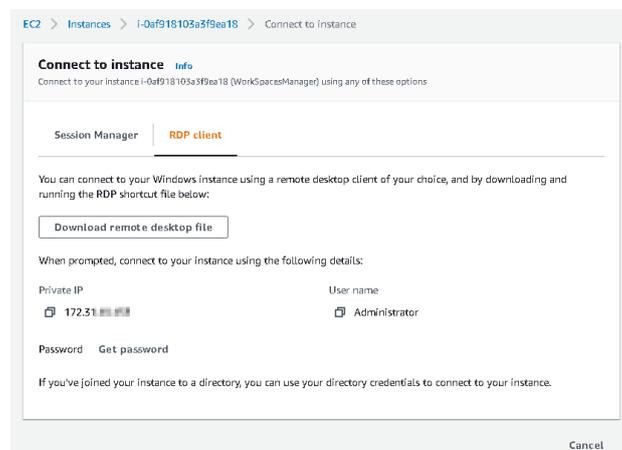
Search events

Timestamp	Logical ID	Status	Status reason
2019-08-15 13:00:38 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	WorkSpacesManagerCloudwatchPolicy	CREATE_COMPLETE	-

If you now view your EC2 instances in the region that you chose to install WorkSpaces Manager, you will 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 state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
WorkSpacesManager	i-0af918103a3f9ea18	Running	t3a.medium	2/2 checks ...	No alarms +	eu-west-1a	-	-

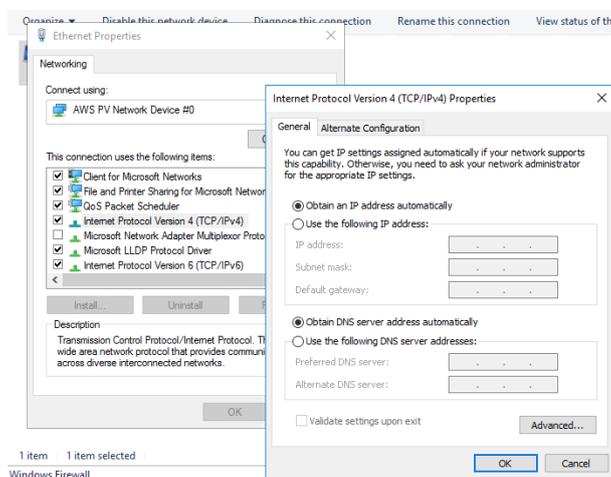
Now RDP to your instance using the Private IP assigned to the instance using the local administrator password and using the KeyName and associated keyfile that you specified in the Stack Details section above. If you cannot RDP to the instance, you need to be connecting from a device in the network CIDR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



5.1 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.

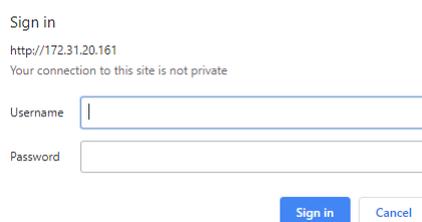


5.2 First Time Setup

Please Note: The instance **MUST** have Internet connectivity.

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.domain.com`) which means that it will most likely be accepted from most 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 (obtained in [Section 4](#)).
- Active Directory settings
- SMTP settings
- Amazon Web Services settings
- Additional options settings

The license key will have been sent via email when you registered on the AWS Marketplace in [Section 4](#).

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

This is an example of the Portal filled in.

Setup
License Key
The License Key will have been sent by email. It can also be obtained from your Nuvens account

12b96[redacted]

SMTP

SMTP Server: smtp.gmail.com
SMTP Port: 587
SMTP Use TLS:
SMTP User: mystmpuser
SMTP Password:
Default Email Address: mystmpuser@nuvens.internal

Amazon Web Services

AWS Account: 1234567890
Default AWS Region: eu-west-1
Cost Optimizer Bucket: workspaces-cost-optimizer-costoptimizerbucket-234980s4
AWS Cost Optimiser:
Dry Run Mode:
Auto Reboot:

Additional Options

AD Group Applications:
Enable RDP:
Enable DameWare:

Active Directory

AD Service Account: workspacesmgrsvc
AD Service Password:
NetBios Name: nuvens
FQDN: nuvens.internal
Default User OU: OU=Users,DC=nuvens,DC=internal
Password Expiry Emails:

Remote Service Account

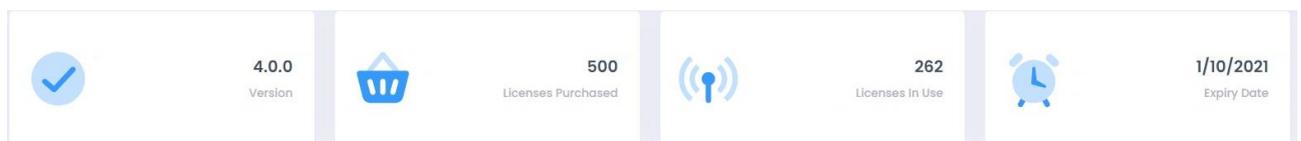
Remote Management Username: mycompanyremote
Remote Management Password:

Now press 'Save'. Please wait for up to 30 seconds for the next screen to appear. Again, make sure that the instance has Internet access otherwise it will give you an error saying that the license code is invalid.

When it completes, it will show the administration section of the portal on the Options\Settings page. You can change settings in here where you see them. The various sections are covered below.

5.2.1 Licenses

This shows the WorkSpaces Manager version, the number of licenses procured, the current number of licenses in use and the expiry date of the license.



5.2.2 SMTP

This enables you to send emails to users when their new WorkSpace is ready and/or if their password is to expire.

You could use AWS Simple Email Service to achieve this, or your own SMTP setup. You can test the connection by selecting the icon highlighted.

WorkSpaces Manager

USER

- User Dashboard
- Change Password
- App Groups
- AppStream Apps

ADMIN

- Admin Dashboard
- Users
- WorkSpaces
- AppStream
- Task Queue
- Help

CONFIG

- Resources >
- Update >

Settings

 **4.0.0**
Version

 **500**
Licenses Purchased

SMTP

SMTP Server	 <input type="text" value="smtp.gmail.com:587"/>
SMTP Port	<input type="text" value="587"/>
SMTP Use TLS	<input checked="" type="checkbox"/>
SMTP User	<input type="text" value="*****@gmail.com"/>
SMTP Password	<input type="password" value="*****"/>
Default Email Address	<input type="text" value="*****@*****.com"/>

5.2.3 Remote Service Account

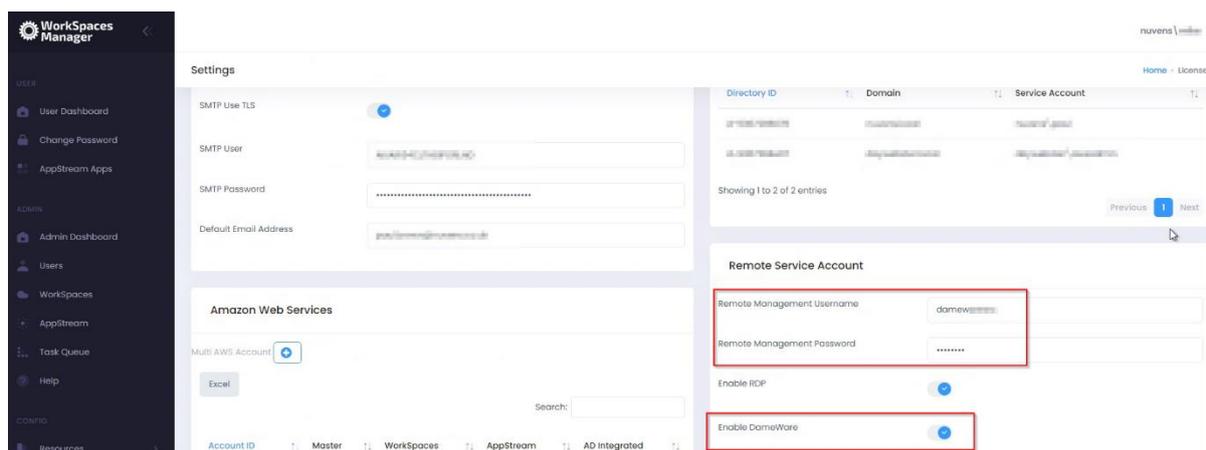
This is an account that you configure to remote control user devices using Dameware, etc. This is the generic account that you connect with (which will be standard throughout your organisation). You can remote control a user's WorkSpaces by selecting 'Dameware' (if you have selected the 'Enable Dameware'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

5.2.3.1 Enable RDP

Enables the option for downloading an RDP file to connect to the user's Workspace from within the Portal. The Security Group must allow inbound TCP/3389.

5.2.3.2 Enable DameWare

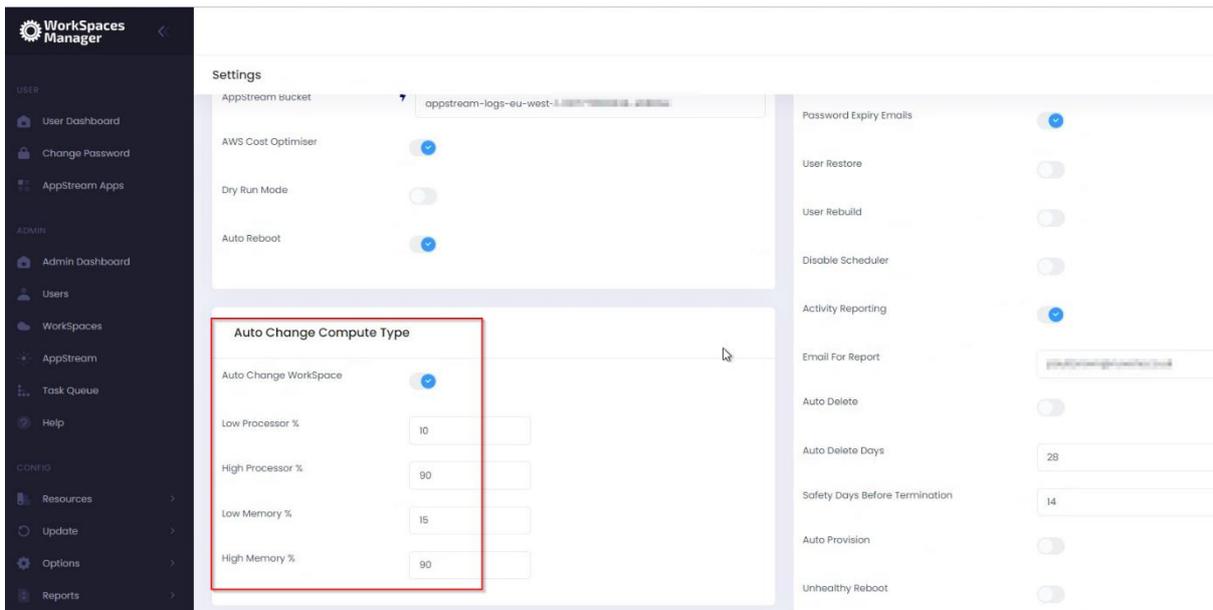
Enables the usage of DameWare Remote Control to connect to the user's Workspace from within the Portal. A license would be required. Security Group must allow for inbound UDP/137, TCP/138-139, TCP/443, TCP/3389, TCP/5900 and TCP/6129-6133.



5.2.4 Auto Change Compute Type

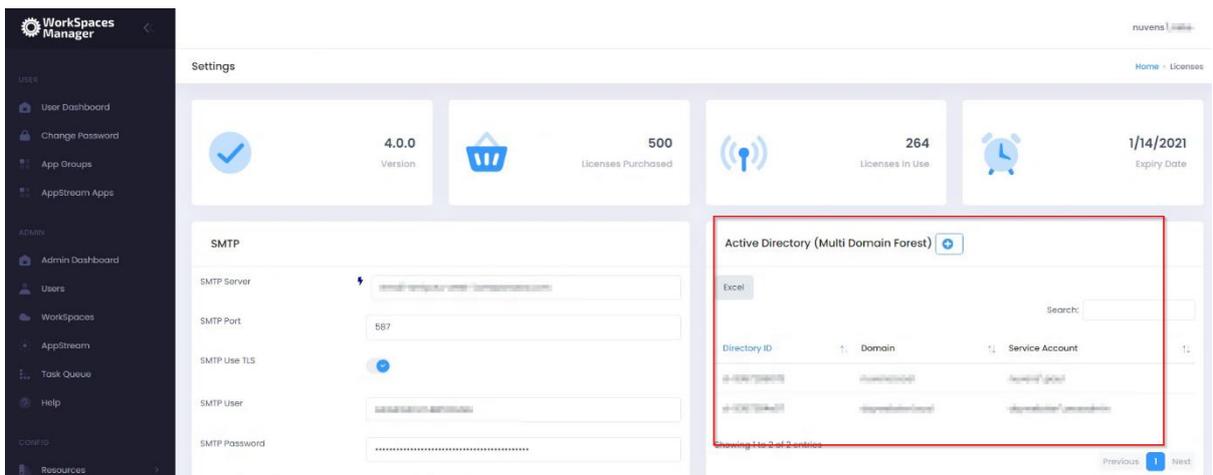
You can opt for WorkSpaces Manager to automatically change compute type of a Workspace. This is useful if, for example, you had a user running heavy spreadsheets on a Standard Workspace and it would benefit them with being upgraded to a Performance Workspace.

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



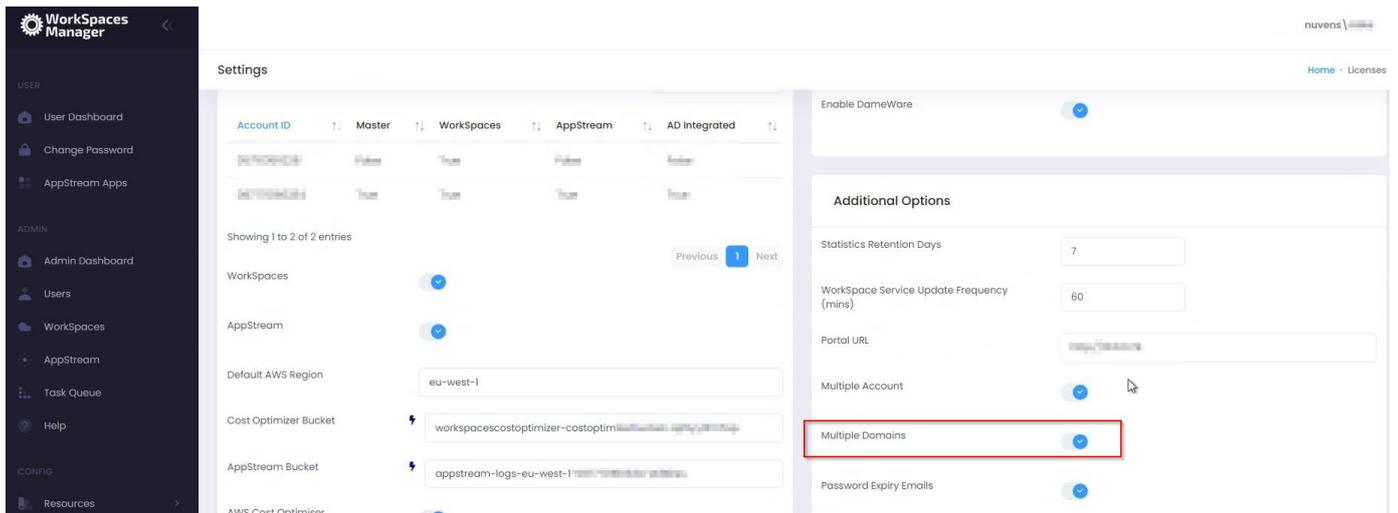
5.2.5 Active Directory (Single\Multiple Domain Forest)

You can either have a single Active Directory domain for WorkSpaces, or multiples.



On initial setup, and by default, you will have one domain. You can enable multiple domains by enabling the feature below in Additional Options.

There is a button to perform an exhaustive test of all domains' AD accounts.



You will then add the details for your domain.

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.

NetBIOS name:

NetBIOS name of the domain that your WorkSpaces will be joining.

FQDN:

Fully Qualified Domain Name of the domain that your WorkSpaces will be joining.

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.

Example:

Add Domain

Directory ID
d-12345678

FQDN
mydomain.local

Netbios Name
mydomain

Default OU
OU=Users,DC=mydomain,DC=local

Service Account
mydomain\serviceaccount

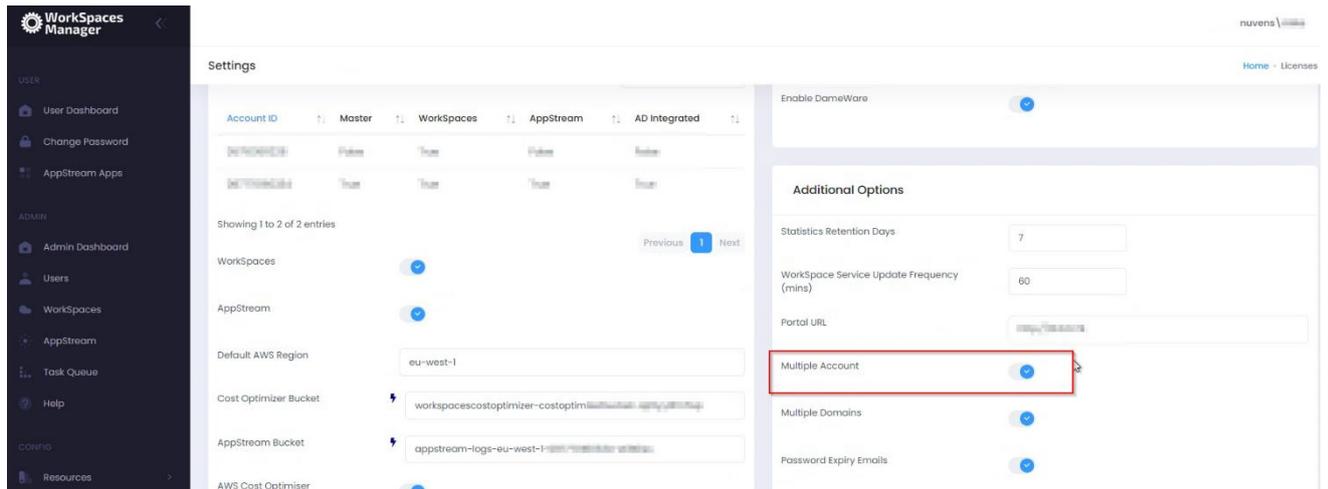
Password
.....|

Save

5.2.6 Amazon Web Services

5.2.6.1 Single\Multi-AWS Account

WorkSpaces Manager allows you manage WorkSpaces across single, or multiple, AWS accounts. When you set up WorkSpaces Manager, you will set up a single account. You can set up multi-AWS accounts by enabling this function and following the instructions in Section 7 of the 'WorkSpaces Manager Administrator Guide'.



You will see a summary of the Account ID(s) when they are added.

Account ID	Master	WorkSpaces	AppStream	AD Integrated
05...	False	True	False	False
0877...	True	True	True	True

Click on one and you will see the options. You can turn some on and off (like Dry Run mode) as preferences.

Preferences

AWS Account 

05-123456789012

Default region

eu-west-1

Role To Assume

arn:aws:iam::05-123456789012:role/VirtualWorkspacesAdmin

AccessLog Group 

/aws/events/workspaceaccess

AD Integrated

WorkSpaces

AWS Cost Optimiser

Cost Optimizer Bucket 

workspacescostoptimizer-costoptimizerbucket-123456789012

Dry Run Mode

AppStream

AppStream Bucket 

Save

5.2.6.2 WorkSpaces

Turns on the WorkSpaces Management menu function.

5.2.6.3 AppStream

Turns on the AppStream Management menu function.

5.2.6.4 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](#).

5.2.6.5 Cost Optimizer Bucket

This is the bucket name mentioned in the 'AWS WorkSpaces Cost Optimizer' section earlier on the document.

5.2.6.6 AppStream Bucket

Specifies the AppStream Usage bucket.

5.2.6.7 AWS Cost Optimizer

This enables the AWS Cost Optimiser.

5.2.6.8 Dry Run

Running the Cost Optimiser in Dry Run Mode will show you the changes that would have been made.

5.2.6.9 Auto Reboot

This gives the ability to set reboot times on WorkSpaces. This is available once you have set up the Portal.

5.2.7 Additional Options

5.2.7.1 Statistics Retention Days

If the Workspace Performance Monitor 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 6](#) for installing the WorkSpaces Performance Monitor Agent). In a large estate, this will create millions of rows within the database over a period. The number of days that are retained within the database can be specified here. If the number of days is too high on a large estate (e.g., 60) then it will have an impact on queries of statistics and increased disk space usage. For smaller estates, you can set this to 30 days and monitor from there.

5.2.7.2 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 would not 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.

5.2.7.3 Portal URL

Enter your portal URL here. e.g. <http://ourwsportal.mycompany.internal>.

5.2.7.4 Multiple Account

This enables management of WorkSpaces across multiple AWS accounts. Please refer to Section 7 of the 'WorkSpaces Manager Administrator Guide' which tells you how to set it up.

5.2.7.5 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.

5.2.7.6 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.

5.2.7.7 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.

5.2.7.8 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.

5.2.7.9 Disable Scheduler

This quickly disables ALL automation of the WSM Appliance.

5.2.7.10 Activity Reporting

This enabled\disables the sending of a daily report on user login, logoff, idle times and when activity was resumed. An example report is shown below:

id	ComputeTypeName	Username	Activity	ActivityTime
386	WSAMZN-9VEI39FQ	nuvens\	User Login	12/9/2020 3:52:11 PM
389	WSAMZN-9VEI39FQ	nuvens\	User Logoff	12/9/2020 3:55:47 PM
393	WSAMZN-9VEI39FQ	nuvens\	User Login	12/9/2020 4:02:49 PM
397	WSAMZN-9VEI39FQ	nuvens\	User Logoff	12/9/2020 4:57:33 PM
399	WSAMZN-9VEI39FQ	nuvens\	User Login	12/9/2020 5:00:00 PM
401	WSAMZN-9VEI39FQ	nuvens\	idle detected	12/9/2020 5:14:59 PM
402	WSAMZN-9VEI39FQ	nuvens\	Activity Resumed after 16 minutes	12/9/2020 5:16:59 PM
405	WSAMZN-9VEI39FQ	nuvens\	idle detected	12/9/2020 5:34:59 PM
406	WSAMZN-9VEI39FQ	nuvens\	Activity Resumed after 15 minutes	12/9/2020 5:35:59 PM
410	WSAMZN-9VEI39FQ	nuvens\	idle detected	12/9/2020 6:00:59 PM
411	WSAMZN-9VEI39FQ	nuvens\	Activity Resumed after 48 minutes	12/9/2020 6:34:59 PM
413	WSAMZN-9VEI39FQ	nuvens\	idle detected	12/9/2020 7:09:00 PM
415	WSAMZN-9VEI39FQ	nuvens\	Activity Resumed after 183 minutes	12/9/2020 9:58:00 PM
416	WSAMZN-9VEI39FQ	nuvens\	idle detected	12/9/2020 10:13:00 PM
383	WSAMZN-421NLAQ3	nuvens\	User Login	12/9/2020 3:15:16 PM
384	WSAMZN-421NLAQ3	nuvens\	User Logoff	12/9/2020 3:24:22 PM
385	WSAMZN-421NLAQ3	nuvens\	User Login	12/9/2020 3:27:56 PM
387	WSAMZN-421NLAQ3	nuvens\	User Logoff	12/9/2020 3:54:35 PM
388	WSAMZN-421NLAQ3	nuvens\	User Login	12/9/2020 3:55:11 PM
390	WSAMZN-421NLAQ3	nuvens\	User Logoff	12/9/2020 3:56:58 PM
391	WSAMZN-421NLAQ3	nuvens\	User Login	12/9/2020 3:59:33 PM
396	WSAMZN-421NLAQ3	nuvens\	idle detected	12/9/2020 4:43:33 PM
398	WSAMZN-421NLAQ3	nuvens\	Activity Resumed after 29 minutes	12/9/2020 4:58:33 PM
403	WSAMZN-421NLAQ3	nuvens\	User Logoff	12/9/2020 5:31:57 PM
404	WSAMZN-421NLAQ3	nuvens\	User Login	12/9/2020 5:32:58 PM
409	WSAMZN-421NLAQ3	nuvens\	idle detected	12/9/2020 5:55:58 PM
412	WSAMZN-421NLAQ3	nuvens\	Activity Resumed after 77 minutes	12/9/2020 6:58:58 PM
414	WSAMZN-421NLAQ3	nuvens\	idle detected	12/9/2020 7:13:58 PM
379	IP-AC1F5495	nuvens\	Activity Resumed after 307 minutes	12/9/2020 2:36:39 AM
380	IP-AC1F5495	nuvens\	idle detected	12/9/2020 3:01:40 AM
381	IP-AC1F5495	nuvens\	Activity Resumed after 341 minutes	12/9/2020 8:22:44 AM
382	IP-AC1F5495	nuvens\	idle detected	12/9/2020 8:44:40 AM
394	IP-AC1F5495	nuvens\	Activity Resumed after 472 minutes	12/9/2020 4:16:41 PM
400	IP-AC1F5495	nuvens\	idle detected	12/9/2020 5:10:41 PM
392	EC2AMAZ-32D5533	nuvens\	User Login	12/9/2020 4:02:30 PM
395	EC2AMAZ-32D5533	nuvens\	idle detected	12/9/2020 4:30:29 PM
407	EC2AMAZ-32D5533	nuvens\	Activity Resumed after 88 minutes	12/9/2020 5:44:29 PM

5.2.7.11 Email For Report

The email of the person\group that receives the Activity report.

5.2.7.12 Auto Delete

You can set up WSM to automatically delete unused workspaces after a defined period of days.

5.2.7.13 Auto Delete Days

This value is the number of days a Workspace should be considered for deletion e.g., 45 or 60 days.

5.2.7.14 Safety Days Before Termination

This value is the number of days a user will be given to inform their helpdesk or IT Function that they still require the Workspace before deletion.

For example, if Autodelete was set for 60 days. On the 60th day of the Workspace being unused, the user that is associated with the Workspace will receive an email informing them that their Workspace is to be deleted in (Safety days VALUE) with the request for

them to contact support remove the Autodeletion request. After the safety days value and if autodeletion is not removed.

5.2.7.15 Auto-Provision

Turns on Auto-Provisioning of WorkSpaces via Active Directory groups. See Section 4.3.5 of the Administration Guide for more information on this.

If Auto-Provision is enabled, the service will poll the Active Directory groups every 15 minutes for new members.

Removing a user from the AD group will not terminate the WorkSpace. This functionality can be obtained in conjunction with Auto-Delete.

5.2.7.16 Unhealthy Reboot

If this option is enabled the service will check for any WorkSpaces with a status of "UnHealthy" every 10 minutes. Any WorkSpaces found in this state will have their status re-evaluated and if still found to be "UnHealthy" they will be rebooted. If after a reboot the status remains at "UnHealthy" the WorkSpace running mode will be set to "Auto-Stop" (if not already) and the WorkSpace Stopped. Once Stopped the WorkSpace will be Started again and its original running mode restored. This action can initiate a migration from the underlying physical host.

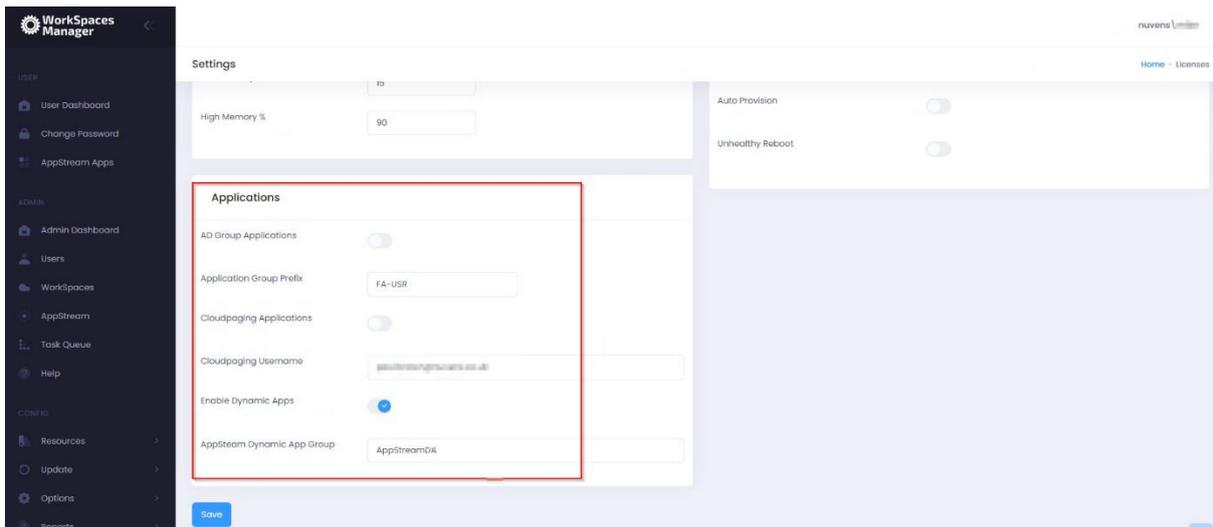
If the WorkSpace remains in an "UnHealthy" state an error is recorded on the admin dashboard.

5.2.7.17 Fixed Tags Values

This turns on the ability to add Fixed Tag values which keeps consistency of tagging in your WorkSpaces environment. You can also apply fixed tags to Auto-Provisioning profiles in WorkSpaces Manager so WorkSpaces are consistently tagged on creation.

5.2.8 Applications

This allows users to Self-Service their applications in their dashboard - from Numecent Cloudpaging and products such as FlexApp, APP-V, etc. You can enable both here.

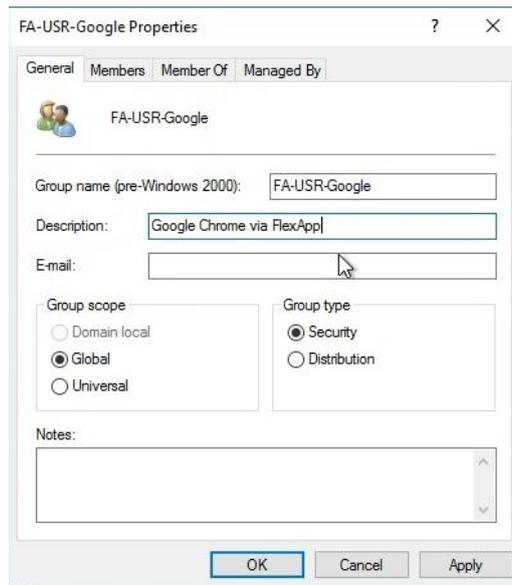


5.2.8.1 AD Group applications

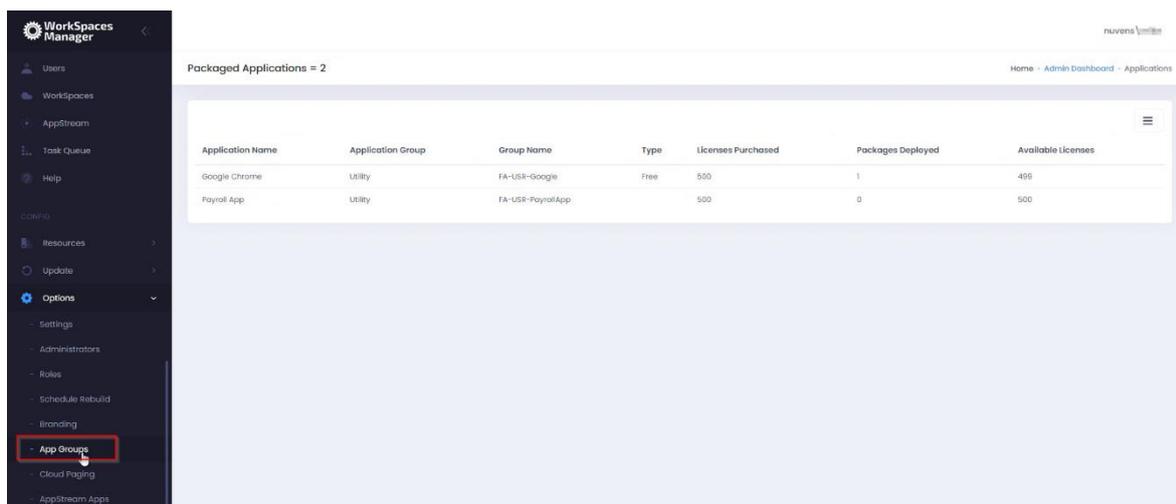
Enable this if you use software distribution on your WorkSpaces from the likes of Liquidware FlexApp, App-V, etc. This allows users to add and remove applications available to them through the Self-Service side of the WorkSpaces Manager Portal. You can change this to your own prefix when you have logged into the Portal. For example, your FlexApp groups could be prefixed 'FA-USR'.

By default, any new imported applications based on the prefix group name (in the example below, 'FA-USR') are given the 'Application Group' of 'App' and the 'Type' of 'Free'.

For an application group to be imported into this list, it will need to have a Description and the group prefix specified in the 'Application Group Prefix' field of 'Options > Settings > Applications'. An example:



This is a list of applications that a user can add\remove as a Self-Service function in the WorkSpaces Manager portal. To know more about this, go to Section 5 of the 'WorkSpaces Manager Administrator Guide' where you will be shown how to amend this list where it says 'Type'. All imported applications are 'Free' of Type by default - a user can add and remove themselves from the application in the WorkSpaces Manager Self-Service portal. However, you may want to amend the 'Type' to 'Paid' for such applications as Visio which have licensing constraints. A user can hence remove themselves from the group, but will have to ask the Service Desk (or another AD administrator) to add them back in.



5.2.8.2 Application Group Prefix

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

5.2.8.3 Cloudpaging Applications

If you want to use Numecent Cloudpaging applications with WorkSpaces, you can enable this feature on [here](#).

5.2.8.4 Cloudpaging Username

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

6. Installing the WorkSpaces Performance Monitor Agent

**** RECOMMENDED FOR FULL FUNCTIONALITY ****

The WorkSpaces Performance Monitor Agent requires .NET 4.6.2 or above. If a lower version is detected, the installation will advise you.

The WorkSpaces Performance Monitor Agent gathers information in both user and WorkSpace Metrics.

The Agent installer ('WSM Performance Monitor.msi') can be found in "D:\WorkSpaceAgent" on the WSM appliance.

The Agent requires registry keys value to be present to locate the database on the appliance. These keys are in D:\WorkSpaceAgent\nuvens.reg and are as follows:

[HKEY_USERS\DEFAULT\Software\Nuvens]

"UpdateFrequency"="60"

"Portal"="http://10.0.1.174"

"Frequency"=dword:00000005

"IdleMinutes"=dword:00000015

"Visible"="false"

"Portal" – Replace with [http://DNS or IP address of your portal](#). (If you are using SSL, use **https** in place of http)

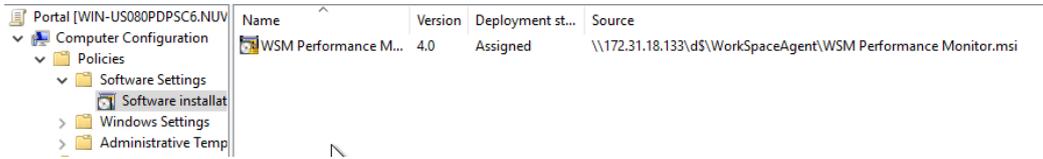
"Frequency" = The value data is a numeric value of minutes (e.g. '5' where the Agent reports back to the database every 5 minutes with metrics. You can change this frequency to an increased value if you have a large estate as a lot of information will be stored in the database).

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' from the 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
 - 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://wsportal).
 - 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 (decimal) 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).
 - Create the "UpdateFrequency" registry value with the key [HKEY_USERS\DEFAULT\Software\Nuvens]
 - The value name is "Frequency" of type REG_SZ (32-bit)
 - The value data is 60
 - Create the "IdleMinutes" registry value with the key [HKEY_USERS\DEFAULT\Software\Nuvens]
 - The value name is "IdleMinutes" of type REG_DWORD (32-bit)
 - The value data is 15 (decimal)
 - Create the "False" registry value with the key [HKEY_USERS\DEFAULT\Software\Nuvens]
 - The value name is "Visible" of type REG_SZ
 - The value data is "false"

7. 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.

PLEASE NOTE: IIS has been configured as of version 4.6.0 to restrict to TLS 1.2

7.1 Database

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

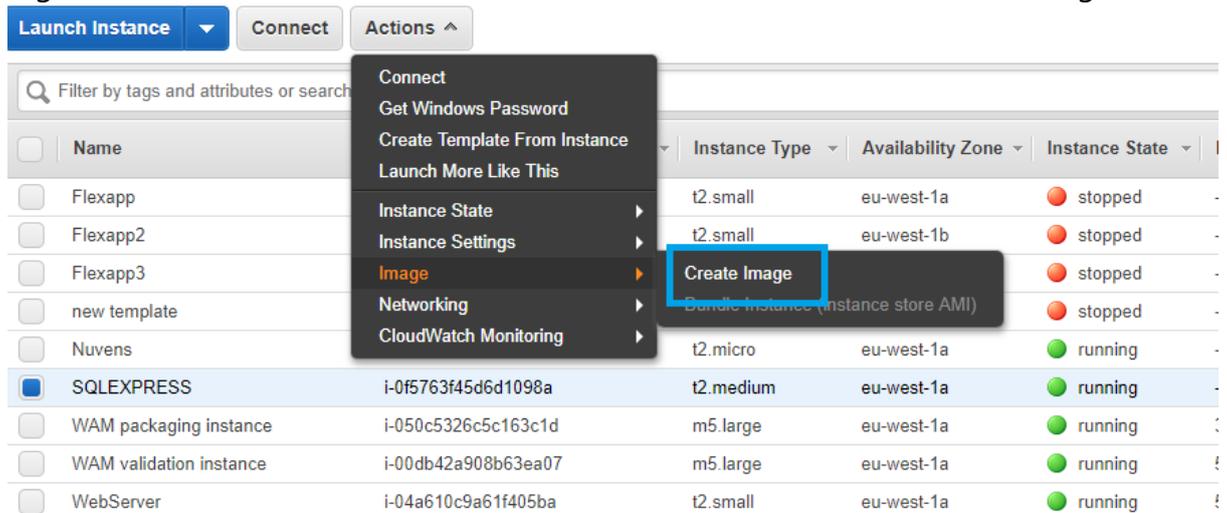
After deploying RDS you will need to do the following actions: -

- 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

7.2 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 (AMI) 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.

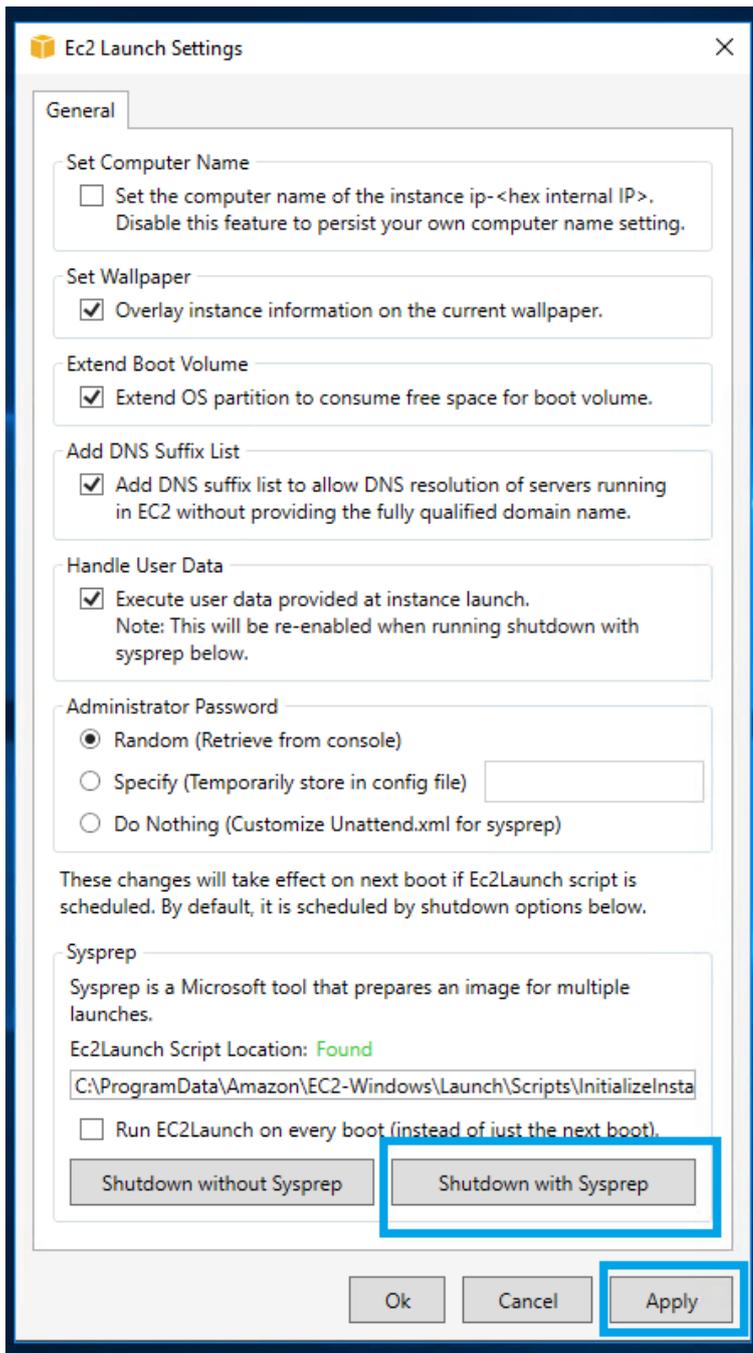


3. Name the Image and click Create Image

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 has 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'.

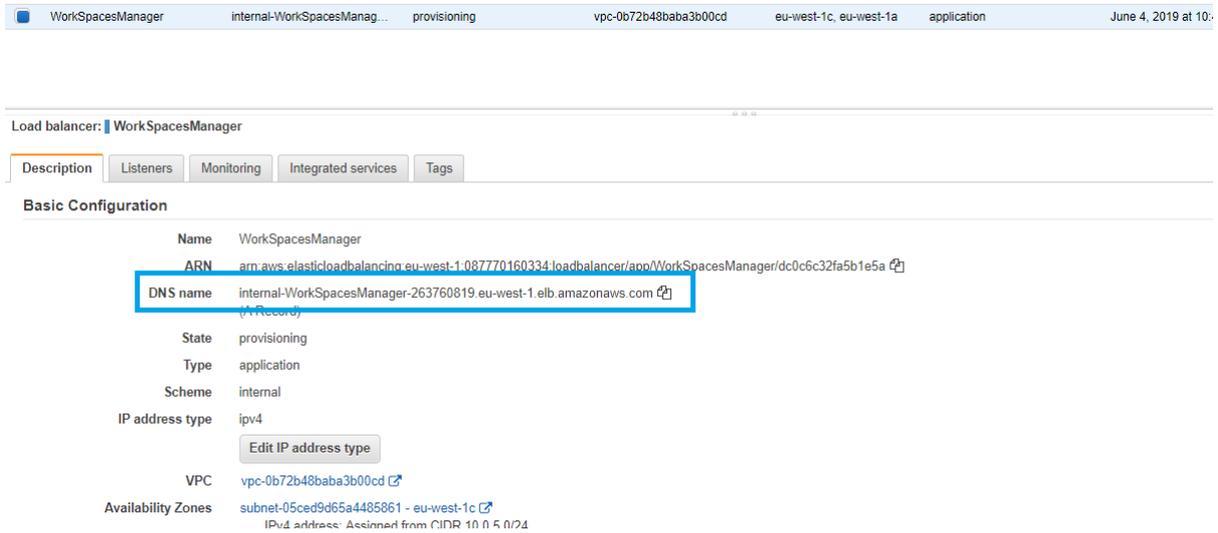
3. Register both WorkSpace Manager appliances with the target group.

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

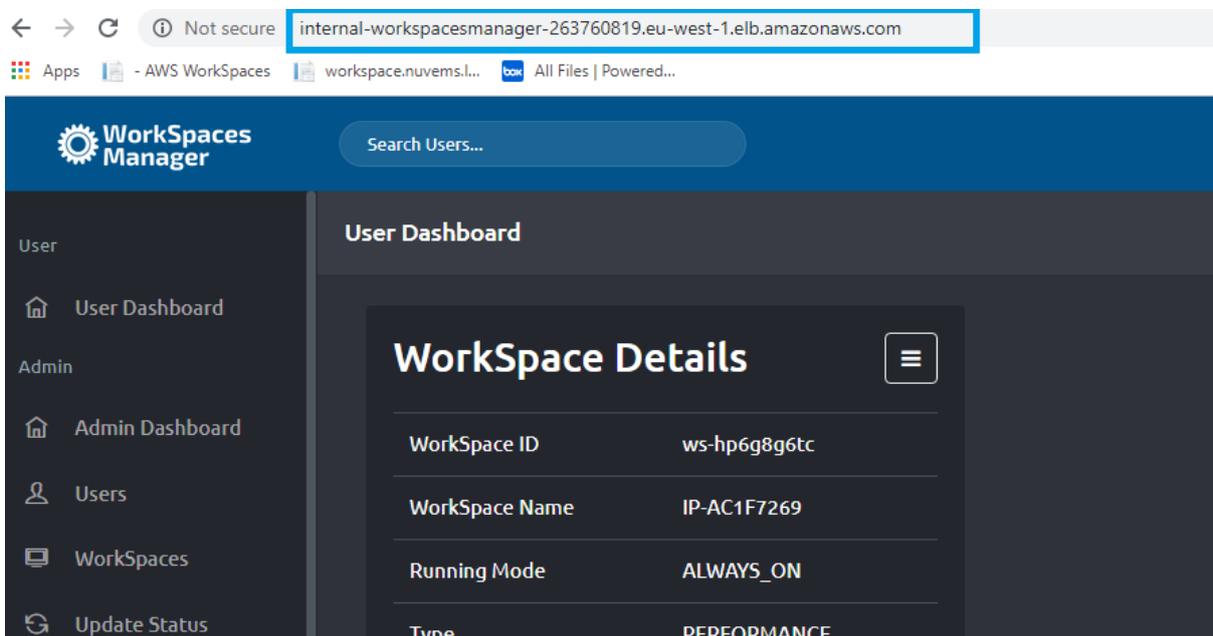
4. Next create an Application Load Balancer ensuring you select the Availability Zones that you used when creating the target group and the Scheme is set as 'Internal'.
5. On Step3: Configure Security Groups, create a new security allowing inbound HTTP from the private subnets.

6. On Step 4: 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.

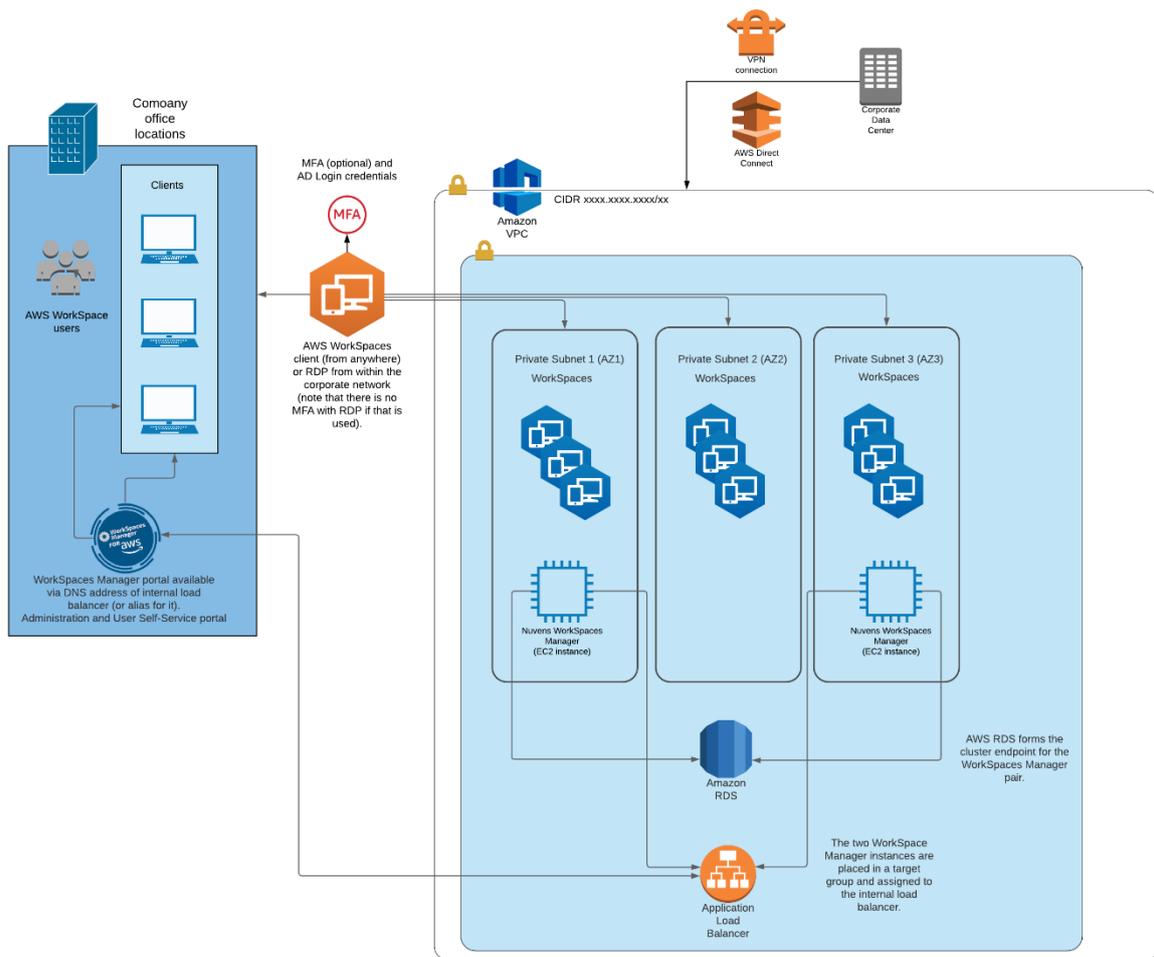


The DNS name can then be used to access the portal which will be load balanced across both instances.

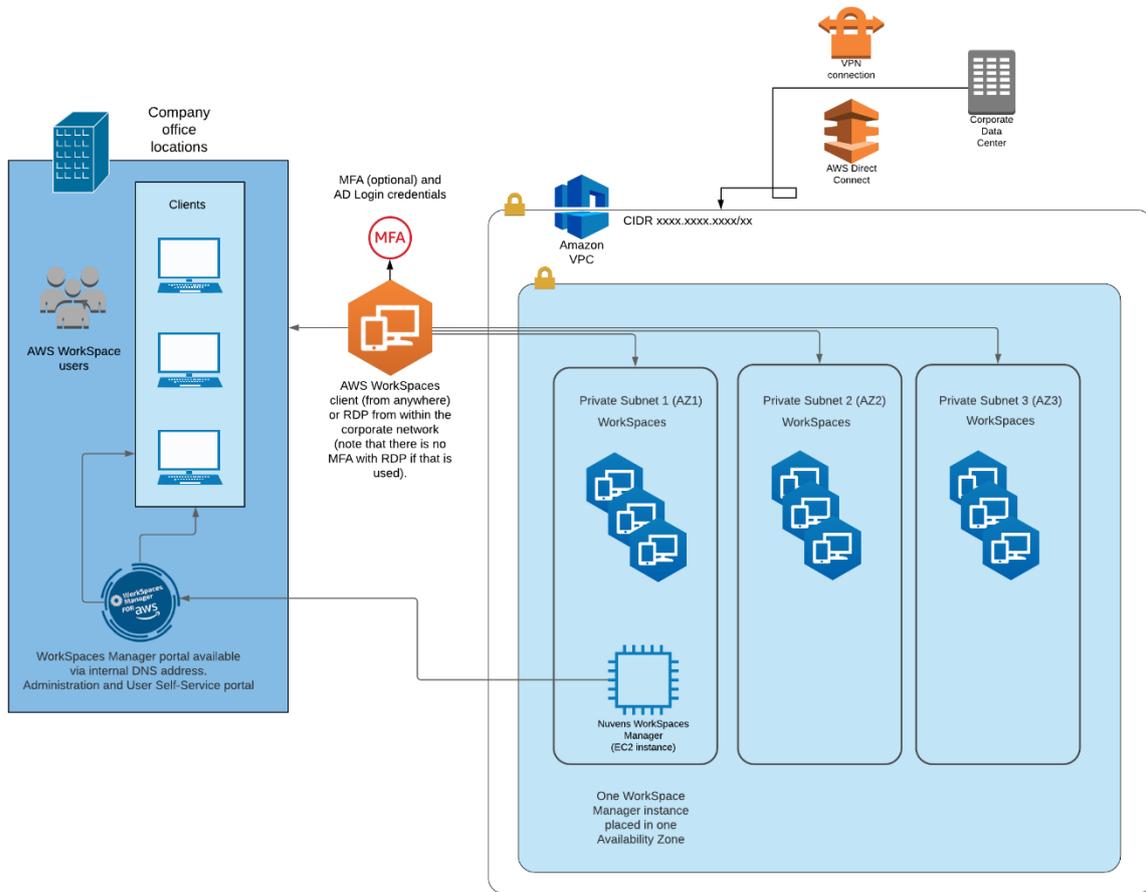


The portal is now in full HA mode load balanced across 2 AZ's with an HA database supporting it. However, the address is not very friendly. See 'Securing the Portal and adding a friendly portal address' in [Section 8](#).

Example of a HA deployment using two Availability Zones.



Example of a single AZ deployment.



8. Securing the Portal and adding a friendly portal address

8.1 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

180] win-feqd27dhp2i... static

New Host

Name (uses parent domain name if blank):
Portal

Fully qualified domain name (FQDN):
Portal.nuvens.local.

IP address:
10.0.1.174

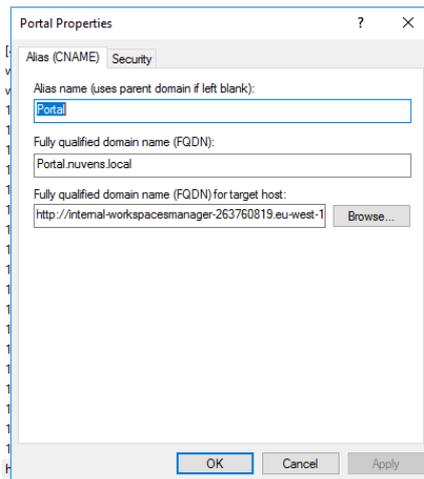
Create associated pointer (PTR) record

Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

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:



8.2 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'.

< Listeners WorkSpacesManager | Add listener Save

Add a new listener. Each listener must include one action of type forward, redirect, fixed response.

WorkSpacesManager | Add listener

Listeners belonging to Application Load Balancers check for connection requests using the protocol and port you configure. Each listener must include a default action to ensure all requests are routed. Once you have created your listener, you can create and manage additional routing rules as needed. [Learn more](#)

Protocol : port
Select the protocol for connections from the client to your load balancer, and enter a port number from which to listen to for traffic.
HTTPS : 443

Default action(s)
Indicate how this listener will route traffic that is not otherwise routed by a another rule.

1. Forward to...
WorkSpaceManager
+ Add action

Security policy
ELBSecurityPolicy-2016-08

Default SSL certificate
From ACM (recommended) www.nuvens.info - 368d7643-dd63-4279-a590-850aceef98ce

Annex 1

To administer user accounts, groups and computers in the Active Directory (globally or on a selected OUs), please refer to the following table for details:

Operation	Permissions Needed
User Management	
Create Users	<ul style="list-style-type: none"> • Must be a member of the built-in Administrators group or Account Operators group, or, • Must have permissions to create, delete, and manage user accounts or equivalent permissions in the relevant OU or container in Active Directory
Modify Users	<ul style="list-style-type: none"> • Must be a member of the built-in Administrators group or Account Operators group, or, • Must have permissions to create, delete, and manage user accounts or equivalent permissions in the relevant OU or container in Active Directory <p>Note: It is also possible to grant the permissions to modify on specific attributes instead of the object as a whole</p>
Delete Users	<ul style="list-style-type: none"> • Must be a member of the built-in Administrators group or Account Operators group, or, • Must have permissions to create, delete, and manage user accounts or equivalent permissions in the relevant OU or container in Active Directory
Computer Management	
Create Computers	<ul style="list-style-type: none"> • Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Computer Objects – Create selected objects in this folder' permission, or an equivalent permission in the relevant OU or container in Active Directory
Modify Computers	<ul style="list-style-type: none"> • Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Computer Objects – Create selected objects in this folder: with write permission', or an equivalent permission in the relevant OU or container in Active Directory
Delete Computers	<ul style="list-style-type: none"> • Must be a member of the built-in Administrators group or Account Operators group, or, • Must have the 'Computer Objects – Delete selected objects' permission, or an equivalent permission in the relevant OU or container in Active Directory

Group Management

Create Groups	<ul style="list-style-type: none">• Must be a member of the built-in Administrators group or Account Operators group, or,• Must have the 'Create, manage and delete user groups' permission, or an equivalent permission in the relevant OU or container in Active Directory
Modify Groups	<ul style="list-style-type: none">• Must be a member of the built-in Administrators group or Account Operators group, or,• Must have the 'Create, manage and delete user groups' permission, or an equivalent permission in the relevant OU or container in Active Directory
Delete Groups	<ul style="list-style-type: none">• Must be a member of the built-in Administrators group or Account Operators group, or,• Must have the 'Create, manage and delete user groups' permission, or an equivalent permission in the relevant OU or container in Active Directory