Workspaces Manager- Installation guide

Updated 11th May 2022 for WorkSpaces Manager 5.3.0

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 Processer, 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 Processer 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, Chocolatey, SCCM or similar products.

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

Version	5.3.0
By	Nuvens 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 Appendix 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
18/11/2021	1.11	Upgraded to WSM version to 4.7.2 Corrected Reporting and Dry-Run for Cost Optimizer 4.2.0
28/01/2022	1.12	Version 5.0.0 with new features WSUS Configuration
24/03/2022	1.13	Upgraded to WSM version to 5.2.0
11/05/2022	1.14	Upgraded to WSM version to 5.3.0

Contents

1. Introduction

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

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@workspacesmanager.com for assistance.

2.1 WorkSpaces Portal requirements

Component	Requirements
Platforms Support	Windows Server 2012/2012 R2/2016/2019. Only 64-bit versions where applicable are supported. Both physical and virtual instances are also supported.
Additional Software	• 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 in which accounts will be created in.

- See Appendix 1 for details

The WSM Portal also reports back to Nuvens the version and the number of licenses in use so that we can better support customers and recommend upgrades.

2.2 Hostname

WorkSpaces Manager appliance's hostname cannot be changed.

2.3 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.

2.4 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 strongly recommend that this is installed and initially configured in "Dry Run" mode, which lists actions without executing them.

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://docs.aws.amazon.com/solutions/latest/workspaces-cost-optimizer/overview.html

After deploying the WorkSpaces cost optimizer, please make a note of the S3 Bucket ARN created, so that you can update it on the Config section.

3.2 Active Directory Service Account

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

- See Appendix 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 otherwise have the administration permissions.

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:

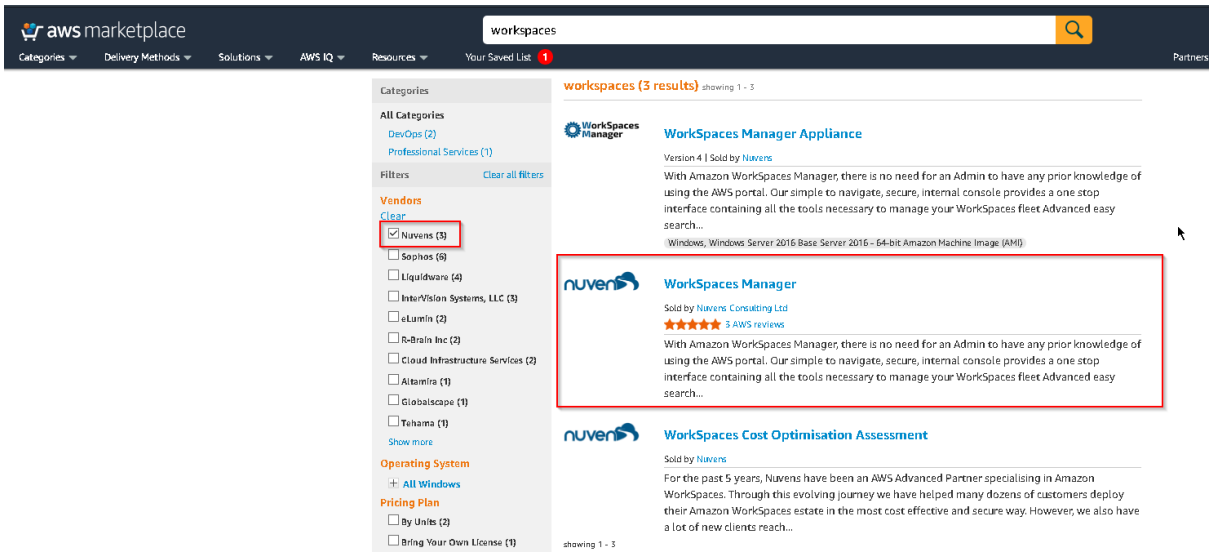
http://technet.microsoft.com/en-us/library/cc759064%28WS.10%29.aspx

Delegating Administration of Account and Resource OUs:

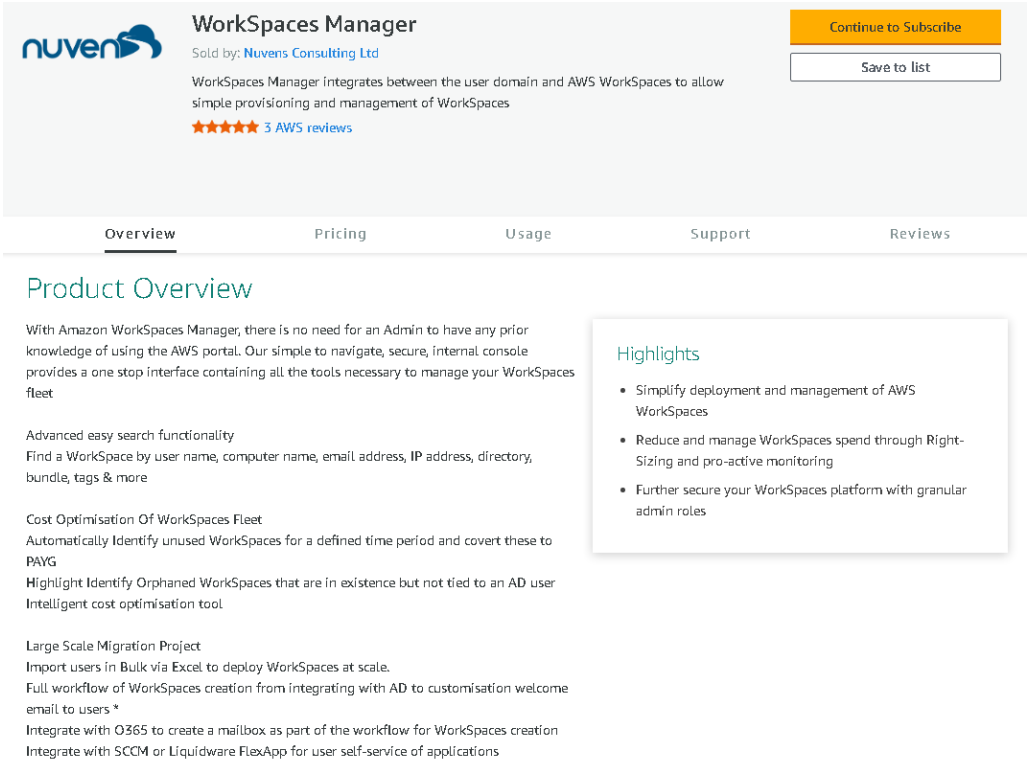
http://technet.microsoft.com/en-us/library/cc784406%28WS.10%29.aspx

4. Obtain a license for the WorkSpaces Manager appliance

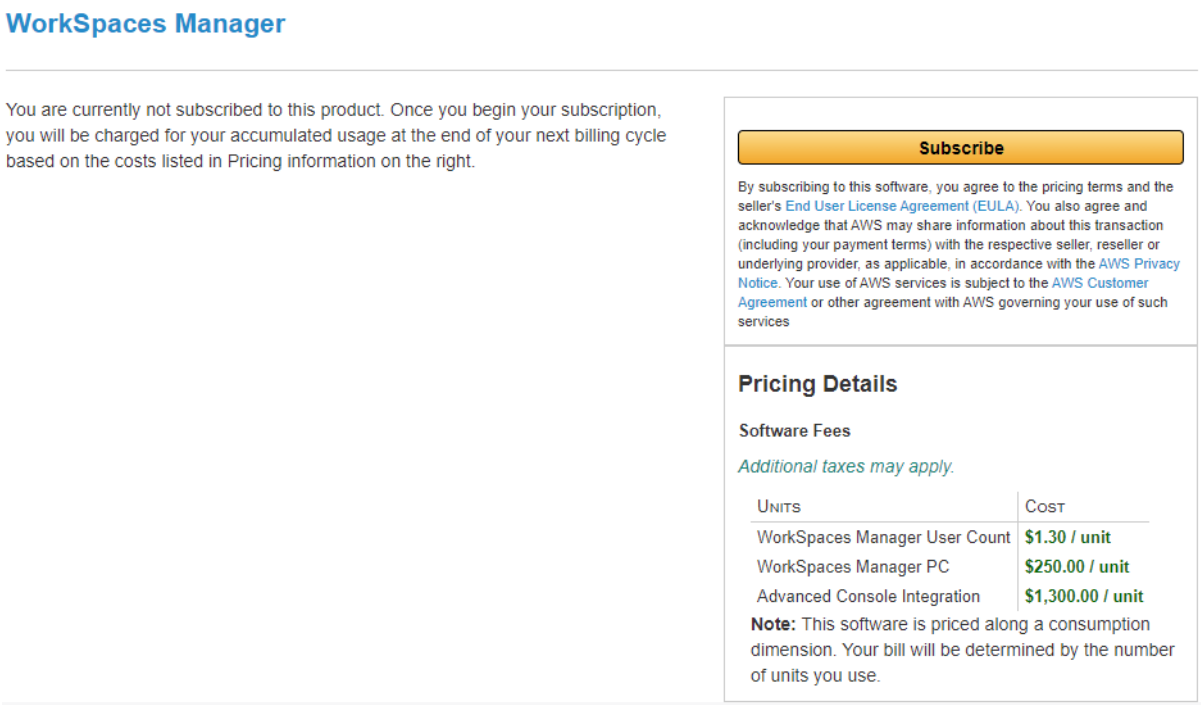
Go to the AWS Marketplace and search for 'Workspaces Manager' and select 'Nuvens' as the Vendor filter. Select the product below.



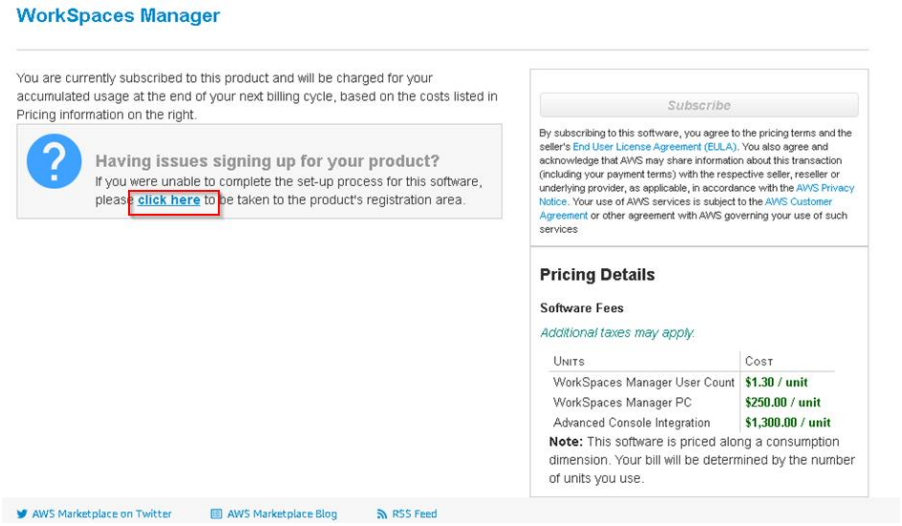
Now, select 'Continue to Subscribe'.



Some regions may ask for a second confirmation:



If you are asked to set up an account, proceed with this. If you have already subscribed to WorkSpaces Manager, but did not set up an account, select the link below which will take you through to the registration area.



Fill in the registration information. The only information necessary for a license are highlighted below.

Estimate the number of licenses that you will cover your entire WorkSpaces estate as the appliance will not work, if too fewer licenses are requested. WSM is provided with a trial period and you will only be charged once this is finished. You will be billed for the amount of licenses you use NOT the amount of licenses you request.

For purpose of clarification: If you request 1000 Licenses but only have 600 WorkSpaces, you will only be billed for the 600 Licenses, 30 days after your trial period ends.

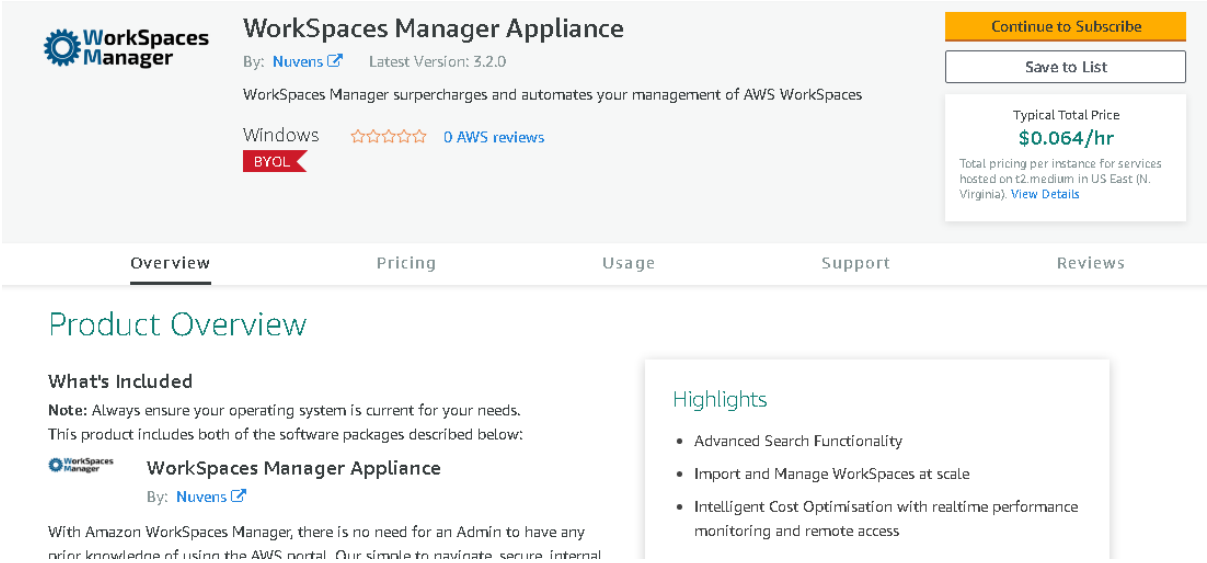
Your license will be emailed to you and you can then proceed with setting up the WorkSpaces Manager appliance in Section 5.

You will then receive an auto-generated email with a temporary key that can be used during the WSM installation.

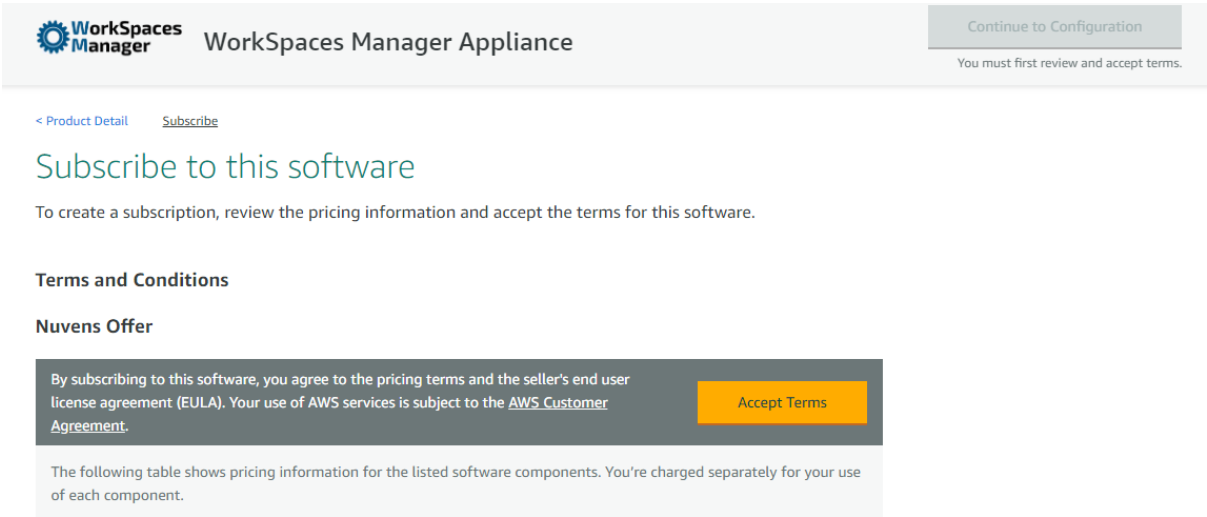
5. Installing the WorkSpaces Management appliance from AWS Marketplace

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.

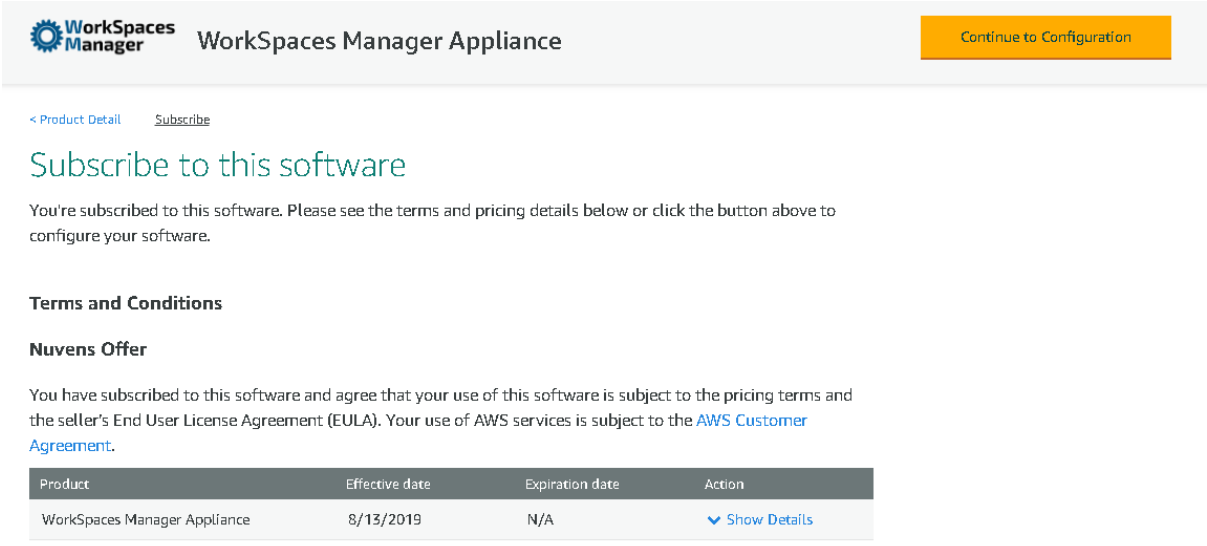
When found, select 'Continue to subscribe'.



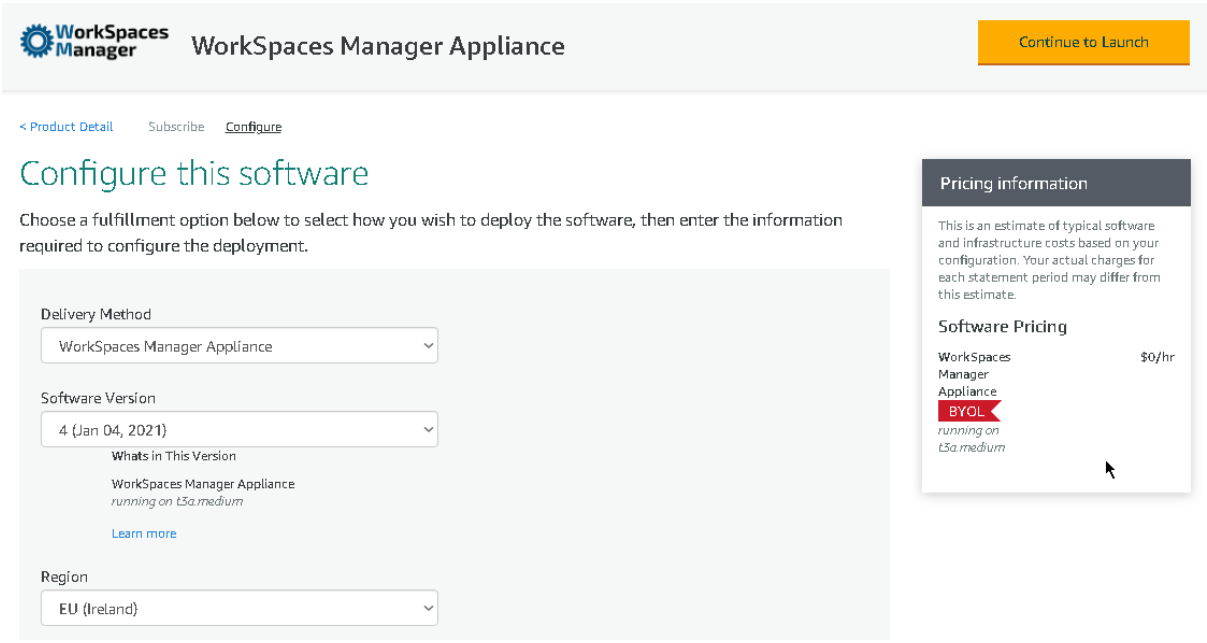
You now need to subscribe to the software. Select 'Accept Terms'.



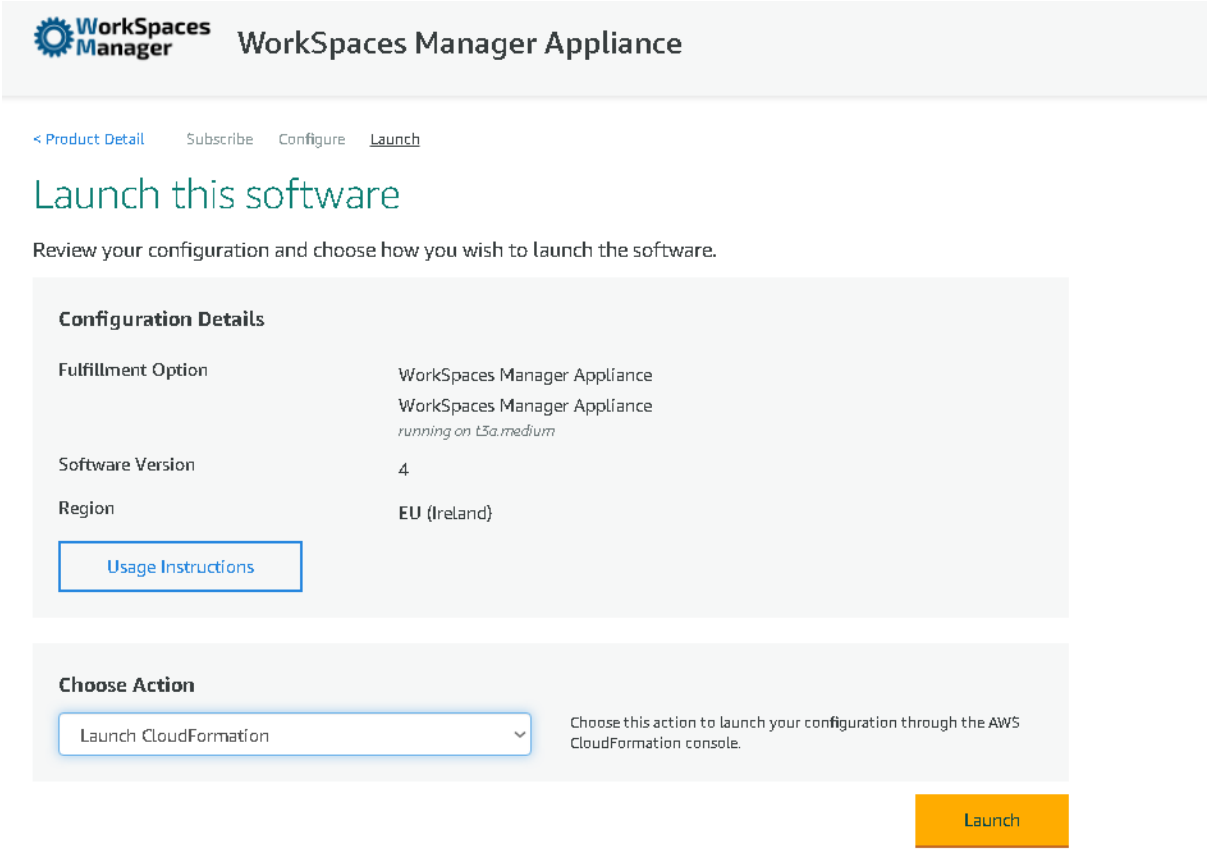
Now, select ‘Continue to Configuration’.



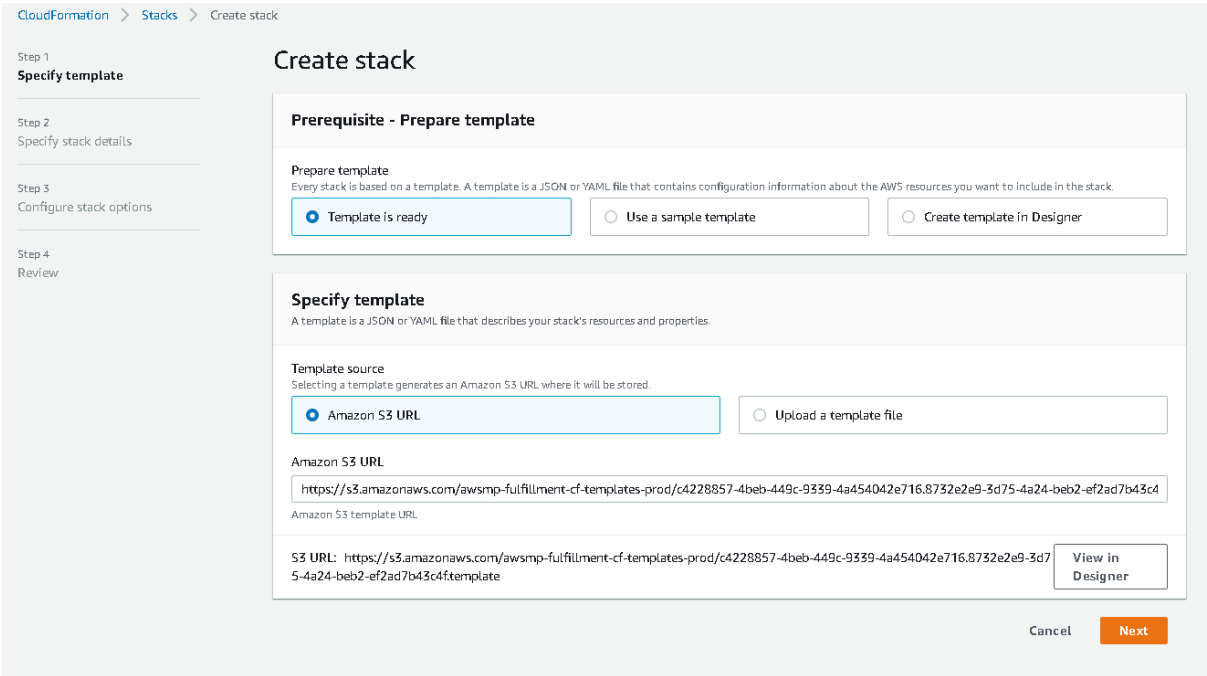
Select the region that you want your WorkSpaces Manager appliance to reside. Then select ‘Continue to Launch’.



From ‘Choose Action’, select ‘Launch CloudFormation’. Then select ‘Launch’.



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



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, like WSM-CF

Instance Type: Leave a t3a.medium (in a drop-down list) as they should be sufficient to run WorkSpaces Manager. We recommended t3a.large for bigger deployments but a t3a.medium is suitable for the majority of installations.

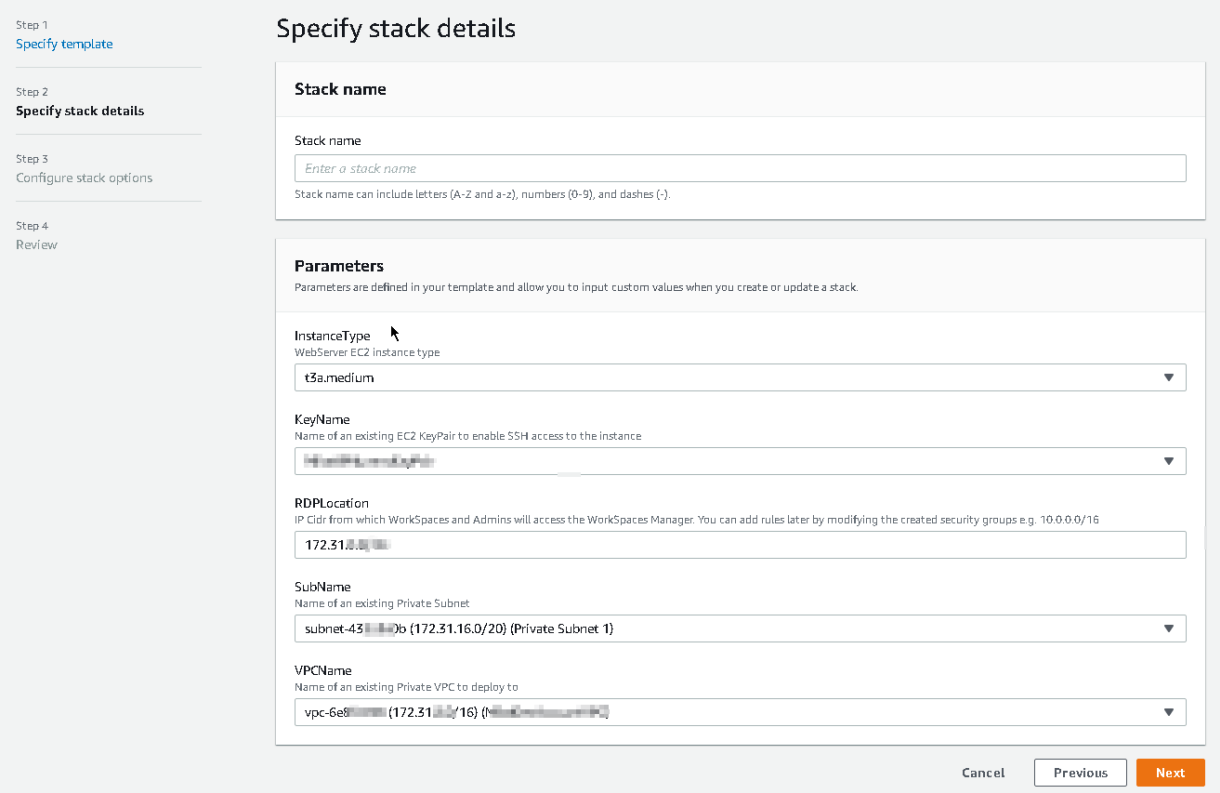
Key Name: You may have multiple key names under your IAM account for your own account. Select one to provide you with the local administrator credentials to the WorkSpaces Manager EC2 instance further down the line

NOTE: You will need the associated key file to be able to decrypt the password later, so we recommend that the key is added to Secrets Manager for future usage

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 (choose from a drop-down list)

VPCName: Select the VPC in which you wish to place the WorkSpaces Manager in (choose from a drop-down list)



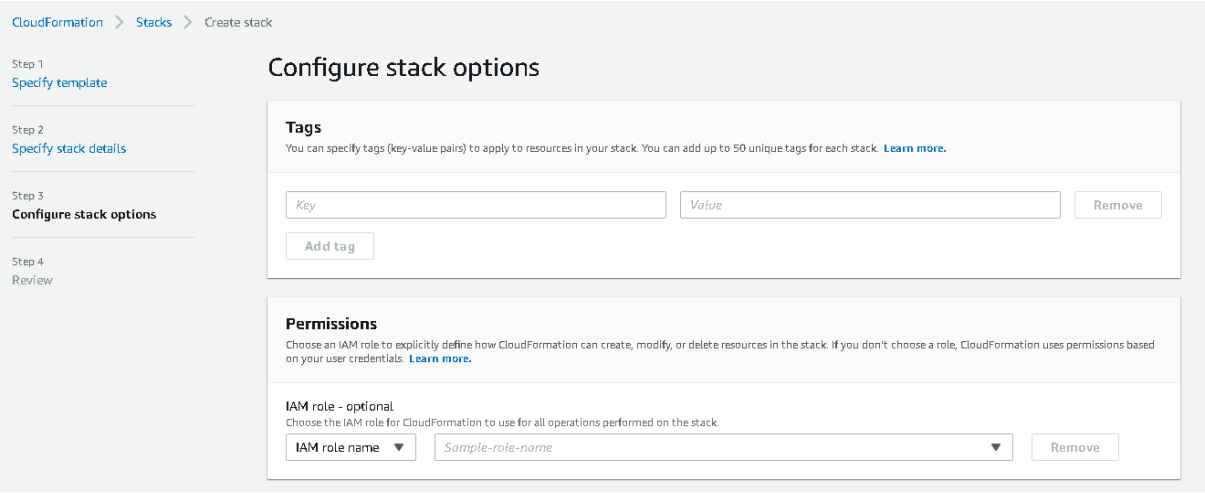
You now configure your stack options.

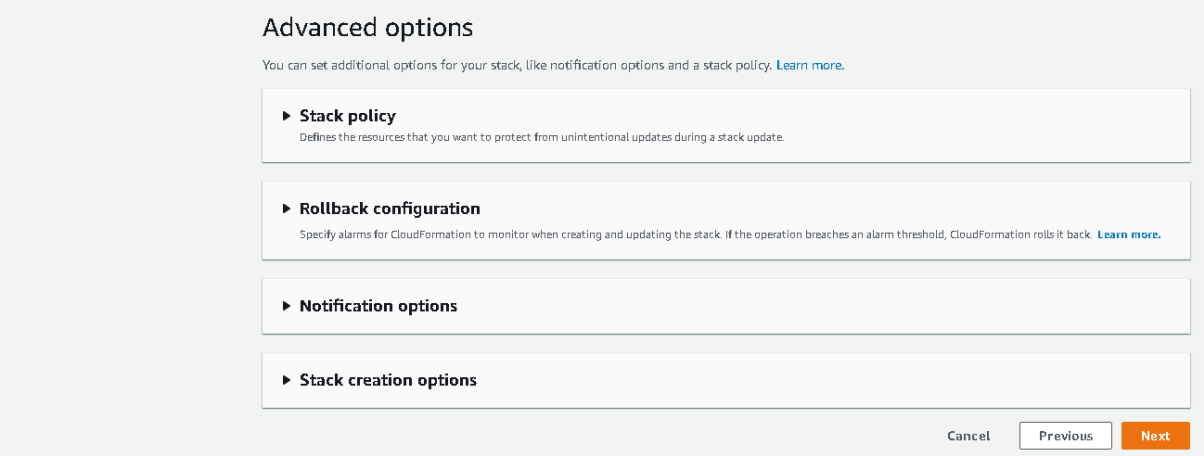
Tags: You can tag the resources if you wish, strongly recommended

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

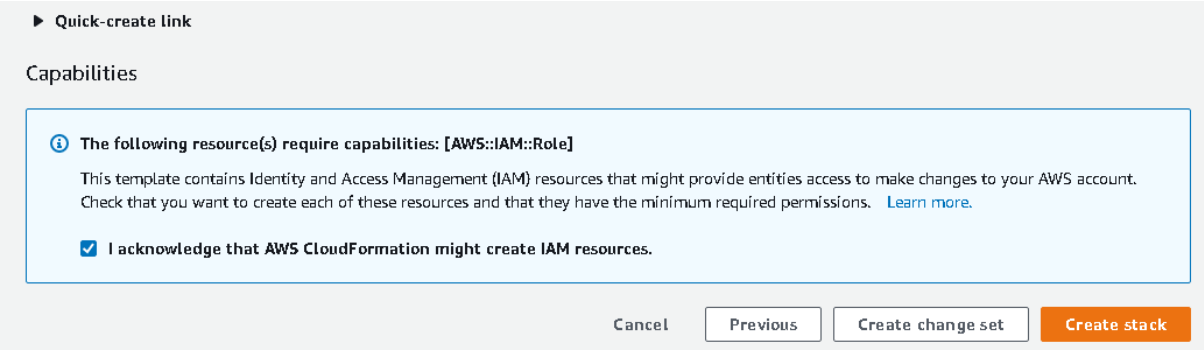
Advanced Options: Keep all options as default. You can enter an SNS Topic ARN to notify you of when the stack is created, but this is not necessary. You will know when it is finished as the WorkSpaces Manager will appear as an EC2 instance in the console

Then select 'Next'.

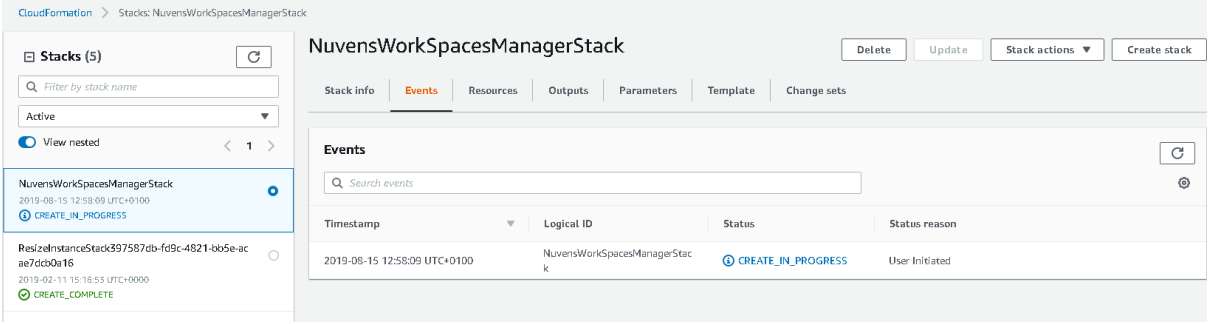




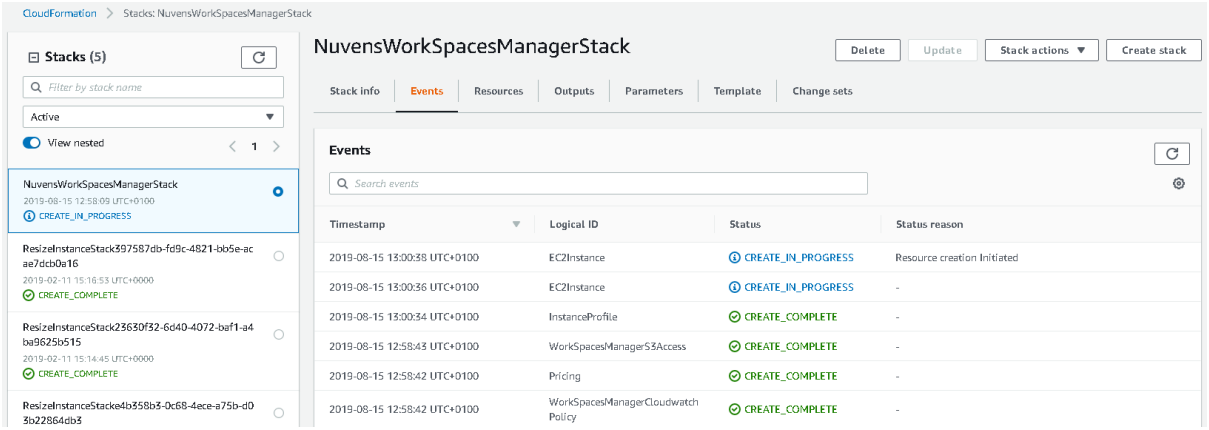
You will now find yourself at the 'Review' screen. Scroll down to the bottom, select the acknowledgement, and then select 'Create Stack'.



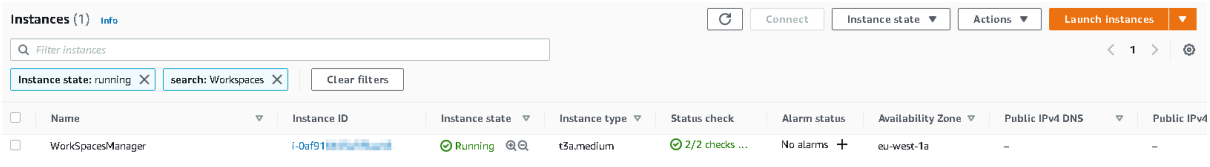
You will now return to the stack status screen where you can see the progress of the WorkSpaces Manager stack.



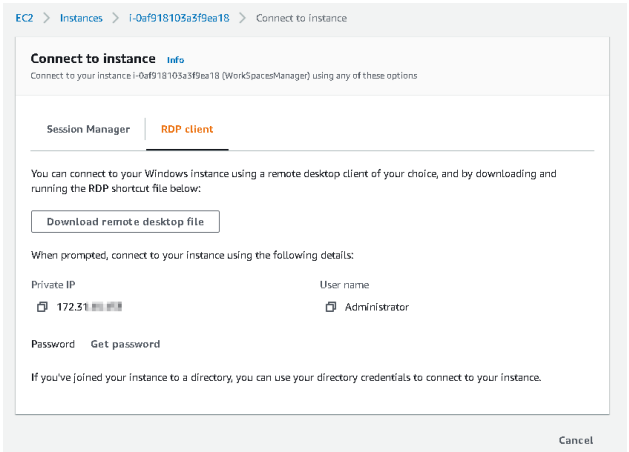
You can view the tasks as they are being performed. When the stack creation is complete, the status will change from 'CREATE_IN_PROGRESS' to 'CREATE_COMPLETE'. The stack creation takes around 3-4 minutes to complete.



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 to be auto generated.



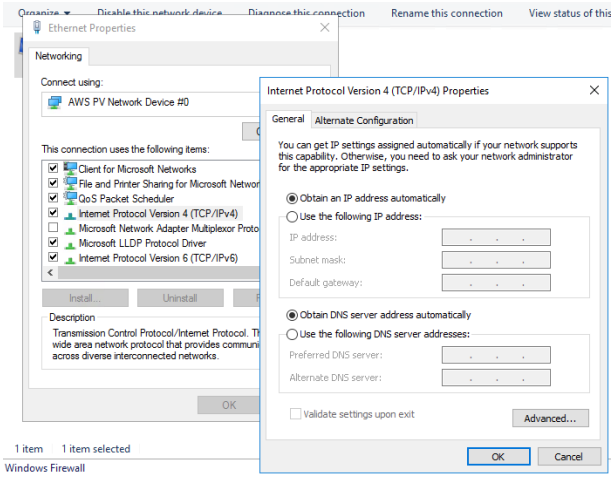
Now, RDP to your instance using the Private IP assigned to the instance using the local administrator password and using the KeyName and associated keyfile that you specified in the Stack Details section above. If you cannot RDP to the instance, you need to ensure you are connecting from a device within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



5.1 Join your WorkSpaces Manager instance to your Active Directory Domain

This is a mandatory requirement and the installation will fail if not joined. 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.



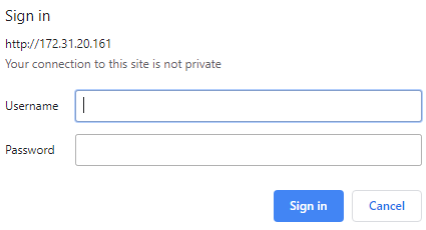
If the instance is not joined to the domain, the appliance will show an error message.

5.2 First Time Setup

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

Log on to the WorkSpaces Manager EC2 instance, go to your preferred browser and go 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'.



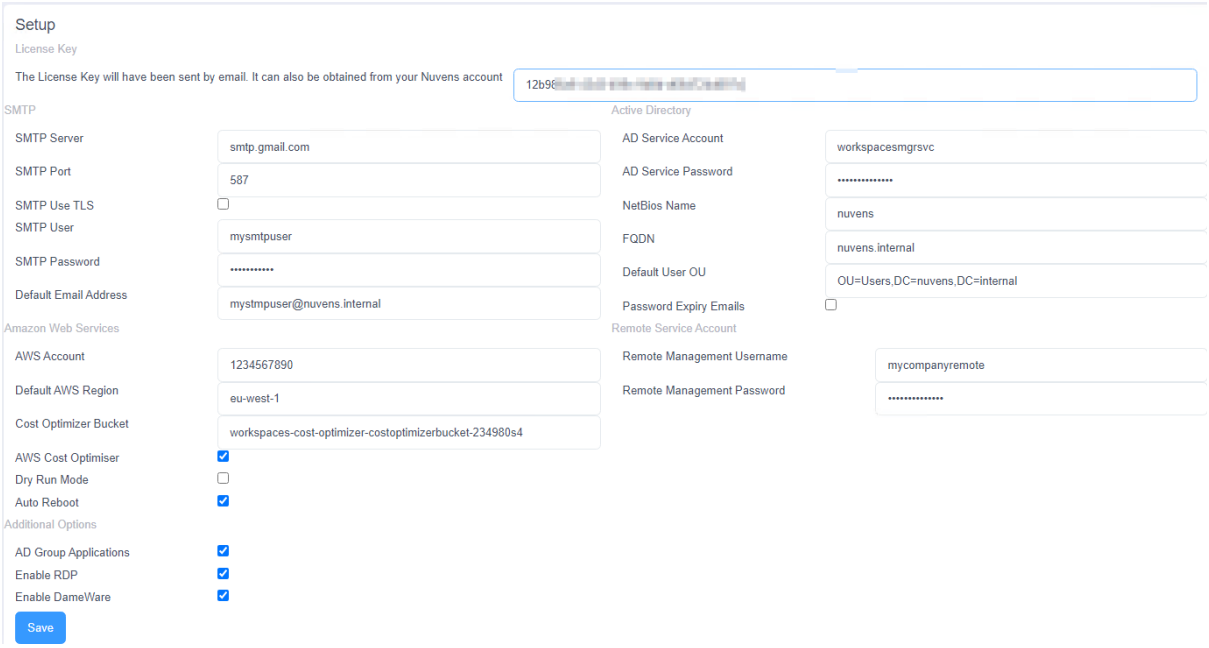
Once you successfully connect to the portal, you will be presented with a setup screen to enter information for:

- License key (obtained in Section 4).
- Active Directory settings
- SMTP settings (not mandatory)
- Amazon Web Services settings
- Additional options settings (not mandatory)

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@workspacesmanager.com

This is an example of the form completed.

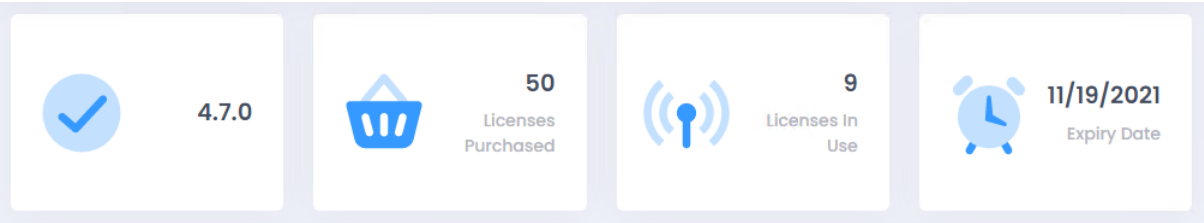


After saving, please wait for up to 30 seconds for the next screen to appear. Again, make sure that the instance has Internet access otherwise it will give you an error saying that the license code is invalid.

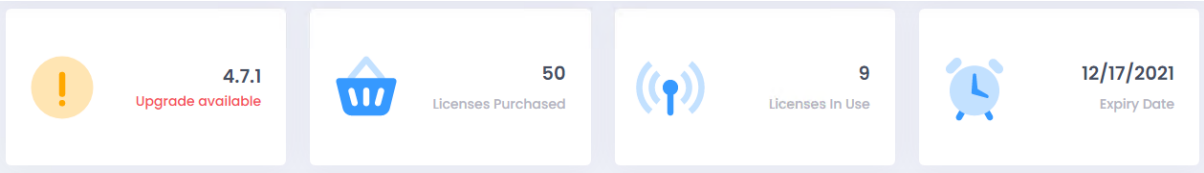
Once complete, WSM will display the administration section of the portal on the Options\Settings page. Further settings can be configured here once the portal is live. The various sections are covered below.

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.



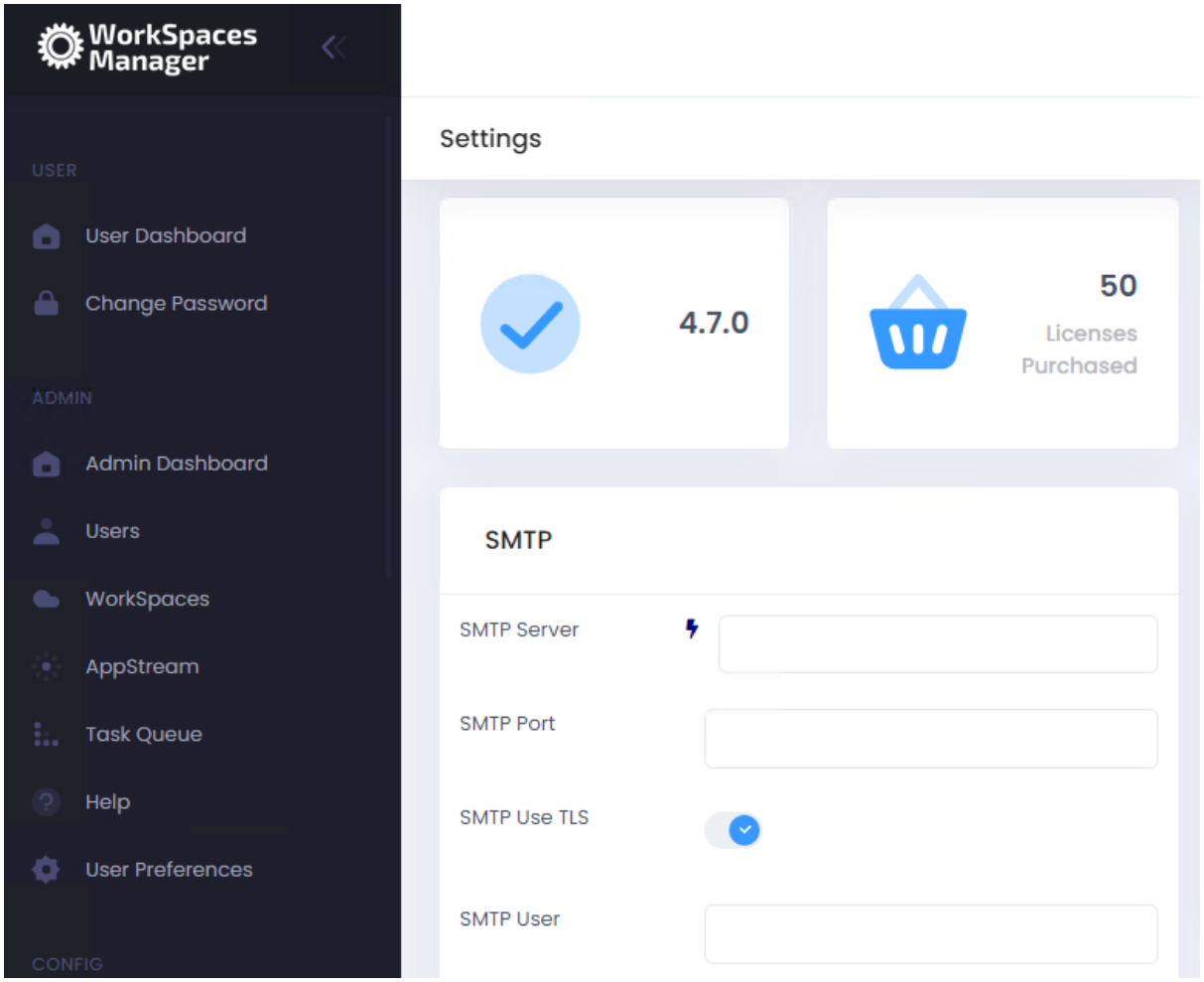
If the latest version is not installed, the system will let you know that a new one is available for download.



5.2.2 SMTP

This enables you to send emails to inform new users once a new WorkSpace is ready and\or if their password is to expire and is required for the auto-delete function.

You could use AWS Simple Email Service (SES) to achieve this, or your own SMTP setup. You can test the connection by selecting the lightning icon to the left of the field. For a guide on how to configure SES, please check Appendix 3.



5.2.3 Remote Service Account

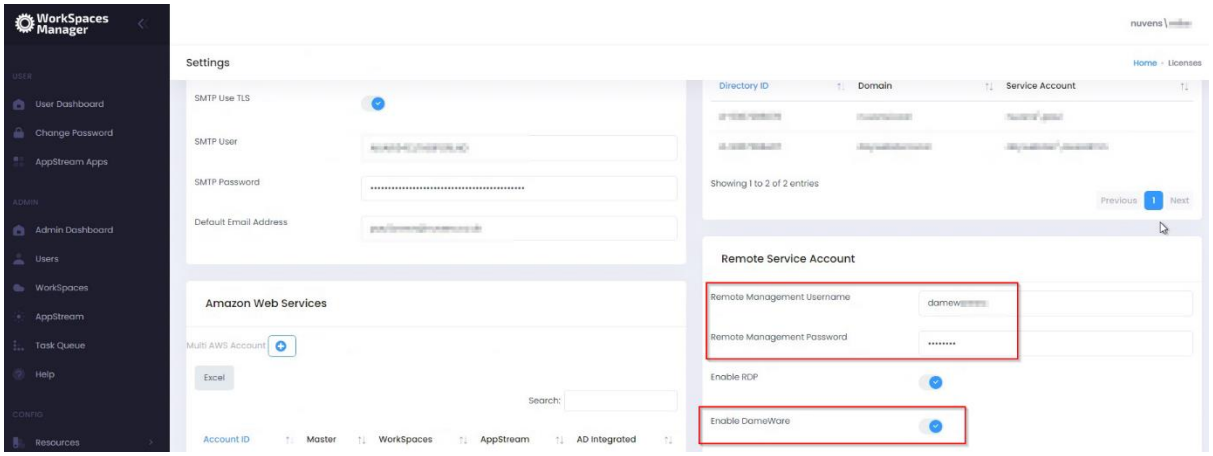
This is an account that you configure to remote control user devices using Remote connection like Dameware. This is the generic account that you connect with, in the format "username" and "password" (which will be standard throughout the organisation). You can remote control a user's WorkSpaces by selecting '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 for TCP/3389.**

5.2.3.2 Enable DameWare

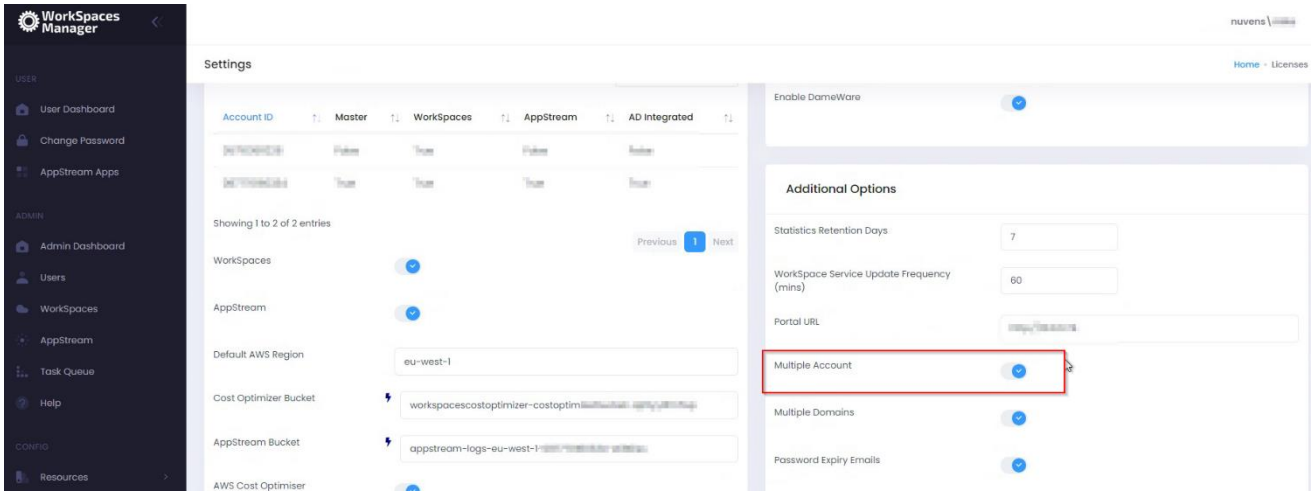
Enables the usage of DameWare Remote Control to connect to the user's WorkSpace from within the Portal. A DameWare license is required. Security Group must allow for inbound UDP/137, TCP/138-139, TCP/443, TCP/3389, TCP/5900 and TCP/6129-6133.



5.2.4 Amazon Web Services

5.2.4.1 (Single\Multi) AWS Account

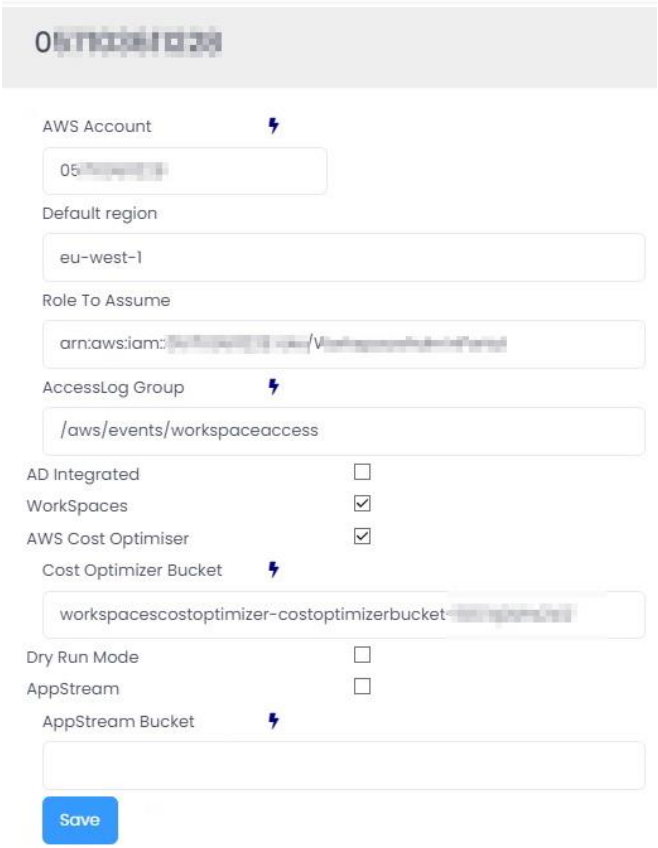
WorkSpaces Manager allows you manage WorkSpaces across single, or multiple, AWS accounts. When you set up WorkSpaces Manager, you will set up a single account. You can set up multi-AWS accounts by enabling this function and following the instructions in Section 7 of the 'WorkSpaces Manager Administrator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



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

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

Select one and you will see the options. These can be toggled on or off (like Dry Run mode) if required.



5.2.4.2 API Retry Attempts

The number of attempts to retry an AWS API Call. **For this change to take effect, the app pool in IIS will need to be restarted.**

5.2.4.3 APP Jitter Period (ms)

Used to create a random delay between API calls. **For this change to take effect, the app pool in IIS will need to be restarted.**

5.2.4.4 WorkSpaces

Turns on the WorkSpaces Management menu function.

5.2.4.5 AppStream

Turns on the AppStream Management menu function.

5.2.4.6 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.

5.2.4.7 Show AWS Bundles

This will enable the AWS default bundles to be visible if required.

5.2.4.8 AccessLog Group

This is to add the CloudWatch Log Group that manages all the information from users' connection, like public IP, client version, latency, etc. Check Appendix 2 for details.

5.2.4.9 Cost Optimizer Bucket

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

5.2.4.10 CO (Cost Optimizer) Alternate Format

This option is used when upgrading from version 1 of the AWS Cost Optimizer to the newest. If there is an error about getting the log from the bucket, we will enable this feature.

5.2.4.11 AppStream Bucket

Specifies the AppStream Usage bucket.

5.2.4.12 AppStream Settings Bucket

Specifies the AppStream Settings bucket and formatted as appstream-app-settings-REGIONID-ACCOUNTID-xxxxxxxx.

5.2.4.13 AWS Cost Optimizer

This enables AWS Cost Optimizer.

5.2.4.14 Dry Run Mode

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

5.2.4.15 Auto Reboot

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

5.2.4.16 Auto Reboot Tag Name

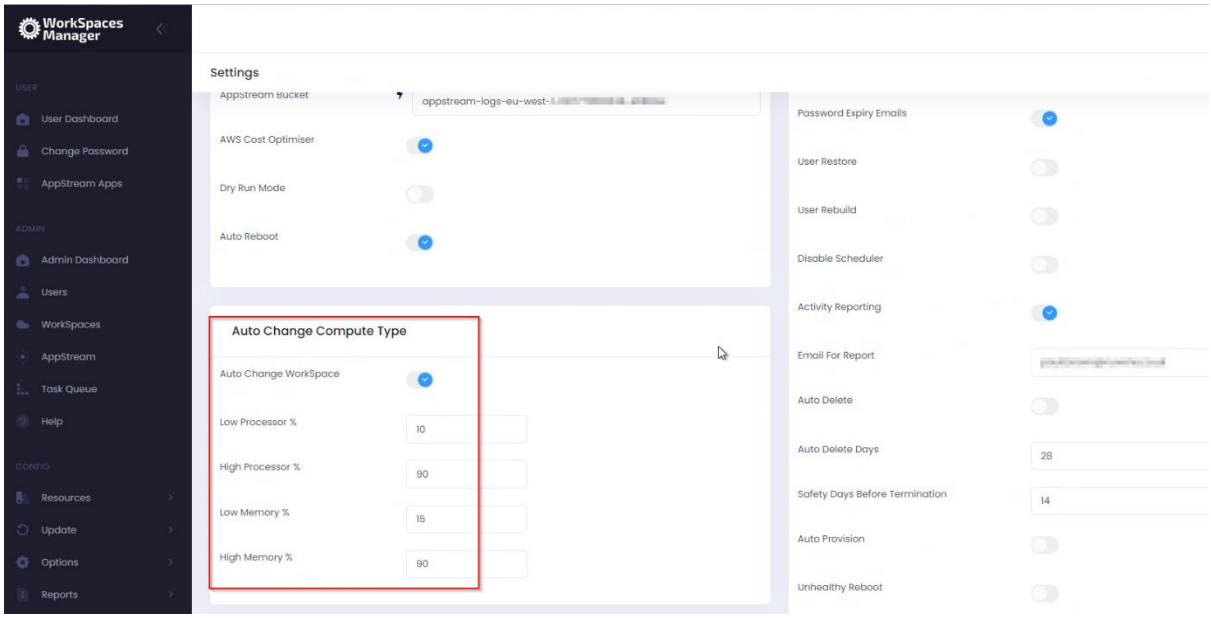
If AutoReboot is enabled and a value is added in this field, the "Reboot Hour" will be taken from this Tag value.

5.2.4 Auto Change Compute Type

You can opt for WorkSpaces Manager to automatically change compute type of WorkSpaces. 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.

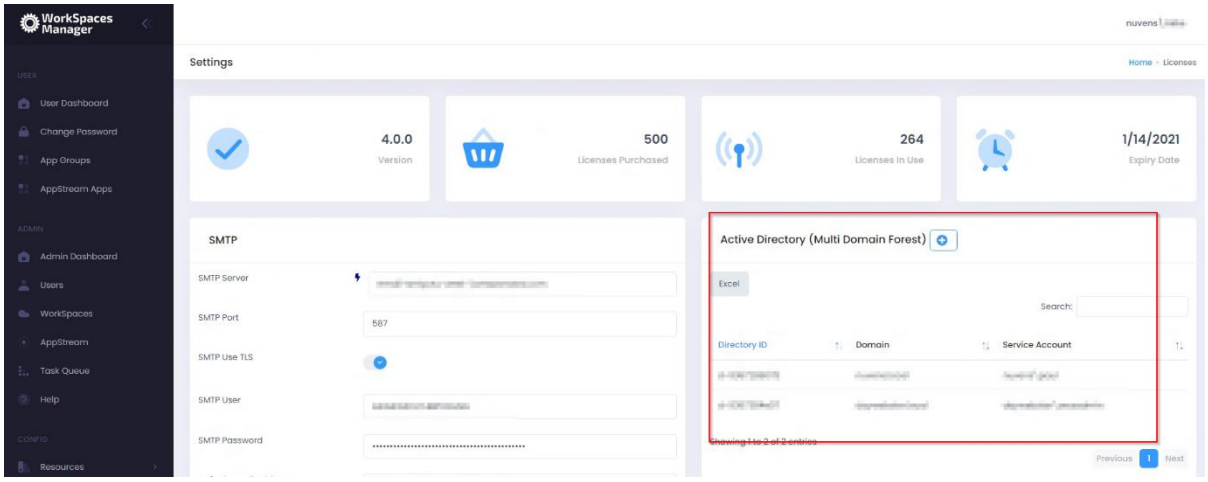
Set Low and High Processor and Memory values (these are up to you). WorkSpaces Manager will also advise you of recommendations.

WSM will also make recommendations if a WorkSpace is oversized based on the users performance needs.



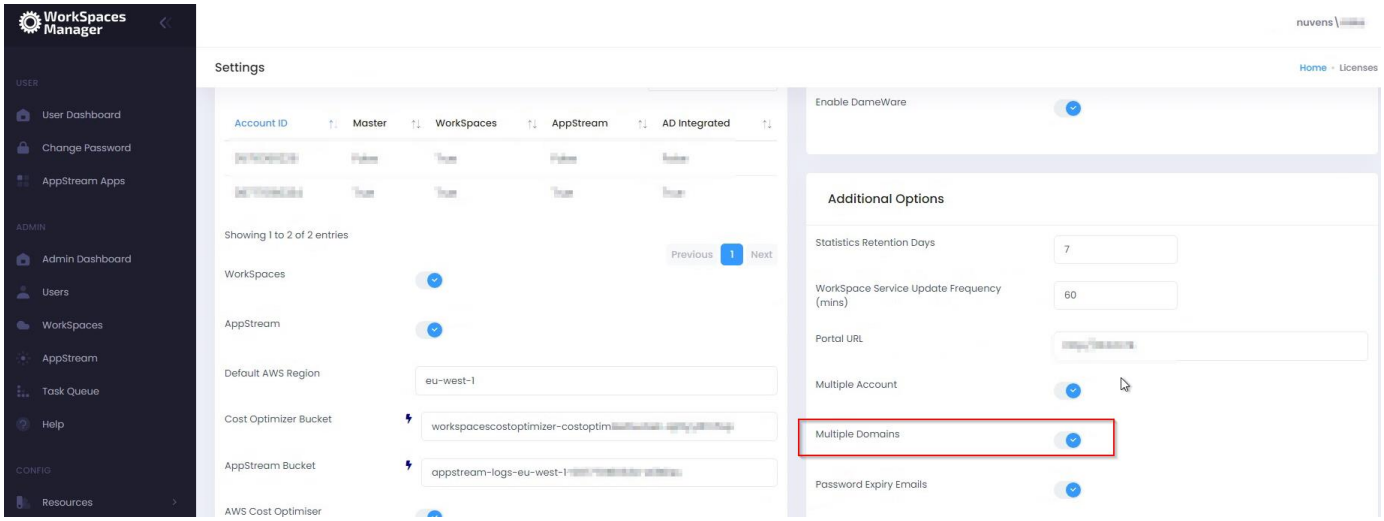
5.2.5 Active Directory (Single\Multiple Domain Forest)

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.



to delete computer objects.

NetBIOS name:

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

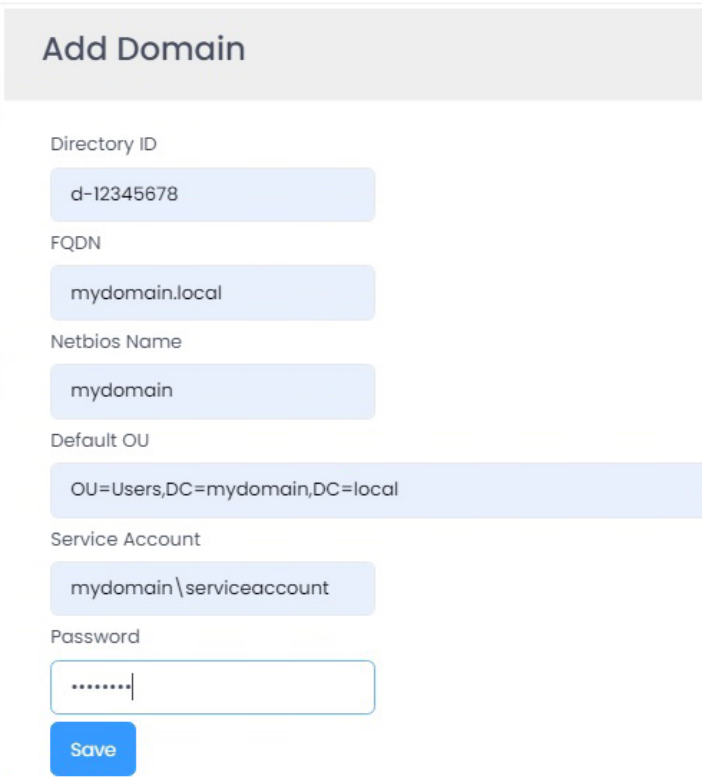
FQDN:

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

5.2.7 Additional Options

5.2.7.1 Statistics Retention Days

If the WorkSpace Performance Monitor Agent has been deployed to the WorkSpaces, it will periodically report back the server key metric statistics 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 of time. 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. https://wsmportal.mycompany.com.

We recommend adding a Network Load Balancer (NLB) offloading SSL certificates in front of the portal, as explained in Appendix 4.

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 through one central WSM appliance.

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 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 to the designator receiver of the reports. It requires the WSM agent to be installed. 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 stated above.

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, the WorkSpace will be deleted.

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 Auto Provision Frequency

This value is how often, in minutes, the WSM Portal will check the AD Groups to trigger auto provision actions.

5.2.7.17 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 for further investigation.

5.2.7.18 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.

5.2.7.19 Use Global AutoStop Time

This sets all the WorkSpaces to have the same AutoStop time. Value in hours.

5.2.7.20 AutoStop Timeout

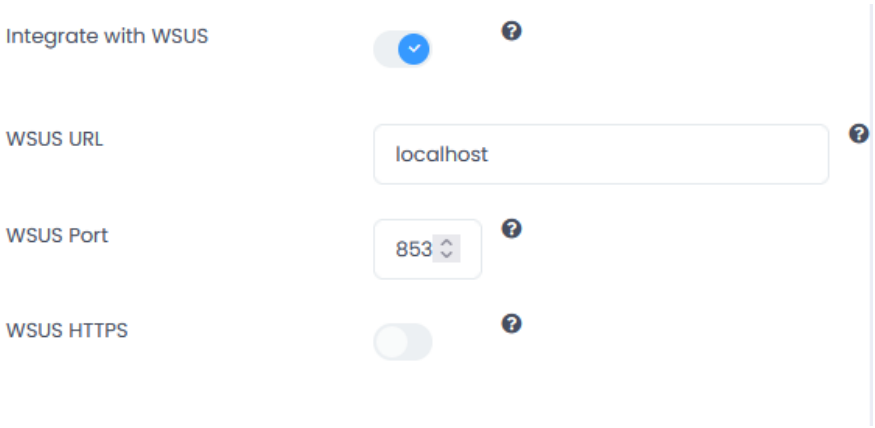
The number of hours for an inactive WorkSpace to hibernate.

5.2.7.21 Alternate Email Tag

Allows to specify an alternate email user or group for the report.

5.2.7.22 Integrate with WSUS

Windows Server Update Services (WSUS) enables to deploy the latest Microsoft product updates in an automatic manner, ensuring that the Windows WorkSpaces are up-to-date in terms of upgrades. More info in Microsoft website.



If this is enable, then we can also set the following elements listed below.

5.2.7.23 WSUS URL

This will normally default to the same node in which WSM runs, so we will use "localhost". This requires to configure the basic options of WSUS. There is an intro in Appendix 5.

5.2.7.24 WSUS Port

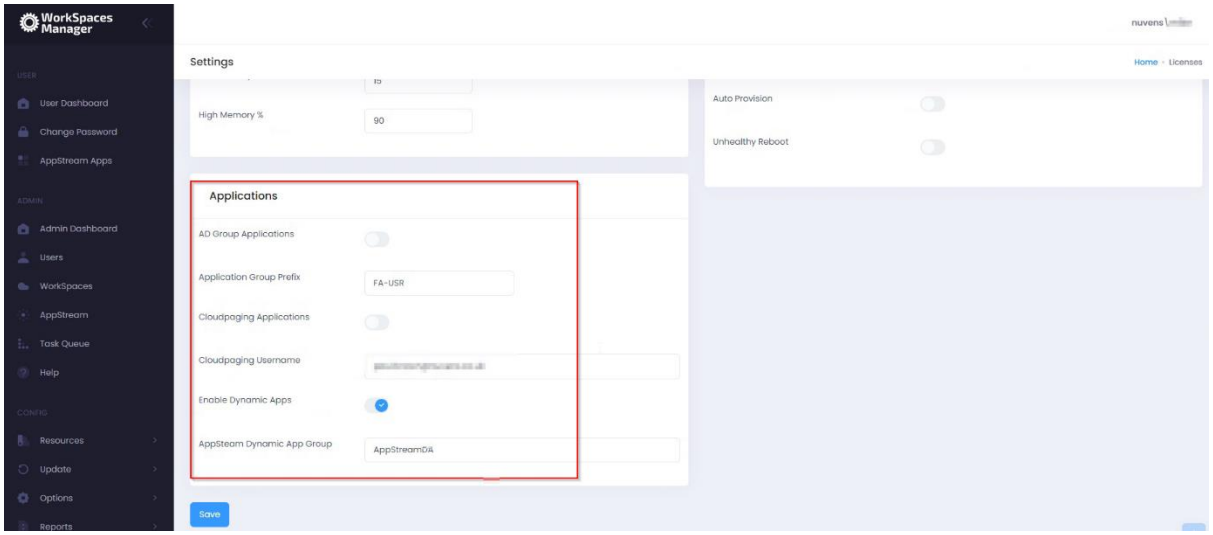
Although this can be changed, we do not recommend to change the values of the WSUS port; so we will use 8530 for http and 8531 for https, as recommended by Microsoft.

5.2.7.25 WSUS HTTPS

This would enable communications with WSUS through HTTPS, which also requires a valid SSL Certificate installed on the WSUS server.

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.

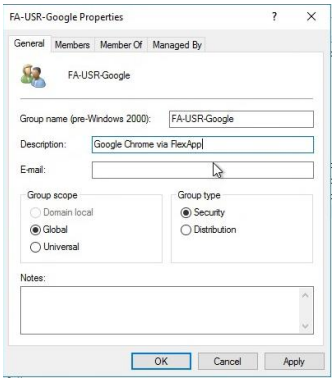


5.2.8.1 AD Group applications

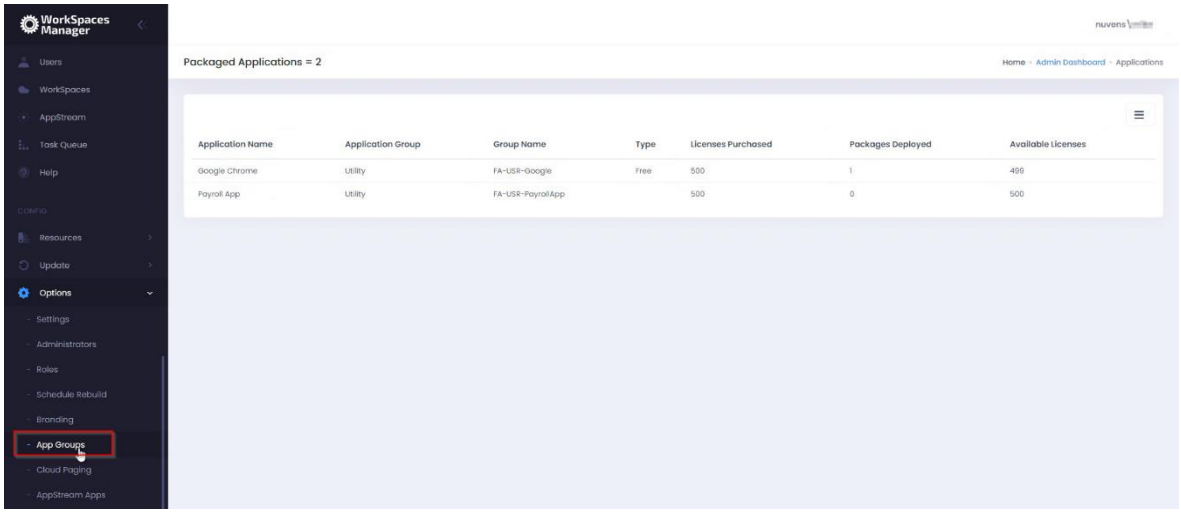
Enable this is you use software distribution on to your WorkSpaces from the likes of Liquidware FlexApp, App-V, etc. This allows users to add and remove applications available to them through the Self-Service side of the WorkSpaces Manager Portal. You can change this to your own prefix when you have 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 understand 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.

5.2.8.5 Enable Dynamic Apps

Enables the AppStream Dynamic Apps features.

5.2.8.6 Dynamic Apps File Path

Specify the local path for the AppStream Dynamic Apps. By default, this path is D:\AppStreamApps

5.2.8.7 AppStream Dynamic Apps Group

Specify the Group whose members will have a dynamic apps file generated

5.2.8.8 AS Group Context

LDAP Path for the AppStream Group, like OU=Groups,DC=example,DC=com

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://10.0.1.2"
"Frequency"=dword:00000005
"IdleMinutes"=dword:00000015
"Visible"="false"

"Portal" – Replace with **Error! Hyperlink reference not valid.**.

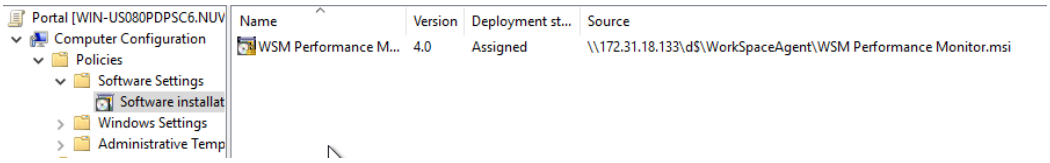
"Frequency" = The value data is a numeric value of minutes (e.g. '5' where the Agent reports back to the database every 5 minutes with metrics. You can change this frequency to a greater value, if you have a large estate, as a lot of information will be stored in the database).

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). It can be also installed in the default golden image/bundle.

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

(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 (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).

(c) 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

(d) 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)

(e) 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 deploying AWS RDS Microsoft SQL Server into at least 2 Availability Zones.

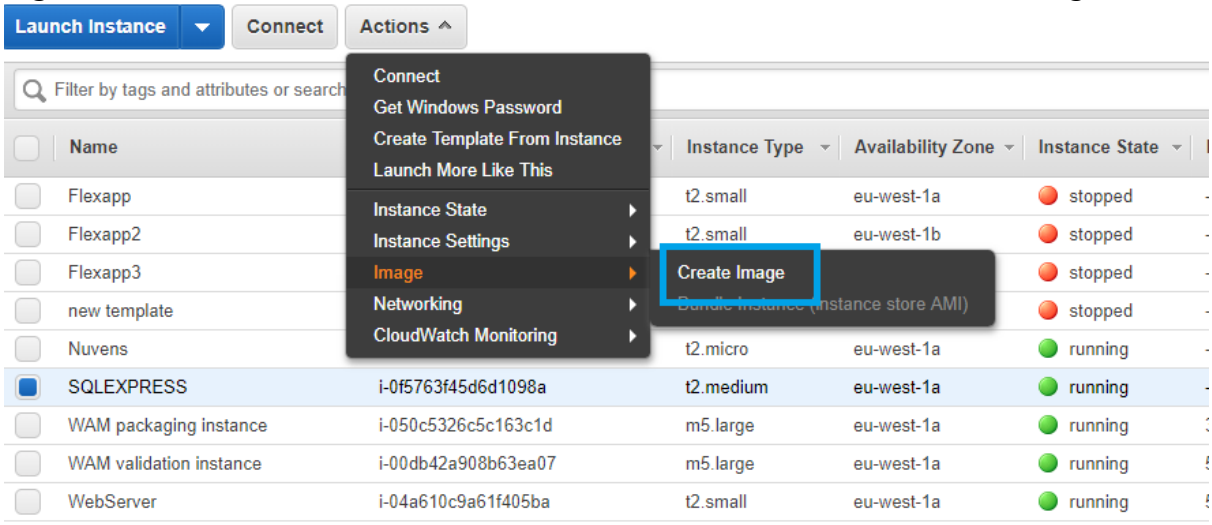
After deploying RDS you will need to do the following actions:

- 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.

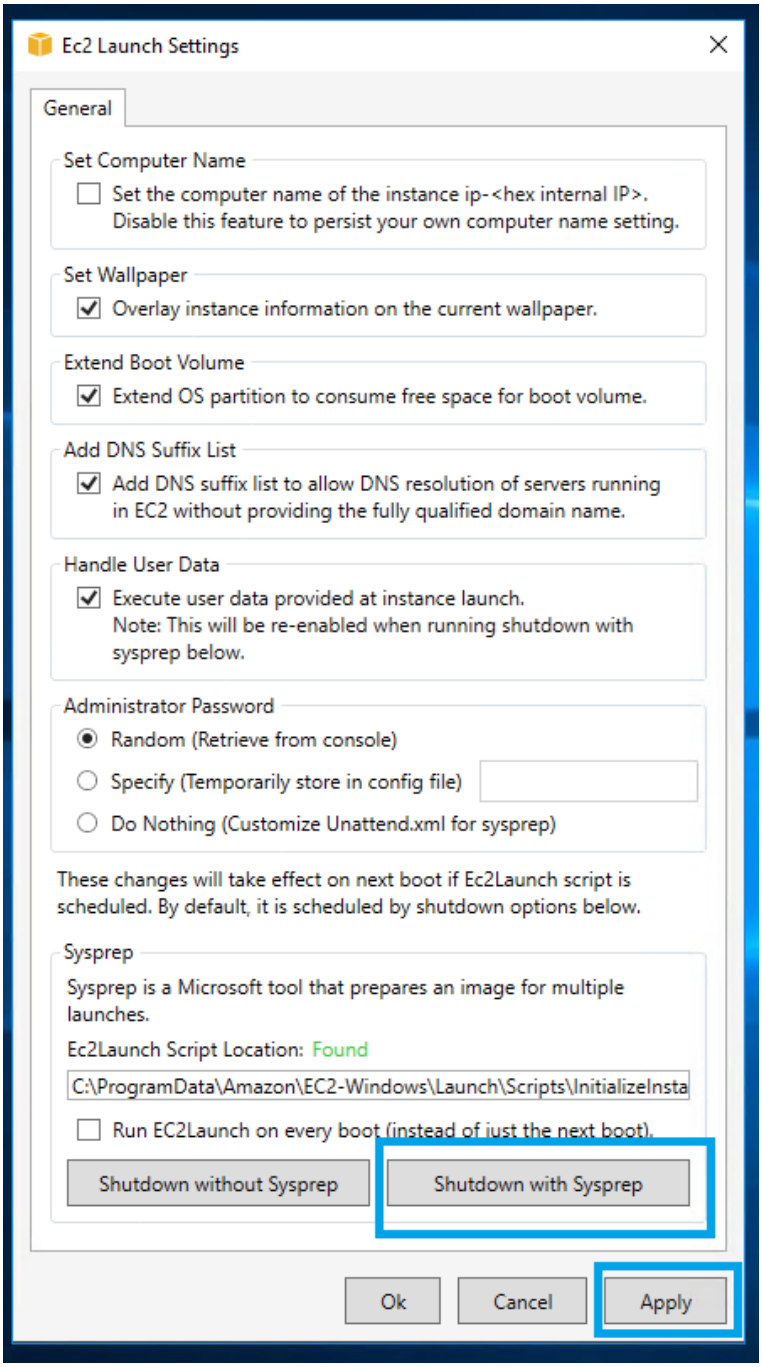


3. Name the Image and click Create Image

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'



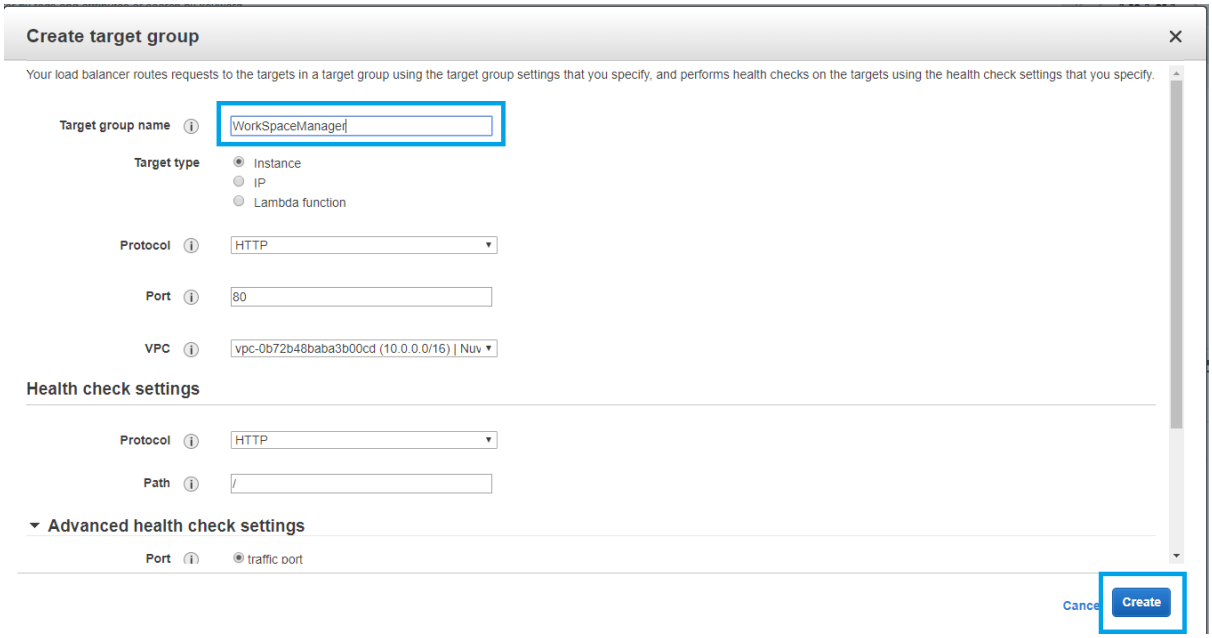
6. This will start a process of removing Windows user and system settings. Once it has completed the instance will be left in a stopped state
7. The original appliance can now be started again
8. The Sysprepped stopped image can now be imaged again to create our master appliance image. Once the AMI has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

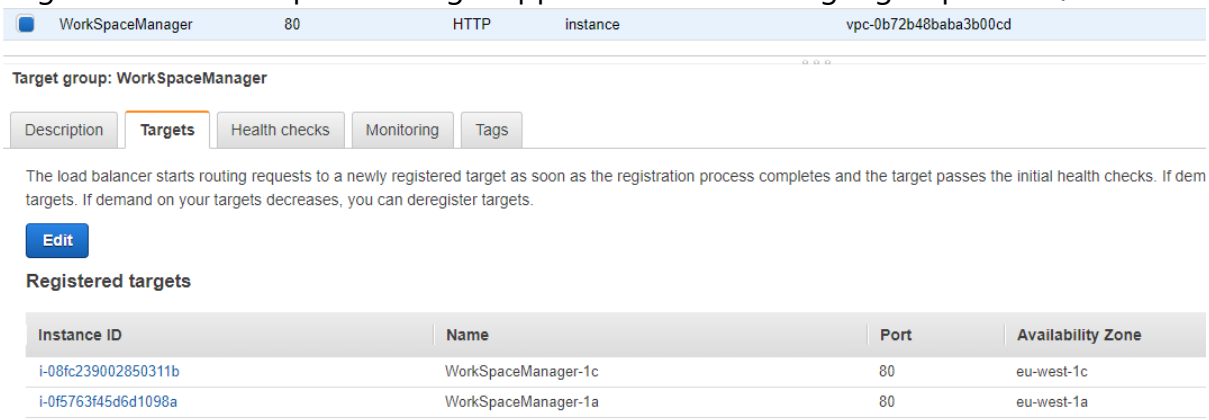
created. If you are launching with domain joined configured and ensuring that you assign the 'WorkSpacesManager' Role, the instance will be available after about 30 minutes.

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'



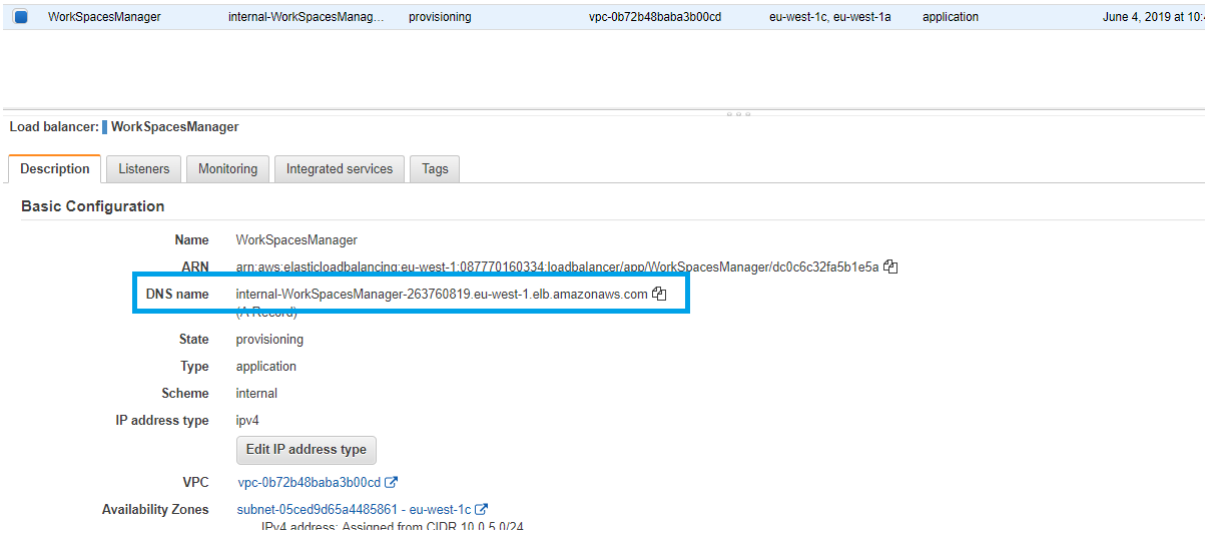
3. Register both WorkSpace Manager appliances with the target group as TCP/80



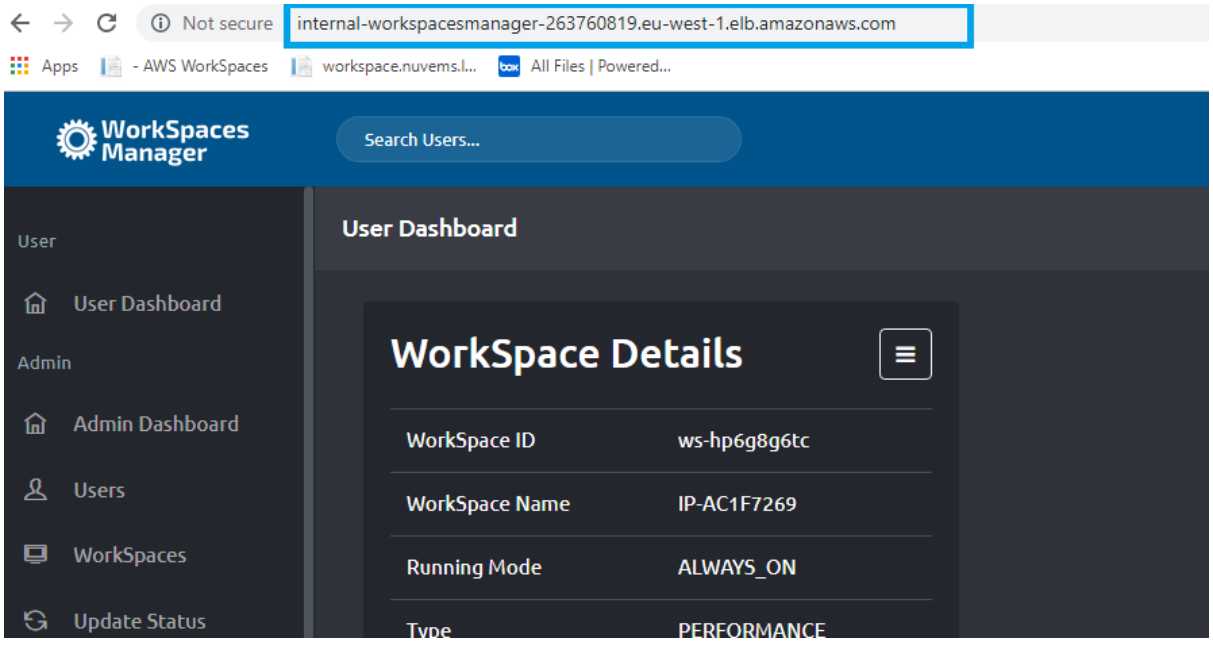
4. Next create a Network Load Balancer (NLB, not ALB or ELB) ensuring you select the Availability Zones that was used when creating the target group and the Scheme is set as 'Internal'
5. On Step3: Configure Security Groups, create a new security allowing inbound HTTP from the private subnets

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.

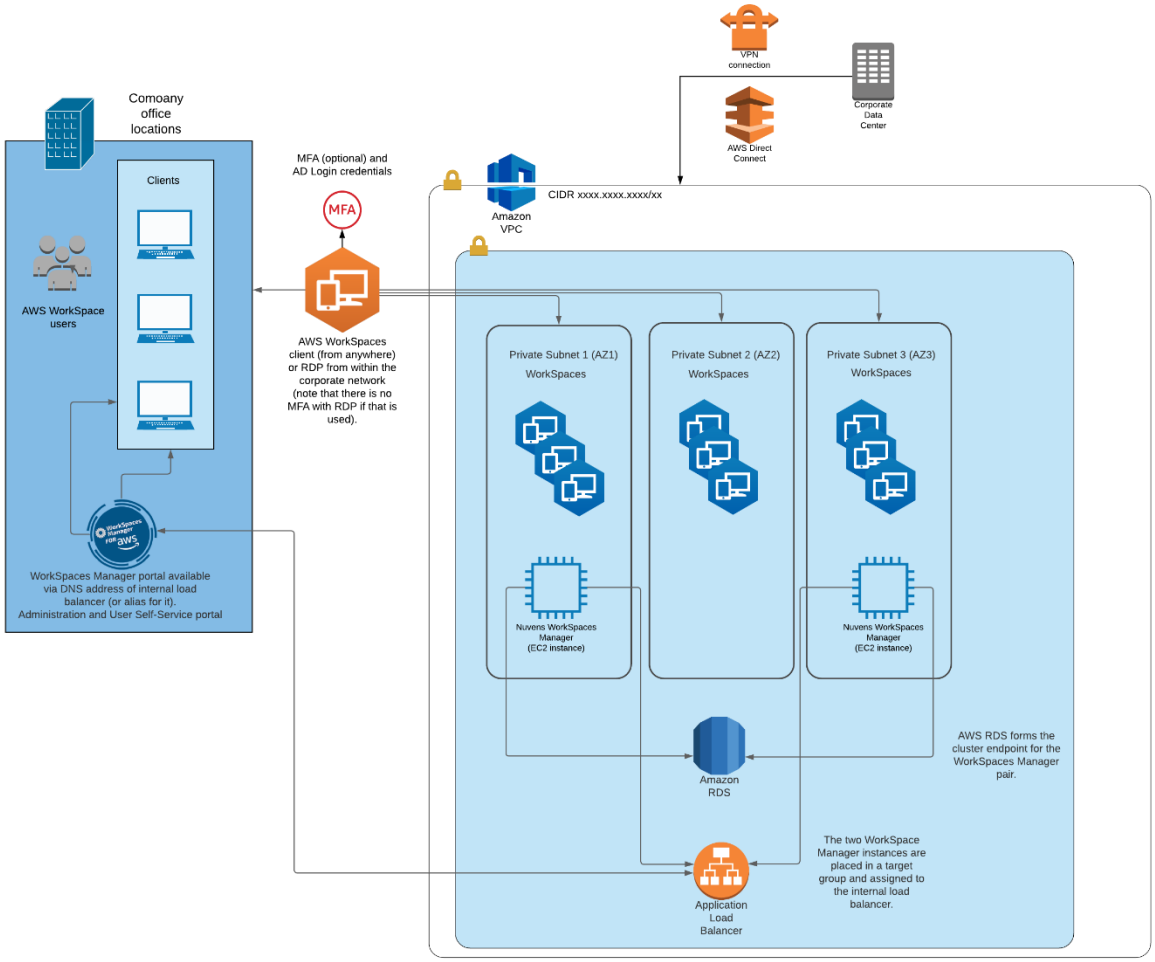


The DNS name can then be used to access the portal which will be load balanced across both instances.

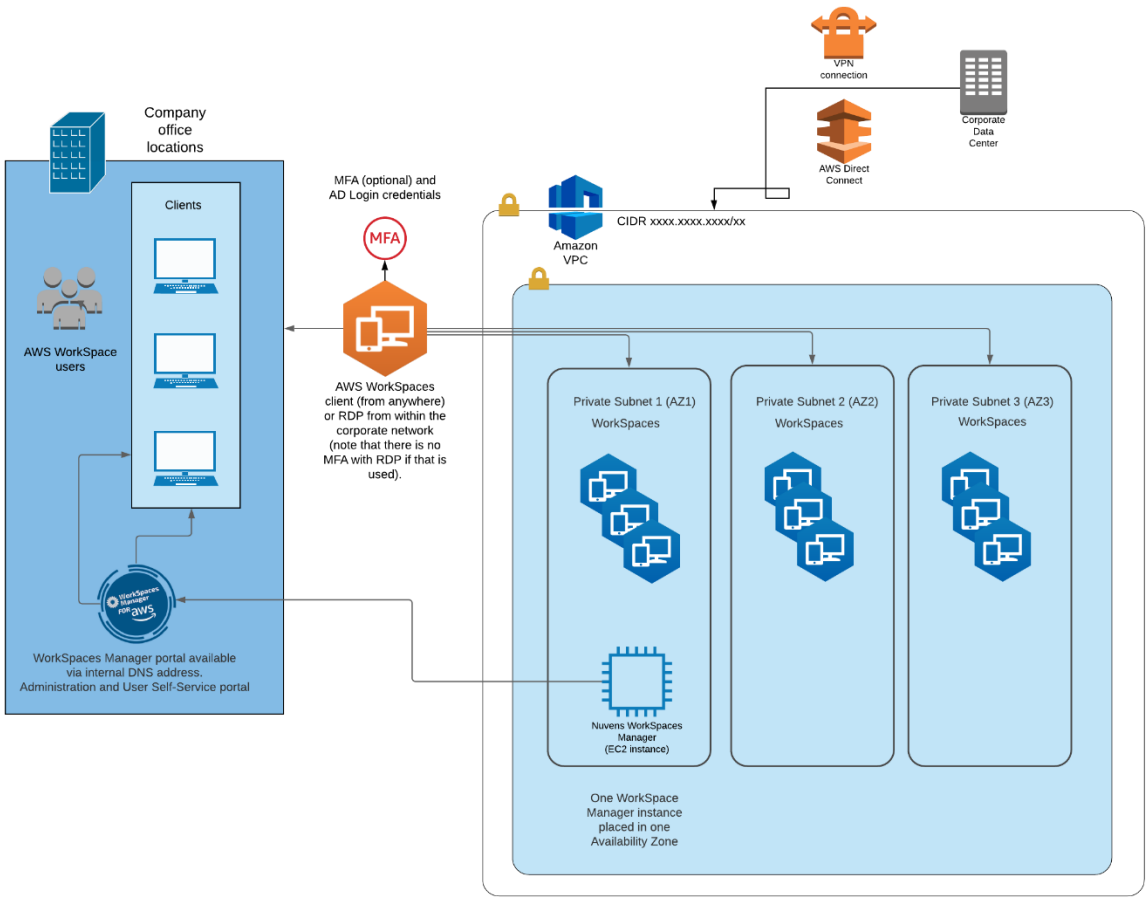


The portal is now in full HA mode load balanced across 2 AZ's with an HA database supporting it. However, the address is not very friendly. See 'Securing the Portal and adding a friendly portal address' in Section 8.

Example of a HA deployment using two Availability Zones.



Example of a single AZ deployment.

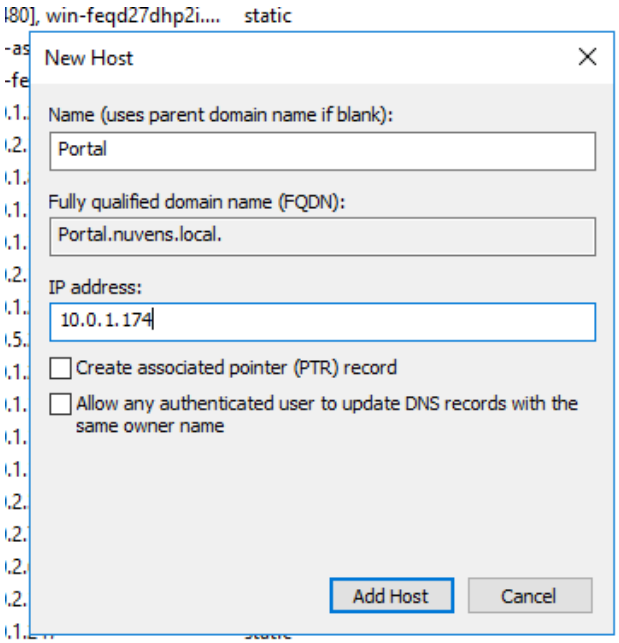


8. Securing the Portal and adding a friendly portal address

8.1 Portal address

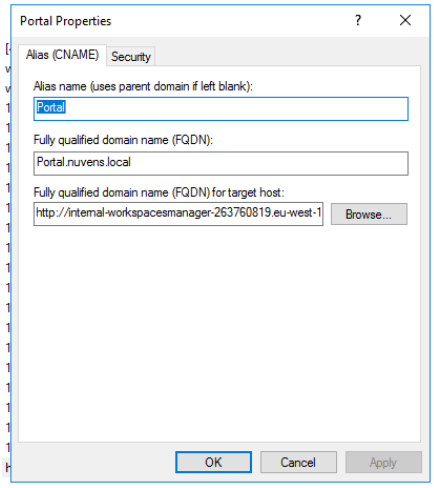
Rather than accessing the Portal via the IP address of the instance you can add a record to your DNS server.

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



This will now allow you to reference the portal, in this scenario we have used http://portal.nuvens.local, but please ensure you use your domain instead of Nuvens.

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


Portal Properties
Alias (CNAME)
Security
Alias name (uses parent domain if left blank):
Portal
Fully qualified domain name (FQDN):
Portal.nuvens.local
Fully qualified domain name (FQDN) for target host:
http://internal-workspacesmanager-263760819.eu-west-1
Browse...
OK
Cancel
Apply

Appendix 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:

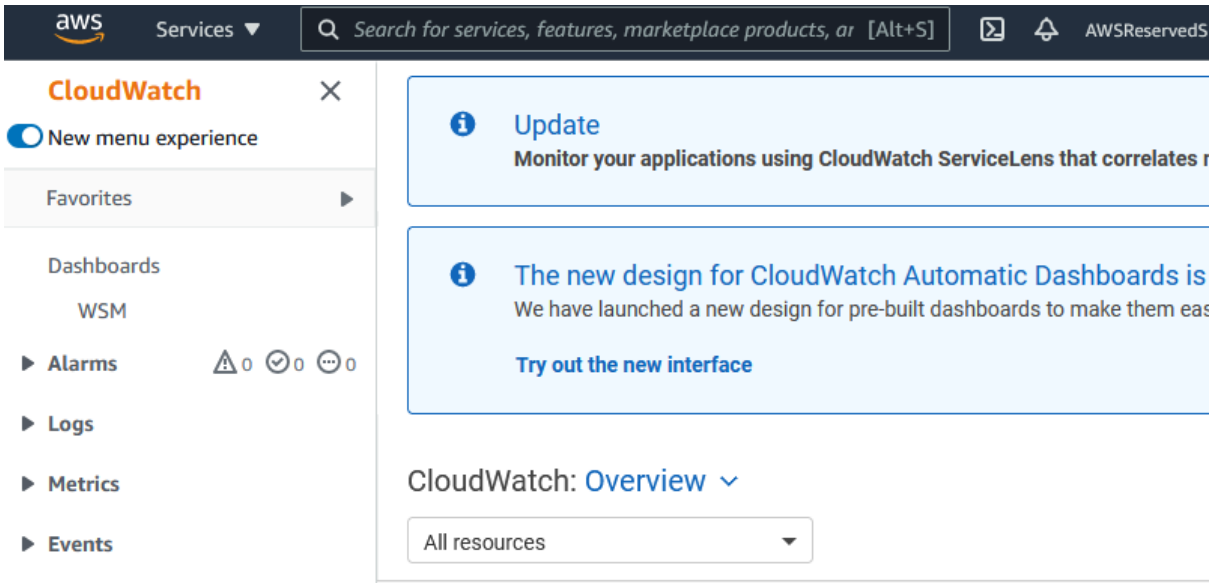
Operation	Permissions Needed
User Management	
Create Users	• Must be a member of the built-in Administrators group or Account Operators group, or, • Must have permissions to create, delete, and manage user accounts or equivalent permissions in the relevant OU or container in Active Directory
Modify Users	• 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 **Note:** It is also possible to grant the permissions to modify on specific attributes instead of the object as a whole
Delete Users	• 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	• 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	• 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	• 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	• 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	• 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	• 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

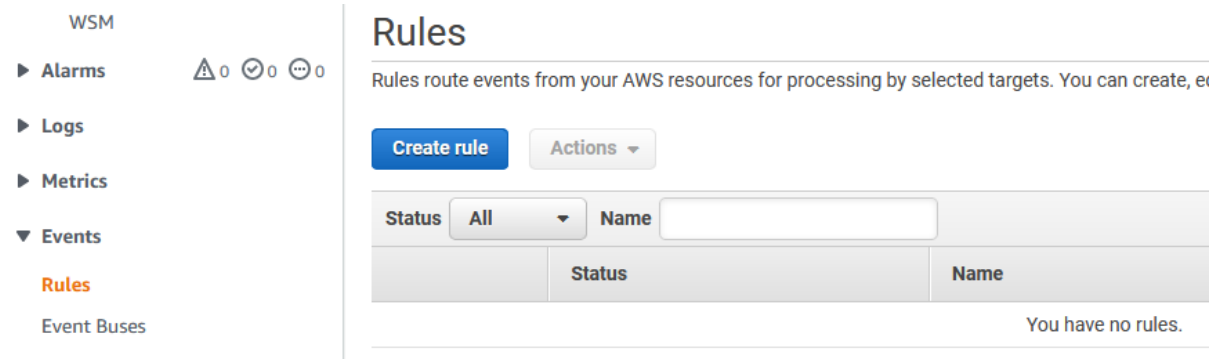
Appendix 2

In order to capture additional information from users and its connections, you need to set up a CloudWatch Log Group that will grant WSM access to information such as latency, client version, public IP, location of IP, etc.

The configuration of CloudWatch is standard and based on the AWS Service, so we will go to the CloudWatch service console in the region we want to configure:

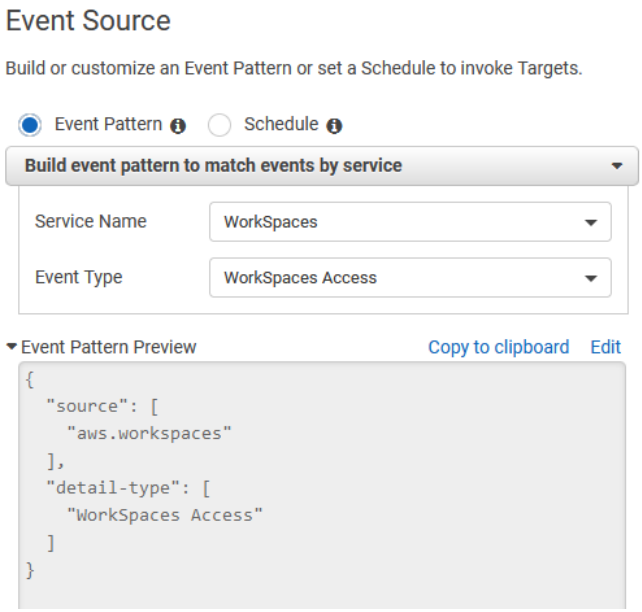


Click on “Events” > “Rules” > “Create rule”



In Step 1, called “Event Source”:

- Choose “Event Pattern”
- Choose “Service Name” as “WorkSpaces”
- Choose “Event Type” as “WorkSpaces Access”

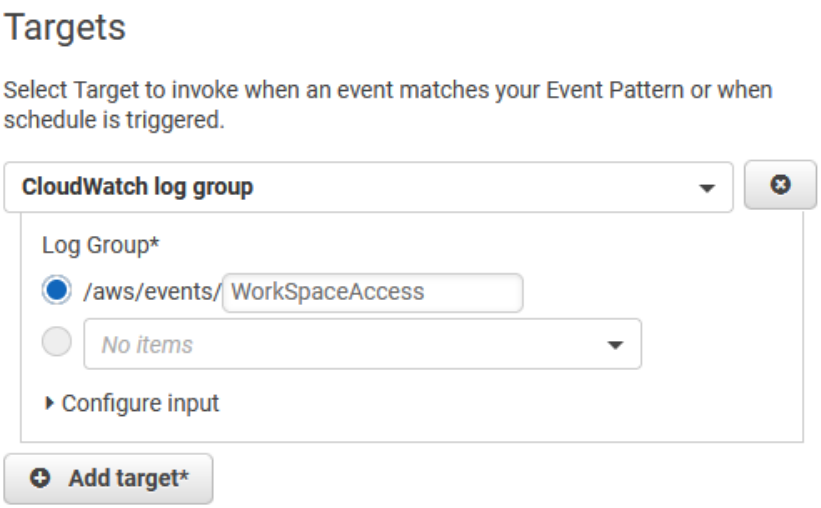


Also, in Step 1 “Targets”:

Click “Add Target”

Choose “CloudWatch log group”

Point the “Log Group” to “**/aws/events/WorkSpaceAccess**”

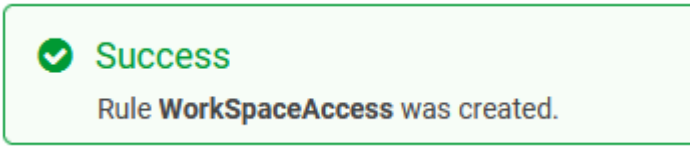


Click “Configure details”

In Step 2, set name to “WorkSpaceAccess” and provide a description

Leave the state as “Enabled” and click “Create rule”

You should receive a success banner like this:



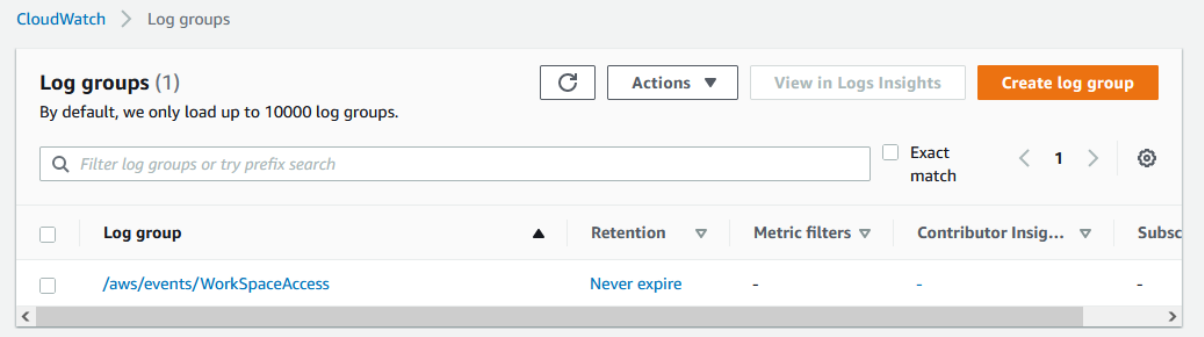
Make sure that the PortalReadCloudwatch policy has the configuration set to:

Service	Access level	Resource
Allow (2 of 290 services) Show remaining 288		
CloudWatch	**Limited**: Read	All resources
CloudWatch Logs	**Full**: Read **Limited**: List	All resources

(JSON format below)

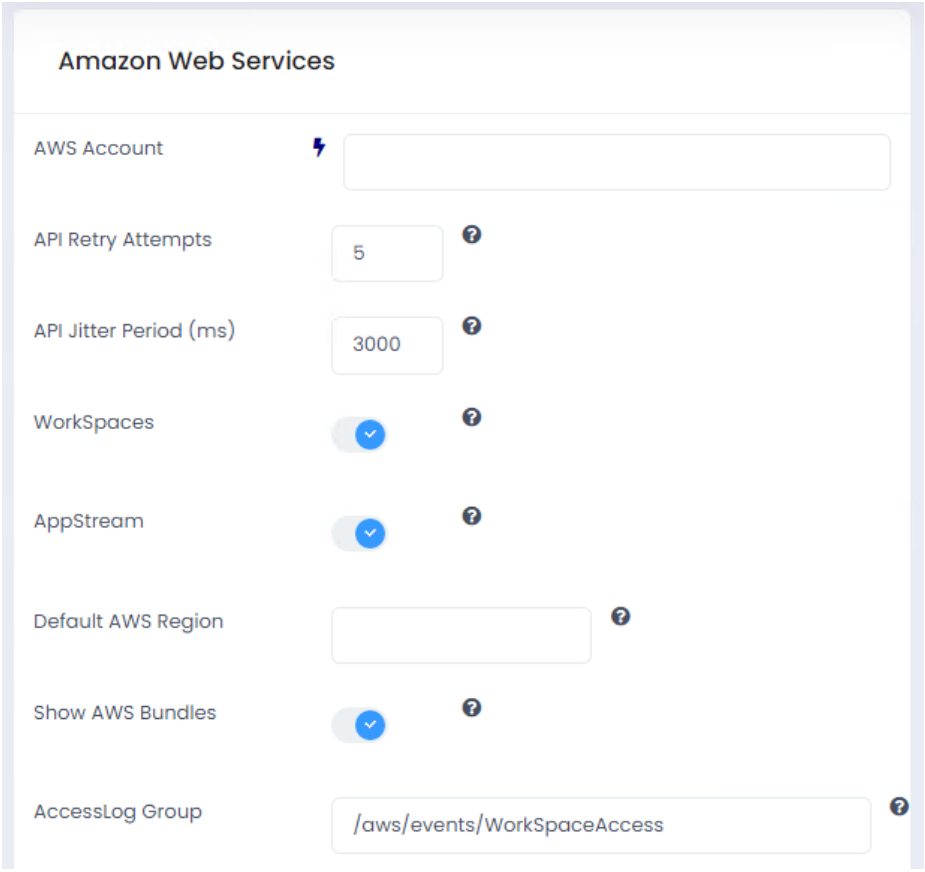
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "logs:ListTagsLogGroup",
            "logs:GetLogRecord",
            "cloudwatch:GetMetricData",
            "logs:DescribeLogStreams",
            "logs:DescribeSubscriptionFilters",
            "logs:StartQuery",
            "logs:DescribeMetricFilters",
            "logs:GetLogDelivery",
            "logs:ListLogDeliveries",
            "cloudwatch:DescribeAlarmHistory",
            "cloudwatch:DescribeAlarmsForMetric",
            "logs:GetLogEvents",
            "logs:FilterLogEvents",
            "cloudwatch:GetMetricWidgetImage",
            "logs:DescribeResourcePolicies",
            "logs:DescribeDestinations",
            "logs:DescribeQueries",
            "cloudwatch:GetDashboard",
            "logs:DescribeLogGroups",
            "logs:StopQuery",
            "logs:TestMetricFilter",
            "cloudwatch:GetMetricStatistics",
            "logs:DescribeExportTasks",
            "logs:GetQueryResults",
            "cloudwatch:DescribeAlarms",
            "logs:GetLogGroupFields"
         ],
         "Resource": "*"
      }
   ]
}
```

Click on “Logs” > “Log groups” > verify the new Log group exist:



Now, in WorkSpaces Manager, in the ‘Config’ section, click on “Options” > “Settings”. Scroll down to the ‘Amazon Web Services’ section and populate the fields “AccessLog Group” with the information:

/aws/events/WorkSpaceAccess

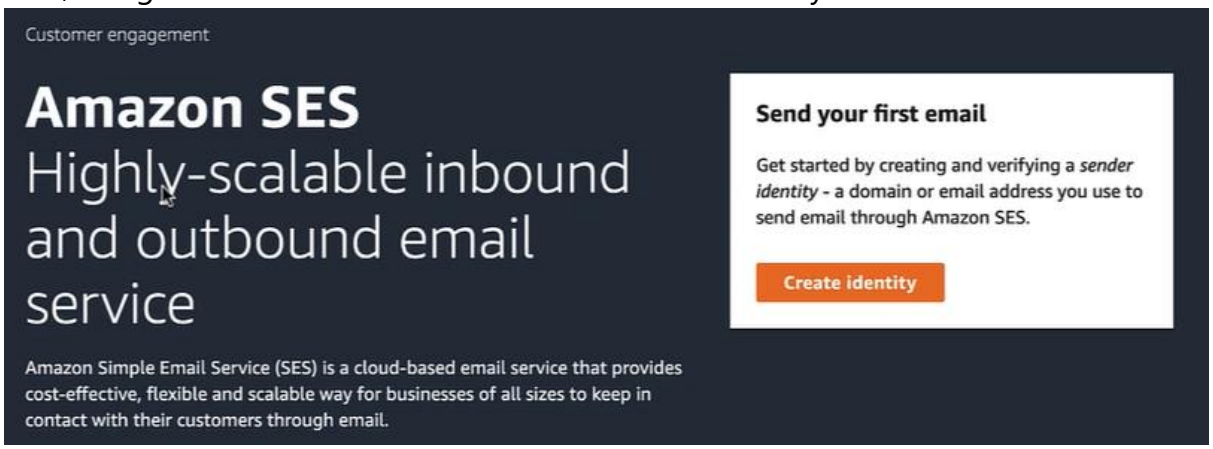


Appendix 3

To configure AWS Simple Email Service (SES) as a SMTP Relay for WorkSpaces Manager, we will need to do the following steps:

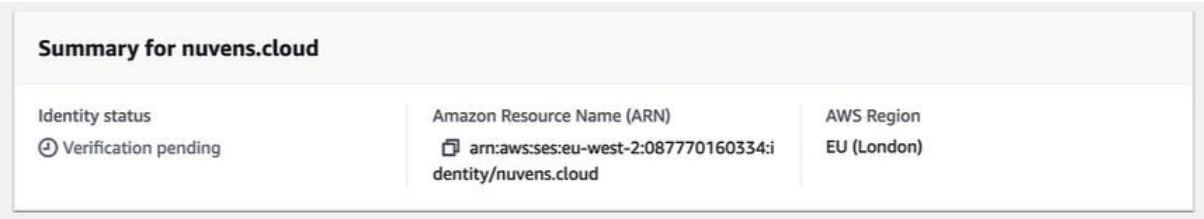
1) DNS Domain to be used as sender
2) Create DNS records as requested
3) Create SMTP Credentials
4) Test emails
5) Configure WSM

First, navigate to Amazon SES and click on "Create Identity":

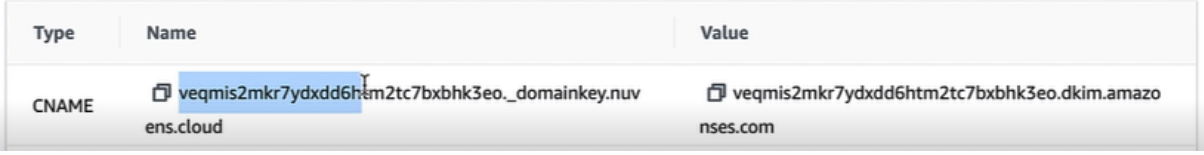


As identity type, we need to choose domain and use the right name of our DNS domain. By default, we will also use DKIM (DomainKeys Identified Mail) to ensure messages are not altered in transit.

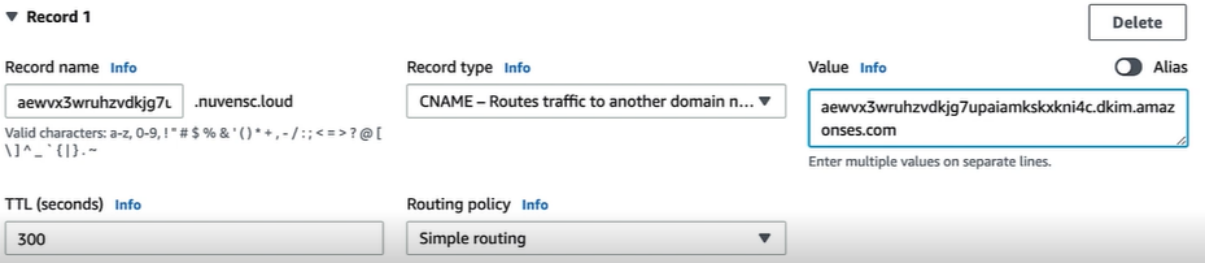
Once requested, the identity will have a status of "Verification pending" and will show the records that need to be created in our DNS for the domain that we are verifying:



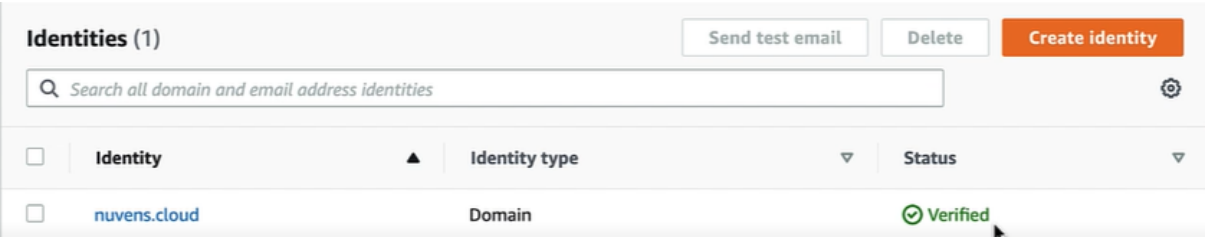
These CNAME records will be different for each request:

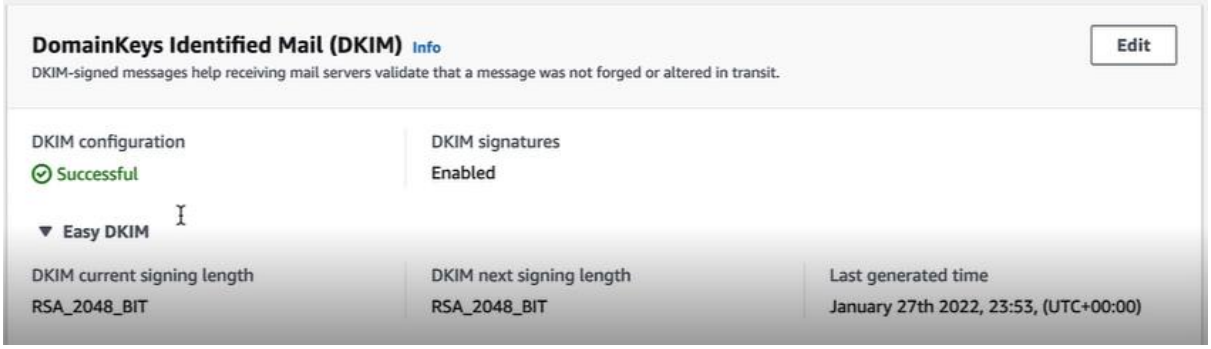


Once the records are created, wait for 10-15 minutes for them to be published and replicated:



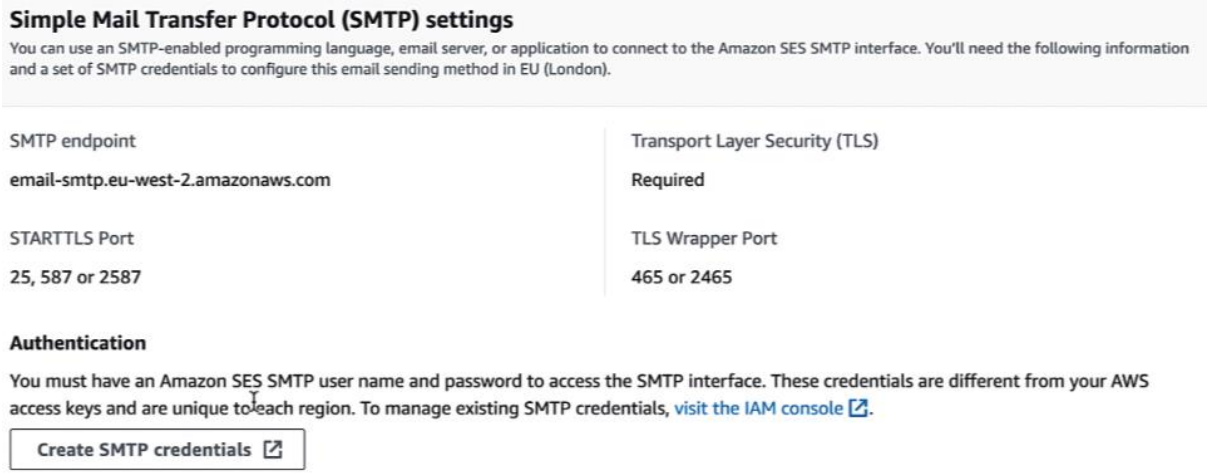
Once the replication happens, AWS will check the status and set the domain as "verified" the endpoint is able to send emails and DKIM successfully registered:



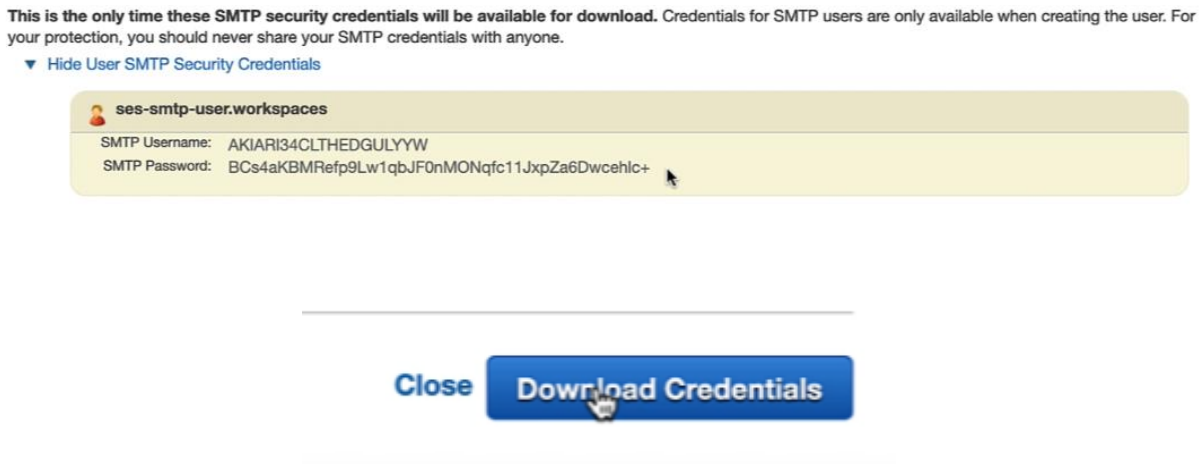


Now, you will generate a credential in AWS IAM to consume the endpoint in the dashboard of the SES service. Select the button to “Create SMTP Credentials”, in which we can also see important information like:

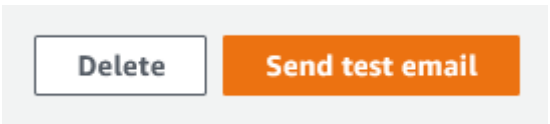
- SMTP Endpoint
- TLS Ports (recommended 587)



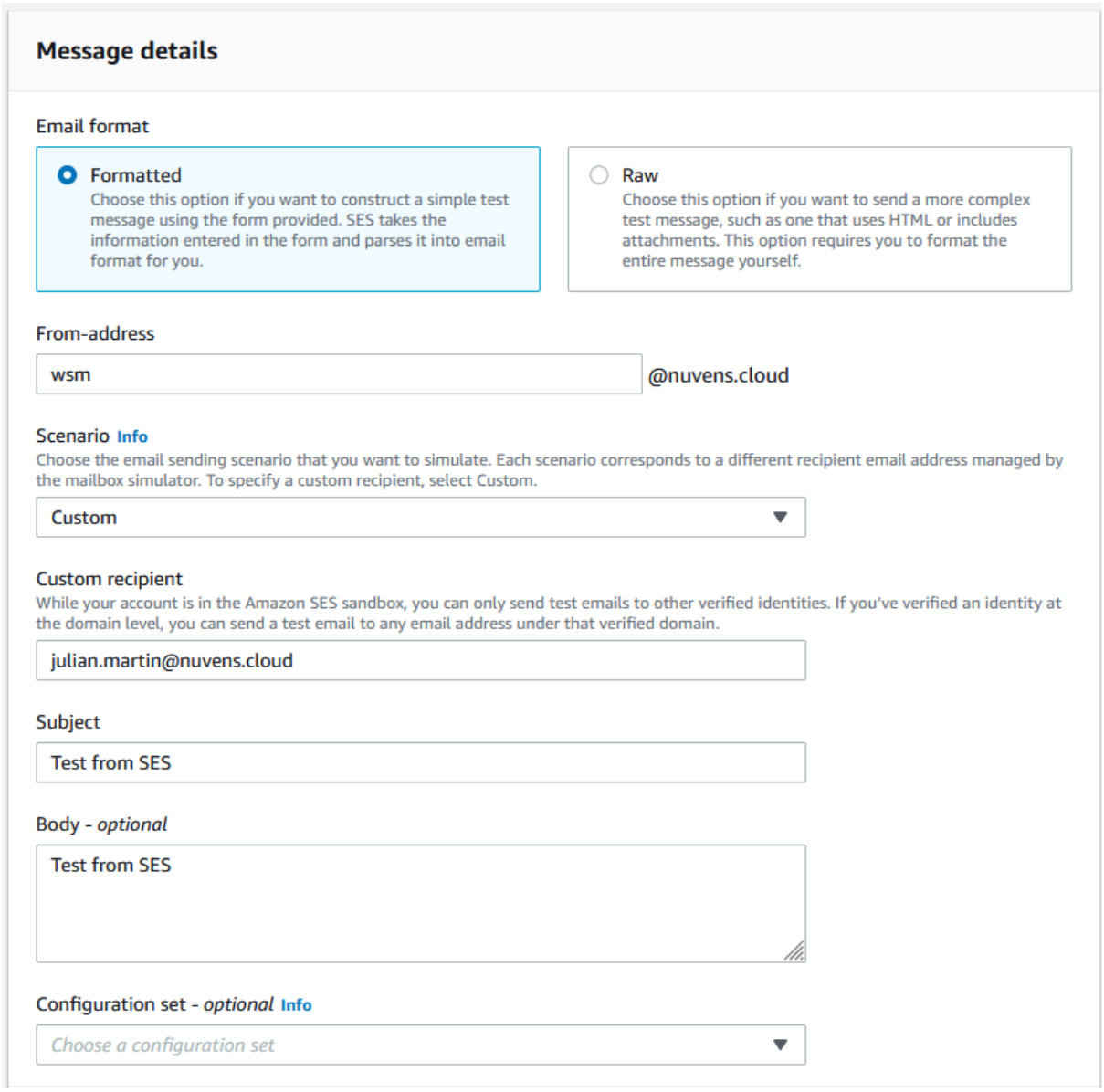
For the credentials, we are creating an IAM User in the AWS account with SES Sending permissions. It is very important to save the SMTP Credentials in a secure location, since these are only displayed once, although they can be downloaded via a CSV file:



You can check to test the email flow works, by clicking on the “Send test email”:



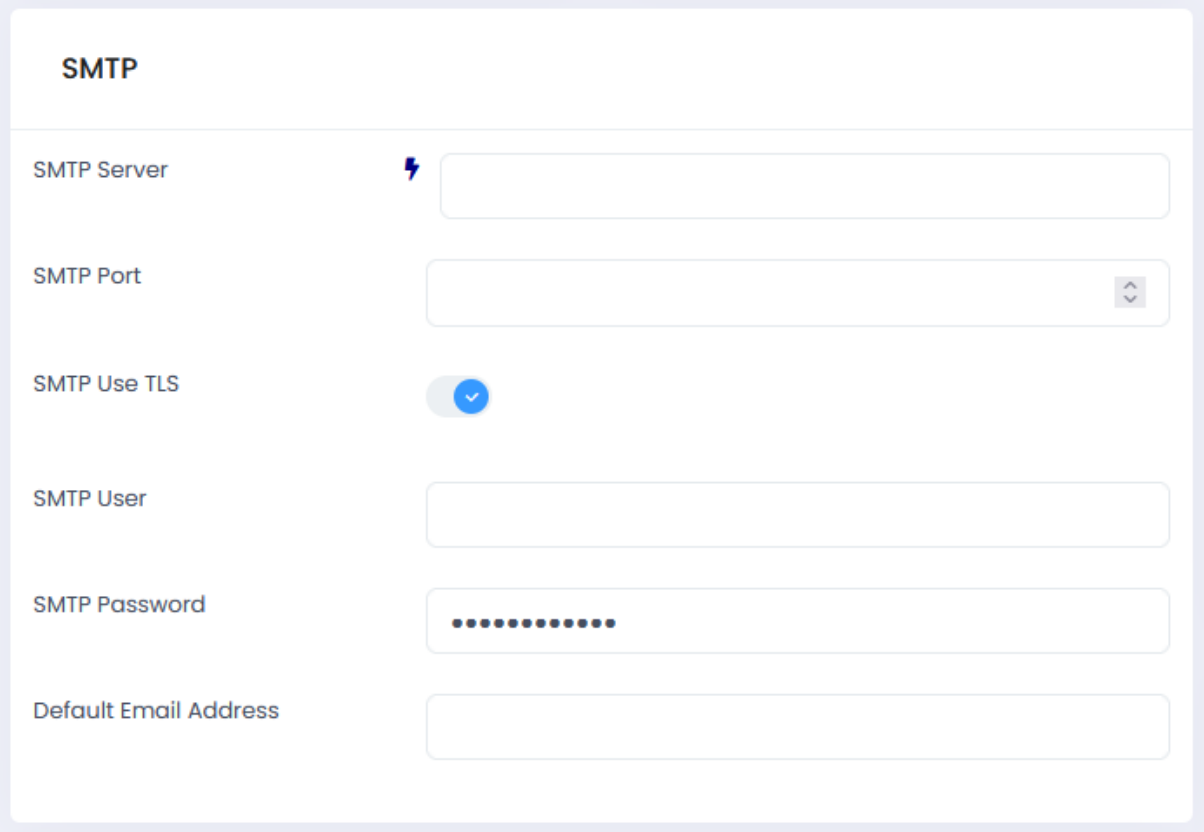
There are several options that you can choose here, so feel free to investigate each one of the boxes:



It is important to mention that when a new SES Identity is created, the domain is set to type "Sandbox", which means that it can exclusively send emails to and from the very same domain that is registered. If we need to send to different DNS domains, then we need to contact AWS Support and ask to convert the domain from "Sandbox" to "Production", as explained here:

https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html

With the information that we have generated, we can populate the SMTP credentials in WorkSpaces Manager:

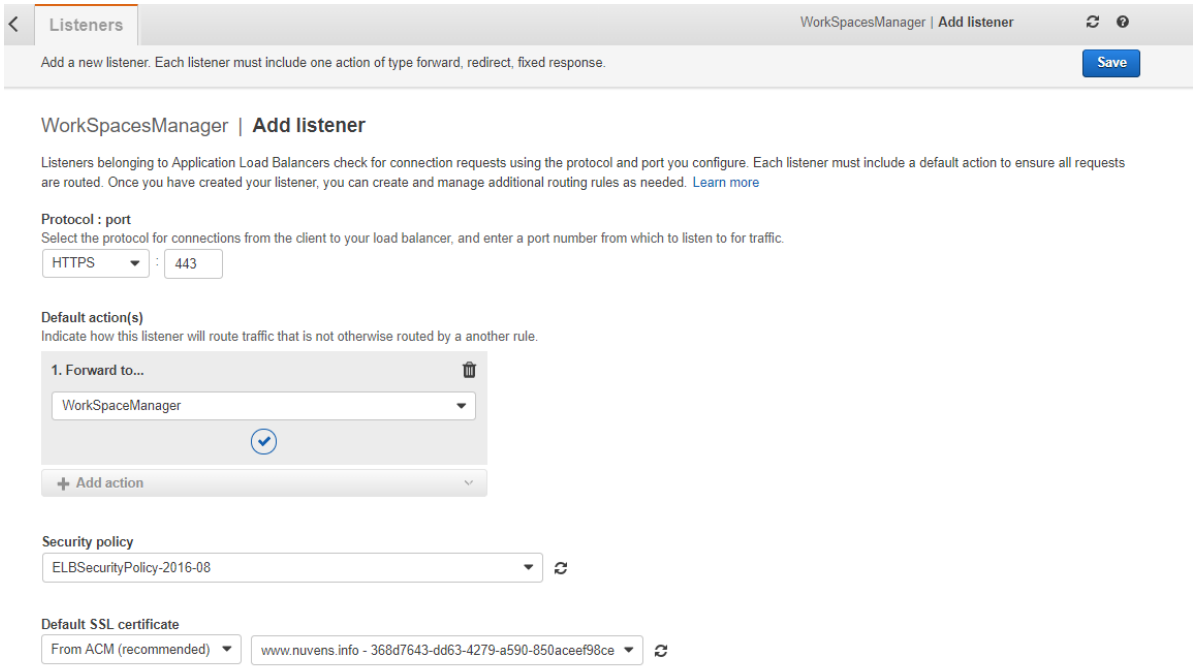


Appendix 4

To configure HTTPS/TLS encryption in front of the WorkSpaces Manager Appliance, you can add a Network Load Balancer as explained below. If you have not created a Network Load Balancer on Section 7.2, refer to it create one NLB.

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'



Appendix 5

To configure WSUS, the default setup has been done previously on the WSM appliance, so we need to follow the wizard to add:

- Network Config
- Languages
- Synchronization Options
- OS and Apps to download
- Auto-Approve