VMware Identity Manager™

3-Node Cluster

Customer Success Team - Tech Notes

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Table of Contents

VMware EUC Customer Success Team

Tech Notes

3 node cluster setup of Identity Manager 2.8

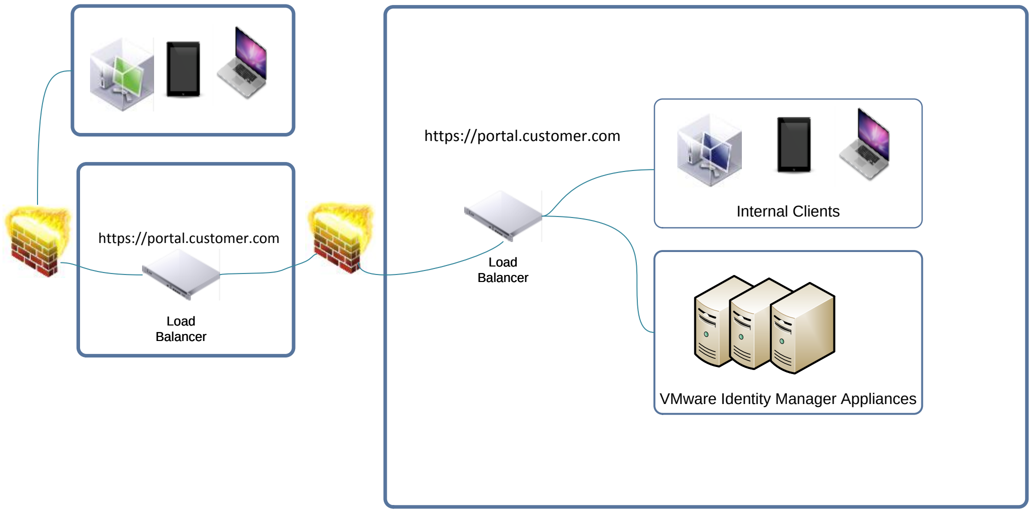
Executive Summary

This guide is meant as a prescriptive guide that includes screenshot of an actual deployment of a 3-node Identity Manager cluster, within the EUC CST Cloud Lab. This guide is also used with our customers to help them understand and deploy a highly-available 3-node cluster of Identity Manager, including configuration steps for SQL Server and F5 LTM. This guide is not meant to replace the Identity Manager installation document, located here.

This guide is focused on a single site deployment. Single Datacenter deployment where all the nodes will be located inside the same DC. If you are looking for a multi-site, deployment for failover and redundancy, you can go here.

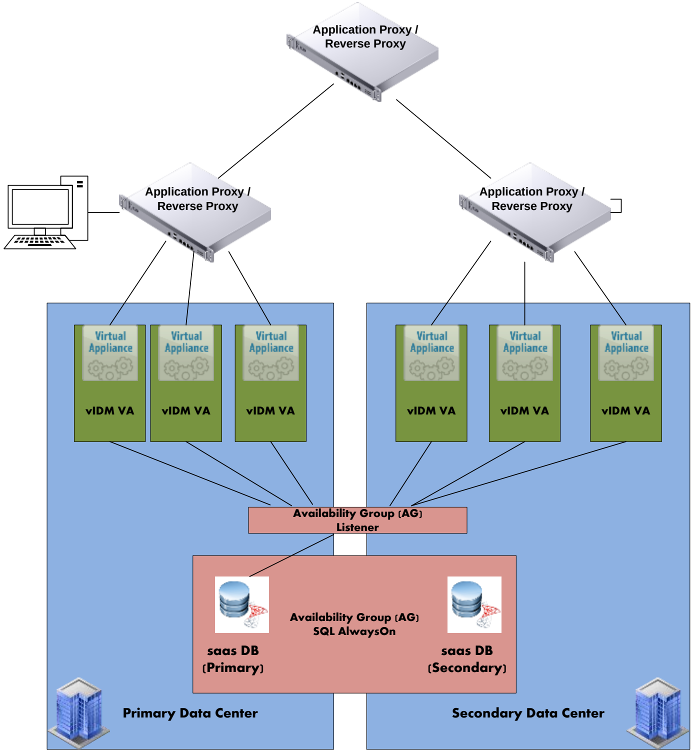
Identity Manager load balancer traffic

When deploying a multi-node Identity Manager environment, you need to have a Load-Balancer in front of all the appliances, to direct traffic coming in from the clients. In this document, we are using F5 Local Traffic Manager as our Load Balancer. The diagram below illustrates how the client devices would connect to the IDM cluster.


https://portal.customer.com
Load
Balancer
https://portal.customer.com
Load
Balancer
Internal Clients
VMware Identity Manager Appliances

Identity Manager High Availability Architecture diagram

This document illustrates the first part of setting up a highly available cluster. From the diagram below, it would be the equivalent of setting up the IDM, SQL and F5 environment in the primary Datacenter. Once the first site is done, you can repeat the process for the second site, modifying your database setup to become a SQL AlwaysOn deployment. We will not detail how to setup SQL AlwaysOn, as this process is well documented, here is one example on how to do it: http://www.careexchange.in/installingconfiguring-sql-2014-always-on-cluster-on-windows-2012-r2-recommended-way/

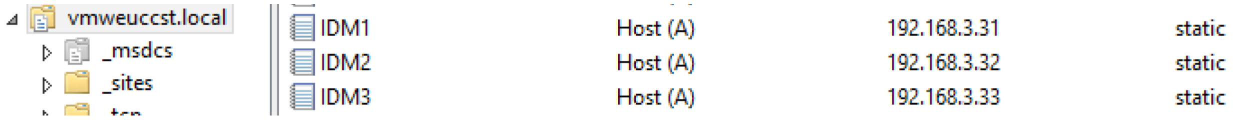

Application Proxy / Reverse Proxy
Application Proxy / Reverse Proxy
Application Proxy / Reverse Proxy
Virtual Appliance
vIDM VA
vIDM VA
vIDM VA
vIDM VA
vIDM VA
vIDM VA
Availability Group (AG) Listener
Availability Group (AG) SQL AlwaysOn
saas DB (Primary)
saas DB (Secondary)
Primary Data Center
Secondary Data Center

Pre-work

All DNS entries should be created ahead of time. In this deployment, we are doing split-DNS configuration. You need to make sure you have the following:

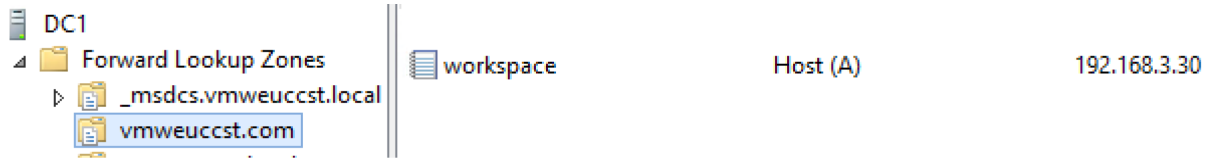
- 3 DNS host entries, forward and reverse record
- 1 DNS host entry for the external FQDN
- Firewall ports configured for proper traffic flow (only default needed: 443, other might be required depending on use case, i.e. Horizon, Citrix, …)

1. setup DNS for the 3 nodes (all internal FQDN)



IDM1	Host (A)	192.168.3.31	static
IDM2	Host (A)	192.168.3.32	static
IDM3	Host (A)	192.168.3.33	static

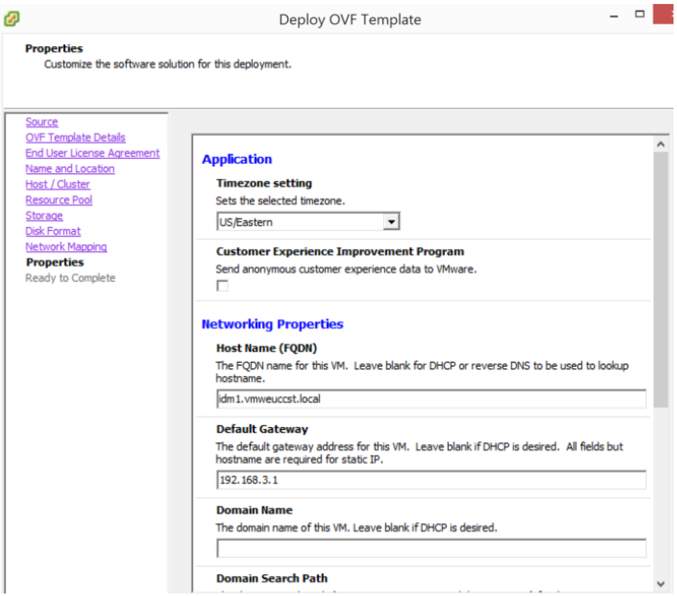
2. setup Internal (Split) DNS for internal VIP FQDN. (change screenshot to be .30)…



workspace	Host (A)	192.168.3.30

3. Setup first node, basically following our normal installation process and using the F5 piece, up to page 16 (https://devcentral.f5.com/Portals/0/userfiles/48273/BIG-IP-Workspace-vIDM-LB-v1_0.pdf)

    a. In IDM deployment, IP screenshot and FQDN screenshot



Properties

Customize the software solution for this deployment.

Application

Timezone setting

Sets the selected timezone.

US/Eastern

Customer Experience Improvement Program

Send anonymous customer experience data to VMware.

□

Networking Properties

Host Name (FQDN)

The FQDN name for this VM. Leave blank for DHCP or reverse DNS to be used to lookup hostname.

idm1.vmweuccst.local

Default Gateway

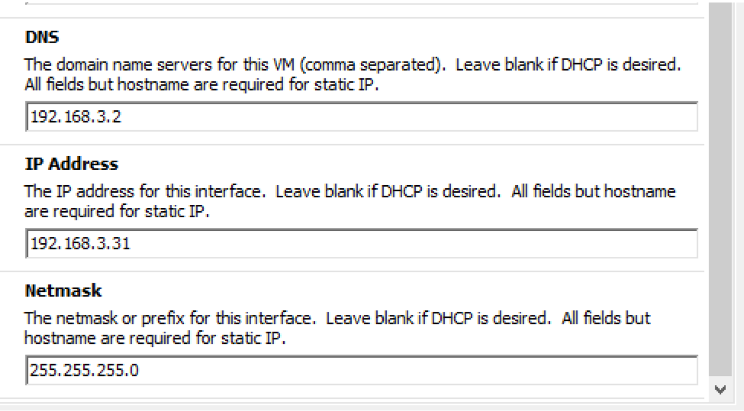
The default gateway address for this VM. Leave blank if DHCP is desired. All fields but hostname are required for static IP.

192.168.3.1

Domain Name

The domain name of this VM. Leave blank if DHCP is desired.

Domain Search Path



DNS

The domain name servers for this VM (comma separated). Leave blank if DHCP is desired. All fields but hostname are required for static IP.

192.168.3.2

IP Address

The IP address for this interface. Leave blank if DHCP is desired. All fields but hostname are required for static IP.

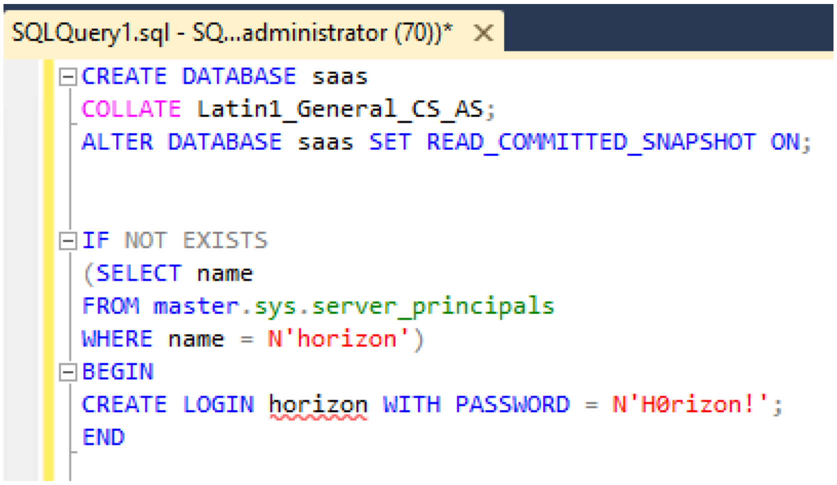
192.168.3.31

Netmask

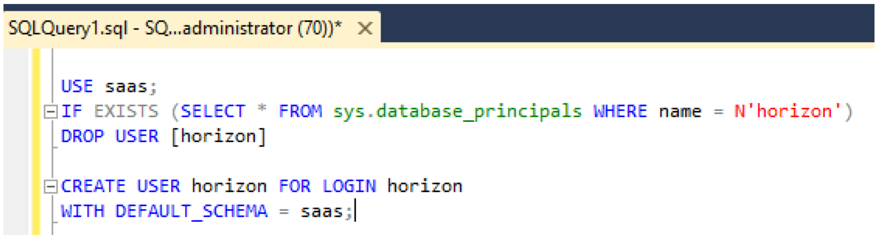
The netmask or prefix for this interface. Leave blank if DHCP is desired. All fields but hostname are required for static IP.

255.255.255.0

b. Before booting appliance, run SQL script to setup DB before node boot



```
CREATE DATABASE saas
COLLATE Latin1_General_CS_AS;
ALTER DATABASE saas SET READ_COMMITTED_SNAPSHOT ON;


IF NOT EXISTS
(SELECT name
FROM master.sys.server_principals
WHERE name = N'horizon')
BEGIN
CREATE LOGIN horizon WITH PASSWORD = N'H0rizon!';
END
```



```
USE saas;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name = N'horizon')
DROP USER [horizon]

CREATE USER horizon FOR LOGIN horizon
WITH DEFAULT_SCHEMA = saas;
```

SQL Script

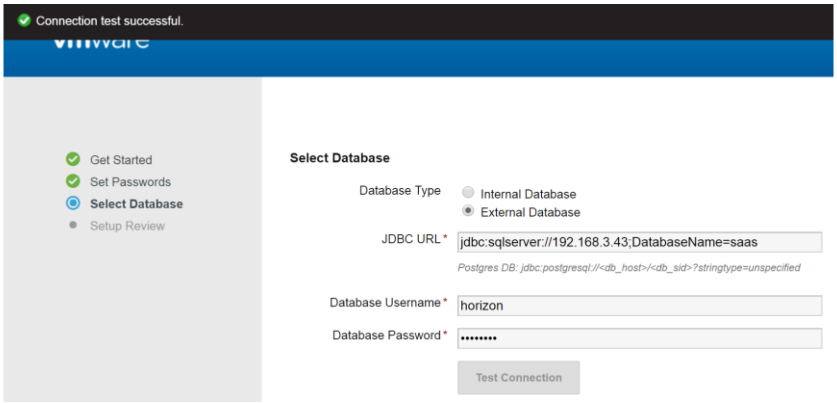
It’s important to note that the database name was chosen as an example. You do not specifically have to use “saas” for the DB name, it can be a different name, just make sure you write it down, as you will need it when you are doing the initial setup of the SQL JDBC in the Identity Manager on-boarding web-based setup. Same goes for the actual user. It does not have to be horizon but again here, make sure you have a user that has DB_Owner permissions to that database.

Script shown above:

```
create database saas
collate Latin1_General_CS_AS;
Alter database saas set READ_COMMITTED_SNAPSHOT ON;
go

begin
CREATE login horizon with password = N'H0rizon!';
end
go

USE saas;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name = N'horizon')
DROP USER [horizon]
GO

create user horizon for login horizon
with default_schema = saas;
go

create schema saas authorization horizon
grant all on database::saas to horizon;
go
```

c. First Identity Manager Appliance boot, Making sure that SQL database is setup and ready to receive node connection (JDBC url)

i.



Connection test successful.

Select Database

Database Type ○ Internal Database ● External Database

JDBC URL* jdbc:sqlserver://192.168.3.43;DatabaseName=saas

Postgres DB: jdbc:postgresql://<db_host>/<db_sid>?stringtype=unspecified

Database Username* horizon

Database Password* ••••••••

In our example, we are using SQL, but keep in mind that Oracle and PostGres are also supported.

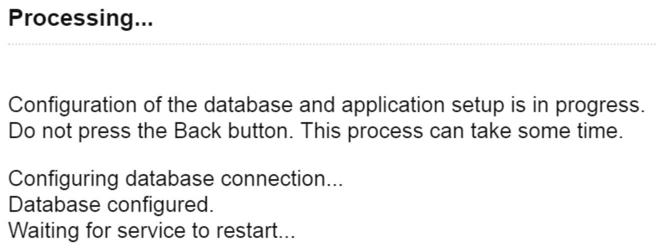
<u>PostgreSQL jdbc</u>: postgresql://IP_address/saas?stringtype=unspecified

<u>Microsoft SQL jdbc</u>: sqlserver://IP_address;DatabaseName=saas

<u>Oracle jdbc</u>: oracle:thin:@//IP_address:port/sid

Once the correct information is entered, you click on Continue, you will see the following message appear, mentioning that it's changing the configuration of the Database and completing the setup.

ii.



Processing...

Configuration of the database and application setup is in progress.
Do not press the Back button. This process can take some time.

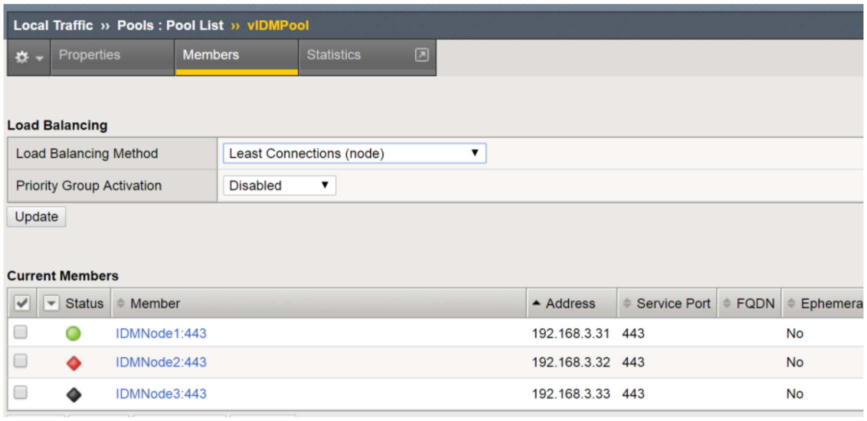
Configuring database connection...
Database configured.
Waiting for service to restart...

4. setup External DNS for VIP FQDN

5. modify firewall for traffic to External VIP (port 443 only.)

** Remember that when going to the management port (8443), you always point to the individual appliance. (config page)

C) Change the FQDN to VIP of environment (after validating that LTM is seeing the node and coming up green in pool)



Load Balancing

Load Balancing Method	Least Connections (node) ▾
Priority Group Activation	Disabled ▾

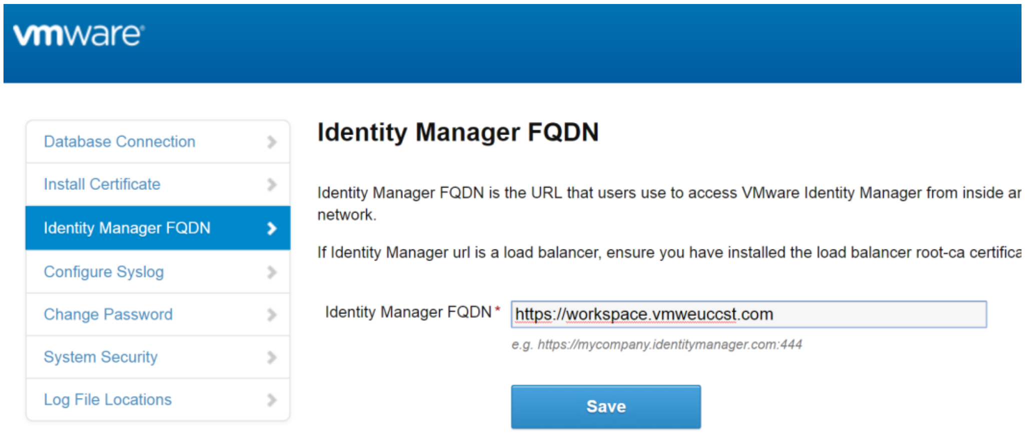
Update

Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemera
□	●	IDMNode1:443	192.168.3.31	443		No
□	♦	IDMNode2:443	192.168.3.32	443		No
□	◆	IDMNode3:443	192.168.3.33	443		No

Only Node 1 will show up green since only 1 node setup so far. The pool config is setup ahead of time on F5 side.

6. Changed FQDN



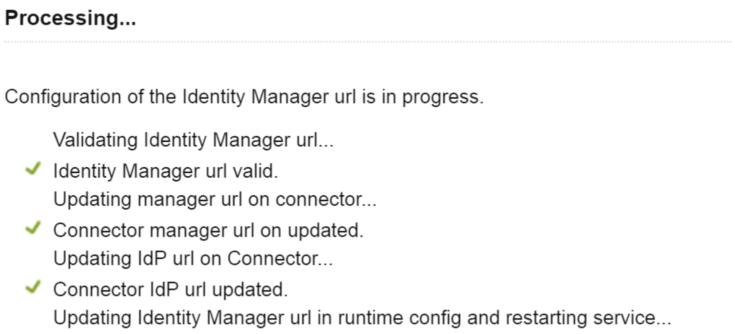
Identity Manager FQDN

Identity Manager FQDN is the URL that users use to access VMware Identity Manager from inside ar network.

If Identity Manager url is a load balancer, ensure you have installed the load balancer root-ca certifica

Identity Manager FQDN * https://workspace.vmweuccst.com

e.g. https://mycompany.identitymanager.com:444



Processing...

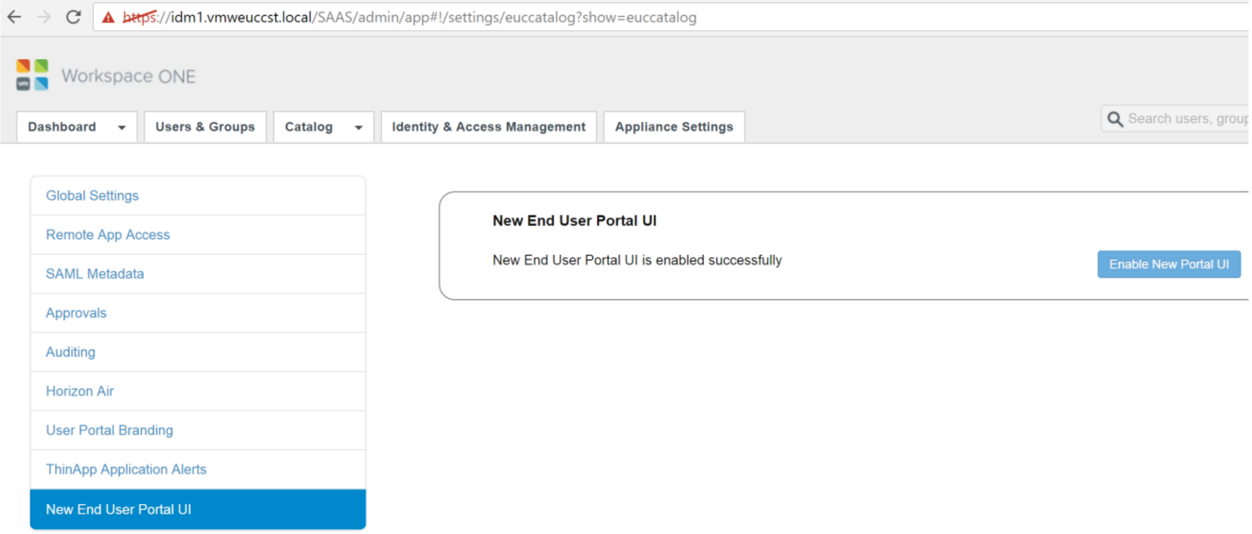
Configuration of the Identity Manager url is in progress.

Validating Identity Manager url...
✓ Identity Manager url valid.
Updating manager url on connector...
✓ Connector manager url on updated.
Updating IdP url on Connector...
✓ Connector IdP url updated.
Updating Identity Manager url in runtime config and restarting service...

Troubleshooting FQDN change

Good post from Peter Bjork on troubleshooting FQDN change: (http://blogs.vmware.com/horizontech/2014/10/troubleshoot-workspace-portal-setup-issues-changing-fqdn.html)

One known issue is that the New Portal UI is disabled when the FQDN of IDM is changed. Make sure to leave the IDM1 web page up, need to re-enable the new UI portal before starting to use the FQDN


~~https~~://idm1.vmweuccst.local/SAAS/admin/app#!/settings/euccatalog?show=euccatalog

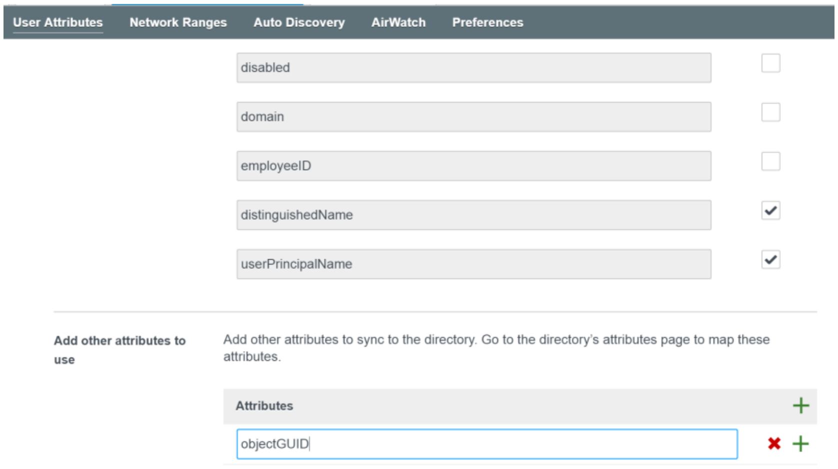
New End User Portal UI

New End User Portal UI is enabled successfully

Once you have successfully changed the FQDN, close down you browser (clearing cache and cookies), then open up your browser and login to the FQDN of the IDM cluster (in our example: https://workspace.myeuc.net)

Good practice is to change the user required Attributes before doing anything else. If you don't do this and you need to add a required attributes after, you will need to remove the configuration and start over.

- Under Identity & Access Management, click on Setup (right side of screen), then choose: Change User Attributes (add UPN, Distinguishedname, objectGUID)



disabled	□
domain	□
employeeID	□
distinguishedName	☑
userPrincipalName	☑

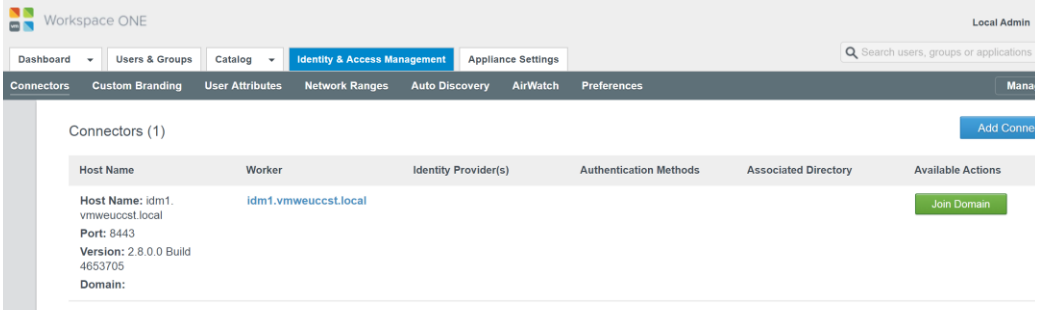
Add other attributes to use

Add other attributes to sync to the directory. Go to the directory's attributes page to map these attributes.

Attributes

objectGUID

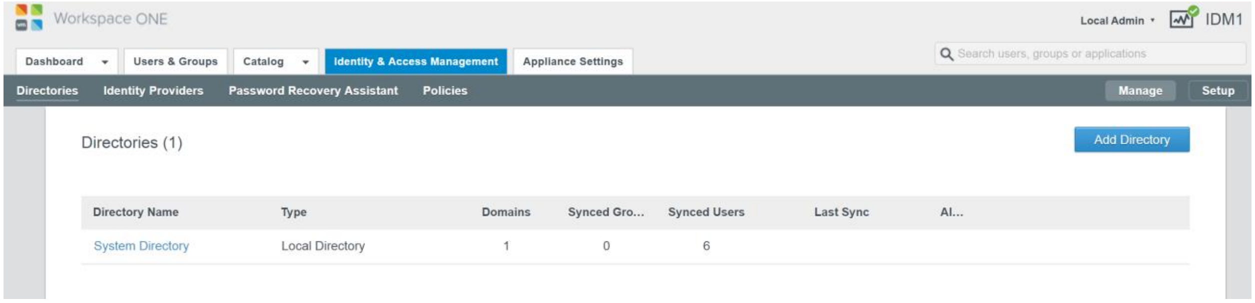
Next click on Connectors, you will see your first node is not domain joined yet. Click on Join domain



Connectors (1)

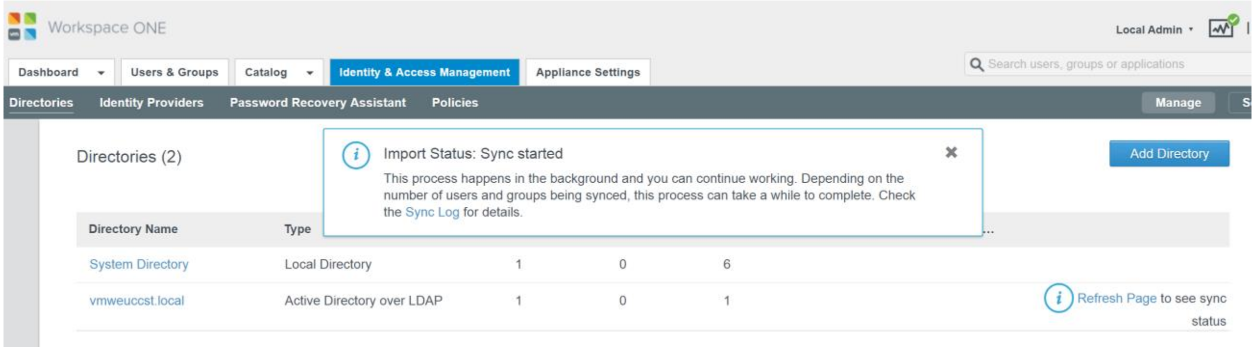
Host Name	Worker	Identity Provider(s)	Authentication Methods	Associated Directory	Available Actions
Host Name: idm1.vmweuccst.local **Port:** 8443 **Version:** 2.8.0.0 Build 4653705 **Domain:**	idm1.vmweuccst.local				Join Domain

Next, you go back in the Manage part and choose the Directories tab. Right side of the screen, you'll see a Add Directory button.



Directories (1)

Directory Name	Type	Domains	Synced Gro...	Synced Users	Last Sync	Al...
System Directory	Local Directory	1	0	6		



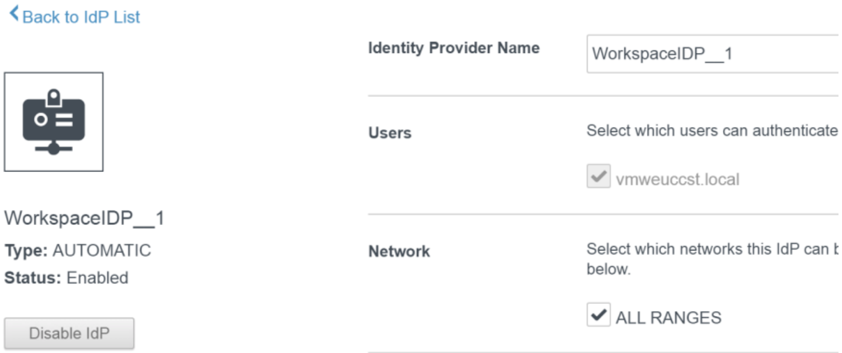
Directories (2)

Import Status: Sync started

This process happens in the background and you can continue working. Depending on the number of users and groups being synced, this process can take a while to complete. Check the Sync Log for details.

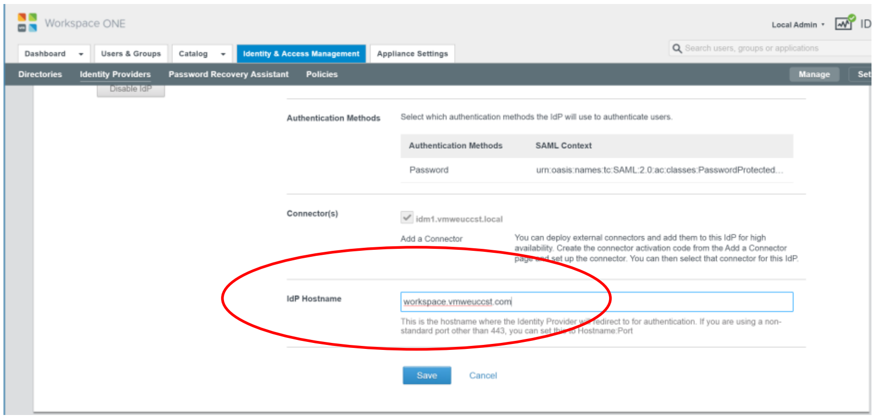
Directory Name	Type				
System Directory	Local Directory	1	0	6	
vmweuccst.local	Active Directory over LDAP	1	0	1	Refresh Page to see sync status

Validate that the IDP hostname is pointing to the VIP FQDN. You might see here the IdP hostname as being the first node. Just change it to the FQDN of the external facing name (the one that is setup with the F5 Load-Balancer).



WorkspaceIDP__1
Type: AUTOMATIC
Status: Enabled

Identity Provider Name	WorkspaceIDP__1
Users	Select which users can authenticate ☑ vmweuccst.local
Network	Select which networks this IdP can b below. ☑ ALL RANGES



Authentication Methods: Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	SAML Context
Password	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected...

Connector(s): ☑ idm1.vmweuccst.local

Add a Connector: You can deploy external connectors and add them to this IdP for high availability. Create the connector activation code from the Add a Connector page and set up the connector. You can then select that connector for this IdP.

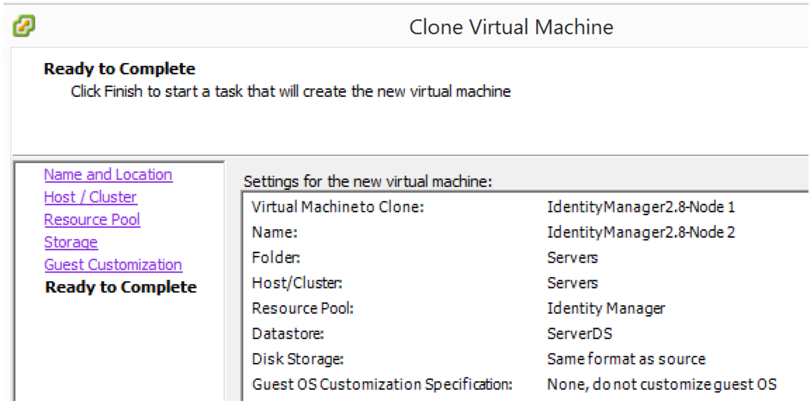
IdP Hostname: workspace.vmweuccst.com

This is the hostname where the Identity Provider will redirect to for authentication. If you are using a non-standard port other than 443, you can set this to Hostname:Port

Image above shows IdP hostname validation.

Creating IDM Node 2 & 3

Shutdown node 1 and clone it.



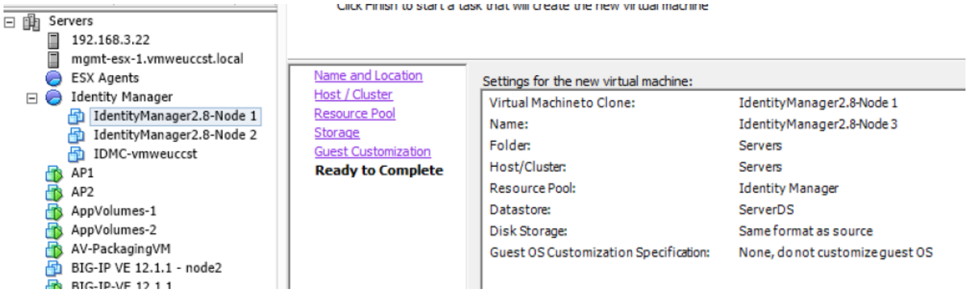
Ready to Complete

Click Finish to start a task that will create the new virtual machine

Settings for the new virtual machine:

Virtual Machineto Clone:	IdentityManager2.8-Node 1
Name:	IdentityManager2.8-Node 2
Folder:	Servers
Host/Cluster:	Servers
Resource Pool:	Identity Manager
Datastore:	ServerDS
Disk Storage:	Same format as source
Guest OS Customization Specification:	None, do not customize guest OS

Clone Node 3 right after node 2 is finished, before booting anything back up.

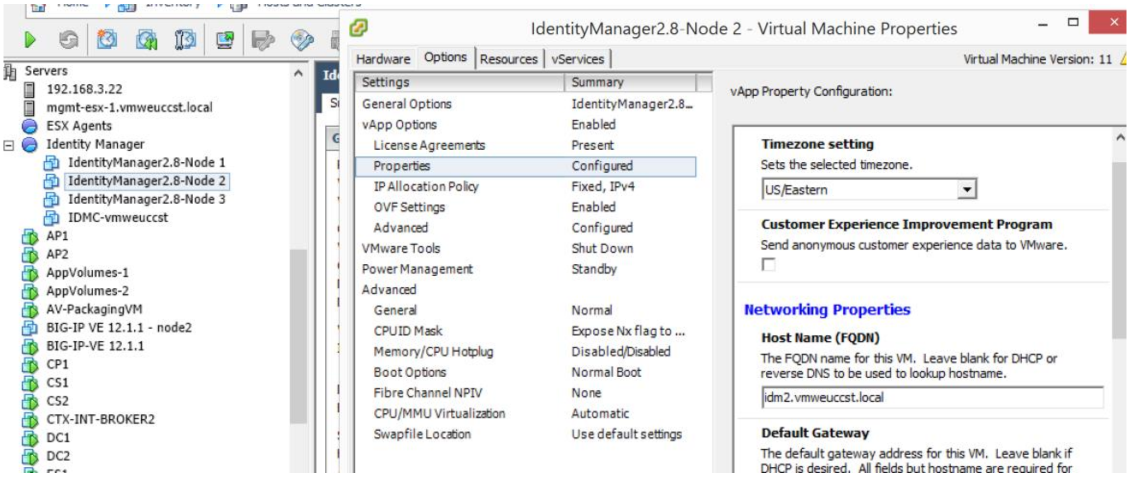


Click Finish to start a task that will create the new virtual machine

Settings for the new virtual machine:

Virtual Machineto Clone:	IdentityManager2.8-Node 1
Name:	IdentityManager2.8-Node 3
Folder:	Servers
Host/Cluster:	Servers
Resource Pool:	Identity Manager
Datastore:	ServerDS
Disk Storage:	Same format as source
Guest OS Customization Specification:	None, do not customize guest OS

9. Before booting 2nd node, **make sure to go in settings**, change the IP and FQDN of the 2nd node



Settings	Summary
General Options	IdentityManager2.8...
vApp Options	Enabled
License Agreements	Present
Properties	Configured
IP Allocation Policy	Fixed, IPv4
OVF Settings	Enabled
Advanced	Configured
VMware Tools	Shut Down
Power Management	Standby
Advanced	
General	Normal
CPUID Mask	Expose Nx flag to ...
Memory/CPU Hotplug	Disabled/Disabled
Boot Options	Normal Boot
Fibre Channel NPIV	None
CPU/MMU Virtualization	Automatic
Swapfile Location	Use default settings

vApp Property Configuration:

Timezone setting
Sets the selected timezone.
US/Eastern

Customer Experience Improvement Program
Send anonymous customer experience data to VMware.
□

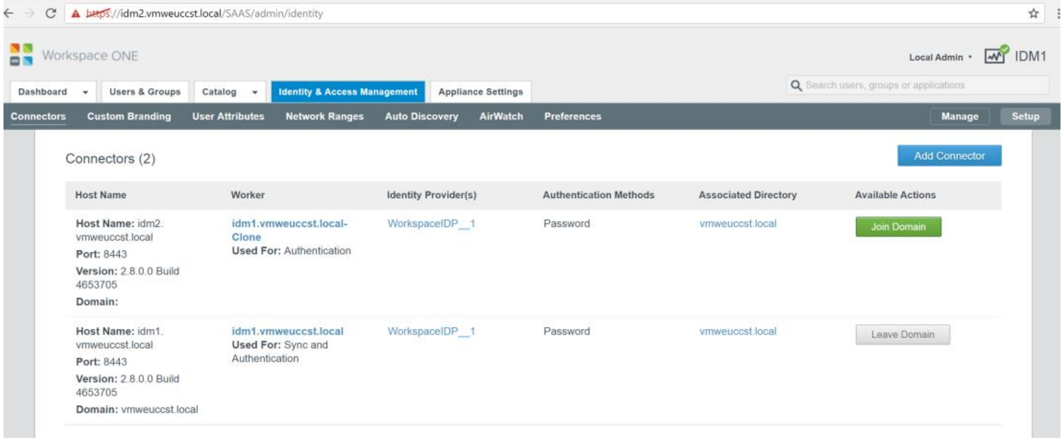
Networking Properties

Host Name (FQDN)
The FQDN name for this VM. Leave blank for DHCP or reverse DNS to be used to lookup hostname.
idm2.vmweuccst.local

Default Gateway
The default gateway address for this VM. Leave blank if DHCP is desired. All fields but hostname are required for

10. Boot 2nd node, once completely booted, join node to domain, from IDM admin Console. Important to wait a while before trying to make any changes. It took close to 10 minutes in our lab for things to settle (i.e. for status to show up green). If, after waiting a long time, status does not come up green, you should shutdown both appliance, then boot them back up. When you do this, make sure to wait 2-30 seconds between booting node1 and node2.

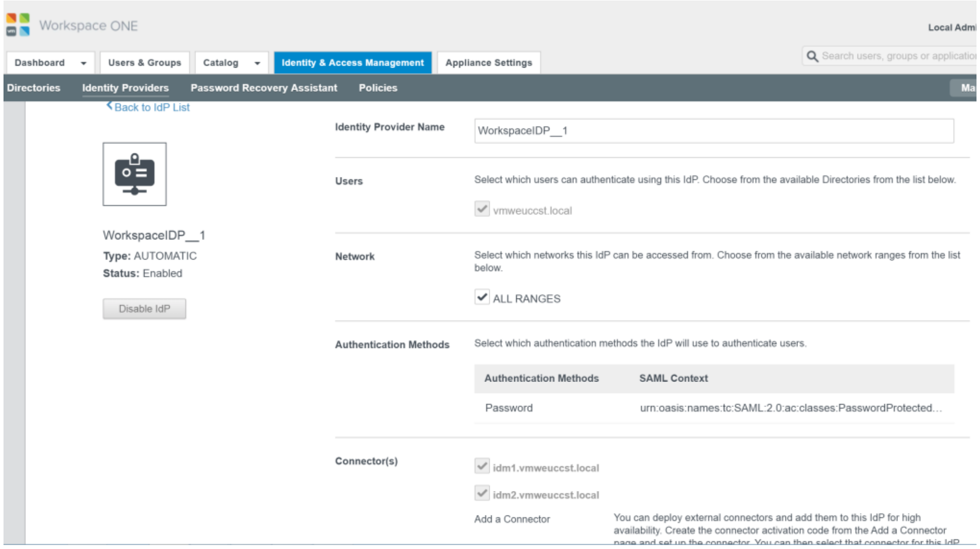
Successful boot, now, need Node2 to join domain.



Connectors (2)

Host Name	Worker	Identity Provider(s)	Authentication Methods	Associated Directory	Available Actions
Host Name: idm2.vmweuccst.local **Port:** 8443 **Version:** 2.8.0.0 Build 4653705 **Domain:**	idm1.vmweuccst.local-Clone **Used For:** Authentication	WorkspaceIDP__1	Password	vmweuccst.local	Join Domain
Host Name: idm1.vmweuccst.local **Port:** 8443 **Version:** 2.8.0.0 Build 4653705 **Domain:** vmweuccst.local	idm1.vmweuccst.local **Used For:** Sync and Authentication	WorkspaceIDP__1	Password	vmweuccst.local	Leave Domain

After domain join, check the IDP to make sure it kept the FQDN hostname. (Should not have changed but just a precaution)



WorkspaceIDP__1
Type: AUTOMATIC
Status: Enabled

Identity Provider Name: WorkspaceIDP__1

Users: Select which users can authenticate using this IdP. Choose from the available Directories from the list below.

☑ vmweuccst.local

Network: Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below.

☑ ALL RANGES

Authentication Methods: Select which authentication methods the IdP will use to authenticate users.

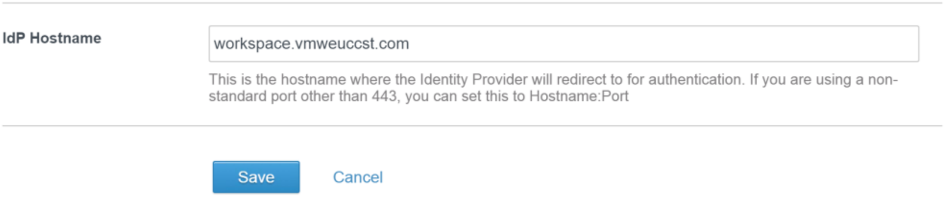
Authentication Methods	SAML Context
Password	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtected...

Connector(s):

☑ idm1.vmweuccst.local

☑ idm2.vmweuccst.local

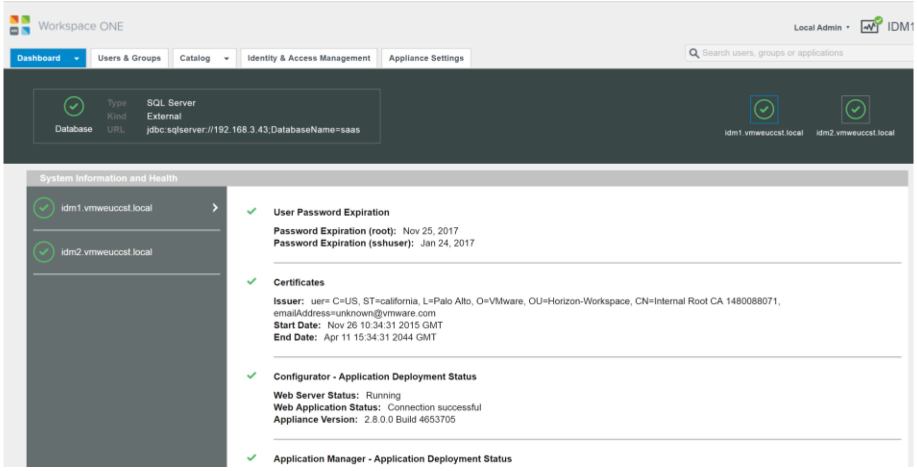
Add a Connector: You can deploy external connectors and add them to this IdP for high availability. Create the connector activation code from the Add a Connector page and set up the connector. You can then select that connector for this IdP.



IdP Hostname: workspace.vmweuccst.com

This is the hostname where the Identity Provider will redirect to for authentication. If you are using a non-standard port other than 443, you can set this to Hostname:Port

Click on right-side dashboard icon will give you something like this:



Database
Type: SQL Server
Kind: External
URL: jdbc:sqlserver://192.168.3.43;DatabaseName=saas

System Information and Health

✓ idm1.vmweuccst.local

✓ idm2.vmweuccst.local

✓ **User Password Expiration**

Password Expiration (root): Nov 25, 2017
Password Expiration (sshuser): Jan 24, 2017

✓ **Certificates**

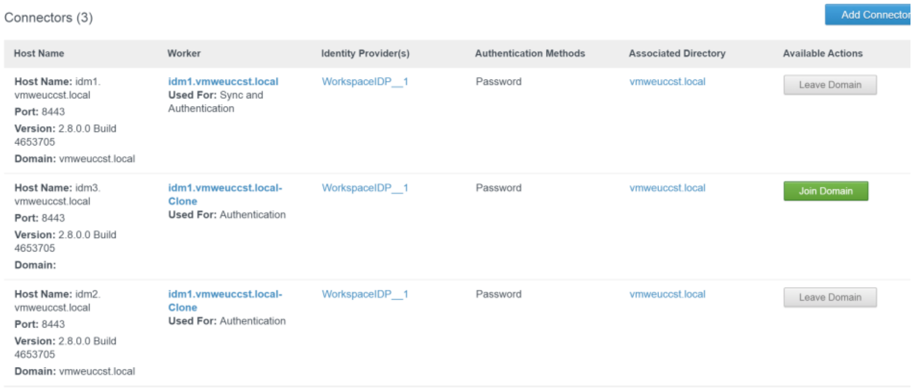
Issuer: uer= C=US, ST=california, L=Palo Alto, O=VMware, OU=Horizon-Workspace, CN=Internal Root CA 1480088071, emailAddress=unknown@vmware.com
Start Date: Nov 26 10:34:31 2015 GMT
End Date: Apr 11 15:34:31 2044 GMT

✓ **Configurator - Application Deployment Status**

Web Server Status: Running
Web Application Status: Connection successful
Appliance Version: 2.8.0.0 Build 4653705

✓ **Application Manager - Application Deployment Status**

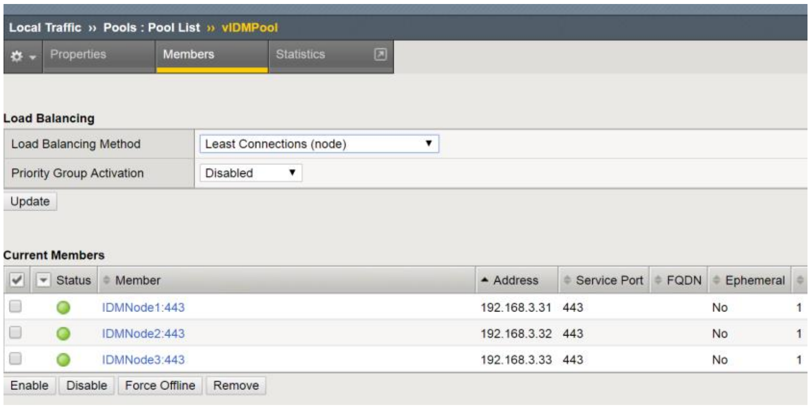
Boot Node3 and after a similar wait period as before, join it to the domain



Connectors (3)

Host Name	Worker	Identity Provider(s)	Authentication Methods	Associated Directory	Available Actions
Host Name: idm1.vmweuccst.local **Port:** 8443 **Version:** 2.8.0.0 Build 4653705 **Domain:** vmweuccst.local	**idm1.vmweuccst.local** **Used For:** Sync and Authentication	WorkspaceIDP__1	Password	vmweuccst.local	Leave Domain
Host Name: idm3.vmweuccst.local **Port:** 8443 **Version:** 2.8.0.0 Build 4653705 **Domain:**	**idm1.vmweuccst.local-Clone** **Used For:** Authentication	WorkspaceIDP__1	Password	vmweuccst.local	Join Domain
Host Name: idm2.vmweuccst.local **Port:** 8443 **Version:** 2.8.0.0 Build 4653705 **Domain:** vmweuccst.local	**idm1.vmweuccst.local-Clone** **Used For:** Authentication	WorkspaceIDP__1	Password	vmweuccst.local	Leave Domain

Check on LTM for status of the 3 nodes



Local Traffic » Pools : Pool List » vIDMPool

Load Balancing

Load Balancing Method	Least Connections (node)
Priority Group Activation	Disabled

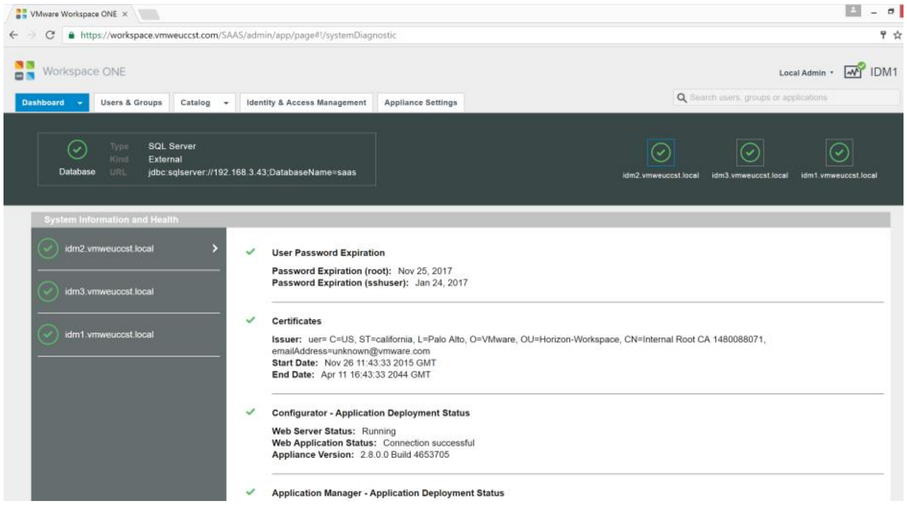
Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	
□	●	IDMNode1:443	192.168.3.31	443		No	1
□	●	IDMNode2:443	192.168.3.32	443		No	1
□	●	IDMNode3:443	192.168.3.33	443		No	1

Green dashboard

In our deployment, to obtain a green checkmark on node 2 & 3, we had to do a reboot of the nodes, once the setup was complete.

The way we have confirmed that works constistently is to reboot node 1, wait 30-45 seconds, then boot node 2&3



Database
Type SQL Server
Kind External
URL jdbc:sqlserver://192.168.3.43;DatabaseName=saas

✓ **User Password Expiration**

Password Expiration (root): Nov 25, 2017
Password Expiration (sshuser): Jan 24, 2017

✓ **Certificates**

Issuer: uer= C=US, ST=california, L=Palo Alto, O=VMware, OU=Horizon-Workspace, CN=Internal Root CA 1480088071, emailAddress=unknown@vmware.com
Start Date: Nov 26 11:43:33 2015 GMT
End Date: Apr 11 16:43:33 2044 GMT

✓ **Configurator - Application Deployment Status**

Web Server Status: Running
Web Application Status: Connection successful
Appliance Version: 2.8.0.0 Build 4653705

✓ **Application Manager - Application Deployment Status**

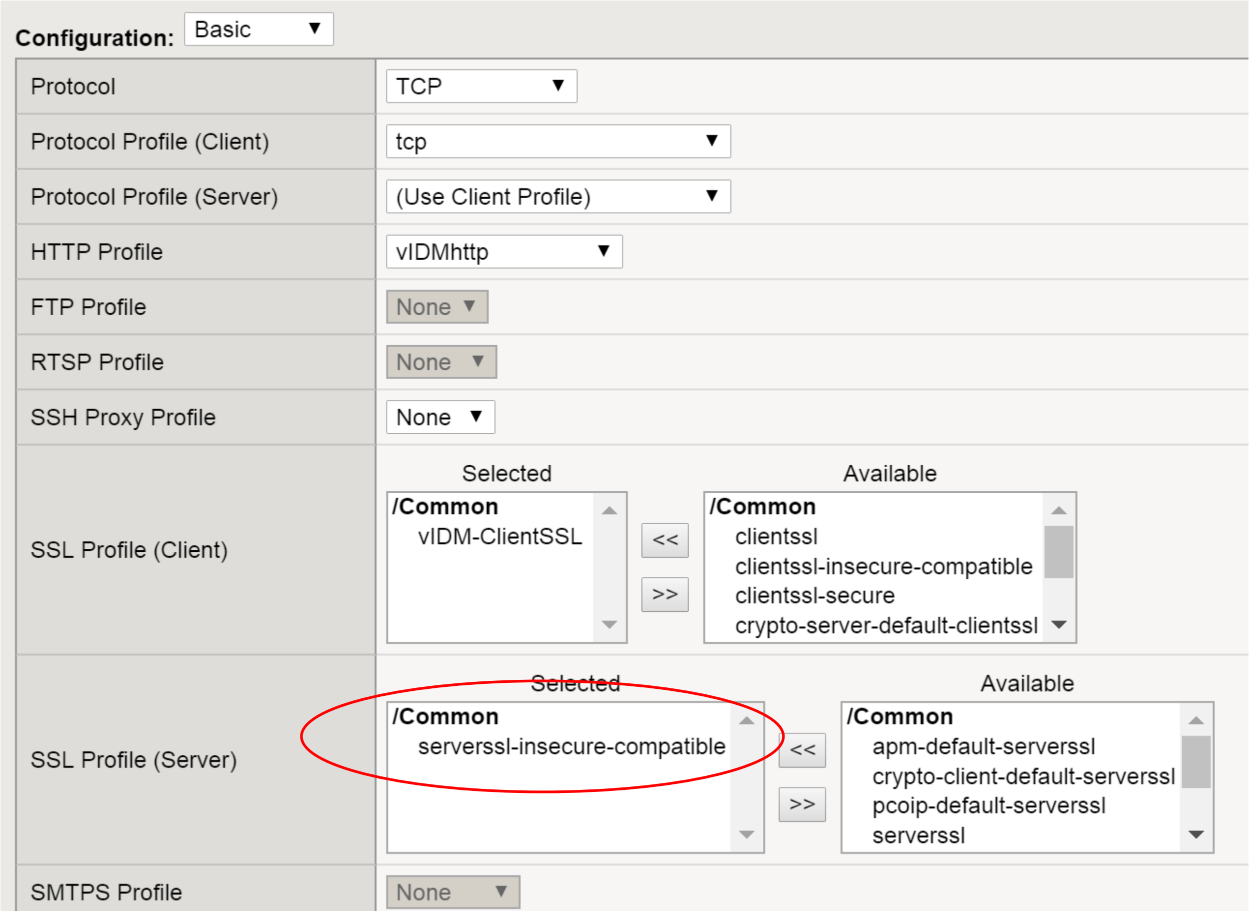
Certificates

Certificates deployment are explained in the Identity Manager Installation guide.

http://pubs.vmware.com/identity-manager-28/topic/com.vmware.ICbase/PDF/vidm-28-install.pdf

There are a few use cases where you need to change the built-in certificates.

One of them is if your load-balancer does not accept untrusted certificates. In our example, we choose F5 LTM and you can see in the Server profile that we accept unsecured connections.



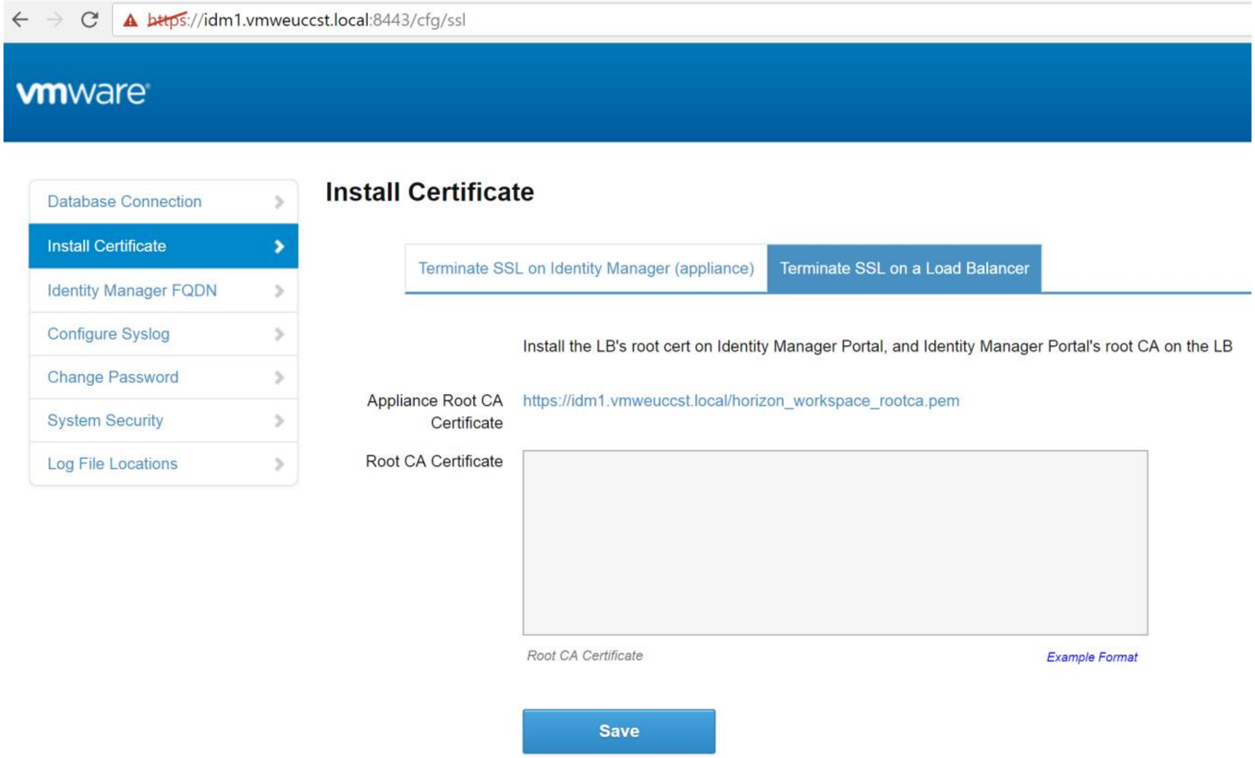
Configuration: Basic ▼

Protocol	TCP ▼
Protocol Profile (Client)	tcp ▼
Protocol Profile (Server)	(Use Client Profile) ▼
HTTP Profile	vIDMhttp ▼
FTP Profile	None ▼
RTSP Profile	None ▼
SSH Proxy Profile	None ▼
SSL Profile (Client)	Selected: **/Common** vIDM-ClientSSL Available: **/Common** clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	Selected: **/Common** serverssl-insecure-compatible Available: **/Common** apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
SMTPS Profile	None ▼

If your Load-Balancer does not accept untrusted connections, you will need to change the self-signed certificates.

You will also need to upload the PEM file to your Load-Balancer trusted certificate list. You grab the PEM file from the Appliance Configuration page, under Certificates.

Another use-case to change the self-signed certificates is when you are using Kerberos authentication, when is required by internal clients (domain-joined).



~~https~~://idm1.vmweuccst.local:8443/cfg/ssl

Install Certificate

Install the LB's root cert on Identity Manager Portal, and Identity Manager Portal's root CA on the LB

Appliance Root CA Certificate: https://idm1.vmweuccst.local/horizon_workspace_rootca.pem

Root CA Certificate:

Troubleshooting Identity Manager

There are a lot of Knowledge Base articles on troubleshooting this solution and we will not list them all here. Here, a few quick tips when problems with various components of IDM.

Unable to login to Identity Manager: https://kb.vmware.com/kb/2146806

Identity Manager Self-Signed gives an HSTS message: https://kb.vmware.com/kb/2147071

Launching Horizon 7 desktops with True SSO fails: https://kb.vmware.com/kb/2147320

Identity Manager – Problems with Analytics Services

The solution seems to be removing an index or all indices (stop elasticsearch, then rm -rf /db/elasticsearch/horizon/nodes/0/indices/v3_2015-08-18) or simply remove all the data and start fresh

Procedure:

1. Login to Identity Manager Console or SSH into Identity Manager and SU.

2. Stop ElasticSearch:

1. sudo service elasticsearch stop

3. Remove the indices

1. rm -rf /db/elasticsearch/horizon/nodes/0/indices/v3_2015-08-18

4. Or simply remove all the data in /indices/ and start fresh

5. Restart ElasticSearch or reboot

1. sudo service elasticsearch start

About the Author

Stephane Asselin is a Lead Senior EUC Architect on the VMware Customer Success Team in the End-User Computing Business Unit. He has been involved in desktop deployments for over 19 years and has extensive field experience with VMware End-User Computing and ecosystem products.

Acknowledgments

This reference architecture is the result of collaboration between VMware Customer Success Team and the Identity Manager Engineering group.

Special thanks to:

- Peter Bjork, VMware Principal Systems Engineer, EMEA
- Ravi Chayanam, Senior Manager, EUC R&D
- Karen Zelenko, Staff Program Manager, EUC CPD
- Pitambari Parekh, EUC CPD Software Engineer
- Chris Halstead, EUC Architect, Customer Success Team