



Configuring VMware® vCenter SSO High Availability for VMware vRealize Automation

Deployment Guide for High-Availability Configurations

Version 6.1 and Later

TECHNICAL WHITE PAPER

Introduction.....	2
Overview.....	2
Environment Prerequisites.....	2
Create Certificate Authority Signed Certificates for vCenter SSO nodes and the vCenter SSO load balancer.....	3
Configure the F5 Load Balancer for Use with vCenter SSO Nodes Deployed in an HA Configuration	6
Install and Configure vCenter SSO 5.5 for High Availability	17
Install vCenter SSO Server Node 1.....	18
Install vCenter SSO Server Node 2.....	22
Set Up the vCenter Single Sign-On System Environment	26
Update the vCenter SSO Services to the vCenter SSO Load Balancer FQDN on vCenter SSO Server Node1	29
Updating Certificates on vCenter SSO Server Node1	33
Updating Certificates on vCenter SSO Server Node2	36
Configure an HA Deployment of vCenter SSO 5.5 for Integration with vRealize Automation	39
Configure vRealize Automation to Use vCenter SSO.....	44
About the Authors	45
Acknowledgements.....	45
References	45

Introduction

This white paper outlines the steps for performing an end-to-end implementation of vCenter Single Sign-On 5.5 U2 in a High Availability (HA) configuration (Active – Passive configuration with automatic failover), and integration with vRealize Automation for Single Sign-On that uses an F5 load balancer.

Supported software components are:

- vRealize Automation 6.1 and later
- vCenter SSO 5.5 U2, U2a, or U2b (Windows-based installation). U2b is recommended.
- F5 load balancer, version BIG-IP 11.4.0 Build 2384.0 Final

Overview

The installation and configuration of vCenter Single Sign-On 5.5 in a highly available (HA) configuration requires the use of an external load balancer (F5 load balancer); it also requires that the various components are implemented in the correct sequence. Failing to follow the documented sequence can create unpredictable consequences and/or dependencies on other components where dependencies should not be placed.

The following list summarizes the steps for deploying vCenter SSO in a high-availability environment with vRealize Automation.

1. Creating Certificate Authority Signed Certificates for vCenter SSO nodes and vCenter SSO load balancer FQDN
2. Configuring an F5 Load Balancer for use with vCenter SSO nodes deployed in a HA Configuration (Active – Passive configuration with automatic failover)
3. Installation and Configuration of vCenter SSO 5.5 U2 for High Availability
 - a. Install vCenter SSO Server Node1
 - b. Install vCenter SSO Server Node 2
 - c. Setup vCenter Single Sign-On System Environment
 - d. Update the vCenter SSO Services to vCenter SSO Load Balancer FQDN on vCenter SSO Server Node1
 - e. Updating Certificates on vCenter SSO Server Node1
 - f. Updating Certificates on vCenter SSO Server Node2
4. Configuring vCenter SSO 5.5 U2 HA setup for integration with vRealize Automation
5. Configuring vRealize Automation with vCenter SSO 5.5 U2 deployed in a HA Configuration (Active – Passive configuration with automatic failover) for SSO

Environment Prerequisites

Before starting the implementation of vCenter SSO HA, you must ensure that certain elements of the environment are in place and fully functional, the following list identifies these elements.

The process to create CA-signed certificates comprises following steps:

1. Creating a certificate request (csr)
2. Generating a signed certificate (cer)

VMware has developed a tool called VMware vCenter Certificate Automation Tool that can be obtained from the [VMware Download Center](#) and is located in the Drivers and Tools section of the vSphere and vCloud Suite download pages (version: 5.5).

You can use the vCenter Certificate Automation Tool to generate the certificate request (csr file) for vCenter SSO, but it does not provide the ability to create SubjectAltName values, in some scenarios this may be acceptable as the team providing certificates may ask for this information at request time. However, if this is not the case, you can manually create the certificate request (csr file) with the SubjectAltName values added, which is a requirement for the vCenter Single Sign-On HA configuration.

The examples in this guide reference the values in the following table:

Name	Host Name	FQDN	IP Address
SSO Load Balancer FQDN	sso	sso.vmware.local	192.168.110.40
SSO Server 1	sso1	sso1.vmware.local	192.168.110.41
SSO Server 2	sso2	sso2.vmware.local	192.168.110.42

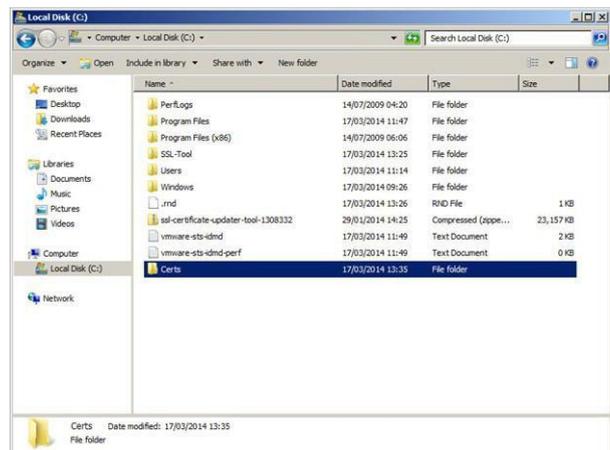
Create Certificate Authority Signed Certificates for vCenter SSO nodes and the vCenter SSO load balancer

After you complete and verify the prerequisites, you create certificates signed by a certificate authority. You configure vCenter SSO server nodes with these certificates later.

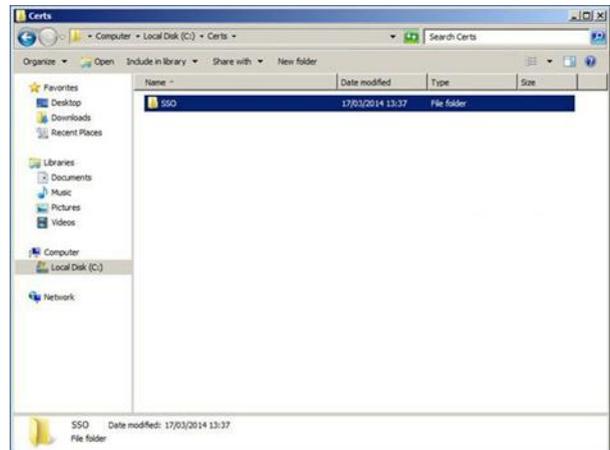
Task ID	Task Description	Screenshot (optional)
---------	------------------	-----------------------

1. Download and extract the VMware vCenter Certificate Automation Tool to a directory on vCenter SSO Server Node1. (In this example the zip file, ssl-certificate-updater-tool-1308332.zip, is extracted to the **C:\SSL-Tool** directory).

2. On the first node for vCenter Single Sign-On, create a folder in which you can store the certificate files. These steps use the **C:\Certs** folder.



3. In the **C:\Certs** folder, create an **SSO** folder to organize your certificate requests and configuration files.



Task ID	Task Description	Screenshot
---------	------------------	------------

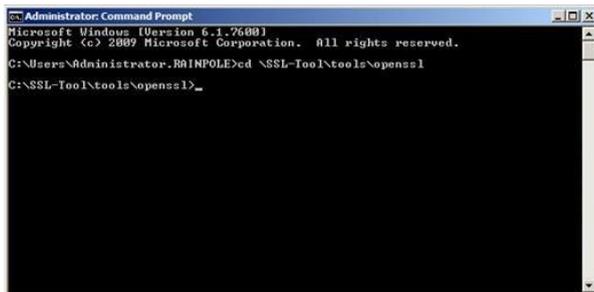
4.	<p>Open a text editor on node1 and create a configuration file using the format provided here.</p> <p>Edit the text highlighted in bold and red with values for your environment.</p> <p>Save the configuration file to the C:\Certs\SSO directory as openssl_sso.cfg.</p>	<pre>[req] default_bits = 2048 default_keyfile = rui.key distinguished_name = req_distinguished_name encrypt_key = no prompt = no string_mask = nombstr req_extensions = v3_req [v3_req] basicConstraints = CA:false keyUsage = digitalSignature, keyEncipherment, dataEncipherment extendedKeyUsage = serverAuth, clientAuth subjectAltName = DNS:sso1, DNS:sso1.vmware.local, DNS:sso2, DNS:sso2.vmware.local, DNS:sso.vmware.local, IP:192.168.110.40 [req_distinguished_name] countryName = US stateOrProvinceName = CA localityName = PA 0.organizationName = VMware organizationalUnitName = vCenter Single Sign On commonName = sso.vmware.local</pre>
----	--	---

5. Open a command prompt and go to the **VMware vCenter Certificate Automation Tool** directory.

In this example the files are extracted to the **C:\SSL-Tool** folder/

Type the following command:

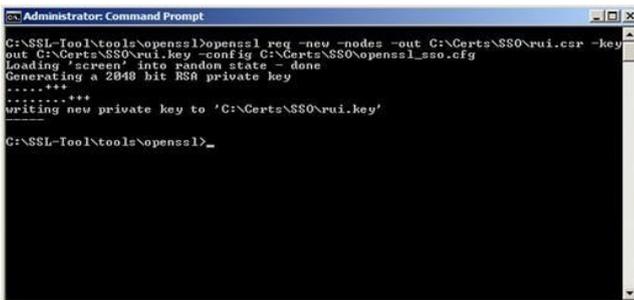
```
cd C:\SSL-Tool\tools\openssl
```

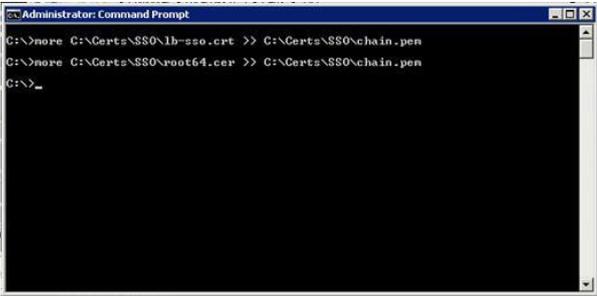


6. Run the following command to create the vCenter SSO certificate request and export the private key:

```
openssl req -new -nodes -out
C:\Certs\SSO\rui.csr
-keyout C:\Certs\SSO\rui.key -config
C:\Certs\SSO\openssl_sso.cfg
```

The vCenter SSO certificate request and the private key files (**rui.csr** and **rui.key**) are now available at **C:\Certs\SSO** directory.



Task ID	Task Description	Screenshot (optional)
7.	<p>You can send the certificate request to your certificate issuing team or you can use Microsoft CA as the trusted root Certificate Authority.</p> <ul style="list-style-type: none"> If you are using your certificate issuing team, follow these steps: <ul style="list-style-type: none"> Send the vCenter SSO certificate request (ruicert.req) to your Certificate issuing team and get the CA signed certificate (ssocert.cer) for vCenter SSO in Base-64 encoded X.509 (.CER) format. Copy the SSO CA-signed certificate (ssocert.cer) to the C:\Certs\SSO directory. If you are using Microsoft CA as the trusted root Certificate authority to sign and issue the certificates for vCenter SSO, enable data encipherment, nonrepudiation, and client authentication on the certificate template. <p>For more information about creating certificate templates in the Microsoft CA server, see VMware Knowledge Base article 2062108 – “Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 5.x”</p> <p>For more information about obtaining the vCenter SSO certificate using Microsoft CA, see Obtain vCenter SSO certificate (part of VMware KB article 2044696)</p>	
8.	<p>Verify that the certificate issuing team has provided the root CA certificate (root64.cer) in Base-64 encoded X.509 (.CER) format. Copy the root CA certificate (root64.cer) to the C:\Certs\SSO directory.</p> <p>Note: Also get the intermediate CA certificates in Base-64 encoded X.509 (.CER) format if you have intermediate CA servers signing the certificate requests.</p>	
9.	<p>Open a command prompt and run the following commands to merge the ssocert.cer and root64.cer file into a .pem file:</p> <ol style="list-style-type: none"> <code>more C:\Certs\SSO\ssocert.cer >> C:\Certs\SSO\chain.pem</code> <code>more C:\Certs\SSO\root64.cer >> C:\Certs\SSO\chain.pem</code> <p>Note: If you have intermediate CA servers signing the certificate requests then you must to add them to the chain.pem file. The order must be vCenter SSO certificate, intermediate CA certificates, and root CA certificate.</p>	 <pre>Administrator: Command Prompt C:\>more C:\Certs\SSO\ssocert.cer >> C:\Certs\SSO\chain.pem C:\>more C:\Certs\SSO\root64.cer >> C:\Certs\SSO\chain.pem C:\>_</pre>
10.	<p>Ensure that both the vCenter SSO certificate and key files (ssocert.cer and ruicert.key), and the root CA certificate (root64.cer) are provided to the F5 load balancer team for F5 configuration.</p>	

Configure the F5 Load Balancer for Use with vCenter SSO Nodes Deployed in an HA Configuration

You can use the procedures in this section to configure an F5 load balancer to run vCenter SSO nodes that have been deployed in a high-availability configuration, an active/passive configuration with automatic failover.

vCenter SSO 5.5 U2, U2a, and U2b are supported for use with vRealize Automation U2b is the recommended version.

The examples in this section reference the values shown in the following table.

Name	Host Name	FQDN	IP Address
SSO Load Balancer FQDN	sso	sso.vmware.local	192.168.110.40
SSO Server 1	sso1	sso1.vmware.local	192.168.110.41
SSO Server 2	sso2	sso2.vmware.local	192.168.110.42

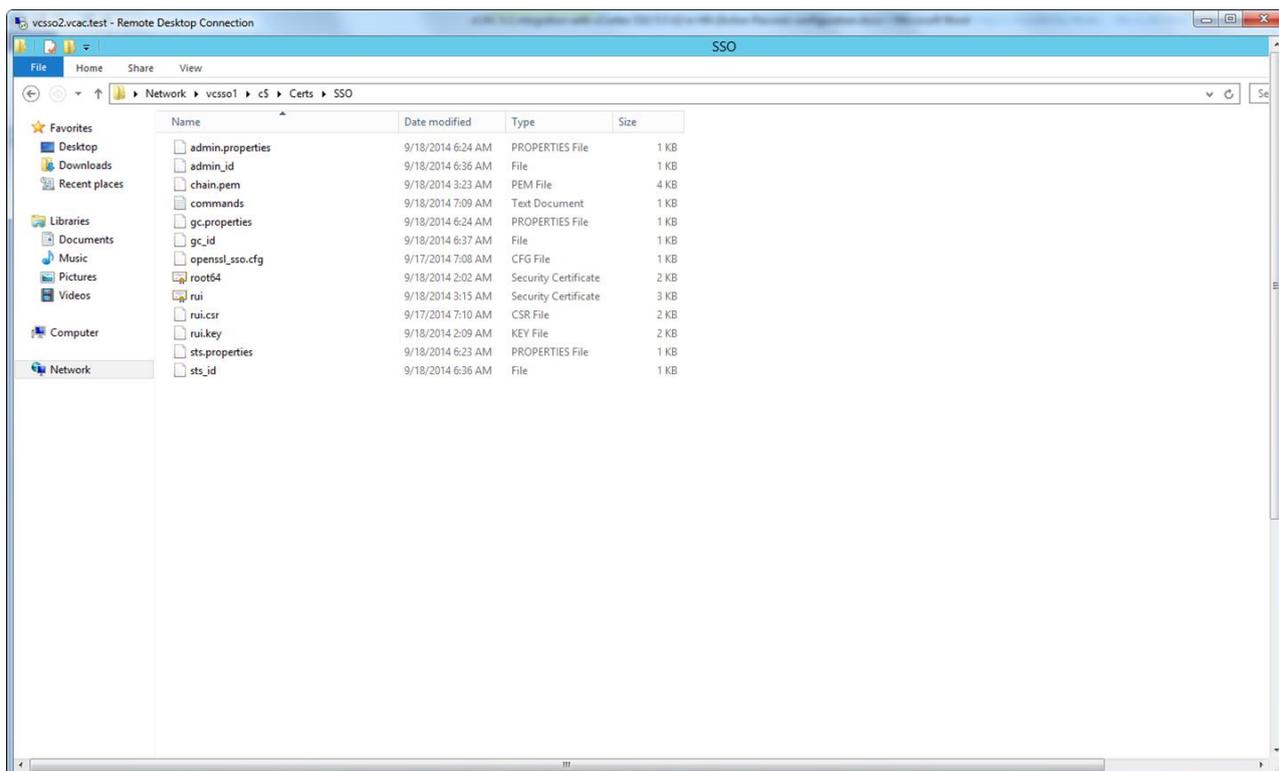
Procedures in this section are based on the following load balancer environment:

1. F5 load balancer that is installed and licensed and for which DNS server configuration is complete
2. F5 load balancer running version 11.4.0 Build 2384.0 Final for BIG-IP

These steps may vary in a different F5 load balancer version.

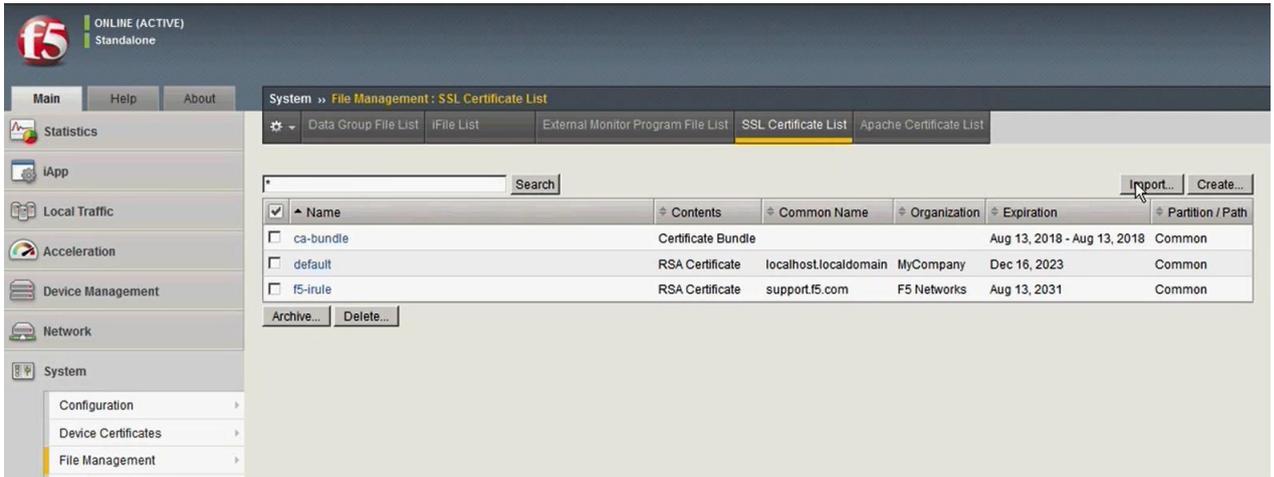
Procedure

1. Make a backup copy of the C:\Certs\sso directory on the vCenter SSO Server Node 1. This directory contains vCenter SSO CA signed certificates and the root CA certificate file **root64.cer**.

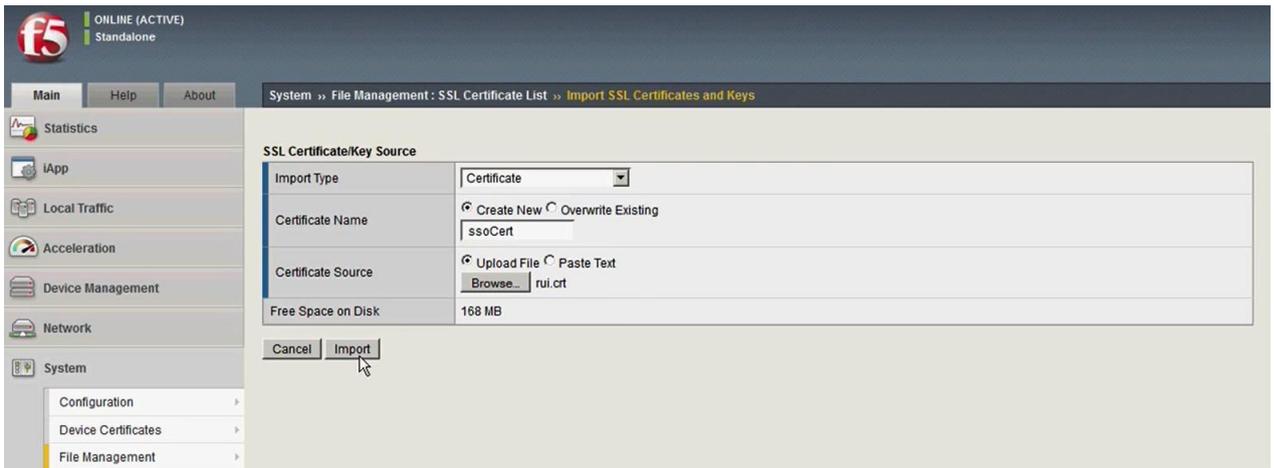


2. Using a supported web browser, open the F5 BIG-IP load balancer management interface (<https://<f5lbhostname>>) and log in.
3. Upload the vCenter SSO certificate to the F5 load balancer.
 - a. From the **Main** tab on F5 user interface, select **System>File Management**.

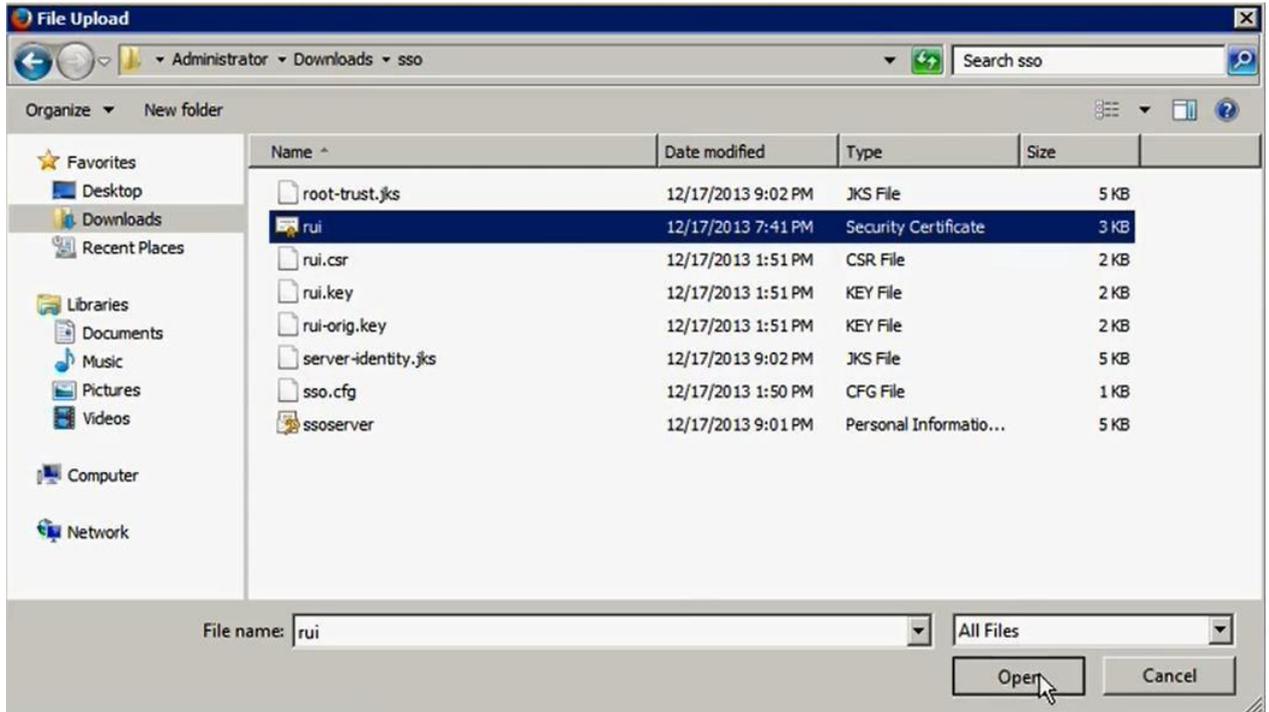
- b. Click the **SSL Certificate List** tab.
- c. On the **SSL Certificate List** screen, click **Import**.



- d. For **Import Type**, select **Certificate**.
- e. For **Certificate Name**, select **Create New** and enter `ssoCert` as the name.
- f. For **Certificate Source**, select **Upload File** and browse to the `sso.cer` file (the vCenter SSO certificate file) in the `C:\Certs\sso` directory you copied in step 1.



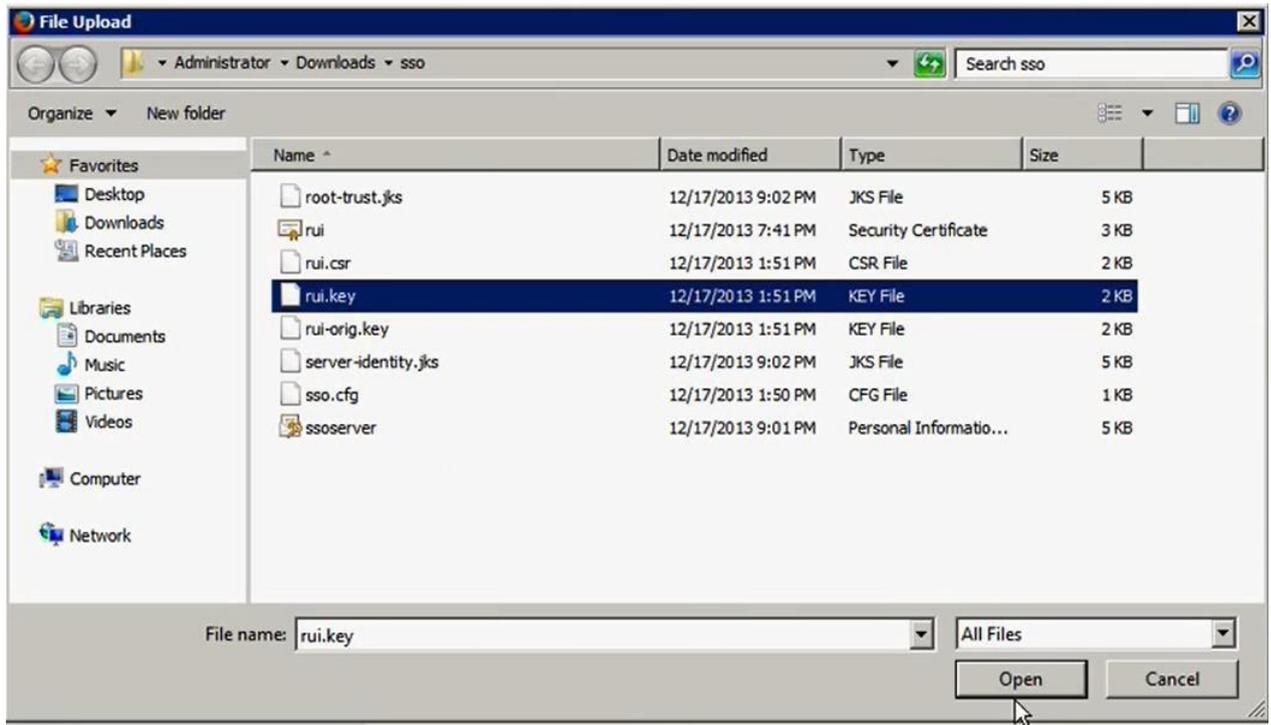
- g. Select the certificate file and click **Open**. The `sso.cer` file is selected in our example.



- h. Click **Import** on the F5 load balancer interface. The ssoCert is now imported.
4. Upload the vCenter SSO key to the F5 load balancer.
- a. On the **SSL Certificate List** screen, click **Import**.
 - b. For **Import Type**, select **Key**.
 - c. For **Key Name**, select **Create New** and enter `ssoKey` as the name.
 - d. For **Key Source**, select **Upload File** and browse to the `rui.key` file (vCenter SSO key file) in the `C:\Certs\sso` directory you copied in step 1.



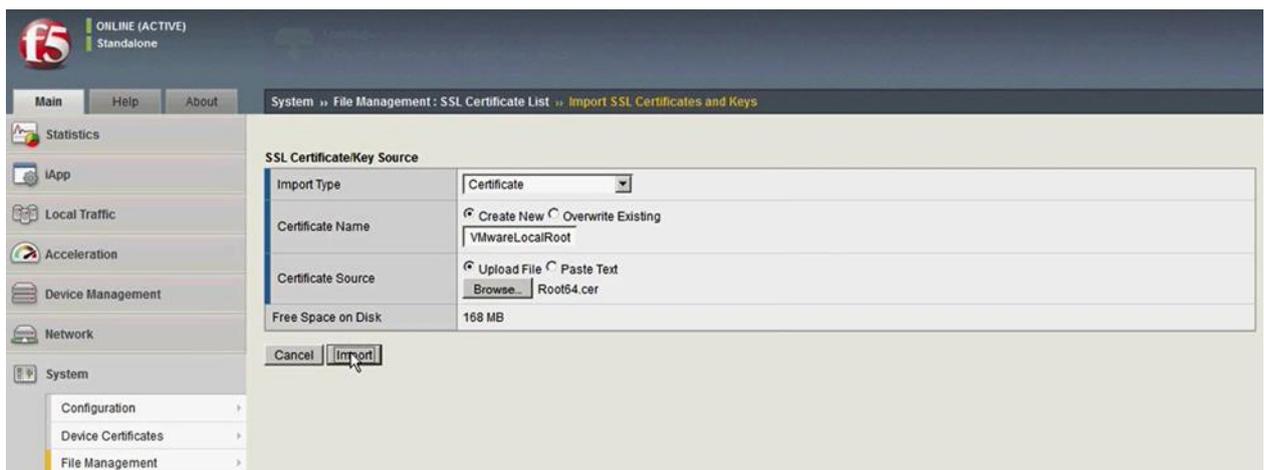
- e. Click **Open** to select the `rui.key` file.



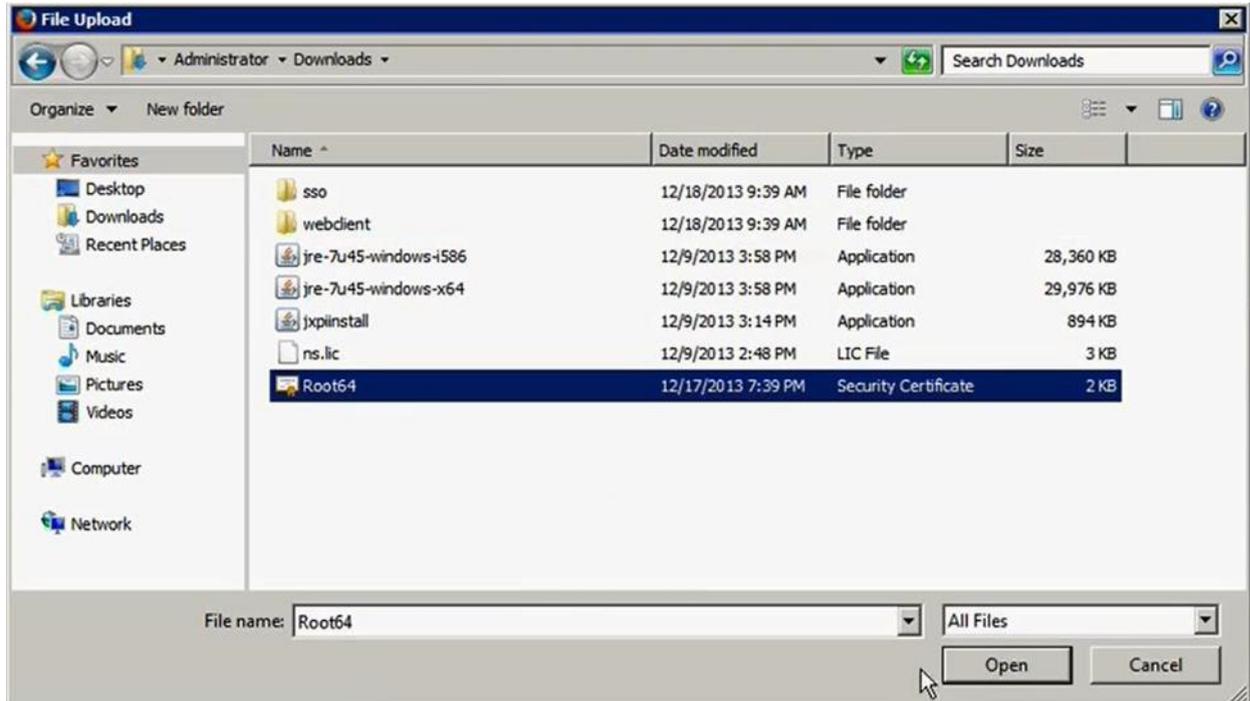
f. From the F5 load balancer interface, click **Import**. The ssoKey is now imported.

5. Upload the CA root certificate to the F5 load balancer.

- a. On the SSL Certificate List screen, click **Import**.
- b. For **Import Type**, select **Certificate**.
- c. For **Certificate Name**, select **Create New** and enter **VMwareLocalRoot**.
- d. For **Certificate Source**, select **Upload File** and browse to the **Root64.cer** file (CA root certificate file) available at the **C:\Certs\sso** directory copied in step 1.

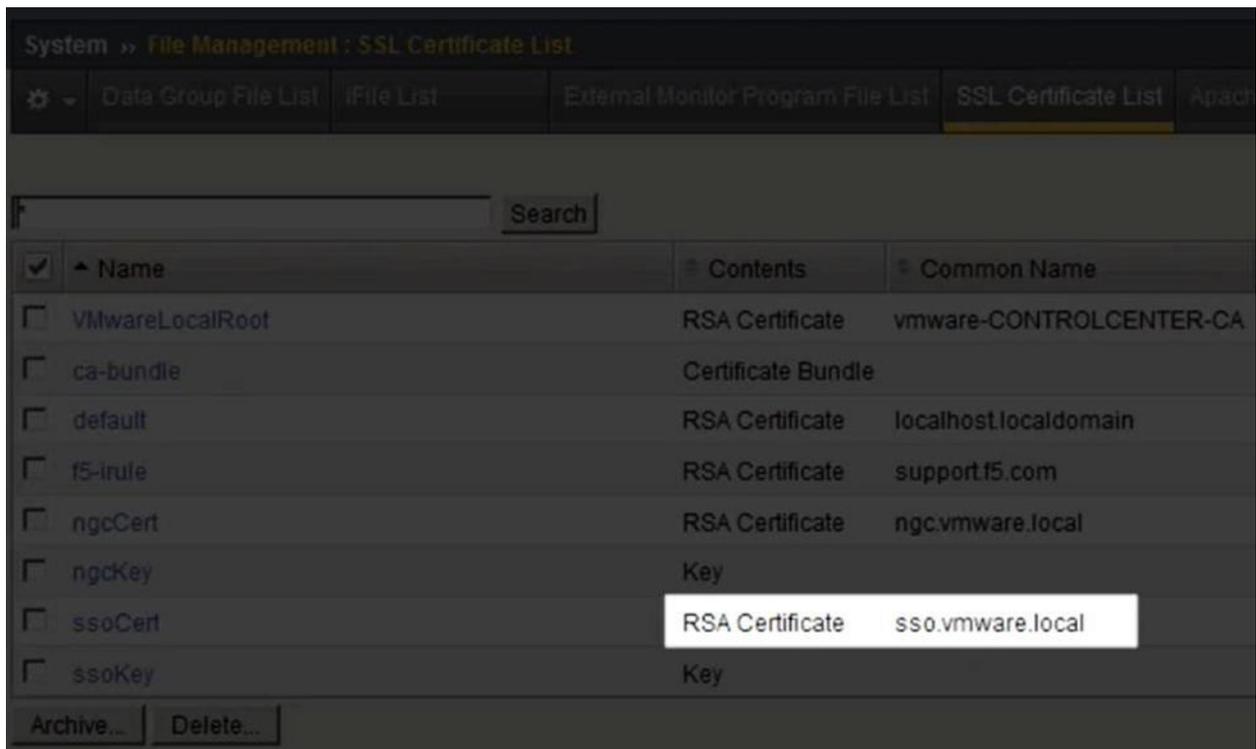


e. Click **Open** to select the CA root certificate file. In our example, this is **Root64**.



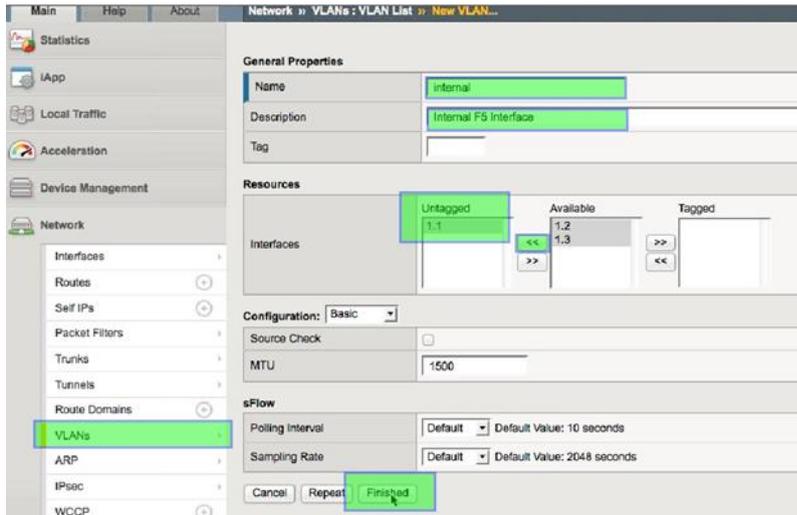
f. Click **Import**. The CA root certificate is now imported.

6. Verify that the **Common Name** for ssoCert is **sso.vmware.local**,



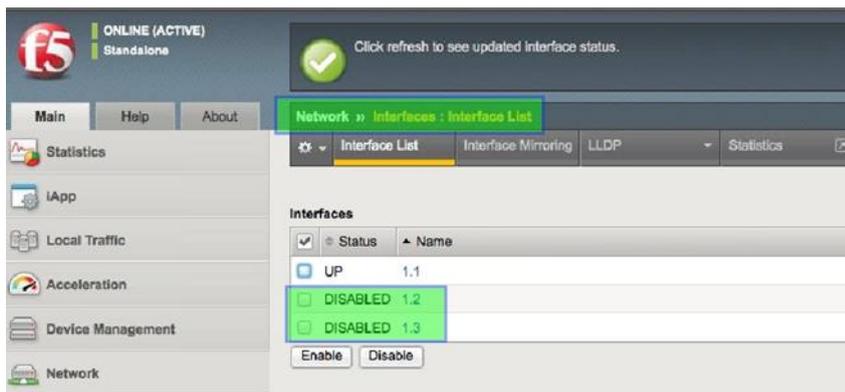
7. Create a VLAN as specified in the next screenshot.

- a. Select **Network>VLANs>VLAN list**.
- b. Click **Create**.
- c. Provide the details and click **Finished**.

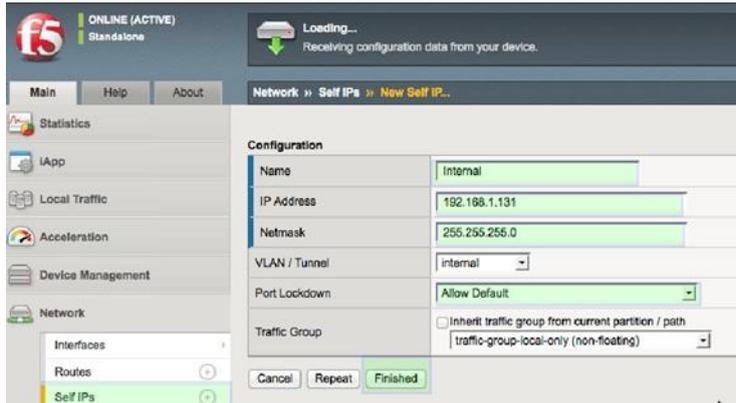


8. Configure the Interfaces List. Ensure that interface 1.1 is up and interfaces 1.2 and 1.3 are disabled.
 - a. Select **Network>Interfaces >Interface List**.
 - b. Select 1.2 and 1.3 under **Name** and then click **Disable**.

Note: This solution uses Management and Internal Interfaces. External (1.2) and HA (1.3) are disabled in this configuration.



9. Configure Self-IP.
 - a. In the F5 load balancer console, select **Network > Self IPs**.
 - b. Click **Create**.
 - c. In the **Name** text box, enter **Internal**.
 - d. Enter values for the Self IP in the **IP Address** and **Netmask** text boxes.
 - e. From the **VLAN/Tunnel** dropdown menu, select **internal**.
 - f. From the **Port Lockdown** dropdown menu, select **Allow Default**.
 - g. From the **Traffic Group** dropdown menu, select **traffic-group-local-only (non-floating)**.
 - h. Click **Finished**.



10. Create the load balancer pool by using the two SSO servers as the two member nodes.

- a. Select **Local Traffic>Pools>Pools List**.
- b. On the Pools List screen, click **Create**.
- c. Enter a name in the **Name** text box; for example, SSO.
- d. In the **Health Monitors** area, select and add **tcp** to the Active column.
- e. Select **Round Robin** from the Load Balancing Method drop-down menu.
- f. Select **Less than** from the Priority Group Activation text box.
- g. Enter **1** in the Available Members text box.
- h. In the **New Members** area, select the **New Node** option and create a new member:

Enter sso1 as the node name in the **Node Name** text box.

Enter an **Address**: 192.168.110.41 (this is the IP address of SSO Server Node1 in our example).

Enter a **Service Port**: 7444 and HTTPS.

Enter a **Priority**: 10.

Click **Add**.

Enter a **Node Name** for the second node: sso2.

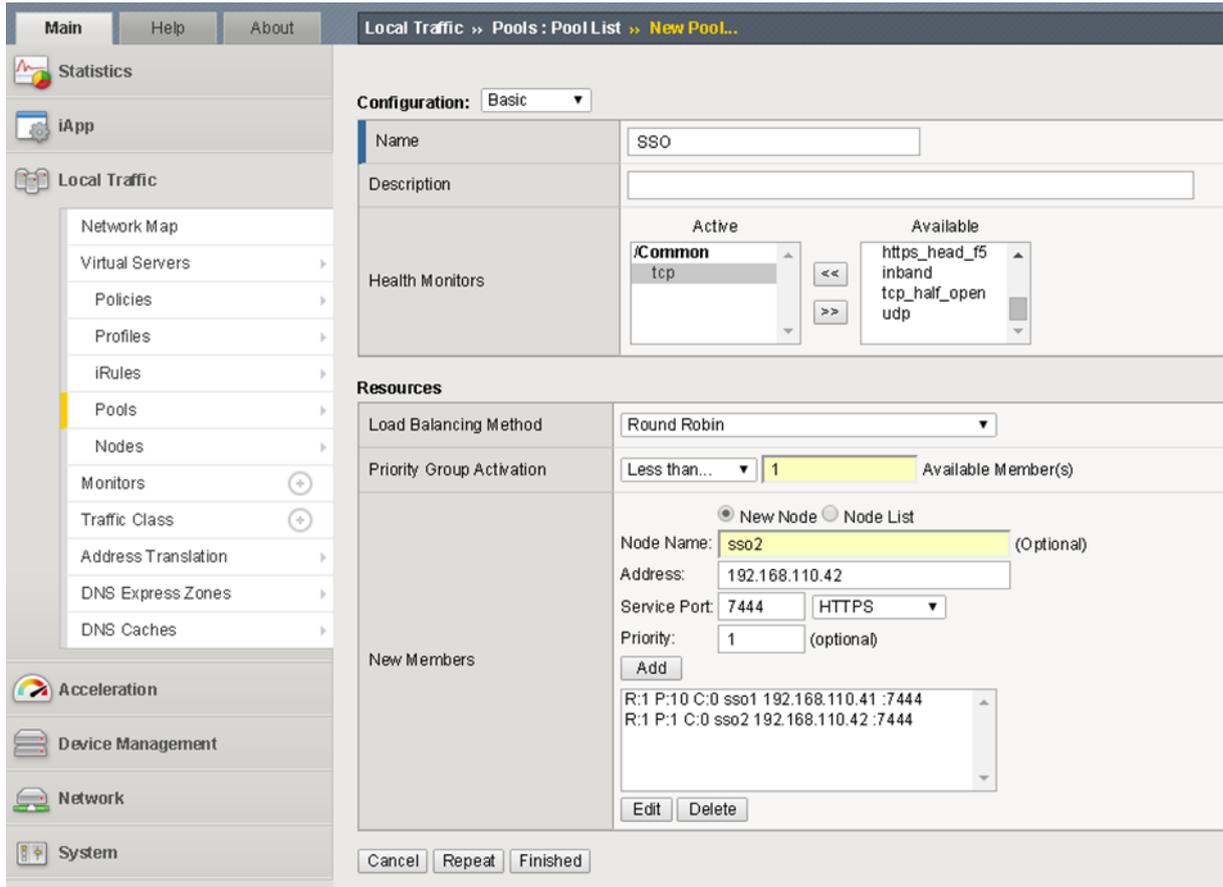
Enter an **Address**: 192.168.110.42 (this is the IP address of SSO Server Node2 in our example).

Enter a **Service Port**: 7444 and HTTPS.

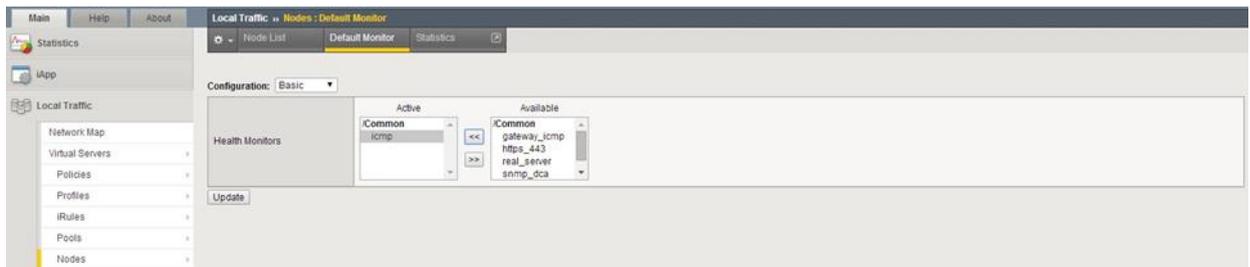
Enter a **Priority**: 1.

Click **Add**.

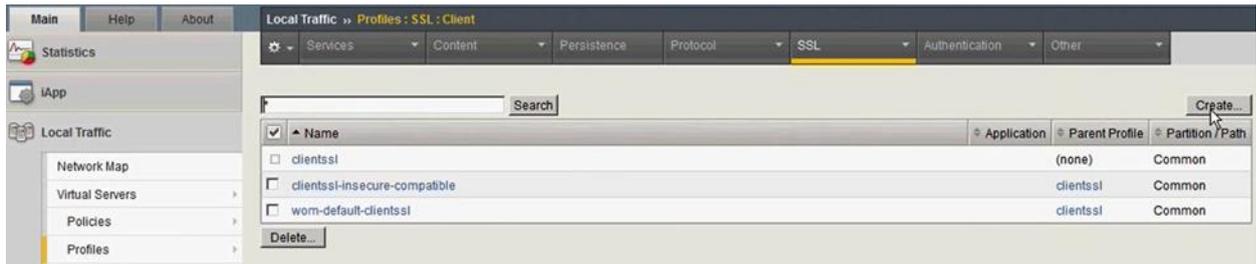
Click **Finished**.



11. Add ICMP as the Default Monitor for Nodes.
 - a. Select Local **Traffic>Nodes> Default Monitor**.
 - b. Select and add **icmp** to the **Active** column.
 - c. Click **Update**.



12. Create an SSL client profile:
 - a. Select **Local Traffic>Profiles** from the left-hand menu.
 - b. Click **SSL**.
 - c. Click **Client**.
 - d. On the Client screen, click **Create**.

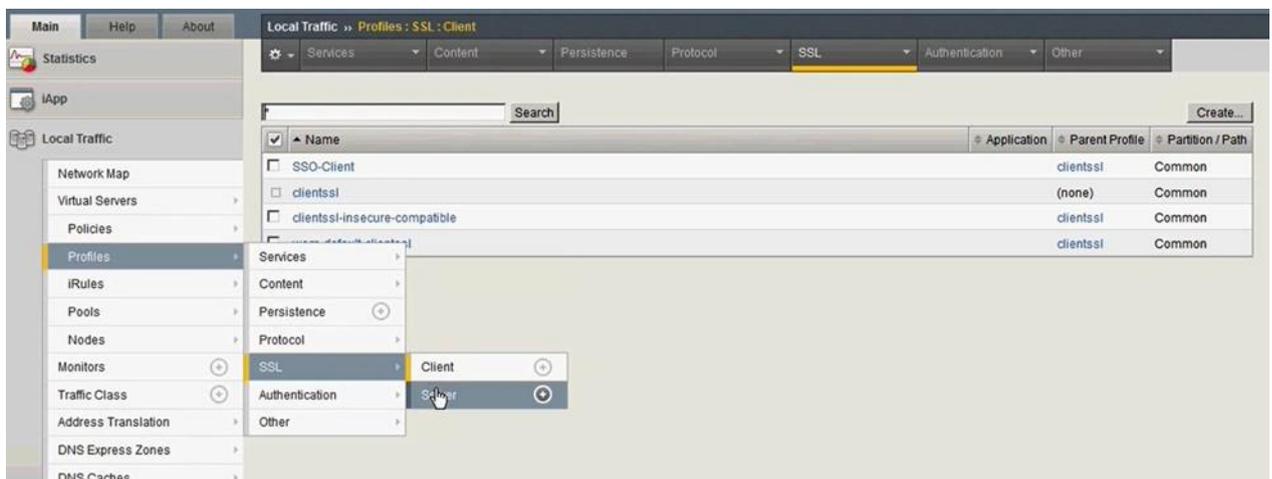


- e. Enter a name, for example, **SSO-Client**, in the **Name** text box.
- f. Select the **Custom** checkbox.
- g. In the **Configuration** area, select **Basic** from the drop-down menu.
- h. Select **ssoCert** from the **Certificate** drop-down menu.
- i. Select **ssoKey** from the **Key** drop-down menu.
- j. Clicked **Finished**.



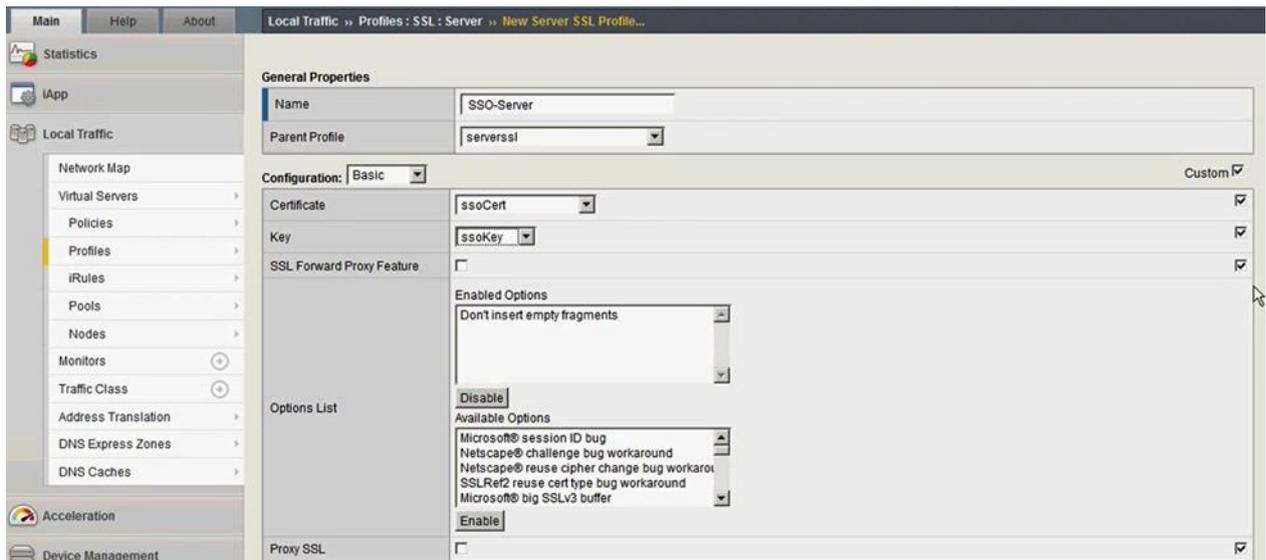
13. Create an SSL server profile:

- a. Select **Local Traffic > Profiles**.
- b. Click **SSL**.
- c. Click **Server**.



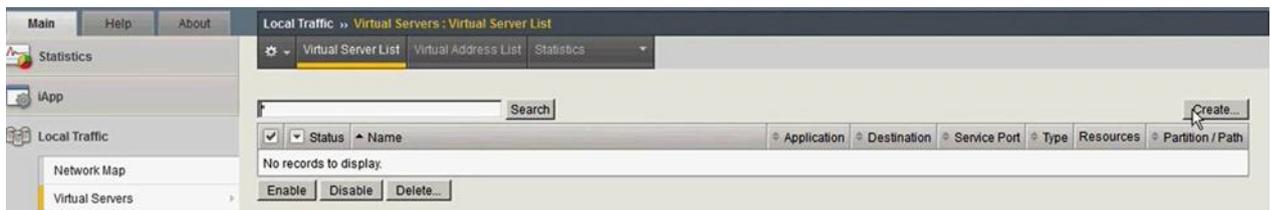
- d. On the Server screen, click **Create**.
- e. Enter a **Name**: **SSO-Server**.
- f. Select the **Custom** checkbox on the right-hand side.
- g. Under **Configuration**:
 - i. For **Certificate**, choose **ssoCert**.
 - ii. For **Key**, choose **ssoKey**.

h. Click **Finished**.

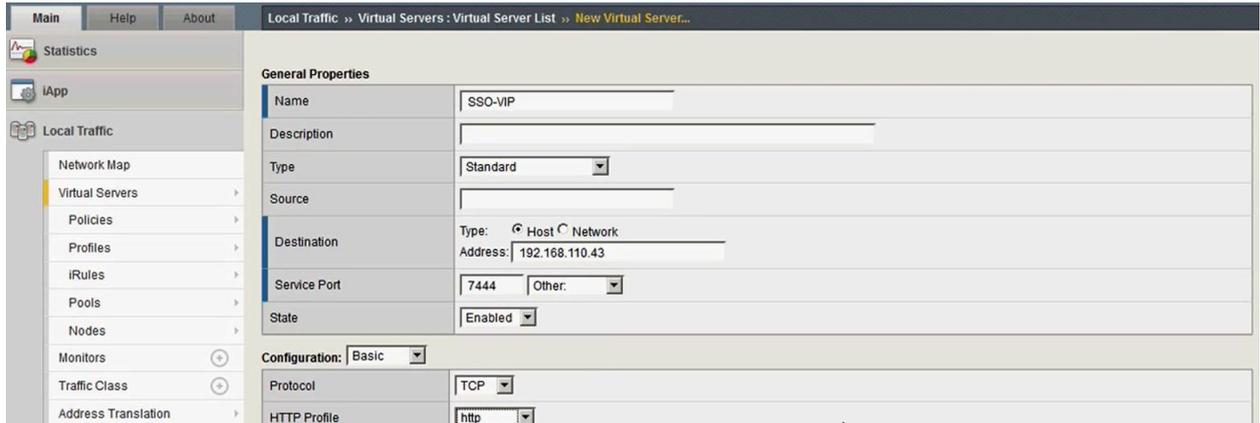


14. Create a Virtual Server. This will use the load balancer IP address (192.168.110.40 in our example):

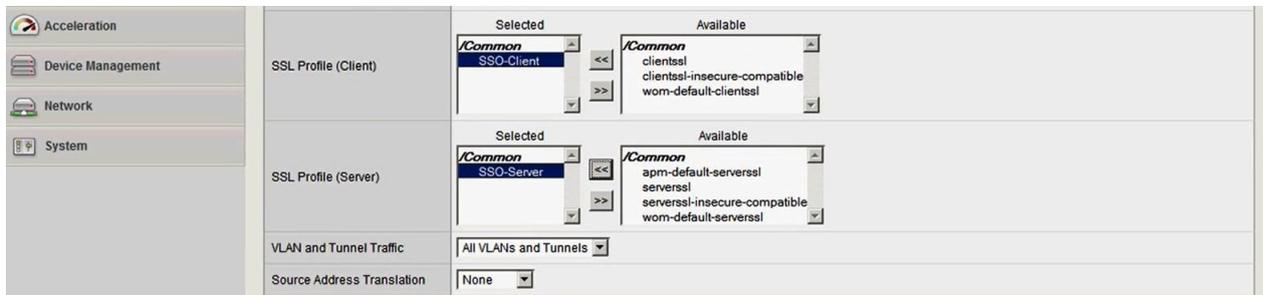
- a. Choose **Local Traffic** from left-hand menu.
- b. Choose **Virtual Servers**.
- c. Choose **Virtual Server List**.
- d. On the Virtual Servers screen, click **Create**.



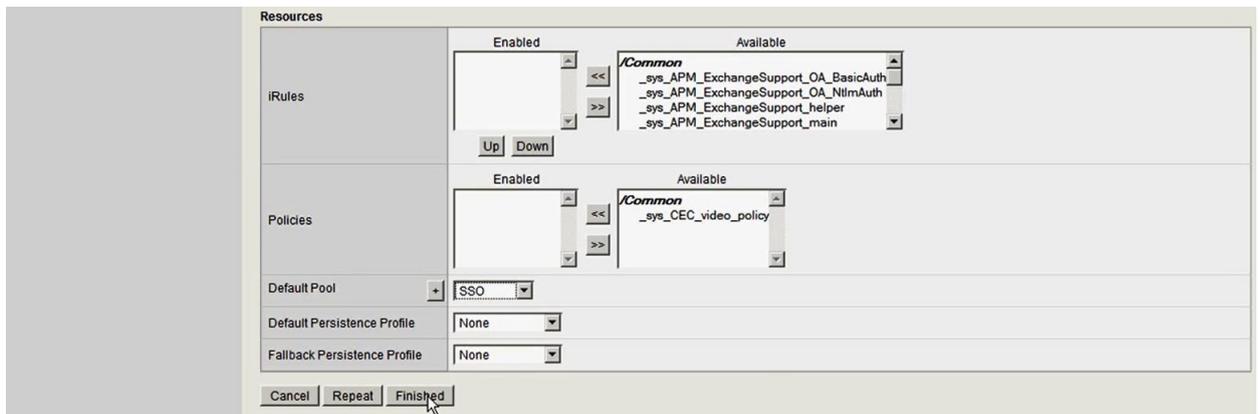
- e. Enter a **Name**: **SSO-VIP**
- f. Provide a **Destination**:
 - i. For **Type**, select **Host**.
 - ii. Enter an **Address**: 192.168.110.40 (this is the load balancer IP address in our example)
- g. Enter a **Service Port**: 7444 and HTTPS
- h. Under **Configuration**.
 - i. For **HTTP Profile**, choose **http**.



- ii. For **SSL Profile (Client)**: choose **SSO-Client**.
- iii. For **SSL Profile (Server)**: choose **SSO-Server**.
- iv. For **Source Address Translation** choose **Auto Map**.



- i. Under **Resources**:
 - i. For **Default Pool**: choose **SSO**.
 - ii. For **Default Persistence Profile**, select **None**.



- j. Click **Finished**.

15. Do not make any entry for **SNAT**.

16. Ensure the vCenter SSO load balancer virtual address is added to your DNS server. Using our example, add an entry for 192.168.110.40 ← → sso.vmware.local into your DNS server)

Install and Configure vCenter SSO 5.5 for High Availability

Before you begin the implementation of vCenter SSO HA verify that the following prerequisites are met:

- Creation of SSO nodes as Virtual Machines
- Registration of SSO nodes within a DNS service
- Installation of the VMware vCenter Certificate Automation Tool (ssl-certificate-updater-tool-1308332.zip) on both SSO nodes. You can obtain the tool from the [VMware Download Center](#) in the Drivers and Tools section of the vSphere and vCloud Suite download pages (version: 5.5).
- CA-signed certificates for SSO nodes and SSO load balancer FQDN
- A fully configured F5 load balancer
- The SSO load balancer FQDN must be registered within a DNS service

The examples in this section reference the values in the following table:

Component	Hostname	FQDN	IP Address
SSO Node1	sso1	sso1.vmware.local	
SSO Node2	sso2	sso2.vmware.local	
SSO Load Balancer FQDN	sso	sso.vmware.local	

Install vCenter SSO Server Node 1

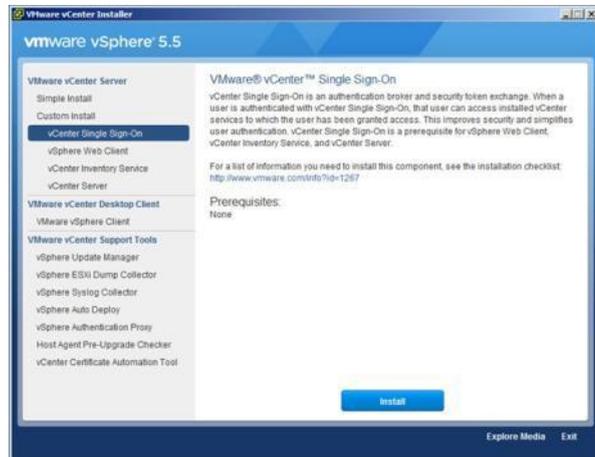
Once you have completed all environmental preparation tasks, you are ready to start following the procedure captured here to implement the first node of the vCenter Single Sign-On HA setup.

Task ID	Task Description	Screenshot
---------	------------------	------------

1. Start the VMware vSphere installer by clicking **autorun.exe**.



2. From the VMware vSphere installer menu, select **vCenter Single Sign-On**.
Click **Install**.

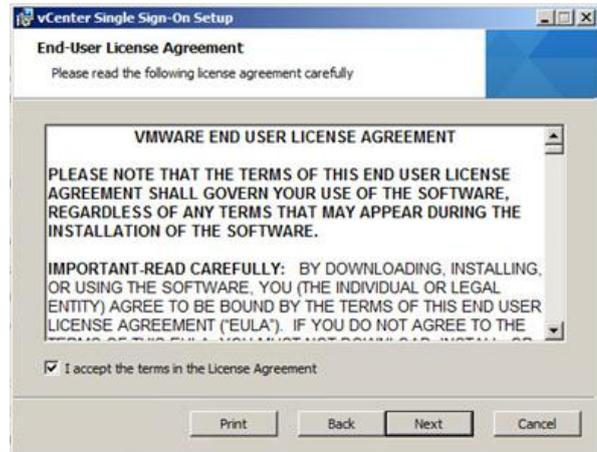


3. At the Welcome to the vCenter Single Sign-On Setup dialog, click **Next**.



Task ID	Task Description	Screenshot
---------	------------------	------------

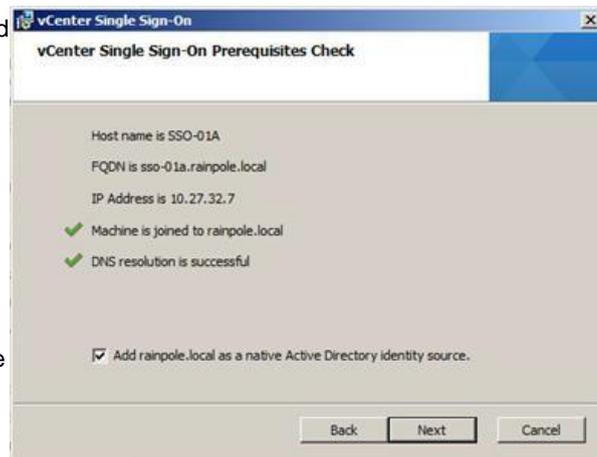
4. At the End-User License Agreement dialog, click the **I accept the terms in the License Agreement** check box.
Click **Next**.



5. The vCenter Single Sign-On Prerequisites Check dialog appears and the installation wizard detects the system configuration.
Verify that the **FQDN** and **IP Address** are correct.
By default the **Add domain_name as a native Active Directory identity source** check box is selected.

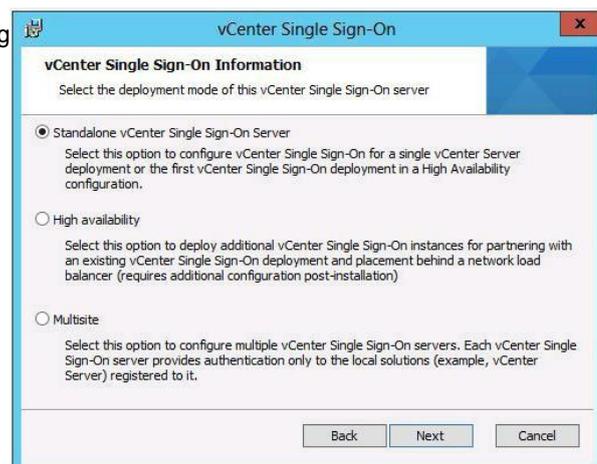
Note: For large Active Directory domains the installer can appear to hang and eventually times out and rolls back while trying to complete this task, in these situations clear the checkbox and add the domain at a later stage.

Click **Next**.



6. At the vCenter Single Sign-On Information dialog for deployment mode, select the **Standalone vCenter Single Sign-On Server** button.

Click **Next**.

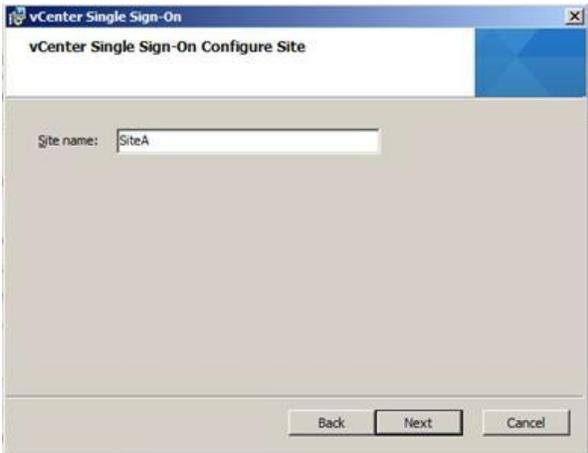


Task ID	Task Description	Screenshot
---------	------------------	------------

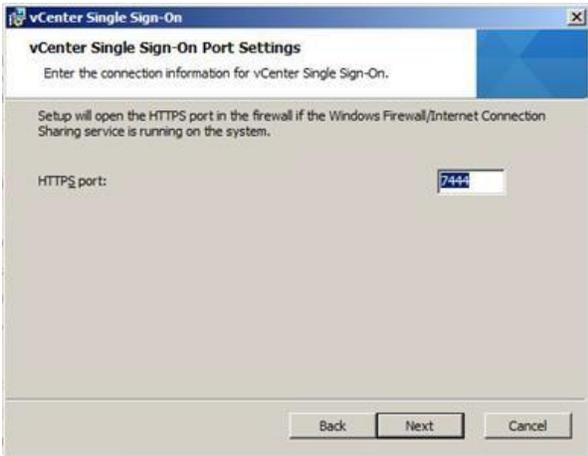
7. At the vCenter Single Sign-On Information dialog for administrator account credentials, type the password for the administrator in the **Password** text box.
- Reenter the password in the **Confirm Password** text box.
- Click **Next**.



8. At the vCenter Single Sign-On Configure Site dialog, type a unique site name into the **Site name** text box or accept the default.
- Click **Next**.

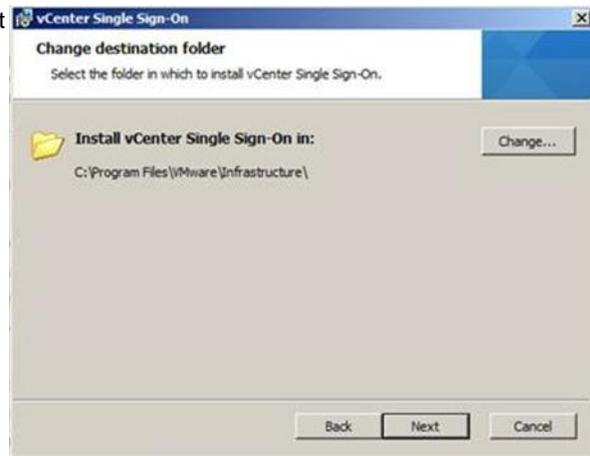


9. At the vCenter Single Sign-On Port Settings dialog, unless you have a requirement to alter the default HTTPS port, leave the default value of **7444**.
- Click **Next**.
- Note:** The remaining procedures assume that the default port of **7444** is used.



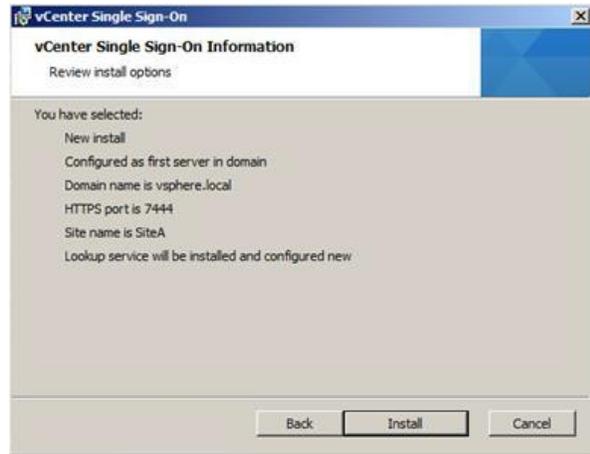
Task ID	Task Description	Screenshot
---------	------------------	------------

10. At the Change destination folder dialog, accept the default path by clicking **Next**.

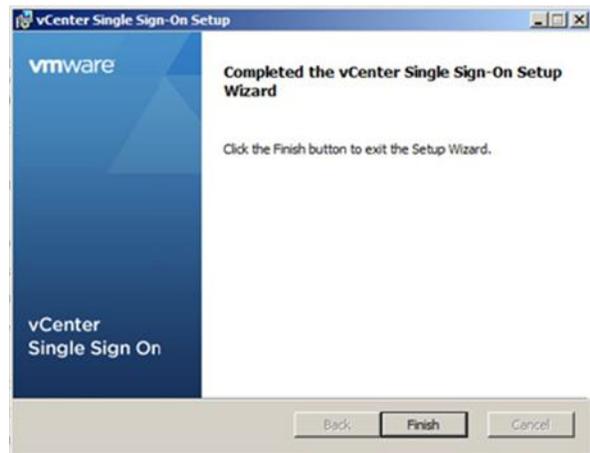


11. At the vCenter Single Sign-On Information dialog for install options, review the install options.

Click **Install**.

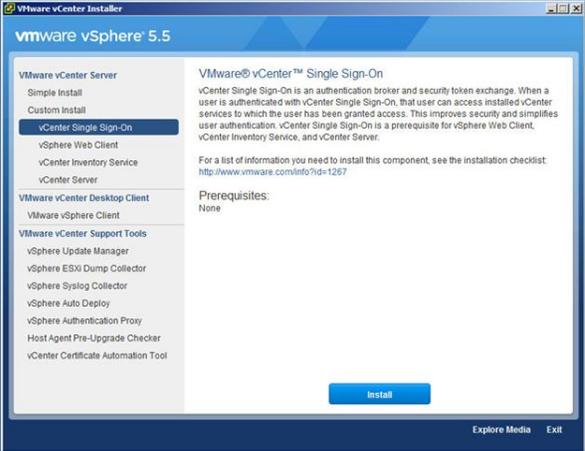
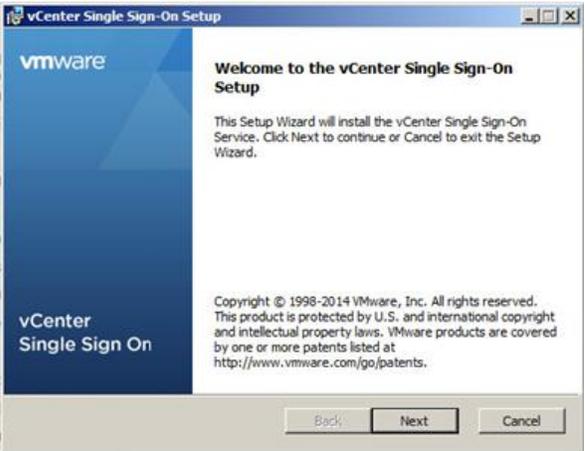


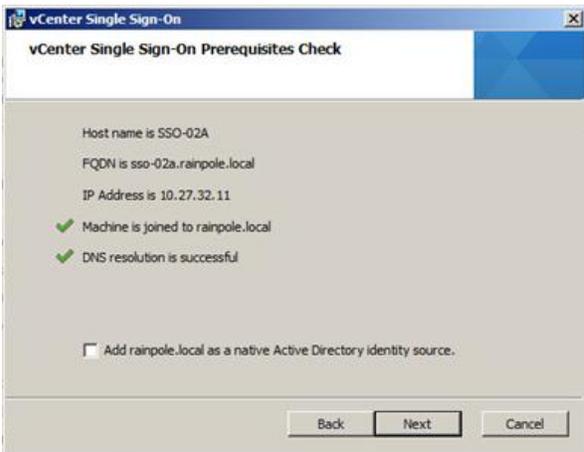
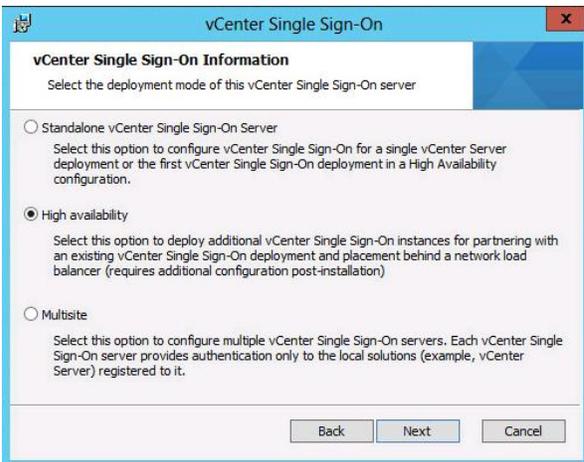
12. At the Completed the vCenter Single Sign-On Setup Wizard dialog, click **Finish**.

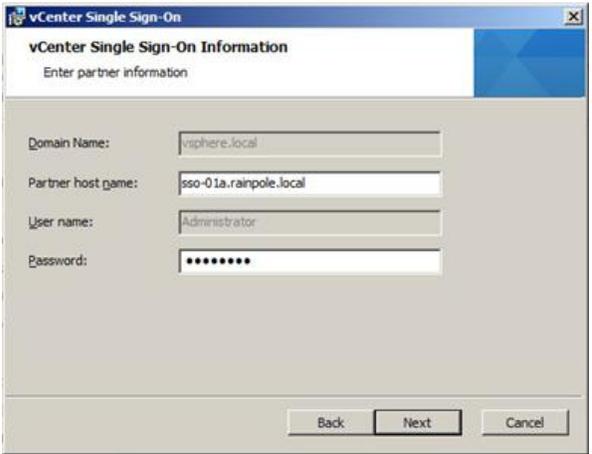
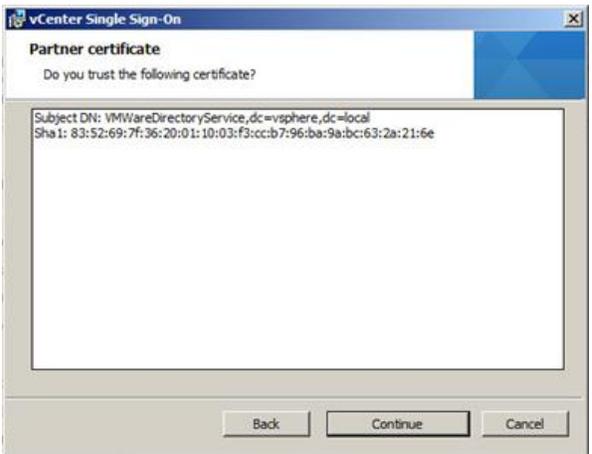
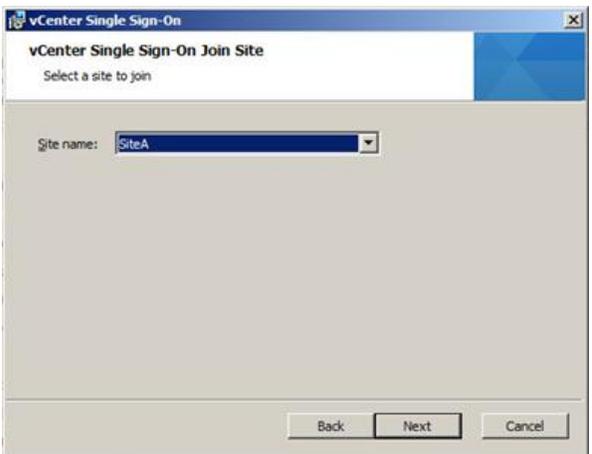


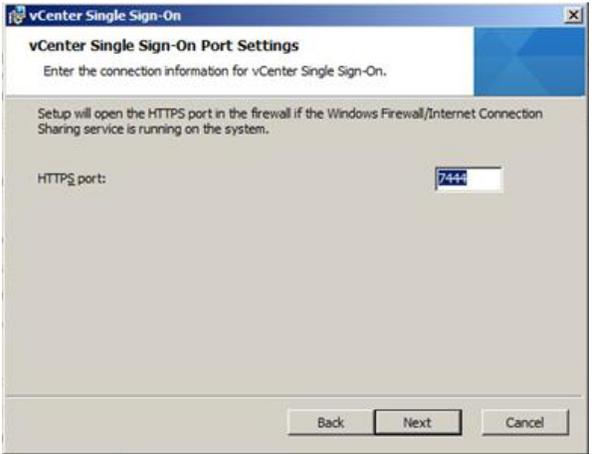
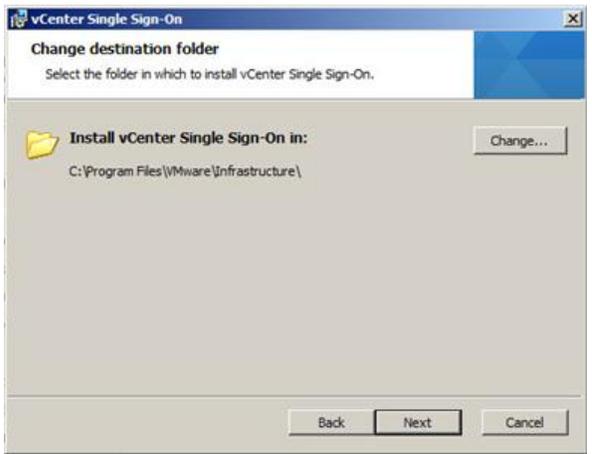
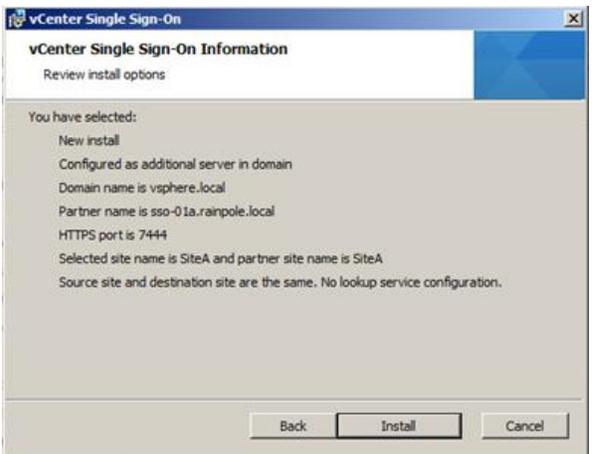
Install vCenter SSO Server Node 2

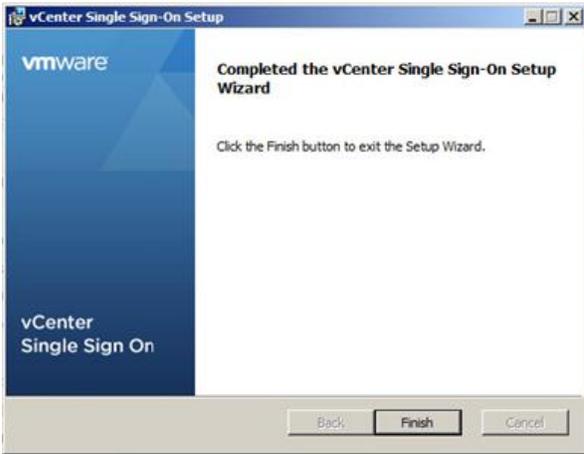
Once the first node has been installed, you must proceed to performing the installation of the second node, this is performed in similar way as the first node but with one key alteration in that you must specify a different deployment mode. Follow the step-by-step procedure documented to complete the installation of the second node of the vCenter Single Sign-On HA setup.

Task ID	Task Description	Screenshot
1.	Launch the VMware vSphere installer by clicking the autorun.exe .	
2.	From the VMware vSphere installer menu, select vCenter Single Sign-On . Click Install .	
3.	At the Welcome to the vCenter Single Sign-On Setup dialog, click Next .	

Task ID	Task Description	Screenshot
4.	<p>At the End-User License Agreement dialog, click the I accept the terms in the License Agreement check box.</p> <p>Click Next.</p>	
5.	<p>At the vCenter Single Sign-On Prerequisites Check dialog, the install wizard detects the system configuration.</p> <p>Verify that the FQDN and IP Address are correct.</p> <p>Because this the second node in the site, uncheck the Add domain_name as a native Active Directory identity source check box.</p> <p>Click Next.</p>	
6.	<p>At the vCenter Single Sign-On Information dialog for deployment modes, select High availability.</p> <p>Click Next.</p>	

Task ID	Task Description	Screenshot
7.	<p>At the vCenter Single Sign-On Information dialog for partner information, enter the following values:</p> <ul style="list-style-type: none"> • FQDN of the first Single Sign-On node in the Partner host name text box (sso1.vmware.local) • Password used for administrator@vsphere.local account during the first node installation in the Password text box <p>Click Next.</p>	 <p>The screenshot shows the 'vCenter Single Sign-On Information' dialog box. It contains four text input fields: 'Domain Name' (vsphere.local), 'Partner host name' (sso-01a.rainpole.local), 'User name' (Administrator), and 'Password' (masked with asterisks). At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.</p>
8.	<p>At the Partner certificate dialog, click Continue to accept the certificate.</p>	 <p>The screenshot shows the 'vCenter Single Sign-On Partner certificate' dialog box. It asks 'Do you trust the following certificate?' and displays the certificate details: 'Subject DN: VMWareDirectoryService,dc=vsphere,dc=local' and 'Sha1: 83:52:69:7f:36:20:01:10:03:f3:cc:b7:96:ba:9a:bc:63:2a:21:6e'. At the bottom, there are 'Back', 'Continue', and 'Cancel' buttons.</p>
9.	<p>At the vCenter Single Sign-On Join Site dialog, use the drop-down menu to select the vCenter Single Sign-On site you wish to join.</p> <p>Click Next.</p> <p>Note: The site name should match the site name specified in Step 8 in the Install vCenter SSO Server Node1 section.</p>	 <p>The screenshot shows the 'vCenter Single Sign-On Join Site' dialog box. It has a drop-down menu for 'Site name' with 'SiteA' selected. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.</p>

Task ID	Task Description	Screenshot
10.	<p>At the vCenter Single Sign-On Port Settings dialog, unless you have a requirement to alter the default HTTPS port, leave the default value of 7444.</p> <p>Click Next.</p>	
11.	<p>At the Change destination folder dialog, accept the default path by clicking Next.</p>	
12.	<p>At the vCenter Single Sign-On Information dialog for install options, review your selections.</p> <p>Click Install.</p>	

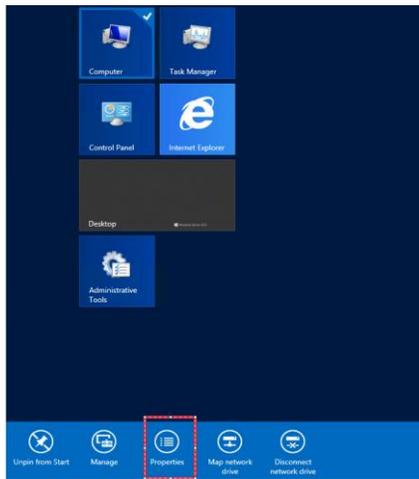
Task ID	Task Description	Screenshot
13.	At the Completed the vCenter Single Sign-On Setup Wizard dialog, click Finish .	

Set Up the vCenter Single Sign-On System Environment

During the configuration process there are numerous command line tasks that must be performed which by default require you to be positioned within the physical directory; this can be alleviated by simply performing a few simple environmental configuration steps within each vCenter Single Sign-On node. This section provides the steps to perform the following tasks:

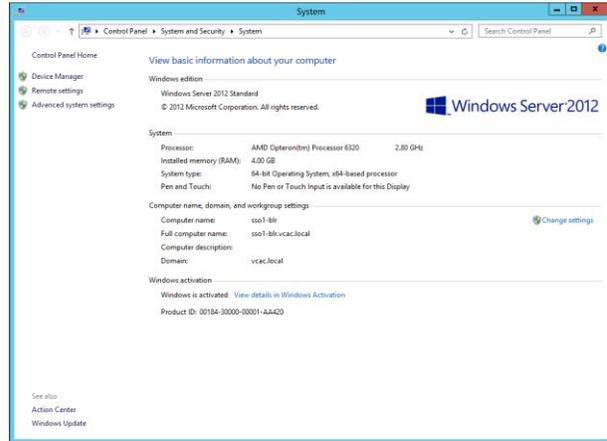
- Configure the JAVA_HOME system variable
- Add additional paths to the PATH system variable

Perform these steps on all SSO nodes (SSO node1 and SSO node2)

Task ID	Task Description	Screenshot
1.	<p>Launch the system properties by clicking Start.</p> <p>Then right click on Computer and select Properties from the menu.</p>	

Task ID	Task Description	Screenshot
---------	------------------	------------

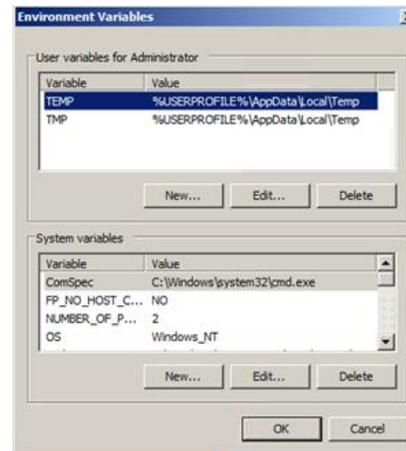
2. On the left-hand side, click **Advanced system settings**.

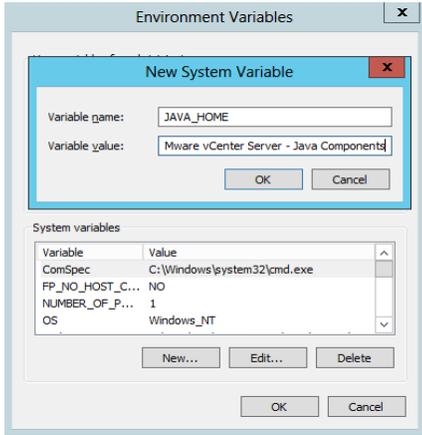
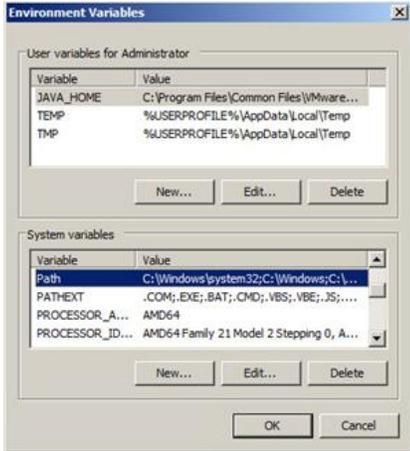
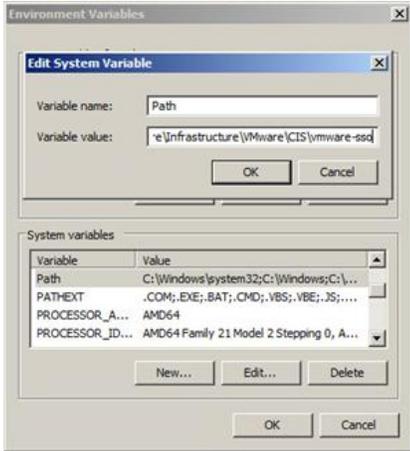


3. At the System Properties dialog, click **Environment Variables**.



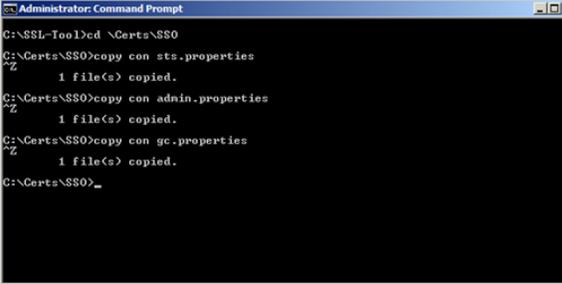
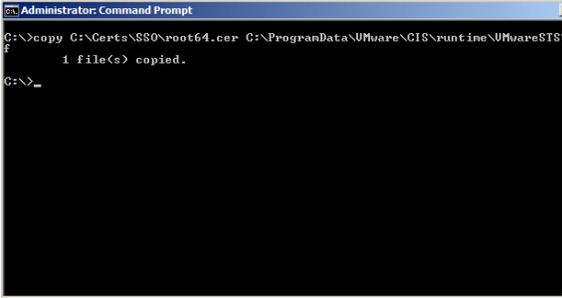
4. At the Environment Variables dialog, under **System variables**, click **New**.

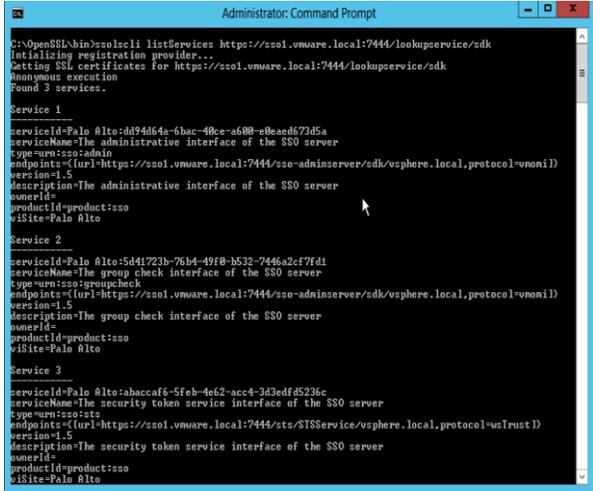


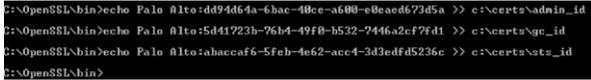
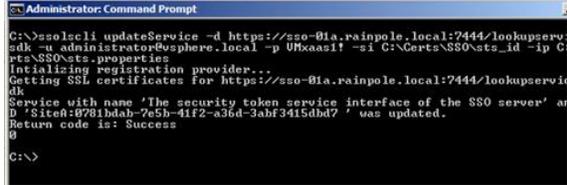
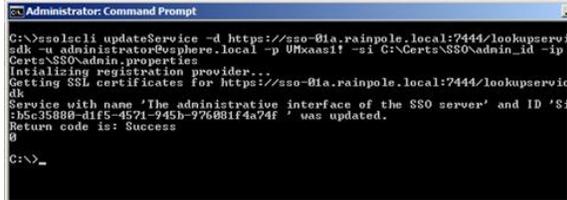
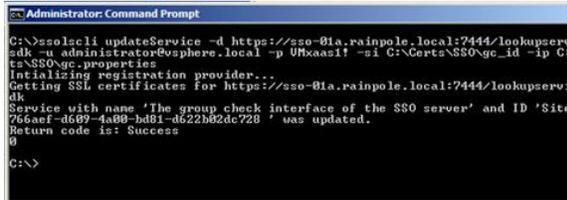
Task ID	Task Description	Screenshot
5.	<p>Create a new variable for the java home folder by entering the following details:</p> <ul style="list-style-type: none"> Enter JAVA_HOME in the Variable Name text box Enter the path C:\Program Files\Common Files\VMware\VMware vCenter Server - Java Components in the Variable Value text box <p>Click OK.</p>	
6.	<p>At the Environment Variables dialog under System variables, locate Path.</p> <p>Click Edit.</p>	
7.	<p>At the Edit System Variables dialog, within the Variable Values text box go to the end and add the following entries with a ; between each:</p> <ul style="list-style-type: none"> C:\Program Files\VMware\Infrastructure\VMware\CIS\vmware-ss %JAVA_HOME%\bin <p>Click OK three times to save and exit the Environment Variables dialog.</p>	

Update the vCenter SSO Services to the vCenter SSO Load Balancer FQDN on vCenter SSO Server Node1

We now need to create property files with the vCenter SSO load balancer FQDN (sso.vmware.local) and update the vCenter SSO services (STS, Admin and GroupCheck).

Task ID	Task Description	Screenshot
1.	<p>Open a command prompt and create three empty text files using the following commands:</p> <pre>cd C:\Certs\SSO copy con C:\Certs\SSO\sts.properties Press F6 and Enter copy con C:\Certs\SSO\admin.properties Press F6 and Enter copy con C:\Certs\SSO\gc.properties Press F6 and Enter</pre>	
2.	<p>Copy the root certificate to the VMware STS folder on both nodes using the following command:</p> <pre>copy C:\Certs\SSO\root64.cer C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\</pre>	
3.	<p>Edit the sts.properties file in a text editor and enter the details as they appear on the right. Save the file.</p>	<pre>[service] friendlyName=The security token service interface of the SSO server version=1.5 ownerId= type=urn:sso:sts description=The security token service interface of the SSO server [endpoint0] uri=https://sso.vmware.local:7444/sts/STS Service/vsphere.local ssl=C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\root64.cer protocol=wsTrust</pre>

Task ID	Task Description	Screenshot
4.	<p>Edit the admin.properties file in a text editor and enter the details as they appear on the right.</p> <p>Save the file.</p>	<pre>[service] friendlyName=The administrative interface of the SSO server version=1.5 ownerId= type=urn:sso:admin description= The administrative interface of the SSO server [endpoint0] uri=https://sso.vmware.local:7444/sso- adminserver/sdk/vsphere.local ssl=C:\ProgramData\VMware\CIS\runtime\VMw areSTS\conf\root64.cer protocol=vmomi</pre>
5.	<p>Edit the gc.properties file in a text editor and enter the details as they appear on the right.</p> <p>Save the file.</p>	<pre>[service] friendlyName=The group check interface of the SSO server version=1.5 ownerId= type=urn:sso:groupcheck description= The group check interface of the SSO server [endpoint0] uri=https://sso.vmware.local:7444/sso- adminserver/sdk/vsphere.local ssl=C:\ProgramData\VMware\CIS\runtime\VMw areSTS\conf\root64.cer protocol=vmomi</pre>
6.	<p>Using the sso1scli command, list the vCenter SSO services (STS, Admin and GroupCheck) to obtain their service IDs:</p> <pre>sso1scli listServices https://sso1.vmware.local:7444/look upservice/sdk</pre> <p>Capture the service ID for each service returned as the first field, will be displayed as:</p> <pre>serviceId=<SSOSiteName>:<thirty two digit hexadecimal value></pre>	

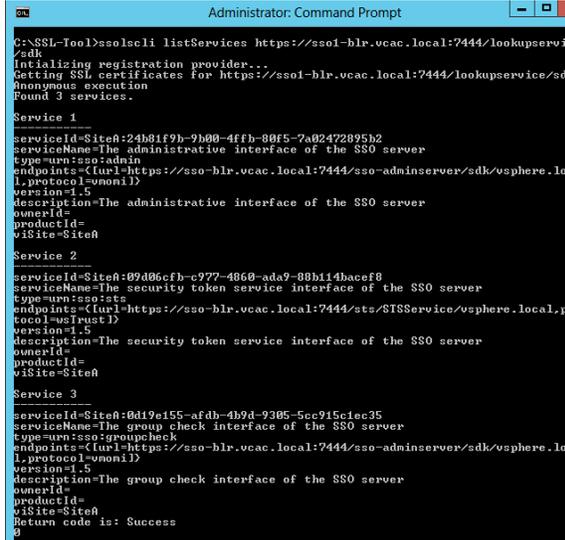
Task ID	Task Description	Screenshot
7.	Using the service IDs captured for vCenter SSO services (STS, Admin and GroupCheck) in step 6, run the following echo commands to capture the service IDs to a file for use in the service update steps:	 <pre> C:\OpenSSL\bin>echo Palo #1to:dd94d64a-6bac-48ce-a600-e0eae673d5a >> c:\certs\admin_id C:\OpenSSL\bin>echo Palo #1to:5d41723b-76b4-49f0-b532-7446a2cf7fd1 >> c:\certs\gc_id C:\OpenSSL\bin>echo Palo #1to:abaccaf6-5feb-4e62-acc4-3d3eafd5236c >> c:\certs\sts_id C:\OpenSSL\bin> </pre>
8.	Updating vCenter SSO services must be performed in the order stated within this document which is STS, Admin and GroupCheck.	
9.	Update the STS service by running the following command:	 <pre> ssolscli updateService -d https://sso-01a.rainpole.local:7444/lookupservice/sdk -u administrator@vsphere.local -p <password> -si C:\Certs\SSO\sts_id -ip C:\Certs\SSO\sts.properties </pre> <p>Note: Wait at least 30 seconds to allow the SSO nodes to sync.</p>
10.	Update the Admin service by running the following command:	 <pre> ssolscli updateService -d https://sso-01a.rainpole.local:7444/lookupservice/sdk -u administrator@vsphere.local -p <password> -si C:\Certs\SSO\admin_id -ip C:\Certs\SSO\admin.properties </pre> <p>Note: Wait at least 30 seconds to allow the SSO nodes to sync.</p>
11.	Update the Groupcheck service by running the following command:	 <pre> ssolscli updateService -d https://sso-01a.rainpole.local:7444/lookupservice/sdk -u administrator@vsphere.local -p <password> -si C:\Certs\SSO\gc_id -ip C:\Certs\SSO\gc.properties </pre> <p>Note: Wait at least 30 seconds to allow the SSO nodes to sync.</p>
12.	If you receive a Server certificate assertion not verified and thumbprint not matched error during update of vCenter SSO services, follow step 14 to restart the VMware Security Token Service and repeat the command.	

Task ID	Task Description	Screenshot
---------	------------------	------------

13. Verify that the vCenter SSO services (STS, Admin and GroupCheck) have been updated on SSO Node1 to the VCenter SSO load balancer FQDN by running the following command:

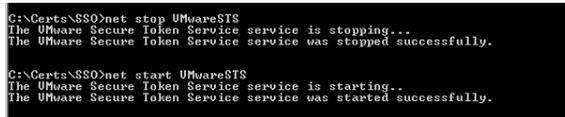
```
ssolscli listServices
https://sso1.vmware.local:7444/look
upservice/sdk
```

Note: The endpoints entry should now show the vCenter SSO load balancer URL (sso.vmware.local) for each service.



14. Restart the VMwareSTS service by running the following commands:

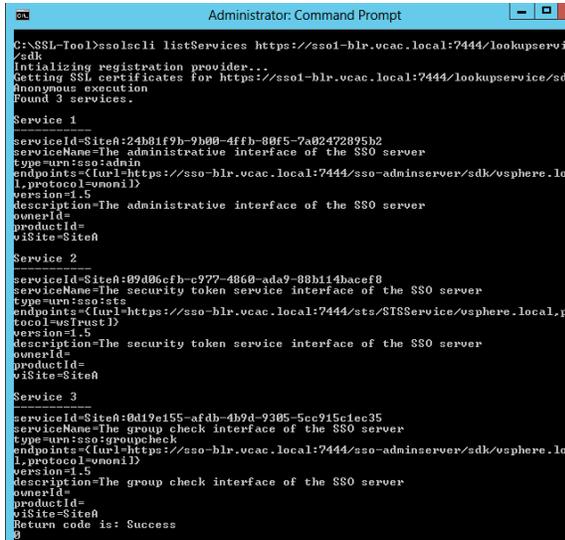
```
net stop VMwareSTS
net start VMwareSTS
```



15. Verify that the vCenter SSO Node1 responds with the correct vCenter SSO services information by running the following command:

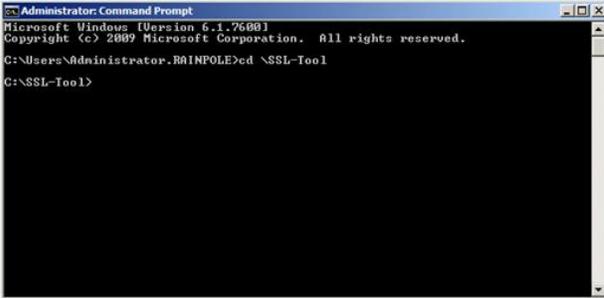
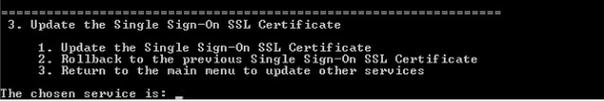
```
ssolscli listServices
https://sso1.vmware.local:7444/look
upservice/sdk
```

Note: The endpoints entry should now show the vCenter SSO load balancer URL (sso.vmware.local) for each service.



Updating Certificates on vCenter SSO Server Node1

Now we must update the certificates on the first vCenter SSO node before we can reconfigure the remaining services. This procedure is performed using the VMware vCenter Certificate Automation Tool on both SSO nodes, which can be obtained from the VMware Download Center and is located in the Drivers and Tools section of the vSphere and vCloud Suite download pages (version: 5.5).

Task ID	Task Description	Screenshot
1.	<p>Open a command prompt and go to the VMware vCenter Certificate Automation Tool directory (for this example the files were extracted to the C:\SSL-Tool folder).</p> <pre>cd C:\SSL-Tool</pre>	
2.	<p>Start the SSL Updater tool by running the following command:</p> <pre>ssl-updater.bat</pre> <p>The main menu appears.</p> <p>Type 3, and then press Enter.</p>	
3.	<p>The Update the Single Sign-On SSL Certificate menu appears.</p> <p>Type 1, and then press Enter.</p>	
4.	<p>You are presented with a series of questions about your environment.</p> <p>Sample responses are shown in red and boldface type; use these values as guidelines for your responses and alter them as needed for your environment.</p>	<pre>Enter location to the new Single Sign-On SSL chain: C:\Certs\SSO\chain.pem Enter location to the new Single Sign-On private key: C:\Certs\SSO\rui.key Enter Single Sign-On Administrator user: administrator@vsphere.local Enter Single Sign-On Administrator password: <password> Do you have a load balancer installed?: yes Is the current machine hosting a primary Single Sign-On node?: yes Is the Single Sign-On administration services accessed via the load balancer?: yes Enter the Single Sign-On HA Load Balancer certificate: C:\Certs\SSO\sso.cer Enter the Single Sign-On HA Load Balancer hostname: sso.vmware.local</pre>

Task ID	Task Description	Screenshot
---------	------------------	------------

5. When the process finishes, the status message Last operation update Single Sign-On SSL certificates completed successfully appears.
- Type **3** at the prompt, and press **Enter** to return to the main menu.

```
Administrator: Command Prompt - ssl-updater.bat
[.] Waiting for service VMwareSTS to stop, 15 seconds.
[.] Service did stop successfully.
[.] Updating service container configuration
[.] Updating the SSO endpoints in the Lookup Service.
[.] This is Single Sign-On HA failover node. No endpoints are served directly fr
on here.
[.] Lookup Service records updated successfully.
[.] The vCenter Single Sign-On service is not currently running but it was in th
e beginning. Starting it.
[.] Waiting for service VMwareSTS to start, 15 seconds.
[.] Service did start successfully.
(17/03/2014 - 14:15:37.50): Last operation update Single Sign-On SSL certificate
completed successfully.
(17/03/2014 - 14:15:37.51): Go to the next step in the plan that was received fr
om Update Steps Planner.
-----
3. Update the Single Sign-On SSL Certificate
    1. Update the Single Sign-On SSL Certificate
    2. Rollback to the previous Single Sign-On SSL Certificate
    3. Return to the main menu to update other services
-----
The chosen service is:
```

6. Type **9** at the main menu prompt and press **Enter** to exit the SSL Update tool.

```
Administrator: Command Prompt - ssl-updater.bat
-----
3. Update the Single Sign-On SSL Certificate
    1. Update the Single Sign-On SSL Certificate
    2. Rollback to the previous Single Sign-On SSL Certificate
    3. Return to the main menu to update other services
-----
The chosen service is: 3
-----
Main menu
Enter the action you want to run
    1. Plan your steps to update SSL certificates(Update Steps Planner)
    2. Generate Certificate Signing Request
    3. Update Single Sign-On
    4. Update Inventory Service
    5. Update vCenter Server
    6. Update vCenter Orchestrator(vCO)
    7. Update vSphere Web Client and Log Browser
    8. Update vSphere Update Manager(UM)
    9. End the update process and exit
-----
The chosen action is: 9
```

7. Verify that the vCenter SSO Node1 responds with the correct vCenter SSO services information by running the following command:

```
ssolscli listServices
https://sso1.vmware.local:7444/lookup
service/sdk
```

Note: The endpoints entry should now show the vCenter SSO load balancer URL (sso.vmware.local) for each service.

```
Administrator: Command Prompt
C:\SSL-Tool>ssolscli listServices https://sso1-blr.vcac.local:7444/lookupservice
/sdk
Initializing registration provider...
Getting SSL certificates for https://sso1-blr.vcac.local:7444/lookupservice/sdk
Anonymous execution
Found 3 services.
-----
Service 1
serviceId=SiteA:24b81f9b-9b00-4ffb-80f5-7a02472895b2
serviceName=The adminstrative interface of the SSO server
type=urn:sso:admin
endpoints=(url=https://sso-blr.vcac.local:7444/sso-adminserver/sdk/vsphere.local
l.protocol=monil)
version=1.5
description=The administrative interface of the SSO server
ownerId=
productId=
vSite=SiteA
-----
Service 2
serviceId=SiteA:09d06cfb-c977-4860-ada9-88b114bacef8
serviceName=The security token service interface of the SSO server
type=urn:sso:sts
endpoints=(url=https://sso-blr.vcac.local:7444/sts/STSService/vsphere.local.pr
otocol=monil)
version=1.5
description=The security token service interface of the SSO server
ownerId=
productId=
vSite=SiteA
-----
Service 3
serviceId=SiteA:0d19e155-afdb-4b9d-9305-5cc915c1ec35
serviceName=The group check interface of the SSO server
type=urn:sso:groupcheck
endpoints=(url=https://sso-blr.vcac.local:7444/sso-adminserver/sdk/vsphere.local
l.protocol=monil)
version=1.5
description=The group check interface of the SSO server
ownerId=
productId=
vSite=SiteA
Return code is: Success
0
```

Task ID	Task Description	Screenshot
---------	------------------	------------

8. Verify that the vCenter SSO load balancer FQDN responds with the correct vCenter SSO services information by running the following command:
- ```
ssolscli listServices
https://sso.vmware.local:7444/lookupservice/sdk
```

**Note:** The endpoints entry should now show the vCenter SSO load balancer URL (sso.vmware.local) for each service.

```
Administrator: Command Prompt
C:\SSL-Tool>ssolscli listServices https://sso-blr.vcac.local:7444/lookupservice/sdk
Initializing registration provider...
Setting SSL certificates for https://sso-blr.vcac.local:7444/lookupservice/sdk
Anonymous execution
Found 3 services.

Service 1

serviceId=SiteA:24b1f9b-9b00-4ffb-00f5-7a02472095b2
serviceName=The administrative interface of the SSO server
type=urn:sso:admin
endpoints=(url=https://sso-blr.vcac.local:7444/sso-adminserver/sdk/vsphere.local.protocol.vmonil)
version=1.5
description=The administrative interface of the SSO server
ownerId=
productId=
visite=SiteA

Service 2

serviceId=SiteA:09d06cfb-c977-4860-ada9-88b114bacef8
serviceName=The security token service interface of the SSO server
type=urn:sso:sts
endpoints=(url=https://sso-blr.vcac.local:7444/sts/STSService/vsphere.local.protocol.wstrust)
version=1.5
description=The security token service interface of the SSO server
ownerId=
productId=
visite=SiteA

Service 3

serviceId=SiteA:0d19e155-afdb-4b9d-9305-5cc915c1ec35
serviceName=The group check interface of the SSO server
type=urn:sso:groupcheck
endpoints=(url=https://sso-blr.vcac.local:7444/sso-adminserver/sdk/vsphere.local.protocol.vmonil)
version=1.5
description=The group check interface of the SSO server
ownerId=
productId=
visite=SiteA
Return code is: Success
0
```

9. Verify that the vCenter SSO Node2 responds with the correct vCenter SSO services information by running the following command:
- ```
ssolscli listServices
https://sso2.vmware.local:7444/lookupservice/sdk
```

Note: The endpoints entry should now show the vCenter SSO load balancer URL (sso2.vmware.local) for each service.

```
Administrator: Command Prompt
C:\SSL-Tool>ssolscli listServices https://sso2-blr.vcac.local:7444/lookupservice/sdk
Initializing registration provider...
Setting SSL certificates for https://sso2-blr.vcac.local:7444/lookupservice/sdk
Anonymous execution
Found 3 services.

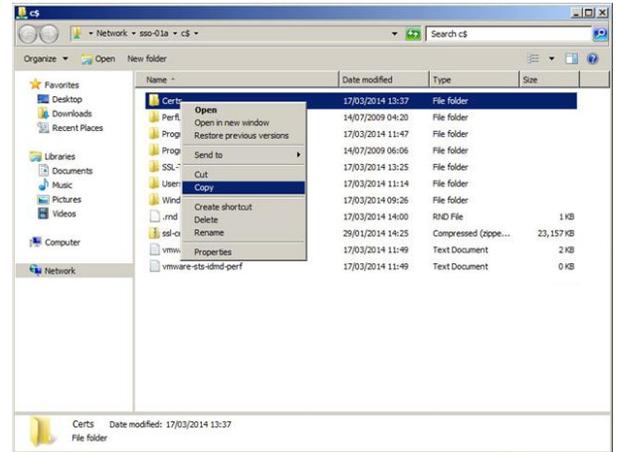
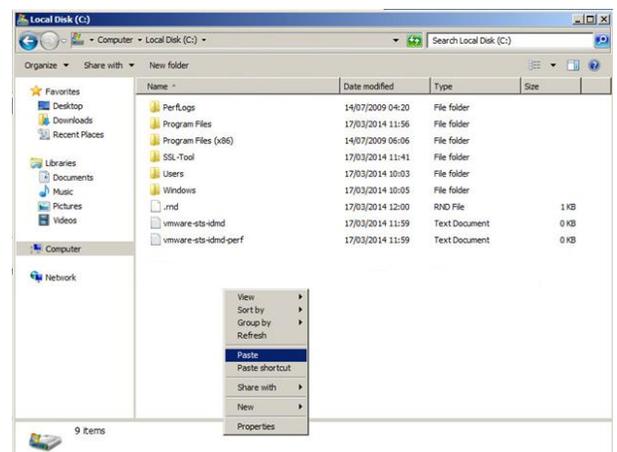
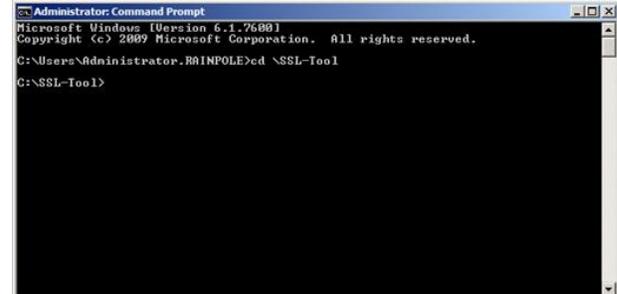
Service 1
-----
serviceId=SiteA:24b1f9b-9b00-4ffb-00f5-7a02472095b2
serviceName=The administrative interface of the SSO server
type=urn:sso:admin
endpoints=(url=https://sso-blr.vcac.local:7444/sso-adminserver/sdk/vsphere.local.protocol.vmonil)
version=1.5
description=The administrative interface of the SSO server
ownerId=
productId=
visite=SiteA

Service 2
-----
serviceId=SiteA:09d06cfb-c977-4860-ada9-88b114bacef8
serviceName=The security token service interface of the SSO server
type=urn:sso:sts
endpoints=(url=https://sso-blr.vcac.local:7444/sts/STSService/vsphere.local.protocol.wstrust)
version=1.5
description=The security token service interface of the SSO server
ownerId=
productId=
visite=SiteA

Service 3
-----
serviceId=SiteA:0d19e155-afdb-4b9d-9305-5cc915c1ec35
serviceName=The group check interface of the SSO server
type=urn:sso:groupcheck
endpoints=(url=https://sso-blr.vcac.local:7444/sso-adminserver/sdk/vsphere.local.protocol.vmonil)
version=1.5
description=The group check interface of the SSO server
ownerId=
productId=
visite=SiteA
Return code is: Success
0
```

Updating Certificates on vCenter SSO Server Node2

We can now update the certificates on the second vCenter SSO node by following the procedure below.

Task ID	Task Description	Screenshot
1.	Copy the C:\Certs\SSO folder from vCenter SSO node1 to node2.	 
2.	Open a command prompt and go to the VMware vCenter Certificate Automation Tool directory (for this example the files were extracted to the C:\SSL-Tool folder). cd C:\SSL-Tool	

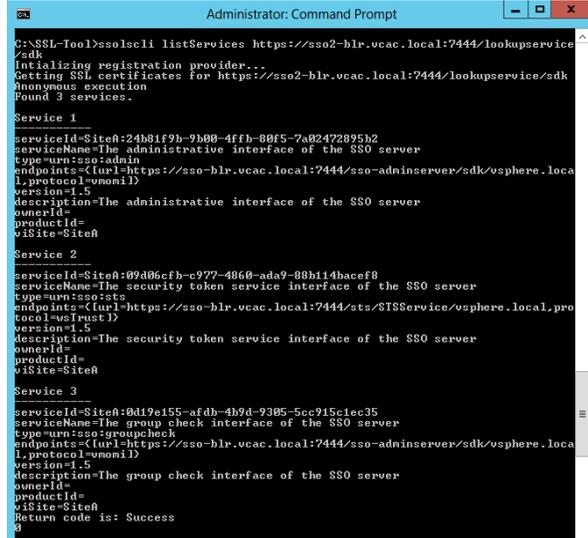
Task ID	Task Description	Screenshot
3.	<p>Start the SSL Updater tool by running the following command:</p> <pre>ssl-updater.bat</pre> <p>The main menu appears.</p> <p>Type 3, and then press Enter.</p>	<pre>C:\SSL-Tool>ssl-updater.bat ===== Main menu Enter the action you want to run 1. Plan your steps to update SSL certificates(Update Steps Planner) 2. Generate Certificate Signing Requests 3. Update Single Sign-On 4. Update Inventory Service 5. Update vCenter Server 6. Update vCenter Orchestrator(vCO) 7. Update vSphere Web Client and Log Browser 8. Update vSphere Update Manager(UM) 9. End the update process and exit The chosen action is: 3</pre>
4.	<p>The Update the Single Sign-On SSL Certificate menu appears.</p> <p>Type 1, and then press Enter.</p>	<pre>===== 3. Update the Single Sign-On SSL Certificate 1. Update the Single Sign-On SSL Certificate 2. Rollback to the previous Single Sign-On SSL Certificate 3. Return to the main menu to update other services The chosen service is: 1</pre>
5.	<p>You are presented with a series of questions about your environment.</p> <p>Sample responses are shown in red and boldface type; use these values as guidelines for your responses and alter them as needed for your environment.</p> <p>Note: Remember that this is not a primary node.</p>	<p>Enter location to the new Single Sign-On SSL chain: C:\Certs\SSO\chain.pem</p> <p>Enter location to the new Single Sign-On private key: C:\Certs\SSO\rui.key</p> <p>Enter Single Sign-On Administrator user: administrator@vsphere.local</p> <p>Enter Single Sign-On Administrator password: <password></p> <p>Do you have a load balancer installed?: yes</p> <p>Is the current machine hosting a primary Single Sign-On node?: no</p> <p>Is the Single Sign-On administration services accessed via the load balancer?: yes</p> <p>Enter the Single Sign-On HA Load Balancer certificate: C:\Certs\SSO\sso.cer</p> <p>Enter the Single Sign-On HA Load Balancer hostname: sso.vmware.local</p>
6.	<p>When the process finishes, the status message Last operation update Single Sign-On SSL certificates completed successfully appears.</p> <p>Type 3 at the prompt, and press Enter to return to the main menu.</p>	<pre>Administrator: Command Prompt - ssl-updater.bat [.] Waiting for service VMwareSTS to stop, 15 seconds. [.] Service did stop successfully. [.] Updating service container configuration [.] Updating the SSO endpoints in the Lookup Service. [.] This is Single Sign-On HA Failover node. No endpoints are served directly from here. [.] Lookup Service records updated successfully. [.] The vCenter Single Sign-On service is not currently running but it was in the beginning. Starting it. [.] Waiting for service VMwareSTS to start, 15 seconds. [.] Service did start successfully. [17/03/2014 - 14:15:37,501]: Last operation update Single Sign-On SSL certificate completed successfully. [17/03/2014 - 14:15:37,511]: Go to the next step in the plan that was received from Update Steps Planner. ===== 3. Update the Single Sign-On SSL Certificate 1. Update the Single Sign-On SSL Certificate 2. Rollback to the previous Single Sign-On SSL Certificate 3. Return to the main menu to update other services The chosen service is: 3</pre>
7.	<p>Type 9 at the main menu prompt and press Enter to exit the SSL Update tool.</p>	<pre>Administrator: Command Prompt - ssl-updater.bat ===== 3. Update the Single Sign-On SSL Certificate 1. Update the Single Sign-On SSL Certificate 2. Rollback to the previous Single Sign-On SSL Certificate 3. Return to the main menu to update other services The chosen service is: 3 ===== Main menu Enter the action you want to run 1. Plan your steps to update SSL certificates(Update Steps Planner) 2. Generate Certificate Signing Requests 3. Update Single Sign-On 4. Update Inventory Service 5. Update vCenter Server 6. Update vCenter Orchestrator(vCO) 7. Update vSphere Web Client and Log Browser 8. Update vSphere Update Manager(UM) 9. End the update process and exit The chosen action is: 9</pre>

Task ID	Task Description	Screenshot
---------	------------------	------------

8. Verify that the vCenter SSO Node2 responds with the correct vCenter SSO services information by running the following command:

```
ssolscli listServices
https://sso2.vmware.local:7444/lookupservice/sdk
```

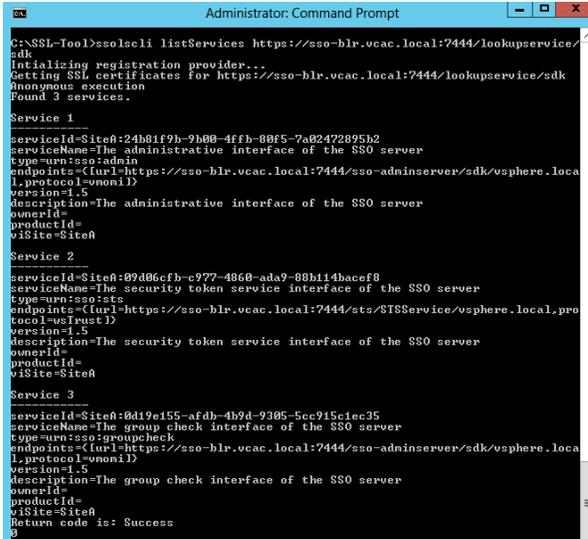
Note: The endpoints entry should now show the vCenter SSO load balancer URL (sso.vmware.local) for each service.



9. Verify that the vCenter SSO load balancer FQDN responds with the correct vCenter SSO services information by running the following command:

```
ssolscli listServices
https://sso2.vmware.local:7444/lookup service/sdk
```

Note: The endpoints entry should now show the vCenter SSO load balancer URL (sso.vmware.local) for each service.



10. Test vCenter SSO automatic failover by shutting down vCenter SSO Node1. You can simulate the node1 down scenario by updating the node1s state to Forced Offline from F5 load balancer Admin UI. Repeat steps 8 and 9.

Configure an HA Deployment of vCenter SSO 5.5 for Integration with vRealize Automation

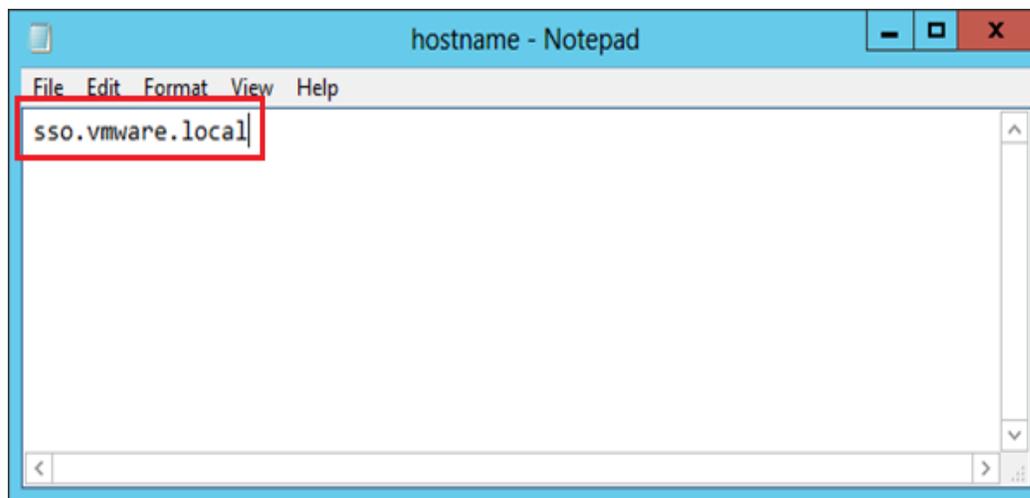
This procedure is used to configure a high availability (HA) deployment of vCenter SSO 5.5 for integration with vRealize Automation. You must use a supported version of vCenter SSO 5.5 U2.

Before you begin, back up or take a snapshot of all vCenter SSO nodes.

Edit the `hostname.txt` and `server.xml` Files

Edit the `hostname.txt` and `server.xml` files for each vCenter SSO node to specify new host name and proxy information.

1. Locate and open the `hostname.txt` file in the `C:\ProgramData\VMware\CIS\cfg\vmware-ss0` directory.
2. Replace the hostname with the fully qualified domain name (FQDN) for the vCenter SSO load balancer, as shown in the following example:



3. Locate and open the `server.xml` file in the `C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf` directory.
4. Locate the element `<Connector SSLEnabled="true">` and add the following attributes:

```
proxyName="sso.vmware.local"  
proxyPort="7444"
```



```

server - Notepad
File Edit Format View Help
connectionTimeout="20000"
executor="tomcatThreadPool"
maxKeepAliveRequests="-1"
port="{bio-custom.http.port}"
protocol="org.apache.coyote.http11.Http11Protocol"
redirectPort="{bio-custom.https.port}"/>
<Connector SSLEnabled="true"
proxyName="sso.vmware.local"
proxyPort="7444"
acceptCount="200"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA"
connectionTimeout="20000"
executor="tomcatThreadPool"
keyAlias="ssoserver"
keystoreFile="{catalina.base}/conf/ssoserver.p12"

```

5. Repeat these steps for each vCenter SSO node.

Replace the STS Certificate and Reinstall the STS Component

Replace the STS Signing Certificate on all additional vCenter SSO nodes with that of the first vCenter SSO node. Perform the following steps on all vCenter SSO nodes except the first vCenter SSO node.

1. Open a Windows Explorer window and go to **C:\ProgramData\VMware\CIS\cfg\vmware-ss0** on second vCenter SSO node.
2. Create a new folder named **backup**.
3. Copy the files in the **ss0** folder to the **backup** folder.
4. Copy the following files in the **C:\ProgramData\VMware\CIS\cfg\vmware-ss0** directory from the first vCenter SSO node to the second vCenter SSO node (replace the files if prompted).

```

ssoserverRoot.crt
ssoserverSign.crt
ssoserverSign.pub
ssoserverSign.key

```

5. Stop STS and Identity Management services by opening a command prompt and entering the following commands:

```

net stop VMwareSTS
net stop VMwareIdentityMgmtService

```

6. Use Jxplorer to connect to LDAP on the second vCenter SSO node.

You can download and install JXplorer from <http://jxplorer.org/downloads>.

Use the following selections to establish a connection.

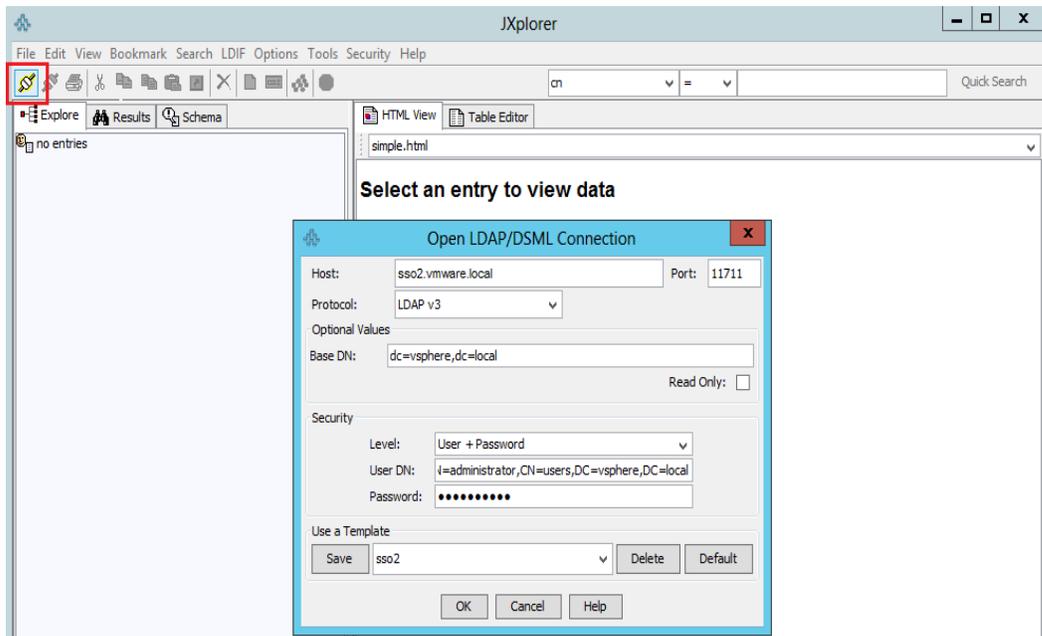
```

Host:    sso2.vmware.local
Port:    11711
Protocol: <use the default>
Base DN: DC=vsphere,DC=local
Level:   User + Password

```

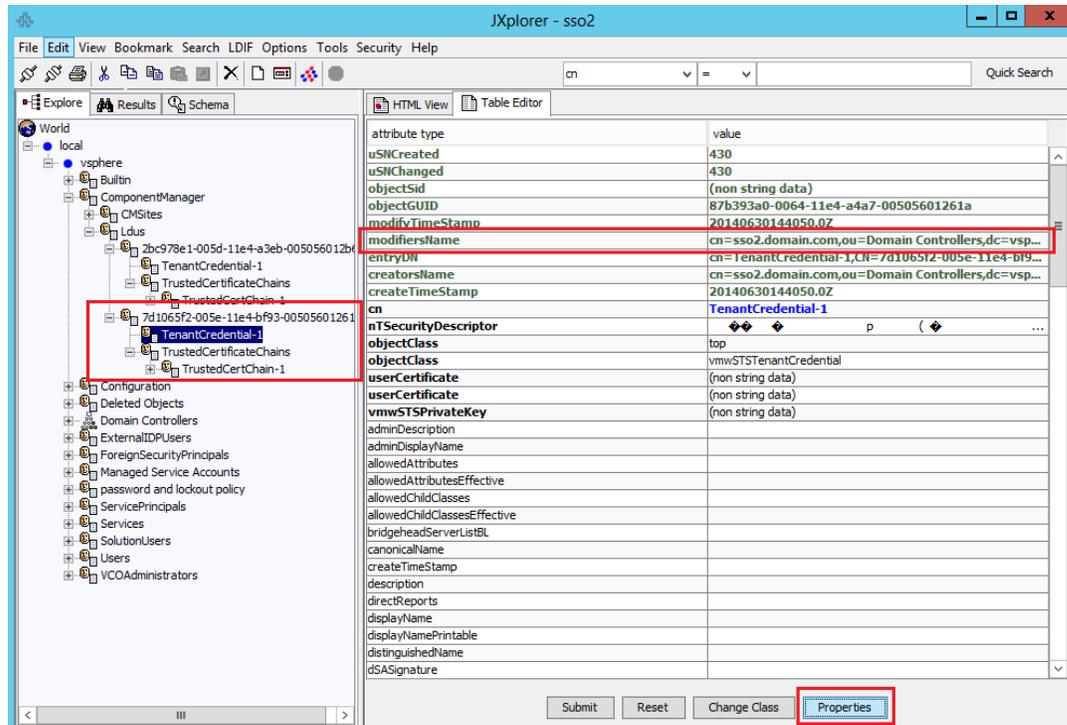
User DN: CN=adminimator, CN=users, DC=vsphere, DC=local

Password: <password>



7. Locate the STS Certificate records for the second vCenter SSO node and delete the TenantCredential-1 and TrustedCertChain-1 attributes.
 - a. Select **local>vsphere>ComponentManager>Ldus**. Each SSO node is listed.
 - b. Expand the entries under **Ldus**.
 - c. Select **TenantCredential-1** for the second node,
 - d. Click **Properties**.
 - e. From the **Table Editor** tab, locate the **modifiersName** attribute. Check that the value matches the second vCenter SSO node to confirm that this is the second vCenter SSO. If it is not, continue checking entries under **Ldus**.
 - f. Delete the **TenantCredential-1** entry that references the second vCenter SSO node.
 - g. Expand **TrustedCertificateChains** and select **TrustedCertChain-1** for the second vCenter SSO node.
 - h. Click **Properties**.
 - i. From the **Table Editor** tab, locate the **modifiersName** attribute. Check that the value matches the second vCenter SSO node.
 - j. Delete the **TrustedCertChain -1** entry.

Note: Repeat this process for every vCenter SSO node except for the first node.



8. Start the Identity Management Service by opening a command prompt and typing the following command.

```
net start VMwareIdentityMgmtService
```

9. Reinstall the STS component using the following procedure.

- Open a command prompt and navigate to C:\ProgramData\VMware\CIS\cfg\vmware-ss0.
- Cut and paste the following command to your command prompt. Note that this is a single command.

```
"c:\Program Files\Common Files\VMware\VMware vCenter Server - Java
Components\bin\java.exe" -cp "c:\Program
Files\VMware\Infrastructure\VMware\CIS\vmware-ss0\*;c:\Program
Files\VMware\Infrastructure\VMware\CIS\vmware-ss0\lib\*;.*"
com.vmware.identity.installer.STSInstaller --install --root-cert-path
ssoserverRoot.crt --cert-path ssoserverSign.crt --private-key-path
ssoserverSign.key --retry-count 2 --retry-interval 30
```

10. Verify that the command returns a success message.

```
Administrator: C:\Windows\system32\cmd.exe
C:\ProgramData\VMware\GIS\cfg\vmware-ssolib>"c:\Program Files\Common Files\VMware\VMware vCenter Server - Java Components\bin\java.exe" -cp "c:\Program Files\VMware\Infrastructure\VMware\GIS\vmware-ssolib\*;.*" com.vmware.identity.installer.STSInstaller --install --root-cert-path ssoserverRoot.crt --cert-path ssoserverSign.crt --private-key-path ssoserverSign.key --retry-count 2 --retry-interval 30
Installing VMware STS...
Successfully installed VMware STS.
C:\ProgramData\VMware\GIS\cfg\vmware-ssolib>
```

11. Open a command prompt and enter the following command to start the STS Service.

```
net start VMwareSTS
```

12. For all nodes, run the following command to verify that the vCenter SSO services are running and reference the vCenter SSO load balancer URL.

```
ssolscli listServices https://sso2.vmware.local:7444/lookupservice/sdk
```

Validate the vCenter SSO Configuration

Verify that certificates are correctly updated for all vCenter SSO nodes in the HA deployment, including the first node.

Perform the following steps for each vCenter SSO node.

1. Download and open the file <https://<ssonode>:7444/webssso/SAML2/Metadata/vsphere.local>, where <ssonode> represents the SSO node server name
2. Verify that the value for <ds:x509Certificate> is the same for all SSO nodes.
3. Verify that each **Location** attribute uses the FQDN for the load balancer and not the hostname of the node <https://sso.vmware.local:7444/>.

Configure vRealize Automation to Use vCenter SSO

Configure the SSO settings that the vRealize Appliance uses to interact with the vCenter SSO. You must use a supported version of vCenter SSO 5.5.

1. Deploy the vRealize appliances as described in the vRealize Automation *Installation and Configuration Guide*, available at <https://www.vmware.com/support/pubs/vcac-pubs.html>.
2. Configure the vRealize Appliance as described in the topic “Configure the vRealize Appliance” in the vRealize Automation *Installation and Configuration Guide*.

When you configure SSO settings, provide the FQDN and port for the vCenter SSO load balancer in the **SSO Host and Port** text box. For example: sso.vmware.local:7444.

The screenshot shows the VMware vCAC Appliance configuration interface. The top navigation bar includes tabs for Services, System, vCAC Settings (selected), Network, Update, IaaS install, and Admin. The vCAC Settings tab is active, and the SSO sub-tab is selected. The SSO Settings page displays a warning: "WARNING! Certificate's Common Name doesn't match vCloud Automation Center Server host name." Below the warning are input fields for SSO Host and Port* (sso.vmware.local:7444), SSO Default Tenant* (vsphere.local), SSO Admin User* (administrator@vsphere.local), and SSO Admin Password* (masked with asterisks). There are "Save Settings" and "Refresh" buttons. At the bottom, the SSO Status is shown as "Connected" with detailed information about the vCenter SSO connection.

3. After you configure the appliance, verify that you can log in to the vRealize Automation console.
 - a. Open a browser and go to <https://vcac-hostname.domain.name/vcac/>.
 - b. If you are prompted, continue past the certificate warnings.
 - c. Login with administrator@vsphere.local and the password that you specified when you configured the single sign-on server.
4. Verify that automatic failover is working.
 - a. Shut down vCenter SSO node1. You can do this from the F5 administrator user interface by changing the node state to **Forced Offline**.
 - b. Repeat step 3 to confirm that you can login to vRealize Automation console after automatic failover of vCenter SSO node1 to node2.

This completes the configuration and integration of vCenter SSO 5.5 U2 with vRealize Automation in a high-availability environment.

About the Authors

Muzibur Shaik and Amrainder Singh are Staff Engineers at VMware in the vRealize Automation group.

Acknowledgements

VMware would like to acknowledge the following individuals for their contributions to this paper and help with content review:

vRealize Automation – Carl Prahla and Jitender Uppal

Technical Documentation – Sally Hehir

References

Portions of this whitepaper are based on [VMware vCenter Server 5.5 Deploying a Centralized vCenter Single Sign-On Server with a Network Load Balancer \(NLB\)](#) by Justin King and Mike Brown, VMware Technical Marketing



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2014 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2014 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.