VMware® vCenter Server™ 5.5

Deploying a Centralized VMware vCenter™ Single Sign-On™ Server with a Network Load Balancer

Technical Reference

TECHNICAL MARKETING DOCUMENTATION
V 1.0/FEBRUARY 2014/JUSTIN KING, MIKE BROWN

vmware®

Table of Contents

Overview

With the release of VMware vSphere® 5.5 and VMware® vCenter Server™ 5.5, multiple components deliver the vCenter Server management solution. One component, VMware vCenter™ Single Sign-On™ server, offers an optional deployment configuration that enables the centralization of vCenter Single Sign-On services for multiple local solutions such as vCenter Server. If not architected correctly, centralization can increase risk, so use of vCenter Single Sign-On server is highly recommended.

This paper highlights the high-availability options for a centralized vCenter Single Sign-On environment and provides a reference guide for deploying one of the more common centralized vCenter Single Sign-On configurations with an external network load balancer (NLB).

When to Centralize vCenter Single Sign-On Server

VMware highly recommends deploying all vCenter Server components into a single virtual machine—excluding the vCenter Server database. However, large enterprise customers running many vCenter Server instances within a single physical location can simplify vCenter Single Sign-On architecture and management by reducing the footprint and required resources and specifying a dedicated vCenter Single Sign-On environment for all resources in each physical location.

For vSphere 5.5, as a general guideline, VMware recommends centralization of vCenter Single Sign-On server when eight or more vCenter Server instances are present in a given location.

Centralized vCenter Single Sign-On Architecture

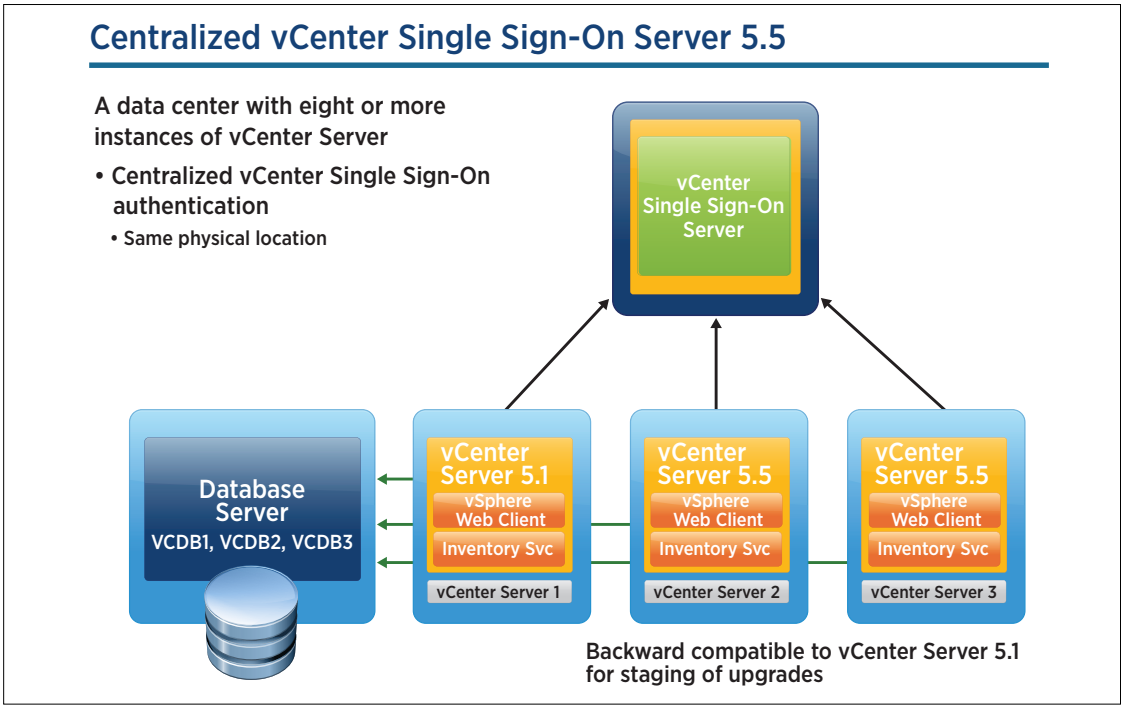

Figure 1. A Centralized vCenter Single Sign-On Server Environment

Centralized Single Sign-On High-Availability Options

The absence of vCenter Single Sign-On server greatly impacts the management, accessibility, and operations within a vSphere environment. The type of availability required is based on the user's recovery time objective (RTO), and VMware solutions can offer various levels of protection.

VMware vSphere Data Protection

VMware vSphere Data Protection™ provides a disk-level backup-and-restore capability utilizing storage-based snapshots. With the release of vSphere Data Protection 5.5, VMware now provides the option of host-level restore. Users can back up vCenter Single Sign-On server virtual machines using vSphere Data Protection and can restore later as necessary to a specified vSphere host.

VMware vSphere High Availability

When deploying a centralized vCenter Single Sign-On server to a vSphere virtual machine environment, users can also deploy VMware vSphere High Availability (vSphere HA) to enable recovery of the vCenter Single Sign-On server virtual machines. vSphere HA monitors virtual machines via heartbeats from the VMware Tools™ package, and it can initiate a reboot of the virtual machine when the heartbeat no longer is being received or when the vSphere host has failed.

VMware vCenter Server Heartbeat

VMware vCenter Server Heartbeat™ provides a richer availability model for the monitoring and redundancy of vCenter Server and its components. It places a centralized vCenter Single Sign-On server into an active–passive architecture, monitors the application, and provides an up-to-date passive node for recovery during a vSphere host, virtual machine, or application failure.

Network Load Balancer

A VMware or third-party NLB can be configured to allow SSL pass-through communications to a number of local vCenter Single Sign-On server instances and provide a distributed and redundant vCenter Single Sign-On solution. Although VMware provides NLB capability in some of its optional products, such as VMware vCloud® Networking and Security™, there also are third-party solutions available in the marketplace. VMware does not provide support for third-party NLB solutions.

Deploying vCenter Single Sign-On Server with a Network Load Balancer

Preinstallation Checklist

The guidance provided within this document will reference the following details:

	Host Name	FQDN	IP Address
Load Balancer	SSO	sso.vmware.local	192.168.110.40
SSO Server 01	SSO1	sso1.vmware.local	192.168.110.41
SSO Server 02	SSO2	sso2.vmware.local	192.168.110.42

Table 1. Centralized vCenter Single Sign-On Requirements

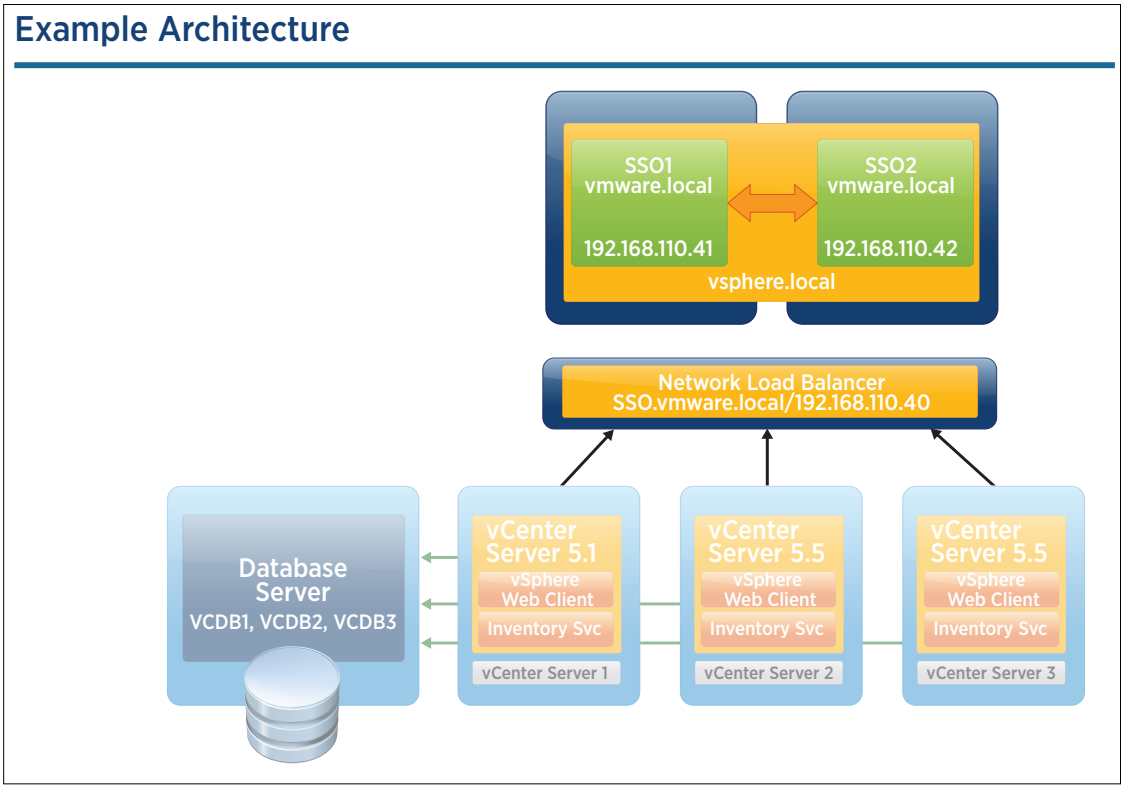

Figure 2. Example of a vCenter Single Sign-On Server with a Network Load Balancer

The following steps must be completed before installing the vCenter Single Sign-On server and configuring for use with an NLB:

1. **Download the vCenter Server distribution.**

   The vCenter Server binaries located on the vCenter Server ISO are required to install vCenter Single Sign-On server.

NOTE: vCenter Server 5.5.0b Build 1476387 is the latest version available and is used throughout this document.

2. **Deploy virtual machines.**

   With a configuration similar to that in Figure 2, deploy at least two appropriately sized virtual machines running Microsoft Windows 2008 SP2 or higher.

Minimum Hardware Requirements for vCenter Single Sign-On, Running on a Separate Host Machine from vCenter Server

vCenter Single Sign-On Hardware	Requirement
Processor	Intel or AMD x64 processor with two or more logical cores, each with a speed of 2GHz.
Memory	3GB. If vCenter Single Sign-On runs on the same host machine as vCenter Server, see Minimum Hardware Requirements for Simple Install Deployment of vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server or Minimum Hardware Requirements for vCenter Server.
Disk storage	2GB.
Network speed	1Gbps

Table 2. Minimum Hardware Requirements for vCenter Single Sign-On Server

NOTE: As of February 2014, Windows 2012 R2 is not a supported operating system (OS) for vCenter Single Sign-On server.

3. **Install the Microsoft Visual C++ 2008 Redistributable Package.**

   We will use OpenSSL to request the vCenter Single Sign-On certificates. The OpenSSL tool has a dependency on the Microsoft Visual C++ 2008 Redistributable Package (32-bit), which can be downloaded and installed from the following: http://www.microsoft.com/en-us/download/details.aspx?id=29

   This must be installed on each deployed vCenter Single Sign-On server.

NOTE: There are newer versions of this file that might already be installed and might cause errors with the (step 4) download and install of WIN32 OpenSSL; the version provided is fully tested with WIN32 OpenSSL.

4. **Download and install WIN32 OpenSSL.**

   The specific version of OpenSSL that should be used for vCenter Single Sign-On server certificates (version 0.9.8) can be downloaded and installed from the following: http://slproweb.com/products/Win32OpenSSL.html

NOTE: For the purposes of this document, WIN32OpenSSL-0_9_8y.exe is a specific requirement and not necessarily the latest version available.

5. **Create certificate folder structure.**

   On the first vCenter Single Sign-On server virtual machine, create the following folder structure: **c:\certs\sso**

6. **Create a vCenter Single Sign-On configuration file.**

   Create a text file and build the file based on the following template, saving the file to **c:\certs\sso\sso.cfg**. This file will provide all host names and FQDNs used in the example configuration as well as the IP address for the NLB.

   See VMware Knowledge Base article 2061934 – *"Creating certificate requests and certificates for vCenter Server 5.5 components."*

Filename: c:\certs\sso\sso.cfg

```
[ 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 = Country
stateOrProvinceName = State
localityName = City
0.organizationName = Company Name
organizationalUnitName = vCenterSSO
commonName = sso.vmware.local
```

NOTE: The bold entries are specific to the environment as discussed in the preinstallation checklist and should be edited to reflect the environment you are installing into.

Deploying vCenter Single Sign-On Server

In this example, we will deploy a vCenter Single Sign-On server instance, deploy a second vCenter Single Sign-On server instance, and configure a load balancer to provide an active–active entry point for all vCenter Single Sign-On service requests in a single physical location.

1. First vCenter Single Sign-On Installation

The following steps will deploy the first vCenter Single Sign-On server:

a. Connect the **vCenter Server ISO image** to the **sso1.vmware.local** virtual machine.

b. Log in to **sso1.vmware.local**.

c. On the DVD menu, choose the **vCenter Single Sign-On** option listed under **Custom Install**.

d. Click **Install**.

e. After the **Welcome to the vCenter Single Sign-On Setup Wizard** screen is shown, click **Next**.

f. Select **I agree to the terms in the License Agreement** and click **Next**.

g. Review the **vCenter Single Sign-On Prerequisites** and click **Next**.

h. On the **vCenter Single Sign-On Information** screen, select the first option, **vCenter Single Sign-On for your first vCenter Server**, because this is the first vCenter Server to be deployed. Click **Next**.

i. Provide and confirm a **Password** for the built-in administrator@vsphere.local account. Click **Next**. Refer to VMware Knowledge Base article 2060746 – *"Installing vCenter Single Sign-On 5.5 fails if the password for administrator@vsphere.local contains certain special character."*

j. On the **vCenter Single Sign-On Configure Site** screen, provide a **Site name**. This can be based on location or organization—for example, **Palo Alto**. Click **Next**.

k. On the **vCenter Single Sign-On Port Settings** screen, click **Next**.

l. On the **Change destination folder** screen, click **Next**.

m. Confirm the **vCenter Single Sign-On Information/Review install options** screen. Click **Install**.

n. On the **Completed the vCenter Single Sign-On Setup Wizard** screen, click **Finish**.

2. Additional vCenter Single Sign-On Installations

The following steps will deploy additional vCenter Single Sign-On servers and partner them with the first server, deployed in step 1.

a) Connect the **vCenter Server ISO** image to the **sso2.vmware.local** virtual machine.

b) Log in to **sso2.vmware.local**.

c) On the DVD menu, choose the **vCenter Single Sign-On** option listed under **Custom Install**.

d) Click **Install**.

e) After the **Welcome to the vCenter Single Sign-On Setup Wizard** screen appears, click **Next**.

f) Select **I agree to the terms in the License Agreement** and click **Next**.

g) Review the **vCenter Single Sign-On Prerequisites** and click **Next**.

h) On the **vCenter Single Sign-On Information** screen, select the second option, **vCenter Single Sign-On for an additional vCenter Server in an existing site**, to pair with an existing local instance. Click **Next**.

i) Provide the **Partner host name** as **sso1.vmware.local**, to pair with the previously deployed vCenter Server Single Sign-On instance to replicate from. Provide the **Password** for the built-in administrator@vsphere.local account used with **sso1.vmware.local**. Click **Next**.

NOTE: All internal vCenter Single Sign-On communications will be direct and will not use the NLB.

j) To accept the host certificate, click **Continue** on the **Partner certificate** screen.

k) On the **vCenter Single Sign-On Join Site** screen, choose the **Site name** used with the first vCenter Single Sign-On instance—for example, **Palo Alto**. Click **Next**.

l) On the **vCenter Single Sign-On Port Settings** screen, click **Next**.

m) On the **Change destination folder** screen, click **Next**.

n) On the **vCenter Single Sign-On Information/Review install options** screen, click **Install**.

o) On the **Completed the vCenter Single Sign-On Setup Wizard** screen, click **Finish**.

Repeat step 2 for any additional vCenter Single Sign-On servers.

You now should have successfully deployed two or more separate vCenter Single Sign-On servers that are part of the same vsphere.local security domain.

vCenter Single Sign-On Certificates

When using an NLB, secure SSL communication with vCenter Single Sign-On server requires an update to the certificates to reflect the NLB entry point. All vCenter Single Sign-On servers that participate in the load-balanced configuration require certificate updates. In our example, we will use a Microsoft certificate authority (CA) as our trusted root authority and will generate certificate requests with OpenSSL. The process is similar for other CAs.

Optional: Creating the Microsoft Certificate Authority Template

The Microsoft CA template that we will use to create updated signed certificates must have data encipherment and client authentication enabled. See VMware Knowledge Base article 2062108 – *"Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 5.x."*

Generate the Certificate Request

You must run the following commands from a command line to prepare and generate the certificate request:

a) Open a command prompt and type the following:
```
CD \OpenSSL\bin
```

b) Run the following to create a certificate request and export the private key:
```
openssl req –new –nodes –out c:\certs\sso\rui.csr –keyout c:\certs\sso\rui-orig.key
–config c:\certs\sso\sso.cfg
```

c) Run the following to convert the key into the proper RSA format:
```
openssl rsa –in c:\certs\sso\rui-orig.key –out c:\certs\sso\rui.key
```

d) Download your CA's root certificate with Base64 encoding. In our example, the file generated is named `certnew.cer` and is saved in `C:\certs` renamed as follows: `Root64.cer`

e) With a text editor, open the private key `C:\certs\sso\rui.csr` and copy the entire contents into the CA certificate request field. Select the template with data encipherment enabled (optional step previously mentioned) and download the certificate as Base64 encoded. In our example, the file generated is named `certnew.cer` and is renamed as `rui.crt` and then placed into the following: `C:\certs\sso`

f) Run the following to create an archive file **(ssoserver.p12)** of all certificates and keys:
```
openssl pkcs12 –export –in c:\certs\sso\rui.crt –inkey c:\certs\sso\rui.key –
certfile c:\certs\Root64.cer –name "ssoserver" –passout pass:changeme –out c:\certs\
sso\ssoserver.p12
```

g) Change to the VMware directory by typing the following:
```
CD C:\Program Files\Common Files\VMware\VMware vCenter Server –
Java Components\bin\
```

h) Run the following to create the Java KeyStore:
```
keytool –v –importkeystore –srckeystore C:\certs\sso\ssoserver.p12 –srcstoretype
pkcs12 –srcstorepass changeme –srcalias ssoserver –destkeystore C:\certs\sso\root-
trust.jks -deststoretype JKS –deststorepass testpassword –destkeypass testpassword
```

If asked whether the existing entry alias ssoserver exists, overwrite? Type: `yes`

i) Run the following to add the root certificate to the Java KeyStore:
```
keytool –v –importcert –keystore C:\certs\sso\root-trust.jks –deststoretype JKS –
storepass testpassword –keypass testpassword –file C:\certs\Root64.cer –alias
root-ca
```

When asked whether to trust this certificate, type: `yes`

j) Run the following to copy the Java KeyStore to the required Java KeyStore name:
```
Copy C:\certs\sso\root-trust.jks C:\certs\sso\server-identity.jks
```

Configuring CA-Signed SSL Certificates

Log in to `sso1.vmware.local` and open an elevated command prompt.

a) Run the following to set the correct environment variables:
```
SET JAVA_HOME=C:\Program Files\Common Files\VMware\VMware vCenter Server –
Java Components
SET PATH=%PATH%;C:\Program Files\VMware\Infrastructure\VMware\CIS\vmware-sso;%JAVA_
HOME%\bin
```

b) Change to the OpenSSL directory; type and run the following:
```
CD \OpenSSL\bin
```

c) Register the new root certificate in the VMware trust store; type and run the following:
```
openssl x509 –noout –subject_hash –in C:\certs\Root64.cer
```

This will create an eight-digit hexadecimal value that will be used in step e).

d) Run the following to create an SSL directory:
```
mkdir c:\ProgramData\VMware\SSL
```

e) Run the following to copy the Root64.cer certificate to the SSL folder:
```
Copy C:\certs\Root64.cer C:\ProgramData\VMware\SSL\<eight digit hexadecimal
value>.0
```

This is the result from step c).

f) Run the following to copy the Root64.cer file to the SSL folder and rename it to ca_certificates.crt:
```
more C:\certs\Root64.cer >> C:\ProgramData\VMware\SSL\ca_certificates.crt
```

g) To change the vCenter Single Sign-On server configuration to reflect the NLB, with a text editor, create three text files within the C:\certs directory and name as shown. These files are used to update the individual vCenter Single Sign-On services with the NLB VIP.

Filename: C:\certs\admin.properties

```
[service]
friendlyName=The administrative interface of the SSO server
version=1.5
ownerId=
productId=product:sso
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:\certs\Root64.cer
protocol=vmomi
```

Filename: C:\certs\gc.properties

```
[service]
friendlyName=The group check interface of the SSO server
version=1.5
ownerId=
productId=product:sso
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:\certs\Root64.cer
protocol=vmomi
```

Filename: C:\certs\sts.properties

```
[service]
friendlyName=STS for Single Sign On
version=1.5
ownerId=
productId=product:sso
type=urn:sso:sts
description=The Security Token Service of the Single Sign On server.

[endpoint0]
uri=https://sso.vmware.local:7444/ims/STSService/vsphere.local
ssl=c:\certs\Root64.cer
protocol=wsTrust
```

h) Run the following to list the vCenter Single Sign-On services:

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

The return should be three services:

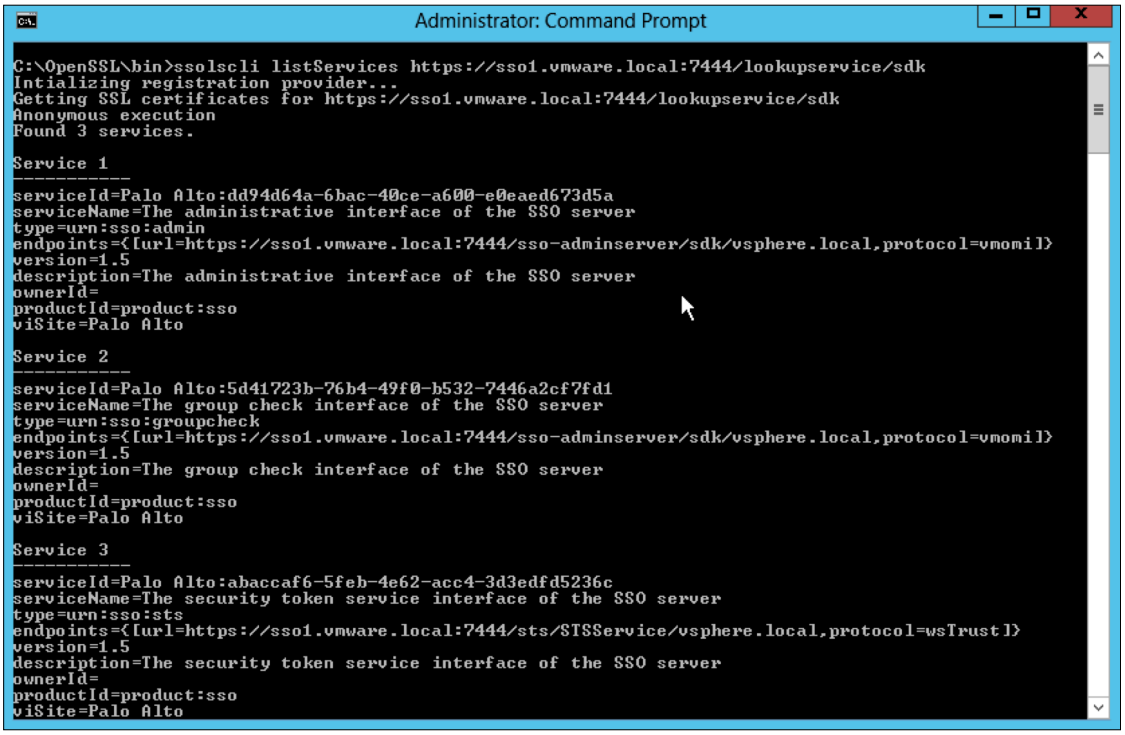

Figure 3. Example of the vCenter Single Sign-On Server CLI List Services Command

i) For each service returned, the first field will display as the following:

```
<serviceId=<SSOSiteName>:<thirty two digit hexadecimal value>
```

Each service site name and 32-digit hexadecimal value must be saved to a text file by using the service type (line 3) and the following syntax for each corresponding service type:

```
ECHO Palo Alto:<thirty two digit hexadecimal value> >> C:\certs\gc_id
ECHO Palo Alto:<thirty two digit hexadecimal value> >> C:\certs\sts_id
ECHO Palo Alto:<thirty two digit hexadecimal value> >> C:\certs\admin_id
```

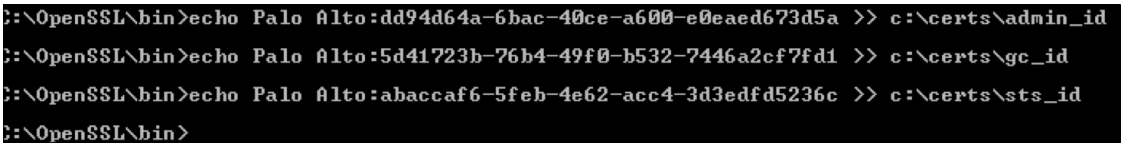

Figure 4. Example of Exporting Service Information to a Text File

j) Open a Windows Explorer window and navigate to the following:
`C:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf`

k) Create a backup directory and make a backup of the following files by copying them into the backup folder:
`ssoserver.crt`
`ssoserver.key`
`ssoserver.p12`

l) In the command prompt windows, copy the three certificate files to the correct destination by typing the following:

```
copy C:\certs\sso\ssoserver.p12 c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\
ssoserver.p12
copy C:\certs\Root64.cer c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\
ssoserver.crt
copy C:\certs\sso\rui.key c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\
ssoserver.key
```

Select `YES` to overwrite the existing file.

m) Before we can update the vCenter Single Sign-On service information, we must add the `sso.vmware.local` into the local host files, because this entry will create an error prior to configuration of the load balancer. Type the following:

```
notepad C:\Windows\System32\Drivers\etc\hosts
```

Then add the following:

```
192.168.110.41      sso.vmware.local
```

n) Run the following to update the three vCenter Single Sign-On services with the service files created with the NLB configuration. Type the following:

```
ssolscli updateService -d https://sso1.vmware.local:7444/lookupservice/sdk -u
administrator@vsphere.local -p <password> -si C:\certs\gc_id –ip C:\certs\
gc.properties

ssolscli updateService -d https://sso1.vmware.local:7444/lookupservice/sdk -u
administrator@vsphere.local -p <password> -si C:\certs\admin_id –ip C:\certs\admin.
properties

ssolscli updateService -d https://sso1.vmware.local:7444/lookupservice/sdk -u
administrator@vsphere.local -p <password> -si C:\certs\sts_id –ip C:\certs\sts.
properties
```

NOTE: If you receive a Server certificate assertion not verified and thumbprint not matched *error, follow step o) to restart the VMware Security Token Service and repeat the command.*

o) You must restart the VMware Security Token Service for the previous step to take effect. Type the following:

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

p) Confirm that the updates have been applied by listing the vCenter Single Sign-On services. Type the following:

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

The endpoints entry (line 4) should now show the load balance URL `sso.vmware.local` for each service.

q) Remove the temporary host entry applied to the local hosts file by deleting the `sso.vmware.local` entry added in step m).

Log in to `sso2.vmware.local` and open an elevated command prompt.

a) Open a Windows Explorer window. Navigate to `\\sso1.vmware.local\c$` and copy the `certs` directory to `C:\ on sso2.vmware.local` `\\sso1.vmware.local\c$\ProgramData\VMware` and copy the `SSL` directory to `C:\ProgramData\VMware` on `sso2.vmware.local`

b) Run the following to set the correct environment variables:

```
SET JAVA_HOME=C:\Program Files\Common Files\VMware\VMware vCenter Server –
Java Components
SET PATH=%PATH%;C:\Program Files\VMware\Infrastructure\VMware\CIS\vmware-sso;%JAVA_
HOME%\bin
```

c) Before we can update the vCenter Single Sign-On service information, we must add the **sso.vmware.local** into the local host's files on **sso2.vmware.local** because this entry will create an error prior to configuration of the load balancer. Type

```
notepad C:\Windows\System32\Drivers\etc\hosts
```

and add

```
192.168.110.42   sso.vmware.local
```

d) In the command prompt window, copy the three update files to the correct destination. Type the following:

```
copy C:\certs\sso\ssoserver.p12 c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\
ssoserver.p12
copy C:\certs\Root64.cer c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\
ssoserver.crt
copy C:\certs\sso\rui.key c:\ProgramData\VMware\CIS\runtime\VMwareSTS\conf\
ssoserver.key
```

Select **YES** to overwrite the existing file.

e) Restart the VMware Security Token Service to accept the updated certificate files. Type the following:

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

f) Update the three services with the current information. Type the following:

```
ssolscli updateService -d https://sso2.vmware.local:7444/lookupservice/sdk –u
administrator@vsphere.local –p <password> –si C:\certs\gc_id –ip C:\certs\
gc.properties
ssolscli updateService -d https://sso2.vmware.local:7444/lookupservice/sdk –u
administrator@vsphere.local –p <password> –si C:\certs\admin_id –ip C:\certs\admin.
properties
ssolscli updateService -d https://sso2.vmware.local:7444/lookupservice/sdk –u
administrator@vsphere.local –p <password> –si C:\certs\sts_id –ip C:\certs\sts.
properties
```

NOTE: If you receive a Server certificate assertion not verified and thumbprint not matched *error, follow step g) to restart the VMware Security Token Service and repeat the command.*

g) You must restart the VMware Security Token Service to effect the previous step. Type the following:

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

h) Confirm by typing the following that the updates have been applied:

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

The endpoints entry (line 4) should now show the load balance URL **sso.vmware.local** for each service.

i) Remove the temporary host entry applied to the local host's file by deleting the **sso.vmware.local** entry added in step c).

Configuring the Network Load Balancer

The following are examples of NLB configurations that can be used for placement with centralized vCenter Single Sign-On servers to provide an active–active distribution of load as well as redundancy. This is to be used as a guide for configuring such NLBs, because VMware does not provide support for the configuration of third-party products.

It is important to have a solid understanding of the setup and administration of the intended NLB prior to proceeding. The following procedures provide guidance on configuring the NLB for use with vCenter Single Sign-On server only and are not intended to provide general guidance on setup and administration of a load balancer.

NOTE: The following NLB configurations will not work with the VMware vCloud Automation Center™, due to its having different vCenter Single Sign-On server communication requirements from those of vCenter Server. A revision is planned for enactment as soon as testing has been completed.

VMware vCloud Networking and Security

Using a supported Web browser, open the VMware vShield Manager™ interface.

1. In the left-hand menu, expand **Datacenters** and choose the data center your vCenter Single Sign-On environment resides in.
2. Configure the virtual IP address (VIP):
    a. Click the **Network Virtualization** tab.
    b. Select your **Edge gateway** device.
    c. Click **Actions**.
    d. Choose **Manage**.
    e. Click **Configure**.
    f. Select the **vNIC** that will house the VIP IP address.
    g. Select **Edit**.
    h. Click the **Green plus** icon.
    i. Enter the **IP Address** of the load balancer: **192.168.110.40**.
    j. Click **Add**.
3. Create the virtual server pool:
    a. Click the **Load Balancer** tab on the edge1 screen.
    b. Click the **green plus** icon to add a pool.
    c. Provide a name: enter **SSO-POOL**.
    d. Click **Next**.
    e. Under **Services**:
        i. Select **TCP**.
        ii. Choose **LEAST_CONN** as **Balancing Method**.
        iii. Enter **7444** as **Port**.

f. Click **Next**.

g. Change the **TCP Monitor Port** to **7444**.

h. Click **Next**.

i. Under **Members**:

i. Click the **green plus** icon.

ii. Enter an IP address: **192.168.110.41**.

iii. Click **Add**.

iv. Click the **green plus** icon again.

v. Enter an IP address: **192.168.110.42**.

vi. Click **Add**.

vii. Click **Next**.

viii. Click **Finish**.

j. Click **Enable**.

k. **Publish Changes** to update configuration.

4. Create a virtual server:

a. Click **Virtual Servers** under the configuration tabs.

b. Click the **green plus** icon.

c. Enter a name: **SSO-VIP**.

d. Enter an IP address: **192.168.110.40**.

e. Under **Services**:

i. Select **TCP**.

ii. Change the **TCP Port** to **7444**.

iii. Click **Add**.

f. Click **Publish Changes** to update configuration.

5. (Optional) Configure firewall if the default rule is set to **Deny**.

a. Click the **Firewall** tab.

b. Click the **green plus** icon.

c. In the new entry:

i. Enter a rule name: **SSO**.

ii. Provide a destination: select **Add IP Addresses**.

iii. Enter a name: **SSO-VIP**.

iv. Enter an IP address: **192.168.110.40**.

d. Click **OK**.

e. Click **Publish**.

F5 BIG-IP

1. Before you start, make a copy of the **C:\certs\sso** directory and **Root64.cer** from one of the installed vCenter Single Sign-On servers.

Using a supported Web browser, open the F5 BIG-IP management interface.

2. Provide SSO certificates to F5 BIG-IP:
   a. Choose **System**.
   b. Choose **File Management**.
   c. Choose **SSL Certificate List**.
   d. On the **SSL Certificate List** screen, click **Import**.
   e. Under **Import Type**, select **Certificate**.
   f. For **Certificate Name**, select **Create New** and enter **ssoCert**.
   g. For **Certificate Source**, select **Upload File** and browse to the **rui.crt** file from the copy of the SSO directory in step 1.
   h. Click **Import**.
   i. On the **SSL Certificate List** screen, click **Import**.
   j. Under **Import Type**, select **Key**.
   k. For **Key Name**, select **Create New** and enter **ssoKey**.
   l. For **Key Source**, select **Upload File** and browse to the **rui.key** file from the copy of the SSO directory in step 1.
   m. Click **Import**.
   n. On the **SSL Certificate List** screen, click **Import**.
   o. For **Import Type**, select **Certificate**.
   p. For **Certificate Name**, select **Create New** and enter **VMwareLocalRoot**.
   q. For **Certificate Source**, select **Upload File** and browse to the **Root64.cer** file from the copy in step 1.
   r. Click **Import**.
   s. Confirm that the **ssoCert** entry shows **sso.vmware.local** under **Common Name**.
3. Create the load balancer pool:
   a. Choose **Local Traffic** from the left-hand menu.
   b. Choose **Pools**.
   c. Choose **Pool List**.
   d. On the **Pool List** screen, click **Create**.
   e. Provide a **Name**: enter **SSO**.
   f. For **Health Monitors**, select and add **tcp** to active column.

g. For **New Members**:
   i. Enter a **Node Name: sso1**.
   ii. Enter an **Address: 192.168.110.41**.
   iii. Enter a service port: **7444**.
   iv. Click **Add**.
   v. Enter a **Node Name** of **sso2**.
   vi. Enter an **Address: 192.168.110.42**.
   vii. Enter a S**ervice Port: 7444**.
   viii. Click **Add**.
   ix. Click **Finished**.

4. Create SSL client:
   a. Choose **Local Traffic** from left-hand menu.
   b. Choose **Profiles**.
   c. Choose **SSL**.
   d. Choose **Client**.
   e. On the **Client** screen, click **Create**.
   f. Enter a **Name: SSO-Client**.
   g. Select **Custom**.
   h. Under **Configuration**:
      i. For **Certificate**, choose **ssoCert**.
      ii. For **Key**, choose **ssoKey**.
      iii. Click **Finished**.

5. Create SSL server:
   a. Choose **Local Traffic** from left-hand menu.
   b. Choose **Profiles**.
   c. Choose **SSL**.
   d. Choose **Server**.
   e. On the **Server** screen, click **Create**.
   f. Enter a **Name: SSO-Server**.
   g. Select **Custom**.
   h. Under **Configuration**:
      i. For **Certificate**, choose **ssoCert**.
      ii. For **Key**, choose **ssoKey**.
      iii. Click **Finished**.

6. Create virtual server:
    a. Choose **Local Traffic** from left-hand menu.
    b. Choose **Virtual Servers**.
    c. Choose **Virtual Server List**.
    d. On the **Server** screen, click **Create**.
    e. Enter a **Name: SSO-VIP**.
    f. Provide a **Destination**:
        i. For **Type**, select **Host**.
        ii. Enter an **Address: 192.168.110.43**.
        iii. Enter a **Service Port: 7444**.
    g. Under **Configuration**:
        i. For **HTTP Profile**, choose **http**.
        ii. For **SSL Profile (Client)**: choose **SSO-Client**.
        iii. For **SSL Profile (Server)**: choose **SSO-Server**.
    h. Under **Resources**:
        i. For **Default Pool**: choose **SSO**.
    i. Click **Finished**.
7. Create SNAT:
    a. Choose **Local Traffic** from left-hand menu.
    b. Choose **Address Translation**.
    c. Choose **SNAT List**.
    d. On the **SNAT List** screen, click **Create**.
    e. Enter a **Name: SNAT-SSO-NGC**.
    f. Under **Configuration**:
        i. For Translation IP address: choose **192.168.110.40**.
    g. Click **Finished**.

Citrix NetScaler

Using a supported Web browser, open the Citrix NetScaler management interface.

1. Create a virtual server:
    a. Choose **Traffic Management**.
    b. Choose **Load Balancing**.
    c. Choose **Virtual Servers**.
    d. Click **Add**.
    e. Enter a Name: **SSO**.

f. Change the protocol from the default **HTTP** to **TCP**.

g. Enter an **IP address: 192.168.110.40**.

h. Enter a **Port: 7444**.

2. Create the services for the virtual server:

a. Select **Add** under the **Services** tab.

b. Enter a **Service Name:** enter **sso1**.

c. Change the protocol from default **HTTP** to **TCP**.

d. Select **Server** and enter **192.168.110.41**.

e. Select **Port** and enter **7444**.

f. Under available **Monitors**, select **TCP** and click **Add**.

g. Click **Create**.

h. Click **Add** again under the **Services** tab.

i. Enter a **Service Name: sso2**.

j. Change the protocol from default **HTTP** to **TCP**.

k. Select **Server** and enter **192.168.110.42**.

l. Select **Port** and enter **7444**.

m. Under available **Monitors**, select **TCP** and click **Add**.

n. Click **Create**.

3. Under available monitors, select **TCP** and click **Add**.

a. Click **Create**.

4. On the **Create Virtual Server** screen:

a. Click **Create**.

b. Click the **Method and Persistence** tab.

c. Confirm that **LB Method** is set for **Least Connection**.

d. Click **Close**.

5. Refresh the configuration.

You now have an NLB that is configured to receive vCenter Single Sign-On requests and to pass through to a member server running vCenter Single Sign-On server.

Postdeployment of a Centralized vCenter Single Sign-On Environment

Having completed the previous steps of installing a centralized vCenter Single Sign-On solution, you can complete the deployment of all vCenter Single Sign-On enabled solutions. Installation of additional VMware solutions is not recommended on the virtual machines hosting the vCenter Single Sign-On environment.

Installing vCenter Server Components

Almost all vCenter Server components utilize a vCenter Single Sign-On solution. They can be deployed in the following order:

1. VMware vSphere Web Client – Specify **sso.vmware.local** for the vCenter Single Sign-On server.
2. vCenter Inventory Service – Specify **sso.vmware.local** for the vCenter Single Sign-On server.
3. vCenter Server – Specify **sso.vmware.loca**l for the vCenter Single Sign-On server.

Any other VMware component that requires vCenter Single Sign-On registration should also specify **sso.vmware.local** when asked for the vCenter Single Sign-On server.

Updating a Previously Installed vCenter Single Sign-On Configuration

If you have deployed a different vCenter Single Sign-On architecture or are upgrading and plan to move to a centralized vCenter Single Sign-On environment, the following is an overview of the process involved.

1. If upgrading, you must do so from the existing vCenter Single Sign-On server to the latest release; that is, vCenter Server 5.5.0b Build 1476387.
2. Deploy a new vCenter Single Sign-On server, as discussed, for an additional vCenter Single Sign-On server, using the existing vCenter Single Sign-On server as the partner host name. This will enable replication of vCenter Single Sign-On configuration, including users and groups, to the newly deployed vCenter Single Sign-On server. This server will become the first vCenter Single Sign-On server in a centralized environment, for placement behind an NLB.
3. Deploy a new vCenter Single Sign-On server, as discussed, for an additional vCenter Single Sign-On server, using the vCenter Single Sign-On server deployed in the previous step as the partner host name. This server will be the second vCenter Single Sign-On server in a centralized environment, for placement behind an NLB.
4. Proceed with the preceding instructions, starting from the vCenter Single Sign-On certificates.

Conclusion

With the release of VMware vCenter Server 5.5 and an improved VMware vCenter Single Sign-On server, the use of network load balancers with a centralized vCenter Single Sign-On environment can provide robust load distribution and redundancy without the limitations found in previous versions. For customers with multiple vCenter Single Sign-On enabled solutions, the centralized model eases the duplication of vCenter Single Sign-On administration. This document provides the necessary steps for deploying and configuring a centralized vCenter Single Sign-On environment with the benefits of utilizing a network load balancer.

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

Docsource: OIC - 13VM004.09