Prerequisites

1. Download the appliance at https://my.vmware.com/group/vmware/get-download?downloadGroup=SKYLINE10
2. Watch this Install Video Walkthrough - https://www.youtube.com/watch?v=DKe9aUJj3yo&t=231s
3. Make sure these ports are open

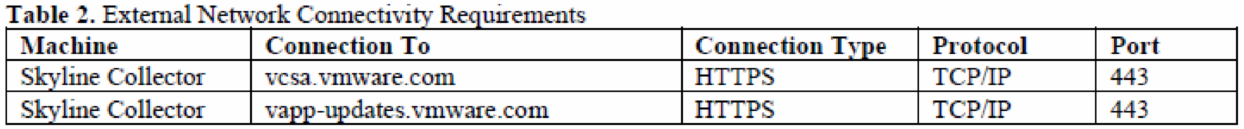


Table 2. External Network Connectivity Requirements

Machine	Connection To	Connection Type	Protocol	Port
Skyline Collector	vcsa.vmware.com	HTTPS	TCP/IP	443
Skyline Collector	vapp-updates.vmware.com	HTTPS	TCP/IP	443

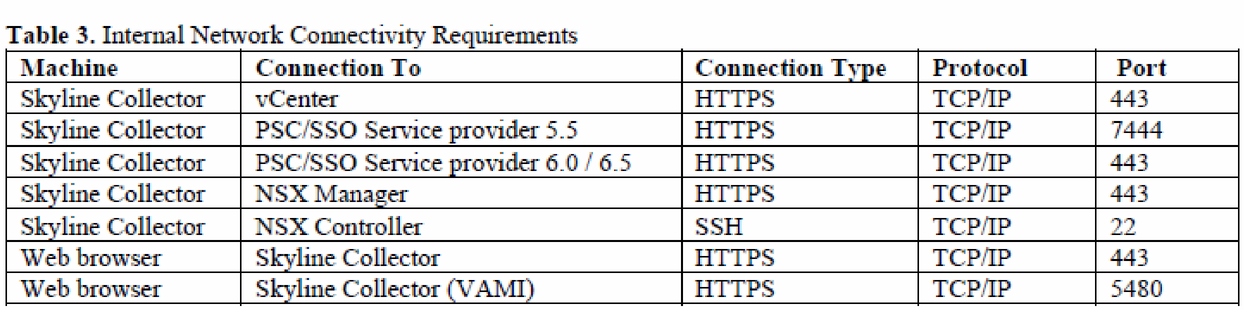


Table 3. Internal Network Connectivity Requirements

Machine	Connection To	Connection Type	Protocol	Port
Skyline Collector	vCenter	HTTPS	TCP/IP	443
Skyline Collector	PSC/SSO Service provider 5.5	HTTPS	TCP/IP	7444
Skyline Collector	PSC/SSO Service provider 6.0 / 6.5	HTTPS	TCP/IP	443
Skyline Collector	NSX Manager	HTTPS	TCP/IP	443
Skyline Collector	NSX Controller	SSH	TCP/IP	22
Web browser	Skyline Collector	HTTPS	TCP/IP	443
Web browser	Skyline Collector (VAMI)	HTTPS	TCP/IP	5480

4. If required to access the internet, have your proxy address, IP, username(optional), and password(optional) ready
5. If using the vSphere Web Client to deploy, ensure the Client Integration Plugin (5.5/6.0) or Enhanced Authentication Plugin (6.5) is installed.

Deploy the OVA

When prompted to customize the appliance, enter following:

- Root password
- Default Gateway
- Domain Name: FQDN of Skyline Collector (i.e. collector01.company.com)
- Domain Search Path: DNS Domain (i.e. company.com)
- Domain Name Server
- IP
- Subnet Mask

Click Finish to deploy

Configuring the Collector

1. Enter the IP or hostname for Skyline in a browser. (Chrome works best)

2. Login with admin / default

3. Change admin password (8 chars, 1 upper case, 1 lowercase, 1 special, 1 number)

4. Log back in with your new Admin password

5. Configure Proxy only if its needed to reach the internet. Click Test Connection.
    - The **Continue** button will light up if the connection is successful
    - Note: NTLM Authentication is not supported

6. Enter myVMware credentials

    If you encounter a problem here, see **Appendix A** at the end of this document

7. Give the collector a name which will identify its region/organization

8. **Configure vCenter endpoint**

    If you encounter a problem here, see **Appendix B** at the end of this document

    - For **embedded SSO/PSC** vCenters (do not have to put in advanced options)
        - Note: If your sso domain is not vsphere.local, proceed to the external SSO/PSC section
        - Hostname for vcenter
        - VC username (Read-Only or greater privileges)
        - Password
        - Leave collect from all Datacenters set to **Yes**
        - Click Add

    - For **external SSO/PSC** vCenters.
        - Hostname for vcenter
        - VC username (Read Only or higher)
        - Password
        - Change *Use external PSC/SSO Service provider OR custom SSO domain* to **Yes**
            - FQDN of SSO/PSC. This will be the vCenter address if its embedded
            - Use the examples to fill out the Advanced Options
                - Replace 10.20.30.40 with your PSC FQDN
                - Replace vsphere.local with your SSO domain (if changed from default)
        - Leave collect from all Datacenters set to **Yes**
        - Click Add

- Note: If you receive a connection error mentioning an address and port 7444, double-check the PSC/SSO URLs. If the error mentions port 443, double-check the vCenter address.

9. **Configure NSX endpoints (Optional)**

    If you encounter a problem here, see **Appendix C** at the end of this document

    - Enter NSX Manager IP or hostname

- Enter NSX Manager username (Read only or higher)
- Enter Password
- Enter NSX Controller username (Needs SSH access, Admin works)
- Enter Password
- Click add

10. Done!

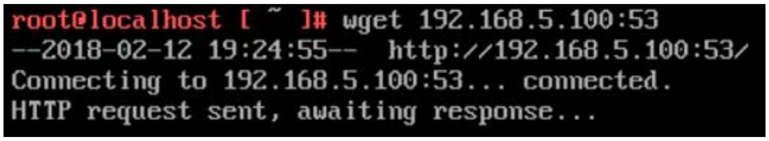
Appendix A

MyVMware Registration Troubleshooting

Unknown Host error

```
Couldn't register due to: UploadException: Couldn't upload data to the REST endpoint.
>>> UnknownHostException: vcsa.vmware.com
```

Unknown Host errors mean that the hostname could not be resolved. During registration, this is the hostname that the collector will send data to, *vcsa.vmware.com*. This might be due to the collector not being able to contact the DNS server(s) configured in `/etc/resolv.conf`. A simple way to test this is to use wget to send a connection request over port 53.



```
root@localhost [ ~ ]# wget 192.168.5.100:53
--2018-02-12 19:24:55--  http://192.168.5.100:53/
Connecting to 192.168.5.100:53... connected.
HTTP request sent, awaiting response...
```

If you see connected, then it was able to reach the DNS server. Note that the https request will not respond because DNS does not respond to HTTP requests normally.

If it does not connect, make sure the IPs in `/etc/resolv.conf` are correct and that the portgroup/subnet the collector is on can reach the DNS servers.

To test if vcsa.vmware.com can be resolved from the command line, use wget

```
wget https://vcsa.vmware.com:443
```

The first thing it will do is try to resolve the hostname, then connect to the IP it gets back. If it resolves, but doesn't connect, check out the troubleshooting section for connection failure

Connection Failure error

This message is seen when the collector cannot reach *vcsa.vmware.com* on *port 443*. You can test this from the command line with wget

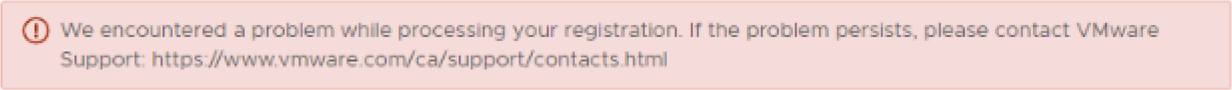
```
wget https://vcsa.vmware.com:443
```

If this returns a “failed Network is unreachable” message, then there is something blocking the https traffic to the backend analytics IP. This could simply be that the network or portgroup the VM is on doesn’t have access to the internet, or that a firewall is blocking the traffic, or a number of other possible things. It is necessary to find this block and remove it before the collector can be registered.

Collector Already registered

This happens when the browser caches information about the registration which makes it believe its already registered. It happens most often on IE. Clear the cache or use a different browser.

General Error



We encountered a problem while processing your registration. If the problem persists, please contact VMware Support: https://www.vmware.com/ca/support/contacts.html

This error means something went wrong while trying to match up the customer credentials and an EA that has Skyline enabled for it. Contact the VMware Skyline engineers to help determine what the problem is and get it corrected.

PKIX Path Building error (https://kb.vmware.com/s/article/52658)

The proxy configuration can be tricky if its an https proxy that uses SSL encryption. When using a proxy that presents an SSL certificate, the cert needs to be added to the local java keystore before it is trusted by the collector. The process is slightly different if the certificate is signed by a local certificate authortity (CA), in that the root and intermediate certs need to be trusted as well.

First, log in to the collector’s console with root. (See **Appendix D** if SSH is desired)

Depending on your proxy certificate type (self signed or CA signed), chose one of the set of steps below.

If the proxy uses a self-signed certificate

1. Use this openssl command to pull and create it:

```
     echo -n | openssl s_client -connect myproxy.domain.local:8080 | sed -ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp/myproxy.cert
```

2. Now import the cert into the *cacerts* java keystore

```
     keytool -importcert -file /tmp/myproxy.cert -alias proxycert -keystore /usr/java/jre-
vmware/lib/security/cacerts -storepass changeit
```

3. Restart the collector

```
     systemctl restart ccf-collector
```

If the proxy uses an CA signed cert

This process is significantly more difficult without a good knowledge of certificate chains.

1. Export the root and any intermediate CA certificates and upload them to the collector with an SCP/FTP client such as WinSCP or Filezilla (https://technet.microsoft.com/en-us/library/dd261928.aspx) **OR** use openssl to display the full chain, then create each cert file manually:

```
        openssl s_client -host proxy.domain.com -port 443 -prexit -showcerts
```

2. In any order, add the certs to the cacerts java keystore. Use a different alias for each one

```
        keytool -importcert -file root.cer -alias proxyroot -keystore /usr/java/jre-
vmware/lib/security/cacerts -storepass changeit
```

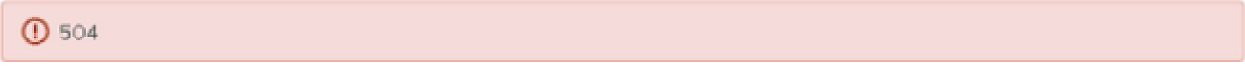
3. Restart the collector service

```
        systemctl restart ccf-collector
```

Appendix B

Troubleshooting adding a vCenter

504 Error

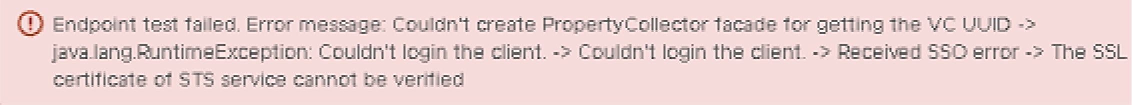


504

The 504 error usually happens when there is a problem communicating with SSO.

- If the PSC is embedded, try leaving the SSO URLs blank.
- If the PSC/SSO is external to the vCenter, make sure the both PSC URLs are updated with the correct fqdn.
- Also, if you changed your SSO domain from vsphere.local, you will need to update the last part of the URL.
- Make sure the PSC URLs are pointing to the SSO server (test them in a browser, it should not return 404)
- Try a different set of credentials (qualified SSO credentials will also work)
- Test basic connectivity to VC environment by logging in to the collecter through a console with root and run:
    - `wget https://PSC_FQDN:7444`
    - `wget https://VC_FQDN:443`

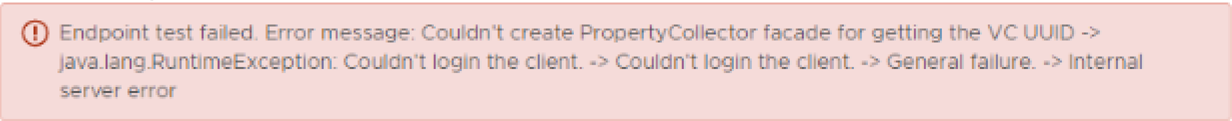
STS Certificate cannot be verified



Endpoint test failed. Error message: Couldn't create PropertyCollector facade for getting the VC UUID -> java.lang.RuntimeException: Couldn't login the client. -> Couldn't login the client. -> Received SSO error -> The SSL certificate of STS service cannot be verified

This is a known issue with the current build of the Skyline Collector. Contact the VMware Support team to request the hot patched build for install. This should also be fixed in Skyline 1.1

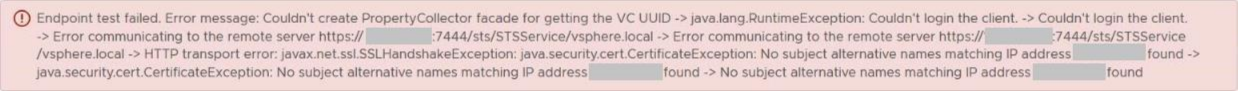
Couldn’t login to the client



Endpoint test failed. Error message: Couldn't create PropertyCollector facade for getting the VC UUID -> java.lang.RuntimeException: Couldn't login the client. -> Couldn't login the client. -> General failure. -> Internal server error

This usually means that the credentials being used are not accepted. Ensure they are at least Read Only on vCenter and all its child objects. Many times this error can be fixed by using a newly create SSO account for skyline. Make sure to qualify the credentials with their domain as well, even if its vsphere.local.

No Subject alternative names matching IP address



```
Endpoint test failed. Error message: Couldn't create PropertyCollector facade for getting the VC UUID -> java.lang.RuntimeException: Couldn't login the client. -> Couldn't login the client.
-> Error communicating to the remote server https://[redacted]:7444/sts/STSService/vsphere.local -> Error communicating to the remote server https://[redacted]:7444/sts/STSService
/vsphere.local -> HTTP transport error: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative names matching IP address [redacted] found ->
java.security.cert.CertificateException: No subject alternative names matching IP address [redacted] found -> No subject alternative names matching IP address [redacted] found
```

This message means that the certificate being presented by the PSC/SSO server does not have the address mentioned in the subject alternative name (SAN). This can usually be fixed by changing the URLs to FQDNs instead of IPs

The server sent HTTP status code 404: Not Found

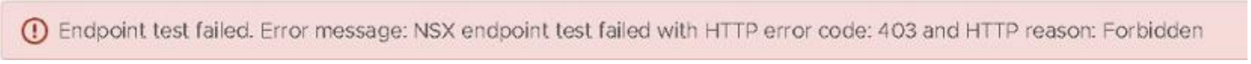
```
Endpoint test failed. Error message: Couldn't create PropertyCollector facade for getting the VC
UUID -> java.lang.RuntimeException: Couldn't login the client. -> Couldn't login the client. ->
Error communicating to the remote server https://PSC_FQDN:7444/STSService/vsphere.local -> Error
communicating to the remote server https://PSC_FQDN:7444/STSService/vsphere.local -> The server
sent HTTP status code 404: Not Found
```

This error usually happens when the SSO URLs entered are incorrect or if the Skyline Appliance cannot communicate with the SSO URL. Sometimes this can be as simple as having an extra space in the URL or forgetting to change the end of the URL to match the SSO domain name.

Appendix C

Troubleshooting adding NSX

HTTP error code: 403 Forbidden



```
Endpoint test failed. Error message: NSX endpoint test failed with HTTP error code: 403 and HTTP reason: Forbidden
```

HTTP 403 errors happen when the collector was able to contact the endpoint, but unable to authorize with the provided credentials. NSX accounts require specific privileges to be configured to add to Skyline.

See https://kb.vmware.com/s/article/2150736 for more information

HTTP error code: 404 Not Found

```
Endpoint test failed. Error message: NSX endpoint test failed with
HTTP error code: 404 and HTTP reason: Not Found
```

If seen, check the address URL, because the Skyline Collector is not getting to the NSX Manager login web page.

Appendix D

General

Enabling SSH

By default, SSH is disabled. To enable SSH access, perform the following steps:

1. Open the Skyline Collector console via the vSphere Client/Web Client
2. Login as root and the root password defined during deployment
3. Run 'vi /etc/ssh/sshd_config'
4. Enter 'i' to modify the file in VI editor
5. Locate the line that contains 'PermitRootLogin' and change it to 'PermitRootLogin yes'
6. Save the changes by hitting ESC + typing ':wq!'
6. Restart the sshd service by running 'service sshd restart'

Collecting Logs

1. Login to the Collector appliance with an SSH client (such as Putty) with the root user
2. Run the following commands:

```
    tar -pczf /tmp/logs.tar.gz /var/log
    tar -pczf /tmp/config.tar.gz /usr/local/skyline/
```

3. Using WinSCP, login to the collector appliance, and obtain the .tgz file generated from the command above
4. Upload the log bundle to the Support Request opened

(KB: https://kb.vmware.com/s/article/2069559)