The steps outlined here have been excerpted from eDocs available here.

These instructions are compiled to have a natural flow for an Administrator integrating NetScaler and Sharefile components. The instructions that follow will depict the method to perform actions using Graphical User Interface (GUI) and subsequently how to perform the same function(s) using the Command Line Interface (CLI).

For purposes of this article, NetScaler v. 10.1 build 118.7nc was used, any NS Firmware 10.x, 9.3 support http callouts (required as part of the configuration), however, only 10.1 allows us to bind callout expressions to SSL Virtual Servers, which is recommended.

1. **Create StorageZone Controller 2.0 Service(s) on NetScaler**
2. **Create and Configure Load Balancing VServers**
3. **Create and Configure Content Switching Policies**
4. **Create and Configure Content Switching VServer**
5. **Create HTTP Callouts**
6. **Create and Configure Responder Policy to use HTTP Callout**
7. **Bind Responder Policy to Load Balancing VServer(s)**
8. **(Optional) Configure Authentication VServer**
1. Create StorageZone Controller Service(s) on NetScaler

Create a Service of Protocol SSL on port 443 for the Sharefile 2.0 Storage Zone Controller server entity. Go to Traffic Management > Load Balancing > Services section of GUI.

GUI Method:

![GUI Method Image]

CLI Command:

```
add service <servicename> <IP ADDRESS> SSL 443 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -usproxyport YES -sp ON -cltTimeout 180 -svrTimeout 360 -CustomServerID "\"None\"" -CKA NO -TCPB NO -CMP YES
```

**Note:** Multiple services can be created (for example, Data_requests_svc, Connector_Svc), however for this example only one is created.
2. Create and Configure Load Balancing VServers

Two Load Balancing Virtual Servers are created in this step. Create a Load Balanced Virtual Server for the StorageZone Controller Data Requests, another for the StorageZone Controller Connector Requests. This allows to differentiate between the two types of traffic received on NetScaler and can scale accordingly.

1. Create First Load Balancing Virtual Server (for SZC Data Requests) of Protocol Type SSL, clear Directly Addressable option. Select the service that was created in Section 1. This will bind the service to the Load Balancing Virtual server. Do not click Create.

2. Go to Method and Persistence tab, set the LB Method to Token. Set the rule to “http.REQ.URL.QUERY.VALUE(“uploadid”)”.

3. Go to the SSL Settings tab and bind the appropriate certificate to the LBVServer, click Create.
4. Perform the same actions to create the other Load Balancing Virtual Server for the StorageZone Controller Connector Requests.

CLI Commands:
```
add lb vserver SZC2.0_LBVData SSL 0.0.0.0 0 -persistenceType SSLSESSION -lbMethod TOKEN -rule "http.REQ.URL.QUERY.VALUE("uploadid")" -cltTimeout 180
bind lb vserver SZC2.0_ LBVData szc20_svc
bind ssl vserver SZC2.0_ LBVData -certkeyName szc20

add lb vserver SZC2.0_LBVConnector SSL 0.0.0.0 0 -persistenceType SSLSESSION -lbMethod TOKEN -rule "http.REQ.URL.QUERY.VALUE("uploadid")" -cltTimeout 180
bind lb vserver SZC2.0_LBVConnector szc20_svc
bind ssl vserver SZC2.0_LBVConnector -certkeyName szc20
```
See the following screen shot for reference when you complete Sections 1 and 2.
3. Create and Configure Content Switching Policies

1. Go to **Content Switching > Policies**. In this example, two policies are created to differentiate the traffic for Data and Connector Requests. First will be named as “Data_Requests”. In the Expression field, type/paste the following qualifier:
   - HTTP.REQ.HOSTNAME.CONTAINS("StorageZoneControllerFQDN")
   - HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.CONTAINS("/sp/").NOT . Click **Create**.

   CLI Command:
   ```bash
   add cs policy Data_Requests -rule "HTTP.REQ.HOSTNAME.CONTAINS("StorageZoneControllerFQDN") && HTTP.REQ.URL.CONTAINS("/cifs/").NOT && HTTP.REQ.URL.CONTAINS("/sp/").NOT"
   ```

2. The second policy will be named as **Connector_Requests**. In the Expression field, type/paste the following qualifier: HTTP.REQ.HOSTNAME.CONTAINS("StorageZoneControllerFQDN") && HTTP.REQ.URL.CONTAINS("/cifs/" // HTTP.REQ.URL.CONTAINS("/sp/").

   Click **Create**.

   CLI command:
   ```bash
   add cs policy Connector_Requests -rule "HTTP.REQ.HOSTNAME.CONTAINS("StorageZoneControllerFQDN") && (HTTP.REQ.URL.CONTAINS("/cifs/") || HTTP.REQ.URL.CONTAINS("/sp/"))"
   ```
See the following screen shot for reference when you complete with Section 3.
4. Create and Configure Content Switching VServer

1. Go to Content Switching > Virtual Servers. Create a Content Switch VServer of Protocol type SSL. Do **not** select Create.

2. Bind the two Content Switch Virtual Server Policies created in previous step. This is performed by inserting CS Policy, the corresponding LBVServer created in Section 2.

3. Go to the SSL Settings tab and bind the certificate (must be a publicly accessible FQDN). Click **Create**.
CLI Commands:

```
add cs vserver szc20_csv SSL 192.168.1.12 443 -cltTimeout 180
bind cs vserver szc20_csv -policyName Data_Requests -targetLBVserver SZC2.0_LBVData - priority 100
bind cs vserver szc20_csv -policyName Connector_Requests -targetLBVserver SZC2.0_LBVConnector - priority 110
bind ssl vserver szc20_csv -certkeyName szc20
```
5. Create HTTP Callouts

1. The purpose of creating HTTP callouts is to validate traffic before allowed to proceed unfettered. Go to AppExpert \ HTTP Callouts section of GUI. Create an HTTP Callout named sf_callout. Define the Virtual Server or IP Address of which we will direct the callout to.
   a. Under **Server Response**, choose a **Return Type** of **Bool**.
   b. In **Expression to extract data from the response** enter: HTTP.RES.STATUS.EQ(200),NOT

2. Under Request to send to the server, click Attribute-based and then click **Configure Request Attributes**.
   a. Select Get Method.
   b. In Host Expression enter the virtual server IP address or the host IP address for any of the StorageZone Controllers. This is required for correct operation.
c. In URL Stem Expression enter: "/validate.ashx?RequestURI=" +
   HTTP.REQ.URL.BEFORE_STR("&h").HTTP_URL_SAFE.B64ENCODE + 
   
   HTTP.REQ.URL.QUERY.VALUE("h")
   
d. Click OK and then return to the Configure HTTP Callout dialog box.

3. Click CREATE.

   CLI commands:
   add policy httpCallout sf_callout
   set policy httpCallout sf_callout -vServer SZC2.0_LBVData -returnType BOOL -hostExpr 192.168.1.12 -
   urlStemExpr "/validate.ashx?RequestURI=" + HTTP.REQUEST.URL.HTTP_URL_SAFE.B64ENCODE + "&h=" +
   HTTP.REQUEST.URL.QUERY.VALUE("h") -scheme http -resultExpr "HTTP.RES.STATUS.EQ(200).NOT"

4. Follow the preceding steps to configure an HTTP callout named sf_callout_y. Use the same settings except modify it to the following expression:

5. In URL Stem Expression enter: "/validate.ashx?RequestURI=" + HTTP.REQUEST.URL.HTTP_URL_SAFE.B64ENCODE + 
   "&h="

   CLI Commands:
   add policy httpCallout sf_callout_y
   set policy httpCallout sf_callout_y -vServer SZC2.0_LBVData -returnType BOOL -hostExpr 192.168.1.12 -
   urlStemExpr "/validate.ashx?RequestURI=" + HTTP.REQUEST.URL.HTTP_URL_SAFE.B64ENCODE + "&h=" -
   scheme http -resultExpr "HTTP.RES.STATUS.EQ(200).NOT"
6. Create and Configure Responder Policy to use HTTP Callout

1. Go to AppExpert > Responder > Policies section of the GUI. Add a new Responder Policy.

2. In the Configure Responder Policy dialog box for Action field, choose Drop expression window. In Expression, enter the following:

   ```
   http.REQ.URL.CONTAINS("&h=") && http.req.url.contains("/crossdomain.xml").not &&
   http.req.url.contains("/validate.ashx?requri").not && SYS.HTTP_CALLOUT(sf_callout) ||
   http.REQ.URL.CONTAINS("&h=").NOT && http.req.url.contains("/crossdomain.xml").not &&
   http.req.url.contains("/validate.ashx?requri").not && SYS.HTTP_CALLOUT(sf_callout_y)
   ```

3. Click Create.

CLI command:
```
add responder policy sf_sz_policy "http.REQ.URL.CONTAINS("&h=") &&
http.req.url.contains("/crossdomain.xml\"\").not &&
http.req.url.contains("/validate.ashx?requri\"\").not &&
SYS.HTTP_CALLOUT(sf_callout) ||
http.REQ.URL.CONTAINS("&h=\"\"\".NOT &&
http.req.url.contains("/crossdomain.xml\")\not &&
http.req.url.contains("/validate.ashx?requri\")\not &&
SYS.HTTP_CALLOUT(sf_callout_y)" DROP
```
7. **Bind Responder Policy to Load Balancing VServer(s)**

1. Bind responder policy to Load Balancing Virtual Server as defined in Section 2, by navigating to **Policies > Responder** under the defined Load Balanced Virtual Server.

   CLI Command:
   ```bash
   bind lb vserver SZC2.0_LBVData -policyName sf_sz_policy -priority 100 -gotoPriorityExpression END -type REQUEST
   ```

   With the completion of the preceding exercises, the NetScaler Configuration has been finalized.
8. Create and Configure Authentication VServer

There is an optional configuration step further securing StorageZone Connector which is used with XenMobile Enterprise, MDM, and App Editions. While authentication to NetScaler is optional, it is a recommended best practice. To configure this feature, complete the following steps:
1. Create LDAP Server Profile/Policy
2. Create/configure associated Session Profile/Policy
3. Create Authentication VServer
4. Bind Authentication Settings to StorageZone Connector VServer

Create LDAP Server Profile/LDAP Policy
1. To create the LDAP Server Profile, navigate to Security > AAA – Application Traffic > Policies > Authentication > LDAP section of the GUI.
2. Click the Servers tab in the right pane to create a new Authentication Server (Profile) entity. Populate this dialogue with all pertinent details.
3. Ensure to add the SSO Name Attribute of “userPrincipalName” before selecting Create. Click the **Create** button to finish adding Authentication Profile.

CLI Method:
```
add authentication ldapAction SZC_Auth -serverIP 192.168.1.10 -ldapBase "DC=nsdemo,DC=ctx" -ldapBindDn admin@nsdemo.ctx -ldapBindDnPassword password -encrypted -ldapLoginName sAMAccountName -groupAttrName memberOf -subAttributeName cn -ssoNameAttribute userPrincipalName
```
4. To create the LDAP Policy, in the same section of the GUI (Security > AAA – Application Traffic > Policies > Authentication > LDAP).

5. Click the Policies tab to create a new Authentication Policy.

6. Assign a Name to the new policy and bind the Server profile created in Section 1. In the Expression field, add the True Value expression and click Create.

![GUI Screenshot of Creating an LDAP Policy](image)

**CLI Command:**

```
add authentication ldapPolicy SZC_AuthPol ns_true SZC_Auth
```

**Create/configure associated Session Profile/Policy**

To create/configure associated Session Profile/Policy associated with the authentication policy defined, complete the following steps:

1. Go to the Security > AAA – Application Traffic > Policies > Session section and click the Profiles tab in the right pane.
2. Select to create a new profile and define the relevant settings, again adding the correct SSO domain.
3. Click Create once completed.
4. To create the Session Policy, in the same section of the GUI Security > AAA–Application Traffic > Policies > Session, click Policies tab to create a new Session Policy. Assign a Name to the new policy and bind the session profile created in Section 1. In the expression field, add the “True Value” expression, click Create.

CLI commands:
add tm sessionAction SZC_SessionProfile -ssoDomain nsdemo.ctx add tm sessionPolicy SZC_SessionPolicy ns_true SZC_SessionProfile

Create Authentication VServer
1. In this step we will create an Authentication Virtual Server and bind the Authentication Policy we created in the previous step. Navigate back up to “AAA – Application Traffic \ Virtual Servers” section and elect to create a new Authentication Virtual Server. Provide relevant data and ensure that the base DN is defined in the domain field. Select the appropriate certificate. Do not click create yet.
2. Go to the Authentication tab and bind the Authentication Policy created in Step 1. Do not click Create. Navigate to the Policies tab.

3. Under the Policies tab, select Session > Insert Policy and bind the Session Policy created in step 8b, click Create.
CLI commands:
add authentication vserver SZC20_AuthVServer SSL 192.168.1.13 443 -AuthenticationDomain nsdemo.ctx
bind authentication vserver SZC20_AuthVServer -policy SZC_AuthPol -priority 100
bind authentication vserver SZC20_AuthVServer -policy SZC_SessionPolicy -priority 100 bind ssl vserver SZC20_AuthVServer -certkeyName wildcard

Bind Authentication Settings to StorageZone Connector VServer
1. In this step, bind the authentication Settings to StorageZone Connector Load Balancing VServer. In the GUI, go to the StorageZone Connector Load Balancing VServer (Traffic Management > Load Balancing > Virtual Servers).

2. Click Advanced tab, scroll down and expand the “Authentication Settings” section. Select the 401 Based Authentication check box and select the defined Authentication VServer (created in the previous section).

3. When complete, go to the Method and Persistence and modify the Persistence method to Cookie
**Insert.** Set the appropriate Time-out value (in minutes).

CLI Commands:
```
set lb vserver SZC2.0_LBVConnector -persistenceType COOKIEINSERT -timeout 240 -authn401 ON -authnVsName SZC20_AuthVServer
```

This concludes the steps required for the Optional configuration.