Guide to Deploying NetScaler as an Active Directory Federation Services Proxy

Enabling seamless authentication for Office 365 use cases

CITRIX®

Table of Contents

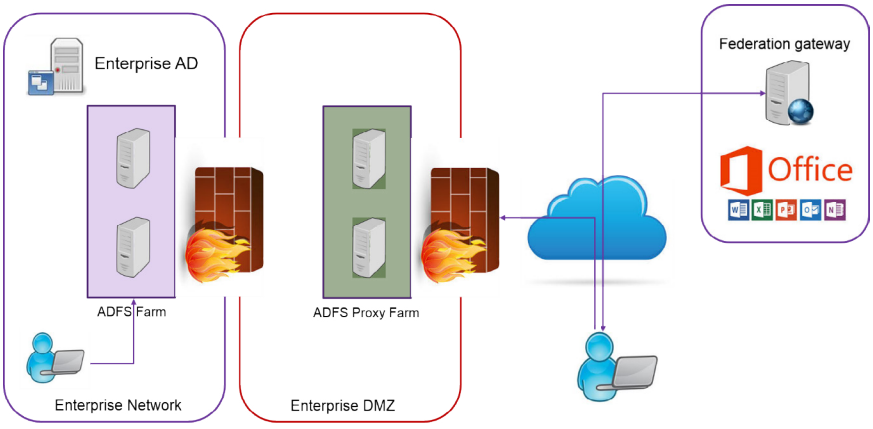
Recently, more enterprises are migrating to a cloud-based application deployment model. Thanks to cloud-based services such as Microsoft Office 365, this migration has accelerated. Cloud-based app deployment provides significant added value, but at the same time, it changes the underlying infrastructure for the enterprise. One of the critical services enterprise IT teams worry about is authentication for users connecting from within and outside the organization.

When migrating to the cloud, enterprises want to ensure the user experience does not change. However, seamless access to services hosted outside the enterprise data center requires a new component in app deployment design. No one wants the Active Directory password to travel on the wire outside the data center. Therefore, federation becomes a natural and proven alternative. Referring to primarily to Microsoft services, Active Directory Federation Services (ADFS) is the solution you are looking for. The ADFS security token service extends the single sign-on, (SSO) experience for Active Directory-authenticated clients to resources outside the enterprise data center.

An ADFS server farm allows internal users to access external cloud-hosted services. But the moment external users are brought into the mix, they must be given a way to connect remotely and access cloud-based services through federated identity. This is where an ADFS proxy plays a major role – giving external users SSO access to both internal federation-enabled resources as well as cloud resources such as Office 365. The purpose of the ADFS proxy server is to receive and forward requests to ADFS servers that are not accessible from the Internet.

The ADFS proxy plays critical role in remote user connectivity and application access. Citrix® NetScaler® has been playing similar roles – remote user connectivity and application access – for more than a decade. NetScaler has the right technology to enable secure connectivity, authentication and handling of federated identity, and thus it becomes the preferred solution for replacing an existing ADFS proxy or supporting a new ADFS implementation. Most enterprises want to reduce the footprint in the DMZ, and hence, they appreciate the fact that, in addition to its traditional functions, NetScaler can serve as ADFS proxy. This approach avoids the need to deploy an additional component in the DMZ.

ADFS proxy deployment



Packet flow of how the ADFS proxy helps with external user access:

1. External user accesses internal or external applications enabled by ADFS.
2. User is redirected to the applicable federation service for authentication.
3. User is redirected to the enterprise's internal federation service.
4. User is connected to the ADFS proxy in the DMZ and is presented with a sign-on page.
5. ADFS proxy takes inputs from the external user and connects to the ADFS farm.
6. ADFS proxy presents external user credentials to the ADFS farm.
7. ADFS server authenticates the external user with enterprise Active Directory.
8. ADFS server returns authorization cookie with a signed security token and claims.
9. ADFS proxy sends the token and claim information to external user.
10. User connects to the federation service where the token and claims are verified.
11. Based on validation, the federation service provides the user with a new security token.
12. The external user provides the new authorization cookie with security token to the resource for access.

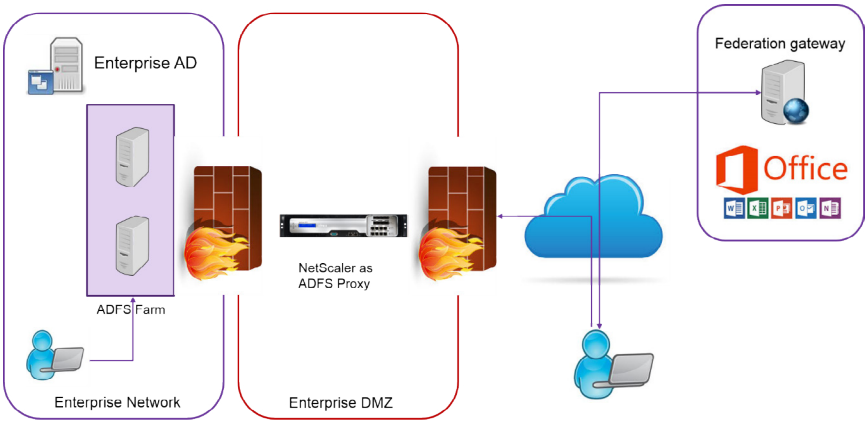
In most use cases you will run ADFS and the ADFS proxy farm, which would require load balancing and scale with high availability. If you are using the NetScaler ADC for load balancing of your ADFS proxy farm and other key services, only one additional step is needed to set up NetScaler as a replacement for the ADFS proxy farm. This means NetScaler does not just play the ADC role, but also assumes ownership of the processes performed by the ADFS proxy for external user access scenario.

NetScaler is a proven remote access solution for the DMZ. We can use the AAA for Traffic Management (AAA-TM) feature of NetScaler to fulfill the ADFS proxy use case while other product security features add to the overall value of this solution.

Microsoft recommendations for third-party ADFS proxies

Microsoft Requirement and Recommendations	NetScaler Competancy
Proxy must not modify Response body	Yes
Proxy must pass through all HTTP headers to back-end STS	Yes
Proxy must not issue HTTP 302 responses	Yes
All requests must be passed through to ADFS farm	Yes
All external requests must be rerouted to back-end STS	Yes
Proxy must persist to same STS for multi-legged NTLM auth flow	Persistency
All requests to ADFS must be rerouted to same URL on back-end STS	Yes
Proxy must pass through all query string parameters	Yes
Proxy may provide form based login	AAA-TM
Proxy may use credentials to perform NTLM auth on ADFS	SSO
Proxy may also perform two factor auth as needed	AAA-TM
For Office 365 access scenarios, Proxy must provide additional info	Yes

Deployment scenario and access flow with NetScaler as ADFS proxy



Packet flow of how NetScaler as ADFS proxy helps with internal/external user access:

1. Internal/external user access to Office 365 application is enabled by ADFS.
2. User is redirected to the applicable federation service for authentication.
3. User is redirected to the enterprise's internal federation service.
4. Internal user is load balanced to the ADFS farm.
5. External user connects to NetScaler AAA-TM logon page.
6. User is authenticated against Active Directory or similar authentication service.
7. Post authentication, NetScaler does SSO (Kerberos/NTLM) to the ADFS farm.
8. ADFS server validates SSO credentials and returns STS token.
9. External user connects to the federation service where the token and claims are verified.
10. Based on validation, the federation service provides the user with a new security token.
11. External user provides authorization cookie with security token to the resource for access.

Here both internal and external users can go through the NetScaler path with the only difference being that external users are required to pre-authenticate with the NetScaler AAA-TM module. For this access scenario, the AAA-TM vserver must be set up on NetScaler for pre-authentication. Internal users can be directly load balanced to the ADFS server farm.

Benefits of using NetScaler as ADFS proxy

1. Caters to both load balancing and ADFS proxy needs
2. Works with both internal and external user access scenarios
3. Supports rich methods for pre-authentication?
4. Provides an SSO experience for end users
5. Supports both active and passive protocols
    a. Examples of active protocol apps – Outlook, Lync
    b. Examples of passive protocol apps – Outlook web app, browsers
6. Hardened device for DMZ-based deployment
7. Adds value with additional core ADC features
    a. Content Switching
    b. SSL offload
    c. Rewrite
    d. Responder
    e. Rate Limit
    f. Security

Note that for active protocol-based scenarios, users connect to Office 365 and provide their credentials. Microsoft Federation Gateway contacts the ADFS service on behalf of the active protocol client and submits their credentials. Post authentication, the ADFS service provides Federation Gateway with a token, which in turn is submitted to Office 365 to provide client access.

For active protocol-based use cases, clients typically authenticate on NetScaler using 401 NTLM. The configuration section below describes how to set up NetScaler for both active and passive protocol-based use cases.

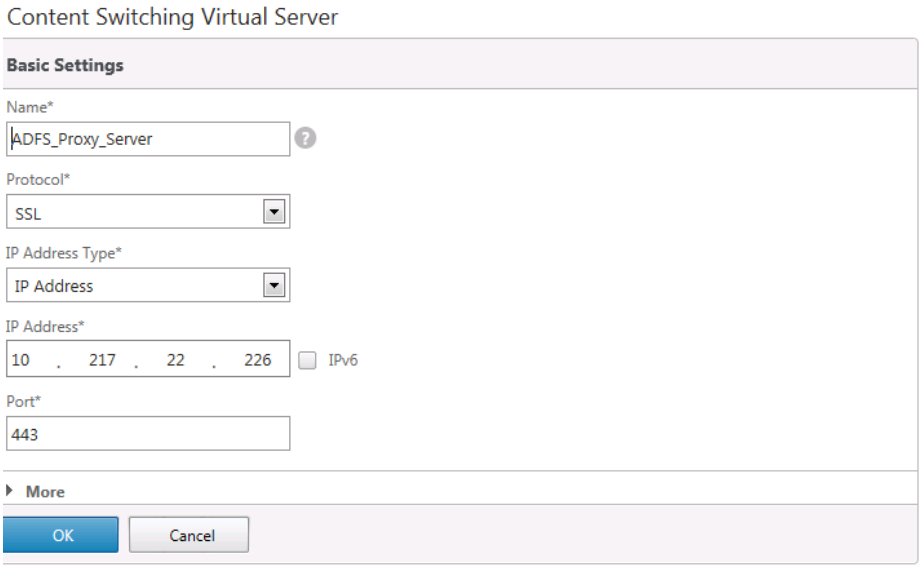
Configuration and setup details

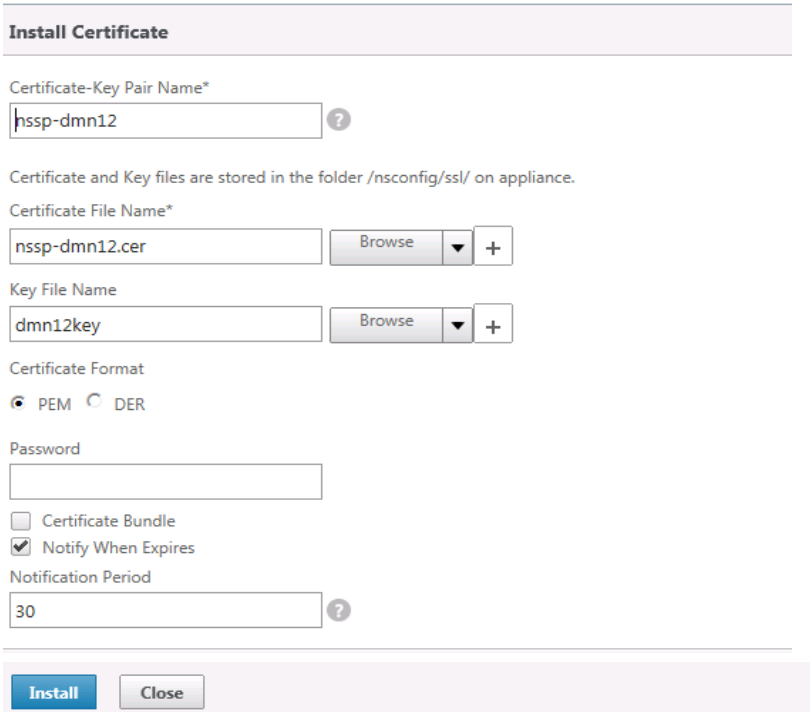
This guide provides the configuration workflow for active clients (Section A) as well as passive clients (Section B). Deployments covering both active and passive clients can follow section A and B sequentially for configuration flow.

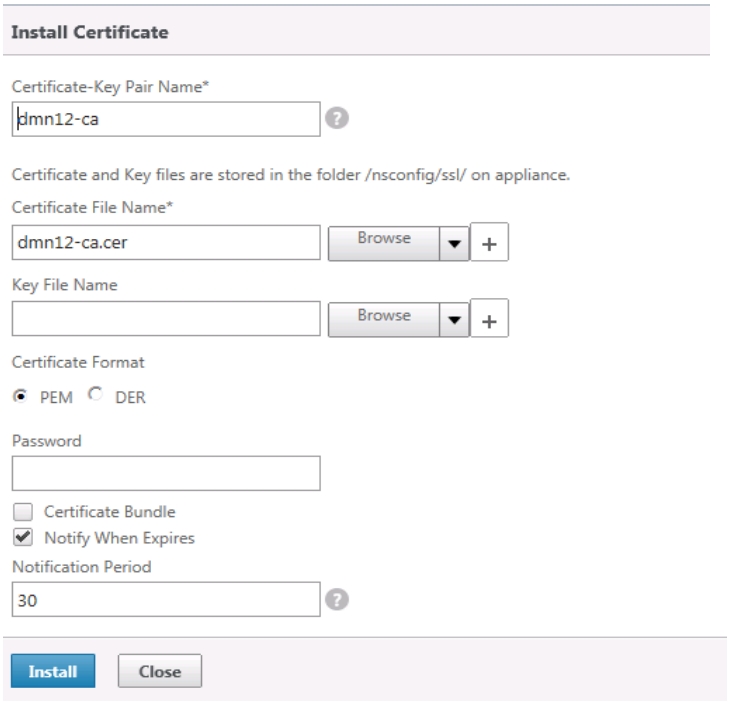
The configuration given below is for external users. For internal users, use NetScaler as a load balancing vserver for the ADFS farm. If internal users have to be authenticated at by NetScaler, Section A configuration will suffice for both passive and active clients.

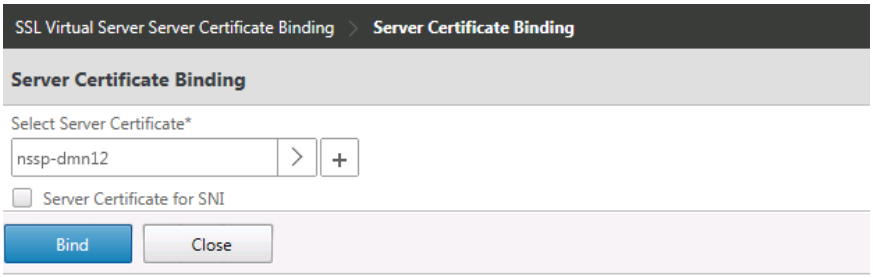
Section A: Active clients / internal user configuration flow

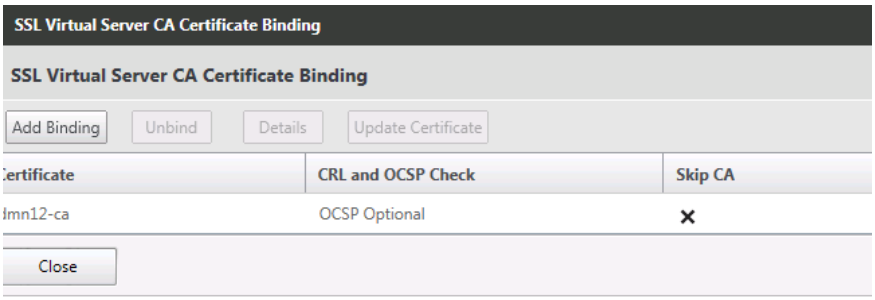
1. Create content switching vserver, bind SSL Certkey, bind CA certificate.



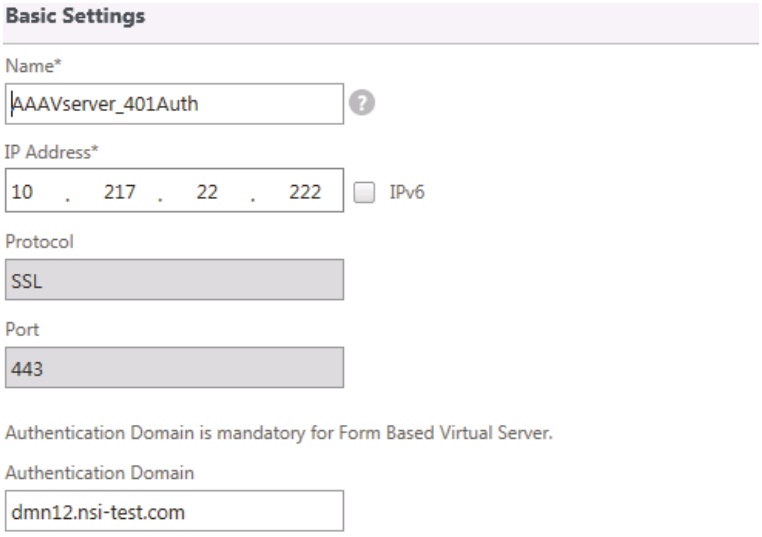



Install Certificate
Certificate-Key Pair Name*
dmn12-ca
Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.
Certificate File Name*
dmn12-ca.cer
Browse
Key File Name
Browse
Certificate Format
PEM
DER
Password
Certificate Bundle
Notify When Expires
Notification Period
30
Install
Close


SSL Virtual Server Server Certificate Binding
Server Certificate Binding
Server Certificate Binding
Select Server Certificate*
nssp-dmn12
Server Certificate for SNI
Bind
Close

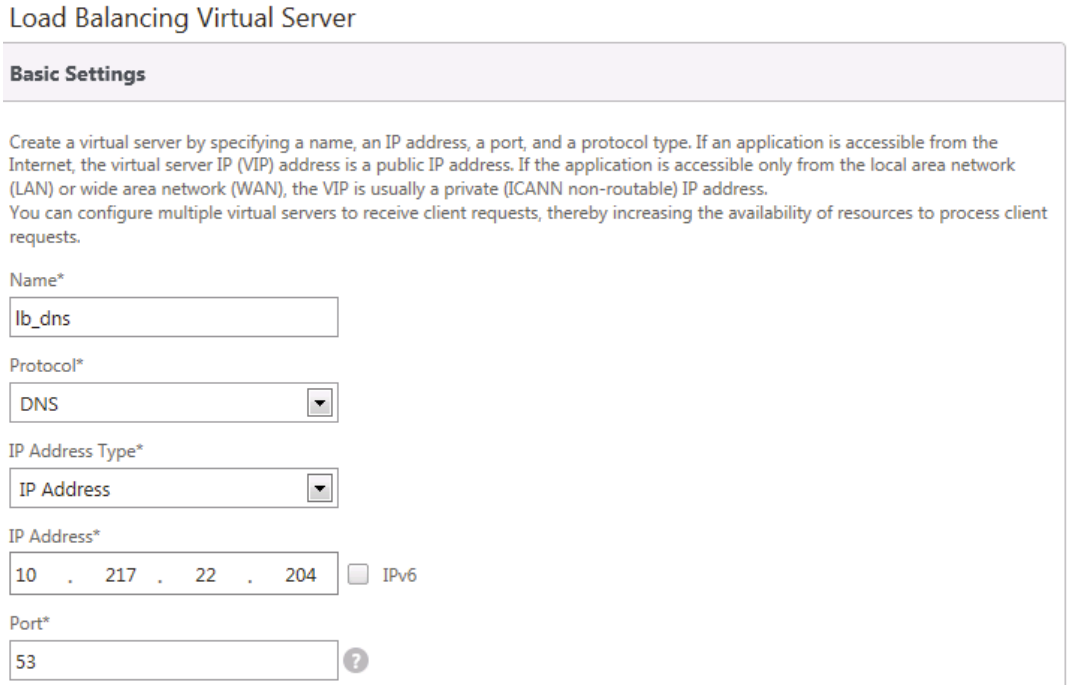

SSL Virtual Server CA Certificate Binding
SSL Virtual Server CA Certificate Binding
Add Binding
Unbind
Details
Update Certificate
CRL and OCSP Check
Skip CA
dmn12-ca
OCSP Optional
Close

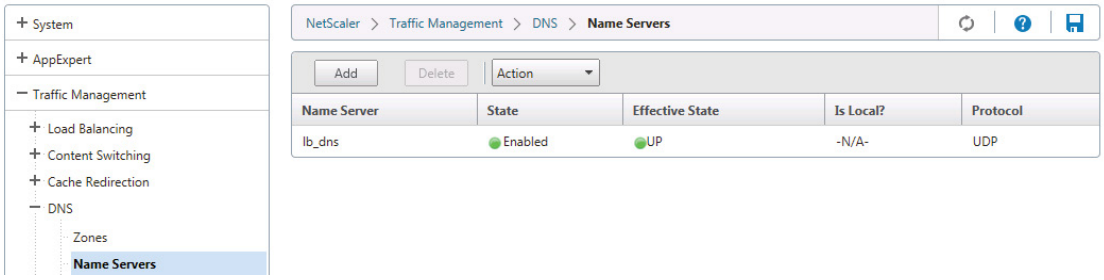
2. Create AAA vserver, bind SSL certificate, bind negotiate policy, bind session policy for Kerberos SSO. This vserver can be set to a private IP address as it is not accessed externally.



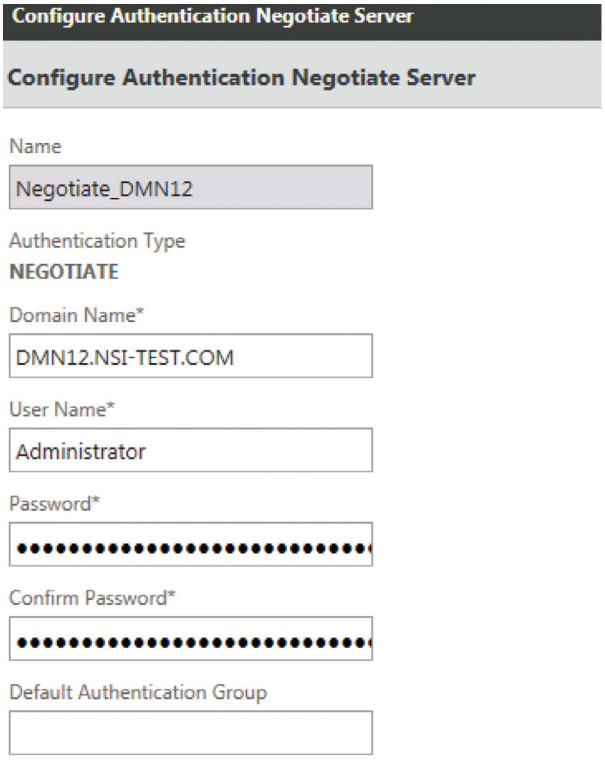
Now bind the server and CA certificate to this vserver as showed in step 1.

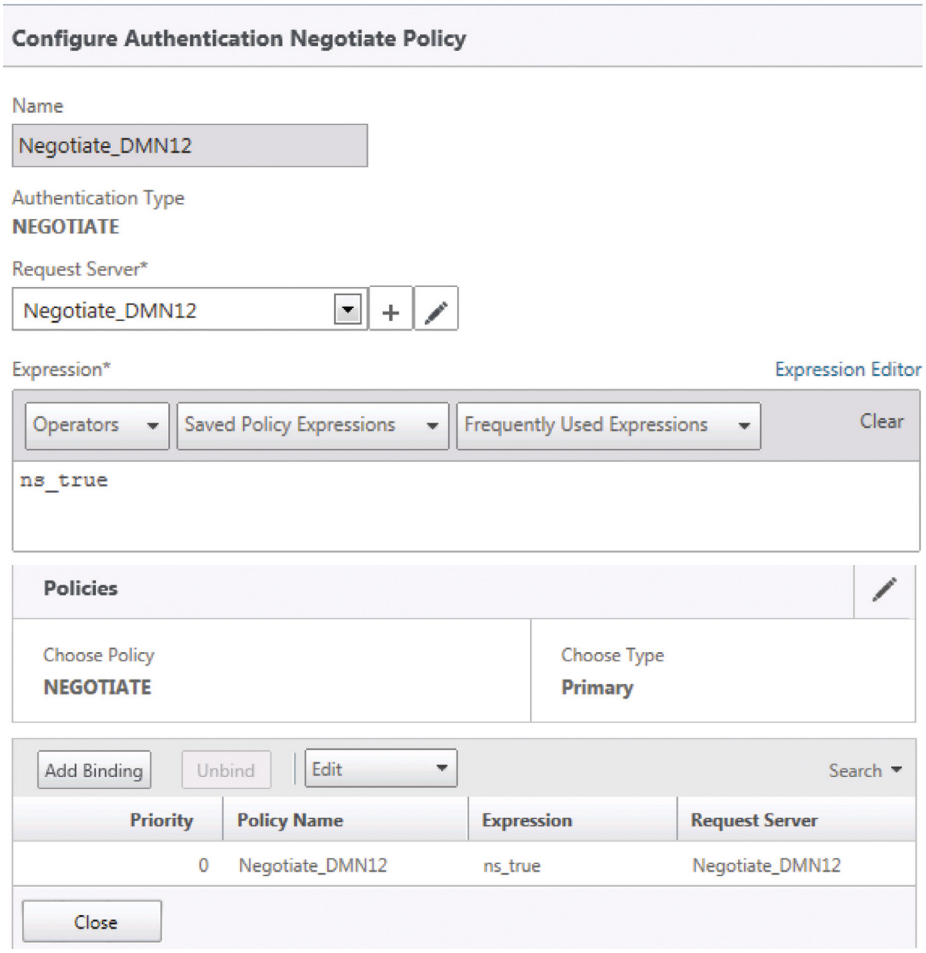
Please ensure that the proper DNS server is configured, which is required for client-side NTLM authentication as well as Kerberos SSO. If you have a single DNS server, create a Nameserver pointing to it. In the below configuration we are binding multiple DNS servers as services to the load balancing vserver.

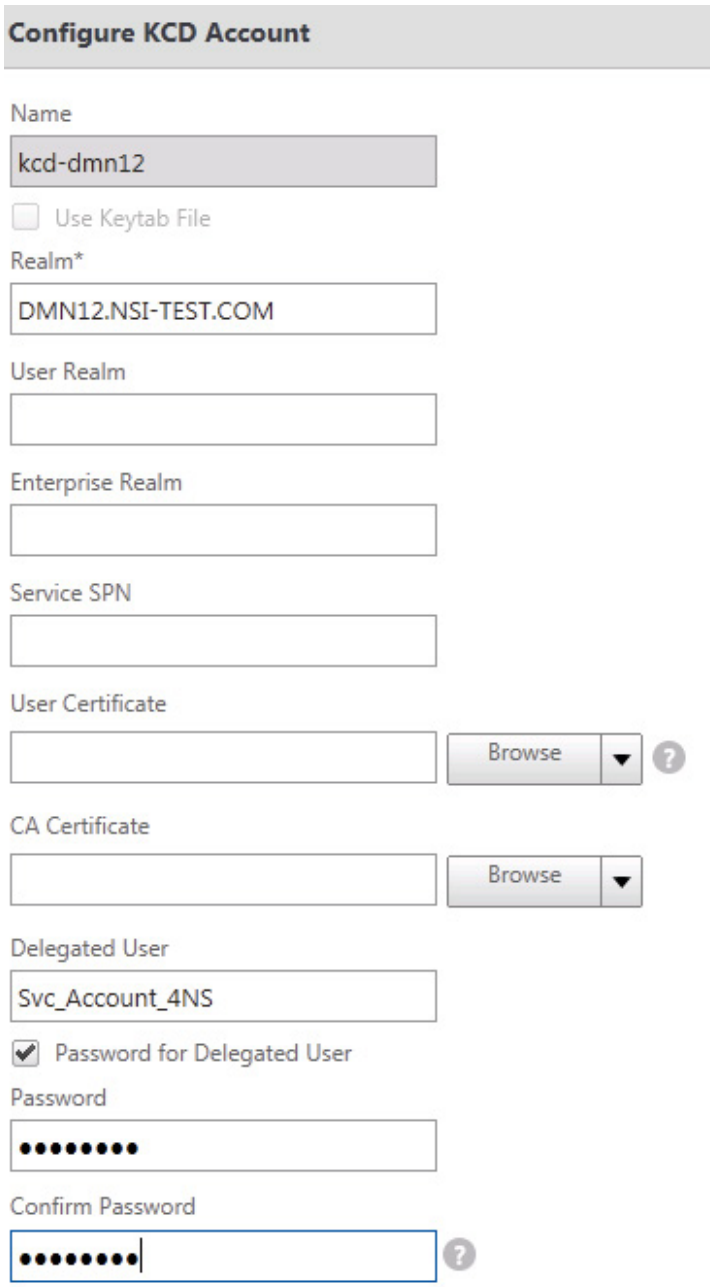


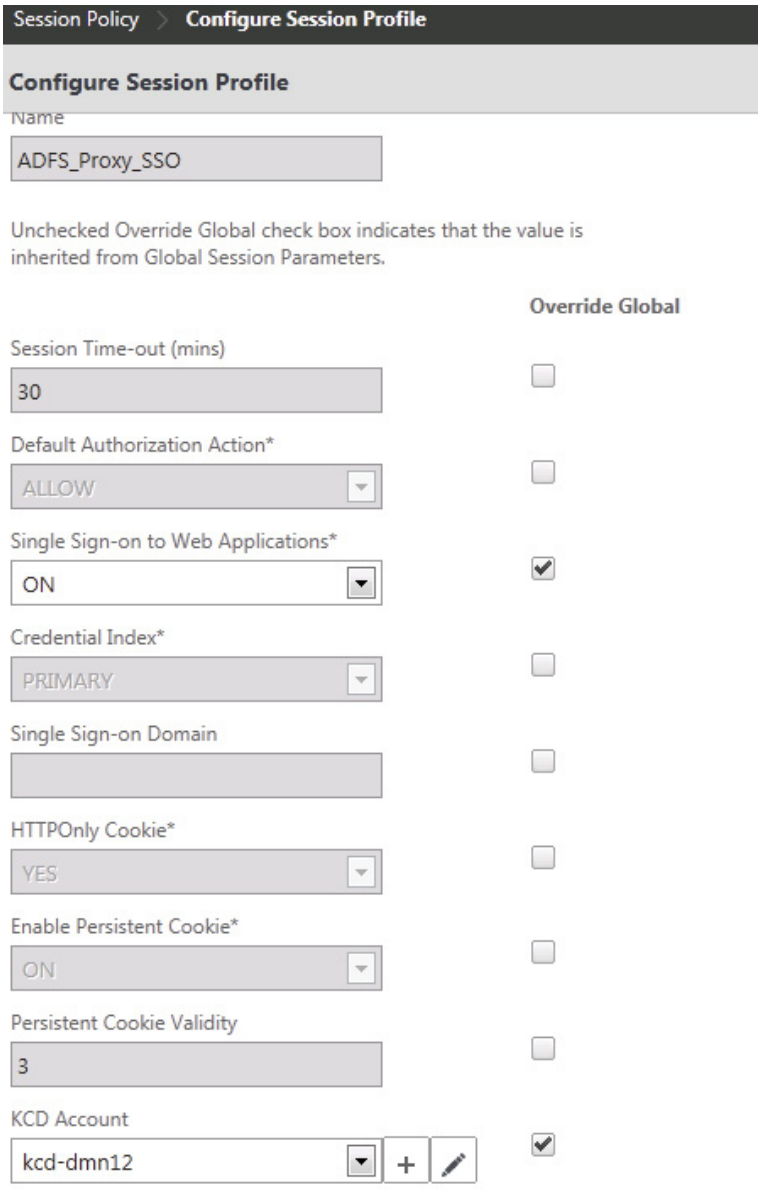


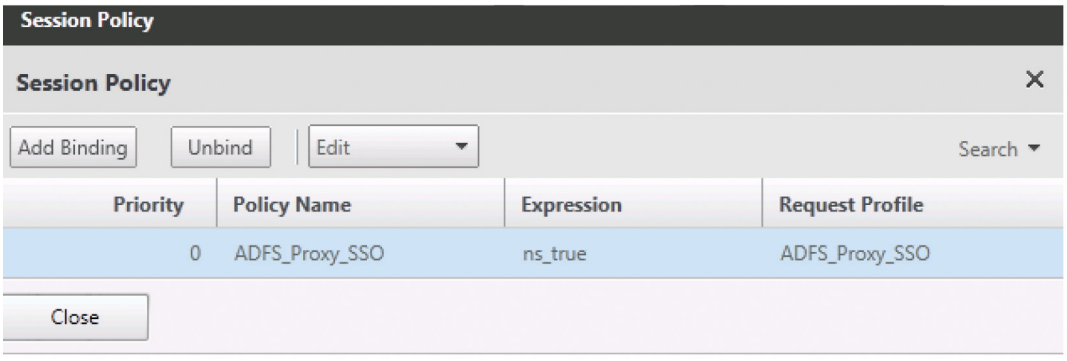
Create a negotiate action policy and bind it to the AAA vserver.




Configure Authentication Negotiate Policy
Name
Negotiate_DMN12
Authentication Type
NEGOTIATE
Request Server*
Negotiate_DMN12
Expression*
Expression Editor
Operators
Saved Policy Expressions
Frequently Used Expressions
Clear
ns_true
Policies
Choose Policy
NEGOTIATE
Choose Type
Primary
Add Binding
Unbind
Edit
Search
Priority
Policy Name
Expression
Request Server
0
Negotiate_DMN12
ns_true
Negotiate_DMN12
Close

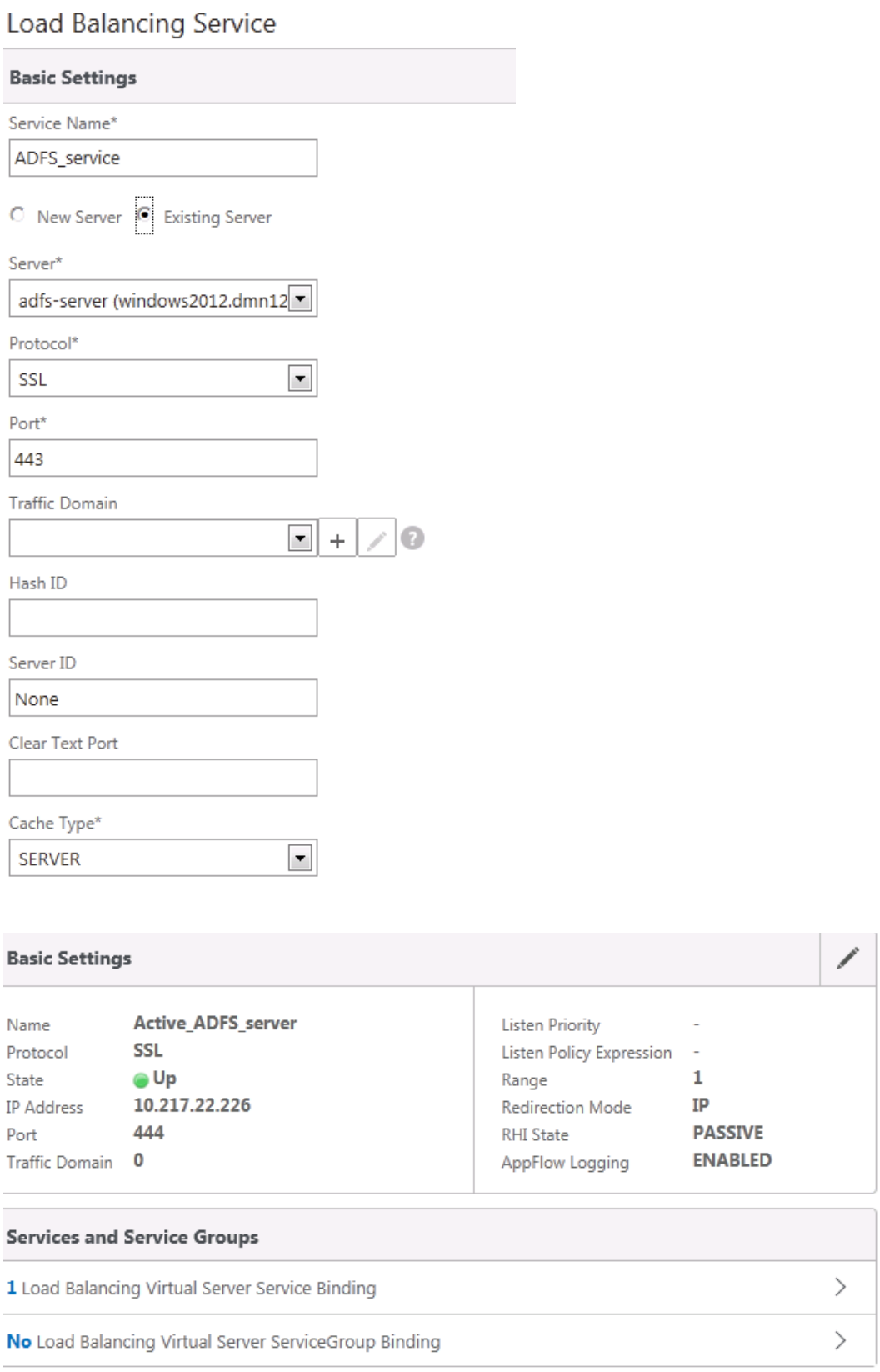

Configure KCD Account
Name
kcd-dmn12
Use Keytab File
Realm*
DMN12.NSI-TEST.COM
User Realm
Enterprise Realm
Service SPN
User Certificate
Browse
CA Certificate
Browse
Delegated User
Svc_Account_4NS
Password for Delegated User
Password
Confirm Password

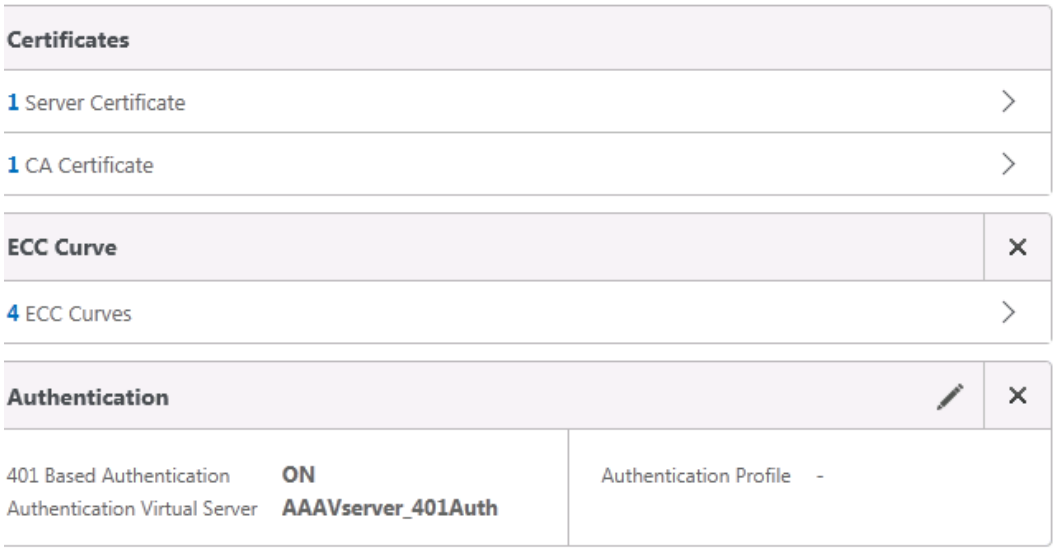




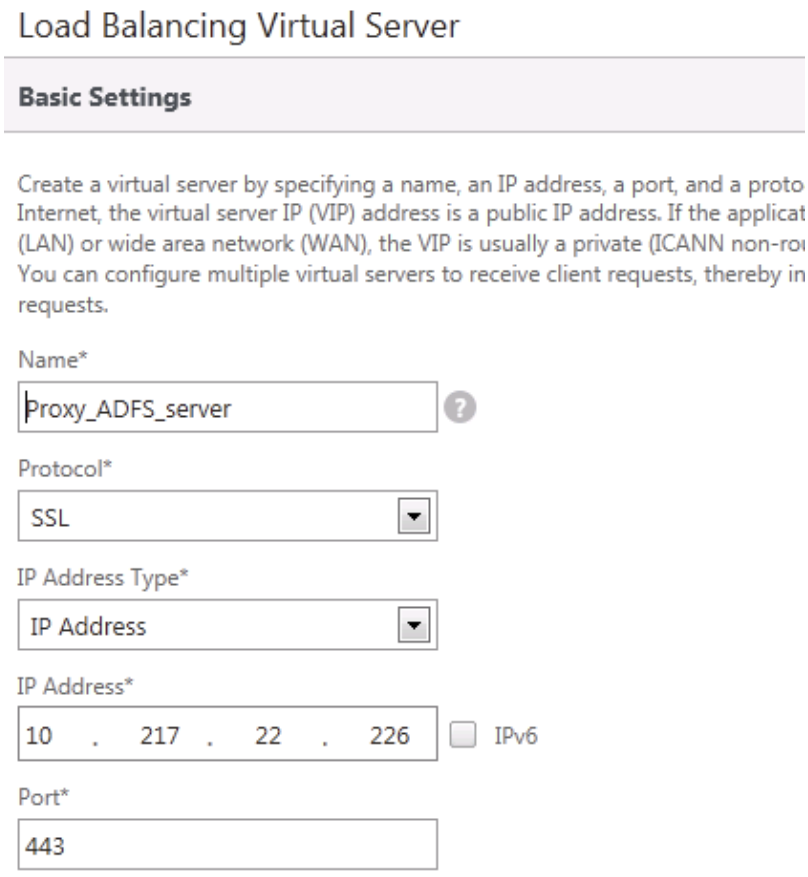
Bind the session policy to the AAA vserver.

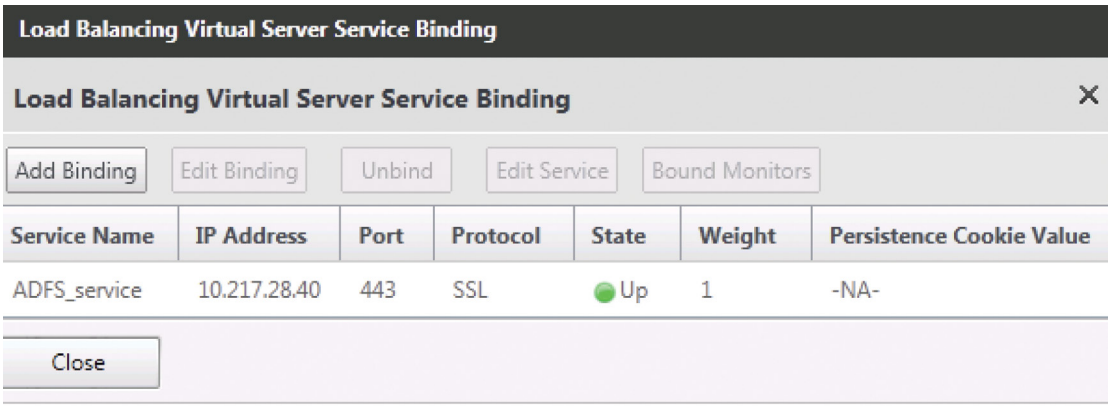
3. Create a default load balancing vserver that will send 401:Negotiate/NTLM response to authenticate the user and perform Kerberos SSO to the backend.


Load Balancing Service
Basic Settings
Service Name*
ADFS_service
New Server
Existing Server
Server*
adfs-server (windows2012.dmn12
Protocol*
SSL
Port*
443
Traffic Domain
Hash ID
Server ID
None
Clear Text Port
Cache Type*
SERVER
Basic Settings
Name
Active_ADFS_server
Protocol
SSL
State
Up
IP Address
10.217.22.226
Port
444
Traffic Domain
0
Listen Priority
-
Listen Policy Expression
-
Range
1
Redirection Mode
IP
RHI State
PASSIVE
AppFlow Logging
ENABLED
Services and Service Groups
1 Load Balancing Virtual Server Service Binding
No Load Balancing Virtual Server ServiceGroup Binding

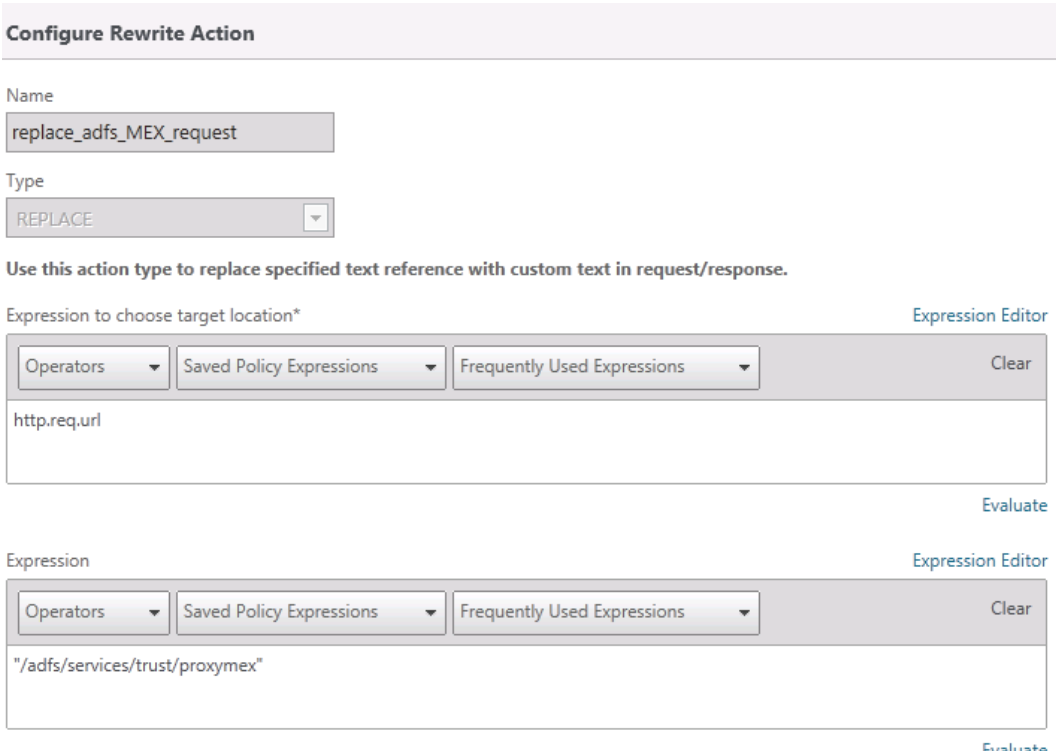


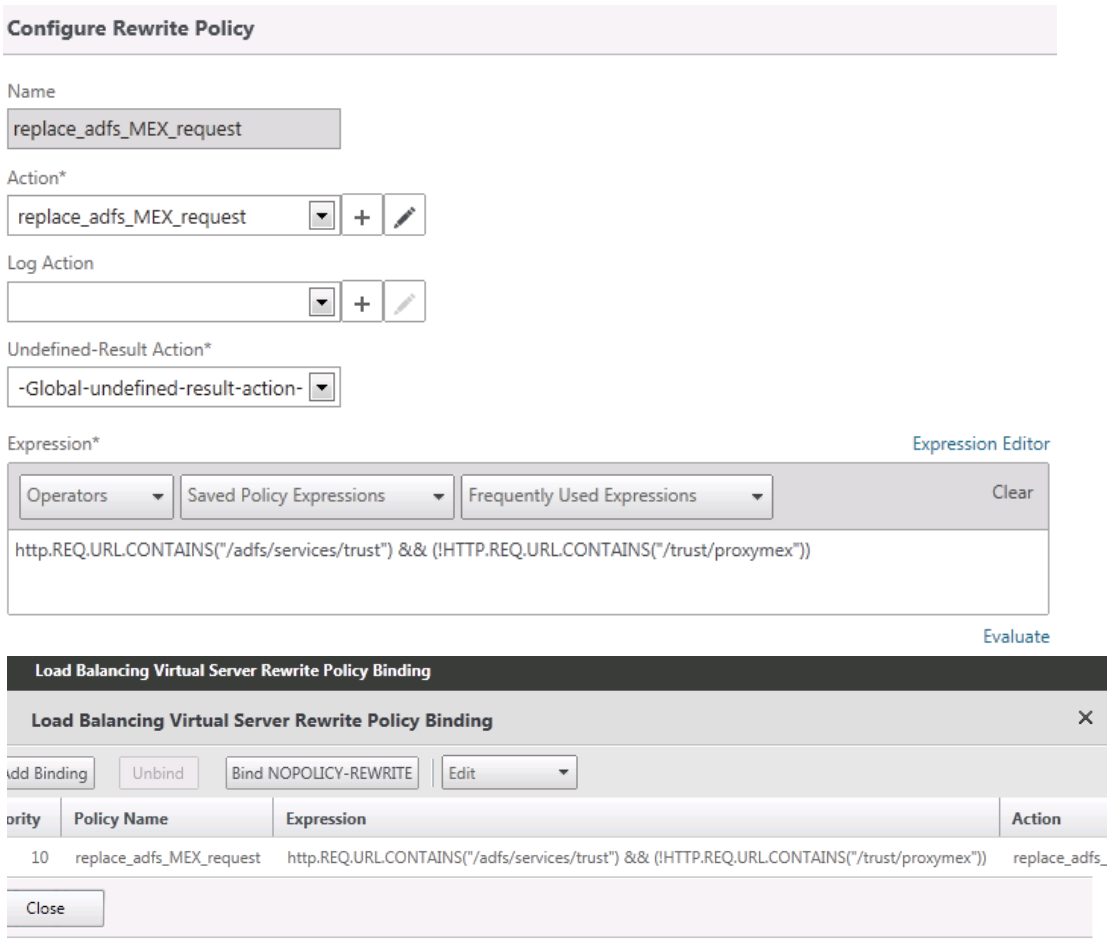
4. Create a load balancing vserver, which will simply pass the requests to the backend and convert the request URL from /adfs/services/trust to /adfs/services/trust/proxymex.



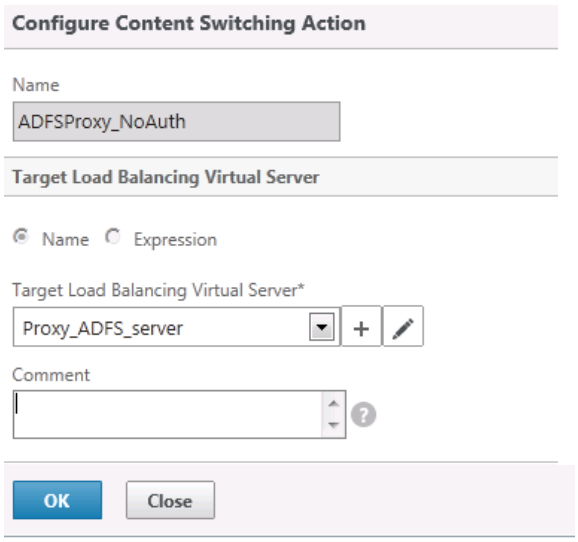


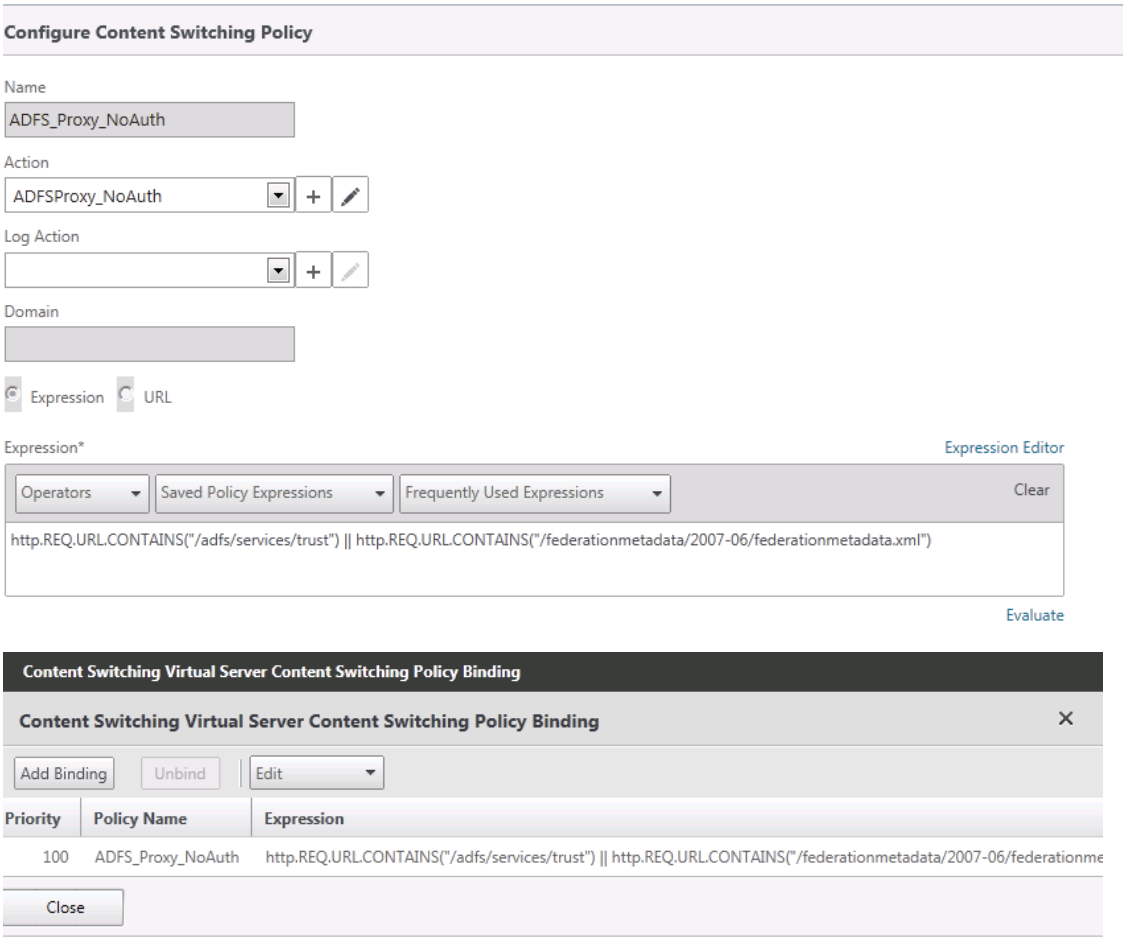
Bind server and CA certificate to the newly created vserver.



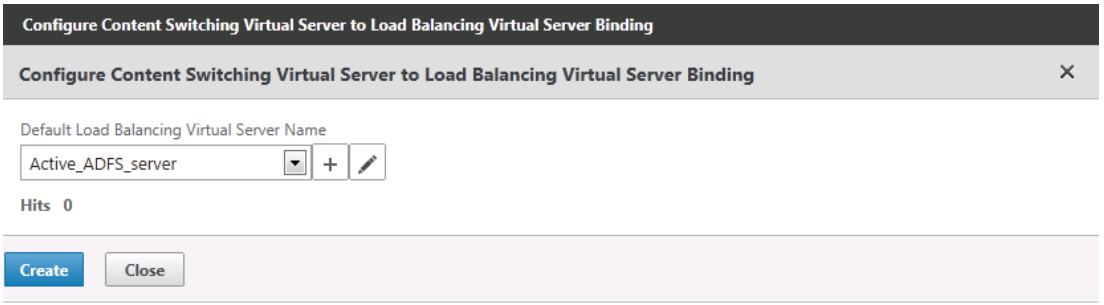


5. Create content switching policy for requests containing /adfs/services/trust and /federationmetadata/2007-06/federationmetadata.xml to go to the proxy server without any authentication.





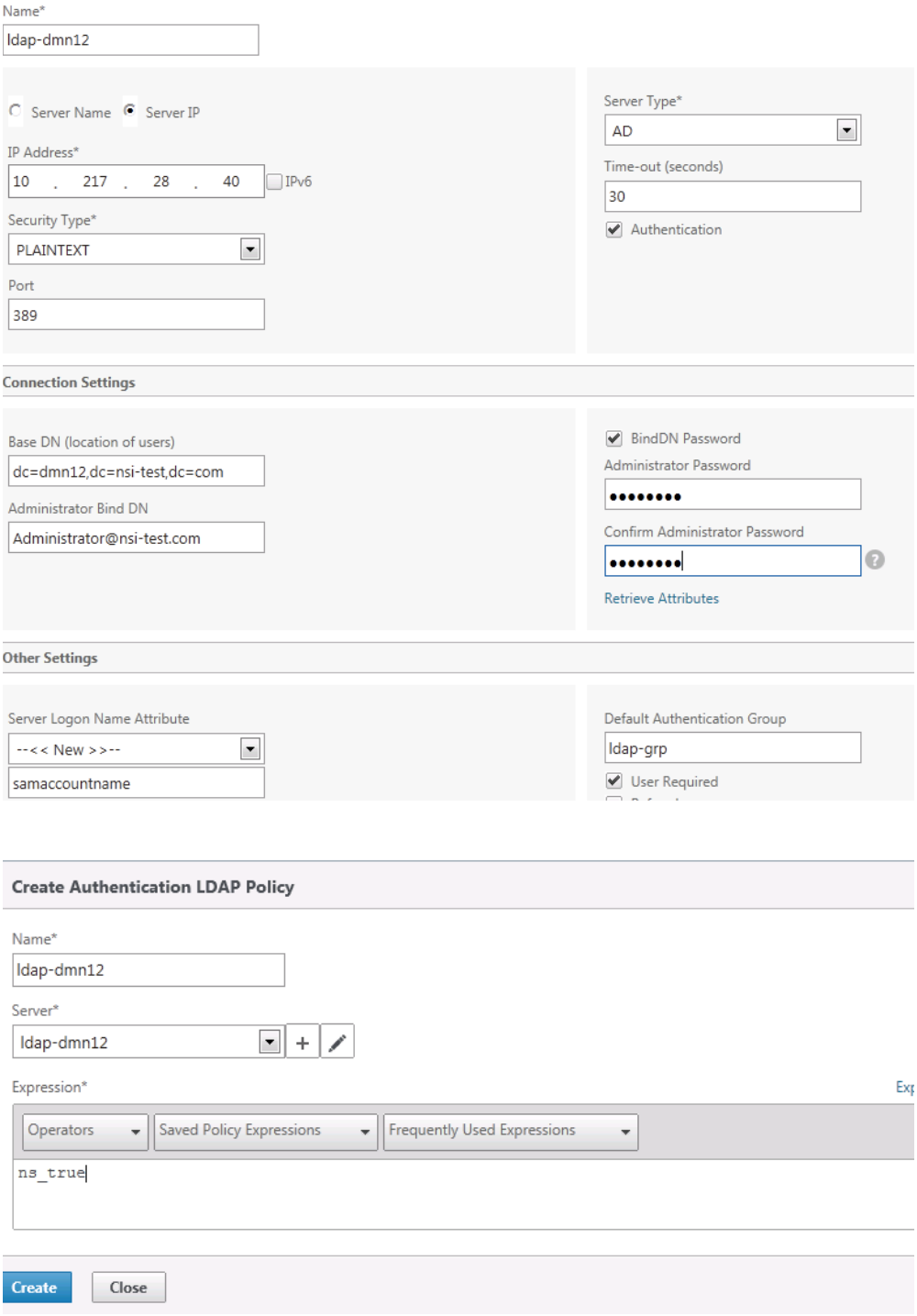
6. Set the load balancing vserver with authentication enabled as the default vserver for the content switching vserver.

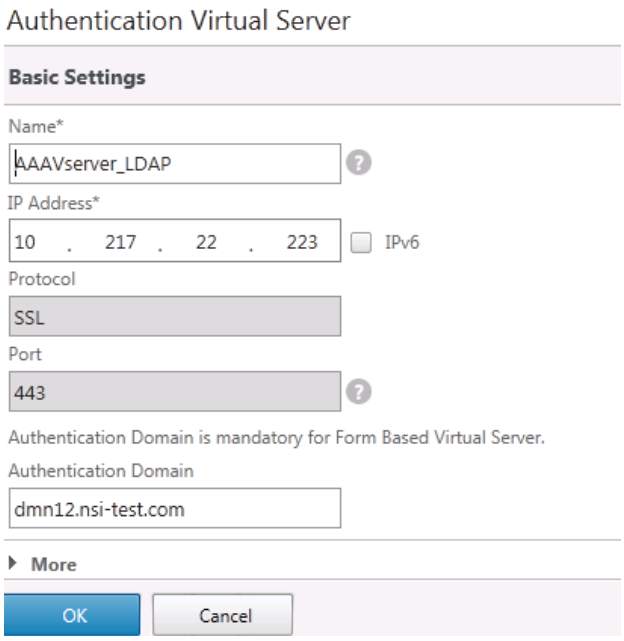


Section B: Passive user configuration flow

Note: we will use the same content switching vserver created in Section A but have different rules corresponding to passive clients.

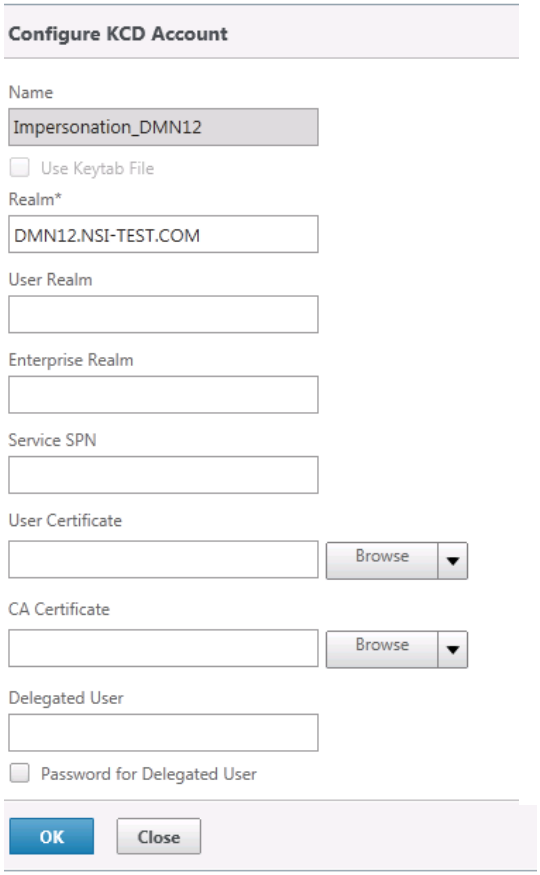
1. Create AAA vserver, set authentication domain and bind LDAP policy.
   a. Create a KCD Account for Kerberos impersonation and a session policy for SSO.





Bind SSL server and CA certificate to the vserver.

2. Create a KCD account for Kerberos impersonation and ensure that DNS and NTP servers are con figured properly. Create a session policy and bind it to the AAA vserver.



Create Session Profile

Name*

Passive_Proxy_SSO

Unchecked Override Global check box indicates that the value is inherited from Global Session Parameters.

Override Globa

Session Time-out (mins)

30

Default Authorization Action*

ALLOW

Single Sign-on to Web Applications*

ON

Credential Index*

PRIMARY

Single Sign-on Domain

HTTPOnly Cookie*

YES

Enable Persistent Cookie*

ON

Persistent Cookie Validity

3

KCD Account

Impersonation_DMN12

Configure Session Policy

Name

Proxy_Passive_SSO

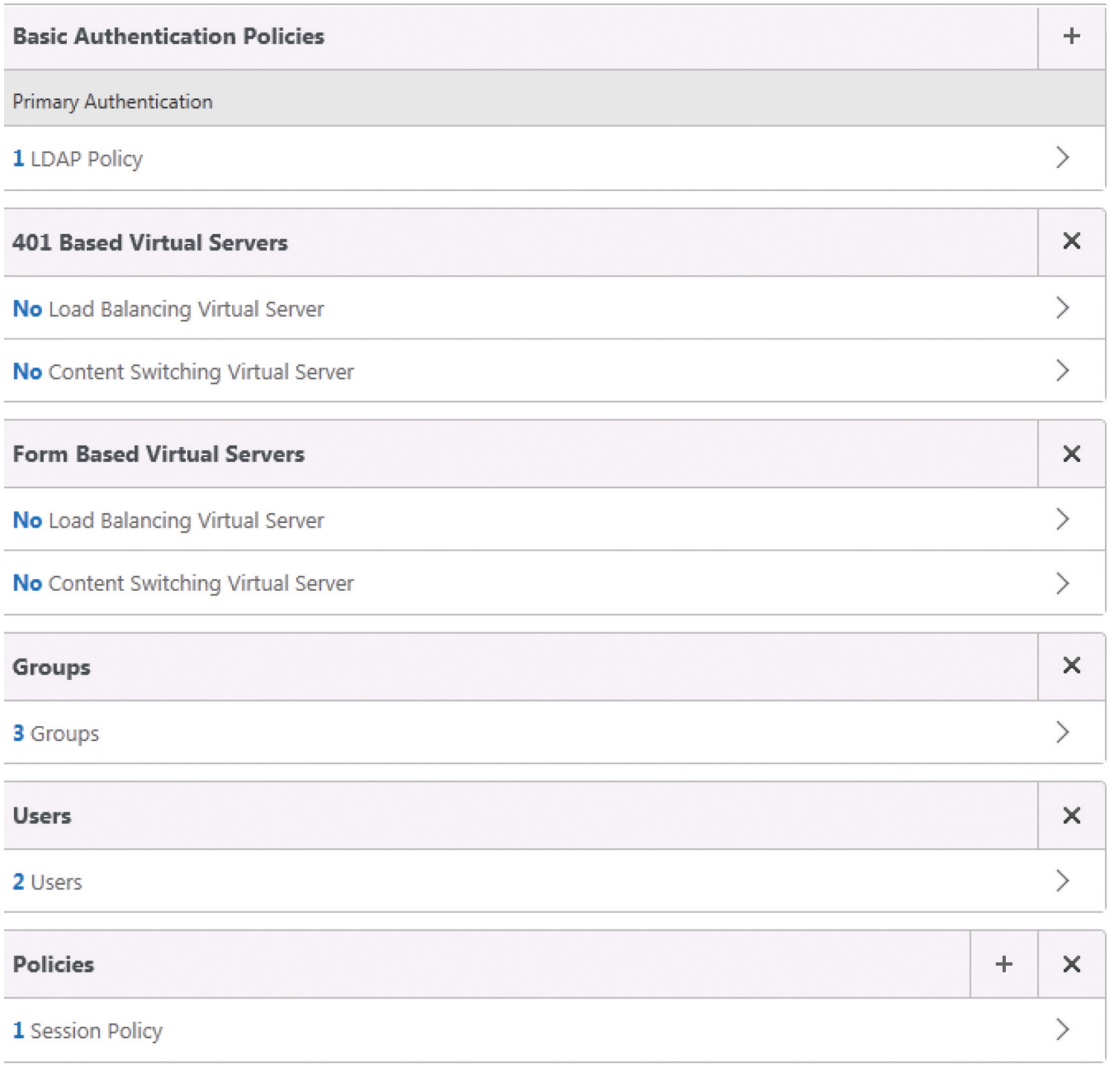
Request Profile*

Passive_Proxy_SSO

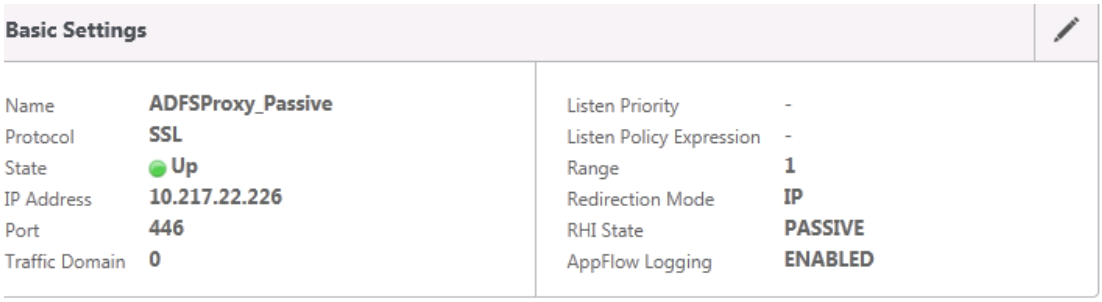
Expression* Expression Editor

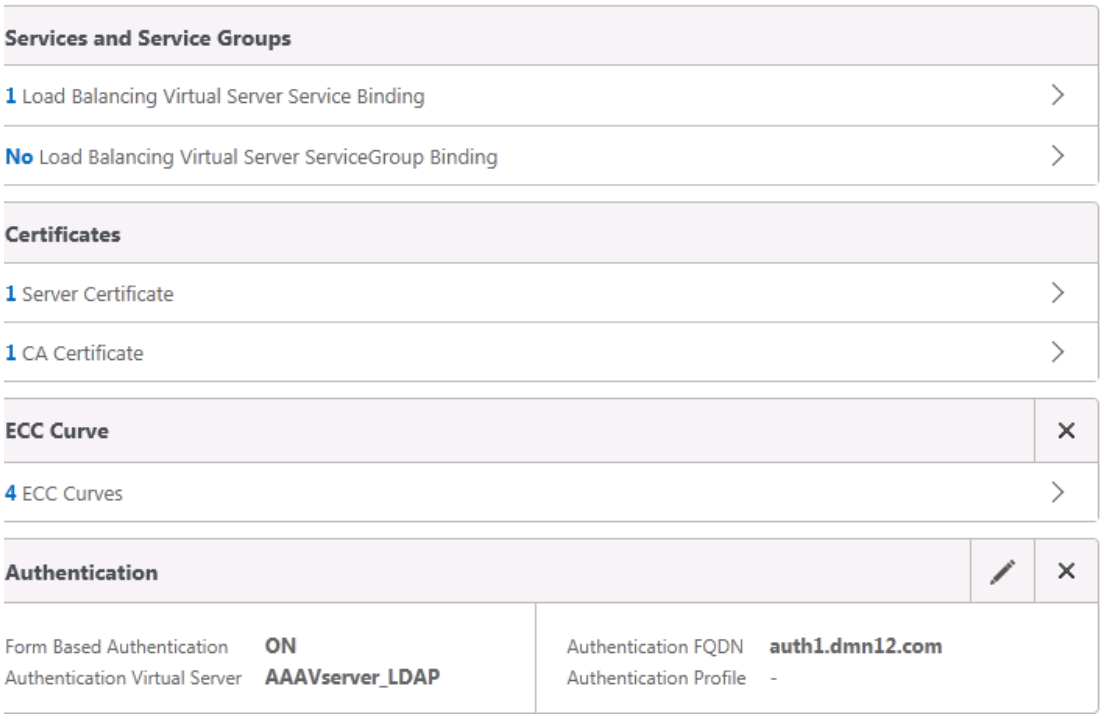
Operators Saved Policy Expressions Frequently Used Expressions Clear

ns_true

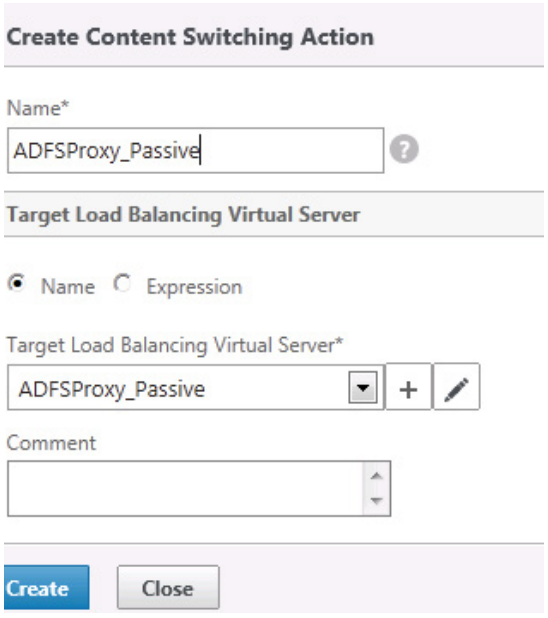


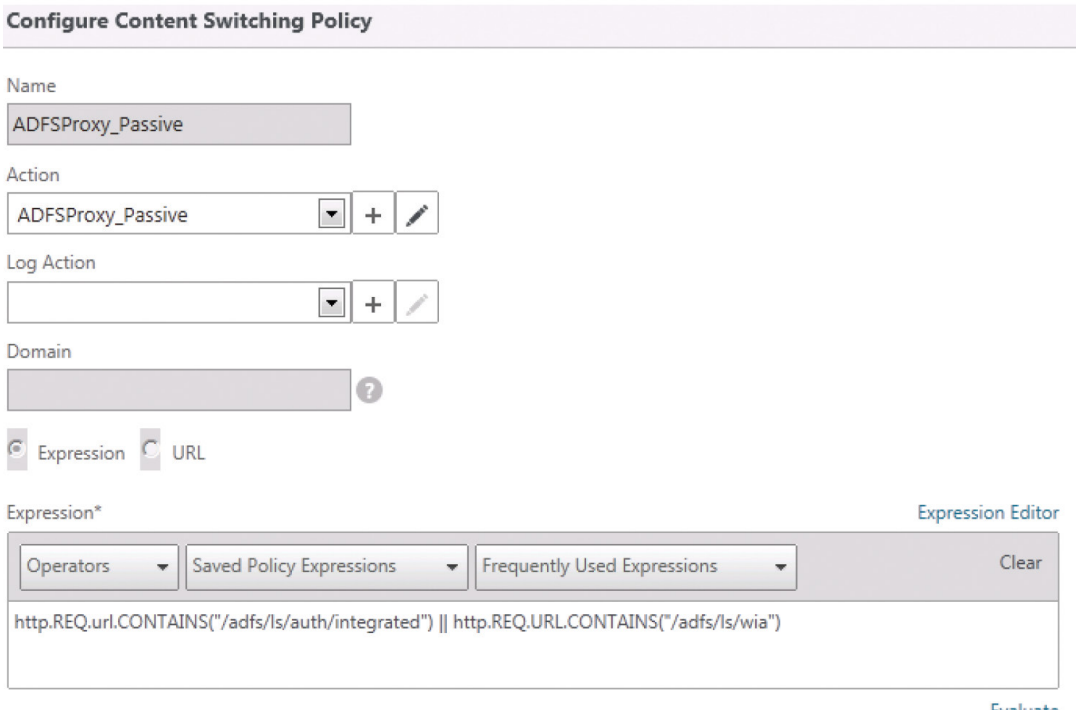
3. Create a load balancing vserver to handle requests /adfs/ls/auth/integrated (for ADFS 2.0) or /adfs/ls/wia (for ADFS3.0). Enable that vserver for form-based authentication.

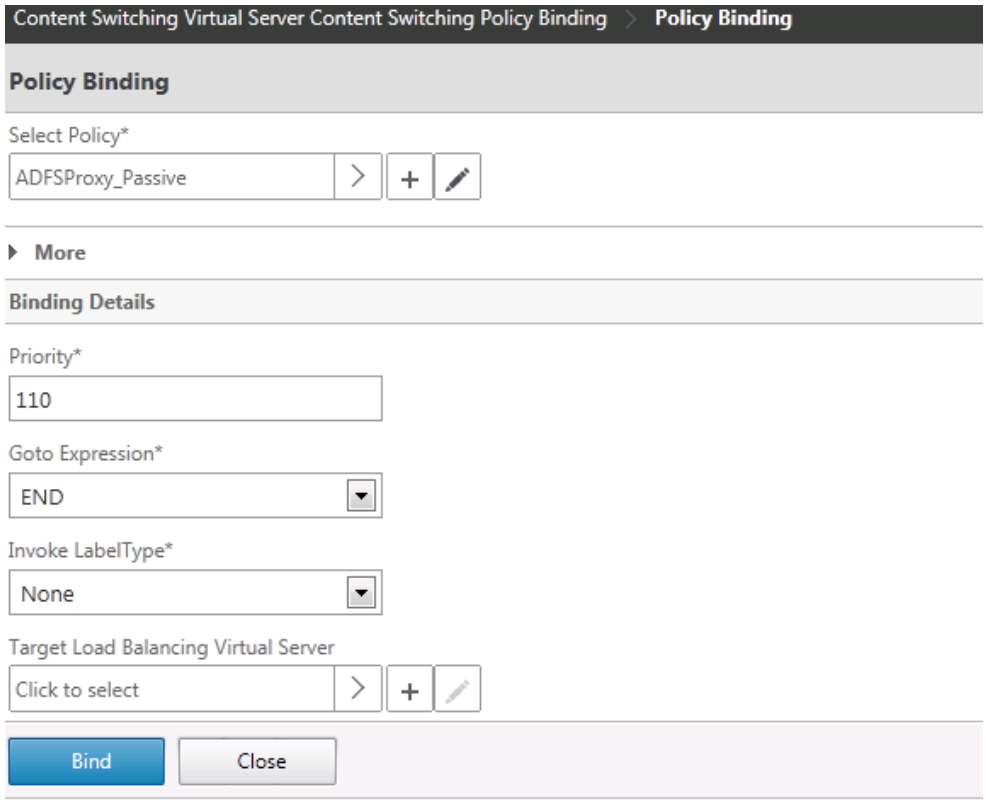




4. Create a content switching action and policy and bind it to the content switching vserver.




Configure Content Switching Policy
Name
ADFSProxy_Passive
Action
ADFSProxy_Passive
Log Action
Domain
Expression
URL
Expression*
Expression Editor
Operators
Saved Policy Expressions
Frequently Used Expressions
Clear
http.REQ.url.CONTAINS("/adfs/ls/auth/integrated") || http.REQ.URL.CONTAINS("/adfs/ls/wia")


Content Switching Virtual Server Content Switching Policy Binding
Policy Binding
Policy Binding
Select Policy*
ADFSProxy_Passive
More
Binding Details
Priority*
110
Goto Expression*
END
Invoke LabelType*
None
Target Load Balancing Virtual Server
Click to select
Bind
Close

Conclusion

NetScaler is a proven solution for fast, reliable, high-availability and secure app delivery in remote access use cases. Extending these capabilities to include functioning as ADFS proxy increases the total value NetScaler delivers to the enterprise. It becomes single gateway point for all enterprise user access, including remote access to Office 365. Beyond its core functionality, NetScaler helps to improve the end-user experience and the scalability and stability of the whole deployment. Furthermore, the same NetScaler appliance can also be used for other remote access use cases, given that it is deployed in the DMZ. There is great value in consolidating all such remote access and authentication use cases through a single NetScaler ADC appliance.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom