How to Integrate an External Authentication Server

https://campus.barracuda.com/doc/41110091/

Required Product Model and Version

This article applies to the Barracuda Load Balancer ADC 540 and above, version 5.1 and above, and to all Barracuda Load Balancer ADC models in version 5.2 and above.

Create an authentication service to connect with and get user information from your existing external authentication server. LDAP, RADIUS, and Kerberos authentication protocols are supported.

LDAP

Lightweight Directory Access Protocol (LDAP) is used for storing and managing distributed information services in a network. LDAP is mainly used to provide a single sign-on solution. It follows the same X.500 directory structure as MSAD.

To add an LDAP authentication service, identify a user who can query the LDAP directory, and specify the parameters for looking up information about users.

To use LDAP authentication with IBM Domino, see the "Application-Specific Instructions" section of How to Configure Access Control (AAA).

1. Go to the **ACCESS CONTROL > Authentication Services** page, and click the **LDAP** tab.
2. In the settings, specify the following:
   - Alias for the server
   - IP address, port, and connection type for connecting to the LDAP server
   - Bind DN, bind password, and login attribute for a user who has read access to all users in the LDAP directory
   - Attributes and filters used to look up and authenticate end users
3. Click **Test LDAP** to verify that a connection can be established with the LDAP server. The test results display at the bottom of the page. If the test fails, re-enter and re-test the LDAP settings.
4. Click **LDAP Discovery** to verify that users can be found with the attributes and filters that you entered. If you want to view detailed query results, select the **Verbose** check box. In the test results:
   - Green dot is displayed next to verified information.
   - Red dot is displayed next to information that must be corrected.

   If any information is incorrect or missing, edit the field and click **LDAP Discovery**.
5. After your settings have been validated, click **Add**. The LDAP service appears in the **Existing Authentication Services** section.

You can now assign the LDAP service to a web service and configure an authorization policy. For instructions, see How to Configure Access Control (AAA).

RADIUS

Remote Access Dial In User Service (RADIUS) is a networking protocol which provides authentication, authorization, and accounting.

To add a RADIUS authentication service, specify the shared key that is used by the Barracuda Load Balancer ADC and RADIUS server to verify each other's identity. Also set a limit to how long the Barracuda Load Balancer ADC waits for a response from the RADIUS server and a limit on the number of times that it can send a request packet.

You can also add a secondary RADIUS server for authenticating users. If the primary RADIUS server fails, the secondary RADIUS server takes over as the primary RADIUS server for authenticating users.

To integrate the Barracuda Load Balancer ADC with a RADIUS authentication server:

1. Go to the **ACCESS CONTROL > Authentication Services** page, and click the **RADIUS** tab.
2. In the settings, specify:
    - An alias for the RADIUS server.
    - The IP address, port, and secret key for the RADIUS server.
    - The maximum **Timeout** and **Retries** for sending packets to the RADIUS server.
3. Click **Add** . The new RADIUS service appears in the **Existing Authentication Services** section.
4. If you want to configure a secondary RADIUS server:
    1. Click **Add** next to the RADIUS authentication service for which you want to add the secondary server.
    2. In the **Add Secondary Radius Server** window, enter the IP address and port of the secondary RADIUS server. All settings for the secondary RADIUS server, except for the IP address and port, must be identical to the settings used for the primary RADIUS server.
    3. Click **Add**.

You can now assign the RADIUS service to a web service and configure an authorization policy. For instructions, see How to Configure Access Control (AAA).

Kerberos

Kerberos is the native authentication method used by Windows 2000 and later Microsoft Windows platforms. Kerberos provides mutual authentication (meaning both the user and the server verify each other's identity). It uses a trusted third party known as the Key Distribution Center (KDC). The KDC must be a part of the Windows Domain Controller Active Directory.

The KDC provides two services:

- Authentication Service (AS) that authenticates a user
- Ticket Granting Service (TGS) that issues a session ticket to a client.

Kerberos relies on Service Principal Names (SPNs) to uniquely identify an instance of a service (which runs on a host) by a client. When you add a Kerberos authentication service, you must also configure an SPN for your web service. The SPN must be registered in Active Directory. SPNs can be formatted as follows:

- `<service type>/<instance/host name>`
- `<service type>/<instance/host name>:<port number>/<service name>`

The port and service name are optional. The port is only required when a non-default service type is used.

If you have multiple servers configured for a service, verify that a single SPN is registered in Active Directory for the service. The SPN is always tied to a server (not the VIP of the service configured on the Barracuda Load Balancer ADC). For example, if you have a service for `web1.domain.com` with two servers that are configured for load balancing, create an SPN for `web1.domain.com` and register the SPN in Active Directory under the user. Both servers must provide required permissions for the user.

Requirements for Kerberos

Before continuing with the procedure for integrating Kerberos, verify that the following requirements are met:

- Barracuda Load Balancer ADC has proper DNS servers configured
- DNS IP address configured in the **BASIC > IP Configuration > DNS Configuration** section must be reachable by the Active Directory domain (the domain where the KDC is installed)
- All host machine clocks are synchronized to within 5 minutes of the Kerberos server clock

Step. 1 Add the Kerberos Server

To integrate the Barracuda Load Balancer ADC with a Kerberos server:

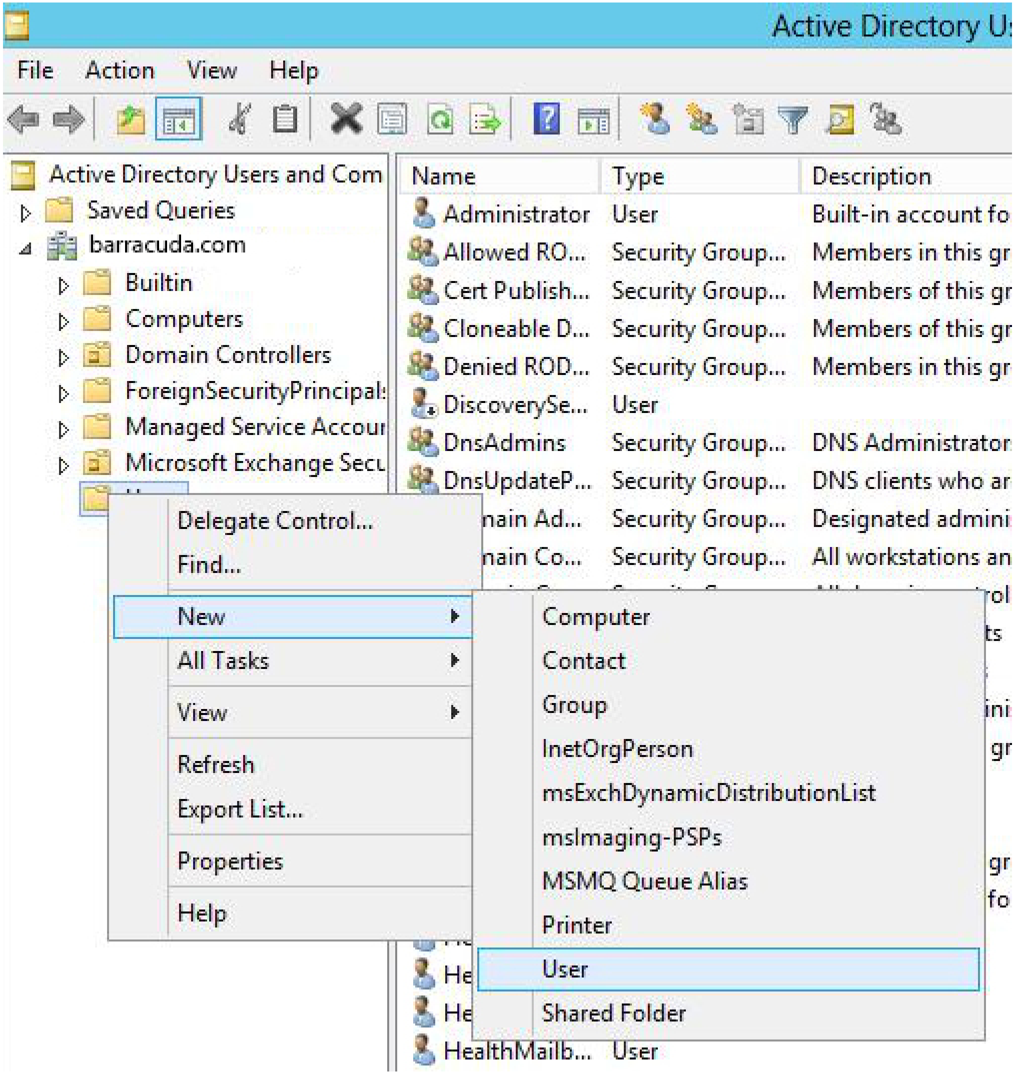
1. Go to the **ACCESS CONTROL > Authentication Services** page, and click the **Kerberos** tab.
2. In the settings, specify:
    - Alias for the server
    - KDC realm name

- ○ IP address or name and the port for the Kerberos server.

3. Click **Add**.

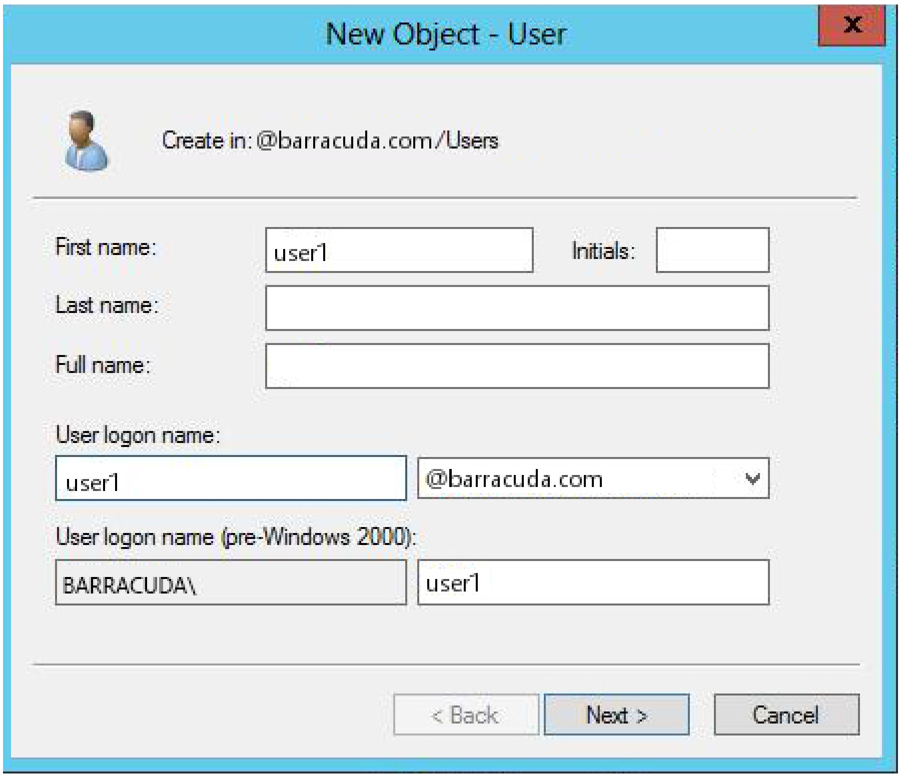
Step 2. Create a New User in Active Directory

1. In the **Active Directory Users and Computers** window, click **Users > New > User**.



Name	Type	Description
Administrator	User	Built-in account fo
Allowed RO...	Security Group...	Members in this gr
Cert Publish...	Security Group...	Members of this gr
Cloneable D...	Security Group...	Members of this gr
Denied ROD...	Security Group...	Members in this gr
DiscoverySe...	User	
DnsAdmins	Security Group...	DNS Administrator
DnsUpdateP...	Security Group...	DNS clients who ar
nain Ad...	Security Group...	Designated admini
nain Co...	Security Group...	All workstations an
He		
He		
HealthMailb...	User	

2. In the **New Object - User** window, specify the name and login credentials for the user.



Create in: @barracuda.com/Users

First name: user1

Initials:

Last name:

Full name:

User logon name:

user1 @barracuda.com

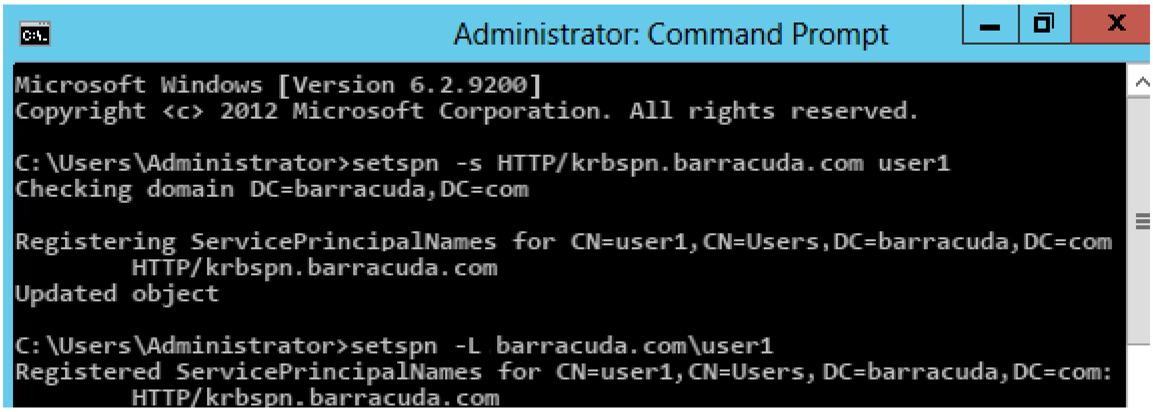
User logon name (pre-Windows 2000):

BARRACUDA\ user1

3. Click **Next**, specify values for other fields as required, and click **Finish**.

Step 3. Create the SPN for the User

Set the SPN under the user account that you just created in Active Directory. Open a command prompt, and execute the `setspn` command. The SPN can be any name. In the following example, the SPN is HTTP/`krbspn.barracuda.com`:



```
Microsoft Windows [Version 6.2.9200]
Copyright <c> 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -s HTTP/krbspn.barracuda.com user1
Checking domain DC=barracuda,DC=com

Registering ServicePrincipalNames for CN=user1,CN=Users,DC=barracuda,DC=com
        HTTP/krbspn.barracuda.com
Updated object

C:\Users\Administrator>setspn -L barracuda.com\user1
Registered ServicePrincipalNames for CN=user1,CN=Users,DC=barracuda,DC=com:
        HTTP/krbspn.barracuda.com
```

Step 4. Create a DNS Entry for your SPN

Add the following entries to the DNS server in the domain:

- Host A record for the SPN that you created (point the record to one of the servers that you configured for the service)

- Reverse PTR record pointing to same name and server.

Figures