Understanding Email Aliases

https://campus.barracuda.com/doc/75694401/

Local Accounts

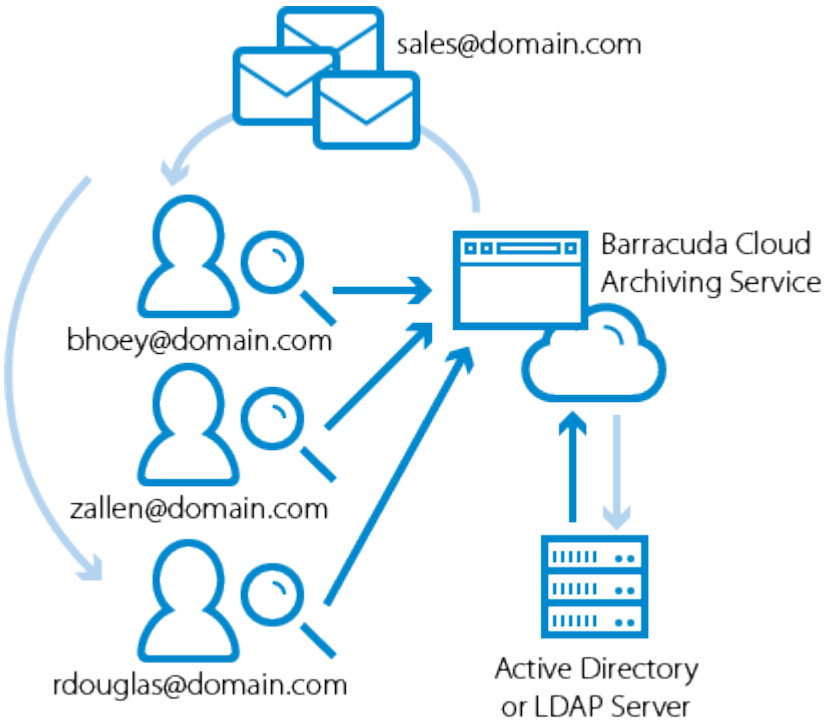
Create local users on the **Users > User Add/Update** page.

Group Membership

To enable group membership for local accounts, you must be using an Active Directory or LDAP server, and the lists must reside on those servers.

Archived messages that are sent to a mailing group are visible in the personal message archive for every member of that group. For example, if **bhoey@domain.com**, **zallen@domain.com**, and **rdouglas@domain.com** are all members of **sales@company.com**, then any message that is sent to **sales@domain.com** is available in the archives of all three users.

Figure 1. Local Account Group Membership.



Alias Linking

You can create a local user account on the Barracuda Cloud Archiving Service that has access to archived messages for multiple users. For example, you want a single user account to see emails for **chris.smith@company.com**, **pat.jones@company.com**, and **alex.pierce@company.com**, in addition to **the_boss@company.com**. To do so, create a local account on the Barracuda Cloud Archiving Service (for example, "local_boss"), and list as aliases the email addresses to which that account is to have access.

To list aliases for a new account,

1. Go to the **Users > User Add/Update** page.
2. Enter the new user **Email Address**, and enter the **User Display Name**.
3. Enter all email addresses used as aliases for this user, one alias per line in the **User Aliases** field.
4. Add the desired password for the account, and click the user role from the **Role** drop-down menu.
5. Click **Save** to save the list of aliases for that user. This account is added to the **Users > Accounts** page including its aliases.

To list aliases for an existing account,

1. Go to the **Users > Accounts** page.
2. Click **Edit** for the primary user account; the **Users > User Add/Update** page displays.
3. Enter all email addresses used as aliases for this user, one alias per line in the **User Aliases** field.
4. Click **Save** to save the list of aliases for that user. The aliases are added to the **Aliases** field for this user in the **Users > Accounts** page.

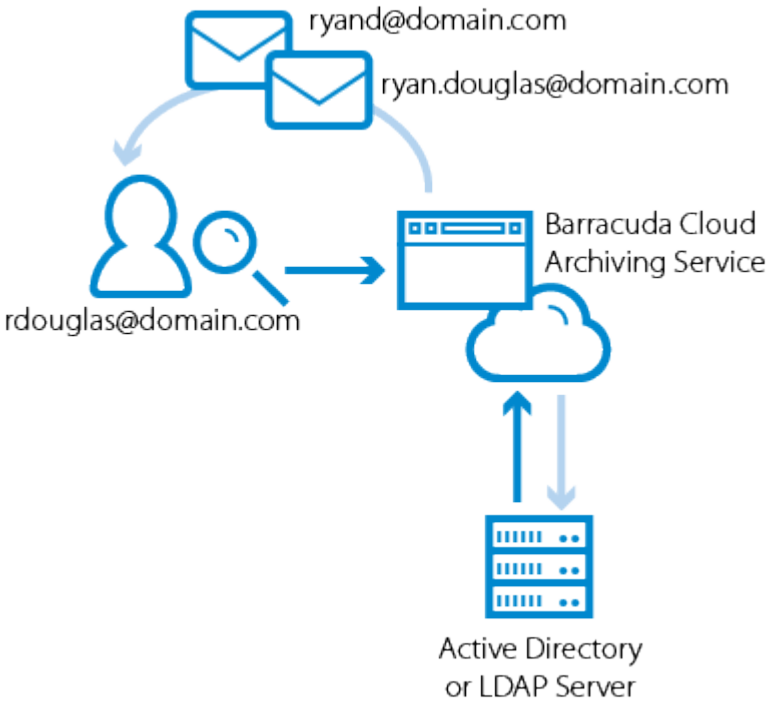
Active Directory

Associated an LDAP or Azure AD user or group to a Barracuda Cloud Archiving Service role and list of email addresses on the **Users > LDAP User Add/Update** page.

Group Membership

LDAP and Azure AD users often have one primary email address that is their user account name along with several aliases for convenience. For example, **rdouglas@domain.com** might also receive messages as **ryand@domain.com** and **ryan.douglas@domain.com**. For organizations that use LDAP or Azure AD, messages sent to any alias are accessible from the primary user account.

Figure 2. Active Directory Group Membership.



You can enter an LDAP or Azure AD group name in the **LDAP User/Group** field and select a role for that group. When a member of that group logs in to the Barracuda Cloud Archiving Service, they log in with the assigned role.

Include/Exclude Rules

You can define exclude/include rules on the **Users > LDAP User Add/Update** page to set permissions on whose mail the user or group members can view. The addresses must belong to a user, group, or public folder on a configured LDAP server or Azure AD. When a configured user runs a search, the following rules are in place:

1. Mail for addresses added to the **Exclude these Addresses** list are not displayed unless the mail includes the user performing the search to assure that a user can always see their own mail.
2. The **Exclude these Addresses** list always takes precedence; addresses added to the **Include these Addresses** list are searchable *unless* the **Exclude these Addresses** list blocks the mail.
3. Because a user with the Admin or Auditor role can by default view all mail, users set to these roles can only edit their **Exclude these Addresses** list.
4. If a user is *not configured* and is a member of a group, then the include/exclude rules assigned to that group apply to that user. Additionally, if the unconfigured user is a member of multiple groups, then the privileges for all of those groups are merged and that user is assigned the *least privileged role* of those groups. This allows the Admin to apply include/exclude rules to all users of a distribution group.
    - Example 1: If Zoe is not individually configured but is a member of the distribution group HR, then the Admin can set the include/exclude rules for the group HR, and Zoe uses

these settings when searching mail rather than seeing only her own mail.
    - Example 2: If Josh is not individually configured but is a member of the distribution group HR which has an Auditor role, and Josh is also a member of the group Employees which has a User role, Josh has only the User role privileges when running a search.
5. A user cannot run a **Search As User** Search on the **Basic > Search** page on a user that is on their **Exclude these Addresses Exclusion Rules** blocklist.

Figures