Basic Configuration

Các thông tin mặc định khởi tạo khi cài đặt

|  |  |
| --- | --- |
| **Main Menu** | **Description** |
| **Common Configuration - These are common settings for all servers** | |
| Hostname | The host name configured in the operating system installation |
| LDAP master host | The LDAP host name. On a single server installation, this name is the same as the hostname. |
| LDAP port | The default port is 389 |
| LDAP Admin password | This is the master LDAP password. |
| Secure interprocess communications | The default is YES. Secure interprocess communications requires that connections between the mail store, and other processes that use Java, use secure communications. It also specifies whether secure communications should be used between the master LDAP server and the replica LDAP servers for replication. |
| Time Zone | Select the time zone to apply to the default COS. The time zone that should be entered is the time zone that the majority of users in the COS will be located in. The default time zone is PST (Pacific Time). |
| IP Mode | IPv4 or IPv6. |
| **zimbra-ldap** | |
| Status | The default is Enabled. For replica LDAP servers, the status can be changed to Disabled if the database is manually loaded after installation completes. |
| Create Domain | You can create one domain during installation. Additional domains can be created from the administration console. |
| Domain to create | The default domain is the fully qualified hostname of the server. If you created a valid mail domain on your DNS server, enter it now. In most cases, you will accept the default. |
| LDAP Root password | The root LDAP password for internal LDAP operations. |
| LDAP Replication password | This is the password used by the LDAP replication user to identify itself to the LDAP master and must be the same as the password on the LDAP master server. |
| LDAP Postfix password | This is the password used by the postfix user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP master server. |
| LDAP Amavis password | This is the password used by the amavis user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP server. |
| **zimbra-logger** | When installed, it is automatically enabled. Logs from the hosts are sent to the mailbox server where zimbra- logger is installed and the information is used to generate the statistics graphs and for message tracing. |
| **zimbra-mta** | |
|  | * **MTA Auth host** — This is configured automatically if the MTA authentication server host is on the same server, but must be configured if the authentication server is not on the MTA. * **Enable Spamassassin** — Default is enabled. * **Enable ClamAV** — Default is enabled. * **Notification address for AV alerts** — Sets the notification address for AV alerts. You can either accept the default or create a new address. If you create a new address, remember to provision this address from the admin console. **Note:**If the virus notification address does not exist and your host name is the same as the domain name on the Zimbra server, the virus notifications queue in the Zimbra MTA server cannot be delivered. * **Bind password for Postfix LDAP user**- Automatically set.This is the password used by the postfix user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP master server. * **Bind password for Amavis LDAP user**- Automatically set. This is the password used by the amavis user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP server. |
| **zimbra-dnscache** | |
|  | * **Master DNS IP address(es)**— * **Enable DNS lookups over TCP**— * **Enable DNS lookups over UDP** — * **Only allow TCP to communicate with Master DNS** |
| **zimbra-snmp(optional)** | |
|  | * **Enable SNMP notifications** — The default is Yes. * **SNMP Trap hostname** * **Enable SMTP notification** — The default is Yes. * SMTP Source email address * **SMTP Destination email address** |
| **zimbra-store** | |
| Create Admin User | The administrator account is created during installation. This account is the first account provisioned on the Zimbra server and allows you to log on to the administration console. |
| Admin user to create | The user name assigned to the administrator account. Once the administrator account has been created, it is suggested that you do not rename the account as automatic Zimbra Collaboration notifications might not be received. |
| Admin Password | You must set the admin account password. The password is case sensitive and must be a minimum of six characters. The administrator name, mail address, and password are required to log in to the administration console. |
| Anti-virus quarantine user | A virus quarantine account is automatically created during installation. When AmivisD identifies an email message with a virus, the email is automatically sent to this mailbox. The virus quarantine mailbox is configured to delete messages older than 7 days. |
| Enable automated spam training | By default, the automated spam training filter is enabled and two mail accounts are created.   1. **Spam Training User** to receive mail notification about mail that was not marked as junk, but should have been. 2. **Non-spam (HAM)** Training User to receive mail notification about mail that was marked as junk, but should not have been.   These addresses are automatically configured to work with the spam training filter. The accounts created have a randomly selected name. To recognize what the account is used for, you may want to change this name. |
| The default port configurations are shown | * **SMTP host** * **Web server HTTP port:** 80 * **Web server HTTPS port:** 443 * **Web server mode** — Can be HTTP, HTTPS, Mixed, Both or Redirect.   + **Mixed** mode uses HTTPS for logging in and HTTP for normal session traffic   + **Both** mode means that an HTTP session stays HTTP, including during the login phase, and an HTTPS session remains HTTPS throughout, including the login phase.   + **Redirect** mode redirects any users connecting via HTTP to an HTTPS connection.   + All modes use SSL encryption for back-end administrative traffic. * **IMAP server port**: 143 * **IMAP server SSL port**: 993 * **POP server port**: 110 * **POP server SSL port**: 995 * **Use spell checker server**, default **Yes** (if installed) * **Spell server URL**: http://<example.com>:7780/aspell.php |
|  | * **Configure for use with mail proxy. FALSE** * **Configure for use with web proxy. FALSE** If either or both of these are changed to TRUE, the proxy setting on the mailbox store are enabled in preparation for setting up zimbra proxy. * **Enable version update checks.** Zimbra Collaboration automatically checks to see if a new Zimbra Collaboration update is available. The default is TRUE. * **Enable version update notifications.** This enables automatic notification when updates are available when this is set to TRUE. * **Version update notification email.** This is the email address of the account to be notified when updates are available. The default is to send the notification to the admin’s account. * **Version update source email.** This is the email address of the account that sends the email notification. The default is the admin’s account.   **Note:** The software update information can be viewed from the Administration Console Tools Overview pane. |
| **zimbra-spell** | (optional) When installed, it is automatically enabled. |
| **Default Class of Service Configuration** | This menu section lists major new features for the Zimbra Collaboration release and whether the feature is enabled or not. When you change the feature setting during Zimbra Collaboration installation, you change the default COS settings Having this control, lets you decide when to introduce new features to your users. |
| c) Collapse menu | Allows you to expand or collapse the menu. |
| r) Start servers after configuration | When the installation and configuration is complete, if this is set to **Yes**, the Zimbra server is automatically started. |
| s) Save config to file | At any time during the installation, you can save the configuration to file. |
| x) Expand menu | Expand menus to see the underlying options |
| q) Quit | Quit can be used at any time to quit the installation. |