

On-premise installation vs. installation in the cloud

Lucy can be installed on-premise or in the internet on any cloud server.

Reasons for installing on an external server in the internet are:

- **Public IP address outside your network range:** Prevents your infrastructure from being blacklisted.
- **Direct access:** The server will not be blocked by any security products already in place within your own infrastructure.
- **Less possible conflicts with integration:** A LUCY server placed directly in the internet will be setup very fast as it does not require a complex integration process with your mail, DNS and firewall infrastructure
- **Smaller attack surface:** As the LUCY server requires a web based access for end users from the internet (e.g. accessing their mails from mobile devices), you might need to punch a hole in your firewall and allow inbound access to a LUCY server. If you place LUCY in the intranet (see [this chapter](#)), you might violate your zone concept.

Reasons for installing LUCY on premises are:

- **Legal:** Some laws might not allow you to store sensitive data on an external server outside your network or outside your country. Especially with the new data protection law in Europe ([GDPR](#)) you need to make sure any personalized or sensitive data is secured.
- **Integration with certain features:** LUCY comes with different API's such as the [LDAP API](#), the [REST API](#) etc. which are common for backend applications that are usually not exposed to the internet.
- **Security:** LUCY might store sensitive data like windows login, user names, emails etc. within the database. Integrating the LUCY server in the internal protection layers (IDS, FW etc.) will minimize the risks of successful attacks.

Where to place LUCY in an on-premise installation?

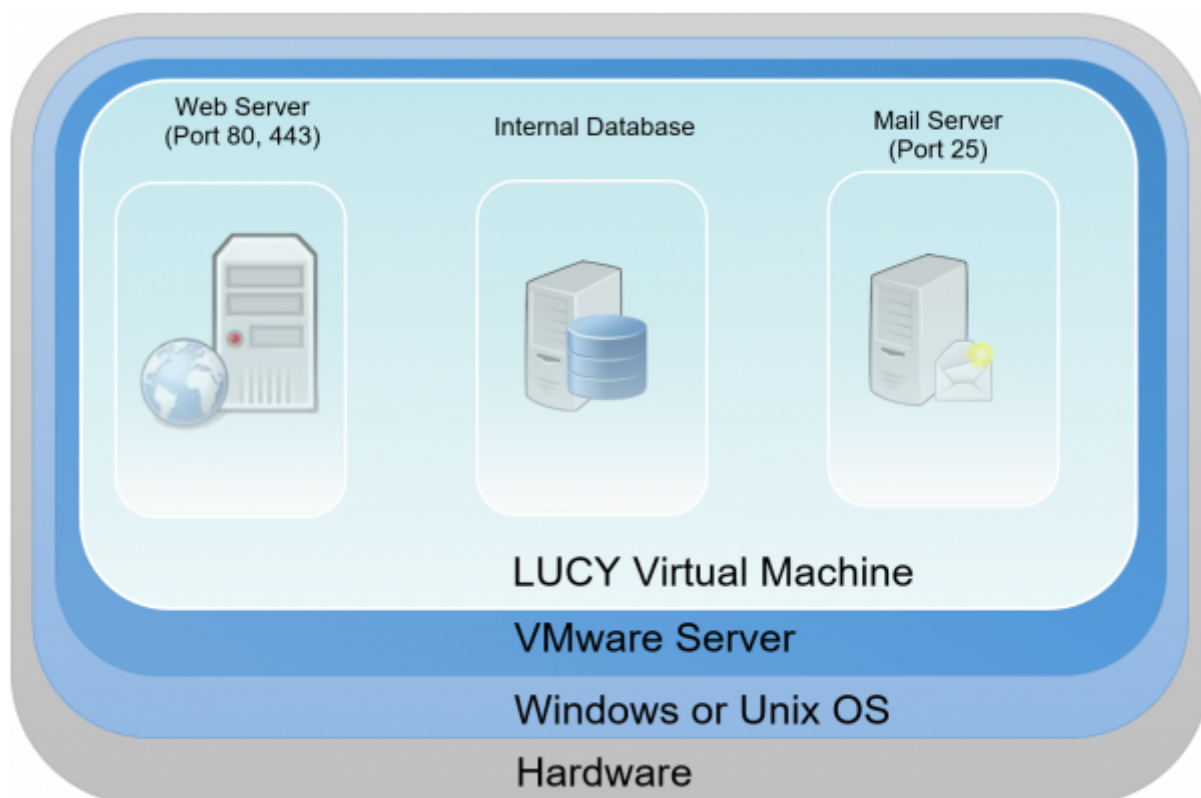
You can place LUCY in the intranet or within a secured zone (DMZ). If you want to allow external users (e.g. mobile users with smartphones) to access LUCY's websites (attack simulations or e-learning), an installation in the intranet is not recommended for security reasons. The web server would be directly accessible from the Internet. In case of a vulnerability in the system or application, an attacker would have direct access to the intranet via the LUCY server. In such a case you should install LUCY in a separate zone. In that case you could consider using one LUCY instance only as a reverse proxy in that zone, and install the main application within the intranet as a "master instance". This configuration is described [here](#).

On premise installation technical checklist

Please consult [this chapter](#).

LUCY Vmware technical components

When you download and boot the VMware Image, all software components are integrated in that image. There is no need to install any additional software. All components (DB, mail server, web server etc,) are bundles within the VMware images and controlled by the internal LUCY software, which runs transparently in the background. The updating of those components is also done within the LUCY software through internal processes, which are not visible to the end user.



From:
<https://wiki.lucysecurity.com/> - LUCY

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=network_design_-_where_to_setup_lucy&rev=1571060696

Last update: 2019/10/14 15:44

