deaddrop requirements

Sysctl AB

2017-04-11

Abstract

Information that is needed by sysctl before a deaddrop appliance can be manufactured. Information about on-site preparation that is needed before on-site delivery.

1 deaddrop requirements

Some of the configuration parameters **must** be delivered to sysctl before a deaddrop appliance can be buildt and delivered. After the delivery of an appliance **must** additional configuration be applied.

1.1 deaddrop appliance requirements before delivery

The following inforamtion is *required* before an appliance server can be built

1.1.1 Appliance server type

- Virtual appliance or a physical appliance
- Server specification (see server-spec.pdf document)

1.1.1.1 Virtual server

- Virtualization technology
- Version of virtualization software
- Can you receive qcow2 harddrive yes/no?
- Support for UEFI yes/no?
- Desired disk size

1.1.2 IP configuration

- ip address (ipv4 and/or ipv6)
- netmask (ipv4 and/or ipv6)
- default gateway (ipv4 and/or ipv6)

1.1.3 DNS configuration

- hostname (ie. deaddrop)
- fqdn (ie. deaddrop.sysctl.se)

1.1.4 SMS configuration

- desired SMS solution (ie. GSM-modem or SMS-gateway provider)
  - GSM modem
  - Tele2
  - Beepsend
  - Telia Telemat
  - Clickatell
  - Sergel

1.1.5 Email configuration

- mailbox for administrators (ie. systemmail, ie hardware failures, malware detection etc)
- mail address to use as sender address from deaddrop to endusers (ie “you have recieved a protected file”)

1.1.6 Password policy

- minimum password length
- complexity (capital letters, lower case, number, special characters)
- sms password (character list)
- sms password length

1.1.7 Other configurations

- user session timeout time
- internal service desk support number
- internal service desk support email
- maximum size of files that is allowed for upload

1.2 Onsite preparation

The following must be ready during delivery

1.2.1 Contact person

One person on site that is able to give access to the console on the delivered appliance.

1.2.2 External firewall

The following is the minimal network connection requirements, relating to firewall rules and opening of UDP and TCP ports, that deaddrop needs to work properly.

1.2.2.1 inbound from internet (access to deaddrop service)

- 80/TCP
- 443/TCP

1.2.2.2 inbound from administrative network or simular

- 8443/TCP

1.2.2.3 outbound to dmz or simular (DNS server[s])

- 53 TCP/UDP

1.2.2.4 outbound to desired NTP server(s)

- 123/UDP

1.2.2.5 outbound to desired SMTP relay

- 25/TCP

1.2.2.6 outbound connection to updates.sysctl.se (software updates, system patches, AV updates)

- TCP/443

It is *extremely* important that the interface used for administration (web via 8443/TCP) is only exposed towards an administrative network, not outward to the Interet.

Additional firewall rules may be needed when integrations to other service (ie SMS gateway or external log server). An SMS gateway provider often allow for connections via HTTPS, so explicit outbound HTTPS connection to the specific provider needs to be added to the firewall.

For explaination about network connections see deaddrop-net document.

1.2.3 DNS

For correct DNS setup, at least the following information is needed: * An A record in DNS for FQDN * A PTR record for IPv4 and/or IPv6 address

1.2.4 SMS

For correct SMS setup, at least one of the following choices needs to be completely configured:

1. GSM modem

- simcard
- pin code to simcard

2. SMS gateway

- username
- password
- additional tokens

1.2.5 CA

- Access to account (or personnel that has access to account) that can issue x509 certificates from a webtrust PKI.

1.2.6 Proccess

All password and secrets will be created or changed onsite during the installation time, please be preparded to handle the new passwords.

1.3 After delivery requirements

1.3.1 Contact persons

- A email adress to a person or group account which information about updates and simular information can be sent to
- If the API is used, a email adress to a person or group account which information about planned changed in the API can be sent to
- If sysctl are handeling software updates, a contact person to request service windows
- If sysctl are handeling software updates, a fixed service window when possible

---