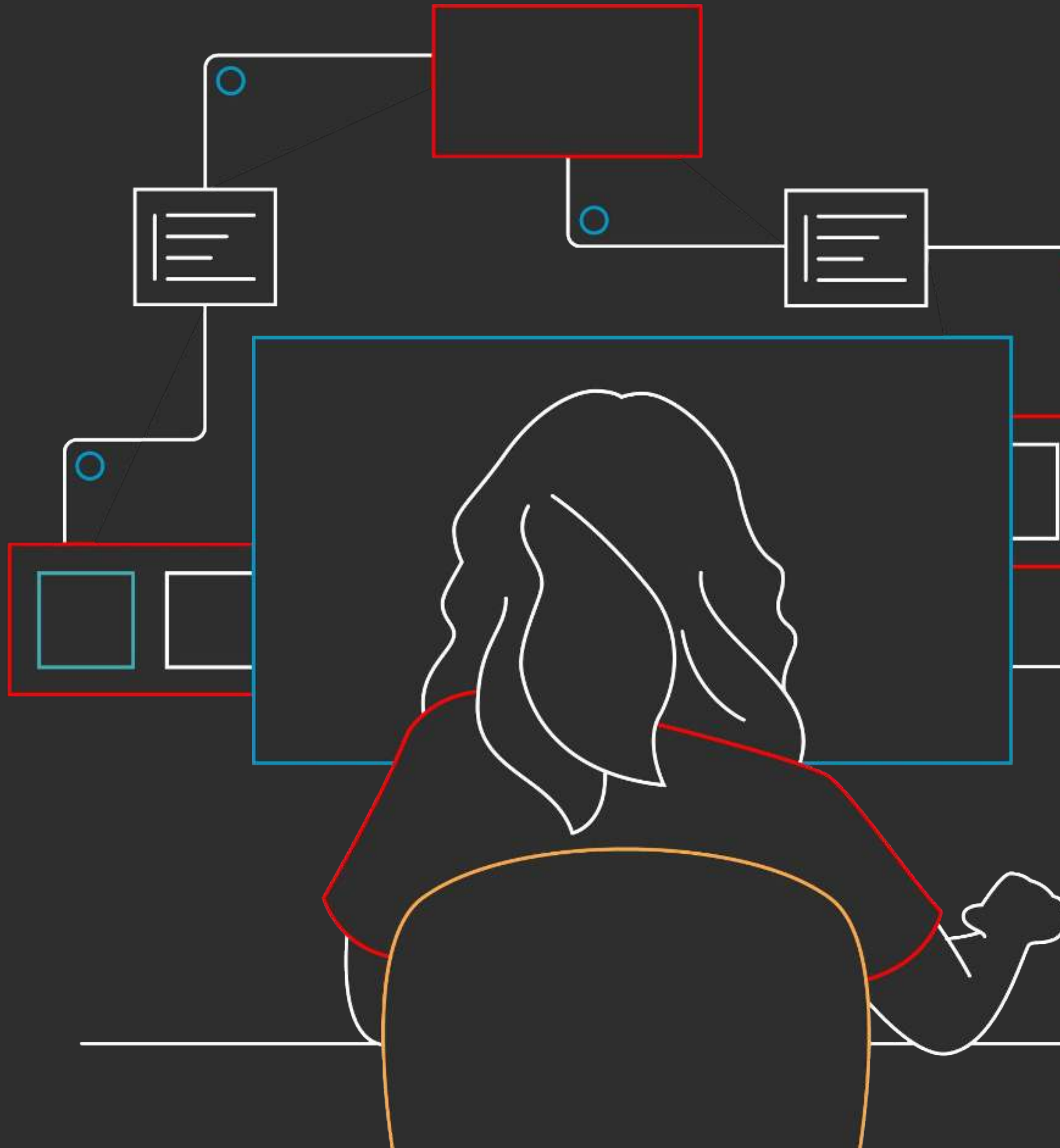
Operation, Update, and Monitoring

Hardening an SAP Environment



Basic considerations

Minimal Installation

- pick “Minimal Install”
  - What’s not installed cannot be attacekd
- Have the system roles install additional required packages

- Tests have shown that a minimal viable system is the minimal install plus
  - compat-sap-c++
  - libtool-ltdl
- additional functions may fail, so additional packages may be required
- changes are possible - tested on RHEL 8.4 only

Basic considerations

Disable Unnecessary Network Services

- Network Services should be reviewed and always seen as a possible attack path from outside (DoS, DDoS) and turn off unused services
- Avoid inherently insecure services which send sensitive data unencrypted over the network such as telnet, ftp, http, smtp.
- Secure services such as NFS or SMB

Disable Telnet

Priority: High

- unsecured protocol listens and sends on tcp/23
- replace with SSH
- procedure for disabling telnet:

```
# systemctl stop telnet.socket
# systemctl disable telnet.socket
# systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
  Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
  Active: inactive (dead)
        Docs: man:telnetd(8)
  Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0
Apr 04 15:12:15 localhost systemd[1]: Listening on Telnet Server Activation Socket.
Apr 04 15:12:15 localhost systemd[1]: Starting Telnet Server Activation Socket.
Apr 04 15:30:14 localhost systemd[1]: Closed Telnet Server Activation Socket.
Apr 04 15:30:14 localhost systemd[1]: Stopping Telnet Server Activation Socket.
```

Restrict sudo

Priority: High

- providing trusted users with limited administrative access
- restrict access to the commands to the group wheel
  ```
  # chgrp wheel /usr/bin/sudo /usr/bin/su
  ```
- Ensure that only the root user and the wheel group can execute the sudo and su commands:
  ```
  # chmod 4550 /usr/bin/sudo /usr/bin/su
  ```
- Edit the /etc/sudoers file.
  ```
  # visudo
  ```
- •Ensure that the following line is present in the /etc/sudoers file:
  ```
  %wheel ALL=(ALL) ALL
  ```
- Add all system administrator users to the wheel group in the /etc/group file:
  ```
  wheel:x:10:<user names of sysadmin users>
  ```

Disabling root logins via SSH

Priority: High

- per default root access is allowed from the outside world
- Make the following changes in the /etc/ssh/sshd_config file:

```
PermitRootLogin no
```

Lock out a User to Log in after a Set Number of Failed Attempts

Priority: Medium

- mechanism provided via `pam_faillock` pam modul
- counts number of failed logins and can lock a user at a number of failed log in attempts
- enable faillock: `# authselect enable-feature with-faillock`
- configure failock in /etc/faillock.conf:

```
deny=4
unlock_time=1200
silent
```

- Using the faillock Command to Reset or View Authentication Failure Records

```
# faillock --user username --reset
```

- sshd configuration adjustment in /etc/ssh/sshd_config

```
ChallengeResponseAuthentication yes
PasswordAuthentication no
```

- restart sshd

```
# systemctl restart sshd
```

Network Bound Disk Encryption (NBDE)

Priority: Medium

- enables key-management for LUKS encryption as part of policy based decryption (PBD)
- requires a running tang server (we use tang.srv in this example)
- Steps to configure automatic unlocking of LUKS-encrypted volumes
  - install the client software: `# dnf install clevis clevis-luks`
  - Identify the LUKS encrypted volume (e.g. `/dev/sda2`)
  - Bind the volume to a Tang server

    ```
    # clevis luks bind -d /dev/sda2 tang '{"url":"http://tang.srv"}'
    ```

Network Bound Disk Encryption (NBDE)

Priority: Medium

The `clevis luks bind` command performs the following steps:

1. Creates a key with the same entropy as the LUKS master key.
2. Encrypts the new key with Clevis.
3. Stores the Clevis JWE object in the LUKS2 header token, or uses LUKSMeta if the non-default LUKS1 header is used.
4. Enables the new key for use with LUKS.

Network Bound Disk Encryption (NBDE)

Priority: Medium

- configure access to the protected disk during the early boot phase

```
# echo "hostonly_cmdline=yes" > /etc/dracut.conf.d/clevis.conf
# dracut -fv --regenerate-all --hostonly-cmdline
```

- verify that the Clevis JWE object is successfully placed in a LUKS header

```
# levis luks list -d /dev/sda2
1: tang '{"url":"http://tang.srv:port"}'
```

fapolicyd Service

Priority: Medium

- concept of trust: an application is trusted when it is installed or updated via rpm
- other installations must create custom rules for fapolicyd
- the hana system role makr the HANA binaries as trusted
- Install and enable the fapolicyd package:

```
# yum install fapolicyd
# systemctl enable --now fapolicyd
```

SAP HANA Network and Communication Security

Communication channels

- internal communication channels
  - between hosts in multiple-host systems
  - between systems in system-replication scenarios
- external access channels
  - Connections for administrative purposes
  - Connections for data provisioning
  - Connections from database clients that access the SQL/MDX interface for the SAP HANA database
  - Connections from HTTP/S clients
  - Outbound connections

Network Security

Configure VPN

- Install Libreswan

  ```
  # yum install libreswan
  ```

- Initialize the NSS database

  ```
  # rm /etc/ipsec.d/*db
  # ipsec initnss
  ```

- start the ipsec daemon from Libreswan

  ```
  # systemctl start ipsec
  ```

- confirm that the daemon is running properly

  ```
  # systemctl status ipsec
  ```

- ensure that Libreswan starts at boot

  ```
  #  systemctl enable ipsec
  ```

Network Security

SSL Configuration on the SAP HANA Server

- TLS/SSL configuration can be configured with SAP Cryptographic Library CommonCryptoLib (`libsapcrypto.so`) between HANA and clients that access the SQL interface of the database.
- must be configured on client and server
- OpenSSL is still supported if you are using trust and key stores in the file system instead of in the database
- Follow the SAP installation guide for details on h

Secure Operating System User

Priority: High

- the *sid*adm user on the OS level can control any aspects of the database
- It is defined or created during DB install with an initial password
- change the password after installation
- limit the users which can assume *sid*adm

SELinux

Priority: High

- SE Linux is meanwhile supported on RHEL 8.2+ by SAP
- SE Linux implements Mandatory Access Control
- SAP Hana processes run in the `unconfined_t` SELinux policy
- read the documentation to get familiar with SE Linux

Security Updates

Priority: High

- Do regular security updates
- Check, if new security fixes are available:

  ```
  # yum check-update --security
  ```

- If a security patch impacts SAP HANA operation, then SAP will publish an SAP note where it is stated
- Use the update procedure explained in the last section
- Limit an update to security relevant fixes:

  ```
  # yum update --security
  ```

Red Hat

Thank You !

in https://linkedin.com/company/Red-Hat

f https://facebook.com/RedHatinc

https://youtube.com/user/RedHatVideos

https://twitter.com/RedHat

SAP Platinum Partner