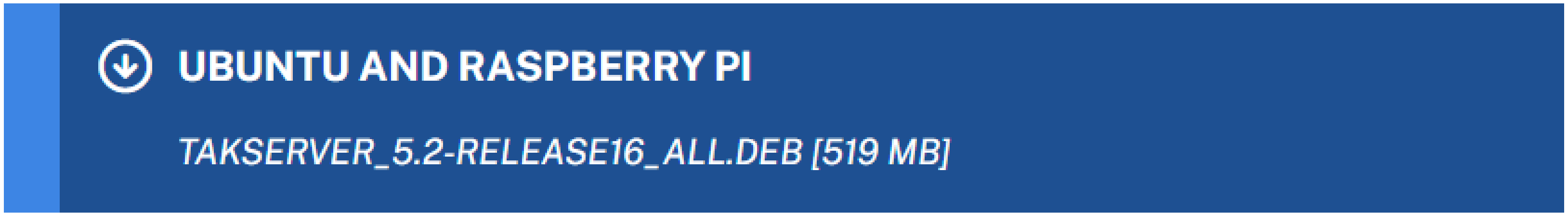
COMMUNICATIONS
APPLICATION GROUP

Slevin’s Guide to Setting up OG TAK Server

- Install Ubuntu
- Login and update ubuntu
- Enable ssh access
- Add user: takadmin
  - Sudo adduser takadmin
  - Assign password and just hit enter for defaults on the rest
- Add takadmin to sudoers group:
  - Login to root
  - sudo adduser takadmin sudo
- Modify Linux pluggable authentication module limits:
  - sudo nano /etc/security/limits.conf
  - or
  - # Increase JVM threads
  - # Each 'tab' is six spaces when typing manually
  - echo -e "*   soft   nofile   32768\n*   hard   nofile   32768\n" | sudo tee --append /etc/security/limits.conf
- Confirm that new limits are set:
  - sudo tail -n 15 /etc/security/limits.conf
- Install PostgreSQL and PostGIS
  - sudo sh -c 'echo "deb https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" > /etc/apt/sources.list.d/pgdg.list'
  - wget -O- https://www.postgresql.org/media/keys/ACCC4CF8.asc | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/postgresql.org.gpg > /dev/null

Check out our other setup and installation guides:
guides.commsag.com

- Update repository database with recent changes:
  - sudo apt update -y
- Check to see if Java installed:
  - java --version
- If not, install Java:
  - sudo apt install openjdk-17-jre
- Download TAK Server package from tak.gov
  - 

    UBUNTU AND RASPBERRY PI

    TAKSERVER_5.2-RELEASE16_ALL.DEB [519 MB]
- Copy the server package from your downloads to Ubuntu machine using Powershell or WinSCP:
  - If you are using Windows, open File Explorer and navigate to the directory of the installation binaries. Hold the Shift key and right-click within the explorer. Select from the options Open in Terminal, Open PowerShell window here, or if you have Windows Subsystem for Linux (SWL), select Open Linux shell here. This will open a terminal window in the desired directory.
  - scp takserver_5.2-RELEASE16_all.deb takadmin@<YOUR IP ADDRESS>:~/
- Login to server CLI and install the TAK Server
  - sudo apt install ./takserver_5.2-RELEASE16_all.deb -y
- After installing, modify default certificate password:
  - sudo su tak
  - cd /opt/tak/certs
  - nano cert-metadata.sh
- Edit the values to match your organization: country, state, city, organization, organizational unit; Change passwords if desired
- Create a self-signed root certificate:
  - ./makeRootCa.sh --ca-name TAK-ROOT-CA-01
- Create an Intermediate Certificate:
  - ./makeCert.sh ca TAK-ID-CA-01
  - Type y to allow system to move files around

- Create a server certificate:
    - ./makeCert.sh server takserver
- Modify the Core Configuration:
    - sed -i 's/truststore-root/truststore-TAK-ID-CA-01/g' /opt/tak/CoreConfig.example.xml
- Validate config changes:
    - cat /opt/tak/CoreConfig.example.xml | grep truststore-
- Exit the tak user session
    - exit
- Enable and start the TAK Server:
    - sudo systemctl enable takserver.service
    - sudo systemctl start takserver.service
- Check the logs to confirm startup:
    - ls -l /opt/tak/logs/
    - or tail the stream:
        - tail -f /opt/tak/logs/takserver-messaging.log
    - ctrl-c to stop log stream
- Create an administrator account, certificate, and elevate for administration:
    - sudo su tak
    - cd /opt/tak/certs
    - ./makeCert.sh client webadmin
    - java -jar /opt/tak/utils/UserManager.jar certmod -A /opt/tak/certs/files/webadmin.pem
    - exit
- Move the administrator certificate so that we can copy and install it on our administrative workstation to make the TAK Server remotely:
    - cd ~
    - sudo cp -v /opt/tak/certs/files/webadmin.p12 .
    - sudo chown -R takadmin:takadmin /home/takadmin
    - ls -l
- Configure the Firewall to accept secure connections over TLS:
    - Check to see if UFW is installed:
        - sudo ufw status

    - If not, install it:
        - sudo apt install ufw -y
    - Configure UFW Firewall:
        - sudo ufw default deny incoming
        - sudo ufw default allow outgoing
        - sudo ufw allow ssh
        - sudo ufw allow 8089/tcp
        - sudo ufw allow 8443/tcp
        - sudo ufw enable
        - y to confirm
        - sudo ufw status
- Configure administrative workstation to access the Marti Dashboard
    - On admin workstation, e.g., Windows PC, navigate to where you want to store the TAK Server's administrative certificate
    - Hold shift key, right click and choose "open in terminal"
    - scp takadmin@<YOUR IP ADDRESS>:~/webadmin.p12 .
    - Double click the certificate in the location you copied it to
    - Keep the defaults and click Next on the next two prompts. When prompted for our certificate password enter atakatak or the password set in the cert-metadata.sh during setup. When asked to specify a Certificate Store select Place all certificates in the following store and click Browse. Select the Personal from the list of available Certificate Stores. Click Next and host to import our certificate to our host truststore.
    - Open Certificate Manager (certmgr.msc) to confirm successful import under Personal > Certificates
    - Select the two CA: TAK-ID-CA-OA & TAK-ROOT-CA-01
    - Move them to: Trusted Root Certification Authorities > Certificates
    - Click yes when prompted
- Adding Users using the Soft Certificate Management method:
    - From the TAK Server CLI
        - sudo su tak
        - cd /opt/tak/certs
        - ./makeCert.sh client <clientname>

Check out our other setup and installation guides:
guides.commsag.com