POLICIA FEDERAL ARGENTINA

Procedimiento Estado Fortinet

Superintendencia FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Tabla de contenido

REVISIÓN ESTADO DEL FORTISIEM **3**

REVISIÓN DE ESTADO DEL SANDBOX **4**

VERIFICACIÓN ESTADO EMS: **5**

VERIFICAR ESTADO DEL FORTIANALYZER **6**

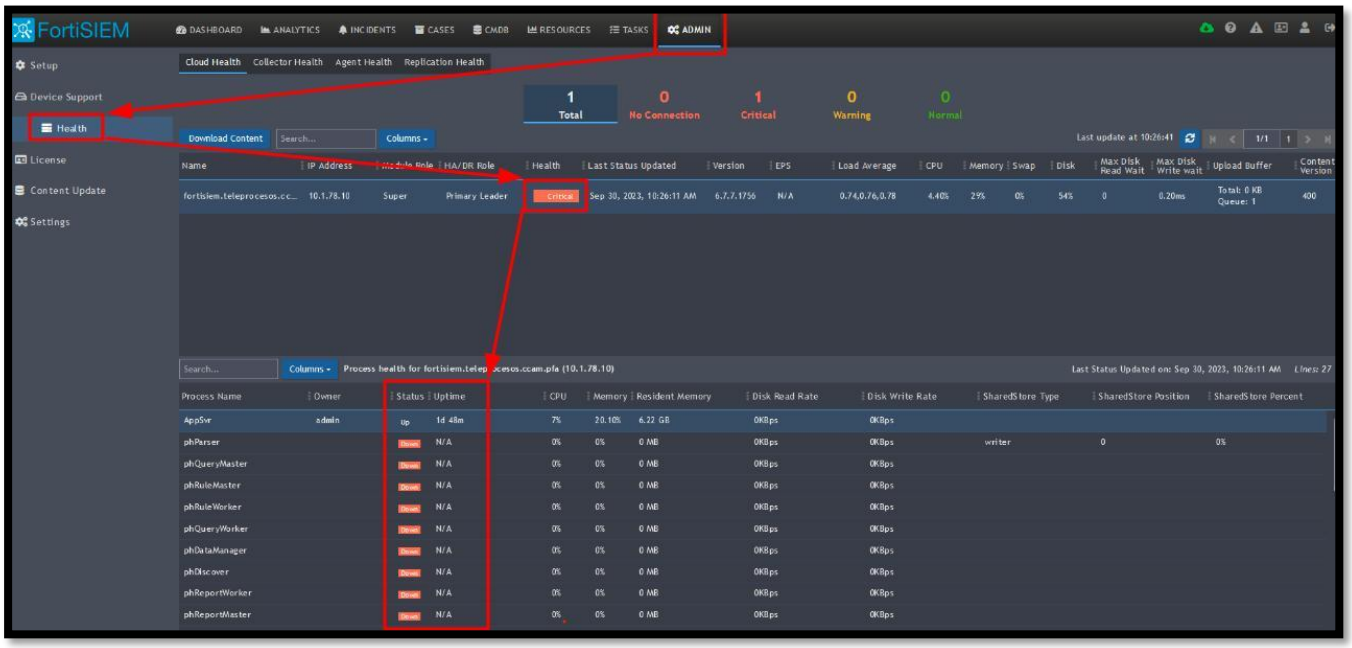
Revisión estado del FortiSIEM

Existen tres (03) estados del SIEM:

- **Normal** (verde)
- **Warning** (amarillo, significa que algún servicio / proceso se inició hace menos de 1 hr.)
- **Critical** (rojo, los servicios / procesos están caídos)

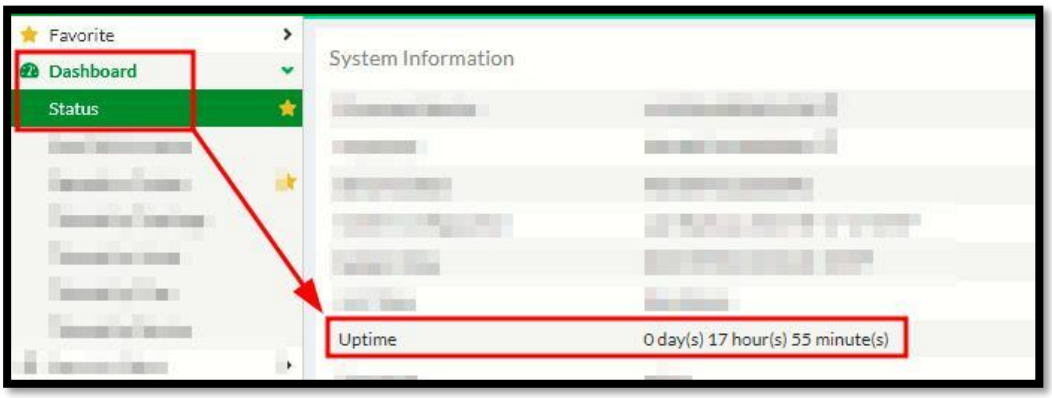
  Si hace clic sobre el estado (el color) se desplegará los servicios / procesos que están en funcionamiento o no.

- **Admin**
  - **Health** (observará el estado del SIEM)

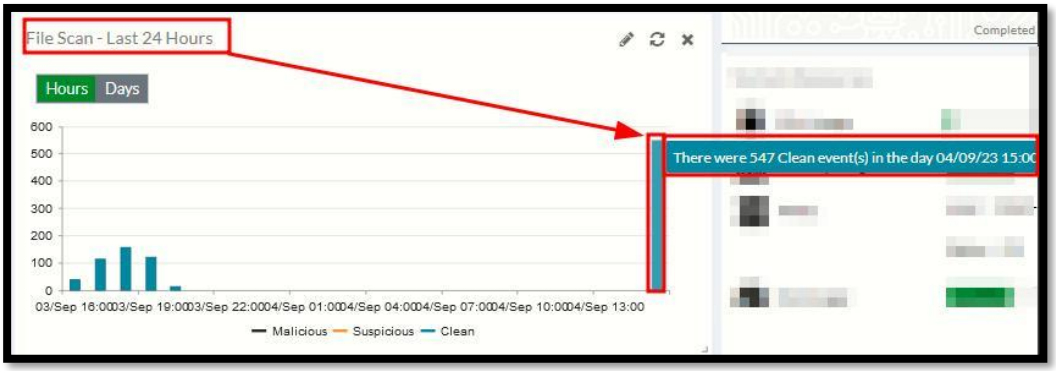


Revisión de estado del Sandbox

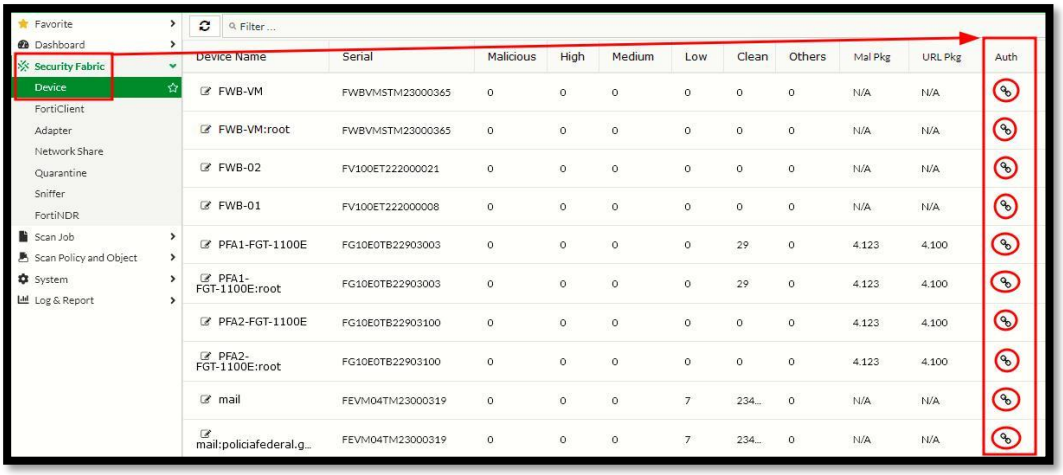
- 1ro. En el **Dashboard** / **Status**
  - Corroborar el **Uptime** (tiempo encendido) en *System Information*.



  - Confirmar **File Scan – Last 24 hours.**

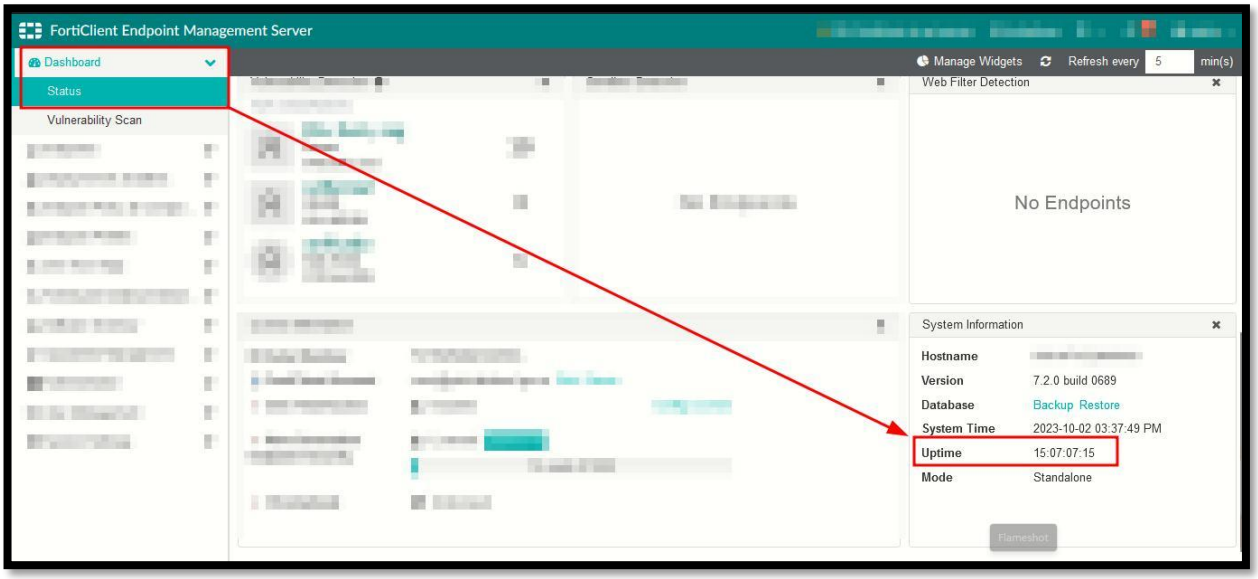


- 2do**.** En caso de que se haya caído realizar la siguiente comprobación y acción.
  - En **Security Fabric / Devices**, hacer clic sobre las cadenas en la columna de *Auth* (autenticación).

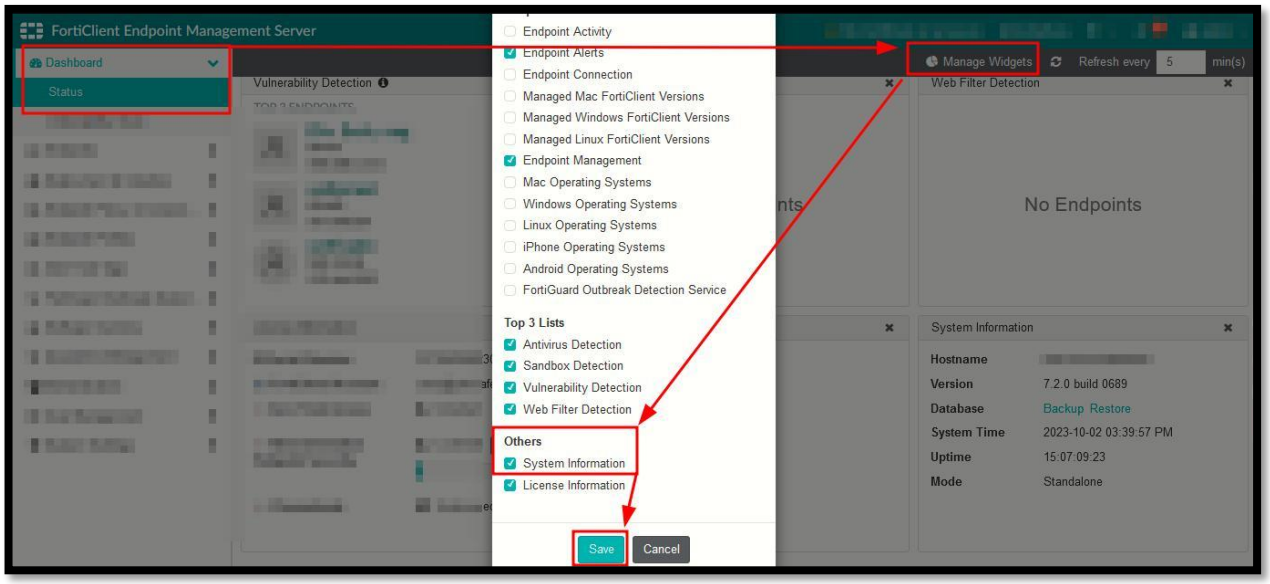


Verificación estado EMS:

- Ingresar a la herramienta, en **Dashboard** ubicarse en **Status**, acto seguido buscar el Widget *System Information*.

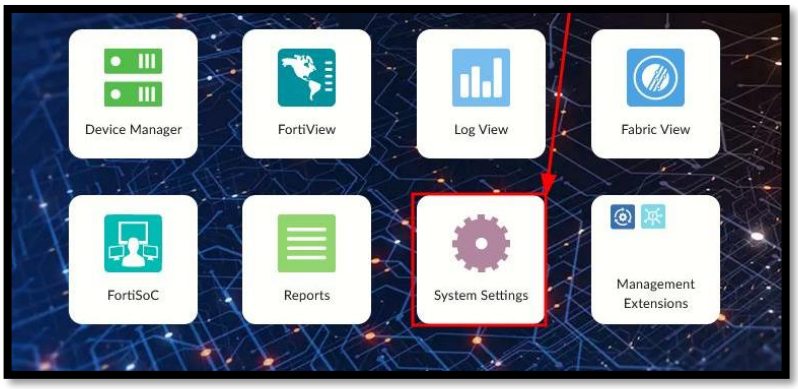


- En caso de no tener el mencionado Widget, habilitarlo con el siguiente método.

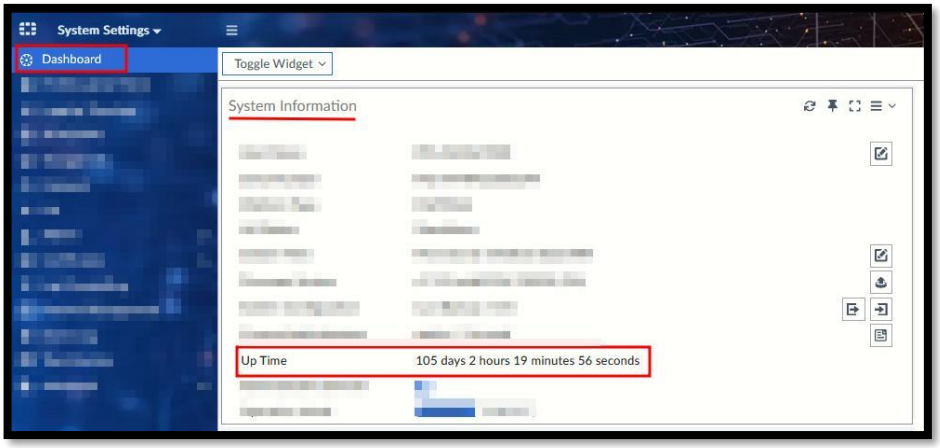


Verificar estado del FortiAnalyzer

- Ingresando a la herramienta, ingresar a cualquier *ADDOM*, luego **System Settings**.



- En **System Settings**, diríjase al **Dashboard**, en el *Widget System Information* busque **Up Time**.



- Preventivamente, haga scroll dentro del **Dashboard** y verifique en el *Widget System Resources* que **el CPU – Memory Usage – Disk Usage** tengan actividad y se encuentren dentro los valores aceptables de funcionamiento.