

MANTENIMIENTO PREVENTIVO

NAC- FORESCOUT



**Datos del Documento**

|  |  |  |
| --- | --- | --- |
| **Elaborado por:**  Ingeniero de Operaciones  *Roger Chauca Zea* | **Revisado por:**  Jefe de Ingenieria e Implementaciones  *Roger Chauca Zea* | **Aprobado por:**  Gerente de Operaciones  *Felix Sandoval* |
| **Fecha:** 21/12/2023 | **Fecha:**  22/12/2023 | **Fecha:**  22/01/2022 |

**Resumen de cambios del Informe**

|  |  |  |  |
| --- | --- | --- | --- |
| Versión | Autor | Fecha | Descripción |
| 1.0 | *Renzo Segura Ccahuana* | *21/12/2023* | *Elaboracion del informe de mantenimiento preventivo sobre los equipos Forescout* |
| 1.1 | *Roger Chauca Zea* | *22/12/2023* | *Revisión* |
|  |  |  |  |

**CONFIDENCIALIDAD**

Este documento contiene información confidencial sobre características del negocio de propiedad del Grupo Electrodata S.A.C. No está permitido ningún tipo de utilización de la información contenida aquí sin previo consentimiento por escrito del Grupo Electrodata S.A.C.

**Índice**

[**1. Resumen Ejecutivo 4**](#_Toc93410618)

[**2. Objetivo 4**](#_Toc93410619)

[**3. Personal 4**](#_Toc93410620)

[**4. Análisis de la Situación Actual 4**](#_Toc93410621)

[**5. Diseño y Despliegue 5**](#_Toc93410622)

[**5.1 Limpieza de Base de Datos 7**](#_Toc93410623)

[**6. Conclusiones 12**](#_Toc93410624)

[**7. Recomendaciones 12**](#_Toc93410625)

# Resumen Ejecutivo

El presente documento tiene como finalidad detallar las actividades realizadas durante el mantenimiento preventivo realiza de manera remota – Limpieza de la base de datos de la solución Forescout instalada en el Datacenter de Caja Arequipa de acuerdo a las especificaciones técnicas del Contrato.

Este informe muestra el procedimiento que sugiere el fabricante el cual es recomendado realizarlo cada 6 meses, el cual nos ayuda a eliminar las inconsistencias que pueden haber dentro de la base de datos.

Al finalizar el informe muestra las conclusiones y recomendaciones que se deben tener en cuenta para mantener la base de datos de la solución Forescout estable.

# Objetivo

El objetivo de este documento es detallar las actividades realizadas durante el mantenimiento preventivo realizada de manera remota - Limpieza de la base de datos de la solución Forescout y validar la operatividad de la solución.

# Personal

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre de Contacto** | **Número de Contacto** | **Empresa** | **Email** |
| Roger Chauca Zea | 998140794 | Electrodata | rogerchz@electrodata.com.pe |

# Análisis de la Situación Actual

Para realizar el análisis de los equipos Forescout de Caja Arequipa se recolectó información de los Siguientes Equipos CounterACT.

|  |  |  |
| --- | --- | --- |
| **Ítem** | **Hostname** | **IP** |
| **1** | APLNACCDP1 | 172.24.110.61 |
| **2** | APLNACCDP2 | 172.24.110.62 |
| **3** | APLNACCDA1 | 172.24.110.60 |
| **4** | ADMNACCDP1 | 172.24.165.9 |
| **5** | ADMNACCDA1 | 172.24.165.10 |

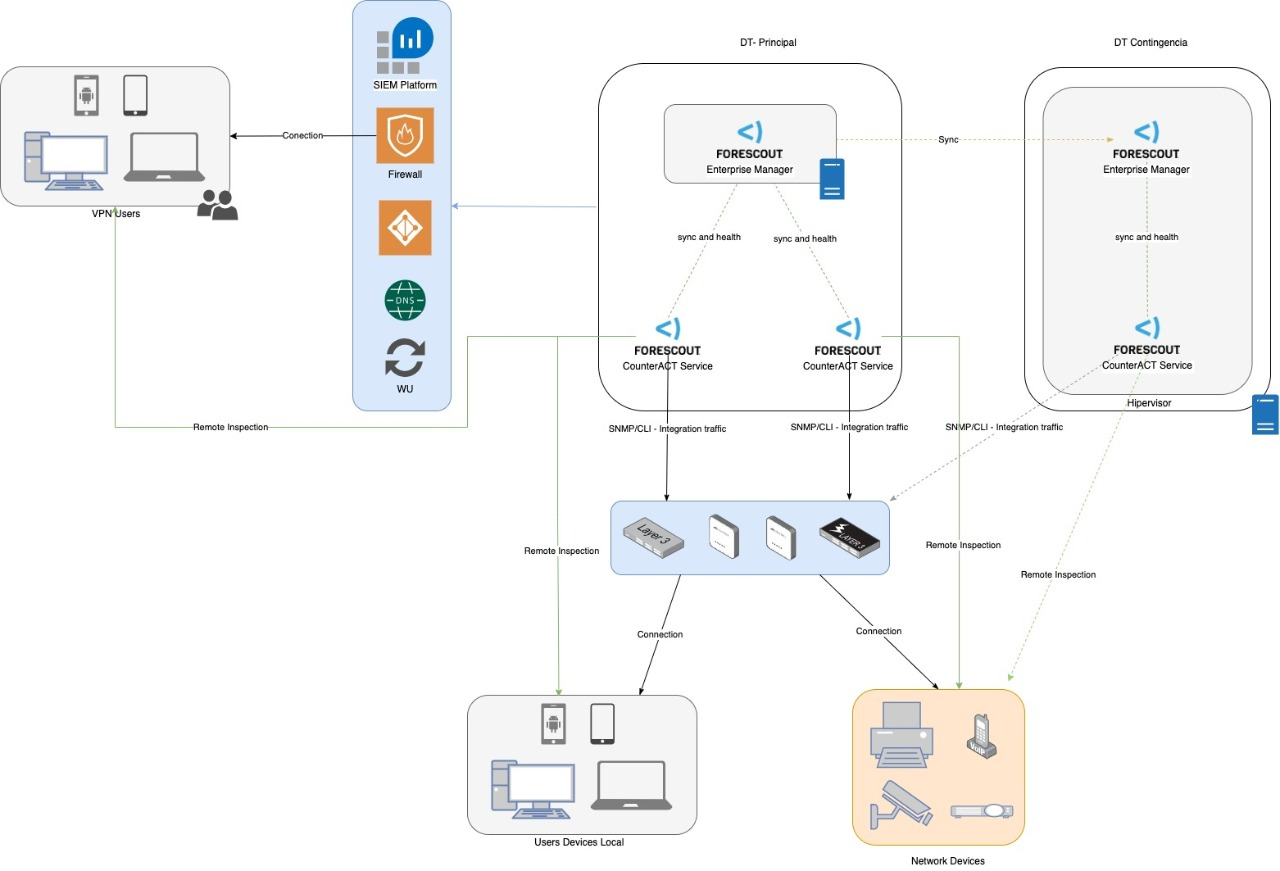
**Tabla 01 – Nombre y dirección IP de Equipos**

El mantenimiento preventivo consiste realizar la limpieza de la base de datos de cada uno de los equipos mencionados.

# Diseño y Despliegue

Actualmente la solucion de Control de Acceso a la red (NAC), cuenta con la siguiente topologia, que esta diseñada para poder descubrir, inspeccionar y controlar todo dispositivo que se conecte a la red corporativa de Caja Arequipa.

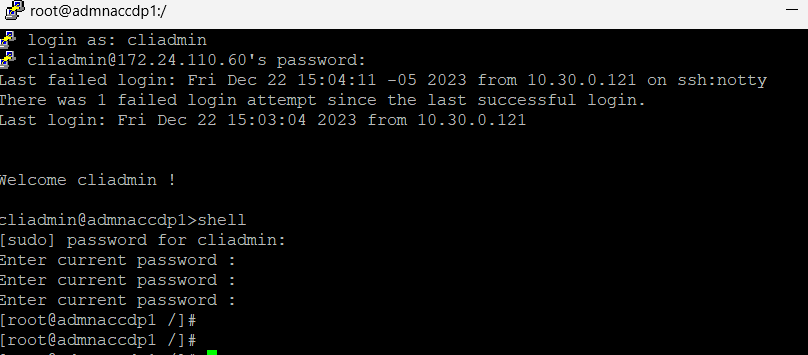
Donde se puede observar la integracion tanto en los data center de Arequipa y Lima.



**Fig.01 - Topología Física**

## **5.1 Limpieza de Base de Datos**

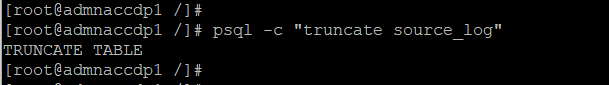
* Ingreso mediante CLI a los equipos a intervenir.



**Fig. 02 – Conexión SSH a equipo.**

* Se procede a realizar la limpieza del origen de los logs, para ello se ejecutó el siguiente comando:

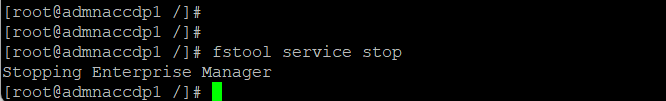
**psql –c “truncate source\_log”**

****

**Fig. 03 – Limpieza de Origen de Log.**

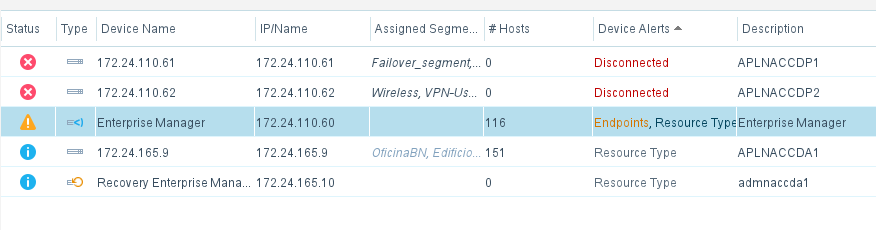
* Se detiene los servicios del equipo intervenido, para ello se ejecutó el siguiente comando:

**fstool service stop**



**Fig. 04 – Detension de servicio.**

* Una vez detenido el servicio, se valida en la consola de Forescout, la alarma de desconexión y sincronización con el equipo.

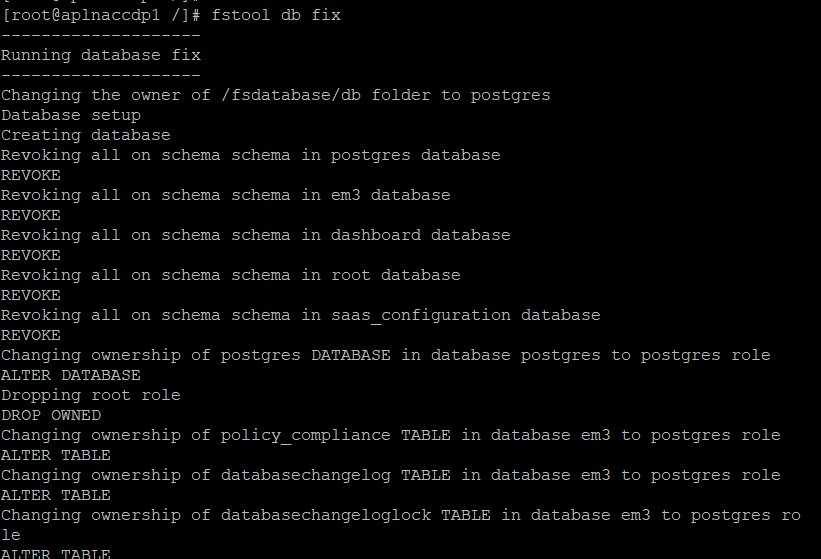


**Fig. 05 – Equipo Desconectado.**

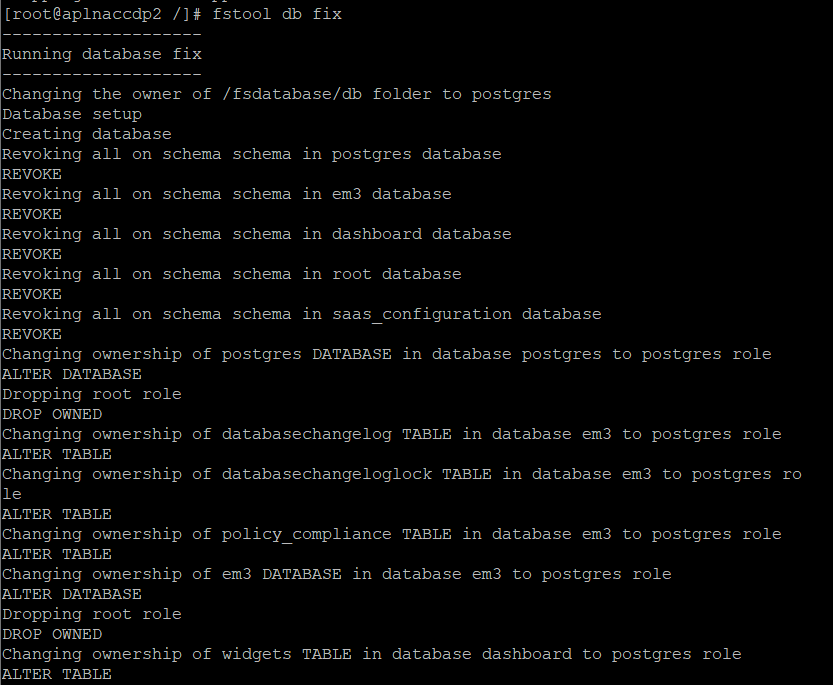
Se procedió con la limpieza de la base de datos de los equipo intervenidos (172.24.110.61 y 172.24.110.62), mediante el comando:

**fstool db fix:**

* Este comando hace que mantenga la mayor cantidad de datos posible, en el peor de los casos se podría haber eliminado información de un 20% del total de endpoint que estén conectados a la caja que administra.
* El procedimiento de la limpieza de base de datos puede gatillar una reinspección de endpoints, sin embargo, lo hace sobre los equipos que se detectan encendidos/ conectados en ese momento a la red.

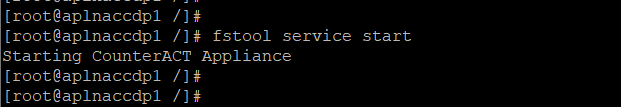


**Fig. 06 – Limpieza de Base de Datos Counter ACT1.**



**Fig. 07 – Limpieza de Base de Datos Counter ACT2**

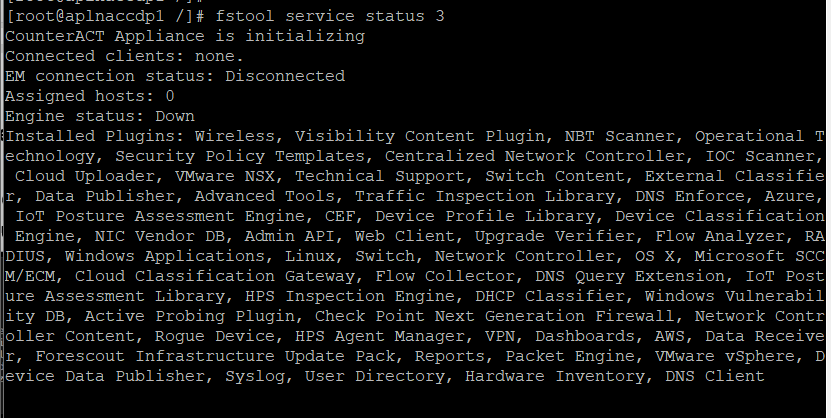
* Luego de finalizar con la limpieza, inmediatamente se levanta el servicio.



**Fig. 08 – Servicio levantado.**

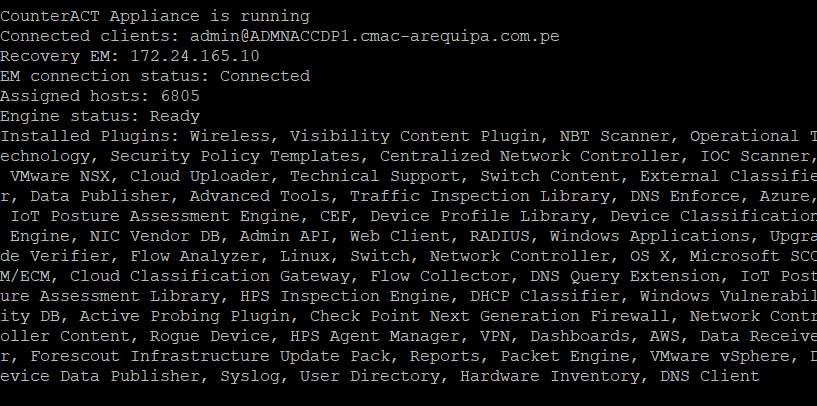
* Para realizar un monitoreo en tiempo real y validar que el servicio se encuentra levantado y sincronizado con el servidor principal (10.80.90.243), se ejecuta el siguiente comando:

**fstool service status 3**



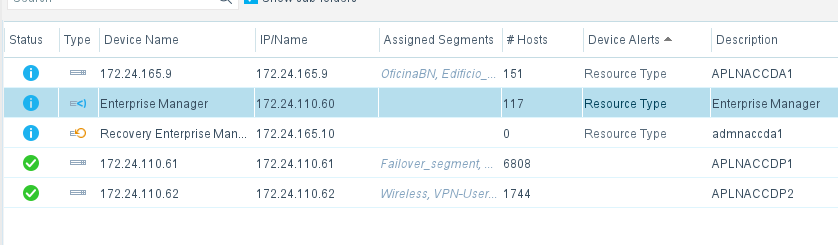
**Fig. 09 – Monitoreo de Servicio.**

* Para validar que el servicio se encuentre levantado, se debe verificar el estado de conectado, el cual se muestra en la siguiente imagen:



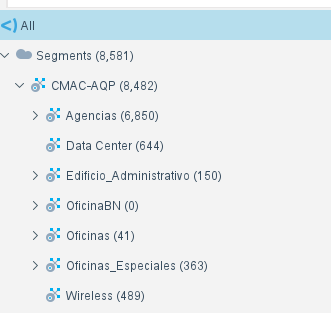
**Fig. 10 – Servicio levantado y sincronizado.**

* De igual manera en la plataforma de forescout se podrá visualizar la sincronización de los appliance Forescout:



**Fig. 11 – Equipo conectado y sincronizado.**

* Una vez realizado la limpieza en todos los equipos intervenidos, se procede a validar el estado y sincronización de todos los equipos.
* Se revisa que los endpoint se encuentren dentro de los segmentos correspondiente.

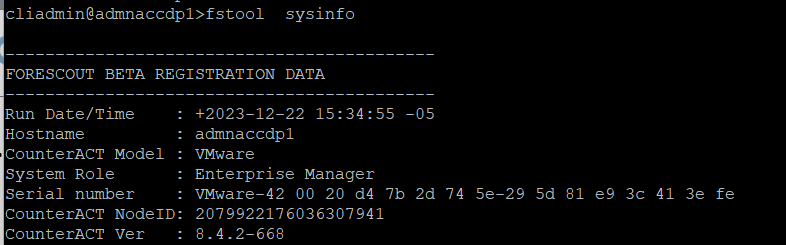


**Fig. 12 Segmentacion Caja Arequipa**

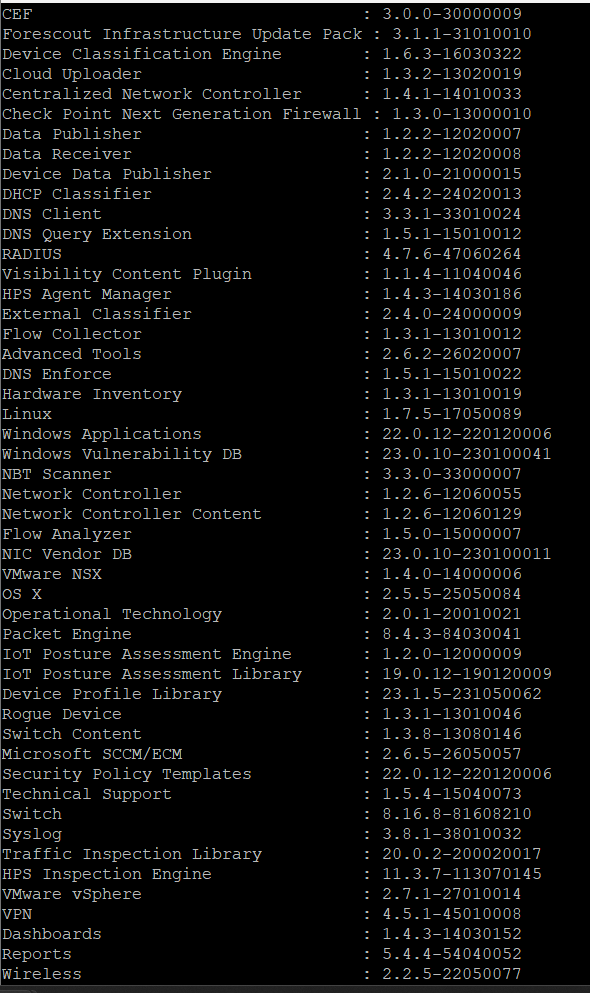
* Se valida que no hubo variación de los equipos/endpoint, durante el mantenimiento.

# Conclusiones

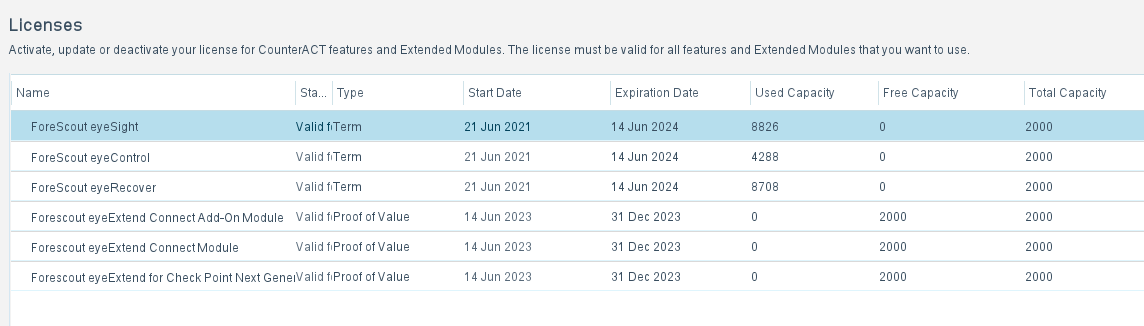
* Actualmente la plataforma trabaja con la versión 8.4.2-668



* Se procedió con la limpieza de base de datos de los equipos de forma exitosa.
* Se validó que los equipos se encuentren con los servicios activos y sincronizados.
* Se validó la normalización de las políticas de descubrimiento y de control.
* Se confirmo que los plugins están actualizados:



* La solución esta licenciado para 2000 endpoint, sin embargo, se están detectando alrededor de 9000 (8826), se necesita actualizar el licenciamiento.



# Recomendaciones

* Realizar el mantenimiento de la base de datos de todos los equipos CounterACT cada 6 meses.
* Actualizar los plugins de las principales funcionalidades (network, radius, Active Directory, Wireless,etc).