



**MANTENIMIENTO PREVENTIVO**  
NAC- FORESCOUT



SISTEMA INTEGRADO DE GESTIÓN				
	Mantenimiento Preventivo – NAC Forescout			
	Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 2 de 12	

## Datos del Documento

Elaborado por:	Revisado por:	Aprobado por:
Ingeniero de Operaciones <i>Roger Chauca Zea</i>	Jefe de Ingenieria e Implementaciones <i>Roger Chauca Zea</i>	Gerente de Operaciones <i>Felix Sandoval</i>
<b>Fecha:</b> 21/12/2023	<b>Fecha:</b> 22/12/2023	<b>Fecha:</b> 22/01/2022

## Resumen de cambios del Informe

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

## 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.

SISTEMA INTEGRADO DE GESTIÓN			
	Mantenimiento Preventivo – NAC Forescout		
	Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 3 de 12

## Índice

<b>1. Resumen Ejecutivo .....</b>	<b>4</b>
<b>2. Objetivo .....</b>	<b>4</b>
<b>3. Personal .....</b>	<b>4</b>
<b>4. Análisis de la Situación Actual .....</b>	<b>4</b>
<b>5. Diseño y Despliegue .....</b>	<b>5</b>
<b>5.1 Limpieza de Base de Datos .....</b>	<b>6</b>
<b>6. Conclusiones .....</b>	<b>11</b>
<b>7. Recomendaciones .....</b>	<b>12</b>

SISTEMA INTEGRADO DE GESTIÓN				
	Mantenimiento Preventivo – NAC Forescout			
	Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 4 de 12	

## 1. 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.

## 2. 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.

## 3. Personal

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

## 4. 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.

SISTEMA INTEGRADO DE GESTIÓN			
Mantenimiento Preventivo – NAC Forescout			
Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 5 de 12	

## 5. Diseño y Despliegue

Actualmente la solución de Control de Acceso a la red (NAC), cuenta con la siguiente topología, 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 integración tanto en los data center de Arequipa y Lima.

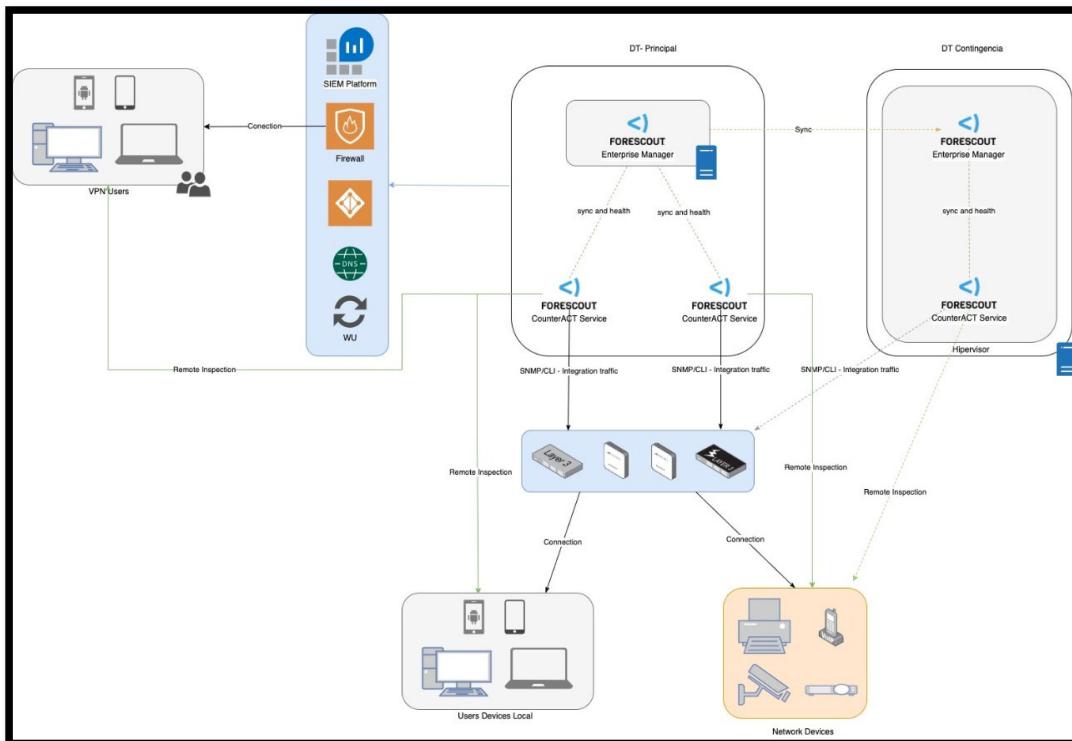


Fig.01 - Topología Física

SISTEMA INTEGRADO DE GESTIÓN			
	Mantenimiento Preventivo – NAC Forescout		
	Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 6 de 12

## 5.1 Limpieza de Base de Datos

- Ingreso mediante CLI a los equipos a intervenir.
- 

```
root@admnaccdp1:~#
login as: cliadmin
cliadmin@172.24.110.60's password:
Last failed login: Fri Dec 22 15:04:11 -05 2023 from 10.30.0.121 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Fri Dec 22 15:03:04 2023 from 10.30.0.121

Welcome cliadmin !

cliadmin@admnaccdp1>shell
[sudo] password for cliadmin:
Enter current password :
Enter current password :
Enter current password :
[root@admnaccdp1 ~]#
[root@admnaccdp1 ~]#
```

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”**

```
[root@admnaccdp1 ~]#
[root@admnaccdp1 ~]# psql -c "truncate source_log"
TRUNCATE TABLE
[root@admnaccdp1 ~]#
```

Fig. 03 – Limpieza de Origen de Log.

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

**fstool service stop**

```
[root@admnaccdp1 ~]#
[root@admnaccdp1 ~]#
[root@admnaccdp1 ~]# fstool service stop
Stopping Enterprise Manager
[root@admnaccdp1 ~]#
```

Fig. 04 – Detencion de servicio.

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

SISTEMA INTEGRADO DE GESTIÓN						
e-data group		Mantenimiento Preventivo – NAC Forescout				
		Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 7 de 12		

Status	Type	Device Name	IP/Name	Assigned Segme...	# Hosts	Device Alerts ▾	Description
✗	≡	172.24.110.61	172.24.110.61	Failover_segment,...	0	Disconnected	APLNACCDP1
✗	≡	172.24.110.62	172.24.110.62	Wireless, VPN-U... ...	0	Disconnected	APLNACCDP2
⚠	➡◀	Enterprise Manager	172.24.110.60		116	Endpoints, Resource Type	Enterprise Manager
ℹ	≡	172.24.165.9	172.24.165.9	OficinaBN, Edificio... ...	151	Resource Type	APLNACCDA1
ℹ	➡⌚	Recovery Enterprise Mana...	172.24.165.10		0	Resource Type	admnnaccda1

**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.

```
[root@aplnaccdp1 /]# fstool db fix
-----
Running database fix
-----
Changing the owner of /fsdatabase/db folder to postgres
Database setup
Creating database
Revoking all on schema schema in postgres database
REVOKE
Revoking all on schema schema in em3 database
REVOKE
Revoking all on schema schema in dashboard database
REVOKE
Revoking all on schema schema in root database
REVOKE
Revoking all on schema schema in saas_configuration database
REVOKE
Changing ownership of postgres DATABASE in database postgres to postgres role
ALTER DATABASE
Dropping root role
DROP OWNED
Changing ownership of policy_compliance TABLE in database em3 to postgres role
ALTER TABLE
Changing ownership of databasechangelog TABLE in database em3 to postgres role
ALTER TABLE
Changing ownership of databasechangeloglock TABLE in database em3 to postgres role
ALTER TABLE
```

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

SISTEMA INTEGRADO DE GESTIÓN			
	Mantenimiento Preventivo – NAC Forescout		
	Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 8 de 12

```
[root@aplnaccdp2 /]# fstool db fix
-----
Running database fix
-----
Changing the owner of /fsdatabase/db folder to postgres
Database setup
Creating database
Revoking all on schema schema in postgres database
REVOKE
Revoking all on schema schema in em3 database
REVOKE
Revoking all on schema schema in dashboard database
REVOKE
Revoking all on schema schema in root database
REVOKE
Revoking all on schema schema in saas_configuration database
REVOKE
Changing ownership of postgres DATABASE in database postgres to postgres role
ALTER DATABASE
Dropping root role
DROP OWNED
Changing ownership of databasechangelog TABLE in database em3 to postgres role
ALTER TABLE
Changing ownership of databasechangeloglock TABLE in database em3 to postgres role
ALTER TABLE
Changing ownership of policy_compliance TABLE in database em3 to postgres role
ALTER TABLE
Changing ownership of em3 DATABASE in database em3 to postgres role
ALTER DATABASE
Dropping root role
DROP OWNED
Changing ownership of widgets TABLE in database dashboard to postgres role
ALTER TABLE
```

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

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

```
[root@aplnaccdp1 /]#
[root@aplnaccdp1 /]# fstool service start
Starting CounterACT Appliance
[root@aplnaccdp1 /]#
[root@aplnaccdp1 /]#
```

**Fig. 08 – Servicio levantado.**

SISTEMA INTEGRADO DE GESTIÓN			
	Mantenimiento Preventivo – NAC Forescout		
	Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 9 de 12

- 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**

```
[root@aplnaccdp1 /]# fstool service status 3
CounterACT Appliance is initializing
Connected clients: none.
EM connection status: Disconnected
Assigned hosts: 0
Engine status: Down
Installed Plugins: Wireless, Visibility Content Plugin, NBT Scanner, Operational Technology, Security Policy Templates, Centralized Network Controller, IOC Scanner, Cloud Uploader, VMware NSX, Technical Support, Switch Content, External Classifier, Data Publisher, Advanced Tools, Traffic Inspection Library, DNS Enforce, Azure, IoT Posture Assessment Engine, CEF, Device Profile Library, Device Classification Engine, NIC Vendor DB, Admin API, Web Client, Upgrade Verifier, Flow Analyzer, RADIUS, Windows Applications, Linux, Switch, Network Controller, OS X, Microsoft SCCM/ECM, Cloud Classification Gateway, Flow Collector, DNS Query Extension, IoT Posture Assessment Library, HPS Inspection Engine, DHCP Classifier, Windows Vulnerability DB, Active Probing Plugin, Check Point Next Generation Firewall, Network Controller Content, Rogue Device, HPS Agent Manager, VPN, Dashboards, AWS, Data Receiver, Forescout Infrastructure Update Pack, Reports, Packet Engine, VMware vSphere, Device Data Publisher, Syslog, User Directory, Hardware Inventory, DNS Client
```

**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:

```
CounterACT Appliance is running
Connected clients: admin@ADMNACCDP1.cmac-arequipa.com.pe
Recovery EM: 172.24.165.10
EM connection status: Connected
Assigned hosts: 6805
Engine status: Ready
Installed Plugins: Wireless, Visibility Content Plugin, NBT Scanner, Operational Technology, Security Policy Templates, Centralized Network Controller, IOC Scanner, VMware NSX, Cloud Uploader, Technical Support, Switch Content, External Classifier, Data Publisher, Advanced Tools, Traffic Inspection Library, DNS Enforce, Azure, IoT Posture Assessment Engine, CEF, Device Profile Library, Device Classification Engine, NIC Vendor DB, Admin API, Web Client, RADIUS, Windows Applications, Upgrade Verifier, Flow Analyzer, Linux, Switch, Network Controller, OS X, Microsoft SCCM/ECM, Cloud Classification Gateway, Flow Collector, DNS Query Extension, IoT Posture Assessment Library, HPS Inspection Engine, DHCP Classifier, Windows Vulnerability DB, Active Probing Plugin, Check Point Next Generation Firewall, Network Controller Content, Rogue Device, HPS Agent Manager, VPN, Dashboards, AWS, Data Receiver, Forescout Infrastructure Update Pack, Reports, Packet Engine, VMware vSphere, Device Data Publisher, Syslog, User Directory, Hardware Inventory, DNS Client
```

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

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

SISTEMA INTEGRADO DE GESTIÓN						
e-data group		Mantenimiento Preventivo – NAC Forescout				
Fecha de Aprobación: 22/12/2023		Número de Versión: 1.1		Página 10 de 12		

Status	Type	Device Name	IP/Name	Assigned Segments	# Hosts	Device Alerts ▲	Description
Info	≡	172.24.165.9	172.24.165.9	OficinaBN, Edificio_...	151	Resource Type	APLNACCDA1
Info	↔	Enterprise Manager	172.24.110.60		117	Resource Type	Enterprise Manager
Info	⟳	Recovery Enterprise Man...	172.24.165.10		0	Resource Type	admnnaccda1
OK	≡	172.24.110.61	172.24.110.61	Failover_segment, ...	6808		APLNACCDP1
OK	≡	172.24.110.62	172.24.110.62	Wireless, VPN-User...	1744		APLNACCDP2

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.

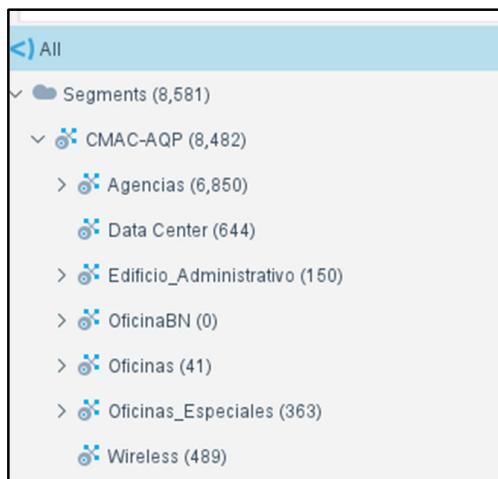


Fig. 12 Segmentación Caja Arequipa

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

## 6. Conclusiones

- Actualmente la plataforma trabaja con la versión 8.4.2-668

```
cliadmin@admnnaccdp1>fstool sysinfo
-----
FORESCOUT BETA REGISTRATION DATA
-----
Run Date/Time      : +2023-12-22 15:34:55 -05
Hostname          : admnnaccdp1
CounterACT Model  : VMware
System Role       : Enterprise Manager
Serial number     : VMware-42 00 20 d4 7b 2d 74 5e-29 5d 81 e9 3c 41 3e fe
CounterACT NodeID: 2079922176036307941
CounterACT Ver    : 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 confirmó que los plugins están actualizados:

```
CEF                      : 3.0.0-30000009
Forescout Infrastructure Update Pack : 3.1.1-31010010
Device Classification Engine      : 1.6.3-16030322
Cloud Uploader                  : 1.3.2-13020019
Centralized Network Controller   : 1.4.1-14010033
Check Point Next Generation Firewall : 1.3.0-13000010
Data Publisher                : 1.2.2-12020007
Data Receiver                 : 1.2.2-12020008
Device Data Publisher          : 2.1.0-21000015
DHCP Classifier               : 2.4.2-24020013
DNS Client                    : 3.3.1-33010024
DNS Query Extension           : 1.5.1-15010012
RADIUS                       : 4.7.6-47060264
Visibility Content Plugin      : 1.1.4-11040046
HPS Agent Manager              : 1.4.3-14030186
External Classifier            : 2.4.0-24000009
Flow Collector                 : 1.3.1-13010012
Advanced Tools                 : 2.6.2-26020007
DNS Enforce                   : 1.5.1-15010022
Hardware Inventory             : 1.3.1-13010019
Linux                         : 1.7.5-17050089
Windows Applications           : 22.0.12-220120006
Windows Vulnerability DB      : 23.0.10-230100041
NBT Scanner                   : 3.3.0-33000007
Network Controller              : 1.2.6-12060055
Network Controller Content     : 1.2.6-12060129
Flow Analyzer                  : 1.5.0-15000007
NIC Vendor DB                 : 23.0.10-230100011
VMware NSX                     : 1.4.0-14000006
OS X                          : 2.5.5-25050084
Operational Technology         : 2.0.1-20010021
Packet Engine                  : 8.4.3-84030041
IoT Posture Assessment Engine : 1.2.0-12000009
IoT Posture Assessment Library: 19.0.12-190120009
Device Profile Library         : 23.1.5-231050062
Rogue Device                   : 1.3.1-13010046
Switch Content                 : 1.3.8-13080146
Microsoft SCCM/ECM             : 2.6.5-26050057
Security Policy Templates      : 22.0.12-220120006
Technical Support              : 1.5.4-15040073
Switch                        : 8.16.8-81608210
Syslog                         : 3.8.1-38010032
Traffic Inspection Library     : 20.0.2-200020017
HPS Inspection Engine          : 11.3.7-113070145
VMware vSphere                  : 2.7.1-27010014
VPN                            : 4.5.1-45010008
Dashboards                     : 1.4.3-14030152
Reports                        : 5.4.4-54040052
Wireless                       : 2.2.5-22050077
```

SISTEMA INTEGRADO DE GESTIÓN						
	Mantenimiento Preventivo – NAC Forescout					
	Fecha de Aprobación: 22/12/2023	Número de Versión: 1.1	Página 12 de 12			

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

Licenses							
Activate, update or deactivate your license for CounterACT features and Extended Modules. The license must be valid for all features and Extended Modules that you want to use.							
Name	Status	Type	Start Date	Expiration Date	Used Capacity	Free Capacity	Total Capacity
ForeScout eyeSight	Valid fTerm		21 Jun 2021	14 Jun 2024	8826	0	2000
ForeScout eyeControl	Valid fTerm		21 Jun 2021	14 Jun 2024	4288	0	2000
ForeScout eyeRecover	Valid fTerm		21 Jun 2021	14 Jun 2024	8708	0	2000
Forescout eyeExtend Connect Add-On Module	Valid fProof of Value		14 Jun 2023	31 Dec 2023	0	2000	2000
Forescout eyeExtend ConnectModule	Valid fProof of Value		14 Jun 2023	31 Dec 2023	0	2000	2000
Forescout eyeExtend for Check Point Next Generation Firewall	Valid fProof of Value		14 Jun 2023	31 Dec 2023	0	2000	2000

## 7. 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).