PROYECTO
REMEDIACIÓN ADDS

Contenido

Introducción

El presente documento tiene por objetivo otorgar la información necesaria respecto al proceso de remediación al cual fueron sometidos los servidores de CCU, correspondientes a la arquitectura de Active Directory y DNS.

Se ejecutarán diagnósticos de servicio y otorgará información necesaria para una administración eficiente en un futuro.

Las acciones ejecutadas en este proceso, han sido guiadas desde el siguiente resumen:

Fases	Actividad
Fase 1	Levantamiento
	Kick Off
	Pruebas de Conectividad
Fase 2	Remediación Replicación DC's
	Remediación DNS
	Remediación BPA SCAN DC's
	Diagrama Solución
	Parchado y paquetización vulnerabilidades
Fase 3	Separación Roles FSMO en DC's
	Validación y deshabilitación Obj. Obsoletos
	Robustecer Contraseñas en Dominio
	Promoción Contraseñas seguras
	Configurar NTP en servidores 02,03 y 04
	Estructurar roles administrativos DC's
Fase 4	Aplicación Healtcheck
	Pruebas de servicio con clientes
	Entrega de Plataforma
	Documentación respectiva

1.0.1 Replicación

Se ejecutan las pruebas de replicación entre máquinas de la arquitectura

Repadmin /showrepl

```
PS C:\Windows\system32> Repadmin /showrepl

Repadmin: running command /showrepl against full DC localhost
Default-First-Site-Name\SRV-DC-04-FJ
DSA Options: IS_GC
Site Options: (none)
DSA object GUID: 86751435-ba56-4269-bd13-1e983b68cfb0
DSA invocationID: 0ffc4594-7f41-47b9-ae96-9dd6dd55d76f

==== INBOUND NEIGHBORS ======================================

DC=ccu,DC=local
    Default-First-Site-Name\SRV-DC-02 via RPC
        DSA object GUID: 0e77c921-9238-4df9-9fc1-188217d38c5a
        Last attempt @ 2020-12-30 15:22:17 was successful.
    Default-First-Site-Name\SRV-DC-01 via RPC
        DSA object GUID: 46f6673d-75d4-49be-b6aa-09be3b61050f
        Last attempt @ 2020-12-30 15:22:24 was successful.

CN=Configuration,DC=ccu,DC=local
    Default-First-Site-Name\SRV-DC-01 via RPC
        DSA object GUID: 46f6673d-75d4-49be-b6aa-09be3b61050f
        Last attempt @ 2020-12-30 14:58:55 was successful.
    Default-First-Site-Name\SRV-DC-02 via RPC
        DSA object GUID: 0e77c921-9238-4df9-9fc1-188217d38c5a
        Last attempt @ 2020-12-30 14:58:55 was successful.

CN=Schema,CN=Configuration,DC=ccu,DC=local
    Default-First-Site-Name\SRV-DC-02 via RPC
        DSA object GUID: 0e77c921-9238-4df9-9fc1-188217d38c5a
        Last attempt @ 2020-12-30 14:58:55 was successful.
    Default-First-Site-Name\SRV-DC-01 via RPC
        DSA object GUID: 46f6673d-75d4-49be-b6aa-09be3b61050f
        Last attempt @ 2020-12-30 14:58:55 was successful.

DC=ForestDnsZones,DC=ccu,DC=local
    Default-First-Site-Name\SRV-DC-02 via RPC
        DSA object GUID: 0e77c921-9238-4df9-9fc1-188217d38c5a
        Last attempt @ 2020-12-30 14:58:55 was successful.
    Default-First-Site-Name\SRV-DC-01 via RPC
        DSA object GUID: 46f6673d-75d4-49be-b6aa-09be3b61050f
        Last attempt @ 2020-12-30 14:58:55 was successful.

DC=DomainDnsZones,DC=ccu,DC=local
    Default-First-Site-Name\SRV-DC-02 via RPC
        DSA object GUID: 0e77c921-9238-4df9-9fc1-188217d38c5a
        Last attempt @ 2020-12-30 15:21:23 was successful.
    Default-First-Site-Name\SRV-DC-01 via RPC
        DSA object GUID: 46f6673d-75d4-49be-b6aa-09be3b61050f
        Last attempt @ 2020-12-30 15:21:59 was successful.
```

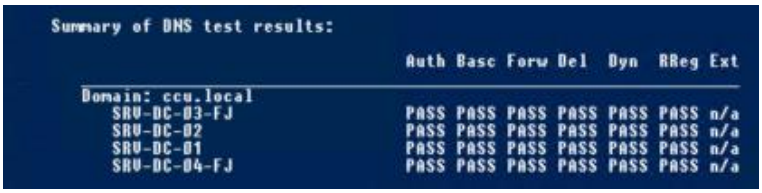
Repadmin /replsummary

```
PS C:\Windows\system32> REPADMIN /replsummary
Replication Summary Start Time: 2020-12-30 09:33:23

Beginning data collection for replication summary, this may take awhile:
  .......

Source DSA          largest delta    fails/total %%   error
 SRV-DC-01                  34m:41s    0 /  10    0
 SRV-DC-02                  34m:41s    0 /  10    0
 SRV-DC-03-FJ               44m:55s    0 /  10    0
 SRV-DC-04-FJ               44m:55s    0 /  10    0

Destination DSA     largest delta    fails/total %%   error
 SRV-DC-01                  44m:55s    0 /  10    0
 SRV-DC-02                  40m:19s    0 /  10    0
 SRV-DC-03-FJ               34m:41s    0 /  10    0
 SRV-DC-04-FJ               34m:29s    0 /  10    0
```

1.0.3 Resolución DNS

Se ejecutan pruebas de DCDIAG DNS para comprobar resolución de nombres

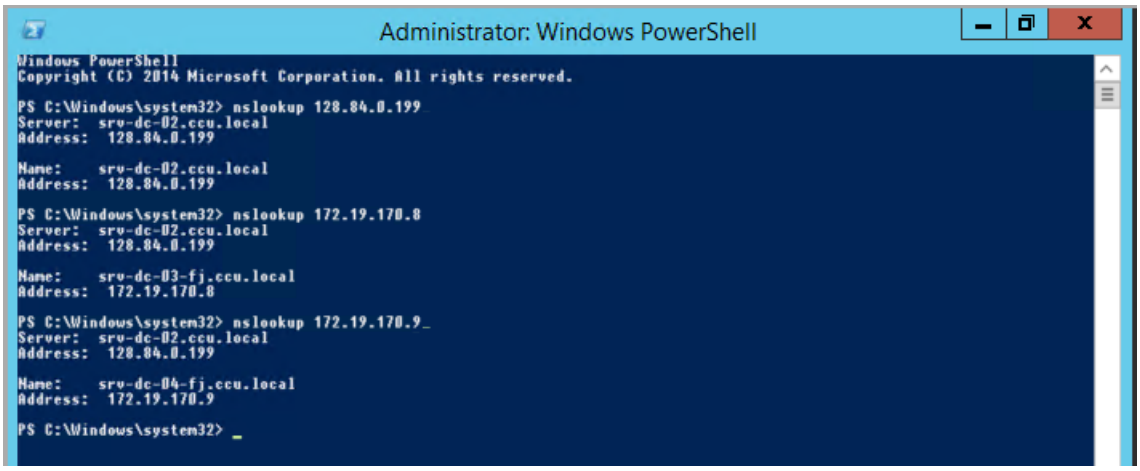
1.0.3.1 DCDIAG /TEST: DNS /e /v



Como se visualiza, todas las máquinas de la arquitectura se encuentran en estado correcto en base a las pruebas realizadas.

1.0.3.2 Reversa

Reversa DNS se encuentra funcional para todos los controladores de dominio de la arquitectura



1.0.4 Roles FSMO

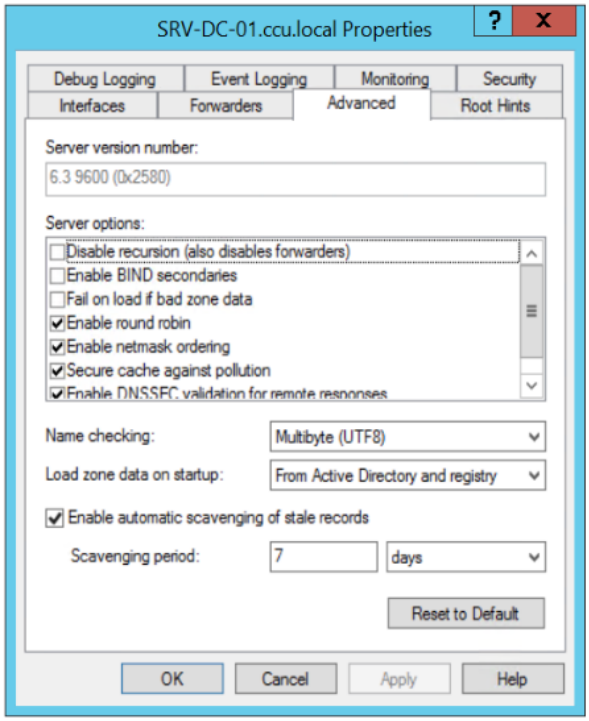
En la evaluación previa se pudo visualizar que los roles FSMO se encontraban en un mismo controlador. Esto tras la remediación ha quedado asignado según las recomendaciones de buenas prácticas.

```
PS C:\Windows\system32> netdom query fsmo
Schema master               SRV-DC-01.ccu.local
Domain naming master        SRV-DC-01.ccu.local
PDC                         SRV-DC-03-FJ.ccu.local
RID pool manager            SRV-DC-03-FJ.ccu.local
Infrastructure master       SRV-DC-03-FJ.ccu.local
The command completed successfully.
```

1.0.5 Bosque DNS Active Directory

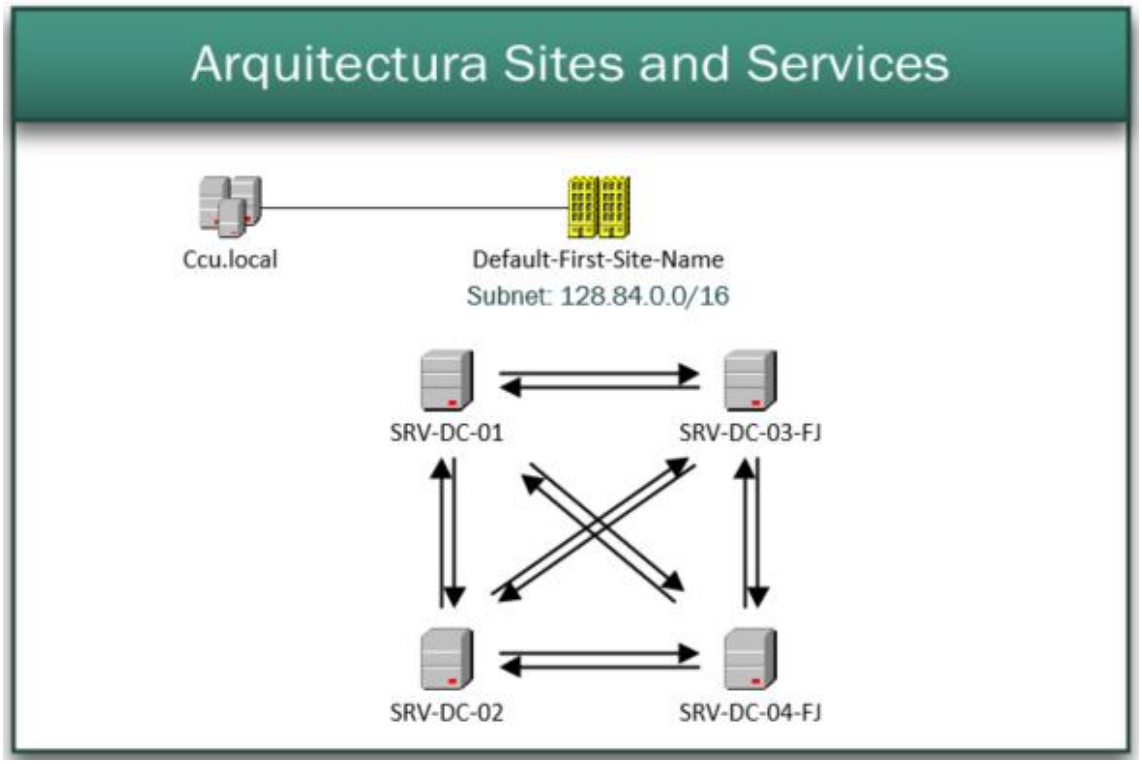
```
PS C:\Windows\system32> dsquery server -o rdn
SRV-DC-01
SRV-DC-02
SRV-DC-04-FJ
SRV-DC-03-FJ
PS C:\Windows\system32> _
```

1.0.6 Validación y deshabilitación de objetos obsoletos



Scavenging queda configurado para ejecutar una evaluación de obsolencias con una frecuencia de 7 días.

1.0.5 Arquitectura Sites and Services



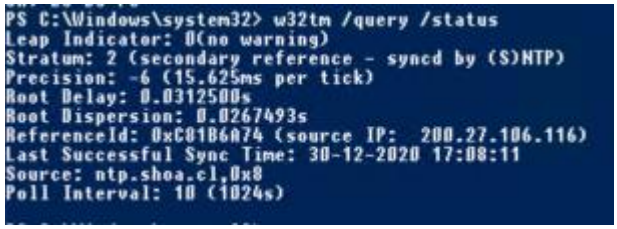
La arquitectura que poseen los servidores de CCU corresponde a enlaces redundantes de replicación. Esto permite una respuesta de alta disponibilidad y no satura los enlaces.

Con respecto a las subnets, los cuatro servidores responden al mismo enlace de asignación y no poseen una separación por site, quedando todos en Default-First-Site-Name

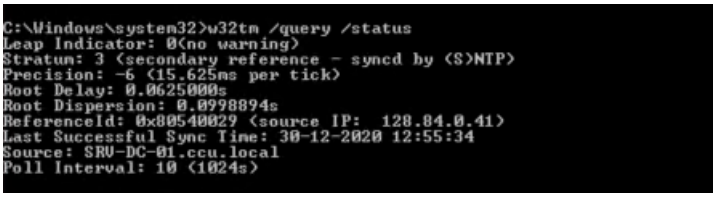
1.0.7 Configuración NTP

El servidor SRV-DC-01 se encuentra apuntando al NTP del SHOA. Y los servidores 02,03 y 04 apuntan por conceptos de buena práctica, al SRV-DC-02. Por lo que están sincronizados correctamente.

Se ha corregido el servicio w32time en SRV-DC-03-FJ Y SRV-DC-04-FJ



Extracto desde SRV-DC-04-FJ



1.0.8 Buenas prácticas

A continuación se dejan recomendaciones y buenas prácticas del entorno Windows Server.

CUENTAS DE USUARIO

- La cuenta Administrador debe usarse sólo para tareas administrativas del servidor tales como inicio y parada de servicios, instalación de software, actualizaciones, reinicios, etc. Para todo lo demás se deben usar cuentas convencionales.
- Los usuarios conectados al servidor que necesiten realizar alguna labor administrativa puntual deberán usar la función “Ejecutar como” del menú contextual para elevar sus privilegios de forma temporal, efectuar el cambio, y continuar trabajando como usuarios con privilegios limitados.
- Las políticas de cambio de contraseñas deben ser observadas de forma estricta, especialmente en cuentas administrativas, para mantener la seguridad en todo momento.
- No se deben crear cuentas de usuario sin contraseña ni cuentas de usuario pertenecientes al grupo Invitados.

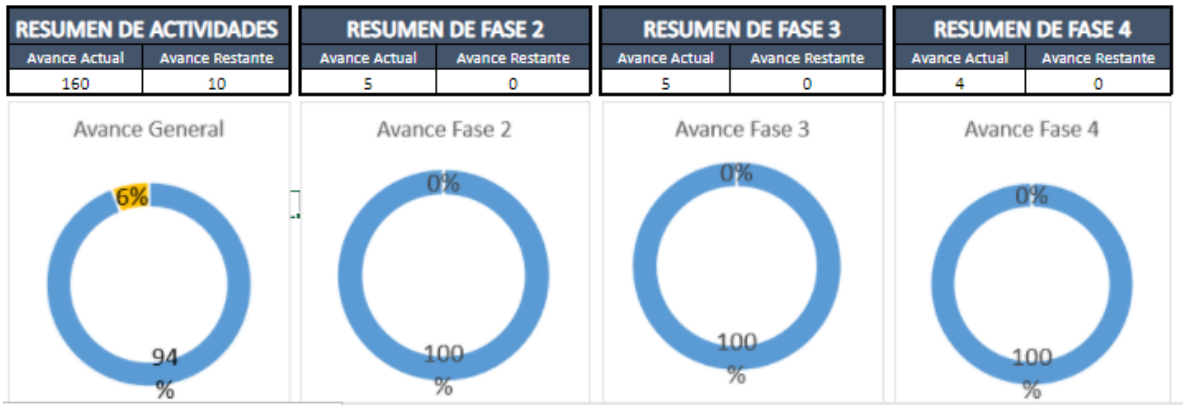
APLICAR PRÁCTICAS SEGURAS ENTRE LOS USUARIOS

- Aplicar una buena política de contraseñas.
- Entrena a los usuarios para que reconozcan los ataques de phishing.
- Evita que los usuarios realicen cambios administrativos en su portátil que puedan comprometer su seguridad.
- Proporciona a los administradores de sistemas dos cuentas. Una será para el uso normal y la otra, una cuenta de administrador para realizar cambios.
- Limita las cuentas administrativas a los sistemas asignados, con redundancias en su lugar, por supuesto. No quieres una sola cuenta de Administrador que pueda abrir todas las ‘puertas’.

1.0.9 Conclusiones y comentarios

Como podemos identificar en las pruebas e información otorgada. Actualmente CCU cuenta con una arquitectura remediada que cumple con las prácticas esperadas y responde de manera eficiente y oportuna los requerimientos que se le han asignado.

A continuación se presenta dashboard de actividades que ha guiado la planificación en este tiempo.



El 6% que se puede distinguir en el dashboard, corresponde a 2 actividades que se indicaron como canceladas por definición CCU.

Robustecer Contraseñas en Dominio	Cumplido	Cancelado por definición CCU
Promoción Contraseñas seguras	Cumplido	Cancelado por definición CCU

Agradeciendo toda su disposición, apoyo y esperando que la experiencia con el equipo a cargo de las actividades haya cumplido las expectativas.

Se procede al cierre del proyecto remediación ADDs