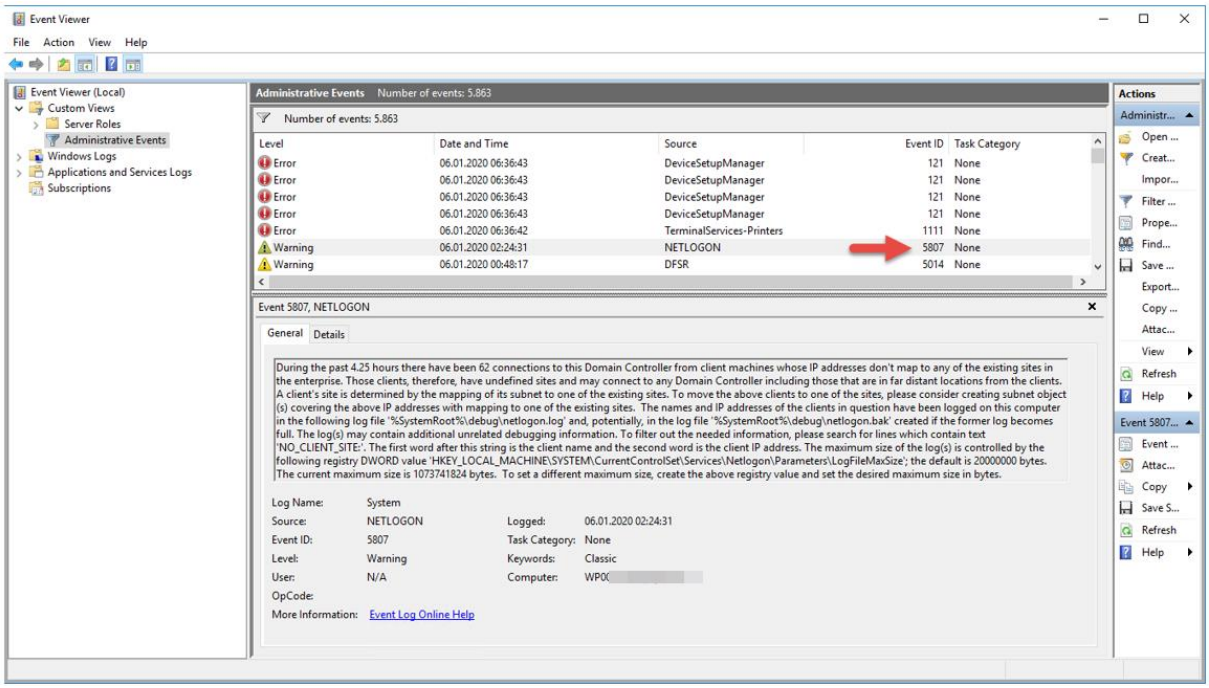
Netlogon Event-ID 5807

Das Problem, welches hieraus entstehen kann ist wie folgt zu erklären.



Bekommt der DC eine Anfrage zur Namensauflösung benötigt er für die Beantwortung Zeit, ganz klar.

Ein Client kann bei einem eingeschaltetem IPv6 Protokoll bis zu 3 IP-Adressen bekommen. Eine IPv6 Private (Link-Local), eine IPv6 Public und eine IPv4 Adresse.

Stellt der Client nun eine Anfrage an den DC versucht der DC (Netlogon), den Client zunächst einem Subnet/Site-Mapping zuzuordnen, das passiert mit dem LDAP-Ping und der übermittelten IP-Adresse des Clients.

Netlogon ist so konzipiert, dass wenn über den LDAP-Ping das Subnet/Site-Mapping nicht bestimmt werden kann, es nochmals mit dem NetBios Namen des Clients versucht wird. Kommt eine Antwort zurück und die IP-Adresse des Clients konnte einem Subnet/Site-Mapping zugeordnet werden ist alles gut.

Wenn dieses Verhalten nun zu Stoßzeiten vermehrt vorkommt, werde andere wichtige LDAP Anfragen verzögert beantwortet. Das Ganze kommt deswegen zu einer Verzögerung, weil der Pool (MaxPoolThreads) von LDAP Anfragen begrenzt ist. Und wenn Netlogon einen weiteren Versuch über den NetBios Namen des Clients startet, wird hier ein Thread aus dem begrenzten LDAP-Pool bis zur Beantwortung blockiert. Anfragen stauen sich auf!

Erstellt von Jörn Walter – 06.01.2020

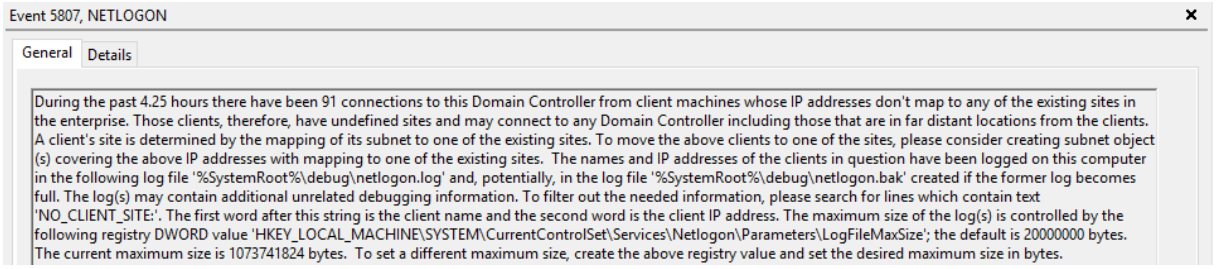
Netlogon Event-ID 5807

Lösung:

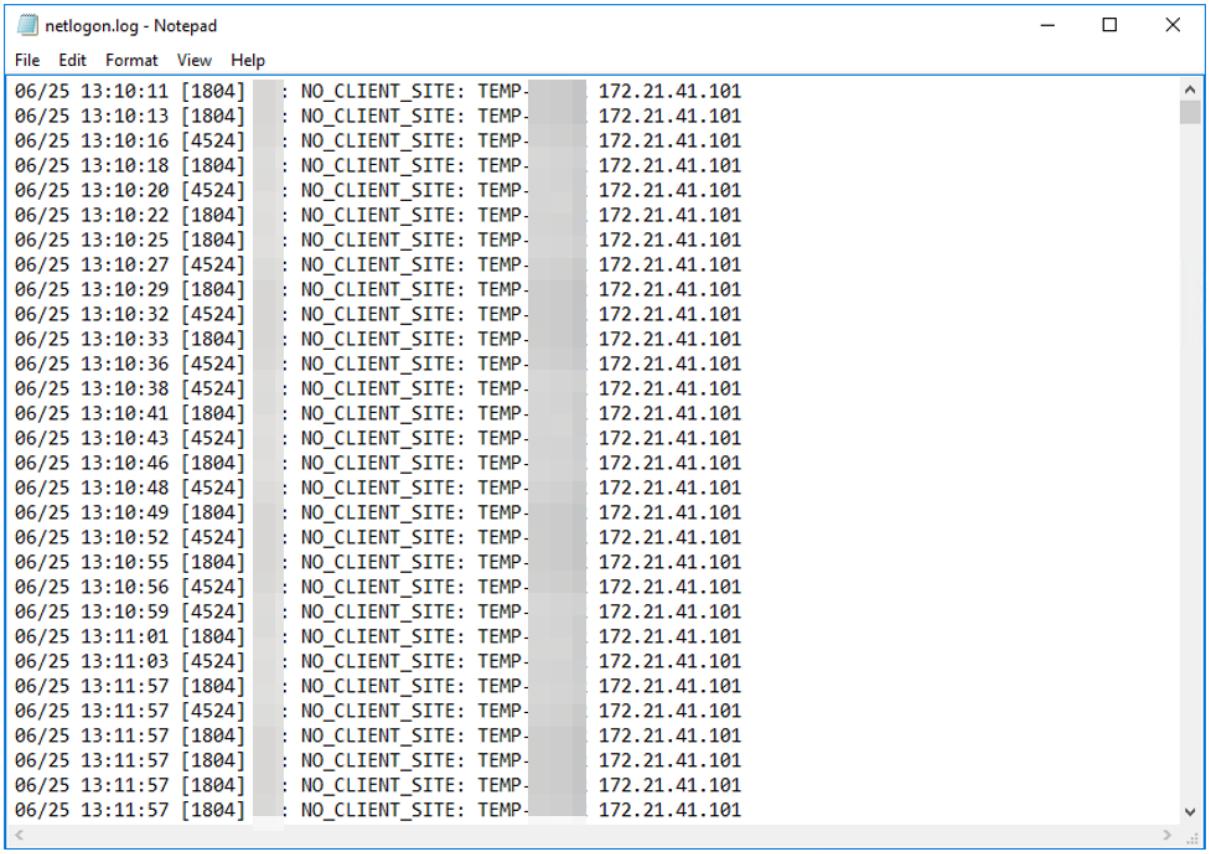
Eine Lösung wäre, die Abschaltung von NetBios over TCP/IP auf der Netzwerkkarte des Clients, um überflüssigen Traffic zu vermeiden.

Die wahre Ursache und Lösung ist:

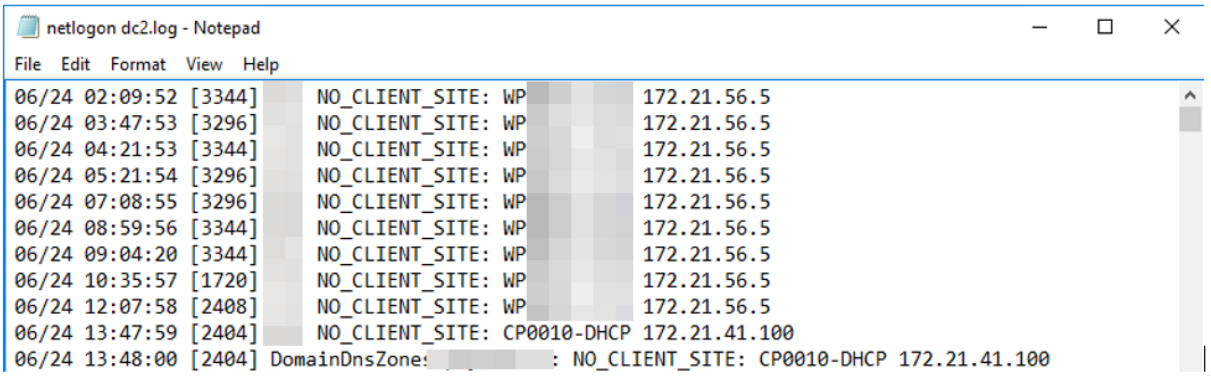
Der Auslöser ist, dass ein IP-Segment keiner Active-Directory-Site zugewiesen wurde. Die Lösung des Problems ergibt sich nun von selbst. 😉



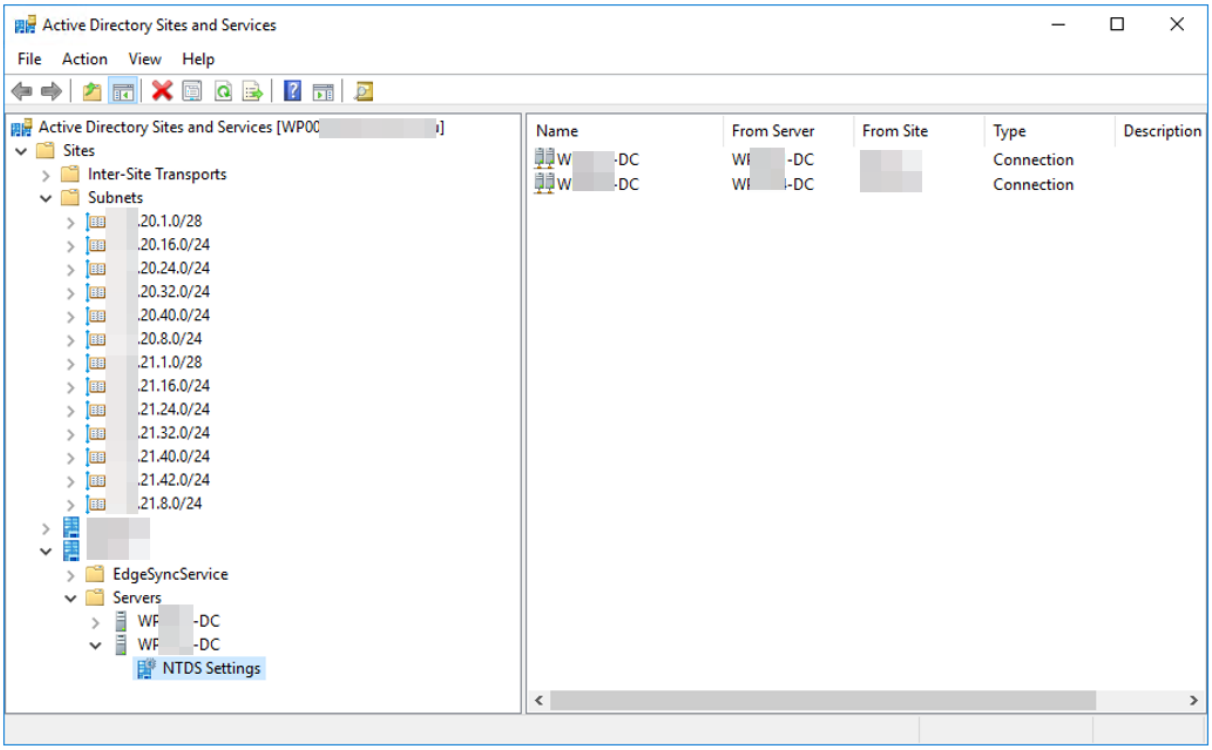
Ein weiterer Blick in das LOG unter %SYSTEMROOT%\Debug\netlogon.log, gibt ganz klar zu erkennen, dass es sich hier um Subnetze handelt die unter Sites & Services nicht angelegt wurde. Bedingt dadurch kann der Client seinen Standort nicht bestimmen.



Netlogon Event-ID 5807



Es fehlen die Subnetze 21 und 41.

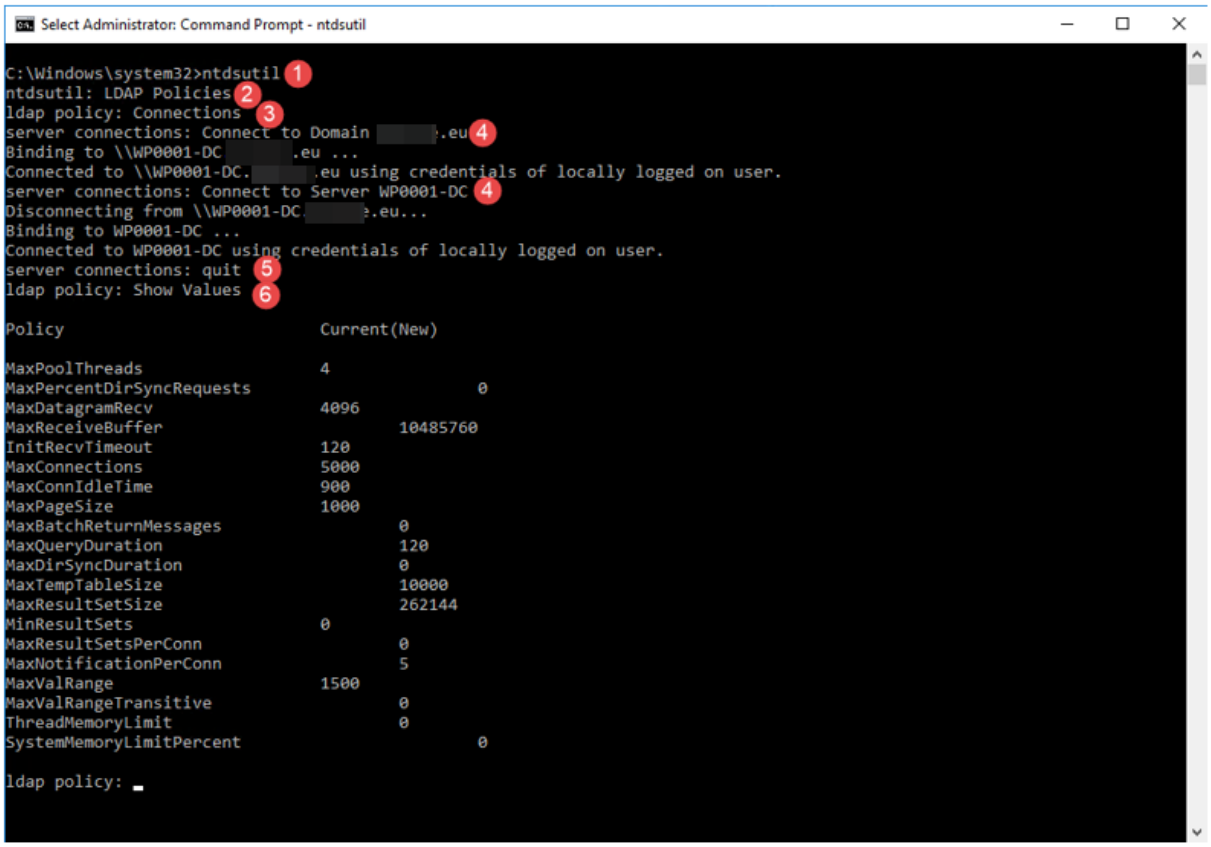


Alternative – Lösung die aber nicht in Betracht gezogen werden sollte, schließlich ist das Problem ja ganz einfach zu lösen.

Anpassung der LDAP Policy:

Pro CPU/Core steht der Wert (default) auf = 4.

1. Ntdsutil
2. LDAP Policies
3. Connections
4. Connect to Domain ndsedv.eu
    - Connect to Server WP0001-DC
5. Quit
6. Show Values



Optional:

Anpassen der LOG-Größe für das netlogon.log:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\LogFileMaxSize

Default ist 20000000 Bytes