SANGFOR

IAM

Panduan Troubleshooting Script SSO

Versi 12.0.18

Perubahan Catatan

Tanggal	Deskripsi Perubahan
2 Desember 2019	Rilis dokument Versi 12.0.18.

Daftar Isi

Bab 1 Troubleshooting

Ringkasang metode Troubleshooting

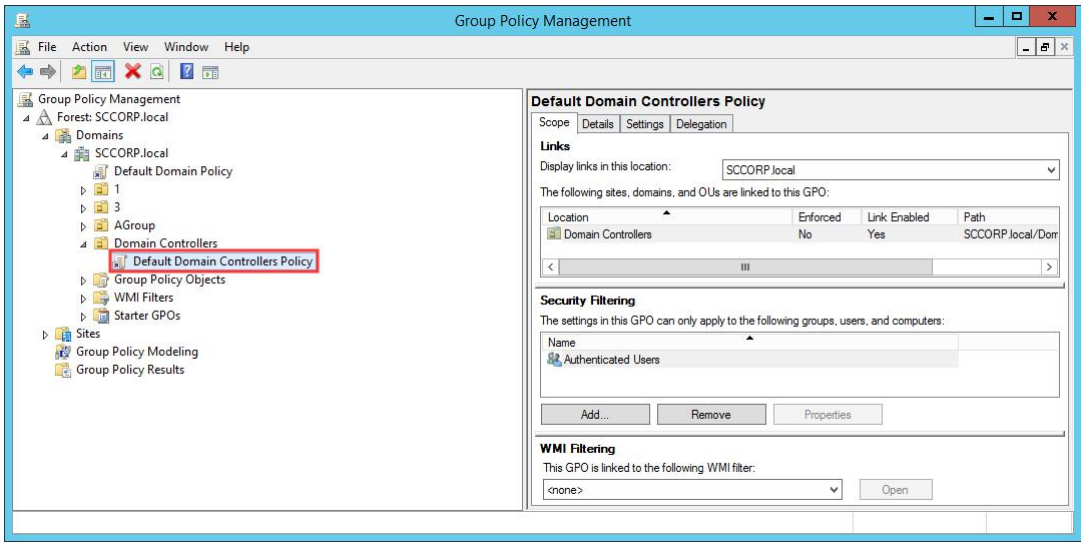
Analisa dari interaksi data dari proses otentikasi

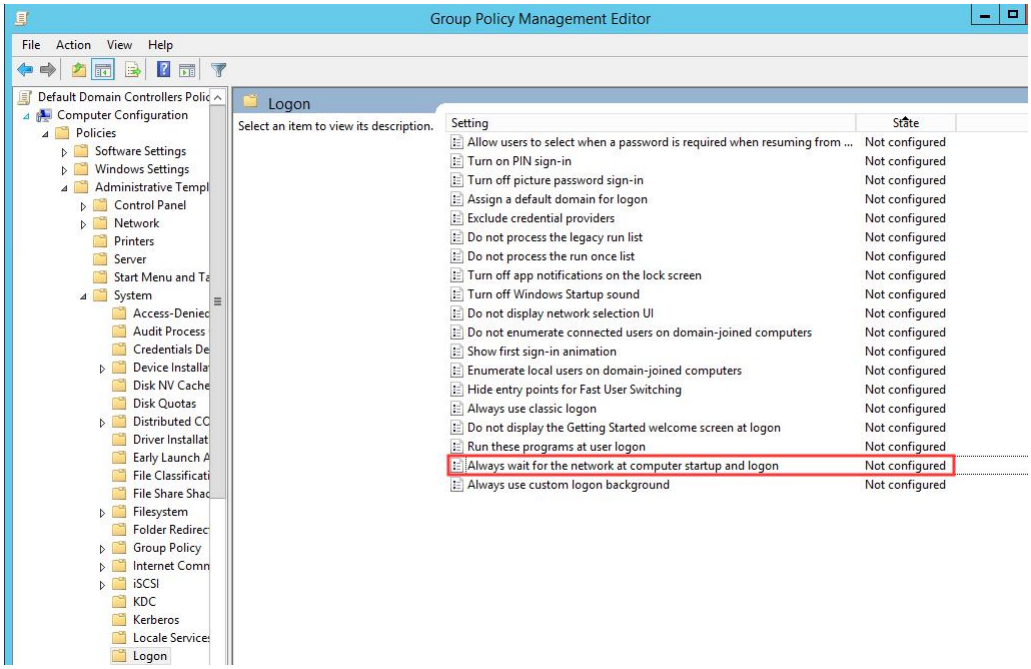
1. PC join Domain.
2. Berhasil bergabung dengan Domain setelah otentikasi domain berhasil.
3. Jalankan logon.exe di PC ketika login.

1 Permintaan PC untuk bergabung dengan Domain

Ketika menggunakan skrip SSO ,Pertama PC itu sendiri harus gabung di dalam domain AD ,dan biasanya tidak mengalamai masalah. Namun, Jika PC bergabung dengan offline domain AD atau PC sudah memiliki koneksi ke jaringan public sebelum bergabung dengan domain AD, single sign-on mungkin akan gagal.

Dalam kasus ini, direkomendasikan untuk menghidupkan domain group policy “Always wait for network when computer starts or logs on.” Gunakan perintah (command) “gpupdate.exe /force” di server domain AD untuk memperbarui group policy.





2 Interaksi antar Data dan PC setelah bergabung dalam Domain

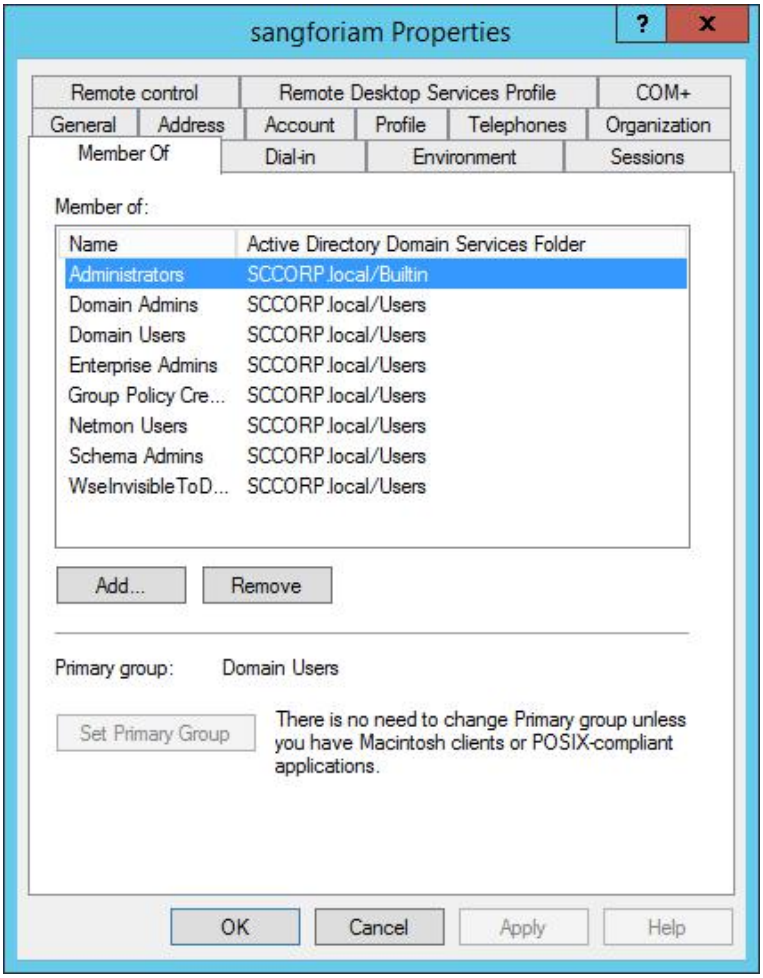
Setelah PC berhasil bergabung dalam domain AD, logon.exe skrip akan dijalankan. Berikut ini adalah beberapa faktor yang dapat membuat proses domain single sing-on gagal:

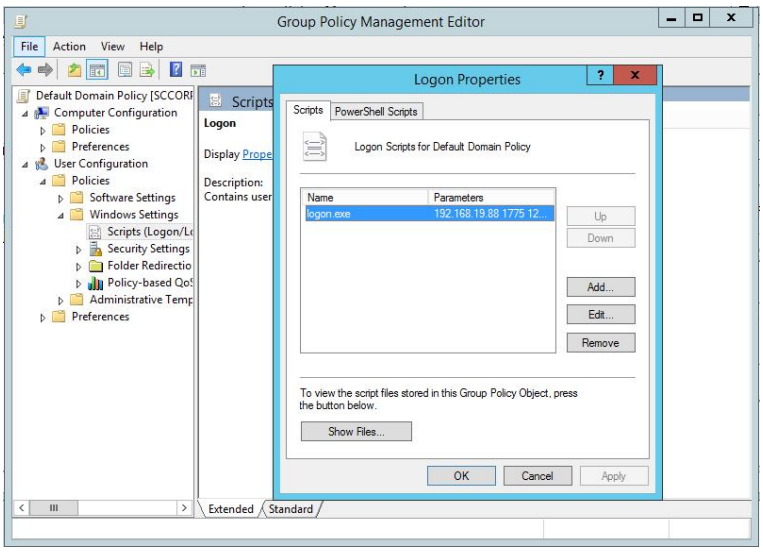
Apakah skrip single sign-on pada server domain AD ditambahkan dan terkonfigurasi secara benar?

Apakah domain group policy telah berhasil didistribusikan ke PC?

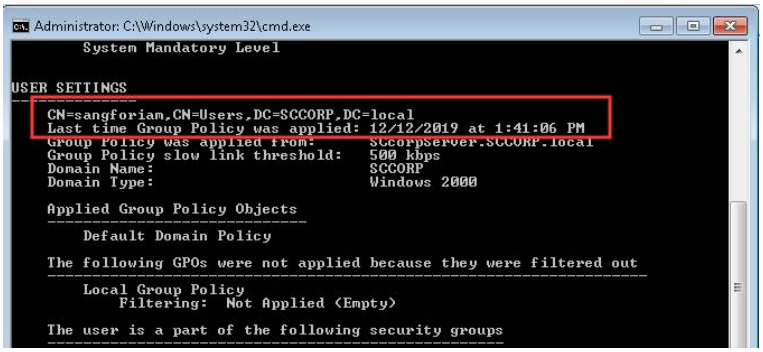
Setelah PC mendapatkan group policy, apakah diotorisasikan untuk menjalankan skrip logon.exe?

1. Periksa pengaturan group policy di server domain, jika ada akun domain yang sesuai, gunakan dsa.msc untuk melihat pengguna (user), dan kemudian lihat pengguna berada di ou yang mana; gunakan gpmc.msc untuk melihat semua domain atau kelompok di dalam satu policy, dan kemudian periksa konfigurasi dasarnya.

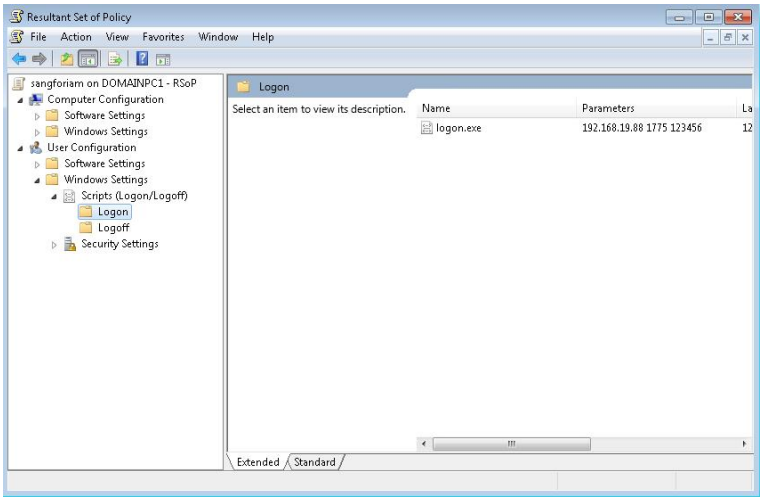




2. Jalankan perintah “gpresult” atau “rsop.msc” di PC uji untuk memeriksa apakah group policy yang dicocokan dengan PC sesuai dengan konfigurasi yang ada di server domain AD. (gpresult ditampilkan di baris perintah (command line), rsop.msc ditampilkan secara grafis)

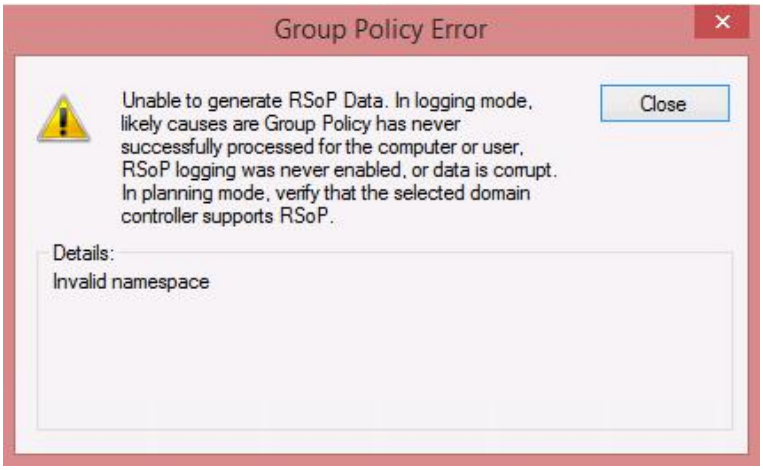


Untuk memastikan apakah domain policy yang sekarang sudah normal, kalian dapat menggunakan perintah rsop untuk mendapatkan domain policy dari domain dalam keadaan normal, seperti yang ditampilkan dibawah ini:

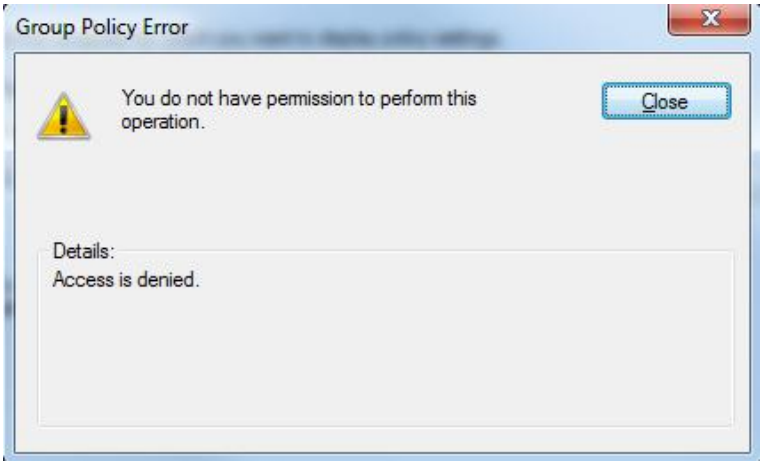


Jikat ada masalah dengan parameter check, kalian perlu untuk memodifikasi parameter seperti IAM IP, default port, dan shared key di skrip login dalam group policy. Shared key dan shared key yang telah terkonfigurasi di IAM harus sesuai.

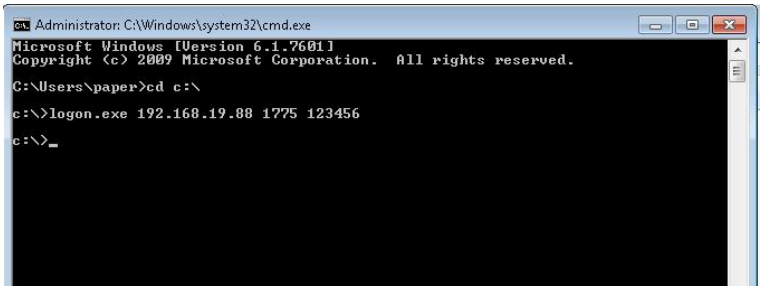
3. Group Policy tidak bisa didapatkan menggunan perintah rsop. Kalian perlu untuk memeriksa apakah group policy hilang.



4. Ketika menggunakan perintah rsop untuk meminta izin yang tidak memadai, kalia perlu untuk menambahkan pengguna domain ke dalam administrator group.



5. Secara manual jalankan skrip logon.exe di PC uji, isi parameter yang relevan, dan periksa apakah eksekusinya berhasil.



3 Jalankan logon.exe di PC

1. Setelah PC berhasil menjalankan logon.exe, akan menghasilkan file log logon.txt (execute %appdata%/.logon) di direktori bersama dari dive C PC (C: \ Documents and Settings \), dan melaporkan berhasil login domain ke perangkat IAM (UDP1775).

Paramater kesalahan log yang biasanya sesuai :

Reply: 401 magic error Shared Key error

reply: 402 Invalid ip IP or source IP is AC's IP

reply: 403 The user login on other ip IAM

reply: 404 The user is disabled reply: 405 The user is expired

reply: 407 Dkey use The current user is a Dkey user

reply: 408 bind ip error The IP / MAC of the logged-in PC is bound by another user

reply: 500 Service stopped authd

reply: 500 (user, ip) is exis

reply: 501 Not allow new user

reply: IP or mac not in restrict range

Selama proses ini, berikut adalah faktor-faktor yang dapat menyebakan single sign-on domain gagal:

Akun domain yang digunakan oleh PC untuk masuk ke domain tidak mempunyai izin untuk merubah/menulis di direktori bersama drive C

IP single sign-on, port, dan kunci IAM yang ditetapkan oleh domain group policy.

PC dan IAM itu sendiri tidak dapat saling berkomunikasi.

Berdasarkan dari faktor-faktory yang diatas yang dapat membuat SSO gagal, pemeriksaan yang perlu kita lakukan adalah sebagai berikut :

1) Periksa akun domain apakah telah memiliki izin untuk merubah/menulis ke direktori bersama drive C. Kalian dapat secara manual membuat verifikasi file di dalam direktori bersama drive C.

2) Periksa apakah file logon.exe dibuat di %appdata%

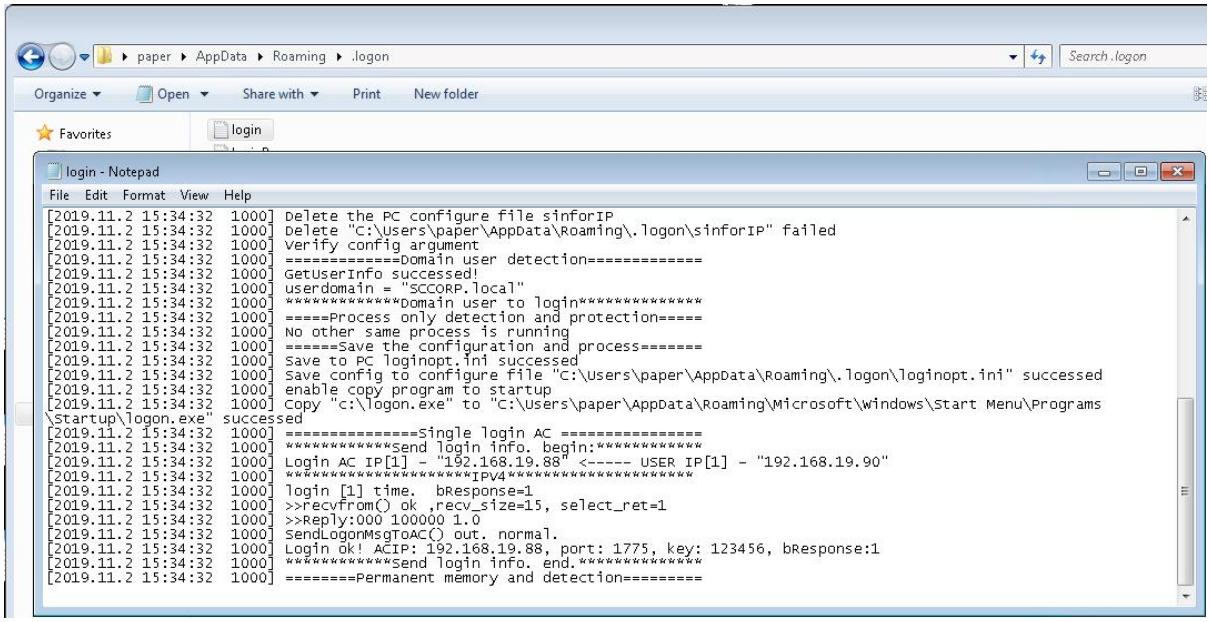
   Jika kalian mempunyai izin read-write tetapi tidak dengan file logon.txt yang dihasilkan, kalian perlu memeriksa apakah Firewal Lokal PC atau perangkat lunak anti-virus melindungi dan mencegah file log untuk diubah. Kalian dapat mematikan perangkat lunak anti-virus dan firewall lokal, kemudian login ke dalam domain untuk melihat apakah file logon.txt telah dihasilkan/dibuat.

   Jika file logon.txt berhasil dibuat dan single sign-on domain tidak berhasil, kalian dapat memeriksa isi-isi dari file logon.txt untuk melihat jika single sign-on tidak berhasil karena masalah konfigurasi, atau PC mengirimkan permintaan ke IAM tanpa adanya tanggapan.

3) Jika file logon.txt menampilkan PC mengirimkan pesan bahwa domain itu berhasil login ke IAM, tetapi IAM tidak merespon, kalian perlu melakukan cek apakah komunikasi antara PC dan IAM normal dan apakah perankat jaringan lainnya mengganggu paket data. Cara yang paling ampuhnya adalah dengan mengambil pake di IAM dan lihat jika perangkat dapat menerima paket data single sign-on yang dikirim dari PC.

4) Dalam satu lingkungan Intranet, beberapa PC berhasil melakukan single sign-on dan beberapa PC tidak berhasil, kalian dapat langsung meletakkan skrip login logon.exe secara lokal di computer yang gagal melakukan login, megambil contoh dari drive C, jalankan di cmd : c:\ logon.exe IAM's ip port key; jika harsil test berhasil, jaringan antara PC dan IAM berjalan normal.

2. Buka direktori %appdata% secara manual, periksa login di file logon, dan lihat waktu proses terkini.



Log kesalahan yang biasa terjadi dijelaskan dibawah ini:

Error Code	Sebab
=ERR: Wrong number of parameters.=	Logon.exe menggunakan metode baris perintah, dan jumlah parameter melebihi jumlah maksimum parameter

=ERR: can not get the module path=	Gagal untuk mendapatkan jalur yang benar logon.exe
=ERR: bad param format=	Parameter yang ditambahkan setelah logon.exe hilang/kurang
=ERR: can not get the startup path or module path, Errorcode:	Biasanya karena pengguna domain login untuk pertama kalinya, direktori lingkup pengguna belum siap, dan direktori *startup* tidak dapat ditemukan
=ERR: can not get the PC sinforIP path=	Gagal untuk mendapatkan file konfigurasi *sinforIP path*
=ERR: can not get the domain sinforIP or PC sinforIP path=	Gagal untuk mendapatkan alamat dari file konfigurasi SinforIP dalam domain maupun PC lokal
=ERR: can not get the loginopt.ini path=	Gagal untuk mendapatkan *loginopt.ini path,* mengindikasikan bahwa baris perintah logon.exe sedang offile untuk mode jalankan
=ERR: Can not load	Gagak memuat file konfigurasi
=ERR: %s - %d= %s represents the parameter, and %d represents the error code, which is generally 87, indicating that the parameter is illegal.	Parameter ilegal, perlu memeriksa validitas dari parameter
=ERR: %s - %d, use default value %d=	Gagal mendapatkan parameter, menggunakan value bawaan (default value)
=ERR: prepare data failed, ERR_Line:	Gagal mendapatkan IP IAM dan IP lokal
=ERR: Login Failed! ACIP: %s, port: %d, key: %s, bResponse:%d=	Gagal login
=ERR: Encrypt message failed, ret:	Gagal untuk mengenkapsulasi data yang dikirim (login atau lout atau *heartbeat*)
=ERR: Send heart beat to AC \"%s\" failed: %d=	Gagal untuk mengirimkan paket *heartbeat*
=ERR: >>Login Failed! port: %d, key: %s=	Gagal untuk mengirimkan paket login
=ERR: >>Logoff failed: %d=	Gagal untuk mengirimkan pake logout
=ERR: SockInit() failed:	Gagal untuk menginisialisasikan *socket*
=ERR: Timeout=	Tidak ada paket balasan yang diterima, IP yang dikirimkan oleh IAM mungkin tidak ada, dan *Firewall* mungkin dihidupkan di win7
=ERR: CreateDirectoryW failed:	Gagal utuk membuat direktori log
=ERR: CryptQueryObject failed:	Gagal untuk mendapatkan *digintal signature.* Dalam kasus ini, hidupkan deteksi *digital signature* di logon.exe
=ERR: CertFindCertificateInStore failed:	Gagal untuk mendapatkan *signing certificate.* Untuk kasus ini, hidupkan deteksi *digital signature* di logon.exe
=ERR: CreateThread for IP detection failed:	Deteksi berkas perubahan IP gagal
=ERR: to OpenProcess %d terminate: %d=	Kesalahan sistem, silahkan login ulang

=ERR: to terminate process:	Gagal untuk mematikan proses yang spesifik
=ERR: OpenProcessToken failed:	Gagal untuk membuka *token handle* ketika sedang mendapatkan informasi pengguna
=ERR: GetTokenInformation failed: or=ERR: LookupAccountSid failed: or=ERR: GetTokenInformation failed: or=ERR: GetUserName failed:	Gagal untuk membuka *token handle* ketika sedang mendapatkan informasi pengguna

BAB 2 Masalah yang Biasa Terjadi

2.1 Pengguna-pengguna sesekali Online dan Offline di IAM

1. Jaringan antara PC dan IAM tidak stabill

   Langkah-langkah pemecahan masalah

   Buka console di IAM dan masukan ping X.X.X.X –t (X.X.X.X adalah IP dari IAM)

   Jika terjadi packet loss, implementasikan solusinya

   Solusi :

   Kurangi repetisi interval login (tergantung dari situasi, pada dasarnya masalah ini tida dapat diselesaikan, ini hanya dapat mengurangi probabilitas kejadian)

2. Waktu habis IAM tanpa lalu lintas waktu logout lebih sedikit dari waktu repitisi siklus waktu login.

   Langkah-langkah pemecahan masalah

   Melihat periode batas waktu habis dari IAM a tanpa logout

   Melihat siklus login berulang b pada file konfigurasi logon

   Solusi

   Modifikasi timeout of no timeout ke poin yang lebih besar untuk membuat periode login repetisi atau close the timeout of no timeout menjadi lebih lama

2.2 Pengguna Domain dalam posisi Online tetapi tidak bisa akses Internet

1. IAM tidak dapat terkoneksi ke Internet

   Langkah-langkah Pemecahan masalah

   Pertama periksa apakah tidak hanya pada IAM. Buka pass-through pada IAM. Jika kamu online, lanjut ke langkah berikutnya.

   Masukkan IAM background melalui background

   Jalankan perintah ping, ping 8.8.8.8 atau ping www.google.com, jika ping gagal, terapkan solusinya

   Solusi

   Menyelesaikan Masalah Jaringan IAM

2. Pengguna atau grup tertentu tidak dapat tersambung ke Internet di dalam kebijakan Internet IAM

   Langkah-langkah Pemecahan Masalah

   Pertama periksa apakah tidak hanya pada IAM. Buka pass-through pada IAM. Jika kamu online, lanjut ke langkah berikutnya.

   Periksa strategi Internet akses IAM dan periksa apakah kebijakan pembatasan akses internet ada pengguna yang gagal untuk mengakses internet

   Solusi

   Modifikasi Manajemen Kontrol Akses (Access Control Management)

3. IP Pengguna yang Online tidak menggunakan IP komunkasi

Langkah-langkah Pemecahan Masalah

Periksa apakah IP Pengguna yang online dan IP IAM tidak sama dalam satu segmen jaringan

Logon memperbolehkan banyak IP untuk Online, dan IAM dikonfigurasi untuk melakukan log off IP lama ketika otentikasi konflik

Setelah kedua kondisi diatas bertemu, implementasi solusi

Solusi

Metode Modifikasi 1: Konfigurasi Logon hanya memperbolehkan satu IP yang dapat Online

Metode Modifikasi 2: Konfigurasi IAM untuk tidak melakukan Log off kepada IP lama ketika otentikasi konflik

2.3 Pengguna Domain tidak onlie di IAM tetapi proses logon sedang jalan di PC

1. PC dan IAM tidak bisa terkoneksi secara langsung

   Langkah-langkah Pemcehan Masalah

   Ping ke IAM dari PC, jika ping gagal, terapkan solusi berikut

   Solusi:

   Bisa saja bahwa IAM menonakftifkan fungsi DNS pengguna. Di antarmuka IAM, aktifkan akses ke layanan DNS.

   Buat PC mempunyai IP yang sama dengan IAM dalam satu segmen jaringan, dan gateway yang dikonfigurasi adalah IP IAM.

2. File Konfigurasi mengalami kesalahan

   Langkah-langkah Pemechan Masalah

   Periksa informasi file konfigurasi. Periksa apakah IP IAM dan IP DNS cocok dengan yang sebenarnya. Jika tidak, implementasikan solusi berikut

   Solusi:

   Metode Modifikasi 1: Ganti / tulis IP sebenarnya IAM dan IP DNS

   Metode Modifikasi 2: Kembali ke file konfigurasi lagi dan hilangkan ruang yang lebih

   Metode Modifikasi 3: ulangi konfigurasi dan deploy file konfigurasi awal (default) berdasarkan dari konfigurasi yang diinginkan

3. Logon terbaru tidak berhasil di deploy dan sinforIP yang baru tidak berpengaruh.

   Langkah-langkah Pemecahan masalah

   Bandingkan sinforIP di dalam Domain, sinforIP lokal dan backup terakhir file konfigurasi loginopt.ini. Jika ada perbedaan, terapkan solusi berikut.

   Solusi:

   Bandingkan sinforIP di dalam Domain, sinforIP lokal dan backup terakhir file konfigurasi loginopt.ini. Jika ada perbedaan, terapkan solusi berikut.

   Aktifkan fungsi repetisi login di konfigurasi logon. Atur login repetisi menjadi sekecil mungkin.