SANGFOR

IAG

Konfigurasi Endpoint Visibility

Versi 13.0.15

Catatan Perubahan

Tanggal	Deskripsi Perubahan
25 Spetember 2020	Rilis Versi 13.0.15

DAFTAR ISI

Bab 1 Latar Belakang Persyaratan Endpoint Visibility.....1
Bab 2 Deskripsi Fungsi Endpoint visibility 1
Bab 2.1 Panduan Konfigurasi 2
Bab 2.1.1 Hasil Identifikasi Endpoint.....3
Bab 2.1.2 Pengaruh dari rentang IP 4
Pencegahan: 5

Bab 1 Latar Belakang Persyaratan Endpoint Visibility

Administrator jaringan tidak dapat melihat jaringan internal perangkat keras , termasuk endpoint, server dan perangkat jaringan lainnya, sehingga perangkat yang tidak diketahui tidak dapat dikendalikan dan akan membawa risiko keamanan ke jaringan internal. Jika administrator jaringan tidak mengetahui penggunaan IP, mengakibatkan pemborosan sumber daya IP.

Pada saat yang sama menyebabkan kesulitan dalam manajemen dan operasi.

Visibilitas endpoint: mendeteksi secara otomatis jenis endpoint, sistem, dan informasi terkait dan penyortiran otomatis.

Bab 2 Deskripsi Fungsi Endpoint visibility

Visibilitas endpoint: mendeteksi secara otomatis jenis endpoint, sistem, dan informasi terkait dan penyortiran otomatis.

Ada dua cara untuk mewujudkan fungsi identifikasi terminal: aktif dan pasif.

1. Proaktif adalah untuk memperluas mekanisme deteksi yang dikembangkan melalui kerangka nmap, terutama sebagai berikut:

onvif: protokol standar kamera, mendeteksi dan mengidentifikasi jenis perangkat dumb terminal lainnya;

Deteksi SMB: terutama untuk MSFT PC, yang dapat memperoleh informasi seperti nama host, sistem operasi, dan kelompok kerja host

SNMP: Peralatan yang tersedia: tabel routing, tabel arp, jenis mesin, deskripsi sistem, identifikasi mac address sistem operasi;

2. Secara pasif mengidentifikasi informasi terminal dengan mengidentifikasi field UA dalam lalu lintas http dan bidang opsi dalam data DHCP;

Mode aktif adalah memindai segmen IP mana yang dikonfigurasi, dan mode pasif memerlukan lalu lintas untuk melewati AC

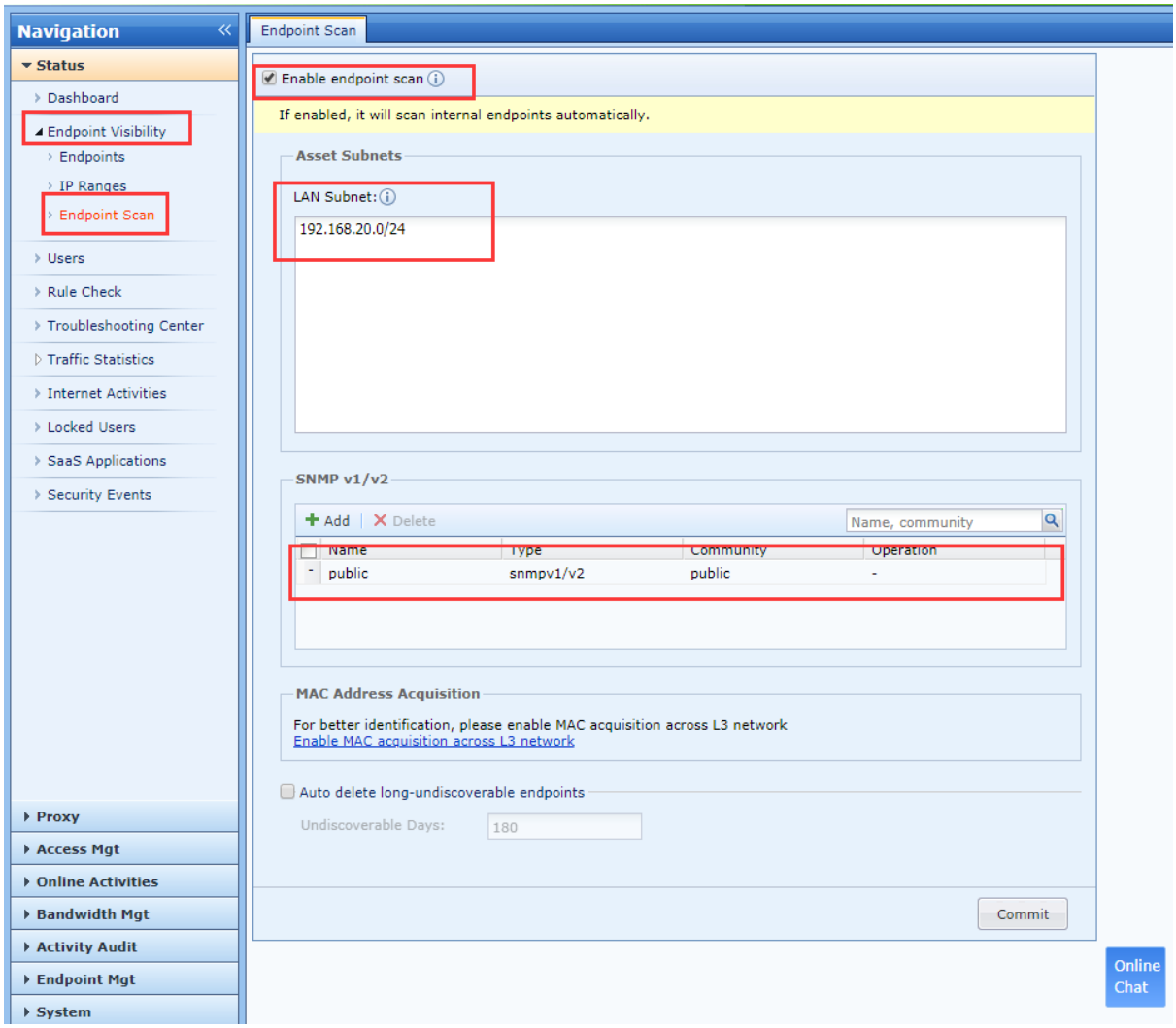
Untuk mengidentifikasi MAC secara akurat di perangkat L3 , Anda perlu mengaktifkan **MAC acquisition across L3 network**.

Mekanisme presentasi IP segment di dalam IP management

1. Dalam daftar segmen IP, segmen jaringan mask 24-bit di mana IP berada hanya akan ditampilkan ketika ada IP yang masih hidup, atau ketika diakui bahwa IP memiliki lalu lintas (IP ada pada pengguna online atau ditampilkan pada pengguna yang gagal mengakses jaringan selama 7 hari) Segmen jaringan dari mask 24-bit di mana IP berada juga akan ditampilkan;

Bab 2.1 Panduan Konfigurasi

1. Navigasi ke Endpoint visibility -> Endpoint scan dan aktifkan fungsi endpoint scan.
2. Konfigurasikan segmen jaringan yang diperlukan untuk scan.
3. Untuk meningkatkan identifikasi, diperlukan untuk mengaktifkan switch dan mengaktifkan fungsi SNMP dan mengatur community string.
4. Jika diperlukan untuk mengaktifkan mac address di L3, perlu untuk mengaktifkan fungsi **MAC acquisition across L3 network**

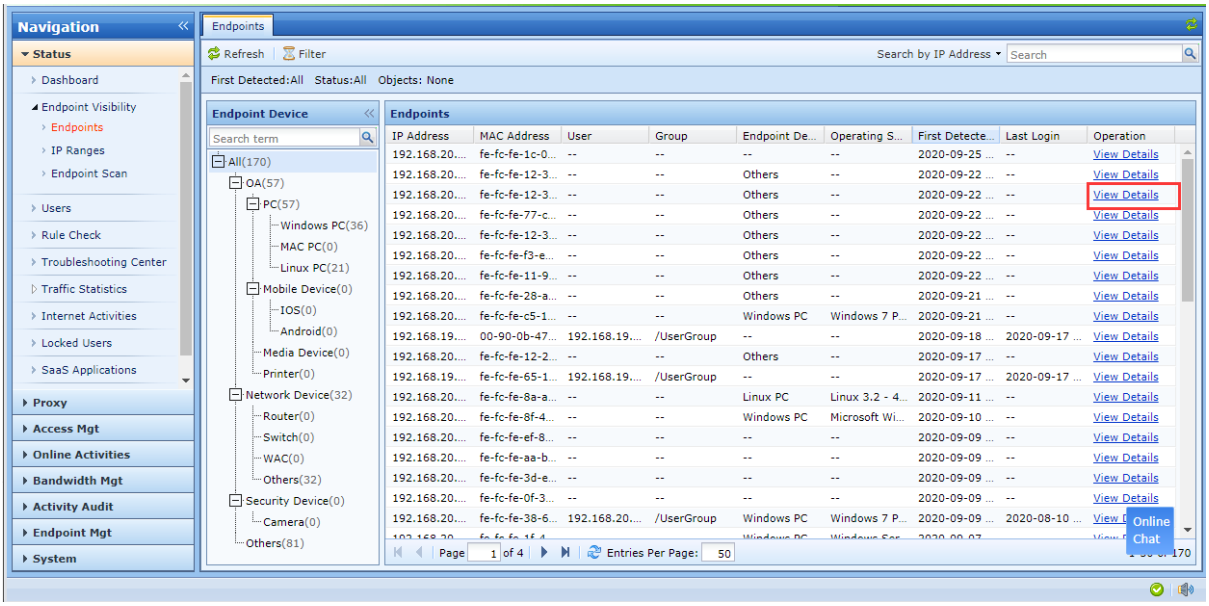


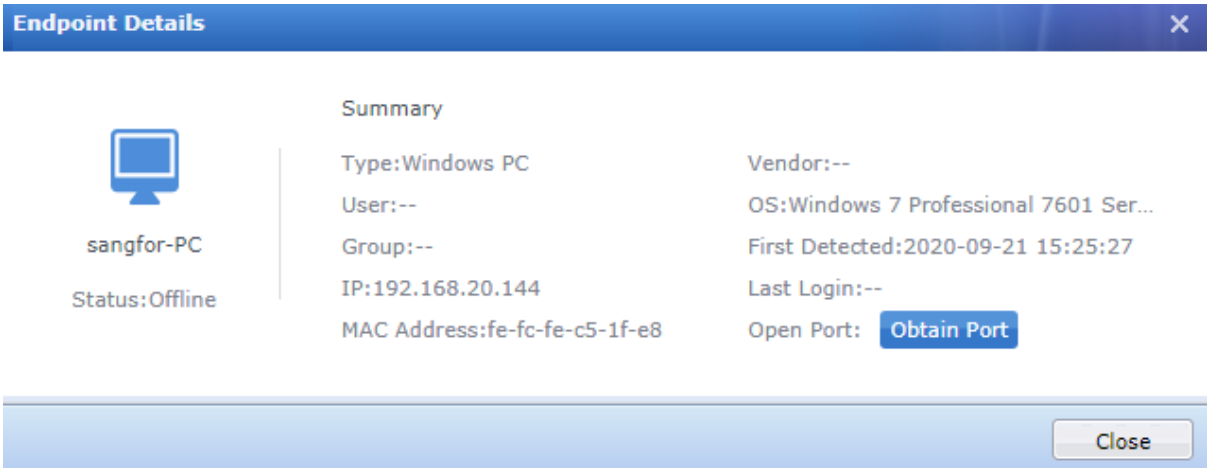
Bab 2.1.1 Hasil Identifikasi Endpoint

Didalam daftar endpoint, anda dapat melihat tipe endpoint, anda dapat meng-klik pada detail untuk melihat deskripsi.

1. Endpoint umum dan beberapa network equipment akan menampilkan nama;

2. Status Online: Online mengacu pada apakah ada endpoint IP pada informasi pengguna online. Kehadiran IP menunjukkan bahwa pengguna telah menggunakan terminal untuk online, dan informasi pengguna dan status grup akan ditampilkan. Offline berarti bahwa IP endpoint saat ini tidak digunakan oleh pengguna.





Bab 2.1.2 Pengaruh dari rentang IP

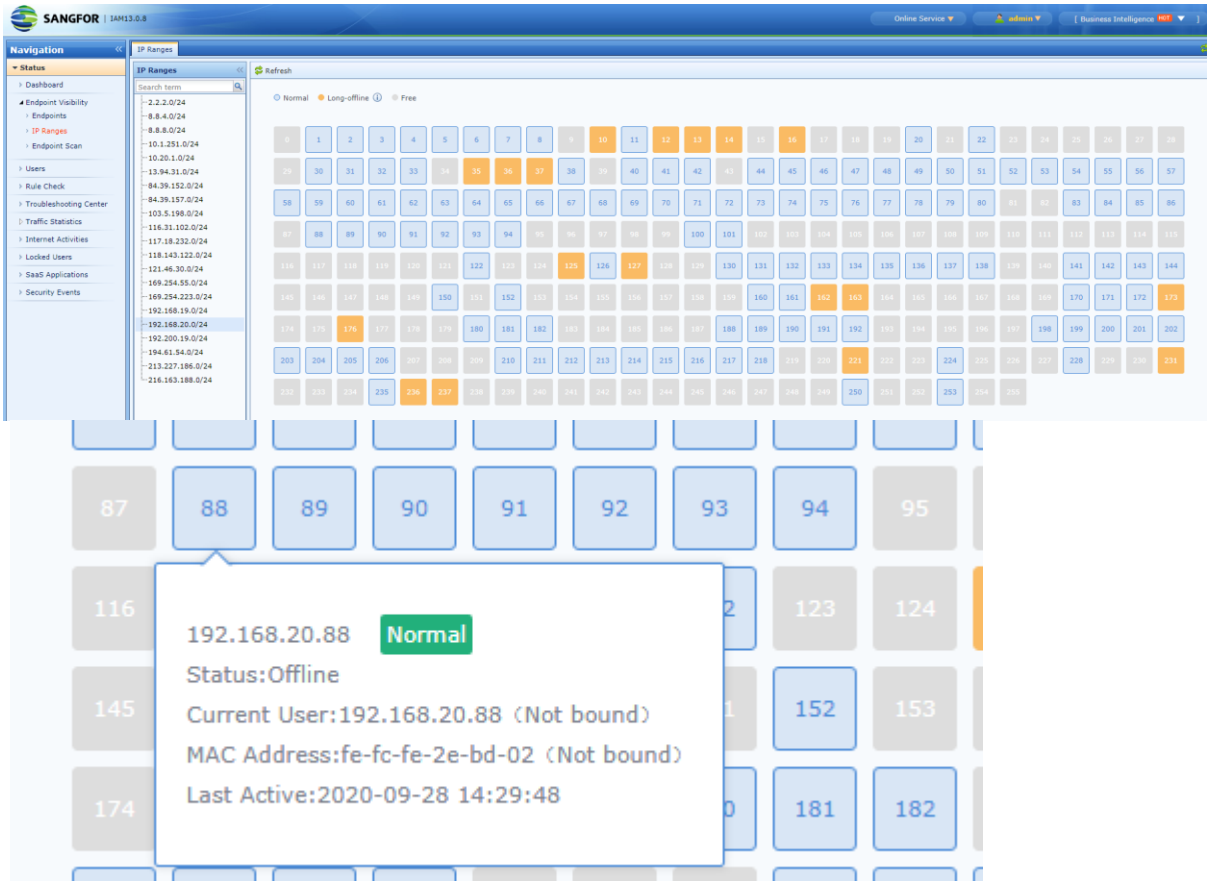
Navigasi ke rentang IP,

Klik pada segmen jaringan untuk melihat penggunaan alamat segmen IP saat ini, klik pada kotak untuk melihat penggunaan terperinci.

Penggunaan Normal : mengacu pada jangka waktu tertentu (umumnya adalah 30 hari, dapat dikonfigurasi) untuk scan IP yang active, stastus online sama dengan bab sebelumnya.

Free: mengacu pada IP yang tidak digunakan.

Long offline: mengacu pada IP yang telah di scan aktif sebelumnya, dan didefinisikan sebagai offline jika tidak discan dalam jangka waktu tertentu (umumnya adalah 30 hari, dapat dikonfigurasi).



Pencegahan:

1. Daftar identifikasi endpoint hanya mendukung untuk menampilkan maksimal 200, 000 IP address.
2. IAM akan secara aktif meng-scan Local network, Jika tidak ada firewall exists di environment. Hal ini akan mempengaruhi hasil identifikasi, juga perlu memastikan pelanggan bisa untuk melakukan pemindaian endpoint di dalam environment.
3. Rentang IP mendukung 1024 IP segments.
4. Pada L3 environment, diperlukan untuk mengaktifkan mac address di L3 environment, diperlukan untuk mengaktifkan MAC acquisition diseluruh fungsi jaringan L3.
5. Tipe endpoint di pengguna online tidak terkait dengan informasi sistem operasi di endpoints seluruh jaringan, dua modul independen.
6. Fungsi scan endpoint dari seluruh jaringan diaktifkan. Jika arp protection diaktifkan pada saat yang bersamaan, modul arp protection module akan terus berbunyi;