AMIYA

AMIYA Global Partner

cloudtech

PT. AWAN TEKNOLOGI GLOBAL

www.cloudtech.co.id

サーバアクセスログ SMASH (ALog)

Operational Monitoring on Server Access

PENDAHULUAN

Saat ini setiap perusahaan pasti memiliki informasi digital penting yang harus dijaga. Menjaga informasi penting agar tidak bocor merupakan prioritas tinggi keamanan.

Memonitor dan membatasi penggunaan PC, Printer, USB, pengiriman email, dan semua perangkat yang ada untuk mencegah terjadinya kebocoran adalah tindakan yang efektif. Termasuk di dalamnya melakukan monitor pada setiap aktifitas yang dilakukan oleh karyawan, untuk mendeteksi setiap perbuatan jahat. Namun itu semua akan membutuhkan usaha dan biaya sumber daya yang sangat besar, termasuk ketidaknyamanan yang dirasakan oleh karyawan karena terus dimonitor. Dengan menggunakan solusi ALog SMASH, monitoring akan fokus pada server dimana data penting tersebut disimpan, ini akan sangat efisien dibandingkan memonitor dan mengontrol setiap PC dan perangkat lainnya.

Ketika terjadi incident, memiliki dan dapat menganalisa dengan baik log sangat membantu penanganan incident, pertama ini akan bisa dijadikan bukti dan kedua juga dapat menghindari kejahatan lebih lanjut. Oleh karena itu dibutuhkan sebuah solusi yang dapat mengelola dan membantu menganalisa log dengan baik. ALog SMASH adalah jawabannya.

Selain manfaat di atas, ALog SMASH juga dapat memberikan peringatan jika ada indikasi kejahatan melalui fitur alert yang dimilikinya.

ALOG SMASH

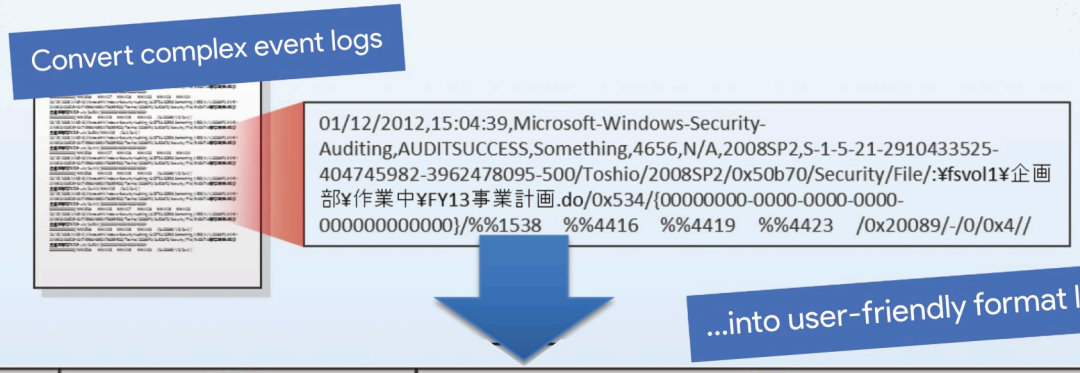
ALog SMASH merupakan varian standalone dari produk ALog ConVerter. ALog SMASH dapat langsung diinstal pada server yang akan dimonitor dan bekerja sebagaimana service. Jadi, ALog SMASH tidak membutuhkan dedicated server khusus untuk bekerja.

ALog SMASH adalah aplikasi yang berfungsi untuk mengumpulkan, menganalisa, dan mengkonversi logs yang rumit menjadi logs operasi yang mudah dibaca oleh siapapun untuk keperluan pencarian dan pelaporan.

Keuntungan menggunakan ALog SMASH adalah:

- Dapat memonitor setiap aktivitas akses ke data penting yang ada di server
- Mudah dan akurat membaca hasil konversi lognya
- Hasil konversi berukuran sangat kecil
- Instalasi yang mudah
- Tidak membutuhkan dedicated server

KONVERSI LOG



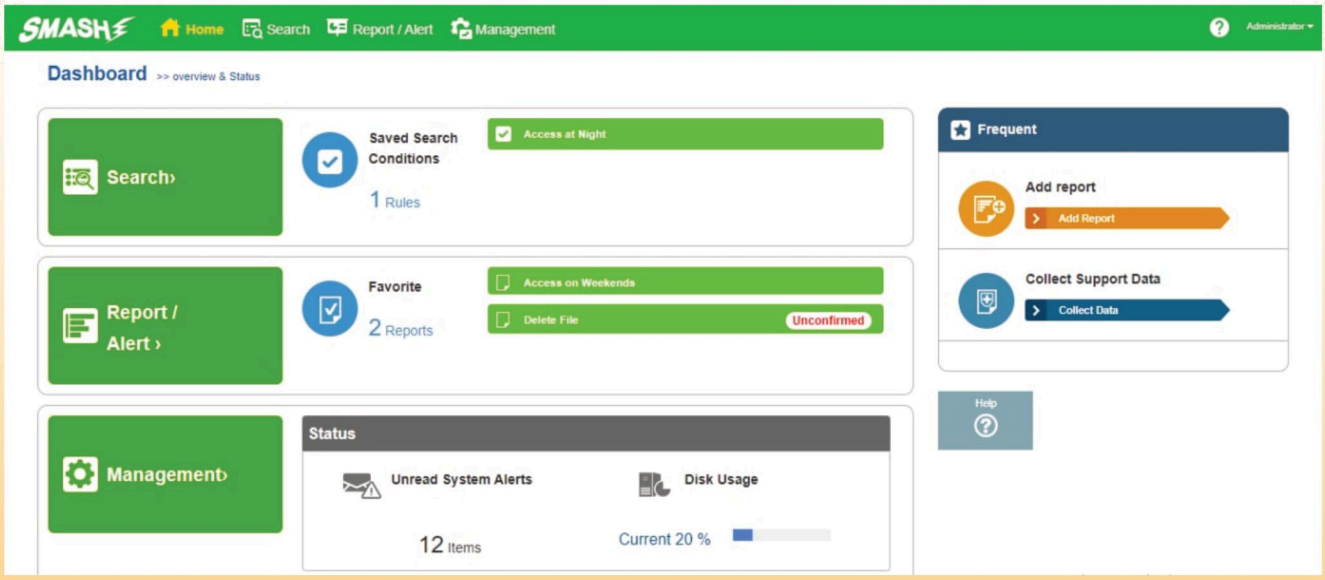
Time	User	Object	Operation
09/03/2021 23:11:17	TARGETSERVER20\andi	C:\Corporate File\IT Folder\Assets Credential - jan 2021.xlsx	READ
09/03/2021 23:11:21	TARGETSERVER20\andi	C:\Corporate File\IT Folder\Corp Infrastructure Diagram - jan 2021.docx	DELETE
10/03/2021 7:42:25	TARGETSERVER20\budi	C:\Corporate File\Admin Folder\Corp Employees PII - jan 2021.docx	COPY
10/03/2021 7:42:25	TARGETSERVER20\budi	C:\Corporate File\Admin Folder\Corp Employees PII - jan 2021 - Copy.docx	WRITE

SISTEM KERJA

ALog SMASH diinstal pada server yang dimonitor dan berjalan sebagai service. Service mengumpulkan event logs dan mengonversi ke access logs untuk menunjukkan histori operasi pengguna.

Konversi access logs disimpan dalam database untuk pencarian logs, dan pada saat yang sama, disimpankan juga dalam bentuk file CSV ke folder lain. Ini sangat cocok, menggunakan database untuk pencarian access logs terakhir dan file CSV untuk penyimpanan dalam jangka waktu yang lama.

TAMPILAN DASHBOARD



SPESIFIKASI

Operating environment:

Item	Requirements
Supported OS	Windows Server 2012/2012 R2 / 2016/2019 Windows Storage Server 2012/2012 R2 / 2016 Windows Server IoT 2019 * Not compatible with 32-bit OS * Compatible with service packs (SP) of each OS * Compatible with each edition (Standard / Enterprise / Datacenter) * Supports virtual environments (VMWare, Hyper-V, Citrix XenServer)
CPU	Recommended Quad Core or higher (minimum Dual Core)
Memory	Recommended 16GB or more (minimum 4GB)
HDD	100GB or more free space
Required Software	.NET Framework 4.6.2 or higher

cloudtech
PT. AWAN TEKNOLOGI GLOBAL

PT. AWAN TEKNOLOGI GLOBAL (CloudTech)

info@cloudtech.co.id

Gedung Tibyan Center, Lantai 2.
Jl. H. Nawi Raya No.17/191, RT.7/RW.10,
Gandaria Utara, Kby. Baru,
Jakarta Selatan, DKI Jakarta 12140

+62 21 2708 8802