Check MK

Monitoraggio dei sistemi IT con tecnologie Open Source

Benefici principali

- Opera su Nagios, un'applicazione open source
- Richiede risorse IT molto contenute
- Realizza un inventario automatico delle componenti controllate sui server

Controllo delle risorse aziendali

Nell'attività quotidiana, al fine di garantire l'efficienza delle soluzioni di business, il monitoraggio dello stato delle infrastrutture IT è di grande importanza.

Di solito, avendo tale attività costi elevati, si ricorre a sistemi di monitoraggio solo dove la rete da amministrare è veramente complessa o dove la criticità dei servizi è molto elevata.

Un approccio semplice ed economico

CLEMPS aiuta i propri clienti a utilizzare **Check MK**, un tool Open Source che, dopo un'installazione veloce e una configurazione molto semplice, consente, in modo intuitivo, di eseguire, tramite Web browser e come illustrato in figura, il monitoring della propria rete, dei sistemi operativi e delle applicazioni attivate, senza alcun costo di licenza software.

Come funziona

I controlli avvengono tramite **Check MK** un plug-in di un altro strumento Open Source denominato **Nagios**, che consente, tramite un Web browser, il monitoraggio di computer, switch, router, stampanti e anche di servizi più o meno standard come HTTP, FTP, POP3 e similari.

Come illustrato in figura, i dati vengono recuperati e visualizzati in quattro fasi:

1. Per ogni server, **Nagios** innesca un controllo attivo per l'intervallo di verifica che richiama **Check MK** come plug-in;
2. **Check MK** connette il server di destinazione tramite TCP recuperando in una sola volta, con un agente, tutti i dati pertinenti su quel server;
3. **Check MK** estrae i dati sulle prestazioni;
4. **Check MK** confronta i dati con dei livelli soglia critici e sottopone tutti i risultati utili a **Nagios**.

Ruolo dei Servizi Professionali

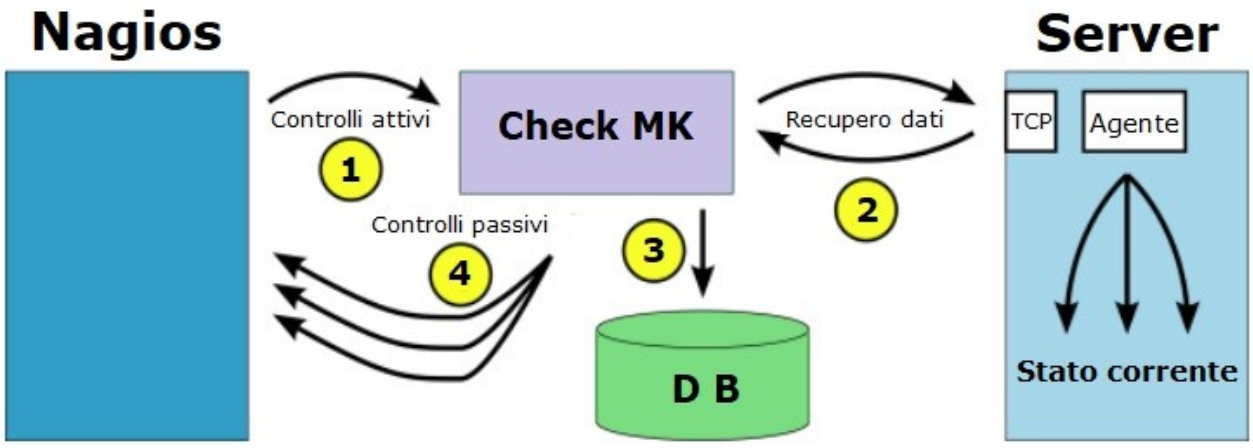
La prima attività dei servizi professionali **CLEMPS** riguarda l'attivazione della piattaforma di monitoraggio, che è basata su un sistema fisico o virtuale Linux CentOS 7.x caratterizzato da:

- Un sistema Nagios e Check MK funzionante;
- Un server Apache con il modulo mod_python per monitorare i sistemi;
- il package di sistema xinetd operativo;
- un sistema Postfix configurato per le notifiche email che perverranno a chi deve essere informato in caso di eventi critici.

Successivamente viene operato un censimento dei sistemi e dei package da controllare e per ogni server:

- viene installato l'agente di monitoraggio Windows o Linux su ogni server;
- vengono definiti i parametri di controllo;
- viene realizzata una breve attività di formazione.

Con sole poche giornate di attività e senza alcun costo di licenza software, qualunque infrastruttura, anche molto complessa, sarà finalmente sotto controllo!



CLEMPS Srl
Via Atene 27
00043 Ciampino (Roma)
Italia

Documento prodotto in Italia nel Giugno 2018

Questo documento è aggiornato alla data iniziale della pubblicazione e può essere modificato in qualsiasi momento.

I dati di esempio citati vengono presentati a puro scopo illustrativo. Le prestazioni effettive possono variare in base alle specifiche configurazioni e condizioni operative. E' responsabilità dell'utente valutare e verificare il funzionamento di qualsiasi prodotto o programma.

LE INFORMAZIONI PRESENTI IN QUESTO DOCUMENTO VENGONO FORNITE COSÌ COME SONO, SENZA ALCUNA GARANZIA, ESPRESSA O TACITA, DI ALCUN TIPO, INCLUSE TUTTE LE GARANZIE DI COMMERCIABILITÀ, IDONEITÀ PER UN FINE PARTICOLARE O NON VIOLAZIONE DI DIRITTI DI TERZI.

Il cliente ha la responsabilità di garantire la conformità alle normative e ai regolamenti applicabili. Non si forniscono consulenze legali né si garantisce che i servizi o i prodotti assicurino la conformità del cliente a normative o regolamenti.

Dichiarazione riguardante la validità delle procedure di sicurezza: la sicurezza dei sistemi IT implica la protezione dei sistemi e delle informazioni tramite la prevenzione, il rilevamento e la gestione degli accessi non autorizzati provenienti dall'interno e dall'esterno dell'azienda. L'accesso non autorizzato può determinare la modifica, la distruzione o l'uso inappropriato delle informazioni o causare danni o utilizzi impropri dei sistemi, con eventuali attacchi ad altri. Nessun sistema o prodotto IT può essere considerato assolutamente sicuro e nessun prodotto o misura di sicurezza può essere totalmente efficace per la prevenzione dell'accesso non autorizzato. Non si garantisce che i sistemi e i prodotti qui indicati siano immuni da condotte dannose o illegali perpetrate da qualsiasi altro soggetto.

Riciclare