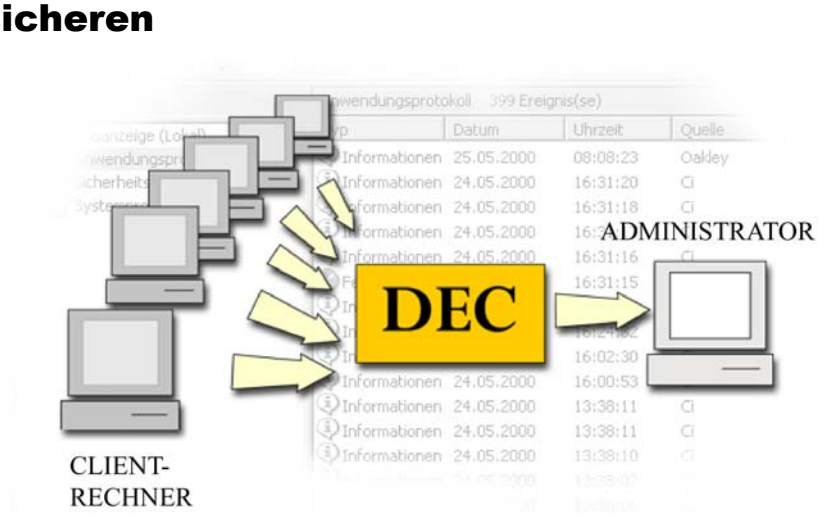
Domain Eventlog Collector - Der einfache Weg zur effektiven und sicheren Administration von Netzwerken

Sie sind Administrator und haben die Verantwortung für ein großes Netzwerk? Sie wollen Kontrolle über die Ereignisse in jedem Ihrer Rechner? Sie wollen sofort automatisch benachrichtigt werden, wenn etwas aus dem Ruder läuft?



Endlich ist synoptische Diagnose und Prophylaxe für das Netzwerk möglich – mit dem neuen Domain Eventlog Collector der active BIT.

Der Domain Eventlog Collector läuft auf einem Ihrer Systeme und sammelt die Ereignisprotokolle sämtlicher Rechner im LAN ein. So können Sie, bequem von Ihrem Arbeitsplatz aus, die Eventlogs jedes dieser Rechner kontrollieren.

Ausgereifte Gruppierungsfunktionen machen es zum Beispiel möglich, die Ereignisse einer bestimmten Anwendung auf allen Rechnern zusammen darzustellen. Dadurch wird die Suche nach globalen Fehlfunktionen einfach.

Durch das Zwischenschalten von Filtern werden bestimmte wichtige Meldungen des Netzwerks zur Ansicht ausgewählt, während andere, weniger wichtige ausgeblendet werden.

Der Benachrichtigungsservice versorgt den Administrator auch in Abwesenheit über das mit wichtigen Ereignismeldungen, per eMail oder Handy mit SMS oder WAP.

Der Domain Eventlog Collector bietet eine einzigartige und elegante Lösung, die dem Administrator die Pflege und Aufrechterhaltung seines Netzwerks in hohem Maße vereinfacht.

Sammeln und Speichern von Eventlogs

- Die Ereignisprotokolle sämtlicher Domänen-Rechner werden von einer zentralen Stelle zyklisch ausgelesen und der aktuelle Stand in einer Datenbank gespeichert.
- Die Computer im lokalen Netzwerk werden vom DEC nach den Gesichtspunkten der gleich installierten Anwendungen und Dienste neu gruppiert.
- Es wird analysiert, von welcher Anwendung die Fehlerquelle ausgeht, und diese Information wird in der Datenbank hinterlegt, sodass Fehler von gleichen Anwendungen aus verschiedenen Rechnern als solche erkannt werden.
- Ist ein Rechner des Netzwerks nicht ansprechbar (z. B. durch fehlende Zugriffsberechtigung), so wird dies ebenfalls protokolliert.
- Durch die zentrale Speicherung ist eine unternehmensweite Archivierung bestimmter Protokollstände in einem einzigen Arbeitsschritt möglich. Diese Sicherungen können bei Bedarf von den Datenträgern in die operative Datenbank zurückgespielt werden. Fehler mit weit zurückreichender Historie sind damit aufspürbar.
- Es kann eingestellt werden, wie lange die Protokollstände in der Datenbank

gespeichert bleiben. Nach Ablauf dieser Zeit werden sie entweder gelöscht oder können an anderer Stelle gesichert werden.

- Der DEC ist mit einer großen Anzahl von Datenbanksystemen kompatibel.

Auswertungen und Analyse der Daten

- Der Zugriff auf die Daten erfolgt ausschließlich über die Datenbank. Die Rechner müssen für diesen Prozess weder angeschaltet noch mit dem Netzwerk verbunden sein. Dies macht ein effizientes Diagnostizieren außerhalb der normalen Arbeitszeiten möglich.
- Mit Hilfe geeigneter Filter- und Suchfunktionen können beliebige Einträge zu jedem Ereignisprotokoll (Anwendungs-, System- oder Sicherheitsprotokoll) auf jeder Maschine gefunden werden. Wird auf einer Maschine ein Fehler lokalisiert, kann auf allen anderen Maschinen nach demselben Fehler gefahndet werden, um so auf einen Schlag gleich Probleme auf mehreren Computern zu erkennen.
- Über alle Anwendungen, Maschinen und andere Parameter werden Nachschlagetabelle angelegt, die jederzeit eingesehen werden können und die Navigation im Protokoll-Gesamtbestand ermöglichen.
- Der Anwender kann eigene Analysen mit Standard-Anwendungen (Crystal Reports) vornehmen. Das Datenmodell ist zu diesem Zweck offengelegt. Somit sind in einfacher Weise automatisch generierte Dokumentationen auch mit statistischem Inhalt möglich.
- Endlich werden Fehlerzustände nachvollziehbar, die sich aus dem Zusammenwirken von mehreren vernetzten Maschinen ergeben.

Verwaltungsfunktionen

- Die Software erkennt automatisch die Windows NT-Systeme der Domäne. Diese Systeme werden beim Einsammeln der Ereignisprotokolle berücksichtigt, sofern der Administrator diese nicht aus dem Verzeichnis entfernt.
- Der Administrator kann zusätzlich Computer in vertrauten Domänen in das System aufnehmen, sodass auch deren Maschinen berücksichtigt werden.
- Die Häufigkeit, mit der die Netzwerk-Rechner überprüft werden, kann festgelegt werden. Überprüfungen sind damit zu bestimmten Uhrzeiten möglich. Hiermit können Lösch-Intervalle bzw. Überschreibungs-Intervalle der dezentralen Protokolle berücksichtigt werden.
- Der Benutzer kann sowohl die Abstände der Aktualisierungs-Zyklen einstellen als auch wie lange die Daten in der Datenbank gespeichert bleiben sollen. Nach Ablauf dieser Zeit werden sie entweder gelöscht, oder aber an einer anderen Stelle gesichert.

Remote Warnsystem

- Ein für konfigurierbares Warnsystem übermittelt dem Administrator kritische Fehlermeldungen sofort per eMail oder SMS an ein Mobiltelefon. So kann eine ernste Störung im Netz frühzeitig erkannt und behoben werden.

Weitere Informationen

active BIT GmbH
Brüsseler Str. 102
53117 Bonn
Fon: 0228-55945-0
Fax: 0228-55945-10
info@active-bit.com
http://www.active-bit.de

Microsoft Certified
Solution Provider