Prehľad monitorovacích nástrojov v CM

V tomto komponente sú zaradené funkcionality, ktoré sledujú určitý stav a ak niečo je mimo očakávaného rozsahu alebo nastane chybová udalosť, systém generuje hlásenia rôznymi formami ako záznam do CM portálu, mailom, SMS.

Prehľad hlavných monitorovacích funkcionalít:

Watches - Online Monitoring

Zoznam podmienok pre OS MS Windows

Zoznam podmienok pre OS Linux/FreeBSD, Mac OS X

Monitoring prostredia

Monitoring HW stavu serverov (HP, DELL, Fujitsu)

Monitoring spojenia medzi CM Serverom a PC (komponent CM Connection guard) [1] **[2]**

Pravidelné sledovanie dôležitých parametrov počítačov a serverov

Vyhodnocovanie logov, reportov z íných programov "Externé programy"

Nepriame monitorovanie funkčnosti aplikácií "Sledované súbory"

Odoslanie zmeny chybového log súboru priamo Operátorovi

Hlavné vlastnosti :

- Podpora pre operačné systémy MS Windows, Linux/FreeBSD, Mac OS X.
- Notifikácia operátorom a ich nadriadeným prostredníctvom Emailov, SMS, dashboardu v CM portáli
- Notifikácia používateľovi PC (zákazníkovi) je priamo na počítači alebo cez notifdikačné správy
- Výborné nastavenia pre potlačenia nežiadúcich notifikačných správ
- Detailné historické údaje v CM portáli 2 mesiace, zosumarizované až 1,5 roka
- Možnosť vykonať automatizovaný opravný úkon po vzniku chybového stavu
- Vysoká univerzálnosť nastavení v každom type monitoringu

Watches - online monitoring

je zameraný na dohľad kritických a dôležitých častí infraštruktúry. Online sledovania Watches sa robia pomocou klienta C-Monitor, ktorý údaje odovzdáva na CM Server na zobrazenie a centrálnu

notifikáciu. C-Monitor klient má svoje možnosti notifikácie, vykonania opravných akcií. K dispozícii je aj podmienené vyhodnotenie, ktoré dovoľuje nastaviť veľmi presný monitoring a vyhnúť sa SPAMovaniu z monitoringu.

Princíp fungovania CM Online Watches je založený na podmienkach, v rámci ktorých sú definované limity - hraničné hodnoty rozhodujúcich o dobrom alebo chybnom stave. Vďaka systému podmienok je uplatenie ďaleko širšie ako pri iných systémoch s pevne preddefinovanými pravidlami. Na určenie výsledného stavu Watchu sa volí logická operácia medzi podmienkami vo forme :

Stav Watchu je CHYBNÝ, ak ..(nie všetky / žiadne / všetky / aspoň jedna).. podmienky sú pravdivé.
State of Watch is FAIL if (NOT ALL / NONE / ALL /AT LEAST ONE) conditions are true.

Skrátený prehľad parametrov k monitorigu v rámci CM Online Watches (Windows)

Podmienky (Conditions) :

Memory Usage - obsadenie fyzickej alebo celkom vytvorenej RAM včítane "swapu"
CPU Usage - percentuálne priemerne zaťaženie jadier CPU spolu
Disk Activity - percentuálne zaťaženie diskov (u Linux systémov aj jednotlivo)
Disk Queue Length - u Windows OS parameter vyjadrujúci zaťaženie disku (počet diskových operácii čakajúcich na spracovanie.
Network Adapter Usage - percentuálne zaťaženie sieť. adaptéra
Internet IP Traffic - prenosová rýchlosť údajov na internet (mimo LAN)
Internet IP Transferred Data - prenosené údaje na internet (mimo LAN)
Free Space on Disk - zostávajúce voľné miesto na disku
Exists File - prítomnosť vybraného súboru
File Size - veľkosť vybraného súboru
File Size in Directory - veľkosť vybraných súborov v adresári
Exists Directory - dostupný adresár na čítanie
Directory Accessible - dostupný adresár na čítanie aj zápis
LoggedOn User - prihlásený používateľ
OS Running Time - čas spustenia operačného systému
Operating System Started - bol vykonaný štart OS v určitom intervale dozadu
Date - určenie nejakého hraničného dátumu
Day of Week - deň v týždni
Time - určenie hraničného času
Time Range - určenie intervalu
Current IP - aktuálna IP adresa (z ktoréhokoľvek sieťového adaptéra)
Performance Counter - vyčítanie akéhokoľvek countra v OS Windows
Hardware Monitoring - vyčítavanie teploty, otáčok ventilátora ... z chipu na základnej doske
Ping - platná odozva z určitej sieťovej lokality (IP adresy)
Ping Round Trip Time - čas odozvy z určitej sieťovej lokality (IP adresy)
Ping Packer Loss - počítanie stratených paketov pri testovaní odozvy
SMTP - základná funkčnosť komunikácie na protokole SMTP
POP3 - základná funkčnosť komunikácie na protokole POP3
HTTP, HTTPS - porovnávanie reťazcov získaných zo stránky http alebo https (aj cez Proxy)
HTTP, HTTPS response time - *čas* načítania zvolenej http alebo https stránky (aj cez Proxy)
Transfer Speed - prenosová rýchlosť na lokálnom sieťovom adaptéri
Transfer Speed of FTP - prenosová rýchlosť pri prenose z/na FTP lokalitu
SNMP - vyčítavanie parametrov cez SNMP protokol
Enviroment Monitoring (SNMP) - meranie teploty, vlhkosti cez zariadenia HW Group Poseidon
Enviroment Monitoring (HTTP) - meranie teploty, vlhkosti cez zariadenia Wanet WARIO
E-Mail Loop Test - odoslanie jedinečného emailu cez SMTP server a prijatie cez POP3 do čas.limitu
EventLog Events Count - počet kritických udalostí na roliach Windows 2008 a vyššie serverov
Chat - interný skriptovací jazyk v C-Monitore pre tvorenie automatizovaných zložitejších meraní
Chat Variable - prenos premennej zo skriptu na vyhodnotenie C-Monitorom
Chat Numeric Variable - prenos numerickej premennej zo skriptu na vyhodnotenie C-Monitorom
Chat Vector Variable - prenos premenných naraz (vektor) zo skriptu na vyhodnotenie C-Monitorom

Service status - stav služby
Loaded Device Driver - prítomnosť ovládača v pamäti (v systéme)
Running Process - prítomnosť procesu v pamäti
Running User Process - prítomnosť procesu v pamäti pod konkrétnymi používateľmi
Unauthorized Admin Process - prihlásenie neautoriz. používateľa s administrátorským oprávneniami
Process Usage - zaťaženie CPU alebo RAM od konkrétneho procesu
Network Presented - aktívna sieť od akéhokoľvek adaptéra
Watch State - vstup na vyhodnotenie od iného Watchu (zreťazenie Watchov)

Preddefinované šablóny v sprievodcovi vo Watches :

Výkonnostné (Preddefined performance templates) :
General performance - sumárny pohľad na zaťaženie serverov
SQL memory, Page splits, Users - Výkonnosť MS SQL serverov, časť 1.
SQL Transactions and deadlocks - Výkonnosť MS SQL serverov, časť 2.
SQL query response time - Výkonnosť MS SQL serverov na základe počítania odozvy z prístupu do DB a vykonania jednoduchého príkazu
SQL query with table response time - Výkonnosť MS SQL serverov na základe počítania času zostavenia a vymazania tabulky v DB
Terminal active sessions - počet aktívne pripojených používateľov k terminálovému serveru

Zdravie systému (Preddefined health templates):
WIN Server roles Event errors - automatická detekcia rolí serverov a vyhľadávanie chýb v Eventlogu
MS SQL Query test - Dostupnosť MS SQL serverov na základe práce s tabuľkami
APC UPS Status a Low Energy - stav záložných zdrojov APC získaný z lokálnej inštalácie Powerchute Business edition

Skrátený prehľad parametrov k monitoringu v rámci CM Online Watches (Linux/FreeBSD, Mac OS X):

Podmienky (Conditions) :

CPU Usage
Disk Free Space
Disk Usage
HTTP(s) response
Load Average
Memory Usage
Network Adapter Usage
OS Running Time
OS Started
Ping
Ping Packet Loss
Ping Round Trip Time
Process Running

Monitoring prostredia

Monitoring prostredia prostredníctvom pripojených zariadení na zmenu fyzikálnych veličín do digitálnej formy pre sieť Ethernet. Podporované zariadenia sú značiek Wario a Poseidon, oboje zakúpiteľné cez adresu kontaktu [3].

Najbežnejšie merané jednotky sú :
Teplota (temperature)

Vhkosť (humidity)
Výpadky 230V
Kontakty - napríklad pre prístup do serverovne alebo do racku

Možné je merať s týmito zariadeniami :
Spotrebu elektrickej energie, meteorologické veličiny - úhrn zrážok, rýchlosť a smer vetra ...

Monitoring HW stavu serverov (HP, DELL, Fujitsu)

Monitoring vyhodnocuje stav hardvéru serverov pomocou nástrojov výrobcov. Monitoring je podporený pre každý operačný systém, na ktorý je možné nainštalovať monitorovací softvér od výrobcu. Ide o programy : Insight Manager (HP), Open Manage (DELL). C-Monitor klient cez Watch vyčítava hodnoty cez SNMP, vyhodnocuje ich a následne odosiela do Servera CM. Riešenie je predkonfigurované, v Sprievodcovi v C-MonitorConsole/Watches si zvolíte typ servera, ktorý chcete monitorovať, doplníte povinne len IP adresu. V manuále Monitoring HW HP, DELL, FUJITSU je popísaná aj prípravná inštalácia pre operačné systémy Windows a vmware ESX.
Monitorované HW parametre sú :

Bezporuchovosť RAM
Bezporuchovosť diskov (včítane automatickej detekcie obsadených slotov)
Bezporuchovosť RAID diskových polí
Bezporuchovosť Napájacích zdrojov
Bezporuchovosť ventilátorov
Teploty na rôznych miestach vo vnútri servera v limitných hodnotách
Stav sieťového adaptéra

Pravidelné sledovanie dôležitých parametrov počítačov

Automatická, 1x za 24hodín vykonávaná kontrola dôležitých parametrov počítačov a serverov. Parametre sú získavané automaticky, bez nutnosti konfigurácie (predvolená konfigurácia je súčasťou C-Monitora) a sú predvolené aj limity pre upozornenia na CM Serveri. Ide o údaje získavané pomocou modulu C-Descript, hranice pre upozornenia sú diferencované na základe zvolenej Priority. Upozornenia sú v prípade neodstránenia poruchy eskalované nadriadenému pracovníkovi.

Voľné miesto diskových jednotiek
informácie o každej partícii zapojeného lokálneho disku
informácie o pripojených sieťových diskoch posledne prihláseného používateľa
HW chybovosť diskov
Údaje o „zdravotnom“ stave diskov S.M.A.R.T. (mimo diskov na RAID radičoch)
Stav antivírového programu
stav aktualizácie a fungovania antivírového programu na základe Security Center z WIN OS - pre všetky antivíry a na všetkých WIN OS (od WIN XP až po WIN8)
stav aktualizácie antivírového programu s konkrétmym dátumom poslednej aktualizácie (ESET, AVG, Microsoft Security Essentials, McAfee, Norton Antivirus, GFI Vipre)
expirácia platnosti licencie ESET, AVG na všetkých OS, ostatné antivíry len na WIN8
Stav service packov a opravných balíkov - registrácia podľa poslednej úspešnej inštalácie
Kontrola posledného bodu obnovenia (System Restore)
Veľkosť dátových súborov programov pre email na PC
Veľkosť dátových súborov poštových klientov: Outlook, Outlook Express, Windows Live Mail
Veľkosť súborov programov pre email na Serveroch
Veľkosť dátových súborov a prípadne aj schránok serverového systému MS Exchange (nastavenie cez Watches)
Pripojenie počítača do siete neregistrovaného v CM
Zoznam počítačov, ktoré boli pripojené do siete a nie sú v CM

Vyhodnocovanie logov, reportov z íných programov "Externé programy"

Vyhodnocovanie logov z akejkoľvek aplikácie / Externé programy - Spracovanie akéhokoľvek mailu z treťostrannej aplikácie, sledovanie jej pravidelného doručovania, aby administrátor mal pomoc pri sledovaní stavu procesov a aplikácií, ktoré nemajú priamu podporu v CM.
Zo sledovanej aplikácie sa musí odosielať mail na adresu CM Servera, V CM sa určujú kritéria úspešnosti / chyby a interval posielania správy z programu.
Výhodnocované sú texty v tele správy, v prílohe. Formáty html, obyčajný text.
Výsledný stav je dostupný v Zóne Externé programy a chybové stavy sú v časti Poruchy.

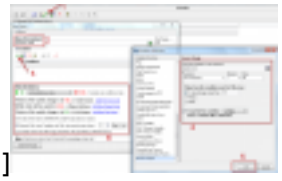
Nepriame monitorovanie funkčnosti aplikácií "Sledované súbory"

Sledovanie zmenených súborov - Prostredníctvom úlohy C-Monitor klienta „Files Watchdog“ sa zbiera zoznam zmenených súborov voči predchádzajúcemu spusteniu úlohy „Files Watchdog“. Ak zoznam je prázdny, tj. k žiadnej zmene neprišlo, signalizuje to chybný stav. Je to vhodné na zjednodušenú kontrolu činnosti programov, kde sa zmena očakáva vo vopred definovaných intervaloch a zmena v súboroch vyjadruje s vysokou spoľahlivosťou správnu funkciu sledovaného programu, napríklad záznamy z kamerového systému, tarifikátory, exporty z SQL databáz a podobne. Údaje na serveri sa zobrazujú v Zóne - Sledované súbory a chybové stavy sú v časti Poruchy.

Odoslanie zmeny chybového log súboru priamo Operátorovi

Odoslanie (zmeneného) obsahu log súboru na adresu administrátora (operátora) - Prostredníctvom úlohy C-Monitor klienta „Send log file(s) to admin’s email address“ je možné dochytiť zmenu sledovaného súboru a zmenený obsah odoslať na akúkoľvek adresu. Niektoré aplikácie majú totiž log chybových stavov, do ktorého nech sa zapíše čokoľvek, znamená to, že treba riešiť. Administrátor do mailovej schránky dostáva priamo aj popis chyby a vie reagovať omnoho rýchlejšie. Celá funkčnosť tohto sledovania ide mimo Server CM (klient C-Monitor odosiela údaje priamo zvolenú emailovú adresu)

Date:
21.12.2012External Links:
Ako funguje CM - Monitoring a diagnostika [4]Obrázky:

[5]


[6]

[7]
[8]

[9]

[10]

[11]
[12]

[13]

Odkazy
[1] https://customermonitor.sk/komponenty/cm-connection-guard
[2] https://customermonitor.sk/komponenty/cm-backup#C-Image
[3] https://customermonitor.sk/kontakt
[4] https://customermonitor.sk/ako-funguje-cm/monitoring-a-diagnostika
[5] https://customermonitor.sk/sites/default/files/pridanie%20watchu%20cez%20c-monitor.png
[6] https://customermonitor.sk/sites/default/files/pridanie%20podmienok%20k%20watchu.png
[7] https://customermonitor.sk/sites/default/files/pridanie%20watchu%20cez%20cm%20portal.png
[8] https://customermonitor.sk/sites/default/files/pridanie%20podmienok%20watchu%20cez%20cm%20portal.png
[9] https://customermonitor.sk/sites/default/files/stav%20watchu.png
[10] https://customermonitor.sk/sites/default/files/staw%20watchu%20na%20cm%20serveri.png
[11] https://customermonitor.sk/sites/default/files/historia%20watchu.png
[12] https://customermonitor.sk/sites/default/files/watches%20v%20tabulkovej%20forme.png
[13] https://customermonitor.sk/sites/default/files/Informacny_panel__do_Komponentov.png