Přehled monitorovacích nástrojů v CM

V tomto komponentě jsou zařazeny funkcionality, které sledují určitý stav a pokud je něco mimo očakáveného rozsahu nebo nastane chybová událost, systém generuje hlášení různými formami jako záznam do CM portálu, mailem, SMS.

P?ehled hlavních monitorovacích funkcionalit :

Watches - Online Monitoring

Seznam podmínek pro OS MS Windows

Seznam podmínek pro OS Linux/FreeBSD, Mac OS X

Monitoring prostředí

Monitoring HW stavu serverů (HP, DELL, Fujitsu)

Monitoring spojení mezi CM Serverem a PC (komponent CM Connection guard) [1] **[2]**

Pravidelné sledování důležitých parametrů, počítačů a serverů

Vyhodnocování logů, reportů z jiných programů "Externí programy"

Nepřímé monitorování funkčnosti aplikací "Sledované soubory"

Odeslání změny chybového log souboru přímo Operátorovi

Hlavní vlastnosti :

- Podpora pro operační systémy MS Windows, Linux / FreeBSD, Mac OS X.
- Notifikace operátorům a jejich nadřízeným prostřednictvím Emailů, SMS, dashboardu v CM portálu
- Notifikace uživateli PC (zákazníkovi) je přímo na počítači nebo přes notifikační zprávy
- Vynikající nastavení pro potlačení nežádoucích notifikačních zpráv
- Detailní historické údaje v CM portálu 2 měsíce, zesumarizovány až 1,5 roku
- Možnost provést automatizovaný opravný úkon po vzniku chybového stavu
- Vysoká univerzálnost nastavení v každém typu monitoringu

Watches - online monitoring

je zaměřen na dohled kritických a důležitých částí infrastruktury. Online sledování Watches se dělají

pomocí klienta C-Monitor, který údaje předává na CM Server na zobrazení a centrální notifikaci. C-Monitor klient má své možnosti notifikace, provedení opravných akcí. K dispozici je také podmíněné vyhodnocení, které dovoluje nastavit velmi přesný monitoring a vyhnout se spamování z monitoringu.

Princip fungování CM Online Watches je založen na podmínkách, v rámci kterých jsou definovány limity - hraniční hodnoty rozhodujících o dobrém nebo chybném stavu. Díky systému podmínek je uplatnení daleko širší než u jiných systémů s pevně předdefinovanými pravidly. K určení výsledného stavu Watch se volí logická operace mezi podmínkami ve formě :

Stav Stav Watche je CHYBNÝ, pokud .. (ne všechny / žádné / všechny / alespoň jedna) .. podmínky jsou pravdivé.
State of Watch is FAIL if (NOT ALL / NONE / ALL /AT LEAST ONE) conditions are true.

Zkrácený přehled parametrů k monitorigu v rámci CM Online Watches (Windows)

Podmínky (Conditions) :

Memory Usage - obsazení fyzické nebo zcela vytvořené RAM včetně "swapu"
CPU Usage - procentní průměrně zatížení jader CPU spolu
Disk Activity - procenní zatížení disků (u Linux systémů i jednotlivě)
Disk Queue Length - u Windows OS parametr vyjadřující zatížení disku (počet diskových operaci čekajících na zpracování.
Network Adapter Usage - procentní zatížení síťového adaptéru
Internet IP Traffic - přenosová rychlost dat na internet (mimo LAN)
Internet IP Transferred Data - přenošené údaje na internet (mimo LAN)
Free Space on Disk - zbývající volné místo na disku
Exists File - přítomnost vybraného souboru
File Size - velikost vybraného souboru
File Size in Directory - velikost vybraných souborů v adresáři
Exists Directory - dostupný adresář pro čtení
Directory Accessible - dostupný adresář pro čtení i zápis
LoggedOn User - přihlášený uživatel
OS Running Time - čas spuštění operačního systému
Operating System Started - byl proveden start OS v určitém intervalu zpět
Date - určení nějakého hraničního data
Day of Week - den v týdnu
Time - určení hraničního času
Time Range - určení intervalu
Current IP - aktuální IP adresa (z kteréhokoliv síťového adaptéru)
Performance Counter - vyčtení jakéhokoliv countru v OS Windows
Hardware Monitoring - vyčítání teploty, otáček ventilátoru ... z chipu na základní desce
Ping - platná odezva z určité síťové lokality (IP adresy)
Ping Round Trip Time - čas odezvy z určité síťové lokality (IP adresy)
Ping Packer Loss - počítání ztracených paketů při testování odezvy
SMTP - základní funkčnost komunikace na protokolu SMTP
POP3 - základní funkčnost komunikace na protokolu POP3
HTTP, HTTPS - porovnávání řetězců získaných ze stránky http nebo https (i přes Proxy)
HTTP, HTTPS response time - *čas* načítání zvolené http nebo https stránky (i přes Proxy)
Transfer Speed - přenosová rychlost na lokálním síťovém adaptéru
Transfer Speed of FTP - přenosová rychlost při přenosu z / na FTP lokalitu
SNMP - vyčítání parametrů přes SNMP protokol
Enviroment Monitoring (SNMP) - měření teploty, vlhkosti přes zařízení HW Group Poseidon
Enviroment Monitoring (HTTP) - měření teploty, vlhkosti přes zařízení wanu WARIO
E-Mail Loop Test - odeslání jedinečného emailu přes SMTP server a přijetí přes POP3 do čas.limitu
EventLog Events Count - počet kritických událostí na rolích Windows 2008 a vyšší serverů
Chat - interní skriptovací jazyk v C-Monitoru pro tvoření automatizovaných složitějších měření
Chat Variable - přenos proměnné ze skriptu na vyhodnocení C-Monitorem

Chat Numeric Variable - přenos numerické proměnné ze skriptu na vyhodnocení C-Monitorem
Chat Vector Variable - přenos proměnných najednou (vektor) ze skriptu na vyhodnocení C-Monitorem
Service status - stav služby
Loaded Device Driver - přítomnost ovladače v paměti (v systému)
Running Process - přítomnost procesu v paměti
Running User Process - přítomnost procesu v paměti pod konkrétními uživateli
Unauthorized Admin Process - přihlášení nautoriz. uživatele s administrátorským oprávněním
Process Usage - zatížení CPU nebo RAM od konkrétního procesu
Network Presented - aktivní síť od jakéhokoliv adaptéru
Watch State - vstup na vyhodnocení od jiného Watche (zřetězení Watchů)

Předdefinované šablony v průvodci ve Watches :

Výkonnostní (Preddefined performance templates) :
General performance - sumární pohled na zatížení serverů
SQL memory, Page splits, Users - Výkonnost MS SQL serverů, část 1.
SQL Transactions and deadlocks - Výkonnost MS SQL serverů, část 2.
SQL query response time - Výkonnost MS SQL serverů na základě počítání odezvy z přístupu do DB a provedení jednoduchého příkazu
SQL query with table response time - Výkonnost MS SQL serverů na základě počítání času sestavení a vymazání tabulky v DB
Terminal active sessions - počet aktivně připojených uživatelů k terminálovému serveru

Zdraví systému (Preddefined health templates):
WIN Server roles Event errors - automatická detekce rolí serverů a vyhledávání chyb v EventLogu
MS SQL Query test - Dostupnost MS SQL serverů na základě práce s tabulkami
APC UPS Status a Low Energy - stav záložních zdrojů APC získaný z lokální instalace PowerChute Business edition

Zkrácený přehled parametrů k monitoringu v rámci CM Online Watches (Linux/FreeBSD, Mac OS X):

Podmínky (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 prostředí

Monitoring prostředí prostřednictvím připojených zařízení na změnu fyzikálních veličin do digitální formy pro síť Ethernet. Podporovaná zařízení jsou značek Wario a Poseidon, obojí zakoupitelná přes adresu kontaktu [3].

Nejběžnější měřené jednotky jsou :
Teplota (temperature)
Vhkost (humidity)
Výpadky 230V
Kontakty - například pro přístup do serverovny nebo do racku

Možné je měřit s těmito zařízeními :
Spotřebu elektrické energie, meteorologické veličiny - úhrn srážek, rychlost a směr větru ...

Monitoring HW stavu serverů (HP, DELL, Fujitsu)

Monitoring vyhodnocuje stav hardwaru serverů pomocí nástrojů výrobců. Monitoring je podpořen pro každý operační systém, na který je možné nainstalovat monitorovací software od výrobce. Jde o programy: Insight Manager (HP), Open Manage (DELL). C-Monitor klient přes Watch vyčítá hodnoty přes SNMP, vyhodnocuje je a následně odesílá do Serveru CM. Řešení je předkonfigurováno, v Průvodci v C-MonitorConsole/Watches si zvolíte typ serveru, který chcete monitorovat, doplníte povinně pouze IP adresu. V manuálu Monitoring HW HP, DELL, FUJITSU je popsána i přípravná instalace pro operační systémy Windows a vmware ESX.
Monitorované HW parametry jsou :
Bezporuchovost RAM
Bezporuchovost disků (včetně automatické detekce obsazených slotů)
Bezporuchovost RAID diskových polí
Bezporuchovost Napájecích zdrojů
Bezporuchovost ventilátorů
Teploty na různých místech uvnitř serveru v mezních hodnotách
Stav síťového adaptéru

Pravidelné sledování důležitých parametrů počítačů

Automatická, 1x za 24 hodin prováděna kontrola důležitých parametrů počítačů a serverů. Parametry jsou získávány automaticky, bez nutnosti konfigurace (výchozí konfigurace je součástí C-Monitoru) a jsou předvolené i limity pro upozornění na CM Serveru. Jde o údaje získávané pomocí modulu C-descript, hranice pro upozornění jsou diferencované na základě zvolené Priority. Upozornění jsou v případě neodstranění poruchy eskalovány nadřízenému pracovníkovi.

Volné místo diskových jednotek
informace o každé partici zapojeného lokálního disku
informace o připojených síťových discích posledně přihlášeného uživatele
HW chybovost disků
Údaje o "zdravotním" stavu disků S.M.A.R.T. (mimo disků na RAID řadičích)
Stav antivirového programu
stav aktualizace a fungování antivirového programu na základě Security Center z WIN OS - pro všechny antiviry a na všech WIN OS (od WIN XP až po Win8)
stav aktualizace antivirového programu s konkrétmym datem poslední aktualizace (ESET, AVG, Microsoft Security Essentials, McAfee, Norton Antivirus, GFI Vipre)
expirace platnosti licence ESET, AVG na všech OS, ostatní antiviry jen na Win8
Stav service packů a opravných balíků - registrace podle poslední úspěšné instalace
Kontrola posledního bodu obnovení (System Restore)
Velikost datových souborů programů pro email na PC
Velikost datových souborů poštovních klientů: Outlook, Outlook Express, Windows Live Mail
Velikost souborů programů pro email na Serverech
Velikost datových souborů a případně i schránek serverového systému MS Exchange (nastavení přes Watches)
Připojení počítače do sítě neregistrovaného v CM
Seznam počítačů, které byly připojeny do sítě a nejsou v CM

Vyhodnocování logů, reportů z jiných programů "Externí programy"

Vyhodnocování logů z jakékoliv aplikace / Externí programy - Zpracování jakéhokoliv mailu z

aplikace třetí strany, sledování jejího pravidelného doručování, aby administrátor měl pomoci při sledování stavu procesů a aplikací, které nemají přímou podporu v CM.
Ze sledované aplikace se musí odesílat mail na adresu CM Serveru, V CM se určují kritéria úspěšnosti / chyby a interval posílání zprávy z programu.
Vyhodnocovány jsou texty v těle zprávy, v příloze. Formáty html, prostý text.
Výsledný stav je dostupný v Zóně Externí programy a chybové stavy jsou v části Poruchy

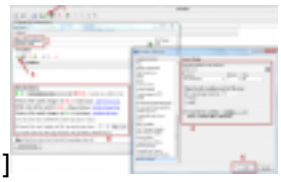
Nepřímé monitorování funkčnosti aplikací "Sledované soubory"

Sledování změněných souborů - Prostřednictvím úkolu C-Monitor klienta "Files Watchdog" se sbírá seznam změněných souborů vůči předchozímu spuštění úlohy "Files Watchdog". Pokud je seznam prázdný, tj. k žádné změně nedošlo, signalizuje to chybný stav. Je to vhodné pro zjednodušenou kontrolu činnosti programů, kde se změna očekává v předem definovaných intervalech a změna v souborech vyjadřuje s vysokou spolehlivostí správnou funkci sledovaného programu, například záznamy z kamerového systému, tarifikátory, exporty z SQL databází a podobně. Údaje na serveru se zobrazují v Zóně - Sledované soubory a chybové stavy jsou v části Poruchy.

Odeslání změny chybového log souboru přímo Operátorovi

Odeslání (změněného) obsahu log souboru na adresu administrátora (operátora) - Prostřednictvím úkolu C-Monitor klienta "Send log file(s) to admin's email address" je možné zachytit změnu sledovaného souboru a změněný obsah odeslat na jakoukoli adresu. Některé aplikace mají totiž log chybových stavů, do kterého ať se zapíše cokoli, znamená to, že je třeba řešit. Administrátor do mailové schránky dostává přímo i popis chyby a umí reagovat mnohem rychleji. Celá funkčnost tohoto sledování jde mimo Server CM (klient C-Monitor odesílá údaje přímo na zvolenou emailovou 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.cz/cz-komponenty/cm-connection-guard
[2] https://customermonitor.cz/komponenty/cm-backup#C-Image
[3] https://customermonitor.cz/kontakt
[4] https://customermonitor.cz/ako-funguje-cm/monitoring-a-diagnostika
[5] https://customermonitor.cz/sites/default/files/pridanie%20watchu%20cez%20c-monitor.png
[6] https://customermonitor.cz/sites/default/files/pridanie%20podmienok%20k%20watchu.png
[7] https://customermonitor.cz/sites/default/files/pridanie%20watchu%20cez%20cm%20portal.png
[8] https://customermonitor.cz/sites/default/files/pridanie%20podmienok%20watchu%20cez%20cm%20portal.png
[9] https://customermonitor.cz/sites/default/files/stav%20watchu.png
[10] https://customermonitor.cz/sites/default/files/staw%20watchu%20na%20cm%20serveri.png
[11] https://customermonitor.cz/sites/default/files/historia%20watchu.png
[12] https://customermonitor.cz/sites/default/files/watches%20v%20tabulkovej%20forme.png
[13] https://customermonitor.cz/sites/default/files/Informacny_panel__do_Komponentov.png