

SAT-2G.303-1-CST-03

PERSONAL MONITORING AND MANAGENENT OF VIRTUAL
INFRASTRUCTURES BASED ON ZABBIX¹⁴⁴

Zdravko Mitev, Dipl. Eng.

Wintel deep technical support engineer , Hewlett Packard Enterprise, Sofia, Bulgaria
E-mail: zdravko.mitev1@gmail.com

Siana H. Valchanova, Dipl. Eng.

PhD Student at Department of Computer Science and Technology
Technical University of Varna
E-mail: Siqna_valchanova@abv.bg

Veneta P. Aleksieva, PhD

Assoc. Professor at Department of Computer Science and Technology
Technical University of Varna
E-mail: VAleksieva@tu-varna.bg

***Abstract:** In this paper is proposed tools for monitoring and management of virtual infrastructures based on Zabbix- monitoring of websites, filling in host's information, monitoring of processes in Windows services, sending of notifications to Gmail customers, monitoring an Apache server, monitoring the size of the Recycle bin- and real-time monitoring of additional devices attached to a given host, etc.*

The results show that these tools are completely appropriate for a large virtual infrastructure with critical devices. This platform completely ensures the constant monitoring, the timely notification of all responsible users when a problem occurs and it overcomes the problem using of external user's scripts.

***Keywords:** Virtualization, Network Monitoring, Network Management, Zabbix.*

ВЪВЕДЕНИЕ

Все по-широкото навлизане на съвременни софтуерни решения като виртуализацията и облачните технологии се налага от нуждата за повишаване на производителността при намаляване на общата цена на притежание на системите. Освен това, чрез сървърна консолидация и едновременна работа на няколко операционни системи и множество приложения на една и съща машина се опростява работата на информационната инфраструктура в компаниите [1].

Според Gartner, Inc. световният пазар на x86 сървърната виртуализация се очаква да достигне \$ 5,6 милиарда през 2016 г., което представлява увеличение от 5,7% спрямо 2015г. [2], като това увеличение се дължи на намаляване на разходите за поддръжка. Според Dell към настоящия момент фокусът от хипервайзора, като решение за виртуални машини върху една платформа, е изместен към аспекти на виртуализацията като преносимост, управление и автоматизация [3].

Съблюдаването на различните изисквания за допустимо (критично) време за отговор от различните приложения, се осигурява от задължително изпълнение на функции по мониторинг и контрол, чрез събиране на нужната информация с минимален обем на обменяните данни между наблюдаваните и управлявани обекти. В настоящия доклад се предлага решение за управление и мониторинг на виртуална мрежова инфраструктура, разработено на база на Zabbix [6].

¹⁴⁴Presented a plenary report of October 28, 2016 with the original title: ПЕРСОНАЛИЗИРАНО НАБЛЮДЕНИЕ И УПРАВЛЕНИЕ НА ВИРТУАЛНИ ИНФРАСТРУКТУРИ НА БАЗА ZABBIX

I. СЪЩЕСТВУВАЩИ РЕШЕНИЯ

Задължителна част от прецизното и ефективно наблюдение на виртуалната инфраструктура са: мониторинг на цялата мрежа, отстраняване на проблеми и за висококачествено обслужване на клиентите, съобщаване за всички открити грешки и проблеми, и посочване на засегнатата система, за да се гарантира нейното бързо възстановяване. Съществуват редица решения, реализиращи виртуализация, с все по-моцнен инструментариум за нейното наблюдение, уведомление и управление.

Windows Server 2008 Hyper-V [4] е решение за виртуализация, което улеснява създаването на виртуални машини. Hyper-V предлага на клиентите надеждна, мащабируема и високопроизводителна виртуализационна платформа, която вече е част от ИТ инфраструктура и позволява консолидирането на най-натоварените сектори.

VMware vSphere [5], първата "cloud" операционна система, използва възможностите на виртуализацията за трансформиране на информационните центрове в значително по-опростена "cloud" компютърна инфраструктура и позволява на ИТ организациите да предоставят ново поколение от гъвкави и сигурни ИТ услуги.

Zabbix [6] е enterprise-class софтуер с отворен код, предоставящ възможност за реализация на система за мониторинг на физически и виртуални мрежи. Той следи множество параметри на мрежата – състоянието, показателите на сървърите и други. Zabbix е безплатна платформа и е написан и се разпространява под GPL General Public License version 2 лиценз.

Nagios [7] е безплатна платформа, която осигурява мониторинг на всички критични инфраструктурни компоненти, включително приложения, услуги, операционни системи, мрежови протоколи и мрежова инфраструктура.

В таблица 1 са представени характеристиките на Zabbix и Nagios. Видно е, че Zabbix притежава по-широк спектър от възможности за наблюдение и управление на мрежовите инфраструктури.

Таблица 1. Предимства и недостатъци на Zabbix и Nagios

	Zabbix	Nagios
Специфични предимства	<ul style="list-style-type: none"> • Интуитивен уеб интерфейс • Агент работещ на Windows, OS X, Linux, FreeBSD, etc • Постъпков уеб мониторинг • Може да сравнява множество обекти • Системни "темплейти" • Мониторинг на лог файлове • Мониторинг на прокси • Персонализирани екрани • Репорти в реално време 	<ul style="list-style-type: none"> • Множество нива на известяване: ERROR, WARNING, OK • "Flapping" управление • Извежда автоматично топологията • Пълен stand-alone, без нужда от допълнителен софтуер • Мониторинг на уеб съдържание
Общи предимства	<ul style="list-style-type: none"> • С отворен код • Позволяват персонализация на мониторинга и управлението • Обслужват всички протоколи- HTTP, FTP, SSH, POP3, SMTP, SNMP, MySQL... • Изпраща аларми на e-mail и/или SMS 	
Специфични недостатъци	<ul style="list-style-type: none"> • Труден за инсталация и конфигурация • Ескалациите са странни • Невъзможност за "flapping" управление • Ограничена документация • Използва бази данни (като MySQL) 	<ul style="list-style-type: none"> • Нуждае се от SSH достъп за да мониторира отдалечени системи • Ограничен уеб интерфейс • Невъзможност за смяна на мониториращите инстанции

II. ПЕРСОНАЛИЗИРАН МОНИТОРИНГ СЪС ZABBIX

Конфигурациите за мониторинг са централизирани в Zabbix сървър, което улеснява управлението на Zabbix агента.

Zabbix агентът поддържа два режима на работа: пасивна и активна проверка. Той може да извършва проверки на базата на фиксиран интервал, но е възможно да се заложи и определено време за стартиране на проверката. В пасивна проверка Zabbix сървърът (или прокси) изисква стойност от Zabbix агента (например натоварване на процесора), след което агентът обработва заявката и връща стойността. При активна проверка Zabbix агентът изисква от Zabbix сървър (или прокси) списък с активните проверки и изпраща резултатите периодично. Вградената функционалност на Zabbix агента може да бъде разширена чрез зареждаеми модули, потребителски параметри и други.

VMware мониторингът в Zabbix дава възможност за автоматично откриване на хипервайзори и виртуални машини, както и мониторинг на VMware vCenter и vSphere инсталации за различни хипервайзори. Zabbix може да използва правило за търсене на ниско ниво, за да открие автоматично VMware хипервайзори и виртуални машини. Наборът от данни по подразбиране в Zabbix предлага няколко готови за използване шаблони за мониторинг на VMware vCenter и vSphere. Тези шаблони съдържат предварително конфигурирани правила, както и редица вградени проверки за мониторинг на виртуални инсталации. В допълнение към вградените проверки в Zabbix е възможно да бъдат създадени и персонализирани проверки.

Zabbix агентът притежава и способността да изпълнява потребителски скриптове. Така функционалността му може да бъде увеличена според персоналните потребности на съответната виртуална инфраструктура чрез създаване на скриптове, написани на Shell script, Perl, Python, Ruby и т.н. Zabbix има няколко предварително определени метода за доставка на известия - чрез е-мейл, SMS (при наличие на GSM модем), посредством Jabber и чрез използване на потребителски скрипт. Той предоставя пълен работен поток: изпращане на уведомления, позволяващи потвърждение на получената информацията, прехвърляне на информация към други потребители, както и способност да се предприемат действия.

III. ЕКСПЕРИМЕНТАЛНИ ИЗСЛЕДВАНИЯ И РЕЗУЛТАТИ

За тестова реализация на системата са използвани Linux сървър с дистрибуция OpenSuse v.13.1 и тестова машина с Windows Server 2008. И двете машини са виртуални и работят върху VMWare ESX сървър. На Linux сървър са инсталирани Zabbix server, Zabbix agent, Zabbix frontend, Postfix mail server, MySQL database, Apache server, SNMP server, Уеб браузър без графичен интерфейс и текстов редактор. На Windows Server 2008 е инсталиран SNMP сървър и е конфигурирана възможността Zabbix агента да изпраща съобщения към адреса на Zabbix сървър.

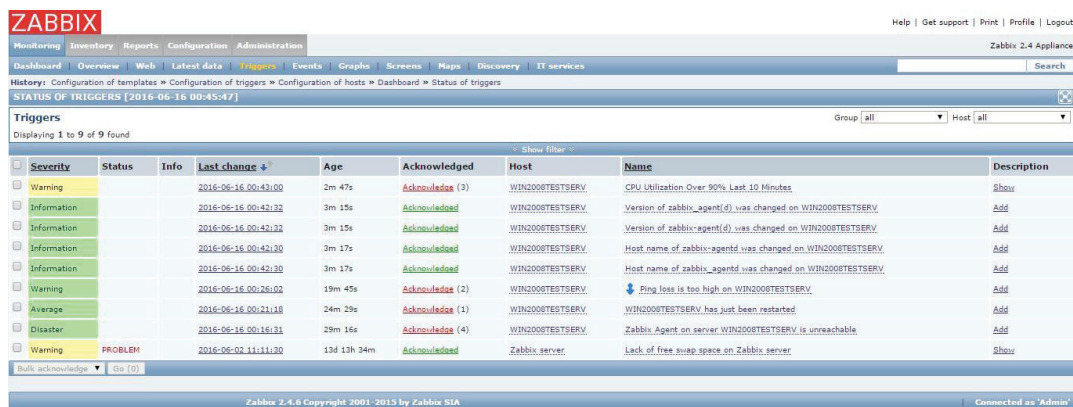
За целите на експерименталните изследвания за да се реализира наблюдение и управление на виртуална структура с критични компоненти, са разработени следните скриптове:

1. Автоматично въвеждане на информация за хоста в Zabbix frontend-a- за целта е създаден темплейт, който се подава на всеки новосъздаден хост. Темплейтът позволява във всеки обект да се конфигурира име на обекта, тип, ключ, тип на информацията, време за опресняване, часови интервал, брой дни за запис на история и др. След промяна на информацията за даден хост, Zabbix сървър изпраща мейл до потребителите в групата на администраторите. На фиг.1 е представено добавянето на хост преди и след изпълняване на скрипта.



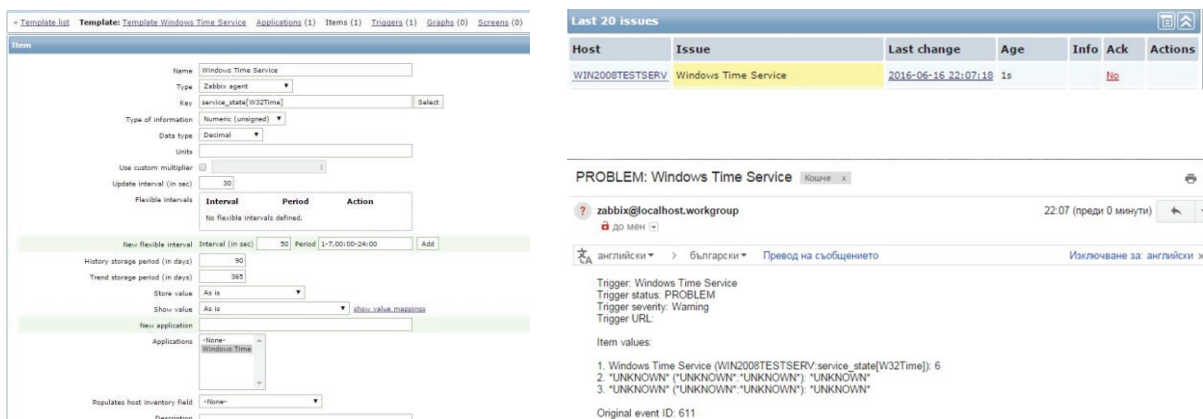
Фиг.1 Автоматично въвеждане на информация за хоста в Zabbix frontend-a

2. Следене на процеси, като ring до хост, ниво на използване на процесора, работа на Apache сървъра и нотификации- Реализирани са посредством конфигуриране на тригери с подадени параметри от клиентската система. Мониторинг и нотификации относно работата на Apache уеб сървъра са представени на фиг.2. Нотификациите могат да бъдат изключени, потвърдени или игнорирани през Zabbix frontend-a.



Фиг.2 Автоматично следене на ring до сървъра и натоварване на процесора

3. Следене работата на процесите в Windows Services – Реализирани са с VB скрипт, който следи състоянието на всички процеси в операционната система на клиента (хоста). Отново се използват обекти за всеки от процесите. Например, при процеса Windows time тригерът се опреснява на всеки 30sec и известява всички конфигурирани клиенти на Zabbix frontend-a.(фиг.3)



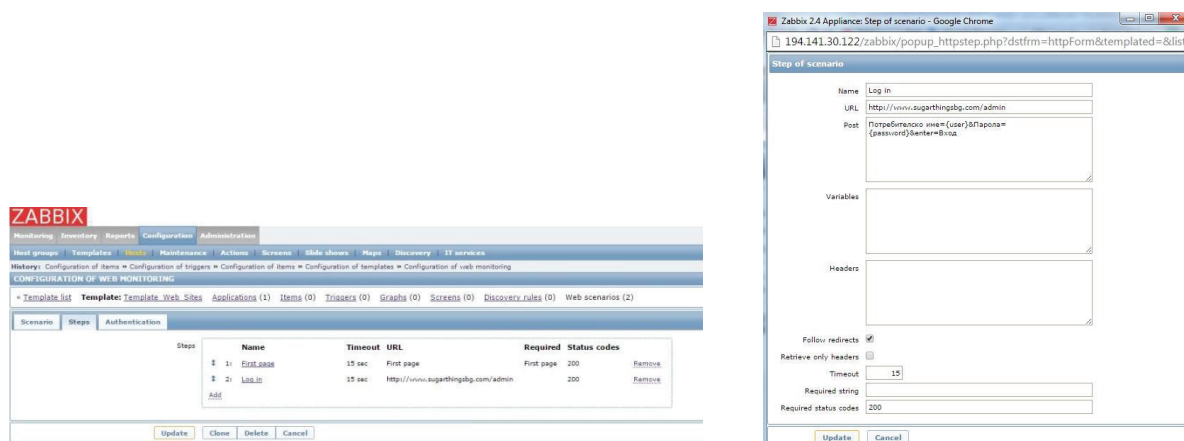
Фиг.3 Реализация на следене на Windows time Services

4. Мониторинг на уеб сайт в реално време - Директно през Zabbix сървъра е реализиран чрез темплейт, който е създаден така, че да изпълнява постъпково сценарий и при неуспешно направена стъпка да известява потребителите. Като променливи се задават имената на кутиите за въвеждане на потребител и парола, за да се реализира реален вход в дадена CMS система.

Един от реализираните сценарии (фиг.4) е следния:

4.1. Тест за достъпност на страница – за отговор връща код 200 и продължава към следващата стъпка

4.2. Тест за успешно логване – при подадени валидни параметри (потребител и парола) ги въвежда в съответните текстови кутии. При успешен вход, за да се валидира, се търси ръчно въведен предварително стринг (в случая търси „Идентифицирали сте се“) и ако го намери връща код 200.



Фиг.4. Сценарий за мониторинг на Уеб сайт в реално време

5. Водене на одит лог- Създаденият скрипт записва в текстов файл- лог одит всяка промяна идваща, както от сървъра, така и от хостовете (фиг.5).

Time	User	IP	Resource	Action	ID	Description	Details
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13914	Symantec has items in Quarantine	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13911	Windows mountpoint on {HOST.NAME} in % is:	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13943	{HOST.NAME} - DHCP Database Error - System Ev. 1016	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13975	Symantec Network Access Control Service - Stopped	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13936	File Replication Service Log SECURITY	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13954	System Log SECURITY	
2016-06-15 23:23:46	Admin	194.12.225.231	Host	Added	10123	WIN2008SERVTEST	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13929	Directory Service Log INFORMATION	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13966	Avg Write Operation to Disk Exceeds 50ms in last 10 Min	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13982	Symantec Endpoint Protection Service - Stopped	
2016-06-15 23:23:46	Admin	194.12.225.231	Trigger	Added	13918	Zabbix agent on {HOST.NAME} is unreachable for 5 minutes	

Фиг.5. Лог одит файл

ЗАКЛЮЧЕНИЕ

В доклада е предложено решение, реализиращо няколко скрипта за пълноценно и качествено следена на виртуални инфраструктури - за мониторинг на уеб сайтове, попълване на информация за хоста (клиента), следене на процеси в Windows services, изпращане на нотификации към Gmail клиенти, мониторинг на Apache сървър, следене

големината на Recycle bin-а в реално време, следене на допълнително закачени устройства към даден хост.

Получените резултати доказват, че за големи инфраструктури с критични устройства е най-подходяща употребата на Zabbix. Тази платформа категорично гарантира постоянен мониторинг, навременно уведомяване на всички отговорни потребители при възникване на проблем, както и неговото отстраняване, чрез използване на външни потребителски скриптове.

Като насока за бъдещо развитие на системата се планира да се направи реализация за управление на хардуерна инфраструктура и по-специално мониторинг на UPS устройства, свързани с нея. Идеята е при постъпване на сигнал по SNMP, идващ от UPS устройството да се активира външен скрипт на отдалечения клиент през Zabbix агента, който да изключи физическата или виртуалната машина, без да предизвиква загуби или проблеми при последващо стартиране.

ЛИТЕРАТУРА

[1] Angeles S., Virtualization vs. Cloud Computing: What's the Difference, <http://www.businessnewsdaily.com/5791-virtualization-vs-cloud-computing.html>, 2014.

[2] Moore S., Gartner Says Worldwide Server Virtualization Market Is Reaching Its Peak, Gartner Inc., <http://www.gartner.com/newsroom/id/3315817>, 2016.

[3] Kirsch B., Server virtualization trends will de-emphasize hypervisor in 2016, <http://searchservvirtualization.techtarget.com/feature/Server-virtualization-trends-will-de-emphasize-hypervisor-in-2016>, 2016.

[4] Microsoft® Hyper-V™ Server 2008 R2, <https://www.microsoft.com/en-us/download/details.aspx?id=3512>.

[5] vSphere and vSphere with Operations Management, <http://www.vmware.com/products/vsphere.html>.

[6] Zabbix- The Enterprise-class Monitoring Solution for Everyone, <http://www.zabbix.com/>.

[7] Nagios- The Industry Standard In IT Infrastructure Monitoring, <https://www.nagios.org/>.