Taak 1: Actualiteit

Enterprise Linux 15-16

Bachelor toegepaste informatica, HoGent Bedrijf en Organisatie

Inhoudsopgave

1 Opdrachtomschrijving

Bij elke rol in de ict-sector is het voortdurend bijwerken van je vakkennis onontbeerlijk om de snelle evolutie in je vakgebied bij te kunnen benen. In Linux systeembeheer is dat niet anders. Wat ons vakgebied kenmerkt is een uitgesproken wil om informatie en kennis te delen. Er is dan ook een schat van informatie te vinden over de meest recente evoluties via blogs, conferenties waarvan de lezingen op Youtube of Vimeo gepubliceerd zijn, enz.

De bedoeling van deze taak is aan te tonen dat je deze evoluties ook opvolgt en probeert toe te passen in de praktijk. Dat toon je aan op drie manieren die verderop in detail worden toegelicht:

- Hou de kennis die je opdoet bij aan de hand van cheat-sheets en checklists
- Probeer een recentelijk gepubliceerde techniek, tool, ... uit in het kader van de Labo-opdrachten
- Doe een bijdrage aan een open source project gerelateerd aan de cursus

Je mag hier tijdens de contacturen aan werken en het is interessant als je kan samenwerken met één of meerdere medestudenten.

1.1 Cheat-sheets en checklists

Wanneer je niet gewend bent om met Linux te werken, dan is het niet evident om op te zoeken en te onthouden welke commando's je nodig hebt voor welke taak. Via Google vind je wel vaak een oplossing, maar dat ligt niet altijd voor de hand. Er zijn bijvoorbeeld recentelijk substantiële wijzigingen doorgevoerd in de architectuur van de belangrijkste Linux-distributies waardoor bepaalde commando's (die je erg vaak tegenkomt bij Googlen) niet meer werken.

Om jezelf te helpen bij het onthouden van de belangrijkste commando's, is het bijhouden van een cheat-sheet of "spiekbriefje" een nuttig hulpmiddel. Als je een bepaald commando een paar keer bent moeten gaan opzoeken, dan is het best dat eens te noteren zodat je het in de toekomst sneller terugvindt en op de duur ook beter onthoudt.

Hetzelfde geldt voor procedures van handelingen die steeds terugkomen. Bijvoorbeeld, als je wil nagaan of de IP-instellingen van een host kloppen, gebruik je altijd dezelfde commando's. Wanneer je die telkens opnieuw moet gaan opzoeken verspil

je tijd en het is best mogelijk dat je zo zaken over het hoofd ziet. Door checklists bij te houden, verminder je het opzoekwerk en kan je ook vlotter werken (Simmons, 2009).

In je repository vind je onder `doc/` een bestand `cheat-sheet.md` dat een aanzet geeft. Er zijn alvast enkele nuttige commando's in opgenomen, maar je kan dit zelf aanpassen naar je eigen smaak. Als het document te groot wordt, kan je het opsplitsen in verschillende bestanden. Je kan nog meer inspiratie opdoen op deze Github-repository waar een aantal cheat-sheets en checklists gepubliceerd zijn: https://github.com/bertvv/cheat-sheets.

Bij de evaluatie wordt er rekening mee gehouden hoe je deze documenten hebt bijgehouden in de loop van het jaar (aan de hand van de commit log).

1.2 Nieuwe technieken uitproberen

Zoals eerder aangegeven, vormen Linux-systeembeheerders een "community" waar er veel informatie uitgewisseld wordt. Sommigen gieten zaken die ze bijleren in een blog-artikel, gaan erover spreken op conferenties, enz.

De bedoeling hier is om zo'n artikel of lezing toe te passen op de labo-opdracht. Een paar voorbeelden als inspiratie:

- Hayden (2015) en Davila (2015) beschrijven een manier om RHEL/CentOS-systemen te testen op vlak van beveiliging, gebaseerd op Ansible. Is het mogelijk dat toe te passen op onze systemen? In het artikel gaat het over versie 6, terwijl wij op versie 7.1 zitten. In hoeverre kan dit aangepast worden?
- Fail2ban is een Intrusion Prevention System dat een server kan beschermen tegen brute-force of denial of service-aanvallen (Sawiyati, 2014). Kan je dit toepassen op onze servers? Het is uiteraard wel de bedoeling dit via Ansible te doen. Dat kan hetzij via een bestaande rol (zie Ansible Galaxy), die je zo nodig aanpast, hetzij één die je zelf schrijft.
- Secure Shell is de standaard manier om Linux-servers op een veilige manier van over het netwerk te beheren. Maar volgens stribika (2015) is het mogelijk om `sshd` nog beter te beveiligen. Kan je dit toepassen op onze servers?
- Zoals onze opstelling nu is, zullen wachtwoorden in de `host_vars` of `group_vars` bestanden opgeslagen worden. Dit is niet ideaal: we steken onze code in een versiebeheersysteem, maar wachtwoorden horen daar met het oog op beveiliging helemaal niet in thuis. Ansible heeft hiervoor een oplossing: Ansible Vault. Blanc (2015) beschrijft een methode om het gebruik van Ansible Vault zo transparant mogelijk te maken. Kan je het toepassen in onze opstelling?
- Johnson (2015) schreef een artikel over het versnellen van Ansible. Kloppen zijn aanbevelingen? Kan je dat aantonen, m.a.w. het tijdverschil meten tussen de standaardinstellingen en zijn aanpassingen?

Je kan de blogs waar naar gerefereerd werd in deze voorbeelden opvolgen (bv. via een RSS reader), hieronder volgen er nog enkele:

- AT Blog: http://www.atcomputing.nl/blog/
- Erika Heidi: http://erikaheidi.com/blog/
- Everything Sysadmin (Tom Limoncelli): http://everythingsysadmin.com/
- Everything is a Freaking DNS Problem (Kris Buytaert): http://www.krisbuytaert.be/blog/
- Fedora Magazine: http://fedoramagazine.org/
- Linux Journal: http://www.linuxjournal.com/
- Major.io (Major Hayden): https://major.io/
- ma.ttias.be (Mattias Geniar): https://ma.ttias.be/
- Planet CentOS: http://planet.centos.org/
- Runaway Sequence (Aaron Hunter): http://sharknet.us/
- Standalone Sysadmin (Matt Simmons): https://www.standalone-sysadmin.com/blog/
- SysadminCasts (Justin Weissig): https://sysadmincasts.com/
- The Geek Stuff: http://www.thegeekstuff.com/

Vond je andere interessante blogs? Geef maar door aan de lector! Andere bronnen van informatie zijn Youtube of Vimeo (voor presentaties van conferenties of screencasts), Twitter, enz.

1.3 Bijdrage aan een open source project

Alle tools waar we in de cursus gebruiken zijn open source. Sommige, zoals Ansible, werden door een softwarebedrijf ontwikkeld die daar een businessmodel rond gebouwd hebben. Andere werden door enthousiastelingen in hun vrije tijd ontwikkeld. In elk geval kunnen we gratis gebruik maken van software van hoge kwaliteit, dankzij de inspanningen van velen.

Het is passend daar iets voor terug te doen, dus de bedoeling is om een significante bijdrage te leveren aan een open source project dat gerelateerd is aan de cursus. Dit kan een kleine bijdrage zijn, maar voorwaarde is wel dat ze aanvaard is door de auteur(s) van het project.

Je mag hiervoor samenwerken met één of meerdere medestudenten, maar de individuele bijdrage van elk teamlid moet aantoonbaar zijn (bv. aan de hand van Git commits).

Enkele mogelijkheden:

- OpsSchool http://www.opsschool.org/en/latest/ is een online handboek voor system engineers. Er zijn onderdelen die nog niet ingevuld zijn.
- Op Ansible Galaxy zijn veel rollen te vinden die beter kunnen. Implementeer een nieuwe feature, zorg er voor dat ze op CentOS 7 draaien, verbeter fouten, ... Ook de lector apprecieert hulp bij het verder ontwikkelen van zijn Ansible-rollen https://galaxy.ansible.com/list#/users/8834 en https://github.com/search?q=user%3Abertvv+ansible.
- Schrijf een Ansible rol (waar nog geen alternatief voor CentOS voor bestaat) en publiceer die op Ansible Galaxy. Dit doe je best in samenwerking met één of meerdere medestudent(en)!
- Pas een techniek die beschreven is voor een andere distributie (CentOS 6, Debian, Ubuntu, ...) toe op CentOS 7. In de vorige sectie vind je een paar concrete voorbeelden.

Andere ideeën zijn ook welkom, bespreek die met de lector. De bijdrage die je levert kan samen hangen met de vorige deelopdracht.

2 Referenties

Blanc, M. (2015) *Transparent encryption with ansible vault revisited.* Random stuff: brain dump on sysadmin & DevOps related topics (blog). Opgehaald op 2015-09-16 van https://leucos.github.io/articles/transparent-vault-revisited/

Davila, J. (2015) *Automatically testing and validating the Ansible STIG Role for Red Hat 6.* blog.davila.io. Opgehaald op 2015-09-16 van http://blog.davila.io/posts/automatically-testing-and-validation-the-ansible-stig-role-for-red-hat-6.html

Hayden, M. (2015) *Automated Testing for Ansible CIS Playbook on RHEL/CentOS 6*. Opgehaald op 2015-09-16 van https://major.io/2015/08/05/automated-testing-for-ansible-cis-playbook-on-rhelcentos-6/

Johnson, A. (2015) *Making Ansible a bit faster.* Adam's Tech Blog. Opgehaald op 2015-09-16 van http://adamj.eu/tech/2015/05/18/making-ansible-a-bit-faster/

Simmons, M. (2009) *If you can't script it, use a checklist.* Standalone Sysadmin (blog). Opgehaald op 2015-09-16 van http://www.standalone-sysadmin.com/blog/2009/07/if-you-cant-script-it-use-a-checklist/

Sawiyati (2014) *How to install Fail2ban on CentOS*. ServerMom blog. Opgehaald op 2015-09-19 van http://www.servermom.org/install-fail2ban-centos/1809/

stribika (2015) *Secure Secure Shell.* This is probably not the site you are looking for (blog). Opgehaald op 2015-09-16 van https://stribika.github.io/2015/01/04/secure-secure-shell.html

3 Evaluatie

Deze taak wordt pas aan het einde van het semester geëvalueerd.

Deliverables:

- Cheat sheet(s) en checklist(s) (op Bitbucket) dat in de loop van het semester regelmatig is bijgewerkt
- Verslag met
  - Toelichting van de bijdrage
  - Toelichting van de gekozen aanpak: welke stappen heb je ondernomen?
  - Testplan en testrapport
  - Gebruikte bronnen voor het uitwerken van de opdracht
- Demo

Om de score in de rechterkolom te halen, moet je **alle** taken tot en met de overeenkomstige lijn realiseren.

Taak	Score
Het labo-verslag is tijdig ingediend en volledig	
Er werd een demo gegeven van de realisatie(s)	
Minstens 2 van de 3 deeltaken zijn gerealiseerd	voldoende

Afhankelijk van de kwaliteit van het resultaat en het geleverde werk, krijg je een hogere score.