

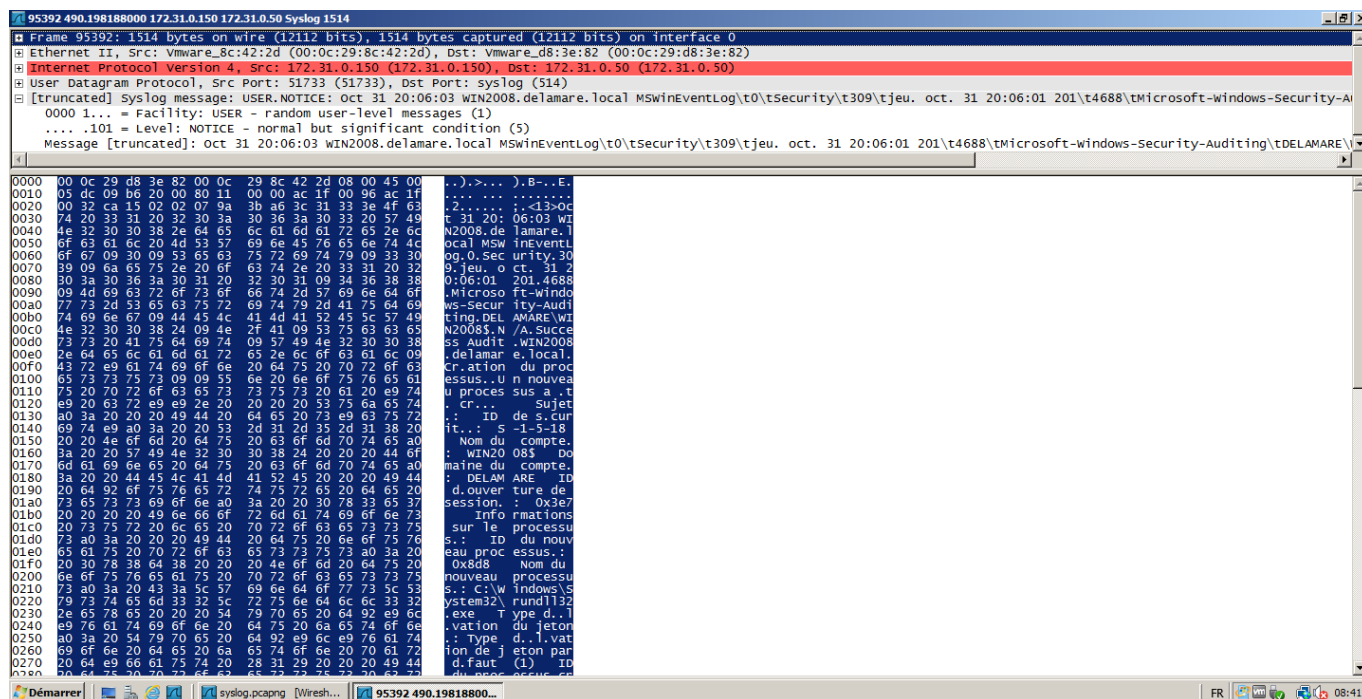
Syslog exercice : Améliorer le paramétrage des applicatifs émetteurs de traces

En vous aidant des documents ci-dessous répondez aux questions suivantes :

- 1) Donner l'adresse du serveur syslog récepteur, l'adresse du serveur émetteur, le port d'écoute utilisé par le serveur de syslog et le protocole utilisé pour le transfert.
- 2) Dire quelle est la priorité du message (en base 10).
- 3) Préciser à quelle date et à quelle heure ce message a été transmis.
- 4) Donner le nom du serveur ayant émis ce message.
- 5) Conclure sur la difficulté d'analyse des messages syslog en cas d'émetteurs différents situés à la même adresse.
 - 6) Proposer, devant l'abondance des messages émis, des modifications dans le paramétrage de Snare afin de faciliter l'analyse.
 - 7) En faisant une synthèse des parties 1 et 2, retrouver sur le diagramme de déploiement les parcours possibles des messages syslog.

Documents de travail

autre message syslog transmis depuis le même serveur et présent dans la même capture de trame



Paramétrage du logiciel Snare

Les OS Windows ne peuvent pas envoyer les logs générés par l'observateur d'événements vers un serveur syslog.

Le logiciel [Open Source Snare](#) permet d'envoyer des messages **syslog**.

The screenshot shows the 'SNARE for Windows' web interface. The main heading is 'SNARE Network Configuration'. Below this, it states: 'The following network configuration parameters of the SNARE unit is set to the following values:'. A table lists various configuration options with their current values:

Override detected DNS Name with:	
Destination Snare Server address	172.31.0.50
Destination Port	514
Perform a scan of ALL objectives, and display the maximum criticality?	<input type="checkbox"/>
Allow SNARE to automatically set audit configuration?	<input checked="" type="checkbox"/>
Allow SNARE to automatically set file audit configuration?	<input type="checkbox"/>
Export Snare Log data to a file?	<input checked="" type="checkbox"/>
Enable SYSLOG Header?	<input checked="" type="checkbox"/>
SYSLOG Facility	User
SYSLOG Priority	Notice

Buttons for 'Change Configuration' and 'Reset Form' are visible. A dropdown menu for 'SYSLOG Priority' is open, showing options: Emergency, Alert, Critical, Error, Warning, Notice (selected), Information, Debug, and DYNAMIC. The footer of the page reads: '(c) Intersect Alliance Pty Ltd 1999-2011. This site is powered by SNARE'.

La visualisation des messages via l'interface web du serveur de traces centralisé

The screenshot shows the 'Php-Syslog-NG 2.9.1: REGULAR RESULTS' interface in Mozilla Firefox. The page title is 'Php-Syslog-NG 2.9.1 Unstable [cdukes] 16-Jun-2006 16:00 EST'. It includes a search bar and a 'SEVERITY LEGEND' with categories: DEBUG, INFO, NOTICE, WARNING, ERROR, CRIT, ALERT, EMERG.

The SQL query used is: `SELECT SQL_CALC_FOUND_ROWS * FROM logs WHERE host not in ('WIN2008') and msg like '%Win2008.'`

SEQ	HOST	FACILITY	DATE TIME	MESSAGE
33167	WIN2008.delamare.local	user-notice	2013-11-02 09:06:03	nov. 02 09:06:01 201#0114688#011Microsoft-Windows-Security-Auditing#011DELMARE#WIN2008S#011N/A#011Success Audit#011WIN2008.delamare.local#011Création du processus#011#011Un nouveau processus a été créé. Sujet : ID de sécurité : S-1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Informations sur le processus : ID du nouveau processus : 0xd38 Nom du nouveau processus : C:\Windows\System32\cmd.exe Type d'élevation du jeton : Type d'élevation de jeton par défaut (1) ID du processus créateur : 0x58c Le type d'élevation du jeton indique le type de jeton qui a été attribué au nouveau processus conformément à la stratégie de contrôle du compte d'utilisateur. Le type 1 est un jeton complet sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton complet est uniquement utilisé si le contrôle du compte d'utilisateur est désactivé, ou si l'utilisateur est le compte d'administrateur intégré ou un compte de service. Le type 2 est un jeton aux droits élevés sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton aux droits élevés est utilisé lorsque le contrôle de compte d'utilisateur est activé et que l'utilisateur choisit de démarrer le programme en tant qu'administrateur. Un jeton aux droits élevés est également utilisé lorsqu'une application est configurée pour toujours exiger un privilège administratif ou pour toujours exiger les privilèges maximum, et que l'utilisateur est membre du groupe Administrateurs. Le type 3 est un jeton limité dont les privilèges administratifs sont supprimés et les groupes administratifs désactivés. Le jeton limité est utilisé lorsque le contrôle de compte d'utilisateur est activé, que l'application n'exige pas le privilège administratif et que l'utilisateur ne choisit pas de démarrer le programme en tant qu'administrateur#011325
33168	WIN2008.delamare.local	user-notice	2013-11-02 09:06:03	nov. 02 09:06:01 201#0114688#011Microsoft-Windows-Security-Auditing#011DELMARE#WIN2008S#011N/A#011Success Audit#011WIN2008.delamare.local#011Fin du processus#011#011Un processus est terminé. Sujet : ID de sécurité : S-1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Informations sur le processus : ID du processus : 0xd38 Nom du processus : C:\Windows\System32\cmd.exe Etat de fin : 0x0#011326
33164	WIN2008.delamare.local	user-notice	2013-11-02 09:01:03	nov. 02 09:01:01 201#0114688#011Microsoft-Windows-Security-Auditing#011DELMARE#WIN2008S#011N/A#011Success Audit#011WIN2008.delamare.local#011Création du processus#011#011Un nouveau processus a été créé. Sujet : ID de sécurité : S-1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Informations sur le processus : ID du nouveau processus : 0xd38 Nom du nouveau processus : C:\Windows\System32\cmd.exe Type d'élevation du jeton : Type d'élevation de jeton par défaut (1) ID du processus créateur : 0x58c Le type d'élevation du jeton indique le type de jeton qui a été attribué au nouveau processus conformément à la stratégie de contrôle du compte d'utilisateur. Le type 1 est un jeton complet sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton complet est uniquement utilisé si le contrôle du compte d'utilisateur est désactivé, ou si l'utilisateur est le compte d'administrateur intégré ou un compte de service. Le type 2 est un jeton aux droits élevés sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton aux droits élevés est utilisé lorsque le contrôle de compte d'utilisateur est activé et que l'utilisateur choisit de démarrer le programme en tant qu'administrateur. Un jeton aux droits élevés est également utilisé lorsqu'une application est configurée pour toujours exiger un privilège administratif ou pour toujours exiger les privilèges maximum, et que l'utilisateur est membre du groupe Administrateurs. Le type 3 est un jeton limité dont les privilèges administratifs sont supprimés et les groupes administratifs désactivés. Le jeton limité est utilisé lorsque le contrôle de compte d'utilisateur est activé, que l'application n'exige pas le privilège administratif et que l'utilisateur ne choisit pas de démarrer le programme en tant qu'administrateur#011323
33165	WIN2008.delamare.local	user-notice	2013-11-02 09:01:03	nov. 02 09:01:01 201#0114688#011Microsoft-Windows-Security-Auditing#011DELMARE#WIN2008S#011N/A#011Success Audit#011WIN2008.delamare.local#011Fin du processus#011#011Un processus est terminé. Sujet : ID de sécurité : S-1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Informations sur le processus : ID du processus : 0xd38 Nom du processus : C:\Windows\System32\cmd.exe Etat de fin : 0x0#011324
33162	WIN2008.delamare.local	user-notice	2013-11-02 09:00:56	nov. 02 09:00:55 201#0114688#011Microsoft-Windows-Security-Auditing#011WIN2008Administrateur#011N/A#011Success Audit#011WIN2008.delamare.local#011Création du processus#011#011Un nouveau processus a été créé. Sujet : ID de sécurité : S-1-5-21-241459311-4228339857-3661958750-500 Nom du compte : Administrateur Domaine du compte : WIN2008 ID d'ouverture de session : 0x526da Informations sur le processus : ID du nouveau processus : 0x4fa Nom du nouveau processus : C:\Program Files\Internet Explorer\iexplore.exe Type d'élevation du jeton : Type d'élevation de jeton par défaut (1) ID du processus créateur : 0xcfc Le type d'élevation du jeton indique le type de jeton qui a été attribué au nouveau processus conformément à la stratégie de contrôle du compte d'utilisateur. Le type 1 est un jeton complet sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton complet est uniquement utilisé si le contrôle du compte d'utilisateur est désactivé, ou si l'utilisateur est le compte d'administrateur intégré ou un compte de service. Le type 2 est un jeton aux droits élevés sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton aux droits élevés est utilisé lorsque le contrôle de compte d'utilisateur est activé et que l'utilisateur choisit de démarrer le programme en tant qu'administrateur. Un jeton aux droits élevés est également utilisé lorsqu'une application est configurée pour toujours exiger un privilège administratif

From: / - Les cours du BTS SIO

Permanent link: /doku.php/sir3/syslog_03

Last update: 2014/11/24 10:26

