Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

CONCOURS EXTERNE
DE TECHNICIEN DE CLASSE NORMALE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

- SESSION 2017 -

Mardi 12 septembre 2017

Option « solutions logicielles et systèmes d'information »

Traitement de questions et résolution de cas pratiques, à partir d'un dossier, portant sur l'une des deux options suivantes choisies par le candidat le jour de l'épreuve :
- infrastructures et réseaux,
- solutions logicielles et systèmes d'information.

Cette épreuve permet d'évaluer le niveau de connaissances du candidat, sa capacité à les ordonner pour proposer des solutions techniques pertinentes et à les argumenter.

Le dossier ne peut excéder 20 pages.

(Durée : 3 heures – Coefficient 2)

Le dossier documentaire comporte 16 pages.

IMPORTANT

IL EST RAPPELE AUX CANDIDATS QU'AUCUN SIGNE DISTINCTIF NE DOIT APPARAITRE NI SUR LA COPIE NI SUR LES INTERCALAIRES.

ECRIRE EN NOIR OU EN BLEU - PAS D'AUTRE COULEUR

SUJET

QUESTIONS

Les réponses devront être rédigées. L'ensemble des questions sera noté sur 10 points.

Question 1 : Que signifie le sigle P2V ?

Question 2 : Que signifie « flasher le BIOS » ?

Question 3 : Définissez la notion de logiciel « Open Source » ?

Question 4 : Qu'est-ce qu'une base de données relationnelle ?

Question 5 : En téléphonie, qu'apporte la 4G par rapport à la 3G ?

Question 6 : Définissez le terme « rançongiciel ». Wanna Cry en est-il un ?

Question 7 : Définissez le terme « cartographie applicative ».

Question 8 : Qu'est-ce que le code ASCII ?

Question 9 : Qu'est-ce qu'une architecture trois tiers ?

Question 10 : Dans le monde du Cloud Computing, que signifie le terme IAAS ?

CAS PRATIQUES

Vous êtes affecté.e à la Direction des Systèmes d'Information et de Communication (DSIC) du Ministère de l'Intérieur, dans une équipe de technicien.ne.s de support de proximité dont le rôle est de dépanner les usager.ère.s de votre site de rattachement.

Cas 1 : (5 points)

Un.e agent.e vous contacte car il/elle constate que son ordinateur est infecté par un virus.
Quelle procédure allez-vous appliquer pour éviter que le virus ne se propage et pour nettoyer le poste bureautique de l'agent.e ?

Cas 2 : (5 points)

Afin de lister les systèmes d'exploitation et les références des ordinateurs déployés sur votre site de rattachement, votre chef.fe de section souhaite disposer de l'inventaire exact. Cela lui permettra de constater l'hétérogénéité du parc informatique, tant logiciel que matériel, de souligner les postes non maintenus et de préparer au mieux les budgets de remplacement.
Expliquez la méthode utilisée pour obtenir et mettre à la disposition de votre chef.fe de section cet inventaire.

Dossier documentaire :

Document 1	La TMA, qu'est-ce que c'est ? http://reseau-informatique.prestataires.com/conseils/tma	Pages 1 à 2
Document 2	Cadre de Cohérence Technique : Référentiel des produits (extrait) http://mgmsic.minint.fr/index.php/documentation-de-reference/cadre-de-coherence-technique-cct#Coeur Version 2.7.3 du 15/06/2016	Pages 3 à 7
Document 3	Les 6 différents types de Virus informatique les plus dangereux https://www.pcsansvirus.com/pages/securite-informatique/les-6-differents-types-de-virus-informatique-les-plus-dangereux-expliquer.html 03 avril 2017	Pages 8 à 9
Document 4	Sécurité : Linux attaquable sans une seule ligne de code http://www.silicon.fr/securite-linux-attaquable-sans-une-seule-ligne-de-code-163468.html 24 novembre 2016, Christophe Lagane	Page 10
Document 5	Réaliser un inventaire physique http://www.isilog.fr/sites/default/files/pdf/fiches_methodes/IWS%20air%20design%20M%C3%A9thodologie%20inventaire%20V01.pdf ISILOG, 2015	Page 11 à 12
Document 6	Que faire si mon ordinateur est infecté ? https://securelist.fr/threats/que-faire-si-mon-ordinateur-est-infecte/	Pages 13 à 15
Document 7	Windows Server Update Services https://fr.wikipedia.org/wiki/Windows_Server_Update_Services 26 avril 2017	Page 16

http://reseau-informatique.prestataires.com/conseils/tma

La TMA, qu'est-ce que c'est ?

La tierce maintenance applicative (TMA) place la maintenance des applications entre les mains d'un tiers. Une source de sérénité pour l'entreprise.

Définition

La TMA ou tierce maintenance applicative consiste à externaliser la maintenance de tout ou partie des applications d'une entreprise auprès d'un prestataire. Celui-ci se voit transférer la responsabilité de l'infogérance des applications d'une entreprise, de leur performance et de leur disponibilité. Dans ce cadre de cette prestation, il a la charge également d'ajuster les applications aux besoins de l'entreprise avec qui il est sous contrat. En revanche, la TMA n'implique pas le développement de nouvelles fonctionnalités.

Principe de la TMA

La tierce maintenance applicative repose sur le principe d'externalisation. Dans le cadre de la TMA, cette externalisation est partielle. Au lieu de placer l'ensemble des processus métiers entre les mains d'un prestataire (comme c'est le cas lors du Business Process Outsourcing), l'entreprise choisit de confier la maintenance de son seul parc applicatif. Le prestataire n'aura à charge que le maintien des performances des applications de l'entreprise ainsi que de leur optimisation et leur disponibilité.

A noter :
Le principe de la TMA rejoint ainsi celui du Saas (Software-as-a-service). Pour l'entreprise, le Saas consiste à consommer des applications hébergées dans un centre de données. L'accès à ces applications Saas s'effectue via un simple navigateur. Ces applications ne sont plus installées en interne dans l'entreprise. Elle a donc choisi d'externaliser ses applications auprès de l'hébergeur (celui qui maintient le centre de données). Celui-ci devient ainsi le prestataire de maintenance, à la fois des applications et des infrastructures associées.

Objectifs

Souscrire un contrat de TMA auprès d'un prestataire permet à l'entreprise de :

- maîtriser les coûts de maintenance,
- gagner en agilité,
- avoir à disposition les bonnes ressources et les bonnes compétences,
- se concentrer sur son cœur de métier,
- se libérer des contraintes de maintenance informatique.

Avantages

La TMA offre un certain nombre d'avantages :

- expertise à portée de main en permanence,
- accès à des technologies à la pointe,
- équipes informatiques internes dégagées de la maintenance de certaines applications,
- hausse des performances du SI de l'entreprise.

Inconvénients

Externaliser une partie de ses ressources présente toujours des inconvénients pour une entreprise. Les désagréments liés à la TMA sont :

- la dépendance des fournisseurs,
- les délais de réactivité, parfois longs, dus à des problèmes de communications entre équipes,
- les budgets initiaux parfois alourdis, si le périmètre opérationnel du prestataire n'a pas été clairement défini (notamment au niveau des mises à jour),
- des équipes internes généralement hostiles à l'externalisation

http://mgmsic.minint.fr/index.php/documentation-de-reference/cadre-de-coherence-technique-cct#Coeur

Cadre de Cohérence Technique : Référentiel des produits

CADRE DE COHERENCE TECHNIQUE

Référentiel des produits

Version 2.7.6 du 02/03/2017

Objet du document :
Ce document liste les composants et environnements de référence (versions et états techniques des composants qualifiés, fournisseurs, contextes d'emploi éventuels).

Remarque :

Pour chaque choix effectué, un statut est associé pour préciser le cadre d'utilisation du produit:
- Recommandé : Lettre "R" sur fond vert. Le produit peut être utilisé librement aussi bien pour un nouveau système que pour une intégration ou un portage d'un système existant.
- Migration : Lettre "M" sur fond jaune. Le produit ne peut être utilisé que pour faciliter la migration ou le portage d'un système existant.
- Assujetti : Lettre "A" sur fond mauve. L'utilisation du produit est soumise à autorisation des référents CCT du ministère. Il peut s'agir d'un produit soumis à licence, ou d'un produit dont on ne souhaite la diffusion au sein du ministère [cct@interieur.gouv.fr]
- Observation : lettre "O" sur fond rose. Le produit est prometteur mais pas nécessairement pérenne. Son utilisation du produit est soumise à autorisation des référents CCT du ministère. Ce statut est temporaire, selon le résultat des premières expérimentations, le produit pourra être passé en recommandé, ou en migration avant d'être retiré.
Les combinatoires de composants sont décrites dans l'annexe piles logicielles.
Convention de typographie: Les logiciels libres sont en caractères gras.
Les produits modifiés par rapport à la précédente version du CCT sont en couleur bleue.
Les nouveaux produits sont en couleur verte.
La 6ème colonne ("Supp. LL") indique les logiciels libres supportés par le marché SLL. Voir le commentaire pour d'éventuelles indications complémentaires sur les versions supportées.

Partie 4 : Sécurité & interopérabilité - [SI]

Pour les logiciels pris en charge au marché de support logiciels libres, il est indiqué "Oui" dans la colonne "Supp. LL"

Chapitre 1 : Appliance - [AP]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SI-1291	**Apache mod_security**	**Apache Software Foundation**		R	**Oui**	*Filtrage des flux HTTP et HTTPS et correction des URL mal formés.*
SI-1301	**DansGuardian**	**dansguardian.org**	2.x	R	**Oui**	*Filtrage de contenu*
SI-1026	i-Sentry	Bee Ware	4.2	A		
SI-1027	i-Trust	Bee Ware		A		
SI-1025	Source Fire Sondes IDS	Source Fire		A		

Chapitre 2 : Antivirus - [AV]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SI-1028	**ClamAV**	**clamav.net**		R	**Oui**	*Inscrit au SILL. Pour OS Linux / Unix. Version distribution.*
SI-1318	ePolicy Orchestrator Agent	McAfee	4.8	M		*Logiciel de distribution et de mise à jour de l'antivirus (infrastructure nationale).*
SI-1398	ePolicy Orchestrator Agent	McAfee	5.1	R		*Logiciel de distribution et de mise à jour de l'antivirus (infrastructure nationale)*
SI-1029	Kaspersky	Kaspersky Lab		R		*Contexte d'emploi: périmètre ST(SI)²*
SI-1030	Kaspersky Security Internet Gateway	Kaspersky		R		*Contexte d'emploi: périmètre serveurs messagerie et passerelles Internet DSIC*
SI-1031	Kaspersky Security Mail Server	Kaspersky		R		*Contexte d'emploi: périmètre serveurs messagerie et passerelles Internet DSIC*
SI-1032	LinuxShield	McAfee	1.5	M		
SI-1399	Server Security - Linux	SOPHOS	9.6	R		*Anti-virus serveur linux*
SI-1400	Server Security - Windows	SOPHOS	10.3	R		*Antivirus serveur Windows*
SI-1033	VirusScan	McAfee	8.7.i	M		*Pour poste de travail Windows*
SI-1317	VirusScan	McAfee	8.8	R		*Pour poste de travail Windows*
SI-1034	VirusScan – Linux	McAfee	1.6	M		*Pour poste de travail Linux*
SI-1430	VirusScan – Linux	McAfee	2.0.2	R		*Pour poste de travail Linux - 64 bits uniquement*

Chapitre 3 : Chiffrement - [CH]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SI-1347	**Keepass**	**Dominique Reichl**	2.10	A		*Inscrit au SILL. Version 2.10 testée et validée par l'ANSSI - GNU v2.Arbitrage SHFD et ANSSI attendu.*
SI-1428	**Keepass**	**Dominique Reichl**	2.29	A		*Inscrit au SILL. Version non validée par l'ANSSI. Arbitrage SHFD et ANSSI attendu.*
SI-1252	Security Box	Arkoon Network Security	6.10.0153	A		*Client de chiffrement*
SI-1383	**TrueCrypt**	**truecrypt.org**	7.1a	R		*Client de chiffrement.*
SI-1251	**TrueCrypt**	**truecrypt.org**	6.0a	M		*Incompatible avec Windows 7. Client de chiffrement (version certifiée par l'ANSSI)*
SI-1493	Prim'X Cryhod	Prim'X Technologies (primx.eu)		O		*Outil de chiffrement physique (disque dur..).Remplacement de TrueCrypt.*
SI-1494	Prim'X Zone Central	Prim'X Technologies (primx.eu)		O		*Outil de chiffrement de zone. Associé à l'AD.*

Partie 5 : Poste de travail (Fixe & mobile) - [PT]

Pour les logiciels pris en charge au marché de support logiciels libres, il est indiqué "Oui" dans la colonne "Supp. LL"Les versions de composants indiquées sont celles en vigueur à la date de publication du CCT.
Les alertes de sécurité et les procédures de mise à jour (ou de contournement) sont disponibles sur le portail de la sécurité des systèmes d'information (http://ssi.minint.fr/index.php/les-alertes).

Chapitre 1 : Système d'exploitation - [SE]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
PT-1040	Mac OS	Apple	10	A		
PT-1039	**Linux Ubuntu**	**ubuntu.org**	10.04 LTS	M	**Oui**	
PT-1387	**Linux Ubuntu**	**ubuntu.org**	12.04 LTS	R	**Oui**	*Supporté jusqu'en avril 2017*
PT-1429	**Linux Ubuntu**	**Ubuntu.org**	14.04 LTS	R	**Oui**	*Long Term Support (LTS). Supporté jusqu'en avril 2019.*
PT-1041	Windows	Microsoft	XP Pro SP3	M		
PT-1042	Windows	Microsoft	Windows 7 SP1	R		
PT-1332	Windows	Microsoft	Embedded Compact	A		*Contexte d'emploi limité à l'expérimentation Terminaux légers au SZSIC de Lyon.Composant anciennement dénommé Windows CE.*
PT-1487	Windows	Microsoft	10 Enterprise	O		*La version entreprise est requise dans le cadre d'un SI homologué DR*
PT-1497	**Android**	**Google**		R		*Système d'exploitation d'équipements mobiles (smartphone, tablette)*
PT-1498	SECdroid	ANSSI		R		*Couche de sécurisation pour le système d'exploitation Android*

Chapitre 2 : Socle applicatif - [SA]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
PT-1324	MS Office	Microsoft	2007	M		*à jour des Services Packs et des correctifs de sécurité*
PT-1325	MS Office	Microsoft	2013	A		*à jour des Services Packs et des correctifs de sécurité.Configurer par défaut sur les formats ODF. Version restreinte à Windws 7.*
PT-1488	MS Office	Microsoft	2016	A		*Version d'office associée à Windows 10*
PT-1349	**LibreOffice**	**The Document Foundation / MimO**	Version SILL	R	**Oui**	*Inscrit au SILL. La version en cours est la version interministérielle de référence. cf. site MIMO : http://www.journal-officiel.gouv.fr/mimo/et site DSIC http://telechargement.dsic.mi pour le téléchargement.*
PT-1262	**OCS-inventory**	**ocsinventory-ng.org**	Version SILL	R	**Oui**	*Inscrit au SILL.*
PT-1396	**Firefox**		31 ESR	M	**Oui**	*Version ESR (Extended Support Release) supportée jusqu'au 4 août 2015.*
PT-1427	**Firefox**	**Mozilla**	Version SILL	R	**Oui**	*Inscrit au SILL. La version de Firefox est la version ESR (Extended Support Release) intégrée au poste de travail.*
PT-1046	Internet Explorer	Microsoft	<9	M		*8.x : utilisation sous Windows XP SP3 sans connexion internet*
PT-1330	Internet Explorer	Microsoft	>=9	A		*Toutes versions d'IE >= 9 sont assujetties*

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
PT-1458	**Navigateur AOSP**	**Google**	Version ANSSI	R		*Navigateur fourni dans la version d'AOSP intégrée aux périphériques mobiles. Dernière version validée par l'ANSSI.*
PT-1061	**Thunderbird – Pablo**	**Mozilla.org**	3.1.x	R	**Oui**	*Client de messagerie*
PT-1060	**Thunderbird**	**Mozilla.org**	Version SILL	A	**Oui**	*Inscrit au SILL. Client de messagerie*
PT-1062	Messagerie tactique (gendarmerie)		3.0	R		*Pour les TDG et les TIE dans le contexte Gendarmerie Nationale*
PT-1059	Outlook	Microsoft	2003 SP3	M		*à jour des Services Packs*
PT-1047	**Gnome**	**gnome.org**	2.30.2	R		*Environnement de bureau pour les distributions linux Ubuntu*
PT-1057	**OCS - Agent Linux**	**ocsinventory-ng.org**	Version SILL	R		*Inscrit au SILL. Agent OCS d'inventaire logiciel et matériel pour linux*
PT-1055	**OCS - Agent Windows**	**ocsinventory-ng.org**	2.0.x	R	**Oui**	*Inscrit au SILL. Agent OCS d'inventaire logiciel et matériel pour Windows*
PT-1056	**OCS - Agent Mac**	**ocsinventory-ng.org**	1.1	A		*Agent OCS d'inventaire logiciel et matériel pour Mac*
PT-1331	**Foxit**	**foxitsoftware.com**	7	R		*Lecteur PDF non libre, largement déployé au ministère via mastersation. Lecteurs pdf libres référencés au SILL : Evince pour Linux*
PT-1382	**JRE Java 7**	**Oracle**	1.7.x	A		*Machine virtuelle JAVA.Sous réserve de la compatibilité des applications installées sur le poste de travail, il est recommandé de migrer vers la dernière version éditeur de JRE pour des raisons de sécurité.*
PT-1419	**JRE Java 8**	**Oracle**	1.8	R	**Oui**	*Machine virtuelle java. La version 8 doit être privilégiée. En cas de compatibilité avec certaines applications la version 7 peut être utilisée.*
PT-1327	Adobe Reader X	Adobe	10.1.x	A		*Lecteur PDF. Branche 10 supportée jusqu'au 18 novembre 2015.*
PT-1365	Adobe Reader XI	Adobe	11.x	A		*Lecteur PDF. Par rapport à la version 10.1.x, à choisir en regard des besoins fonctionnels. Branche 11 supportée jusqu'au 15 octobre 2017.*
PT-1431	Adobe Flash Player	Adobe		M		*Plugin animation flash pour firefox et IE - Phase d'obsolescence.*
PT-1328	Adobe Shockwave Player	Adobe	12.x	A		
PT-1298	Jaws	Freedom Scientific		A		*JAWS est un logiciel de revue d'écran pour les personnes mal ou non voyantes pour le système d'exploitation Microsoft Windows.*
PT-1519	**NVDA**	**nvda-fr.org**	Version SILL	R		*Inscrit au SILL. NonVisual desktop Access (NVDA) est un logiciel de revue d'écran pour les personnes mal ou non voyantes, gratuit et à source ouverte pour le système d'exploitation Microsoft Windows.*
PT-1260	**Ultravnc**	**ultravnc.fr**	1.0.9.x	M		*Prise de main à distance - Compatible Windows 7.En environnement Windows, pour des raisons de sécurité, à remplacer progressivement par les outils natifs au poste de travail (Assistance à distance et RDP)*

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SG-1217	MapInfo	Pitney Bowes MapInfo	10	A		*Conception de cartes, géocodage, analyse.*
SG-1220	MapXTreme	Pitney Bowes MapInfo	10	A		*Kit de développement de logiciels MapInfo (versions Java, .Net)*
SG-1224	Push and see	Pitney Bowes MapInfo	10	A		*Développement d'applications cartographiques MapInfo. Interface d'administration s'appuyant sur MapXtreme (gestion du site et publication de cartes)*
SG-1227	SylvanMaps	Sylvan Maps	4	A		*Composant ActiveX de cartographie. Plus maintenu.*

Chapitre 5 : Services d'accès - [SA]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SG-1503	DatAdvantage	Varonis	6	A		*Audit et protection des données. Périmètre réduit à l'administration centrale sous contrôle DSIC.*
SG-1402	**LemonLDAP::NG**	**OW2**	1.3	R	**Oui**	
SG-1356	**LemonLDAP::NG**	**OW2**	1.2	M	**Oui**	*Périmètre DSIC : la version retenue est celle fournie avec les distributions Linux de référence.*
SG-1201	**Kerberos**		5	R	**Oui**	
SG-1354	Validation Server (DVS)	Dictao	4.11	A		*Composant proposant des services de validation de signatures, jetons, et certificats.*

Chapitre 6 : Téléphonie - [TL]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SG-1496	Cryptosmart	Ercom (Ercom.fr)		R		*Solution de téléphonie chiffrée, qualifiée par l'ANSSI, et intégrée à l'offre de service Hesperis-NG de la DSIC*

Chapitre 7 : Gestion de parc – Télé-déploiement/Télédistribution - [GP]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SG-1233	**GLPI**	**glpi-project.org**	Version SILL	R	**Oui**	*Inscrit au SILL.*
SG-1230	CMDB	BMC Software	2	A		
SG-1231	Configuration Discovery	BMC Software	7	A		
SG-1235	Topology Discovery	BMC Software		A		
SG-1333	Kace	Dell		A		*Contexte d'emploi limité à l'expérimentation par la Préfecture de Police*
SG-1234	Qualiparc	PS'SOFT	SP5	A		

Chapitre 8 : Référentiels transverses - [RF]

Chapitre 9 : Qualité des données - [QD]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SG-1236	DataMasker	Cortina		A		*Outil d'anonymisation uniquement compatible avec le SGBD Oracle.*

Chapitre 10 : Gestion de contenu (ECM/GED) - [GC]

Référence	Composant	Fournisseur	Version	Statut	Supp. LL	Commentaires
SG-1243	**Zope**		2.x	M		
SG-1237	**Alfresco**	**Communauté Alfresco**	4.x	R	**Oui**	*Suite d'outils pour le collaboratif via portail Web.*

Document 3

https://www.pcsansvirus.com/pages/securite-informatique/les-6-differents-types-de-virus-informatique-les-plus-dangereux-expliquer.html

Les 6 différents types de Virus informatique les plus dangereux

Un virus informatique est un petit programme situé dans le corps d'un autre qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmées.

La définition pourrait être la suivante :

Tout programme capable d'infecter un autre programme en le modifiant de façon à ce qu'il puisse à son tour se reproduire est un virus informatique
Le véritable nom donné aux virus informatique est CPA « Code Auto-Propageable » , mais par analogie avec le domaine médical, le nom de « virus » a été donné.
Ils se reproduisent en infectant des « applications hôtes« , c'est-à-dire en copiant une portion de code exécutable au sein d'un programme existant.

Or, afin de ne pas avoir un fonctionnement chaotique, ils sont programmés pour ne pas infecter plusieurs fois un même fichier.
Les virus vont de la simple balle de ping-pong qui traverse l'écran, aux virus informatiques les plus dangereux destructeur de données.
Ce dernier étant la forme de virus la plus virulente. Ainsi, étant donné qu'il existe une vaste gamme de virus ayant des actions aussi diverses que variées,
les virus informatiques ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection.

Les antivirus sont capables de les détecter si il les connaissent , permettant ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou des virus sont trouvés.
On parle ainsi d'éradication de virus pour désigner la procédure de nettoyage de l'ordinateur.

Ils intègrent ainsi dans l'application infectée une suite d'octets leur permettant de vérifier si le programme a préalablement été infecté :
il s'agit de la signature virale. Les antivirus s'appuient ainsi sur cette signature propre à chacun d'entre eux pour les détecter.
Il s'agit de la méthode de recherche de signature (scanning), la plus ancienne méthode utilisée par les antivirus. Cette méthode n'est fiable que si l'antivirus possède une base virale à jour, c'est-à-dire comportant les signatures de tous les virus connus.

Toutefois cette méthode ne permet pas la détection de tous n'ayant pas encore répertoriés par les éditeurs d'antivirus.
De plus, les programmeurs malveillants les ont désormais dotés de capacité de camouflage, de manière à rendre leur signature indétectable,
il s'agit de « virus polymorphes ». Certains antivirus utilisent un contrôleur d'intégrité pour vérifier si les fichiers ont été modifiés.
Ainsi le contrôleur d'intégrité construit une base de données contenant des informations sur les fichiers exécutables du système (date de modification, taille, et éventuellement une somme de contrôle).

Ainsi, lorsqu'un fichier exécutable change de caractéristiques, l'antivirus prévient l'utilisateur de la machine.

Les 3 catégories de virus informatique On distingue ainsi 3 catégories types :
- les vers sont des virus capables de se propager à travers un réseau
- les troyens (cheval de Troie) sont des virus permettant de créer une faille dans un système généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle.
- les bombes logiques sont des virus capables de se déclencher suite à un évènement particulier (date système, activation distante, ect …)

Les 6 différents types de Virus informatique :

1. Le Virus informatique Mutant En réalité, la plupart des virus sont des clones, ou plus exactement des « mutants », c'est-à-dire ayant été réécrits par d'autres programmeurs afin d'en modifier leur comportement ou bien uniquement leur signature. Le fait qu'il existe plusieurs versions (on parle de variantes) d'un même virus le rend d'autant plus difficile à repérer dans la mesure où les éditeurs d'antivirus doivent ajouter ces nouvelles signatures à leurs bases de données …
2. Le Virus informatique polymorphes Etant donné que les antivirus détectent (entre autres) les virus informatique grâce à leur signature (la succession de bits qui les identifie), certains créateurs malveillant ont pensé à leur donner la possibilité de modifier automatiquement leur apparence, tel un caméléon, en les dotant de fonction de chiffrement et de déchiffrement de leur signature de telle manière à ce que seul le virus soit capable de reconnaître sa propre signature. Ce type de virus informatique est appelé polymorphe (ce mot provenant du grec signifie qui peut prendre plusieurs formes).
3. Les rétrovirus On appelle « rétrovirus » ou « virus flibustier » (en anglais bounty hunters) un virus ayant la capacité de modifier les signatures des antivirus afin de les rendre inopérants.
4. Le Virus informatique de boot On appelle virus de boot, un virus informatique capable d'infecter le secteur de démarrage d'un disque (MBR, soit Master Boot Record), c'est-à-dire un secteur du disque copié dans la mémoire au démarrage de l'ordinateur, puis exécuté afin d'amorcer le démarrage du système d'exploitation.
5. Le Cheval de Troie Représente une faille dans la sécurité d'un réseau en créant une connexion dissimulées qu'un pirate pourra utiliser pour s'introduire dans le système, ou pour lui fournir des informations. Ces virus marquent les systèmes de telle façon à ce qu'ils puissent être repérés par leurs créateurs. De tels virus informatique dévoilent l'ensemble des systèmes d'informations d'une machine et brisent ainsi la confidentialité des documents qu'elle renferme, on les appelle cheval de Troie
6. Le macros virus informatique Avec la multiplication des programmes utilisant des macros, Microsoft a mis au point un langage de script commun pouvant être inséré dans la plupart des documents pouvant contenir des macros, il s'agit de VBScript, un sous-ensemble de Visual Basic. Ces virus informatiques arrivent actuellement à infecter les macros des documents Microsoft Office, c'est-à-dire qu'il peut être situé à l'intérieur d'un banal document Word ou Excel, et exécuter une portion de code à l'ouverture de celui-ci lui permettant d'une part de se propager dans les fichiers, mais aussi d'accéder au système d'exploitation (Windows). Celui-ci a la possibilité, lorsqu'il est ouvert sur un client de messagerie Microsoft, d'accéder à l'ensemble du carnet d'adresse et de s'auto diffuser par le réseau. Ce type est appelé un ver (ou worm en anglais). Je vous invite à participer en commentant. Le partage va tous nous aider à être bien informé de tous ces dangers.

Document 4

http://www.silicon.fr/securite-linux-attaquable-sans-une-seule-ligne-de-code-163468.html

Sécurité : Linux attaquable sans une seule ligne de code

Un chercheur démontre comment il a utilisé une faille propre au décodeur gstreamer et au format FLIC pour contourner les mesures de sécurité de Linux.

Jusqu'à une époque encore récente, les systèmes Linux étaient réputés plus sécurisés que les environnements Windows. Notamment parce que les malwares, outils de piratages ou encore vulnérabilités zero day sont considérés comme moins nombreux à cause (ou grâce) au faible intérêt que portent les pirates aux PC sous Linux, beaucoup moins courants que ceux équipés de Windows ou Mac (2,18% des OS desktop en octobre 2016, selon NetMarketShare). Et bien évidemment aussi grâce aux fonctionnalités de sécurité intégrées dans l'OS Open Source.

Et pourtant, celles-ci seraient contournables sans une seule ligne de code ou presque. A cause d'une vulnérabilité zero day (exploitable et non corrigée) présente dans la plupart des distributions modernes. « Une vulnérabilité importante amenant un risque de corruption [mémoire] est présente dans le décodeur gstreamer pour le format de fichier FLIC », *révèle* Chris Evans dans un billet daté du 21 novembre. Le chercheur en sécurité fait notamment référence aux distributions populaires et récentes Ubuntu 16.04 et Fedora 24 sur lesquelles gstreamer est livré par défaut. Il a pour sa part réalisé son exploit sur une machine dotée de Fedora.

Ubuntu a un problème

La faille permet de contourner deux systèmes de sécurité Linux : ASLR (address space layout randomization) et DEP (data execution protection) également connus comme NX (no execute). Le premier limite les risques d'exploitation en chargeant aléatoirement le code en mémoire. Le second est censé bloquer l'accès des exploits à la mémoire. Selon Chris Evans, s'attaquer au système en se confrontant à ces deux protections est un vrai défi. Mais attaquer le décodeur des fichiers FLIC ne nécessite même pas une seule ligne de code. « L'attaquant peut soumettre un tas d'octets sans script dans le décodeur et essayer d'obtenir l'exécution du code sans autre interaction », assure l'expert.

Sans entrer dans les détails du mode opératoire (que le chercheur livre dans son billet), la faille lui a permis de « commander la lecture, l'écriture et même les additions en mémoire, pour lentement mais sûrement faire avancer l'exploit et gagner en contrôle ». Pour lui, si cet exploit est « assez ridicule […] cela valait la peine de le faire parce que c'est la preuve que des exploits sans script sont possibles, même dans le contexte d'un ASLR 64-bits décent ». Autrement dit : « Ubuntu a un problème. » Un problème que les éditeurs devraient corriger assez vite comme c'est généralement la règle dans l'Open Source.

[Mise à jour du 25/11] GStreamer a publié un correctif de son décodeur qui sera inclus dans la prochaine version de maintenance de GStreamer 1.10.

Document 5

http://www.silicon.fr/securite-linux-attaquable-sans-une-seule-ligne-de-code-163468.html

ISILOG

FICHE MÉTHODOLOGIE

Réaliser un inventaire physique

IWS by isilog NF

En bref

Module : IsiCAB

Profil : Tous

Problématique :

Préparer et réaliser un inventaire physique ;

Processus cibles :

Asset Management (gestion de parc informatique, mobilier, téléphonie etc.).

IWS by isilog NF

Inventaire – Mode d'emploi

Cette fiche détaille les bonnes pratiques permettant de réaliser avec succès l'inventaire de votre parc.

La préparation de l'inventaire constitue une étape non négligeable d'un inventaire. Ci-dessous sont présentés les éléments devant retenir toute votre attention.

Définitions des référentiels

Les référentiels sont généralement existants, voire intégrés dans l'outil de gestion de parc. Les nomenclatures des sites, unités organisationnelles (UO), utilisateurs et références de matériels doivent être homogénéisées structurées et figées avant d'entamer toute session d'inventaire. Quelques conseils :

- Identifier chaque site / UO / utilisateur par un identifiant unique ;
- Identifier les références par un prélèvement d'échantillon de matériels de votre parc (éléments représentatifs) ;
- Ne pas hésiter à utiliser des références « génériques » pour les objets classiques (hors informatique) sur lesquels il est évident que le modèle risque d'évoluer dans le temps (bureau, table, chaise, armoire).

Créer des books

Un book est un document généré à partir d'un référentiel. L'idéal étant de pouvoir constituer le document à la volée par un simple publipostage ou export à partir de l'outil de gestion de parc.

Type : Bureau

Référence	Code	Code barre	
BUREAU	BUR		
BUREAU AVEC RETOUR	BAR		
BUREAU DIRECTION	BUD		

Ce document va reprendre chaque élément unique du référentiel pouvant être lu avec le lecteur optique. Dans le cadre d'un inventaire complet, nous retrouverons donc, sous format papier :

- La liste des sites, des UO, des utilisateurs ;
- La liste des références (modèles) ventilées par type de bien ;
- La liste de commentaires (facultatif) permettant par exemple d'identifier la vétusté de l'objet inventorié.

Eléments à faire figurer dans le book

La version papier des books doit contenir différents éléments :

- Le code barre de la référence (format code à barre Alpha 39 Ver 2.0 (A-39.TTF), 39251, 3 of 9 Barcode) + la correspondance alphanumérique ;
- La photo de la référence ;
- L'endroit adéquat où coller l'étiquette (identifiant unique de l'objet).

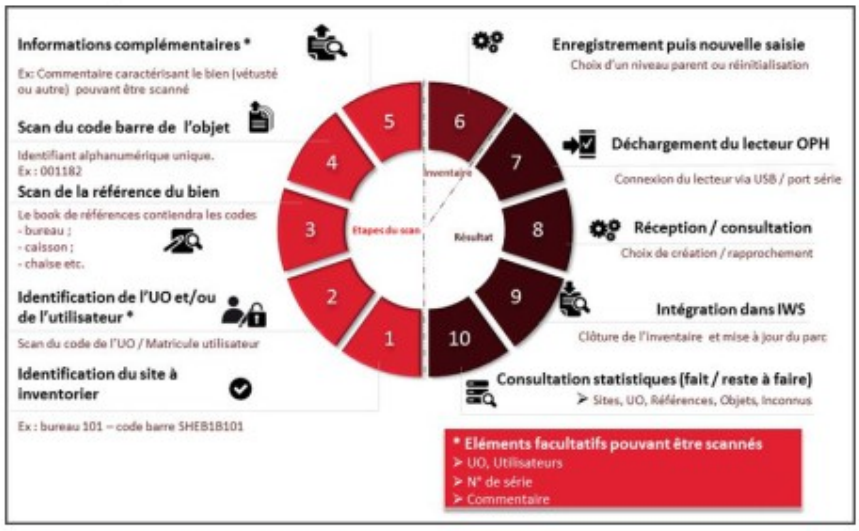
Création de modes opératoires

Créer un mode opératoire, permettant à toute personne, d'adapter la procédure adéquate pour les cas suivants :

- Procédure pour réaliser l'inventaire (initialisation / inventaire / collecte de données, périmètre de l'inventaire) ;
- Procédure permettant la mise à jour et l'édition des référentiels (books) ;
- Procédure à adopter lorsqu'un écart est identifié (élément manquant du référentiel, non conformité etc.) ;
- Fourniture des plans des locaux ;
- Fiches manuelles permettant de avec encart permettant de signaler d'éventuels problèmes (accès bloqués, placards fermés etc.).

Inventaire d'un site pilote

Réaliser une phase d'inventaire sur un site pilote est une étape incontournable permettant de vérifier et de valider le travail de préparation et d'identifier rapidement les éventuelles incohérences. Le schéma ci-dessous détaille la cinématique de l'inventoriste.



Contrôle de cohérence et intégration

Une fois le site pilote inventorié, il sera nécessaire de procéder au déchargement des informations relevées à l'aide du lecteur optique. Il sera ainsi possible :

- Vérifier la cohérence des informations ;
- Intégrer les données dans l'outil de gestion de parc et effectuer un suivi d'avancement .

Facteurs clés de succès

- Ne pas négliger la **phase de préparation** des référentiels ;
- Définir un **site pilote** pour valider les procédures ;
- Utiliser des **codes barres sur étiquettes autocollantes adaptées au support** (exemple : étiquette polyester ou métallique etc.).

IWS by isilog NF

Bonnes pratiques :

1. Définir des modes opératoires ;
2. Utiliser des rouleaux d'étiquettes ne comportant que des séquences (ex: 001182) / éviter l'attribution d'un N° d'identifiant en fonction du type de matériel ;
3. Constituer les books de manière à visualiser à la fois le code à barre et la valeur alphanumérique associée ;
4. Décharger le lecteur optique tous les jours voire toutes les ½ journées ;
5. Dans le cadre d'un inventaire informatique, scanner les postes de travail avec un agent WMI.

A propos

Depuis 1992, ISILOG est spécialisée dans l'offre de solutions de gestion des services informatiques et des infrastructures aux moyennes et grandes entreprises.
La suite logicielle IWS de ISILOG permet la mise en œuvre des processus de gestion des services informatiques, la gestion des infrastructures (parc IT, réseaux télécoms, automobile, mobilier et immobilier) et la gestion des demandes des utilisateurs (Helpdesk, achats, etc.).
Basée à Paris et à Nantes, ISILOG compte plus de 800 clients et réalise une importante part de ses ventes par son réseau de partenaires.

ISILOG

ZAC de la LORIE
8 rue Sacco et Vanzetti
44813 Saint-Herblain Cedex
Tél : +33 2 40 92 09 72
Email : info@isilog.fr
Web : www.isilog.fr

afaq ISO 9001 Qualité afaq ISO 20000-1 Système d'information

Document 6

https://securelist.fr/threats/que-faire-si-mon-ordinateur-est-infecte/

Que faire si mon ordinateur est infecté ?

Malheureusement, il peut parfois arriver que le logiciel antivirus installé sur votre ordinateur soit incapable de détecter de nouveau virus, vers ou chevaux de Troie, même s'il est à jour. La triste vérité est qu'aucun logiciel antivirus ne peut vous garantir une sécurité fiable à 100%. Si votre ordinateur est infecté, vous devrez déterminer l'origine de l'infection, identifier le fichier infecté et l'envoyer au fournisseur dont le produit n'a pas détecté le logiciel malveillant et n'a pas réussi à protéger votre ordinateur.
Néanmoins, les utilisateurs sont souvent incapables de détecter une infection sur leur ordinateur par eux-mêmes sauf s'ils sont aidés par une solution antivirus. De nombreux vers et chevaux de Troie ne révèlent jamais leur présence. Exceptionnellement, certains chevaux de Troie informent directement l'utilisateur que leur ordinateur a été infecté : il se peut qu'ils chiffrent les fichiers personnels de l'utilisateur afin de demander une rançon en échange d'un utilitaire de déchiffrement. Cependant, un cheval de Troie s'installe normalement sur un système de manière secrète et emploie des méthodes spéciales afin de rester caché. L'infection peut donc uniquement être détectée de manière indirecte.

Les symptômes d'une infection

Une augmentation du trafic sortant est généralement indicatrice d'une infection : cela s'applique aussi bien aux ordinateurs individuels qu'aux réseaux d'entreprise. Si aucun utilisateur ne travaille sur Internet pendant une période de temps spécifique (par exemple, la nuit), mais que le trafic Web continue, cela pourrait signifier que quelqu'un d'autre est actif sur le système, et il s'agit probablement d'activités malveillantes. Si un firewall est configuré sur le système, des tentatives de connexions à Internet établies par des applications inconnues peuvent également indiquer une infection. L'ouverture de nombreuses fenêtres pop-up alors que vous visitez des sites Web peut également indiquer que votre système est infecté par un adware. Si un ordinateur se bloque ou crashe fréquemment, cela peut également être lié à l'activité d'un malware. De tels problèmes de fonctionnement proviennent plus souvent de problèmes liés au matériel ou à des logiciels qu'à des activités malveillantes. Néanmoins, si de tels symptômes se produisent simultanément sur plusieurs ordinateurs d'un même réseau, accompagnés d'une augmentation considérable du trafic interne, il y a de grandes chances qu'un vers ou qu'un cheval de Troie exploitant une backdoor se soit répandu sur le réseau.

Une infection peut également être détectée indirectement grâce à des symptômes qui ne sont pas liés à l'ordinateur, tels qu'une facture de téléphone indiquant des appels que personne n'a effectués ou des SMS que personne n'a envoyés. Ces éléments pourraient indiquer qu'un cheval de Troie a infecté votre ordinateur ou votre téléphone mobile. Si on a accéder à votre compte bancaire ou que votre carte de crédit a été utilisée sans autorisation, un spyware pourrait se trouver dans votre système.

Que faire ?

La première chose à faire est de vous assurer que les bases de données de votre antivirus sont à jour pour ensuite réaliser une analyse de votre ordinateur. Si cela n'aide pas, les solutions antivirus d'autres fournisseurs pourraient faire l'affaire. De nombreux fabricants d'antivirus offrent des versions d'essai gratuites de leurs produits : nous vous recommandons d'utiliser un de ces produits sur votre ordinateur. Si un virus ou un cheval de Troie est détecté, assurez-vous d'envoyer une copie du fichier infecté à l'éditeur de la solution antivirus qui n'a pas réussi à le détecter avant. Cela aidera ce dernier à développer une protection contre cette menace plus rapidement et à empêcher les autres utilisateurs qui utilisent également cet antivirus d'être infectés.

Si un autre antivirus ne détecte pas de malware, nous vous recommandons de déconnecter l'ordinateur d'Internet ou du réseau local, de désactiver la connexion Wi-Fi et le modem, avant de rechercher des fichiers infectés. N'utilisez le réseau que si c'est absolument nécessaire. N'utilisez surtout pas les systèmes de paiement en ligne ou les services bancaires en ligne. Évitez d'utiliser des données personnelles ou confidentielles, n'utilisez pas de site Web qui requiert un nom d'utilisateur et un mot de passe.

Comment trouver un fichier infecté

Dans certains cas, détecter un virus ou un cheval de Troie peut être complexe et peut requérir des qualifications techniques : néanmoins, dans d'autres cas cela peut être très facile et tout dépend du degré de complexité du malware et des méthodes utilisées pour cacher le code du malware intégré dans le système. Dans les cas les plus difficiles quand des méthodes spéciales (comme par exemple des technologies rootkits) sont employées pour dissimuler un code malveillant dans un système, une méthode non-professionnelle ne sera peut-être pas capable de localiser le fichier infecté. Ce problème peut nécessiter des utilitaires et des actions spéciales, comme connecter le disque dur à un autre ordinateur ou démarrer le système depuis un CD. Néanmoins, s'il s'agit d'un ver normal ou un simple cheval de Troie, vous pourrez peut-être le localiser en utilisant des méthodes relativement simples.

La grande majorité des vers et des chevaux de Troie ont besoin de prendre le contrôle de l'appareil à son démarrage. Il existe donc deux méthodes relativement simples pour cela :

- Un lien vers le fichier infecté est écrit dans les clés autorun du registre de Windows.
- Le fichier infecté est copié dans un fichier autorun de Windows.

Les dossiers autorun les plus communs sur Windows 2000 et XP sont les suivants :

%Documents and Settings%\%user name%\Start Menu\Programs\Startup\
%Documents and Settings%\All Users\Start Menu\Programs\Startup\

Il existe un certain nombre de clés autorun dans le registre du système, les clés les plus populaires incluent Run, RunService, RunOnce et RunServiceOne et elles se situent dans les dossiers suivants :

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\]
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\]

Il y a de grandes chances pour qu'une recherche dans ces dossiers fasse apparaitre plusieurs clés avec des noms qui ne fourniront pas beaucoup d'informations et d'accès vers les fichiers exécutables. Une attention particulière doit être portée aux fichiers situés dans le catalogue du système Windows ou dans le répertoire racine. Souvenez-vous du nom de ces fichiers, vous en aurez besoin dans l'analyse suivante.

Écrire sur la clé suivante est également une pratique commune :

[HKEY_CLASSES_ROOT\exefile\shell\open\command\]

La valeur par défaut de cette clé est » %1 » » %* « .

Le catalogue du système de Windows (et système 32) et le répertoire racine sont les endroits les plus communs pour installer des vers et des chevaux de Troie. Cela est dû à deux choses : les contenus de ces catalogues ne sont pas montrés dans l'exploreur par défaut et ces catalogues hébergent un nombre important de fichiers du système et de fonctions qui sont complètement inconnus pour un utilisateur moyen. Même un utilisateur expérimenté trouvera certainement difficile de définir si un fichier appelé winkrnl386.exe fait partie du système d'exploitation ou s'il s'agit d'un fichier étranger.

Il est recommandé d'utiliser un gestionnaire de fichiers qui pourra organiser les fichiers par date de création/modification et organiser les fichiers situés dans les catalogues mentionnés précédemment. Tous les fichiers créés et modifiés apparaitront en haut du catalogue : ces fichiers seront essentiels pour vos recherches. Si certains de ces fichiers sont identiques à ceux trouvés dans les clés autorun, il s'agit déjà d'un premier signe.

Les utilisateurs avancés peuvent également vérifier les ports de réseau ouverts en utilisant Netstat, un utilitaire standard. Nous vous recommandons également d'utiliser un firewall et d'analyser les processus en cours dans les activités du réseau. Vérifiez également la liste des processus en cours en utilisant des utilitaires adaptés disposant de fonctionnalités avancées au lieu des utilitaires Windows standard : de nombreux chevaux de Troie réussissent à ne pas être détectés par les utilitaires Windows standard.

Il est néanmoins impossible de vous donner des conseils universels qui pourraient s'appliquer à toutes les situations. Les vers et les chevaux de Troie avancés sont souvent difficiles à localiser. Dans ce cas, il est mieux de consulter le support technique de votre fournisseur de sécurité informatique, de contacter une société offrant des services d'assistances en sécurité, ou de demander de l'aide sur des forums spécialisés. Ces ressources Web incluent www.virusinfo.info, www.rootkit.com et www.gmer.net (en anglais). De nombreuses sociétés antivirus disposent également de forums similaires conçus pour aider les utilisateurs.

https://fr.wikipedia.org/wiki/Windows_Server_Update_Services

Windows Server Update Services

Windows Server Update Services (WSUS) est un service permettant de distribuer les mises à jour pour Windows et d'autres applications Microsoft sur les différents ordinateurs fonctionnant sous Windows au sein d'un parc informatique. WSUS est un rôle pour serveur Windows lui permettant ainsi de devenir un serveur de mises à jour local (ou proxy de mises à jour). Ce serveur télécharge et stocke ponctuellement l'ensemble des mises à jour disponibles auprès des serveurs Windows Update de Microsoft et rend possible le contrôle de la diffusion de celles-ci dans le parc.
Par défaut chaque ordinateur sous Windows faisant ses mises à jour, les télécharge directement sur les serveurs de Microsoft, ce qui demande beaucoup de bande passante au niveau de l'accès internet dans un parc composé de nombreuses machines.

Historique

WSUS a d'abord[Quand ?] été connu sous le nom Software Update Services (SUS) et ne permettait que de diffuser les patchs et hotfixes de Windows. WSUS, bien qu'inspiré de SUS permet de mettre à jour beaucoup plus de logiciels tels que les suites Microsoft Office, les pilotes pour les périphériques ou encore des composants comme le Framework .NET.

Administration

Windows Server Update Services 2.0 comprenait un répertoire de stockage des mises à jour et autres packages téléchargés depuis le site web de Microsoft, et une instance de MSDE, un service est alors chargé de rechercher les mises à jour sur le web puis un site virtuel IIS distribue les mises à jour. La gestion est assurée au moyen d'une interface web, permettant d'approuver manuellement ou automatiquement les mises à jour et permettant de générer des rapports basiques.
Les administrateurs réseau peuvent utiliser WSUS avec les stratégies de groupe d'Active Directory afin de configurer les PC clients pour la recherche de mises à jour et l'envoi d'état de mises à jour. En l'absence d'Active Directory il est possible d'éditer le registre de windows.
La version 3 est plus robuste : permettant de gérer plus de mises à jour et plus de programmes, elle utilise une console d'administration mmc pour l'administration.
Microsoft fournit WSUS gratuitement sur son site web.

Historique des versions

- 22 mars 2005 - Version 2.0 Release Candidate
- 6 juin 2005 - Version 2.0 finale (build 2340)
- 31 mai 2006 - V 2.0 Service Pack 1 (support de Windows Vista, langues supplémentaires et utilisation possible de Microsoft SQL Server 2005
- 14 août 2006 - 3.0 beta 2 (administration par MMC et nombreuses nouvelles fonctions)
- 30 avril 2007 - 3.0 finale (build 3.0.6000.318)
- 1er novembre 2007 - V 3.0 Service Pack 1 RC
- 7 février 2008 - WSUS 3.0 Service Pack 1 finale (prise en charge de Windows Server 2008)
- 25 août 2009 - WSUS 3.0 Service Pack 2 (prise en charge de Windows 7 et Windows Server 2008 R2)