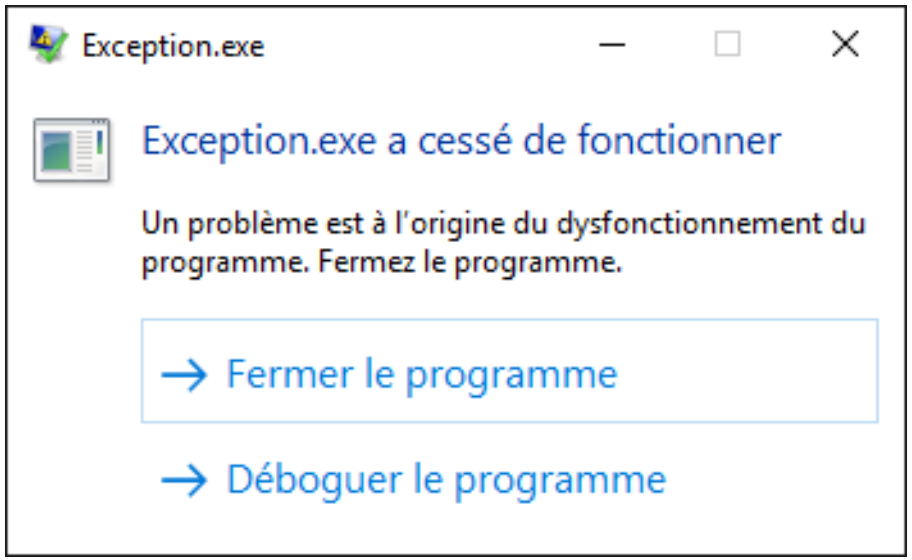
WER

Aurélien Bordes

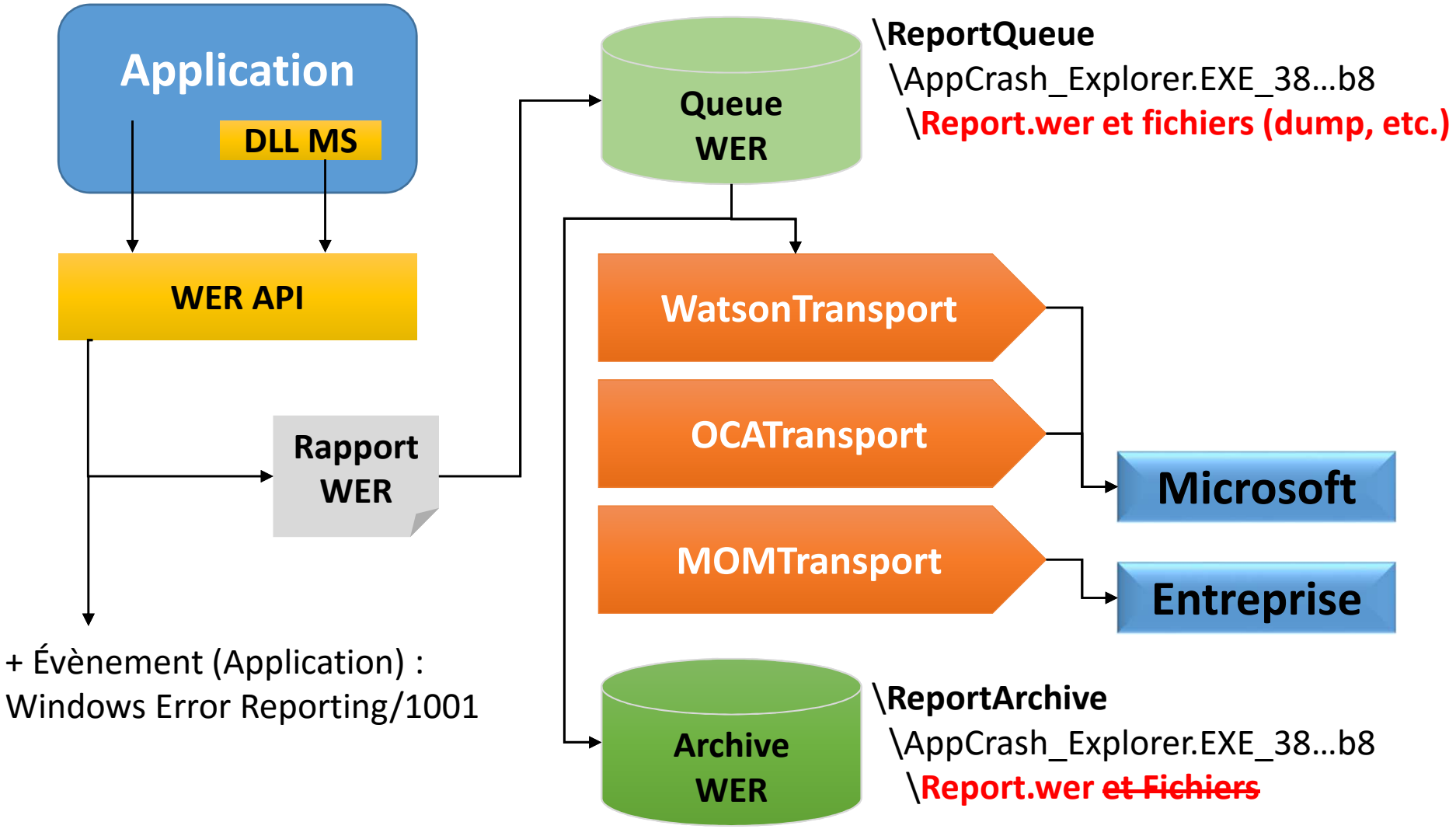
SSTIC – 3 juin 2016

De Dr Watson à *Windows Error Reporting*

- WER est apparu avec Windows Vista
- WER permet de générer des rapports d'erreur (crash d'application, crash du noyau, blocage d'application, problème spécifique, etc.)
- Ces rapports sont envoyés à Microsoft



Principe de WER



L'API de WER

- `WerReportCreate()`
  - **pwzEventType**
  - **repType** :
    - NonCritical (0), Critical (1), ApplicationCrash (2), ApplicationHang (3), Kernel (4)
- `WerReportSetParameter()`
  - WER_P0 à WER_P9
- `WerReportAddFile()`
- `WerReportAddDump()`
  - MicroDump, MiniDump, HeapDump
- `WerReportSubmit()`
- `WerReportCloseHandle()`

Intégration de WER dans Windows (1/3)

- Dans certains scénarios, le système génère automatiquement des rapports WER
  - **Crash d'application** (exception non gérée) :
    - `pwzEventType = APPCRASH`
    - `repType = ApplicationCrash (2)`
    - `Sig[0] Nom de l'application Explorer.EXE`
    - `Sig[1] Version de l'application 10.0.10586.0`
    - `Sig[2] Horodatage de l'application 5632d4c0`
    - `Sig[3] Nom du module twinui.appcore.dll`
    - `Sig[4] Version du module 10.0.10586.11`
    - `Sig[5] Horodateur du module 56457778`
    - `Sig[6] Code de l'exception 80270233`
    - `Sig[7] Décalage de l'exception 0000000000166be4`

Démo 1

- Crash d’application
- Visualisation du rapport dans la file d’attente
- Visualisation de la synthèse du rapport (Rapport.wer)
- Exemple d’historique

Intégration de WER dans Windows (2/3)

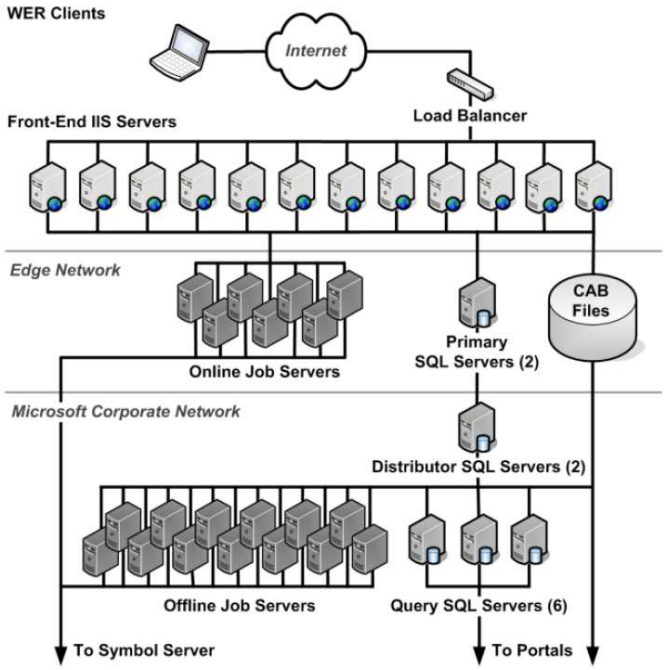
- **Blocage d'application** :
  - `pwzEventType = AppHangB1`
  - `repType = AppHang (3)`
  - Sig[0] Application Name POWERPNT.EXE
  - Sig[1] Application Version 14.0.4754.1000
  - Sig[2] Application Timestamp 4b967cf0
  - Sig[3] Hang Signature 3f7d
  - Sig[4] Hang Type 134217728

Intégration de WER dans Windows (3/3)

- **Crash du noyau** :
  - `pwzEventType = BlueScreen`
  - `repType = Kernel (4)`
  - `Sig[0] Code (bugcheck)`
- **Pilote de périphérique non trouvé** :
  - `pwzEventType = PnpDriverNotFound`
  - `repType = NonCritical (0)`
  - `Sig[0] Architecture x64`
  - `Sig[1] ID du matériel USB\VID_0A5C&PID_5800`
- **Problème d'installation Windows Update** :
  - `pwzEventType = StoreAgentScanForUpdateFailure0`
  - `repType = NonCritical (0)`
- **Service Hangs, Installation Failures, App. Compat. Issues, AppxDeploymentFailure, etc.**

Traitement des rapports par Microsoft

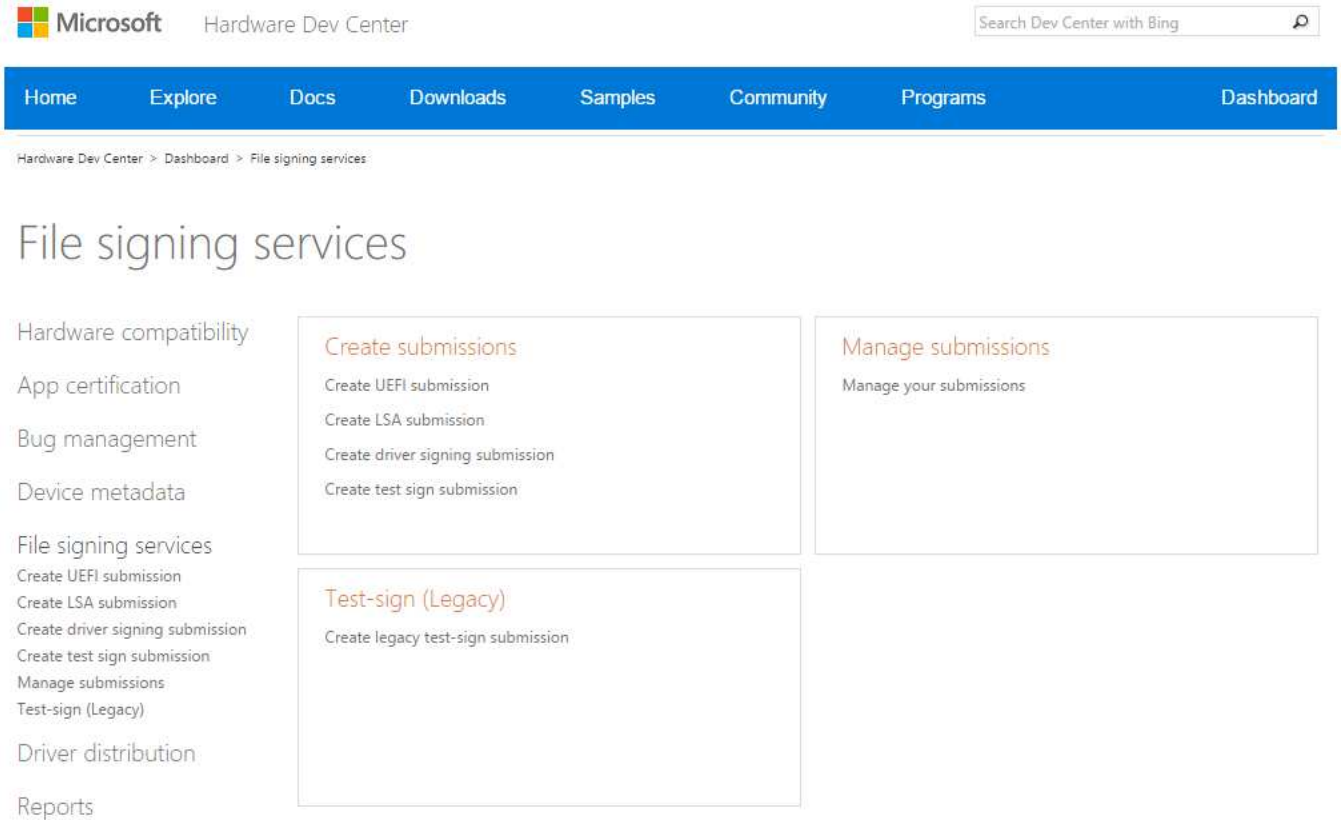
- Voir « *Debugging in the (Very) Large: Ten Years of Implementation and Experience* » (octobre 2009) [1]
  - Problématique du volume important
  - Traitement et catégorisation automatique (*Bucketing*)
- L'architecture WER mise en oeuvre permet :
  - de rapidement détecter et corriger les bugs
  - de détecter des attaques informatiques (exemple : détection de MS08-067 [2])



[1] http://research.microsoft.com/apps/pubs/default.aspx?id=81176
[2] https://blogs.technet.microsoft.com/johnla/2015/09/26/the-inside-story-behind-ms08-067/

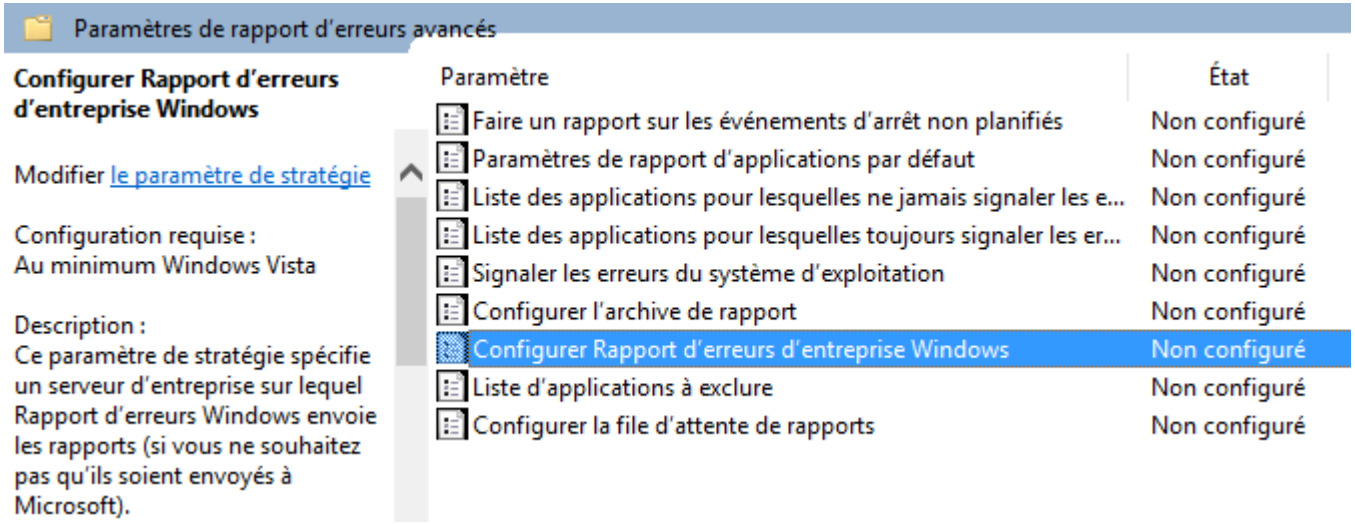
Accès aux rapports

- Les rapports WER peuvent être consultés par les éditeurs de logiciels enregistrés sur le portail *Hardware Dev Center* (anciennement *Windows quality online services*)



Collecteur WER d'entreprise

- WER permet de définir un collecteur d'entreprise en remplacement de celui de Microsoft
- La mise en place d'un tel collecteur permet :
  - d'éviter la fuite d'information
  - de disposer d'une source d'information très précieuse pour la détection de compromission et le *forensic*

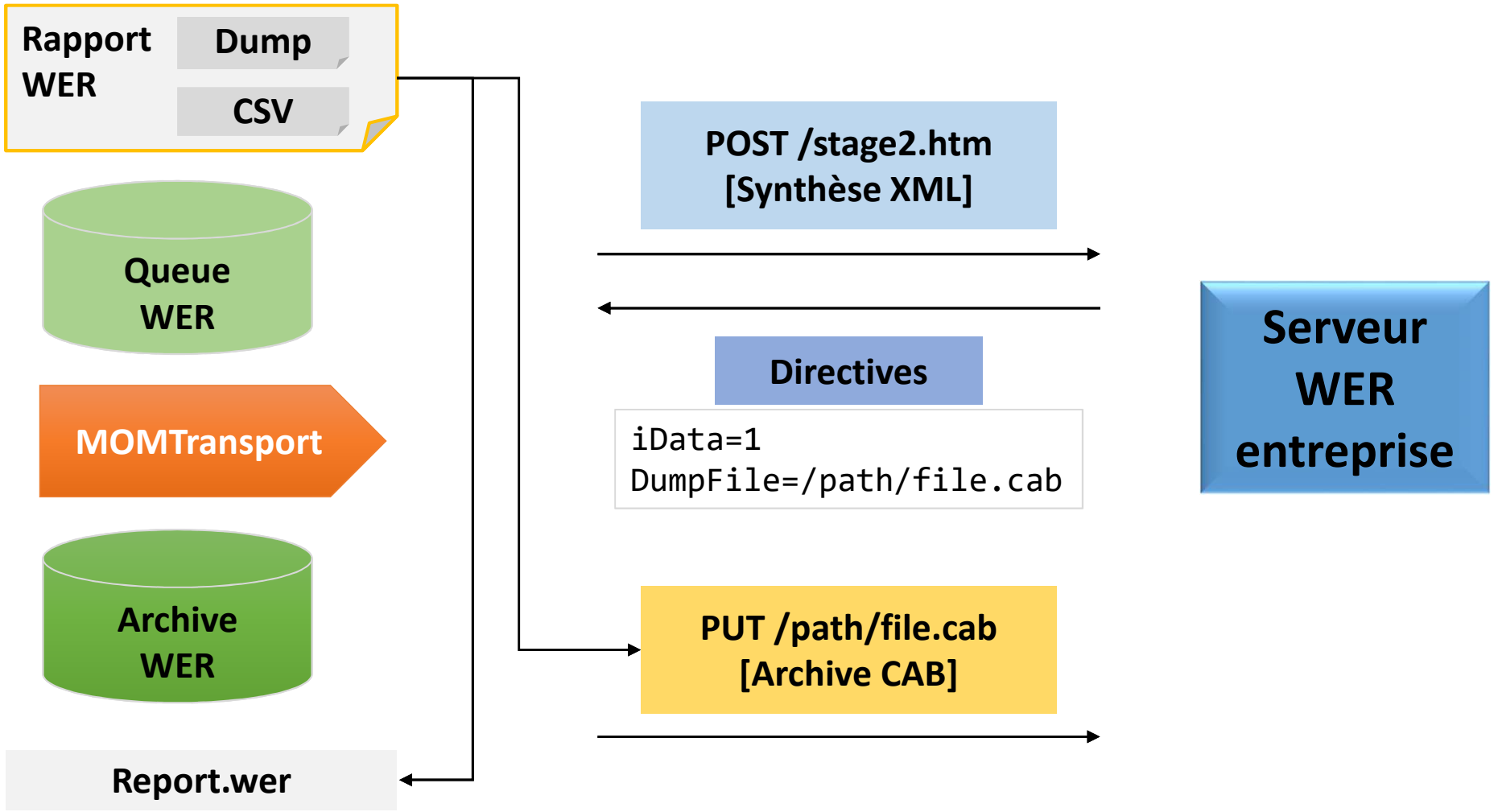


Corporate Error Reporting (CER) *protocol*

- v1 [XP/2003]
  - Remonté des rapports via SMB
- v2 [Vista+]
  - Utilisé par WER
  - Remonté des rapports via HTTP ou HTTPS

[MS-CER]: Corporate Error Reporting Version 1.0 Protocol	Specifies the Corporate Error Reporting Version 1.0 Protocol, which enables an organization to copy error reports from a set of client machines to a CER file share on a specified Server Message Block (SMB) Protocol file server with additional configuration options. Click here to view this version of the [MS-CER] PDF.
[MS-CER2]: Corporate Error Reporting V.2 Protocol	Specifies the Corporate Error Reporting V.2 Protocol, which enables enterprise computing sites to manage all error reporting information within the organization. Click here to view this version of the [MS-CER2] PDF.

Remonté des rapports WER avec un serveur d'entreprise



Démo 2

- Code PHP du collecteur
- Configuration du serveur de rapport d'erreurs d'entreprise
- Capture réseau
- Visualisation du contenu du rapport
- Consultation de la base du serveur

Directives optionnelles du serveur

- Lors de la 1re requête du client, le serveur peut envoyer des directives particulières afin d'inclure des informations supplémentaires dans le rapport :
  - MemoryDump
  - GetFileVersion
  - GetFile
  - fDoc
  - RegKey
  - RegTree
  - WQL (exécution de requête WMI)
- Le résultat sera inclus dans l'archive CAB envoyée lors de la 2e requête

Démo 3

- Ajout de directives supplémentaires
- Visualisation des fichiers ajoutés

Disponibilité du code

- POC du serveur WER disponible à l'adresse :

  https://github.com/aurel26/wer-server

- Attention à la sensibilité du collecteur

Structure | Données | Contraintes | Index | Déclencheurs | DDL

Vue tableau | Vue formulaire

Filtre de do... | Total dee lignes chargées: 50

	id_file_report	date	remote_ip	reporttype	eventtype	
1	4a8ab84e0f128d9004006bedc0f4d1ba	2016-05-19 19:39:28	172.16.50.63	2	APPCRASH	
2	44991536615e4ca8948becf495af5cad	2016-05-19 20:04:25	172.16.50.63	2	APPCRASH	
3	f302b90c2941d40ec981bb3a5ce5524a	2016-05-19 20:08:53	172.16.50.63	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
4	2540eecbc75c3fa41db6e5e9c499dd97	2016-05-19 23:52:02	172.16.50.53	4	BlueScreen	
5	cc5b0ed8bc818f7c0847c23ddf67b321	2016-05-19 23:52:18	172.16.50.53	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
6	4001fe8a3d073864e1ff7a973723f6b0	2016-05-19 23:57:22	172.16.50.53	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
7	da2e690671c2bbfb6bc012e6f0ee8374	2016-05-20 00:02:10	172.16.50.53	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
8	35b62a013d5f083a741cfafb191e71d6	2016-05-20 00:22:09	172.16.50.53	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
9	b50b48a84db2eaa39c2be1ca122276c0	2016-05-20 00:23:32	172.16.50.1	2	APPCRASH	
10	f611fa9d20330e1237718f553339372c	2016-05-20 00:28:51	172.16.50.1	2	APPCRASH	
11	6e1f78bb58cb48b5310fe3db6c0a5756	2016-05-20 00:29:59	172.16.50.1	2	APPCRASH	
12	d77f52de7528d2761a55c0aa57e5c084	2016-05-20 00:33:24	172.16.50.53	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
13	b52e3510c50fa44235ead58f9aca7335	2016-05-20 00:37:04	172.16.50.52	0	AEAPPINVW8	
14	99d1eca20775628bb54ffdf08cf6b9b0	2016-05-20 00:37:07	172.16.50.52	0	AEAPPINVW8	
15	96b18f2cffa591a1923402ab9d6968ee	2016-05-20 00:43:17	172.16.50.53	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
16	e8cdb4ece522f4d0f4d460e2c0a9351b	2016-05-20 00:56:27	172.16.50.53	2	APPCRASH	
17	b00440dcbfe13aede68383f60e5e0d25	2016-05-20 00:57:44	172.16.50.53	2	APPCRASH	
18	a9d75a2961d32a19d2120c36f7036ddb	2016-05-20 01:02:24	172.16.50.53	2	APPCRASH	
19	980dcfaa152263aec00b07a294f74b56	2016-05-20 01:06:13	172.16.50.53	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
20	c2ebe6c9ce03fb820b5939d6733f248f	2016-05-20 05:47:59	172.16.50.53	0	WindowsUpdateFailure3	Une mise à jour Windows ne s'est pas installée
21	dc39a925d3884a84f86cf6bb20183dc9	2016-05-20 05:54:19	172.16.50.53	2	APPCRASH	
22	03aaf7bcd855156ace6d8f29d5abd63c	2016-05-20 05:55:33	172.16.50.53	2	APPCRASH	
23	7f8612a7361b487541efa232603b4a9c	2016-05-20 06:09:58	172.16.50.53	2	APPCRASH	
24	230cf38c2680c84cd8c93c83aff681b5	2016-05-20 06:12:48	172.16.50.53	2	APPCRASH	

/var/www/html/reports

Name	Ext	Size	Changed	Rights	Owner
cf92c1b1bb8c4aecd0a04ea808096e17			20/05/2016 08:19:23	rwx---r-x	www-d...
894499d35d95a69aede9f22f66a22034			20/05/2016 08:18:54	rwx---r-x	www-d...
707d14147da0e917709e593514768f0b			20/05/2016 08:14:24	rwx---r-x	www-d...
230cf38c2680c84cd8c93c83aff681b5			20/05/2016 08:12:48	rwx---r-x	www-d...
7f8612a7361b487541efa232603b4a9c			20/05/2016 08:09:58	rwx---r-x	www-d...
03aaf7bcd855156ace6d8f29d5abd63c			20/05/2016 07:55:33	rwx---r-x	www-d...
dc39a925d3884a84f86cf6bb20183dc9			20/05/2016 07:54:20	rwx---r-x	www-d...
c2ebe6c9ce03fb820b5939d6733f248f			20/05/2016 07:47:59	rwx---r-x	www-d...
980dcfaa152263aec00b07a294f74b56			20/05/2016 03:06:13	rwx---r-x	www-d...
a9d75a2961d32a19d2120c36f7036ddb			20/05/2016 03:02:24	rwx---r-x	www-d...
b00440dcbfe13aede68383f60e5e0d25			20/05/2016 02:57:44	rwx---r-x	www-d...
e8cdb4ece522f4d0f4d460e2c0a9351b			20/05/2016 02:56:27	rwx---r-x	www-d...
96b18f2cffa591a1923402ab9d6968ee			20/05/2016 02:43:18	rwx---r-x	www-d...
99d1eca20775628bb54ffdf08cf6b9b0			20/05/2016 02:37:07	rwx---r-x	www-d...
b52e3510c50fa44235ead58f9aca7335			20/05/2016 02:37:04	rwx---r-x	www-d...
d77f52de7528d2761a55c0aa57e5c084			20/05/2016 02:33:24	rwx---r-x	www-d...
6e1f78bb58cb48b5310fe3db6c0a5756			20/05/2016 02:29:59	rwx---r-x	www-d...
f611fa9d20330e1237718f553339372c			20/05/2016 02:28:51	rwx---r-x	www-d...
b50b48a84db2eaa39c2be1ca122276c0			20/05/2016 02:23:32	rwx---r-x	www-d...
35b62a013d5f083a741cfafb191e71d6			20/05/2016 02:22:10	rwx---r-x	www-d...
da2e690671c2bbfb6bc012e6f0ee8374			20/05/2016 02:02:10	rwx---r-x	www-d...
4001fe8a3d073864e1ff7a973723f6b0			20/05/2016 01:57:22	rwx---r-x	www-d...
cc5b0ed8bc818f7c0847c23ddf67b321			20/05/2016 01:52:19	rwx---r-x	www-d...

Questions ?

aurelien26 (at) free.fr