Dell Data Protection | Encryption

Utilitaires administrateur

2014-05

Sommaire

1

Utilitaire de téléchargement administrateur

Cet utilitaire permet de télécharger un bundle de données concernant la clé destiné à une utilisation sur un ordinateur n'étant pas connecté à un serveur. Les utilitaires administrateur peuvent alors se servir de ces bundles de données hors connexion.

En fonction du paramètre de ligne de commande transmis à l'application, cet utilitaire utilise l'une des méthodes suivantes pour télécharger un bundle de données concernant la clé :

- Mode Administrateur - Utilisé si **-a** est inscrit dans la ligne de commande ou si aucun paramètre de ligne de commande n'est employé.
- Mode Forensic - Utilisé si **-f** est inscrit dans la ligne de commande.

Les fichiers de consignation se trouvent aux emplacements suivants :

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, et Windows 8.1 - C:\ProgramData\CmgAdmin.log

Utilisation de l'utilitaire de téléchargement administrateur en mode Administrateur

1. Double-cliquez sur **cmgad.exe** pour lancer l'utilitaire.

   ou

   À l'emplacement de l'utilitaire de téléchargement administrateur, ouvrez une invite de commande et saisissez **cmgad.exe -a** (ou cmgad.exe).

2. Saisissez les informations suivantes (il est possible que certains champs soient déjà renseignés).

Serveur :	nom d'hôte complet du serveur clé, tel que keyserver.domaine.com
Numéro de port :	par défaut, 8050
Compte serveur :	utilisateur de domaine exécutant Key Server. Le format est domaine\nom d'utilisateur. L'utilisateur de domaine exécutant l'utilitaire doit être autorisé à effectuer le téléchargement à partir du serveur clé.
MCID :	ID de l'ordinateur, par exemple IDordinateur.domaine.com
DCID :	huit premiers chiffres de l'identité Shield à 16 chiffres

   Cliquez sur **Suivant >**.

3. Dans le champ **Phrase de passe :**, saisissez une phrase de passe pour protéger le fichier de téléchargement. La phrase de passe doit comporter au moins huit caractères et contenir au moins un caractère alphabétique et un caractère numérique.

   Confirmez la phrase de passe.

   Vous pouvez accepter le nom et l'emplacement d'enregistrement par défaut du fichier ou cliquer sur ... pour sélectionner un autre emplacement.

   Un message vous indique que les données concernant la clé ont été correctement déverrouillées. Les fichiers sont maintenant accessibles.

4. Lorsque cette opération est terminée, cliquez sur **Terminer**.

Utilisation de l'utilitaire de téléchargement administrateur en mode Forensic

1. À l'emplacement de l'utilitaire de téléchargement administrateur, ouvrez une invite de commande et saisissez **cmgad.exe -f**.
2. Saisissez les informations suivantes (il est possible que certains champs soient déjà renseignés).

   URL du serveur périphérique : URL complète du serveur périphérique.

   Si Enterprise Server est antérieur à la version 7.7, le format est le suivant : https://deviceserver.domaine.com:8081/xapi

   Si Enterprise Server est ultérieur à la version 7.7, le format est le suivant : https://deviceserver.domaine.com:8443/xapi/

   Administrateur Dell : Nom de l'administrateur disposant des certificats d'administrateur Forensic (activés dans le serveur Enterprise), tel que jdoe

   Mot de passe : mot de passe de l'administrateur Forensic

   MCID : ID de l'ordinateur, par exemple IDordinateur.domaine.com

   DCID : huit premiers chiffres de l'identité Shield à 16 chiffres

   Cliquez sur **Suivant >**.
3. Dans le champ **Phrase de passe :**, saisissez une phrase de passe pour protéger le fichier de téléchargement. La phrase de passe doit comporter au moins huit caractères et contenir au moins un caractère alphabétique et un caractère numérique.

   Confirmez la phrase de passe.

   Vous pouvez accepter le nom et l'emplacement d'enregistrement par défaut du fichier ou cliquer sur **...** pour sélectionner un autre emplacement.

   Un message vous indique que les données concernant la clé ont été correctement déverrouillées. Les fichiers sont maintenant accessibles.
4. Lorsque cette opération est terminée, cliquez sur **Terminer**.

2

Utilitaire d'exécution administrateur

Cet utilitaire de ligne de commande permet aux administrateurs de déverrouiller des fichiers cryptés de l'utilisateur ou des fichiers communs cryptés sur un ordinateur pendant qu'un processus est en cours d'exécution.

Cet utilitaire est utilisé pour exécuter des tâches à partir d'une console de gestion. Cet utilitaire doit être copié sur l'ordinateur client et toute tâche nécessitant un accès aux fichiers cryptés de l'utilisateur ou aux fichiers communs cryptés est modifiée pour exécuter cet utilitaire en transmettant la ligne de commande pour la tâche de gestion à l'utilitaire. L'utilitaire se ferme dès que ce processus est terminé.

En fonction du paramètre de ligne de commande transmis à l'application, cet utilitaire utilise l'une des méthodes suivantes pour déverrouiller des fichiers :

- Mode Administrateur - Aucun commutateur nécessaire.
- Mode Forensic - Utilisé si **-f** est inscrit dans la ligne de commande.
- Mode Fichier de Sauvegarde - Utilisé si **-b** est inscrit dans la ligne de commande.

Les fichiers de consignation se trouvent aux emplacements suivants :

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, et Windows 8.1 - C:\ProgramData\CmgAdmin.log

Utilisation de l'utilitaire d'exécution administrateur en mode Administrateur

Syntaxe pour le mode Administrateur

CmgAlu -k -vX -aServerPrincipal -pPort [-r] [-XServer [-dMCID] [-sSCID]] “command”

Paramètres du mode Administrateur	Description
-k	Indique que Kerberos (Mode Administrateur) doit être utilisé. CmgAlu nécessite l'option-k pour travailler en Mode Administrateur.
X	Niveau connexion. Les niveaux connexion sont compris entre 0 et 5 (0 correspond à aucune connexion / 5 correspond au niveau de débogage).
ServerPrincipal	Compte AD (Compte de domaine) sous lequel le serveur clé est exécuté.
Port	Port TCP sur lequel le serveur clé doit être connecté.
Server	Nom/Adresse IP du serveur clé.
-r	Donne l'ordre à l'utilitaire de charger le nom du serveur clé et le MCID (ou SCID) de l'ordinateur à partir du registre. Si –r n'est pas spécifié, le nom du serveur clé et le MCID (ou SCID) doivent être fournis.
MCID	ID du périphérique à déverrouiller. Le MCID est également appelé « identifiant unique DUID » ou « nom d'hôte ».

Paramètres du mode Administrateur	Description
SCID	Identité Shield du périphérique à déverrouiller. Le SCID est également appelé « DCID » ou « ID de récupération ».
-?	Aide de la ligne de commande.

Utilisation de l'utilitaire d'exécution administrateur en mode Forensic

Syntaxe pour le mode Forensic

CmgAlu -f -vX -aAdminName -AAdminPwd [-r] [-XURL [-dMCID] [-sSCID]] “command”

Paramètres du mode Forensic	Description
-f	Indique que le mode Forensic doit être utilisé.
AdminName	Nom d'utilisateur de l'administrateur disposant des certificats d'administrateur Forensic.
AdminPwd	Mot de passe de l'administrateur Forensic.
URL	URL complète du serveur périphérique. Si Enterprise Server est antérieur à la version 7.7, le format est le suivant : https://deviceserver.domaine.com:8081/xapi Si Enterprise Server est ultérieur à la version 7.7, le format est le suivant : https://deviceserver.domaine.com:8443/xapi/
-r	Donne l'ordre à l'utilitaire de charger l'URL du serveur périphérique et le MCID (ou SCID) de l'ordinateur à partir du registre. Si –r n'est pas spécifié, l'URL/le serveur et le MCID (ou SCID) doivent être fournis.
X	Niveau connexion. Les niveaux connexion sont compris entre 0 et 5 (0 correspond à aucune connexion / 5 correspond au niveau de débogage).
MCID	ID du périphérique à déverrouiller. Le MCID est également appelé « identifiant unique DUID » ou « nom d'hôte ».
SCID	Identité Shield du périphérique à déverrouiller. Le SCID est également appelé « DCID » ou « ID de récupération ».
-?	Aide de la ligne de commande.

Utilisation de l'utilitaire d'exécution administrateur en mode Fichier de Sauvegarde

Syntaxe pour le mode Fichier de Sauvegarde

CmgAlu -vX -b"FilePath" -ABackupPwd "command"

Paramètres du mode Fichier de Sauvegarde	Description
X	Niveau connexion. Les niveaux connexion sont compris entre 0 et 5 (0 correspond à aucune connexion / 5 correspond au niveau de débogage).
-b"FilePath"	Le chemin du système de fichiers pour le fichier de sauvegarde, généralement un fichier LSA de récupération ou un un fichier de sortie téléchargé à partir de CmgAd.
BackupPwd	Le mot de passe utilisé pour créer le fichier de sauvegarde.
-?	Aide de la ligne de commande.

3

Utilitaire de déverrouillage administrateur

Cet utilitaire permet d'accéder aux fichiers cryptés de l'utilisateur, aux fichiers communs cryptés ou aux fichiers cryptés par SDE sur un disque esclave, un ordinateur démarré sous un environnement de pré-installation Windows (Windows PE) ou un ordinateur auquel aucun utilisateur activé n'est connecté.

Cet utilitaire utilise la méthode suivante pour télécharger un bundle de données concernant la clé :

- Mode Administrateur - Aucun commutateur nécessaire. Il s'agit du mode par défaut.
- Mode Forensic - Utilisé si **-f** est inscrit dans la ligne de commande.

Les fichiers de consignation se trouvent aux emplacements suivants :

Windows XP - C:\Documents and Settings\All Users\Application Data\CmgAdmin.log

Windows 7, Windows 8, et Windows 8.1- C:\ProgramData\CmgAdmin.log

Utilisation de l'utilitaire de déverrouillage administrateur pour travailler hors connexion avec un fichier téléchargé antérieurement

Lorsque vous travaillez hors connexion avec un fichier téléchargé antérieurement, le fonctionnement de CMGAu reste le même, quel que soit le mode de lancement. Autrement dit, les opérations exécutées sont identiques quand vous double-cliquez sur .exe, lancez l'utilitaire sans commutateur dans la ligne de commande ou utilisez le commutateur -f.

1. Double-cliquez sur **cmgau.exe** pour lancer l'utilitaire.
2. Sélectionnez **Oui : travailler hors connexion avec un fichier téléchargé antérieurement**. Cliquez sur **Suivant >**.
3. Dans le champ **Fichier téléchargé :**, accédez à l'emplacement d'enregistrement des données concernant la clé. Ce fichier a été enregistré lors de l'exécution de l'utilitaire de téléchargement administrateur.

   Dans le champ **Phrase de passe :**, saisissez la phrase de passe utilisée pour protéger le fichier contenant les données concernant la clé. Cette phrase de passe a été définie lors de l'exécution de l'utilitaire de téléchargement administrateur.

   Cliquez sur **Suivant >**.

   Un message vous indique que les données concernant la clé ont été correctement déverrouillées. Les fichiers sont maintenant accessibles.
4. Lorsque vous n'avez plus besoin des fichiers cryptés, cliquez sur **Terminer**. *Une fois que vous aurez cliqué sur Terminer, les fichiers cryptés ne seront plus disponibles.*

Utilisation de l'utilitaire de déverrouillage administrateur pour effectuer un téléchargement à partir d'un serveur maintenant en mode Administrateur

1. Double-cliquez sur **cmgau.exe** pour lancer l'utilitaire.

   ou

   À l'emplacement de l'utilitaire de déverrouillage administrateur, ouvrez une invite de commande et saisissez **cmgau.exe**.
2. Sélectionnez **Non, effectuer un téléchargement à partir d'un serveur maintenant**. Cliquez sur **Suivant >**.

3 Saisissez les informations suivantes (il est possible que certains champs soient déjà renseignés).

Serveur :	nom d'hôte complet du serveur clé, tel que keyserver.domaine.com
Numéro de port :	par défaut, 8050
Compte serveur :	utilisateur de domaine exécutant Key Server. Le format est domaine\nom d'utilisateur. L'utilisateur de domaine exécutant l'utilitaire doit être autorisé à effectuer le téléchargement à partir du serveur clé.
MCID :	ID de l'ordinateur, par exemple IDordinateur.domaine.com
DCID :	huit premiers chiffres de l'identité Shield à 16 chiffres

Cliquez sur **Suivant >**.

Un message vous indique que les données concernant la clé ont été correctement déverrouillées. Les fichiers sont alors accessibles.

4 Lorsque vous n'avez plus besoin des fichiers cryptés, cliquez sur **Terminer**. *Une fois que vous aurez cliqué sur Terminer, les fichiers cryptés ne seront plus disponibles.*

Utilisation de l'utilitaire de déverrouillage administrateur pour effectuer un téléchargement à partir d'un serveur maintenant en mode Forensic

1 À l'emplacement de l'utilitaire de déverrouillage administrateur, ouvrez une invite de commande et saisissez **cmgau.exe -f**.

2 Sélectionnez **Non, effectuer un téléchargement à partir d'un serveur maintenant**. Cliquez sur **Suivant >**.

3 Saisissez les informations suivantes (il est possible que certains champs soient déjà renseignés).

URL du serveur périphérique :	URL complète du serveur périphérique. Si Enterprise Server est antérieur à la version 7.7, le format est le suivant : https://deviceserver.domaine.com:8081/xapi Si Enterprise Server est ultérieur à la version 7.7, le format est le suivant : https://deviceserver.domaine.com:8443/xapi/
Administrateur Dell :	Nom de l'administrateur disposant des certificats d'administrateur Forensic (activés dans le serveur Enterprise), tel que jdoe
Mot de passe :	mot de passe de l'administrateur Forensic
MCID :	ID de l'ordinateur, par exemple IDordinateur.dell.com
DCID :	huit premiers chiffres de l'identité Shield à 16 chiffres

Cliquez sur **Suivant >**.

Un message vous indique que les données concernant la clé ont été correctement déverrouillées. Les fichiers sont alors accessibles.

4 Lorsque vous n'avez plus besoin des fichiers cryptés, cliquez sur **Terminer**. *Une fois que vous aurez cliqué sur Terminer, les fichiers cryptés ne seront plus disponibles.*


0 XXXXXA0 X