Dell Data Protection | Encryption

Utilità di amministrazione

2014-05

Indice

1 Utilità di download amministrativa 5

Utilizzo dell'utilità di download amministrativa in modalità amministrazione **5**

Utilizzo dell'utilità di download amministrativa in modalità forense **6**

2 Utilità di avvio amministrativa 7

Utilizzo dell'utilità di avvio amministrativa in modalità amministrazione **7**

Sintassi per la modalità amministrazione 7

Utilizzo dell'utilità di avvio amministrativa in modalità forense **8**

Sintassi per la modalità forense. 8

Utilizzo dell'utilità di avvio amministrativa in modalità file di backup **9**

Sintassi per la modalità file di backup 9

3 Utilità di sblocco amministrativa 11

Utilizzo dell'utilità di sblocco amministrativa per lavorare non in linea con un file scaricato in precedenza **11**

Utilizzo dell'utilità di sblocco amministrativa per eseguire l'azione "download da un server ora" in modalità amministrazione. **11**

Utilizzo dell'utilità di sblocco amministrativa per eseguire l'azione "download da un server ora" in modalità forense. **12**

1

Utilità di download amministrativa

Questa utilità consente di scaricare un pacchetto di materiali chiave da utilizzare su un computer non connesso al server aziendale. Le utilità di amministrazione possono quindi utilizzare i pacchetti in modalità non in linea.

Questa utilità sfrutta uno dei seguenti metodi per scaricare un pacchetto di materiali chiave, a seconda del parametro della riga di comando passato all'applicazione:

- **Modalità amministrazione**: usata se il parametro **-a** viene passato sulla riga di comando o se non viene usato nessun parametro della riga di comando.
- **Modalità forense**: usata se il parametro **-f** viene passato sulla riga di comando.

I file di registro si trovano in:

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

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

Utilizzo dell'utilità di download amministrativa in modalità amministrazione

1. Fare doppio clic su **cmgad.exe** per avviare l'utilità.

   Oppure

   Nel percorso in cui si trova l'utilità di download amministrativa, aprire un prompt dei comandi e digitare **cmgad.exe -a** (o cmgad.exe).

2. Immettere le seguenti informazioni (alcuni campi potrebbero essere precompilati).

Server:	nome host completo del server chiave, ad esempio serverchiave.dominio.com
Numero di porta:	il numero di porta predefinito è 8050
Account server:	l'utente di dominio utilizzato per eseguire il server chiave. Il formato è dominio\nome utente. L'utente di dominio che esegue l'utilità deve essere autorizzato a effettuare il download dal server chiave
MCID:	ID della macchina, ad esempio IDmacchina.dominio.com
DCID:	prime otto cifre dell'ID Shield di 16 cifre

   Fare clic su **Next >** (Avanti).

3. Nel campo **Passphrase**, digitare una passphrase per proteggere il file di download. La passphrase deve essere lunga almeno otto caratteri e contenere almeno una lettera e un numero.

   Confermare la passphrase.

   Accettare il nome predefinito e il percorso in cui verrà salvato il file oppure fare clic su **...** per scegliere un percorso diverso.

   Verrà visualizzato un messaggio, che indica che il materiale chiave è stato sbloccato. A questo punto sarà possibile accedere ai file.

4. Una volta completata l'operazione, fare clic su **Finish** (Fine).

Utilizzo dell'utilità di download amministrativa in modalità forense

1. Nel percorso in cui si trova l'utilità di download amministrativa, aprire un prompt dei comandi e digitare **cmgad.exe -f**.
2. Immettere le seguenti informazioni (alcuni campi potrebbero essere precompilati).

   URL del server del dispositivo: URL completo del server del dispositivo

   Se il server aziendale in uso è precedente alla versione 7.7, il formato sarà https://serverdispositivo.dominio.com:8081/xapi

   Se la versione del server aziendale in uso è 7.7 o successiva, il formato sarà https://serverdispositivo.dominio.com:8443/xapi/

   Amministratore : nome dell'amministratore con credenziali di amministrazione forense (abilitate nel server aziendale), ad esempio jdoeDell

   Password: password dell'amministratore forense

   MCID: ID della macchina, ad esempio IDmacchina.dominio.com

   DCID: prime otto cifre dell'ID Shield di 16 cifre

   Fare clic su **Next >** (Avanti).
3. Nel campo **Passphrase**, digitare una passphrase per proteggere il file di download. La passphrase deve essere lunga almeno otto caratteri e contenere almeno una lettera e un numero.

   Confermare la passphrase.

   Accettare il nome predefinito e il percorso in cui verrà salvato il file oppure fare clic su **...** per scegliere un percorso diverso.

   Verrà visualizzato un messaggio, che indica che il materiale chiave è stato sbloccato. A questo punto sarà possibile accedere ai file.
4. Una volta completata l'operazione, fare clic su **Finish** (Fine).

2

Utilità di avvio amministrativa

Questa utilità di riga di comando consente agli amministratori di sbloccare file crittografati comuni o dell'utente su un computer durante l'esecuzione di un processo.

Questa utilità viene usata per avviare processi dalla console di gestione. L'utilità deve essere copiata sul computer client e qualsiasi processo che richiede accesso a file crittografati comuni o dell'utente viene modificato per eseguire questa utilità, passando la riga di comando per il processo di gestione all'utilità. Con la chiusura di un processo viene chiusa anche l'utilità.

Questa utilità sfrutta uno dei seguenti metodi per sbloccare file, a seconda del parametro della riga di comando passato all'applicazione:

- Modalità amministrazione: nessun parametro richiesto.
- Modalità forense: usata se il parametro **-f** viene passato sulla riga di comando.
- Modalità file di backup: usata se il parametro **-b** viene passato sulla riga di comando.

I file di registro si trovano in:

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

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

Utilizzo dell'utilità di avvio amministrativa in modalità amministrazione

Sintassi per la modalità amministrazione

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

Parametri della modalità amministrazione	Descrizione
-k	Indica che deve essere utilizzata Kerberos (Modalità amministrazione). CmgAlu richiede il flag-k per lavorare in Modalità amministrazione.
X	Livello di log. I livelli di log vanno da 0 a 5 (0 è il livello senza log/5 è il livello di debug).
ServerPrincipal	Account AD (account di dominio) sotto cui si esegue il server chiave.
Porta	Porta TCP su cui connettere il server chiave.
Server	Nome/indirizzo IP del server chiave.
-r	Ordina all'utilità di caricare il nome del server chiave e l'MCID (o SCID) del computer dal registro. Se il parametro –r non viene specificato, sarà necessario fornire il nome del server chiave e l'MCID (o SCID).
MCID	ID del dispositivo da sbloccare. MCID è definito anche come ID univoco del dispositivo o nome host.

Parametri della modalità amministrazione	Descrizione
SCID	ID Shield del dispositivo da sbloccare. SCID è definito anche DCID o ID di ripristino.
-?	Guida per riga dei comandi.

Utilizzo dell'utilità di avvio amministrativa in modalità forense

Sintassi per la modalità forense

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

Parametri della modalità forense	Descrizione
-f	Indica che deve essere utilizzata la modalità forense.
AdminName	Nome utente dell'amministratore con credenziali di amministrazione forense.
AdminPwd	Password dell'amministratore forense.
URL	URL completo del server del dispositivo. Se il server aziendale in uso è precedente alla versione 7.7, il formato sarà https://serverdispositivo.dominio.com:8081/xapi Se la versione del server aziendale in uso è 7.7 o successiva, il formato sarà https://serverdispositivo.dominio.com:8443/xapi/
-r	Ordina all'utilità di caricare l'URL del server del dispositivo e l'MCID (o SCID) del computer dal registro. Se il parametro –r non viene specificato, è necessario fornire l'URL/il server e l'MCID (o SCID).
X	Livello di log. I livelli di log vanno da 0 a 5 (0 è il livello senza log/5 è il livello di debug).
MCID	ID del dispositivo da sbloccare. MCID è definito anche come ID univoco del dispositivo o nome host.
SCID	ID Shield del dispositivo da sbloccare. SCID è definito anche DCID o ID di ripristino.
-?	Guida per riga dei comandi.

Utilizzo dell'utilità di avvio amministrativa in modalità file di backup

Sintassi per la modalità file di backup

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

Parametri della modalità file di backup	Descrizione
X	Livello di log. I livelli di log vanno da 0 a 5 (0 è il livello senza log/5 è il livello di debug).
-b"FilePath"	Il percorso del file di sistema per il file di backup, in genere sia un file di ripristino LSA o di un file di output scaricato da CmgAd.
BackupPwd	La password utilizzata per creare il file di backup.
-?	Guida per riga dei comandi.

3

Utilità di sblocco amministrativa

Questa utilità consente di accedere ai file crittografati SDE, comuni o dell'utente, su un'unità slave, un computer avviato in un ambiente preinstallato o un computer a cui un utente abilitato non ha effettuato l'accesso.

L'utilità sfrutta il seguente metodo per scaricare un pacchetto di materiali chiave:

- Modalità amministrazione: nessun parametro richiesto. È la modalità predefinita.
- Modalità forense: usata se il parametro **-f** viene passato sulla riga di comando.

I file di registro si trovano in:

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

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

Utilizzo dell'utilità di sblocco amministrativa per lavorare non in linea con un file scaricato in precedenza

Se si sceglie di lavorare non in linea con un file scaricato in precedenza, CMGAu funziona nello stesso modo, a prescindere da come viene avviata; ovvero, il processo è identico se si fa doppio clic sul file .exe per avviare l'utilità, se si avvia senza parametri nella riga di comando o se si avvia tramite il parametro -f nella riga di comando.

1. Fare doppio clic su **cmgau.exe** per avviare l'utilità.
2. Selezionare **Yes, work offline with a previously downloaded file** (Sì, lavora non in linea con un file scaricato in precedenza). Fare clic su **Next >** (Avanti).
3. Nel campo **File scaricato:** cercare il percorso del materiale chiave salvato. Il file è stato salvato durante l'utilizzo dell'utilità di download amministrativa.

   Nel campo **Passphrase** immettere la passphrase usata per proteggere il file del materiale chiave. La passphrase è stata impostata durante l'utilizzo dell'utilità di download amministrativa.

   Fare clic su **Next >** (Avanti).

   Verrà visualizzato un messaggio, che indica che il materiale chiave è stato sbloccato. A questo punto sarà possibile accedere ai file.
4. Dopo aver finito di lavorare sui file crittografati, fare clic su **Finish** (Fine) *Dopo aver fatto clic su Finish, non sarà più possibile accedere ai file crittografati.*

Utilizzo dell'utilità di sblocco amministrativa per eseguire l'azione "download da un server ora" in modalità amministrazione.

1. Fare doppio clic su **cmgau.exe** per avviare l'utilità.

   Oppure

   Nel percorso in cui si trova l'utilità di sblocco amministrativa, aprire un prompt dei comandi e digitare **cmgau.exe**.
2. Selezionare **No, perform a download from a server now** (No, esegui il download da un server ora). Fare clic su **Next >** (Avanti).

3 Immettere le seguenti informazioni (alcuni campi potrebbero essere precompilati).

Server:	nome host completo del server chiave, ad esempio serverchiave.dominio.com
Numero di porta:	il numero di porta predefinito è 8050
Account server:	l'utente di dominio utilizzato per eseguire il server chiave. Il formato è dominio\nome utente. L'utente di dominio che esegue l'utilità deve essere autorizzato a effettuare il download dal server chiave
MCID:	ID della macchina, ad esempio IDmacchina.dominio.com
DCID:	prime otto cifre dell'ID Shield di 16 cifre

Fare clic su **Next >** (Avanti).

Verrà visualizzato un messaggio, che indica che il materiale chiave è stato sbloccato. A questo punto sarà possibile accedere ai file.

4 Dopo aver finito di lavorare sui file crittografati, fare clic su **Finish** (Fine). *Dopo aver fatto clic su Finish, non sarà più possibile accedere ai file crittografati.*

Utilizzo dell'utilità di sblocco amministrativa per eseguire l'azione "download da un server ora" in modalità forense.

1 Nel percorso in cui si trova l'utilità di sblocco amministrativa, aprire un prompt dei comandi e digitare **cmgau.exe -f**.

2 Selezionare **No, perform a download from a server now** (No, esegui il download da un server ora). Fare clic su **Next >** (Avanti).

3 Immettere le seguenti informazioni (alcuni campi potrebbero essere precompilati).

URL del server del dispositivo: URL completo del server del dispositivo

Se il server aziendale in uso è precedente alla versione 7.7, il formato sarà https://serverdispositivo.dominio.com:8081/xapi

Se la versione del server aziendale in uso è 7.7 o successiva, il formato sarà https://serverdispositivo.dominio.com:8443/xapi/

Dell Amministratore:	nome dell'amministratore con credenziali di amministrazione forense (abilitate nel server aziendale), ad esempio jdoe
Password:	password dell'amministratore forense
MCID:	ID della macchina, ad esempio IDmacchina.dell.com
DCID:	prime otto cifre dell'ID Shield di 16 cifre

Fare clic su **Next >** (Avanti).

Verrà visualizzato un messaggio, che indica che il materiale chiave è stato sbloccato. A questo punto sarà possibile accedere ai file.

4 Dopo aver finito di lavorare sui file crittografati, fare clic su **Finish** (Fine). *Dopo aver fatto clic su Finish, non sarà più possibile accedere ai file crittografati.*


0 XXXXXA0 X