LDT (Linux Diagnostic Tool) の取得方法

2019/1/31

項番	実施内容	確認
0	**事前準備**	
0-1	参考資料の確認 この手順は、以下の Advanced Threat Defense 4.6.0 CLI Reference Guide を参照して作成しています。 詳細は、CLI Reference Guideの項目を参照してください。 **Advanced Threat Defense 4.6.0 CLI Reference Guide** https://kc.mcafee.com/corporate/index?page=content&id=PD28106 p16 **run ldt** コマンド及び各パラメータの説明が記載されております。 p30 **show hardware** パラメータ "ldtlog" についての説明が記載されております。 LDT (Linux Diagnostic Tool) は、主にATDのハードウェア障害の調査を行う際に必要な情報となります。 部品交換や筐体交換を判断するためには必須で取得いただく情報です。 **注意** LDTファイルの生成処理では、ATDの負荷が上がります。 その為、LDTファイルの取得は負荷の低い時間帯での実施をご検討ください。 ATD 4.4以下のバージョンについては、従来通りUSBによる取得が必要となりますので、以下のドキュメントを参照してください。 **McAfee Linux Diagnostic Tool Reference Guide** https://kc.mcafee.com/corporate/index?page=content&id=PD27890	☐
0-2	必要な機器 LDTファイルは、CLIからファイル生成を実行し、GUIまたはSCPでファイルをダウンロードします。 その為、以下が可能な端末を準備します。 ・ GUIに接続できる端末 ブラウザに「https://<ATD IP Address>/」を入力し、ATDのGUIにログインできる端末をご利用ください。 ・ CLIで接続するためのソフトウェアがインストールされている端末 ATDにCLIで接続する際に、PuttyやTeraTerm等のソフトウェアを使用します。 ・ SCPで接続するためのソフトウェアがインストールされている端末 ATDにSCP接続する際に、WinSCPやFilezilla等のソフトウェアを使用します。 本手順では、GUIからのダウンロード方法 (2a) とSCPでのダウンロード方法 (2b) の両方を記載いたします。	☐

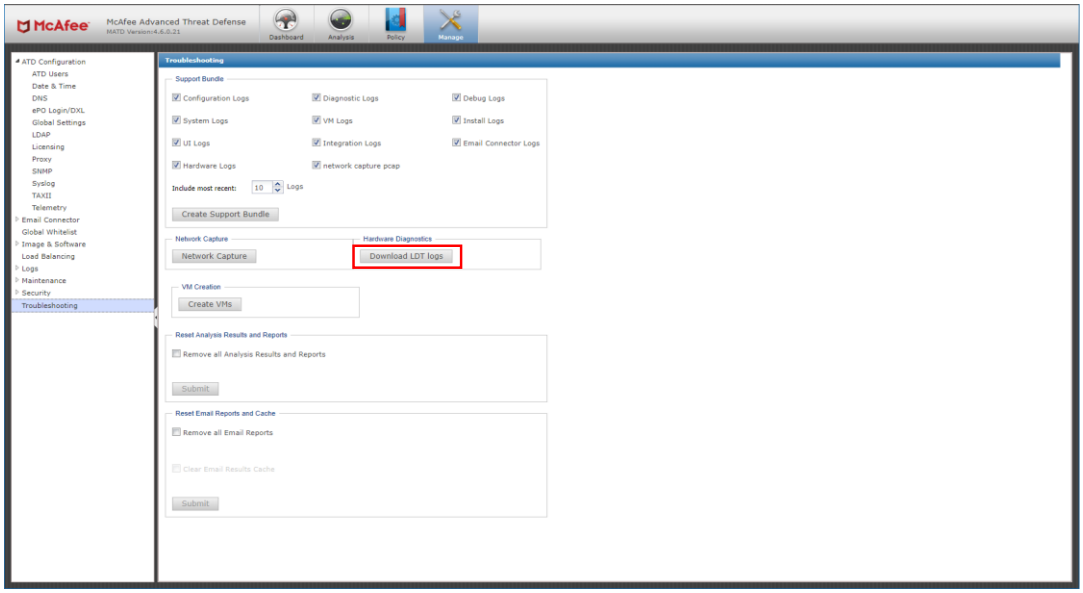
1	LDTファイルの生成	
1-1	ATDにCLIでログイン 対象のATDに対し、CLIでログインします。 CLIのアカウント：**cliadmin** CLIのパスワード：********	□

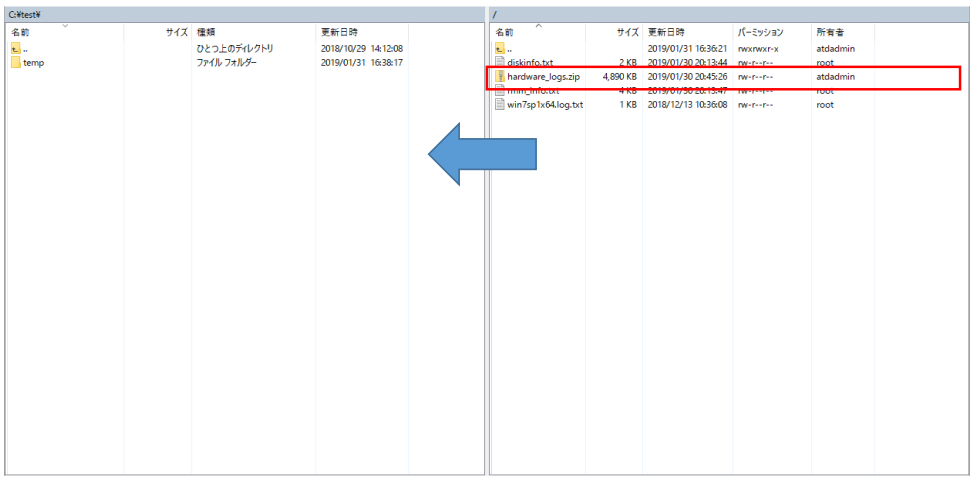
1-2	LDTファイル の生成状況の確認
	"**run ldt status**" にて、LDTファイルの生成処理が実行されていないことを確認 します。
	実行例）
	`ATD-3000> run ldt status`
	`LDT log collection is not running`
		□

1-3	LDTファイルを生成
	"**run ldt tool**" を実行してLDTファイルの生成処理を開始します。
	実行例）
	`ATD-3000> run ldt tool`
	`NOTICE: running the log collection tool may impact system performance.`
	`Running LDT log collection. Please stand by.`
	`LDT log collection has been started`
	LDTファイルの生成処理は、対象機器の負荷等に依存しますが、30～40分程度要します。
	生成処理はATDの負荷が上がりますので、実行する時間帯などにご注意ください。
		□

1-4	LDTファイルの生成状況の確認
	"**run ldt status**" でLDTファイルの生成処理が完了していることを確認します。
	実行例）
	`ATD-3000> run ldt status`
	`LDT log collection is not running`
	`Use 'show hardware ldtlog' to view summary.`
		□

1-5	LDTファイルのsummary.txtを確認
	"**show hardware ldtlog**" にて、LDTファイルに含まれる一部の情報をまとめた summary.txt の内容を表示することができます。
	全ての内容を表示するには、スペースキーまたはエンターキーを押してください。
	途中で終了する場合や (END) が表示された場合は、「**q**」を入力して、表示画面を終了することができます。
	実行例）内容は割愛しています。
	`ATD-3000> show hardware ldtlog`
	`WARNING: terminal is not fully functional`
	`/vedata/logs/ldt/summary.txt  (press RETURN)`
	
	`date logs collected: Wed Jan 30 03:45:24 PST 2019`
	`>>>>>> System Information`
	`Manufacturer: McAfee, Inc.`
	`Product Name: ATD-3000`
	`...`
	
	`>>>>>> Important Events: (from ipmi_sel.txt)`
	`...`
	`...`
	
	`>>>>>> Firmware Status`
	
	`No updates available for controller or HDD firmware.`
	
	`~`
	`~`
	`~`
	`(END)`
	生成したLDTファイルは、GUIからの取得 (2a) またはSCPでの取得 (2b) を実施してください。
		□

2a	LDTファイルの取得 (GUI)	
2a-1	ATDにGUIでログイン ブラウザに対象のATDのIPアドレスを入力し、GUIでログインします。 https://<ATD IP Address>/ GUIのアカウント：**admin** GUIのパスワード：******** ※上記のアカウント名はデフォルトの名前になります。	□
2a-2	LDTファイルのダウンロード [Manage] > [**Troubleshooting**] にて、[**Download LDT logs**] をクリックしてください。  上記にて、"**atd_LDT_log.zip**" がダウンロードできます。 **GUIでのLDTファイルのダウンロード方法は以上です。**	□

2b	LDTファイルの取得 (SCP)	
2b-1	SCPでATDにログイン SCP接続が行えるソフトウェア (FilezillaやWinSCP等) にて、ATDにアップロードアカウントでログインします。 アップロードアカウント：atdadmin アップロードパスワード：******** ※上記のアカウント名はデフォルトの名前になります。	□
2b-2	LDTファイルをダウンロード ログインしたディレクトリ配下に "**hardware_logs.zip**" があることを確認し、ファイルをダウンロードします。 実行例）WinSCPを使用した場合（"**hardware_logs.zip**" をドラッグ&ドロップしてダウンロードすることができます。）  **SCPでのLDTファイルのダウンロード方法は以上です。**	□

Apx	LDTファイルの生成処理の中断	
	LDTファイルの生成処理を中断する場合の手順について、以下の通り記載します。 尚、処理を中断した場合、最初からの実施となります。	
Apx-1	ATDにCLIでログイン 対象のATDに対し、CLIでログインします。 CLIのアカウント：**cliadmin** CLIのパスワード：********	☐

Apx-2	LDTファイル の生成状況の確認
	"**run ldt status**" にて、LDTファイルの生成処理が実行されていることを確認します。
	実行例）
	`ATD-3000> run ldt status`
	`LDT log collection in progress`
		☐

Apx-3	LDTファイルの生成処理の中断
	"**run ldt abort**" にて、LDTファイルの生成処理を中断します。
	実行例）
	`ATD-3000> run ldt abort`
	`LDT log collection aborted`
		☐

Apx-4	LDTファイルの生成状況の確認
	"**run ldt status**" でLDTファイルの生成処理が実行されていないことを確認します。
	実行例）
	`ATD-3000> run ldt status`
	`LDT log collection is not running`
		☐

	LDTファイルの生成処理の中断方法は以上です。	