# LT Auditor+

## Windows Assessment Build21 Release

Installation & Configuration Guide

#### **Table of Contents**

CHAPTER1 — OVERVIEW
CHAPTER2 — NSTALLITALDITOR+WINDOWSASSESSIVIENT
System Requirements.       3         Prerequisites for the LT Auditor+ Windows Assessment installation       3         LT Auditor+ WINDOWS ASSESSMENT COMPONENTS       3         INSTALLATION STEPS.       4         LT Auditor+ Windows Assessment Manager Component (LTWAMC)       4
CHAPTER3 - SETUPSCANS WITH LTAUDITOR+WINDOWS ASSESSIVENT (LTWA)
CHAPTER4-SCANSCRIPTS
Active Directory Scans (Prefix AD_)
CHAPTERS REPORTINGFORLTAUDITOR+WINDOWSASSESSIVENT
CHAPTER6 — SETTINGUP DELETION JOB
APPENDIXA — POWERSHELLSCRIPTS
APPENDIXB — SETTINGUP ACTMEDIRECTORYSCANSONA MACHINETHATIS NOTA DOMAINCONTROLLER
PREREQUISITES:
APPENDIXC-TROUBLESHOOTING
CHECKPOINTS
APPENDIXD — WHAT IS NEW IN LTAUDITOR+WINDOWSASSESSIVENTBUILD21
APPENDIXE — UPGRADING TO LT AUDITOR+WINDOWSASSESSIVIENTBUILD21

## Chapter 1 – Overview

The LT Auditor+ Windows Assessment (LTWA) application can be used to collect and record information on configuration settings, vulnerabilities and permissions on the following entities:

- Active Directory Users, Groups, and other objects.
- Windows (NTFS) File Systems such as DAS (Direct Attached Storage), SAN (Storage Area Networks) and NAS (Network Attached Storage) systems.

LTWA integrates into the LT Auditor+ framework and can leverage audit data collected with other LT Auditor+ modules. Insights can now be gained on who has the rights to access critical file shares while documenting who does access these file systems. The architecture diagram below shows how the LTWA integrates into the LT Auditor+ ecosystem.



## Chapter 2 – Install LT Auditor+ Windows Assessment

The section provides an overview of how LTWA is installed and configured. Included in this section are systems requirements and prerequisites. Please review "APPENDIX D" for details on what is new in LT Auditor+ Windows Assessment SP3.

#### **System Requirements**

• Meet the same systems requirement to install an LT Auditor+ Windows Agent described in the LT Auditor+ Installation Guide.

Prerequisites for the LT Auditor+ Windows Assessment installation

- Must have LT Auditor+ installed.
- PowerShell 3.0 and above.

Installer must have administrative privileges to install LT Auditor+ Windows Assessment.

Note: Please review the LT Auditor+ Installation Guide for documentation on installation or upgrade to LT Auditor+.

#### LT Auditor+ Windows Assessment Components

The LT Auditor+ Windows Assessment component is included in the standard LT Auditor+ Build21 release download. After you download and extract the files, the following file should be available for the installation process:

#### Setup\_LT\_Assessment\_Manager\_x64.exe

#### **Installation Steps**

#### LT Auditor+ Windows Assessment Manager Component (LTWAMC)

The Manager component (LTWAMC) can be installed on any machine as long as the prerequisite requirements are met. Blue Lance recommends that LTWAMC be installed on the machine that hosts the LT Auditor+ Manager.

In the following section, the term Setup.exe will be used to refer to **Setup\_LT\_Assessment\_Manager\_x64.exe**.

1. Run Setup.exe file from the root of the installation folder to launch the installation of the LTWAMC.

LT Auditor+ Windows Assessment - InstallShield Wizard				
LT Auditor + Windows Assessment requires the following items to be installed on your computer. Click Install to begin installing these requirements.				
Status Requirement				
Pending LT Auditor + Agent (x64)				
Install Cancel				

2. Click Install to bring up the following screen.



3. Click Next to bring up the License Agreement screen.

LT Auditor + Windows Assessment - InstallShield Wizard	x
License Agreement Please read the following license agreement carefully.	
Software License Agreement	
IMPORTANT - READ CAREFULLY: This is a legal agreement between you and Blue Lance, Inc. by which certain software (and accompanying materials) are being licensed, not sold, to you. By clicking the 'I accept the terms of the license agreement' icon, you agree to the terms and conditions of this Agreement. If you do not agree to these terms and conditions, you are not licensed to use the Software; therefore, you must not install the software and you must promptly return the Software (including all accompanying materials) to Blue Lance, Inc.	
I accept the terms in the license agreement	
$\bigcirc$ I <u>d</u> o not accept the terms in the license agreement	
InstallShield	_
< <u>B</u> ack <u>N</u> ext > Cancel	

Read the Software License Agreement, and if acceptable, click on "I accept the license terms in the license agreement" and click Next.

B LT Auditor + Windows Assessment - InstallShield Wizard	x
Ready to Install the Program         The wizard is ready to begin installation.	
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
InstallShield	

#### 4. Click Install to start the installation.

👸 LT Aud	litor + Windows Assessment - InstallShield Wizard 🗖 🗖 🗙
-	LT Auditor+ Windows Assessment ram features you selected are being installed.
15	Please wait while the InstallShield Wizard installs LT Auditor + Windows Assessment. This may take several minutes.
	Status:
	Starting services
InstallShield	
	< <u>B</u> ack <u>N</u> ext > Cancel



5. Click Finish to complete the installation of the LTWAMC.

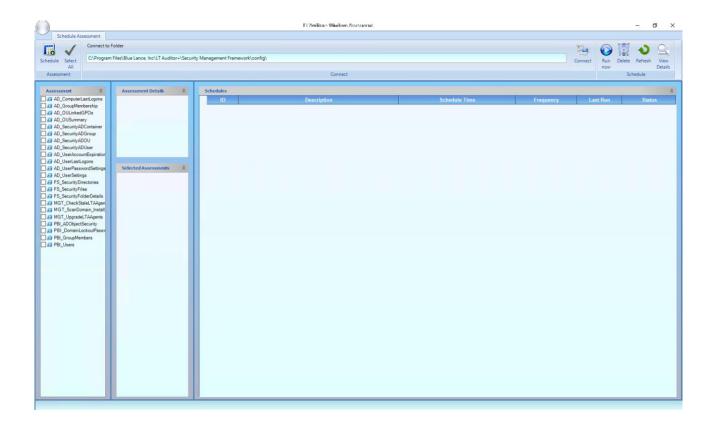


LTAWMC is installed to the LT Auditor+ folder that hosts the LT Auditor+ SMF installation. The same module can be installed on other Windows machines in the environment as long as an LT Auditor+ Agent is on the machine.

## Chapter 3 – Setup Scans with LT Auditor+ Windows Assessment (LTWA)

This section provides instructions on how to use the LT Auditor+ Windows Assessment Console (LTWAC) to schedule scans. This application is installed on the machine where the LTWAMC was installed.

To launch the LTWAC, click Start  $\rightarrow$  All Programs  $\rightarrow$  Blue Lance, Inc. $\rightarrow$  Windows Assessment Console to bring up the following window.



The left pane (Assessment Pane) displays a list of scripts that can be selected for any scan job. Click on any script to display the possible reports that be generated in the Assessment Details pane.

The following events can be performed with the LTWAC.

#### **Schedule Scan Jobs**

To schedule a scan job:

- 1. Select one or more scripts listed in the Assessment pane.
- 2. Click the Schedule button to bring up the Schedule window.

Schedule ×						
Schedule	2					
Select the settings for the schedule job and click the Save button.						
Description :	SecurityDirectories,	Security	Files		Save (	Cancel
	Details				Acti	on
Schedule						\$
Frequency :	Single	~	Start Time :	4:47:3	31 PM	<b>÷</b>
Day of Week :	Sunday	$\checkmark$	Date :	09/04/	2014	~
Data Transfe	Mode					\$
● LT Auditor+ ○ Syslog	settings (Default)		Syslog Setting Server : Port :	s 1468		
Parameters						\$
Files Start	ude Inherited Permiss ing Path de Inherited Permissi		0	Valu	ue	^ 
Note : Please exit ou	t of edit mode from Va	alue field	l before clicki	ng on Si	ave button.	>

- 3. Select the desired frequency for the job.
- 4. Select Data Transfer Mode. The default data transfer mode leverages LT Auditor+'s communication protocols to transfer data to the LT Auditor+ Manager. This is the recommended approach; however, customers can choose to transfer using a syslog server. To use syslog:
  - a. Select Syslog and enter the IP address of the server where the LT Auditor+ Syslog Processor has been installed.
  - b. Select the protocol to use for sending data collected during the scan to the syslog server.



Please review Appendix B for additional configuration information when using syslog.

- 5. Input parameters that can be passed for certain scan jobs. If a selected script requires parameters, the Parameters section will display the default parameters that can be modified. Details on parameters are discussed in "APPENDIX A."
- 6. Click the Save 🛄 button to save the scan job.

#### **Job Status**

The status of any job is displayed by clicking the + symbol that prefixes all scheduled jobs. Details are available on whether the job ran successfully or failed.

#### **Delete Scan Jobs**

To delete a scan job:

- 1. Click on the desired scan job to delete in the Schedule pane.
- 2. Right-click and select Delete or click the Delete key button.

#### **Run Now**

To run a job immediately:

- 1. Click on the desired scan job in the Schedule pane.
- 2. Right-click and select Run Now or click on the Run Now  $\heartsuit$  button.

#### **Connect to a Remote Server**

To schedule jobs on remote machines:

1. Click the Connect button and browse to the Security Management Framework (SMF) folder where LT Auditor+ has been installed.

Application Verifier		Name	Size	Туре	Date Modified
Blue Lance, Inc		Agent		File Folder File Folder	1/2/2014 7:28 A
IT Auditor+		Bin Casta		File Folder	12/26/2013 11:
Manager Console		Config		File Folder	12/26/2013 11:
Reporting Console		Manager			
Security Management Framework		Outbin		File Folder	1/3/2014 10:55
Agent	H	Requests	4.1/5	File Folder	1/2/2014 7:29
Di Bin		LTAudit.iif	12501015	File	12/26/2013 11:
Config		RebootNotRequired.txt	U KE	Document	12/26/2013 11:
Manager					
Dutbin					
Requests					
Syslog Device Service					
Windows Assessment					
🛅 Bonjour					
Common Files					
Dell					
	-				

2. Set up a scan job as described above.



Prior to clicking the Connect button, please ensure that you have a drive mapped to the target agent machine.

## Chapter 4 – Scan Scripts

The following table describes the scans that can be scheduled to run with the LTWAMC. Periodic scans can be run for the following categories:

### Active Directory Scans (Prefix AD\_)

Active Directory scans can be scheduled to collect information on Users, Groups, Organization Units and Computers.

Purpose	Scripts
Group Membership Information	AD_GroupMembership.ps1
Information on Users, Password Settings and Last Logon Activity	AD_UserAccountExpiration.ps1 AD_UserLastLogons.ps1 AD_UserPasswordSettings.ps1 AD_UserSettings.ps1
Computer Information	AD_ComputerLastLogons.ps1
Data on permissions (DACLS) assigned to Active Directory Objects	AD_SecurityADContainer.ps1 AD_SecurityADGroup.ps1 AD_SecurityADOU.ps1 AD_SecurityADUser.ps1
Information on OUs	AD_OULinkedGPOs.ps1 AD_OUSummary.ps1

Prior versions of LT Auditor+ Windows Assessment scans did not have any prefix in the name. If those files have been scheduled to run, please delete schedules and files and proceed to set up new scheduled scans.

### File System Scans (Prefix FS\_)

File system scans can be scheduled to collect information on permissions assigned to principals for scanned files and folders.

Purpose	Scripts
	FS_SecurityDirectories.ps1 FS_SecurityFolderDetails.ps1
Scan Files	FS_SecurityFiles.ps1

### Scans for LT Auditor+ Power BI Panels (Prefix PBI\_)

File system scans can be scheduled to collect information on permissions assigned to principals for scanned files and folders.

Purpose	Scripts
Scans required for LT Auditor+ Power BI panels	PBI_ADObjectSecurity.ps1 PBI_DomainLockoutPasswordPolicy.ps1 PBI_GroupMembers.ps1 PBI_Users.ps1

### Scans for LT Auditor+ Maintenance (Prefix MGT\_)

These scans can be scheduled to install, update and maintain LT Auditor+ Agents in the environment.

Purpose	Scripts
Scan to check status of LT Auditor+ Agents. Can be configured to delete stale agents, update IP Addresses and restart LT Auditor+ services on agents that are not active.	MGT_CheckStaleLTAAgents.ps1
Scan to check Active Directory domain for new computers (Workstations or Servers) that do not have LT AUDITOR+ installed. If such systems are discovered, the script proceeds to install LT Auditor+ Agent on these machines to ensure organizational auditing and compliance policies are met.	MGT_ScanDomain_Install_LTA_Agen
Scan to upgrade LT Auditor+ Agents with the latest updates.	MGT_UpgradeLTAAgents.ps1

ΝΟΤΕ

For maintenance scripts, the Windows Assessment service must be started with an account that has permissions to install LT Auditor+ on remote machines, as well as have access to read and update the LT Auditor+ database.

## Chapter 5 – Reporting for LT Auditor+ Windows Assessment

The default reports are created under the Windows Assessment reporting group as shown below:

LT Auditor + Report Console					
Report Help					
D 🕅 🖉 🗶 🕨 Generate Report 🔞 🗅 📴 🚱 🕼 🕼 🤪 🖓 🖓 🧐 Change Database 🔒					
BLVM02 - LTAProdu	ictionDB				
ET Auditor+ for Windows Enterprise Suite	Audit Sub Systems				
	Addit Sub Systems				
ET Auditor+ for Syslog Devices					
CT Auditor+ for NetWare	Audit Sub System				
Cyber Governance & Oversight Reports      Cyber Governance & Oversight Reports	10 Windows Assessment				
LT Auditor+ for Windows Assessment					
Windows Assessment					
Windows Assessment Reports					
E-D Group Membership Reports					
Group Memberships					
Members of Domain Admins/Enterprise Groups					
🧑 Groups Belonged To					
Groups Without Members					
🖃 📄 Last Logon Reports					
Users Who Have Not Logged In For 90 Days					
Users Who Have Never Logged In					
Password Settings Reports					
Users with Expired Passwords					
Users With Passwords That Never Expire					
Users who do not Require Passwords					
Account Expiration Reports					
1 User Accounts Expiring In 90 Days					
Expired User Accounts					
for accounts That Never Expire					
Active Directory Security Permissions Reports					
Security Principals on UDs     Security Permissions on Users					
Security Principals on Users					
Security Permissions on Groups					
Security Principals on Groups					
Security Permissions on Containers					
File/Folder Security Permissions Reports					
Security Permissions on Files					
Security Principals on Files					
Window Control (Control of the second s					
- Geounty Permissions on Folders					
Ownership/Security Permissions on Folders					
Dirganizational Unit (OU) Reports					
UU Summary					
⊡ User Settings Reports					
User Settings					
Users Without Email Addresses					
USers without managers					
	Connection & Alexandron Manderson District Channel Connection and Alexandron Manderson Connection				
	Currently Authenticated Windows User: BLUEINC\bluser License Expires on 1/1/2015 7:00:00 AM				

Click on any of the reports, and details on how to query a report are provided in the description field.

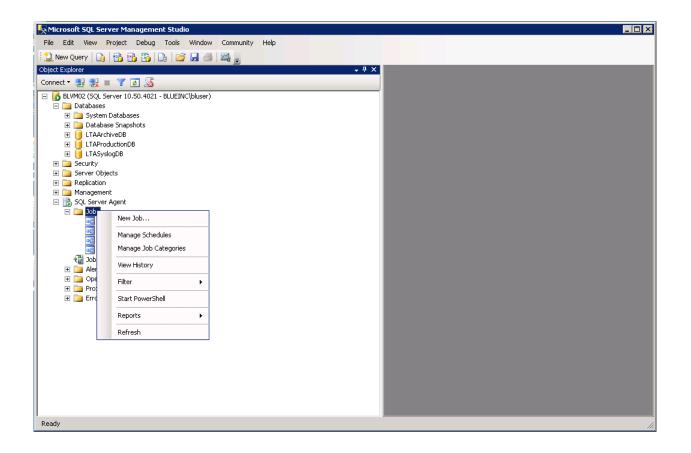
DLT Auditor + Report Console		_ <del>_</del> <del>_</del> <del>_</del> <del>_</del> <del>_</del>
Report Help		
📄 👩 🥖 🜻 🕨 Generate Report 🔞 📭 🍞 🕵	🗊 🎯 Change Database 🟦 💡	
🛛 🚺 BLVM02 - LTAProdu	LICTIONDB	
LT Auditor+ for Windows Enterprise Suite	Report Query Details	Advanced Settings
Of the second seco	Report Query Details	Auvanced Setunds
LT Auditor+ for NetWare	Statements New Edt Delete	Description Update
🗈 💑 LT Auditor+ Cross Platform Reports		()
🗈 🔮 Cyber Governance & Oversight Reports	Statement Name	To customize this query use the following parameters
Comparison of the set of the	Members of Domain Admins/Enterprise Groups	
Windows Assessment Reports		Depart Query Statement
😑 📄 Group Membership Reports		Report Query Statement
👘 Group Memberships		
Members of Domain Admins/Enterprise Groups		Users tab - To query for Member names (Sam Account Name)
Groups Belonged To		Objects tab - To query Group Names
- D Last Logon Reports		
Users Who Have Not Logged In For 90 Days		Date & Time - To query for a particular scan (Active only if % ShowAllScans=1)
		ShowAllScans=1)
⊟- D Password Settings Reports 		
User Passwords Expiring in 30 days		Advanced Auditing - Additional arguments
Users With Passwords That Never Expire		
👘 Users who do not Require Passwords		
Account Expiration Reports		%ShowAllScans=1 (Reports on all scans - Default will ONLY display last
User Accounts Expiring In 90 Days		scan)
Accounts That Never Expire		
Active Directory Security Permissions Reports		Example: %ShowAllScans=1 - Will display all scans collected with LT
🔞 Security Permissions on OUs		Auditor+.
🧓 Security Principals on OUs		
Geourity Permissions on Users     Geourity Principals on Users		
Security Finitepars on Osers		
Security Principals on Groups		
— m Security Permissions on Containers		
File/Folder Security Principals on Containers           Image: Security Permissions Reports		
Security Permissions Reports		
Security Principals on Files		
🛅 Ownership/Security Permissions on Files		
— Image of the security Permissions on Folders		
Ownership/Security Principals on Folders		
- 10 Olganizational on traditional on traditional of the points		
Image: The second se		
User Settings Reports		
User Settings Users Without Email Addresses		
Users Without Email Addresses		
E - O LT Auditor+ Utilities		
	Currently Authenticated Windows User: BLUEINC\bluser License Expires on 1/1/2015 7:00	00 AM

Please review the LT Auditor+ Configuration Guide for details on configuring and scheduling reports.

## Chapter 6 – Setting Up Deletion Job

Scheduling the deletion of Windows Assessments from the database is done by following these steps:

1. Log in to the Microsoft SQL Server Management Studio and navigate to the section "Jobs." Right-click and select "New Job..." to create a new job.



2. Enter the details as shown below.

📧 New Job				
Select a page	<u>S</u> Script 👻 🚺 Help			
General Steps Schedules Alerts	<u>N</u> ame: <u>D</u> wner:	DeleteAssessmentData		
Protifications Protocology Targets	<u>C</u> ategory:	[LT Auditor+]		
	<u>D</u> escription:			
Connection Server: BLVM02 Connection: BLUEINC\bluser View connection properties Progress Ready Ready	▼ <u>E</u> nabled			
			ОК	Cancel

3. Select Steps and click on New to create a new step, and enter the following

#### details: [dbo].[usys\_AssessmentDataFindForDelete] @SourceDBName = 'LTAProductionDB', @SourceDBSchemaName = 'dbo',

#### @DeleteBatchSize = 10000

Note: Select the Production Database only

📲 New Job			
Select a page	🛒 Script 👻 📑 H	Help	
General			
Steps	Job step list:		
Alerts	St., Name	Type On Success On Failure	
🛛 🚰 Notifications			
🚰 Targets	💽 New Job Step		_ 🗆 🗙
	Select a page	🔄 Script 👻 📑 Help	
	🚰 General		
	Advanced	Step name:	
		Find and Delete	
		Туре:	
		Transact-SQL script (T-SQL)	•
		Run as:	
		Database: LTAProductionDB	
Connection		Command: [dbo].[usys_AssessmentDataFindForDelete]	<u> </u>
		@SourceDBName = "LTAProductionDB",	
Server: BLVM02		@SourceDBSchemaName = 'dbo', @DeleteBatchSize = 10000	
		Open @DeleteBatchSize = 10000	
Connection: BLUEINC\bluser		Select All	
Uiew connect			
	Connection	Сору	
Progress		Paste	
Ready	Server: BLVM02		
riculy	Connection:	Parse	
	BLUEINC\bluser		
	Section properties		
			_
	Progress	4	
	Ready		
		Next Previ	ous
		OK Can	

4. Select Schedules and enter the details as shown below.

💽 New Job		
Select a page	🔄 Script 👻 📑 Help	
General Steps	Schedule list:	
Steps Schedules		
Alerts	ID Name	Enabled Description
Targets	New Job Schedule	
	Name:	
	Name:	Jobs in Schedule
	Schedule type:	Recurring 🔽 🗹 Enabled
	One-time occurrence	1/15/2014 Time: 3:40:50 PM 🚍
	Date:	
	Frequency	
	Occurs:	Daily
	Recurs every:	1 day(s)
Connection	Daily frequency	
Server:	<ul> <li>Occurs once at:</li> </ul>	12:00:00 AM
BLVM02		
Connection:	O Occurs every:	1 Starting at: 12:00:00 AM
BLUEINC\bluser		Ending at: 11:59:59 PM 🚍
View connection properties	Duration	
Progress	Start date:	1/15/2014 C End date: 1/15/2014 -
Ready		<ul> <li>No end date:</li> </ul>
No.	Summary	
	Description:	Occurs every day at 12:00:00 AM. Schedule will be used starting on 1/15/2014.
		OK Cancel Help

5. Click OK to save the details.

## ΝΟΤΕ

The deletion job retains the last assessment run, and all older jobs are deleted for each category.

## APPENDIX A – PowerShell Scripts

LT Auditor+ Windows Assessment uses PowerShell scripts to perform scans. The following table describes the available scripts and the parameters that are accepted for each script.

Script Name	Reports for this script	Parameters
AD_GroupMembership	Group Memberships	
	Members of Domain Admins/Enterprise	-
	Groups	
	Groups Belonged To	-
	Groups Without Members	
AD_UserLastLogons	Users Who Have Not Logged In For 90	
	Days	
	Users Who Have Never Logged In	
AD_Computers Last Accessed	Computers not accessed in the last 90	
	days	
	Computers that have never been	
	accessed	
AD_UserPasswordSettings	User Passwords Expiring In 30 days	
	Users with Expired Passwords	
	Users With Passwords That Never Expire	
	Users who do not Require Passwords	
AD_UserAccountExpiration	User Accounts Expiring In 90 Days	
	Expired User Accounts	
	Accounts That Never Expire	
AD_SecurityADOU	Security Permissions on OUs	
	Security Principals on OUs	
AD_SecurityADUser	Security Permissions on Users	
	Security Principals on Users	
AD_SecurityADGroup	Security Permissions on Groups	
	Security Principals on Groups	
AD_SecurityADContainer	Security Permissions on Containers	
	Security Principals on Containers	-
FS_SecurityFiles	Security Permissions on Files	FilesIncludeInherited,
	Security Principals on Files	FilesStartPath
	Ownership/Security Permissions on Files	
FS_SecurityDirectories	Security Permissions on Folders	FolderIncludeInherited,
-	Ownership/Security Permissions on	FolderStartPath
	Folders	
AD_OUSummary	OU Summary	
AD_OULinkedGPOs	OUs Linked with GPOs	
AD_UserSettings	User Settings	
	Users With no Email Addresses	1
	Users With no Managers	1

## APPENDIX B — Setting Up Active Directory Scans on a Machine That Is Not a Domain Controller

To run Active Directory scans on machines that are not Domain Controllers, you will need to install the PowerShell RSAT-AD and GPMC modules. Instructions to install these components are listed below.

#### **Prerequisites**:

- Operating System Windows 2012R2 and above.
- PowerShell version 3.0 and above.
- The Windows machine must be in the Active Directory domain.

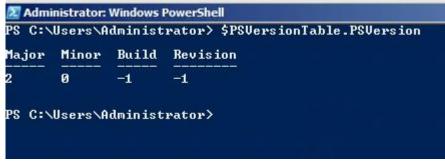
#### Installation:

- 1. Log in to Windows machine with a domain admin account.
- Open a PowerShell Window (Run as Administrator) and ensure that you can run PSHELL commands by running the following command: Set-ExecutionPolicy Unrestricted
- 3. Execute the following commands:
  - Import-Module ServerManager
  - Add-WindowsFeature RSAT-AD-PowerShell
  - Add-WindowsFeature –Name GPMC
- 4. Run Set-ExecutionPolicy Restricted to reset PowerShell settings.

## **APPENDIX C**—Troubleshooting

#### **Checkpoints**

- 1. Ensure that scanned data is received by the Kiwi Syslog Server.
- Check PowerShell versions for all agent servers. Supported versions are 2.0 and 3.0. To check, launch the PowerShell windows and run the command: \$PSVersionTable.PSVersion, and this should return the version information as shown below:



3. Ensure that you run the scans for Active Directory objects on a Windows Domain Controller.

#### **Error Messages**

Any error messages are logged to the Application log.

1. The term "Get-ADUser" is not recognized as the name of a cmdlet, function, script file or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

Resolution – Please run the scripts on an Active Directory environment.

2. Failed. Error trying to send message.

Resolution – Check the connectivity to the syslog server from the machine running the scripts.

Also check the application "log event id 5005" for detailed error.

## APPENDIX D — What is new in LT Auditor+ Windows Assessment Build21

- 1. Added scans for LT Auditor+ Power BI panels.
- 2. Added scan for automating the discovery and installation of LT Auditor+ on new machines in the environment.
- 3. Added scans to maintain and upgrade LT Auditor+ Agents.

## APPENDIX E — Upgrading to LT Auditor+ Windows Assessment BUILD21

To upgrade to SP3 follow these steps. (Note In the following section, the term Setup.exe will be used to refer to either

Setup\_LT\_Assessment\_Manager\_x64.exe or

**Setup\_LT\_Assessment\_Manager\_x32.exe** based on the operating system selected.

- 1. Download LT Auditor+ for Windows Assessment SP3 and extract the zip file.
- 2. On the manager machine, run Setup.exe to bring the following window.

LT Auditor+ Windows /	ssessment - InstallShield Wizard	x
This setup will perf Assessment'. Do yo	m an upgrade of 'LT Auditor+ Windows want to continue?	
	Yes No	

3. Click Yes to start the upgrade process, and the following screen will appear.

岁 LT Au	ditor + Windows Assessment - InstallShield Wizard
2	Resuming the InstallShield Wizard for LT Auditor+ Windows Assessment
	The InstallShield(R) Wizard will complete the installation of LT Auditor + Windows Assessment on your computer. To continue, click Next.
47	
	< Back Next > Cancel
Click Next to st	art the upgrade process.
	litor + Windows Assessment - InstallShield Wizard
	ditor + Windows Assessment - InstallShield Wizard
	ditor+ Windows Assessment - InstallShield Wizard
	ditor + Windows Assessment - InstallShield Wizard InstallShield Wizard Completed The InstallShield Wizard has successfully installed LT Auditor +
	ditor + Windows Assessment - InstallShield Wizard InstallShield Wizard Completed The InstallShield Wizard has successfully installed LT Auditor +
	ditor + Windows Assessment - InstallShield Wizard InstallShield Wizard Completed The InstallShield Wizard has successfully installed LT Auditor +
	ditor + Windows Assessment - InstallShield Wizard InstallShield Wizard Completed The InstallShield Wizard has successfully installed LT Auditor +
	ditor + Windows Assessment - InstallShield Wizard InstallShield Wizard Completed The InstallShield Wizard has successfully installed LT Auditor +

4.

5. Click Finish to complete.



Prior versions of LT Auditor+ Windows Assessment scans did not have any prefix (AD\_, FS\_) in the name. If those files have been scheduled to run, please delete schedules and files and proceed to set up new scheduled scans.