

LT Auditor+

Configuration Guide

Intellectual Property

Copyright © 2021

Blue Lance, LT Auditor+, and the Report Generator are registered trademarks of Blue Lance, Inc.

Microsoft, Windows 2003, Window 2008, Windows XP, Windows 7, Microsoft SQL Server 2005, Microsoft SQL Server 2008, and Microsoft SQL Server Express Edition are registered trademarks of Microsoft Corporation in the United States and other countries.

Novell, SUSE Linux and NetWare are registered trademarks of Novell, Inc.

Intel and Pentium are registered trademarks of Intel Corporation.

Oracle, Oracle 8*i*, Oracle 9*i*, Oracle 10*g*, Oracle 11*g* are trademarks of Oracle Corporation.

NetApp and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries.

EMC Isilon is a registered trademark of EMC² Corporation.

Blue Lance shall not be held accountable for technical or editorial errors within this document. This document is provided "as is" without warranty of any kind and is subject to change without notice.

Special Conventions

The following special icons are used in this document to alert the reader to important pieces of information:

Icons	Description
STOP	WARNING: Alerts the reader to a potential action, practice or situation that can result in major damage to data or the system. Damage is permanent and irreversible. Results may be contrary to what is expected or intended.
CAUTION	CAUTION: Alerts the reader to a potential action, practice or situation that can result in minor damage to data or the system. Results may be contrary to what is expected or intended.
ΝΟΤΕ	NOTE: Extra or supplementary information that needs to be emphasized to the reader. Can provide further context, instructions or understanding
TIP	TIP: Useful tips or pointers that can help the reader while they are using the product or this document.

BLUE LΔΠCE

Table of Contents

INTELLECTUAL PROPERTY	2
CHAPTER1-ABOUTTHE DOCUMENT	6
Document Purpose	
Document Audience	
Document Scope	
Using this Document	7
Document Structure	7
CHAPTER2-LTAUDITOR+WORKSPACE	
CONNECTING TO THE WORKSPACE	-
Manager Groups	
CREATING AGENT GROUPS	
Workstation Groups	
Removable Device:	
Windows Agent Groups	
Manager Groups	
Modifying Manager Group Settings	
Modifying Agent Group Settings	
NATIVE EVENT LOG ARCHIVE SETTINGS	
CHAPTER3—AUDITPOLICIES	24
Configuring LT Auditor+ Audit Policies	
Notes	
Objects:	
Classes:	
Attributes:	
File / Folders Settings – File System Filter	
Files and Folders:	
Description Settings – Native Event Log Filter	
All Descriptions	
CHAPTER4 — CONFIGURINGIMANAGER AND AGENTIOBS	
MANAGER DATA ROLLUP JOB	
Agent Data Transfer Job	
Сиѕтом Јов	
CHAPTER4-CONFIGURE THELT AUDITOR+REPORTCONSOLE	
Starting the Report Console	
REPORT GROUPS AND REPORT ARMS	
CREATING A REPORT QUERY	
Scheduling a Report	70
CHAPTER5—SECURINGLT AUDITOR+	71
AUTHENTICATING TO THE WORKSPACE	
LT Auditor+ Security Level 1	
LT Auditor+ Security Level 2	



Adding Authorized Users or Groups to the LT Auditor+ Reporting Console	. 79
APPENDIX A	. 83
Update Agents	. 83
APPENDIX B	. 86
Auditing EMC Isilon	. 86

Chapter 1 – About the Document

This chapter provides a general overview of this document and contains the following major subsections:

- •Document Purpose
- •Document Audience
- Document Scope
- Using this Document
- Getting Technical Support

Document Purpose

This document is intended to serve as a document that best describes the procedures and steps for Installing LT Auditor+. It focuses on the prerequisites, system requirements and pre-installation of LT Auditor+.

Document Audience

This document is intended for the following users:

Team or person responsible for using the LT Auditor+ application Team or person entrusted with deploying LT Auditor+ in the environment

Document Scope

The scope of this document includes information that will help you understand the functionalities of LT Auditor+.

The scope includes the following major topics:

- Description of key features
- Details on configuring and using LT Auditor+

Using this Document

This section explains the installation and configuration of the LT Auditor+.

Document Structure

The document is divided into the following chapters:

Chapter	Description
About the Document	Provides information about this document, including what it is used for, who should read it, what it contains, how it is presented and how it is used.
About LT Auditor+ Configuration Guide	Provides information about LT Auditor+ configuration, deployment and management of audit policies.

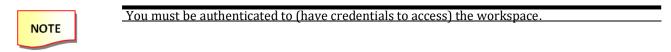
Chapter 2 – LT Auditor+ Workspace

This section will provide detailed steps to show you how to use LT Auditor+ Security Management Console to configure your workspace.

Connecting to the Workspace

1. To launch the Security Management Console click Start \rightarrow All Programs \rightarrow Blue Lance, Inc \rightarrow Management Console.

The first screen prompts you for the database connection information. This lets you connect to the workspace that you need to configure.



For SQL (Management Console):

Database Connect	tion Details			X
Database Type	2			
Micros	oft SQL Server			
Microsoft SQL	Server Settings			
<u>S</u> erver:	10.0.4.134			
<u>D</u> atabase	ii hf2h			
O Use	<u>N</u> T Integrated Sec	urity		
• • U <u>s</u> er	rName and passwo	ord		
<u>U</u> ser Na	me: ana			
<u>P</u> asswor	rd: ***			
	Test Connection	ок	Cancel	<u>H</u> elp

- 2. Select Microsoft SQL Server for database type.
- 3. Provide Server ID.

- 4. Provide Database Name.
- 5. Select Use NT Integrated Security or User Name and Password.
- 6. If User Name and Password is selected, provide the username and the password.
- 7. Click OK.

For Oracle (Management Console):

Database Connection	Details			X
Database Type				
Oracle				•
Oracle Settings				
<u>H</u> ost String:	LTA9			
<u>U</u> ser Name:	ana			_
<u>U</u> ser Name.				
<u>P</u> assword:	***			
I	est Connection	ок	Cancel	<u>H</u> elp

- 1. Select Oracle for database type.
- 2. Provide host string.
- 3. Provide username
- 4. Provide password.
- 5. Click OK.

The Management Console will be launched as soon as you are authenticated to the workspace as displayed in the screen below:

LT Auditor+ Management Console					- 0	×
system Options Help						
🎻 😼 Add Agent 🚂 Author	rized User 🚺 Job	Filter Statement	/ 🗶	D 🖻 🐕		
🔒 Corp						
Corb						
						_
						_
Corp	🗿 Domain (Controller (Group -	Primary Manag	er [EC2AMAZ-V	101
	Domain (Group -		er [EC2AMAZ-V	
Manager Group Windows Agent Group Domain Controller Group Member Server Group	11 0	0 Total a				Se
O Manager Group Monose Agent Group Omain Controller Group Momber Server Group O Monkstation Group O SharePoint Group	Agent Name EC2AMAZ-4UNGPQH		gent(s) : 1		er [EC2AMAZ-V Last Rollup 12/9/2020 6:43:57 PM	IO Se
Manager Group Mindows Agent Group Momain Controller Group Member Server Group Workstation Group	Agent Name	0 0 Total a	gent(s) : 1 Version	Last Policy Deployed	Last Rollup	Se
 ⊕ O Manager Group ⊕ O Mindows Agent Group ⊕ O Manin Controller Group ⊕ Member Server Group ⊕ Warkstation Group ⊕ SharePoint Group ⊕ A RedHat Linux Group 	Agent Name	0 0 Total a	gent(s) : 1 Version	Last Policy Deployed	Last Rollup	Se
⊕ ⊕ Manager Group ⊕ ⊕ ⊕ Mindows Agent Group ⊕ ⊕ ⊕ ⊕ Manain Controller Group ⊕ ⊕ Mindows Server Group ⊕ ⊕ Mindows Server Group ⊕ ⊕ Mindows Mindows ⊕ ⊕ Addat Linux Group ⊕ ⊕ SuSE Linux Group ⊕ ⊕ Syslag Devices Group	Agent Name	0 0 Total a	gent(s) : 1 Version	Last Policy Deployed	Last Rollup	Se
Manager Group Mindows Agent Group Mindows Agent Group Al Domain Controller Group Mindows Agent Group	Agent Name	0 0 Total a	gent(s) : 1 Version	Last Policy Deployed	Last Rollup	Se

The Management Console is divided into two views. The left pane shows the currently configured workspace with the workspace name as the root node of the tree. Below the root nodes are the manager groups and agent groups of the workspace. The right pane displays the details of each node highlighted on the left side.

Select the workspace root node in the tree to display all the manager groups and agent groups in the pane on the right side.

Manager Groups

Manager groups cannot be created using the Management Console. These groups are created when you install the LT Auditor+ Manager as discussed in the LT Auditor+ Installation Guide. A workspace can contain more than one manager residing in more than one manager group.



You need to place managers in different manager groups if you intend to have different policies for each manager.

Creating Agent Groups

New agent groups are created from the Management Console. To create a new Windows agent group, choose one of the following:

- 1. Click on System \rightarrow New \rightarrow Windows Agent Group OR
- 2. Click on the toolbar icon Windows Agent Group OR
- 3. Right-click on the Workspace.
- 4. Click Windows Agent Group.

When creating a new agent group in the Management Console, the user must determine the type of agent group being created. There are four types of agent groups available for creation in LT Auditor+ for Windows; these include:

- Windows Agent Group This group type is intended for backward compatibility with older versions of LT Auditor+. It may contain machines of any type.
- **Domain Controller Group** This group type may only contain domain controller machines.
- Member Server Group This group type may only contain member server machines.
- **Workstation Group** This group type may only contain nonserver machines in the domain.

To create a new agent group:

- 1. Right-click on the root node of the workspace in the left pane of the Management Console.
- 2. Select Agent Group (Windows/SUSE Linux or any other application)
- 3. The new form for agent group creation appears as below:

Add Agent Group	\mathbf{X}
<u>G</u> roup Name:	
Group <u>T</u> ype:	
Windows Agent Group	•
Windows Agent Group Domain Controller Group File Server Group Workstation Group Ditle-yssbrigkn26	
Joine-Appoidkuse	<u> </u>
·	
	OK Cancel <u>H</u> elp

The selection of domain and group type will determine which agent machines are available in the workspace for addition to the new agent group.

A primary manager is responsible for deploying policies that change within that group. Also, all agents within that group will attempt data transfer with the primary manager first, before attempting to transfer to any other manager in the workspace.

Default Filter Statement

Default filter statements will now be set for each agent group upon creation and will vary according to group type as is appropriate. Default filter statements may be modified in any way to suit specific auditing needs and may be restored to their original configuration at any time by selecting the Restore Default Settings option in the menu.

To view default filters:

ΒΓΠΕ ΓΥUCE

 Highlight the agent group or a specific audit subsystem whose filters you would like to view in the left pane of the Management Console. The default filters will appear in the right pane list view.

> S LT Auditor - Man Options Itelp 🗊 200-1 🗸 Eker Statemert... 🥖 🎥 🦣 🎒 😤 1 R Agent. ... 💁 Authorited Uper. WK 💅 Audit SubSystems filters for test er Type Filter Status SubS Default Exclude Filter Default Exclude Filter Default Include Filter Default Include Filter ADA ADA GPA LSA up Policy Auditing on Server Auditing Auditing re Event Log Au Curently Authenticated User BLINC\mbaun 👘 start 🔰 🧷 🐻 🖤 🐻 🗠 C Regular CO LEE CA 2 1 10215 N 11.7 前日日

To restore the default settings after reconfiguration:

- 2. Right-click on the agent group
- 3. Select Restore Default Filter Settings from the menu. Restoring default filter settings may only be done for all audit subsystems within an agent group simultaneously. Default settings may not be restored for an individual subsystem.

Agent Subsystems	6]
Men Hanager Group Send Group Jacon Group Jacon Group Jacon Group Jacon Group Jacon Jacon	THE THE PARTY OF T
Agent IVame Agent IF Version	Last Policy Deployed
Restore Default Filter Settings	
@ 21.	
B Agent	
/ Edit	
🐡 Doiste	
PB Ger	
器 <u>faite</u>	
SMTP Settings	
SNUP Settings	
Change Primary Manager Mystrine Event: Log Andrine Settings	
Properties	
Legecy LT Audtor+ Settings	

The default filters for each group type are listed below:

Domain Controller Groups Active Directory:

Exclude Noise Users Statement – Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, -, \,*ANONYMOUS LOGON*

- a. Exclude Modify Object Statement Excludes the "modify object" operation
- b. Include Statement Includes all operations

Group Policy:

a. Include Statement – Includes all operations

Logon Server:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, \, *ANONYMOUS LOGON*
- b. Include Statement Includes operations Interactive Logon, Remote Interactive Logon, All Directory Authentications, All Failed Logons

Member Server Groups

Logon Server:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, ,\,*ANONYMOUS LOGON*
- b. Include Statement: Includes the operations Interactive Logon, Remote Interactive Logon, All Failed Logons

Removable Device:

- a. Exclude Noise Events Statement: Excludes the operation Write Attribute
- b. Include Statement: Includes all operations

SAM:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, \,,*ANONYMOUS LOGON*
 - a. Exclude Modify Object Statement Excludes the Modify Object operation
 - b. Include Statement Includes all operations

Workstation Groups

Logon Server:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, -, \,,*ANONYMOUS LOGON*
- b. Include Statement Includes the operations Interactive Logon, Remote Interactive Logon, All Failed Logons

Removable Device:

- a. Exclude Noise Events Statement Excludes the operation Write Attribute
- b. Include Statement Includes all operations

SAM:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, \,,*ANONYMOUS LOGON*
- b. Exclude Modify Object Statement Excludes the Modify Object operation
- c. Include Statement Includes all operations

Windows Agent Groups

Active Directory:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -,\,*ANONYMOUS LOGON*
- b. Exclude Modify Object Statement Excludes the Modify Object operation
- c. Include Statement Includes all operations

Group Policy:

a. Include Statement - Includes all operations

Logon Server:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, \,,*ANONYMOUS LOGON*
- b. Include Statement Includes the operations Interactive Logon, Remote Interactive Logon, All Directory Authentications, All Failed Logons

Removable Device:

- a. Exclude Noise Events Statement Excludes the operation Write Attribute
- $b. \quad Include \ Statement-Includes \ all \ operations$

Manager Groups

Active Directory:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, \,,*ANONYMOUS LOGON*
- b. Exclude Modify Object Statement Excludes the Modify Object operation
- c. Include Statement Includes all operations

Group Policy:

a. Include Statement – Includes all operations

Logon Server:

- a. Exclude Noise Users Statement Excludes Users: *\$*, *NT Authority*, *\System*, -\-, -, \,,*ANONYMOUS LOGON*
- b. Include Statement Includes the operations Interactive Logon, Remote Interactive Logon, All Directory Authentications, All Failed Logons

Removable Device:

- a. Exclude Noise Events Statement Excludes the operation Write Attribute
- b. Include Statement Includes all operations

Adding Agents to Agent Groups

Use this option if the LT Auditor+ Agent is already installed on agent being added to Agent Group. To add an agent to a Windows agent group, choose one of the following:

- 1. Click on System \rightarrow New \rightarrow Agent OR
- 2. Click on the toolbar icon Agent OR
- 3. Right-click on Agent Group.
- 4. Click Agent.
- 5. Provide the IP address or the machine name of the agent that needs to be added.
- 6. The machine must already have the agent installed, be running, and be a free agent in order to be added to an agent group.

To browse for agents:

- 1. Right-click on the agent group to which you would like to add a gents.
- 2. Select Agent from the menu. The following form will appear:

ΒΓΠΕ ΓΥUCE

Add Agent	
<u>A</u> gent	Name:
	<u>B</u> rowse
	OK Cancel <u>H</u> elp

3. Click the Browse button. The following selection form will appear:

d Agent	
Select Computers	×
Select this object type:	
Computers	Object Types
From this location:	
bldragon.com	Locations
Enter the object names to select (examples):	
l	Check Names
Advanced	OK Cancel

- 4. Type a machine name or click Advanced to browse Active Directory for machines to install.
- 5. Click OK.
- 6. The agents will be added to the chosen agent group.

Renaming agent groups:

- 1. To rename a group, right-click on the group.
- 2. Click Edit.
- 3. Provide the new name for the group and click Enter.

Modifying Manager Group Settings

- 1. Right-click on Manager Group.
- 2. Click Manager Settings.

Manager S	iettings
	Native Event Log Settings - Number of Days to Keep
	Native Event Log Files: 14
	Audit Files: 14
	Archive Threshold: 10000
	Time Out: 10000 🕂 Milliseconds
	Rollup Interval: 15 Minutes
	<u>Simultaneous Connections:</u> 500
	Manager Poll Interval:
	OK Cancel <u>H</u> elp

Number of Days to Keep Native Event Logs: This setting is used by the manager to decide how long to keep the archived native event logs of the manager and agents. The default setting is 14 days. The minimum setting is 0 days, and the maximum setting is 90 days.

Rollup Interval: This setting is used by the manager to determine the time that elapses between rollups. The default setting is 15 minutes. The minimum setting is 0 minutes, and the maximum setting is 59 minutes.

Simultaneous Connections: This setting is used by the manager as a threshold of connections. The manager will reject all connections exceeding this setting. This setting is used by the manager for load balancing. The default setting is 500 connections. The minimum setting is 1 connection. There is no maximum setting.

Manager Polling Interval: The manager uses this interval to check with the workspace database to see if there are any policy changes for itself as well as the agents that it manages. The default setting is 1 minute. The minimum setting is 0 minutes, and the maximum setting is 15 minutes.

Modifying Agent Group Settings

- 1. Right-click on the agent group.
- 2. Click Properties.

Ag	ent Group Sett	ings	
	<u>P</u> rimary Mana	ger: blinc-dev01	
	Archive Sett	ings	
		<u>A</u> rchive Threshold:	10000
	~	<u>D</u> ays to Keep Files:	14
	-Transfer Set	tings	
	F	<u>T</u> ransfer Interval:	9 🔹 Minutes
		<u>T</u> ime out (ms):	60000
			OK Cancel <u>H</u> elp

Archive Threshold: The agent machine will create an archived file as soon as it reaches this threshold. The default setting is 10,000 records. The minimum setting is 1,000 records, and the maximum setting is 10,000 records.

Days to Keep File: The agent machine backs up archived files after they are sent over to the manager. This setting decides how many days the agent will continue to store the backed-up files on the agent machine. The default setting is 14 days. The minimum setting is 0 days, and the maximum setting is 90 days.

Transfer Interval: The agent machine can send archived data files over to the manager on a regular interval. This setting is used to decide this interval. A setting of 0 disables the interval-based data transfer and relies totally on job-based data file transfers. The default setting is 15 minutes. The minimum setting is 0 minutes and the maximum setting is 59 minutes.

Time out: This setting determines the interval of time an agent will attempt to establish a connection with the manager. The default setting is 60,000 milliseconds. The minimum setting is 10,000 milliseconds and the maximum setting is 120,000 milliseconds.

BLUE LΔΠCE

Native Event Log Archive Settings

- 1. Right-click on the manager or agent group
- 2. Click on Native Event Log Archive Settings to show a list of all Native Event Logs that need to be archived at a specific percentage of their maximum settings.

Event Log Name	Threshold
Application	80
1010	
	<u> </u>
Te	Add <u>M</u> odify <u>D</u> elete

To add a new Native Event Log archive setting, choose one of the following:

- 1. Click Add.
- 2. Choose appropriate name from list OR
- 3. Type in the name.
- 4. Click OK.

To modify a NEL archive setting:

- 1. Select the Event Log Name.
- 2. Click Modify.
- 3. Change the data.
- 4. Click OK.

To delete an NEL archive setting:

- 1. Select the Event Log Name
- 2. Click Delete. The system will ask for confirmation.
- 3. Click Yes.

Archive Threshold: Provide the threshold percentage. The default setting is 80 percent. The minimum setting is 15 percent, and the maximum setting is 95 percent.

Modify the Threshold: Choose the event log, click Modify, change the threshold.

Delete the Threshold: Choose the event log, click Delete, and confirm by clicking Yes.

Event Log Threshold

This setting allows for the archiving of event logs based on specified thresholds. Archiving of event logs will create a local copy of the log, which will then be processed by LT Auditor+. For extremely busy servers, setting a threshold to force archives should be considered to not lose audit data due to standard event log overwrite settings.

To apply threshold limitations through the Manager:

- a. Right-click on the Manager node in the left pane of the Management Console.
- b. Select Manager Settings from the drop-down menu.

S LT Auditor+ Management Console	
System Options Help	
🎻 😨 Agent 🔬 Authorized User 顶	205 🔯 Elter Statement 🧪 🌲 📭 🏟 💱
🔒 work space	
e 🔗 work space	MGR
Job	agers
	-dev01
Edit Delete	
SMTP Settings	
SNMP Settings	
Native Event Log Archive Settings	
Event File Iransfer Settings	
Manager Settings	
Currently Authenticated User: BLINC\mhaun	
🛃 start 🤌 🙆 🥙 🔯 Inbox - Microsoft O	u 🎦 d\$ on Software Dev 🔯 2 Microsoft Office 🔹 🔮 LT Auditor+ Manage 🦿 😨 😨 😤 🖏 🗐 🖉 🚺 11:48 AM

- c. Provide a number of events in the Maximum Event Log Threshold for an Arm field. The default setting is 5,000 events. The minimum setting is 5,000 events, and the maximum setting is 100,000 events.
- d. Click OK once the desired setting has been entered.

The settings will take effect the next time the manager polls the database for policy changes. This is dependent on the "Poll Interval" setting.

Manager Sett	tings	2
	Native Event Log Settings -	Number of Days to Keep
	Native <u>E</u> vent Log Files:	14
	<u>A</u> udit Files:	14
	<u>A</u> rchive Threshold:	10000
	<u>T</u> ime Out:	10000 🔺 Milliseconds
	<u>R</u> ollup Interval:	15 Minutes
	<u>S</u> imultaneous Connectior	ns: 500 ÷
	<u>M</u> anager Poll Interval:	1 A Minutes
	Ma <u>x</u> imum Event log Threshold for an Arm:	5000 📑
		OK Cancel <u>H</u> elp

To apply threshold limitations through an agent group:

- 1. Right-click on the Agent Group node in the left pane of the Management Console.
- 2. Select Properties from the drop-down menu.

System Opt	or+ Management Console tions Help Agent Authorized User	D 200 1	Eliter Statem	ent 🧷 .	* 6 6 7			
work	work space	9			nary Manager		sv011	
	GR Data Rollup Authorized Users Audit SubSystems	Agent Name w2k3maggie	Agent IP 10.0.4.115	Version	Last Policy D 11/20/2007 1	eployed		
	Eilter Statement Job <u>Agent</u>							
	Edit Delete Copy Asses							
	SMTP Settings SNMP Settings							
	Native Event Log Archive Setting	s						
	Eroperties Legacy LT Auditor+ Settings							
Currently Authen	nticated User: BLINC\mhaun	os ն d\$ on :	Softwar	Z Microsoft	LT Auditor+ M	2 Paint	/ 2 2 1	🤹 🗐 12:03 PM
- start		us' 🛃 d\$ on :	sortwar	Z Plicrosoft	UT Auditor+ M	a z Panc	. S. S. R. R. 1	2 12:03 PM

ΒΓΠΕ ΓΥUCE

- 3. Provide a number of events in the Event Log Threshold Settings field. The default setting is 5,000 events. The minimum setting is 5,000 events and, the maximum setting is 100,000 events.
- 4. Click OK once the desired setting has been entered.

The settings will take effect the next time that policies are deployed to the agents.

Agent Group Settings					
<u>P</u> rimary Manager:	blinc-dev01				
Archive Settings					
	rchive Threshold:	10000		÷	
	ays to Keep Files:	14		÷	
Transfer Setting	S				
т 🏹 т	ansfer Interval:	9 🔅	Minutes		
Ш. Ці	me out (ms):	60000		*	
EventLog Thresh	old Settings				
Maxim Thresh	um <u>E</u> vent log old for an Arm:	5000	i.		
		ОК		Cancel	<u>H</u> elp

Event File Transfer Settings

LT Auditor+ has the capability to archive native event logs onto a local disk through agents/managers. Given that the size of archive data is not limited, there is an increasing probability of issues resulting in a filled disk or not enough disk space. Event file transfer allows the ability to compress and move this data to another physical location. The manager has the capability to compress and move these backup files onto another file server or shared folder. This feature should be configurable in terms of shared folder path and user's credentials to access this folder. Data will be archived whenever rollup occurs.

To launch the Event File Transfer Settings:

1. Click on Options \rightarrow Event File Transfer Settings. The following screen will be displayed.

ΒΓΠΕ ΓΥUCE

Event File Transfer Settings		×
	Activate Backup Backup Folder : User Name: Password: Re-type Password:	
	QK Qancel	Help

2. To activate transfer settings, check Activate Backup.

Backup Folder: The user should designate the backup folder in which the files will reside once transferred. **User Name and Password:** This is the username and password that the user enters to connect to the shared folders or network.

Chapter 3 – Audit Policies

Configuring LT Auditor+ Audit Policies

Common Filter Settings

To create any new Active Directory filter, Group Policy filter, file system filter, logon server filter, or Native Event Log filter, begin by highlighting the chosen subsystem in the left pane of the Management Console. Then select one of the following:

1. Click System \rightarrow New \rightarrow Filter Statement

OR

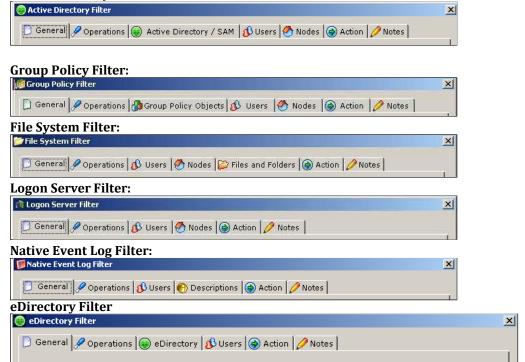
2. Click Filter Statement on the toolbar icon

OR

3. Right-click on the chosen subsystem, then click Filter Statement.

Given below are the samples of the tabs for the various auditing filters:

Active Directory Filter:



Logon Server Filter

General Settings

ogon Server Filter	
General 🖉 Operations 🚯 Users 🥙 Nodes 🕻	Action Provide a constraint of the second seco
Filter <u>N</u> ame: MED LSA Filter Statement	
	Filter Statement Type
	 Include Statement
	C Exclude Statement
101010101010	OT All Day
	Start Time: 12:00:01 AM +
	End Lime: 11:59:59 PM +
	TT(24(24.5M)
	Enable <u>F</u> ilter

Filter Name: Provide a name to identify the filter statement from a collection of filters that have been created.

Filter Statement Type: Include Statement audits a particular operation only if all of the filter criteria are met. Exclude Statement rejects a particular operation and does not audit if any of filter criteria are met.

All Day: Each filter statement can be modified with a time the statement would be active. Select All Day to have filter statement active for the entire day, or select a specific start time and end time to determine when the filter statement will be active.

Enable Filter: To completely disable the filter settings, uncheck the Enable Filter.

User Settings

🎾 File System Filter	×
📄 General 🖋 Operations 🚯 Users 🥙 Nodes 🔛 Files and Folders 🎯 Action 🂋 Note	s
All Users	
Users	<u>A</u> dd
	Modify
	Delete
OK	el <u>H</u> elp

All Users:

To audit all users performing any active directory operation:

- 1. Select All Users.
- 2. To monitor specific user accounts, uncheck All Users.
- 3. Click Add. Provide the usernames to be audited.



A wildcard (*) may be used.

4. Click OK.

Tomodifyauser:

- 5. Highlight the user, click Modify.
- 6. Change the user data, click OK.

To delete a user:

- 7. Highlight the user.
- 8. Click Delete. The system will ask you for confirmation.
- 9. Click Yes.

BLUE LΔΠCE

Node Settings

ile System Filter	
) General 🖉 Operations 🚯 Users 💆 Nodes 😂 Files and Folders 🛞 Action 💋 Notes	5
· · · · · · · · · · · · · · · · · · ·	
All Nodes	
Nodes	<u>A</u> dd
	Modify
	<u>D</u> elete
OK Cance	el <u>H</u> elp

All Nodes:

To audit all specific workstations from which active directory operations are performed:

- 1. Select All Nodes.
- 2. To monitor specific nodes, uncheck All Nodes.
- 3. Click Add.
- 4. Provide the specific nodes to be audited.
- 5. Click OK.

To modify a Node:

- 1. Highlight the node.
- 2. Click Modify.
- 3. Change the node data.
- 4. Click OK.

To delete a Node:

- 1. Highlight the node.
- 2. Click Delete. The system will ask you for confirmation.
- 3. Click Yes.

Operations Settings

Active Directory Filter	Đ
] General 🖋 Operations 🍥 Active Directory / SAM 🚯 Users 🕙 Nodes 🛞 Action 🎾 Not	es
F All Operations	
🗊 🗖 Create Object	~
🔁 🗖 Delete Object	
🔁 🗖 Modify Object	
🗄 🗖 Modify Security DACL	
🖻 🔲 Account Modification	
🗈 🗖 Enable Account	
🕀 🗖 Disable Account	
E Set Password	
E ☐ User Account Unlocked	
□ □ Group Membership	
E □ Trusted Domain Added	
	~
	<u> </u>

- 1. Select All Operations to audit all subsystem operations.
- 2. To select specific operations of interest, uncheck All Operations.
- 3. Select the appropriate operation(s) to audit.

NOTE

Operations will vary between subsystems, but the method of selection will remain the same in all subsystems with the exception of the Native Event Log operations filter, whose method is described below.

Native Event Log Operations:

- 1. Select the appropriate event to be monitored. A single filter can monitor from any of the six standard event logs in Windows or any newly created event log on the machine.
- 2. Click Add to add a new Native Event Log operation. The following screen will open:

ΒΓΠΕ ΓΥUCE

Add Operations	×
<u>D</u> escription:	
<u>E</u> vent Log:	Application
<u>S</u> ource:	All Source
<u>C</u> ategory:	All Categories
	All Event ID's
<u>E</u> vent ID:	
	OK Cancel <u>H</u> elp

Each Native Event Log operation is made of the event log name, source name, category of the event and the actual event number.

Provide a description of the new event:

- 1. Select a Native Event Log type.
- 2. Select either All Source or provide the name of the source to be audited.
- 3. Select either All Categories or provide a name of the category to be audited.
- 4. Select either All Event IDs or provide the specific event ID to be audited.

Action Settings

Searching Active Directory Filter
📄 General 🖉 Operations 🍥 Active Directory / SAM 🚯 Users 🥙 Nodes 🕘 Action 🥖 Notes
C Exclude Alert
□ S <u>N</u> MP Alert
<u>S</u> MTP Alert
Erom:
Subject:
Net Alert
Message:
то:
☐ <u>R</u> un Emergency Transfer Job
OK Cancel <u>H</u> elp

Each included filter statement can be configured to send out real-time alerts if the filter criteria are met in the form of SNMP messages, email alerts or regular Windows messages. By checking the Exclude Alert box, specific users can be excluded from receiving alerts for the same event, which is defined for all users.

- To send SNMP messages, check SNMP Alert.
- To send email alerts, check SMTP Alert.

Provide the following information in the SMTP form: From, Subject (of the message), To and CC. The To and the CC lists of addresses should be separated by semicolons.

an [11 12			
o: Machine_Nam	e		

To send a Windows Messenger Alert, check Net Alert (Net Alert works only for Windows XP and Windows 2003).

Provide the following information in the Net Alert form: Message is customized text followed by **%cT** (see example above); To is the machine name or IP address the Net Alert should be sent to.

Notes

📂 File System Filter		×
🗋 General 🔗 Operatio	ns 🚯 Users 🥙 Nodes 🔛 Files and Folders 🕞 Action 💋 Notes	
<u>C</u> reated By:	BLTRAIN50\Administrator	
C <u>r</u> eated On:	12/12/2006 1:15:21 PM	
Last Modified By:	BLTRAIN50\Administrator	
L <u>a</u> st Modified On:	12/13/2006 3:27:31 PM	
Filter <u>N</u> otes:		
	OK Cancel <u>H</u> elp	1

The program will automatically keep track of the filter creator, date, filter modifier and date it was modified. The Filter Notes field is provided for the user to track why the filter was created or modified.

Filter Settings Specific to a Subsystem

To create a new filter statement for a category specific to a subsystem (i.e., Active Directory/SAM, eDirectory), highlight your chosen auditing arm in the audit subsystem tree in the left pane of the Management Console, then select one of the following:

1. Click System \rightarrow New \rightarrow Filter Statement

OR

2. Click Filter Statement on the toolbar icon.

OR

3. Right-click on the Active Directory Subsystem, and then click Filter Statement.

Select the tab specific to that subsystem and follow the instructions below to configure that setting.

ΒΓΠΕ ΓΥUCE

Active Directory / SAM Settings – Active Directory Filter

Active Directory Filter General Operations F Entire Active Direct	active Directory / SAM 🛛 🚯 Users 🧑	X
<u>C</u> ontext:	ners	
All Objects	🔽 <u>A</u> ll Classes	✓ All Attrib <u>u</u> tes
	Classes	Attributes
<u>A</u> dd <u>M</u> odify	A <u>d</u> d M <u>o</u> dify	Add Modi <u>fy</u>
Delete	Delete	Dele <u>t</u> e
		OK Cancel <u>H</u> elp

Entire Active Directory / SAM:

To audit the entire active directory on a domain controller or to audit the local Windows accounts on a standalone machine, select Entire Active Directory / SAM.

Context: If the Entire Active Directory / SAM option is not checked, the context field will become active. Select the ellipsis [...] to browse for the container in the active directory forest that needs to be monitored.

Include Subcontainers: If this is selected, LT Auditor+ will monitor the container specified in the context field and all the subcontainers within it. To monitor only the container specified, but not the subcontainers, uncheck this option.

Objects:

- 1. To audit all objects, select All Objects.
- 2. To audit specific objects, uncheck All Objects.
- 3. Click Add.
- Provide description of the object(s) to be audited. Utilizing a wildcard '*' will specify any part of the object name. For example, cn=john* will audit any object containing the string cn=john.
- 5. Click OK.

To modify the object:

- 1. Highlight the object in the list.
- 2. Click Modify.
- 3. Edit the object data. Click OK.

To delete the object:

- 1. Highlight the object in the list.
- 2. Click Delete. The system will ask you for confirmation.
- 32 | Confidential and Proprietary

ΒΓΠΕ ΓΥUCE

3. Click Yes.

Classes:

To audit all classes:

- 1. Select All Classes.
- 2. To audit specific classes within the active directory, uncheck All Classes.
- 3. Click Add.
- 4. Provide the description of the class to be audited. A wildcard '*' can be used.
- 5. Click OK.

To modify the class:

- 1. Highlight the class in the list.
- 2. Click Modify.
- 3. Edit the class data.
- 4. Click OK.

To delete the class:

- 1. Highlight the class in the list.
- 2. Click Delete. The system will ask you for confirmation.
- 3. Click Yes.

Attributes:

To audit all attributes:

- 1. Select All Attributes.
- 2. Uncheck All Attributes to audit specific attributes within the active directory.
- 3. Click Add.
- 4. Provide the description of the attribute(s) to be audited. A wildcard '*' can be used.
- 5. Click OK.

To modify the attribute:

- 1. Highlight the attribute in the list, click Modify.
- 2. Edit the attribute data.
- 3. Click OK.

To delete the attribute:

- 1. Highlight the attribute in the list.
- 2. Click Delete when prompted for confirmation.
- 3. Click Yes.

BLUE LΔΠCE

Group Policy Objects Settings – Group Policy Filter

🕼 Group Policy Filter	×
🗋 General 🖋 Operations 🚺 Group Policy Objects 🚯 Users [🕙 Nodes 🎯 Action 🍃	Notes
✓ <u>All</u> Objects	
Objects	<u>A</u> dd
	<u>M</u> odify
	Delete
OK Cance	el <u>H</u> elp

ject 🛛 🔀
Object Name:
CN={0EA69124-709E-41EC-88A8-6E69C805D524},CN=Policies,CN=Sy
OK Cancel <u>H</u> elp

All Objects:

- 1. To audit all the Group Policy objects within the Active Directory, select All Objects.
- 2. To audit specific Group Policy objects within the Active Directory, uncheck All Objects.
- 3. Click Add.
- 4. Browse through the Active Directory to locate Group Policy objects within the Active Directory.
- 5. Click OK.

🕼 Group Policy Filter	X
🗋 General 🖋 Operations 🕼 Group Policy Objects 🚯 Users 🥙 Nodes 💩 Action 🍃	Notes
☐ <u>A</u> ll Objects	
Objects	<u>A</u> dd
{0EA69124-709E-41EC-88A8-6E69C805D524}	
	<u>M</u> odify
	Delete
OK Canc	el <u>H</u> elp

To modify Group Policy Objects:

- 1. Highlight the object.
- 2. Click Modify.

To edit the Group Policy Object data:

- 1. Highlight the object.
- 2. Click OK.

To delete Group Policy Objects:

- 1. Highlight the object.
- 2. Click Delete.
- 3. The system will ask you for confirmation. Click Yes.

BLUE LΔΠCE

File / Folders Settings – File System Filter

e System Filter	
General 🖉 Operations 🚯 Users 🥙 Nodes 🔛 Files and Folders 🔿 🗛	ction 🖉 Notes
	12 1
Eile Path:	
TInclude Sub Folders	
All Eiles and Folders Files and Folders	Add
	<u>H</u> uu.,
	<u>M</u> odify
	<u>D</u> elete
ок	Cancel <u>H</u> elp

File Path: Select the file system folder path to be monitored.

Include Sub Folder: To include all subfolders, select Include Sub Folders. To monitor only the folders specified, but not the subfolders, uncheck this option.

Files and Folders:

To audit all files and folders within the specified file path:

- 1. Check All Files and Folders.
- 2. To audit specific files or folders from the file path, select Add.
- 3. Provide the complete addresses of the files or folders to be audited.

NOTE

A wildcard (*) may be used

To modify a file or folder:

- 1. Highlight the file or folder.
- 2. Click Modify.
- 3. Change the file or folder data.
- 4. Click OK.

To delete a file or folder:

- 1. Highlight the file or folder.
- 2. Click Delete.
- 3. The system will ask you for confirmation.
- 4. Click Yes.

All <u>D</u> escriptions		
Descriptions	 	 <u>A</u> dd
		Modify
		<u>D</u> elete

Description Settings – Native Event Log Filter

Operation Settings – Native Event Log

- 1. Select All Operations to audit all subsystem operations.
- 2. To select specific operations of interest, uncheck All Operations.
- 3. Select the appropriate operation(s) to audit.

Ge	neral 🖉 Operations 🚯 Users 酌 Descriptions 🛞 Action 🎾 Notes	
	Logon Failure - Account Locked Out (Source= Security, Category= *, Event A File Object Access (Source= Security, Category= *, Event ID= 560) File Object Deleted (Source= Security, Category= *, Event ID= 564) [2008/Vista] - Logon (Source= Security, Category= *, Event ID= 4624) [2008/Vista] - Logonf (Source= Security, Category= *, Event ID= 4634) [2008/Vista] - Logoff (Source= Security, Category= *, Event ID= 4634) [2008/Vista] - Service Ticket Granted (Source= Security, Category= *, Event ID= 4634) [2008/Vista] - Service Ticket Granted (Source= Security, Category= *, Event ID= 2008/Vista] - Ticket Granted (Source= Security, Category= *, Event ID= 2008/Vista] - Ticket Granted Renewed (Source= Security, Category= *, Event ID= 2008/Vista] - Action Ticket Request Failed (Source= Security, Category= *, Event ID= 2008/Vista] - Account Mapped For Logon Failed (Source= Security, Category= *, Event ID= 2008/Vista] - Account Mapped For Logon Failed (Source= Security, Category= *, Event ID= 2008/Vista] - NTLM Authentication Sailed (Source= Security, Category= *, Event ID= 2008/Vista] - NTLM Authentication Failed (Source= Security, Category= *, Event ID= 2008/Vista] - Account Created (Source= Security, Category= *, Event ID= 2008/Vista] - Account Created (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Security, Category= *, Event ID= 2008/Vista] - Account Enabled (Source= Se	Add Modify Delete
<		

All Descriptions

To monitor all the description strings from the event log:

- 1. Select All Descriptions.
 - To monitor specific events from the event log with certain description strings in them:
 - 1. Uncheck All Descriptions.
 - 2. Click Add.
 - 3. Provide the description strings.
 - 4. Click OK.



A wildcard (*) may be used. For example, if you wanted to audit all failed applications, you would type failed applications *.

To modify a description:

- 1. Highlight the description.
- 2. Click Modify.
- 3. Change the description data.
- 4. Click OK.

To delete a description:

- 1. Highlight the description.
- 2. Click Delete.
- 3. The system will ask you for confirmation.
- 4. Click Yes.

Chapter 4 – Configuring Manager and Agent Jobs

This section will provide detailed steps to show you how to use the LT Auditor+ Management Console to configure the agents to send data over to the manager, and to configure the manager to consolidate the data into the database.

Manager Data Rollup Job

In addition to automated rollup settings described in the section <u>Modified Group Settings</u>, rollup jobs can be scheduled to transfer audit data to the LT Auditor+ database. Each manager can be configured to perform multiple data rollup jobs, scheduled to run at a specific time and frequency.

To create a new data rollup job:

- 1. Click Data Rollup node in a Windows Manager Group.
- 2. Select one of the following:
 - Click System \rightarrow New \rightarrow Job.

ΒΓΠΕ ΓΌΠCΕ

- Click Job on the toolbar.
- Right-click on Data Rollup and click Job.

Job Details		×
	Select Job Type: Rollup Job]
	Job <u>N</u> ame:	
	Job Frequency: Single Job 🔽 Job Start Time: 5:21:33 PM 🗧	
	Day of Week: Date: 12/14/2006	
	<u>F</u> ile Name:	
	<u>C</u> ommand Line Parameters:	
	OK Cancel <u>H</u> elp	

Job Name: Provide the description of the job.

Job Frequency: Provide how often to run the job. Selection options are single, daily or weekly. **Job Start Time:** Specify the time to start the job.

To set up a custom job:

- 1. Select Custom from the drop-down menu.
- 2. Select options to suit needs as necessary.

Agent Data Transfer Job

In addition to automated transfer settings described in the section <u>Agent Group Setting</u>, jobs can be configured to transfer audit data to the manager. Each agent group can be configured to perform multiple data transfer jobs, scheduled to run at a specific time and frequency.

To create a new Data Transfer Job:

1. Click Data Transfer node in a Windows agent group.

- 2. Select one of the following:
 - Click System \rightarrow New \rightarrow Job.
 - Click Job on the toolbar.
 - Right-click on Data Transfer.
 - Click Job.

Job Details	×
	Select Job <u>Type:</u>
	Job <u>N</u> ame:
	Job Frequency: Single Job 💌 Job Start Time: 5:20:42 PM 🔅
	Day of Week: Date: 12/14/2006
	Eile Name:
	Command Line Parameters:
	OK Cancel <u>H</u> elp

Job Name: Provide the description of the job.

Job Frequency: Provide how often to run the job. Selection options are single, daily or weekly. **Job Start Time:** Specify the time to start the job.

Custom Job

Custom jobs can be set up to perform unique tasks like transferring miscellaneous files to the manager.

To create a new Custom Data Transfer Job:

- 1. Click Data Transfer node in a Windows agent group.
- 2. Select one of the following:
 - Click System \rightarrow New \rightarrow Custom Job.
 - Click Custom Job on the toolbar.
 - Right-click on Data Transfer. Click Custom Job.

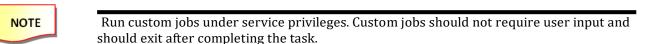
ΒΓΠΕ ΓΥUCE

Job Details	×
	Select Job <u>Type:</u> Custom Job
	Job <u>N</u> ame:
	Job Frequency: Single Job 🔽 Job Start Time: 5:21:51 PM 😨
	Day of Week: Date: 12/14/2006
	<u>F</u> ile Name:
	<u>C</u> ommand Line Parameters:
	OK Cancel <u>H</u> elp

Job Name: Provide the description of the job.

Job Frequency: Determine how often to run the job. Selection options are single, daily or weekly. **Job Start Time**: Specify the time to start the job.

File Name: Provide the complete application name, i.e., **C:\directory\filename**. **Command line**: Provide the required parameters for the application.



Chapter 4 – Configure the LT Auditor+ Report Console

This section will provide detailed steps to show you how to use LT Auditor+ Report Console to create report queries and run reports on the consolidated data collected in the workspace.



To access the Report Console, you must first be certain to be authenticated to the workspace with which you want to work.

Starting the Report Console

- 1. Click Start \rightarrow All Programs \rightarrow Blue Lance, Inc \rightarrow Reporting Console. The following screen gets displayed.
- 2. It will prompt you for the database connection information.

For SQL (Report Console):

Date	abase Connect	ion D	etails			X
	Database Type					
	Dicroso	oft SC	L Server			•
	Microsoft SQL S	erve	Settings			
	<u>S</u> erver:	10.	0.4.134			
	<u>D</u> atabase:	hf2	'n			
	🔘 Use)	T Iח	itegrated Sec	urity		
	- • U <u>s</u> er	Nam	e and passwo	ord		
	<u>U</u> ser Nai	ne:	ana			
	<u>P</u> asswor	d:	***			
		<u>T</u> es	t Connection	ок	Cancel	<u>H</u> elp

Select Microsoft SQL Server for Database Type.

- 1. Provide server ID.
- 2. Provide database name.
- 3. Select Use NT Integrated Security OR User Name and Password.
- 4. If User Name and Password is selected, provide the username and the password.
- 5. Click OK.

For Oracle (Report Console):



Oracle client tools are needed to connect to the database using the Report Console.

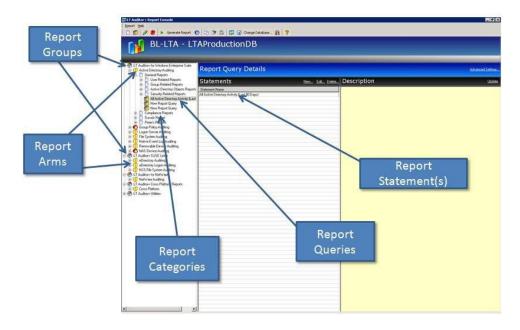
BLUE LΔΠCE

Da	atabase Connection	n Details			
	Database Type				
	0racle				•
	Oracle Settings				
	<u>H</u> ost String:	LTA9			
	<u>U</u> ser Name:	ana			_
	<u>o</u> ser Name.	Jana			
	<u>P</u> assword:	***			
		<u>r</u> est Connection	ок	Cancel	<u>H</u> elp

- 1. Select Oracle for database type.
- 2. Provide host string.
- 3. Provide username.
- 4. Provide password.
- 5. Click OK.

ΒΓΠΕ ΓΥUCE

The Report Console will be launched as soon as you are authenticated to the workspace. The Report Console screen is shown in the following screen:



The Report Console is divided into two views:

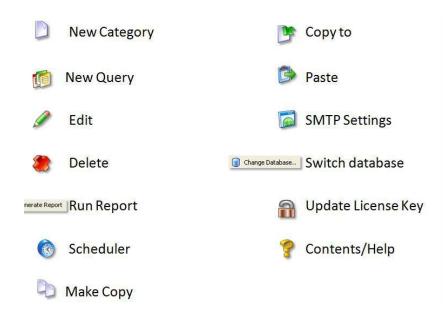
- The left pane shows all the report groups available for reporting.
- The right pane provides detailed information about each selected entity on the left.

Each reporting group has report arms that relate to Blue Lance products or tools. Reporting arms can have multiple report categories within them. Each report category can further have subcategories or actual report queries within them. Each report query is made up of one or more report query statements.

Report Icons

The icons used in the LT Auditor+ Report Console are listed below:

ΒΓΠΕ ΓΟUCE



Report Groups and Report Arms

The following table lists report groups and report arms available with LT Auditor+.

Report Group	Report Arms	Description
LT Auditor+ for Window Enterprise Suite	Active Directory Auditing	Reports for Active Directory Changes.
*	Group Policy Auditing	Report for Group Policy changes.
	Logon Server Auditing	Reports for authentications.
	File System Auditing	Reports for access to files and Folders.
	Native Event Log Auditing	Reports on Windows event logs.
	Removable Media Auditing	Reports on access to flash drives and other removable media.
	NAS Devices Auditing	Reports for access on devices like NetApp and EMC Isilon.
LT Auditor+ Windows Assessment	Windows Assessment	Reports for Active Directory Users, Groups, OUs, Computers, Object permissions (ACLs) and File/Folder permissions.
LT Auditor+ for SUSE Linux	eDirectory Auditing	Report on eDirectory changes.
	eDirectory Logon Auditing	Reports on authentications to eDirectory.
	NSS File System Auditing	Reports on access to NSS file systems on SUSE Linux systems.
LT Auditor+ for Syslog Devices	Syslog Device Auditing	Reports on data received from Syslog-enabled devices using LT

		Auditor+ Syslog Server.
LT Auditor+ Compliance Reports	Compliance Reports	Mappings to FFIEC, PCI-DSS, HIPAA, NIST and SOX .
LT Auditor+ Cross Platform Reports	Cross Platform Reports	Reports that can be consolidated across any of the report arms.

LT Auditor+ Utilities	Audit the Auditor	Reports on configuration and
		status changes made within LT
		Auditor+.
	Rollup Status Monitoring	Reports on status of audit data
		inserted into the LT Auditor+
		Database.

Report Categories

Report Categories hosts groups of report queries that allow users the option to group similar queries under a single category for ease of access and use.

Create a new report category:

- 1. Highlight the appropriate report arm:
 - Click Report \rightarrow New Report Category OR
 - Click New Report Category on the toolbar.
- 2. Provide a name for the report category.
- 3. Press Enter.

Modify a report category:

Select the report category and one of the following:

- Click Report, click Edit
 - OR
- Click Edit on the toolbar.

Delete a report category:

- 1. Select the report category and one of the following:
 - Click Report, click Delete
 - OR
 - Click Delete on the toolbar.
- 2. The system will ask you for confirmation.
- 3. Click Yes.

Creating a Report Query

Report queries determine how data is retrieved from the database for reporting. Every report query is comprised of one or more query statements. The following steps outline how to create a report query with one report query statement.

- 1. Select the report arm category in the left pane of the Report Console.
- 2. Select one of the following:
 - Highlight the report category.
 - Click on the Create Report Query icon.

A new report query is made up of one or more report query statements. A report statement is created when creating a report query. Each query can be configured in terms of desired output, format of report and additional parameters by selecting Advanced Setting, which will be discussed later in this session.

Report Statements

A report query statement contains a set of parameters that specifies how data is retrieved from the database on executing the query. A statement is comprised of multiple tabs that allow users to define the database query.

There are common tabs for all report arms as well as tabs specific to each arm.

Common Report Statement Tabs for All Report Arms

The common tabs on report statements for all report arms are:

- Date &Time
- Users
- Nodes
- Servers
- Operations Though this tab is common, its content varies for each report arm. We will discuss the Operations tab for each report arm in the "Specific Tabs" section.

Date & Time

This tab is used to specify date range for retrieval of data.

Active Directory Report Query Statement	x
Statement Name: All Active Directory Activity (Last	t 90 Days)
 ✓ Operations () Objects () Classes () Attraction ✓ Select Date ✓ Start Date: ✓ Sunday , January 01, 2006 ▼ ✓ End Date: Thursday , December 14, 2006 ▼ 	ributes 🚯 Users 🕐 Nodes 😡 Servers 💿 Date Time Select Time © Continuous © Block
C Reference Date	AM PM 12 2 4 6 8 10 12 2 4 6 8 10 D A Y
	OK Cancel <u>H</u> elp

- **Select Date** runs reports between a start date and an end date.
- **Reference Date** runs reports from prior days up to present date
- **Select Time** runs reports for a specific time.
- **Continuous Time** This option reports activity from the start date and start time to the end date and end time.
- **Block of Time** This option reports activity from the start date to the end date and all operations that fall within the specified start time and end time.

Users

Specifies what users are to be reported on.

Active Directory Report Query Statement	×
Statement Name: All Active Directory Activity (Last 90 Days)	
🖋 Operations 闥 Objects 🔝 Classes 😭 Attributes 🚯 Users 🔗 Nodes 😡 Servers 🔞 Date Time	
All Users	
Include Users	
C Exclude Users	
User Name	
BLINC\JoeSmith	
OK Cancel <u>H</u> elp	
	_

Wild card characters are accepted. For example, to report on all users that contain the words admin, type in *admin*.



Actions common for all tabs

- Include/Exclude selection criteria. •
 - > All query statement tabs, with the exception of the Date & Time tab, provide the choice of including or excluding the selection criteria specified in that tab.
 - Selecting Include will produce reports containing criteria selected in the tabs.
 - > Selecting Exclude will produce reports containing all audited data except those items selected in the tabs.
 - > Wild card characters are accepted.
 - Adding , Deleting , and Browsing
 - within tabs > In most tabs, when selecting specific items rather than all items for reporting, you may use the Add, Delete, and Browse icons to modify the items for which you would like to report.

Nodes

•

Specifies what nodes are to be reported on.

BLUE LΔΠCE

Active Directory Report Query Statement	×
Statement Name: All Active Directory Activity (Last 90 Days)	1
🖋 Operations 爾 Objects 🕅 Classes 🌪 Attributes 🚯 Users 🥙 Nodes 🖫 Servers 🔞 Date Time	
All Nodes	
🖲 Include Nodes	
C Exclude Nodes	
Node Name	
10.0.4.115	
OK Cancel <u>H</u> elp	

Servers

Specifies what servers are to be reported on.

Active Directory Report Query Statement	×
Statement Name: All Active Directory Activity (Last 90 Days)	
🖋 Operations 镧 Objects 🔝 Classes 🌟 Attributes 🚯 Users 🔗 Nodes 😼 Servers 🔞 Date Time	
All Servers	
• Include Servers	
C Exclude Servers	
Server Name	
BLDC1	
OK Cancel Help	

ΒΓΠΕ ΓΟUCE

Report Statement Tabs for File System, Removable Devices, NAS Devices and NSS File Systems Report Arms

For these report arms, the following tabs are applicable for enhanced querying.

Files

Specifies what files and folders are to be reported on.

File System Report Qu	ery Sta	tement	×
Statement <u>N</u> ame:	All File	Operation Report	-
🖋 Operations 🔞	Files	🚯 Users 🥙 Nodes 😡 Servers 🔞 Date Time	
All Files			
Include F	iles		
C <u>E</u> xclude F	iles		
File Name			
FinancialData*			
		OK Cancel <u>H</u> elp	

Example:

- Including ***.xlsx** will report on all files with the .xlsx extension.
- Excluding *.tmp will report on all files except files with the extension of .tmp

BLUE LΔΠCE

Operations

Species file operations to query for in the report.

File System Report Query Statement	
Statement Name: New Report Query Statement	-
🥜 Operations 爾 🛛 Files 🛛 🚯 Users 🥙 Nodes 😽 Servers 💿 Date & Time	
All Operations	
Include Operations	
C Exclude Operations	_
□ ✓ File ✓ □ ✓ ✓ ✓ □	
Berry Access File Directory Berry Remove Directory Berry Rename Directory Berry Access Directory Berry Access Directory	
OK Cancel <u>H</u> elp	

Operations are grouped into the following sections:

- File Operations Create, Write, Rename, Delete and Access
- Directory Operations Make, Remove, Rename and Access
- File & Directory Operations Write Security DACL/Write Attribute

Report Statement Tabs for the Active Directory, eDirectory and NetWare Report Arms

Classes

Classes are a group of objects defined by a certain set of attributes. Classes can include users, groups, organizational units, computers and any others defined in the Active Directory/eDirectory environment. Select the classes to report on in this tab.

BLUE LΔΠCE

Active Directory Report Query Statement	×
Statement Name: All Active Directory Activity (Last 90 Days)	
🖋 Operations 爾 Objects 🧊 Classes 🙀 Attributes 🚯 Users 🥙 Nodes 😡 Servers 🔞 Date Time	
© Include Classes	
O Exclude Classes	
Class Name	
organizationalUnit	
OK Cancel <u>H</u> elp	

Attributes

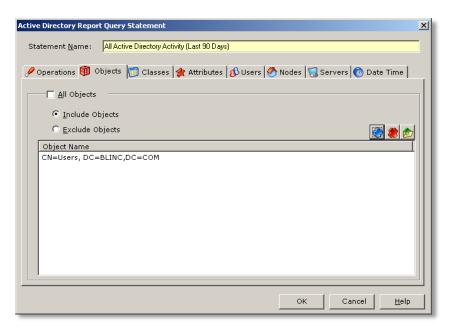
Attributes are any properties that define an object. Report on specific attributes like DACL, description and surname. Reports can also be generated on values given to attributes.

Active Directory Report Query Statement	X
Statement Name: All Active Directory Activity (Last 90 Days)	
🖋 Operations 🔞 Objects 🔝 Classes 🞓 Attributes 🚯 Users 🔗 Nodes 🗟 Servers 🔞 Date Time	
All Attributes	
O Exclude Attributes	
Attribute Name	
cn	
OK Cancel <u>H</u> elp	

ΒΓΠΕ ΓΥUCE

Objects

Objects are entities in the directory. Specific objects to report on are in this tab.



Operations

The operations available for reporting in a Directory query are actions related to changes in objects, accounts, group membership and administration.

Active Directory Report Query Statement	×
Statement Name: All Active Directory Activity (Last 90 Days)	
🥙 Operations 爾 Objects 🗊 Classes 🙀 Attributes 🚯 Users 🥙 Nodes 😡 Servers 🔞 Date Time	
All Operations	
Include Operations	
C Exclude Operations	
Object Account Modification Zenable Account Success Of Disable Account Disable Account Of Success Set Password Of Success Of Change Password Of Success Of Change Password Of Success Of Change Password Of Success Of Sucess Of Success Of Success Of Sucess O	
OK Cancel Help	

The operations available for reporting include object creation, modification, and deletion; account modification; changes in group membership; password changes and changes in administration.

BLUE LΔΠCE

Report Statement Tab for the Group Policy Report Arm

Objects

In Group Policy, a group policy object is a container where policy settings are stored.

Group Policy Report Query Statement	x
Statement Name: All Group Policy Changes Report	
🖋 Operations 🔀 Group Policy 🌟 Attributes 🚯 Users 🕙 Nodes 📆 Servers 🔞 Date Time	
All Group Policy Objects Include Group Policy Objects	
C Exclude Group Policy Objects	
GPOs Name	
Domain Group Policy	
OK Cancel <u>H</u> elp	1

Attributes

Attributes are properties that define the group policy and LT Auditor+ allows for granular reporting.

Active Directory Report Query Statement	×
Statement Name: All Active Directory Activity (Last 90 Days)	
🖋 Operations 镧 Objects 🔝 Classes 🎓 Attributes 🚯 Users 🔗 Nodes 😡 Servers 🔞 Date Time	
All Attributes	
C Exclude Attributes	
Attribute Name	
cn	
OK Cancel <u>H</u> elp	

ΒΓΠΕ ΓΥUCE

Report Statement Tab for the NetWare Report Arm

Values

Values assigned to attributes can be queried for in this tab.

NetWare Report Query Statement
Statement Name: All NetWare Activity Report
🖋 Operations 爾 Objects 🗊 Classes 🌟 Attributes 🔼 Values 🚯 Users 🥙 Nodes 🐻 Servers 🔞 (🕨
All Values
C Include Values
C Exclude Values
Value Name
OK Cancel <u>H</u> elp

Report Statement Tab for the Cross-platform Report Arm

The cross-platform reports allow users to report consolidated information across all report arms. For example, if a single report of Active Directory, eDirectory and NetWare activity was required, one can do so with cross-platform reports. Another example would be a query for a particular user's entire activity across everything, audited with LT Auditor+.

A cross-platform report statement contains a combination of all tabs discussed above as shown below.

ΒΓΠΕ ΓΥUCE

Cross Platform Report Query Statement	×
Statement <u>N</u> ame: Activity Report	
🖋 Operations 🔯 Objects 🗊 Classes 🌟 Attributes 🚯 Users 🧭	Nodes 😡 Servers 🌀 Date & Time
All Operations	
Include Operations	
C Exclude Operations	
 ☐ Active Directory Auditing ☐ Group Policy Auditing ☐ Logon Server Auditing ☑ File System Auditing ☑ Mative Event Log Auditing ☑ Removable Device Auditing ☑ NetWare Auditing ☑ eDirectory Auditing ☑ eDirectory Auditing ☑ eDirectory Logon Auditing ☑ MAS Device Auditing 	
	OK Cancel <u>H</u> elp

Report Statement Tab for the Audit the Auditor Report Arm

Audit the Auditor reports display information on modifications made to configurations and policies within LT Auditor+. It is important to audit the activity of LT Auditor+ administrators. The screen below displays the standard tabs available for querying.

Audit The Auditor Report Query Statement
Statement Name: All Audit The Auditor Activity Report
🖉 Operations 🙀 Objects 🗊 Classes 🚖 Attributes 🚯 Users 🤣 Nodes 🔞 Date & Time
Include Operations
C Exclude Operations
□ Workspace □ Sign in □ Filter Statement Added □ Filter Statement Deleted □ Filter Statement Modified □ Job Added □ Job Deleted □ Job Deleted □ Job Deleted □ Authorized User Added □ Group Settings Changed □ Group Added □ Agent Added
OK Cancel <u>H</u> elp

Report Statement Tab for the Rollup Status Monitoring Report Arm

The rollup status monitoring reports provide information on the status of data inserted into the LT Auditor+ database. Users can get information such as:

- How many records were inserted per agent.
- How many agents did not send data.
- Patterns for volume of audit data collected over time.

The following screen displays tabs available to query for rollup information.

Rollup Status Monitoring Report Query Statement 🛛 🗙
Statement Name: Audit Sub System Rollup Activity (Prev 1 Day)
🔂 Agents 爾 Audit Sub Systems 🔞 Date & Time
All Agents
C Include Agents
C Exclude Agents
Server Name
OK Cancel <u>H</u> elp

Advanced Settings

The Advanced Settings option in the Report Console allows users the following options:

- Choose the report output type (email, send to printer, etc.).
- Choose the type of report (chronological columnar, etc.).
- Determine whether multiple statements will be linked by "AND" or " OR."
- Give the report a description.

To access Advanced Settings:

- 1. Select the report query statement.
- 2. Click Advanced Settings in the top right pane.

The Advanced Settings window has multiple tabs discussed below.

Report Settings

eport Query Adva	nced Settings 🛛 🗴
Report Quer	y Statements
<u>C</u> riteria:	OR
Show Rej	port Title
Tit <u>l</u> e:	LT Auditor+
Su <u>b</u> - Title:	Radar For Your Network
Show Re	port <u>H</u> eader / Footer
H <u>e</u> ader:	LT Auditor+
F <u>o</u> oter:	(c) Copyright Blue Lance, Inc. 2011. All Rights Reserved.
<u>A</u> dditional Argu	iments
	OK Cancel <u>H</u> elp

Criteria – Used when combining multiple query statements within a query, they may be linked by either the logical phrase "AND" or the logical phrase "OR."

- AND Using the phrase AND to link query statements will return only the data that applies to the parameters of all statements.
- OR Using the phrase OR to link query statements will return data that applies to the parameters of any statement in a query, not necessarily all statements.

Show Report Title and Subtitle – In this field you may choose to show, hide or change the report's title and subtitle.

Show Report Header and Footer – In this field you may choose to show, hide or change the report's header and footer.

Additional Arguments – This field is used to write in additional information necessary to run specific types of reports.

Output – Under the Output tab, you will be able to select how you would like to organize the report and where you would like it to be viewed.

eport Query Advanced Settings					X
🌟 Report Settings 🖋 🛛 Output	🚯 Description				
LSAChronologi LSAChronologi LSASummaryG LSASummaryG LSAFailedLogin LSASummaryG © Show Report LSASummaryG	roupedByUserA roupedByNodeA	upedByUser.rpt tion.rpt pt ndDate.rpt ndUser.rpt			•
Send Report To Printer	Subject:	Email Address			+
💮 Export Report To File					
💮 Email Report	Cc:	Email Address			+ // ×
			ок	Cancel	Help

You may have it shown on screen, sent to a printer, exported to a file or sent in an email. If you choose to send the report in an email, you may enter the email settings as desired in the right portion of this window. You must give the report a file name and format when sending it to a file or via email.



Choosing to show the report on screen will prevent you from being able to schedule the report, so it should only be used when generating a single report.

Selection of a Report File Name determines the format of the report. There are multiple report formats defined based on the report arm selected. Some are displayed below:

Chronological Columnar

This report output type is the default setting for most reports generated. It is viewed in columns of text with the data listed from least to most recent.

Generated Generated		sday, December 10, 2020 RAGON\pthomas	1					
Date & Tin	ne	User	Node	Operation	Class	Object	Server	Remarks
11/1/2020 10:00:00AN	И	BLDRAGON\AHende rson	98.197.208.193	Modify Object	user	CN=Ruth Quinn,OU=OU-Mar keting,OU=Corp,D C=bldragon,DC=co m	EC2AMAZ-4UN GPQH bldragon .com	Modified Attribute User-Account-Control to ['Don't Expire Password - Enabled] of user CN=Ruth Quinn,OU=OU-Marketing,O U=Corp,DC=bldragon,DC = com
11/3/2020	8:00:29PM	BLDRAGON\pthoma s	98.197.208.193	Delete Attribute Value	domainDNS	DC=bldragon,DC =c om	EC2AMAZ-4UN GPQH.bldragon .com	Deleted value of attribute nTSecurityDescriptor [O:BAG:BAD:AI(OA;:CR;3e 0f7e18-2c7a-4c10-ba82-4d 926d] for DC=bIdragon,DC=com [domainDNS]
11/3/2020	8:00:29PM	BLDRAGON\pthoma s	98.197.208.193	Modify Security DACL	domainDNS	DC=bldragon,DC=c om	EC2AMAZ-4UN GPQH.bldragon .com	Modified Security DACL of domainDNS DC=bldragon,DC =com
11/3/2020	8:00:29PM	BLDRAGON\pthoma s	98.197.208.193	Set Password	user	CN=Collin Evans,OU=Corp,D C=bldragon,DC=co m	GPQH bldragon	Set Password for user CN=Collin Evans,OU=Corp,DC=bldrag on,DC=com
11/3/2020	8:00:29PM	BLDRAGON\pthoma s	98.197.208.193	Enable Account	user	CN=Collin Evans,OU=Corp,D C=bldragon,DC=co m	GPQH bldragon	Enabled Account CN=Collin Evans,OU=Corp,DC=bldrag on,DC=com
11/3/2020	8:00:29PM	BLDRAGON\pthoma s	98.197.208.193	Enable Account	user	CN=Collin Evans,OU=Corp,D C=bldragon,DC=co m	GPQH bldragon	Enabled Account CN=Collin Evans,OU=Corp,DC=bldrag on,DC=com

Chronological Columnar Grouped by User

This report output type is similar to the one prior, but data is grouped by user. It is then listed in chronological form from least to most recent data within each user's group of data.

				LT Auditor+	Oversight Report		
Generated Generated		day, December 10, 3 AGON\pthomas	2020				
Date & Tin		Node	Operation	Class	Object	Server	Remarks
Jser: BL	DRAGON	AHenderson					
12/7/2020	1:49:04AM	98.197.208.193	Modify Security DACL	container	CN=AdminSDHolder,C N=System,DC=bldrago n,DC=com	EC2AMAZ-4U NGPQH.bldrag on.com	Modified Security DACL of container CN=AdminSDHolder,CN=System,DC=b dragon,DC=com
Jser: BL	DRAGON	pthomas					
11/3/2020	8:00:29PM	98.197.208.193	Modify Security DACL	domainDNS	DC=bldragon,DC=com	EC2AMAZ-4U NGPQH.bldrag on.com	Modified Security DACL of domainDNS DC=bldragon,DC=com
11/3/2020	8:00:29PM	98.197.208.193	Enable Account	user	CN=Collin Evans,OU=Corp,DC=bl dragon,DC=com	EC2AMAZ-4U NGPQH.bldrag on.com	Enabled Account CN=Collin Evans,OU=Corp,DC=bldragon,DC=com
11/3/2020	8:00:29PM	98.197.208.193	Enable Account	user	CN=Collin Evans,OU=Corp,DC=bl dragon,DC=com	EC2AMAZ-4U NGPQH.bldrag on.com	Enabled Account CN=Collin Evans,OU=Corp,DC=bldragon,DC=com
11/3/2020	8:00:29PM	98.197.208.193	Enable Account	user	CN=Clare Schmitt,OU=Corp,DC= bldragon,DC=com	EC2AMAZ-4U NGPQH.bldrag on.com	Enabled Account CN=Clare Schmitt,OU=Corp,DC=bldragon,DC=co m
11/3/2020	8:00:29PM	98.197.208.193	Enable Account	user	CN=Clare Schmitt,OU=Corp,DC= bldragon,DC=com	EC2AMAZ-4U NGPQH.bldrag on.com	Enabled Account CN=Clare Schmitt,OU=Corp,DC=bldragon,DC=co m
11/3/2020	8:00:29PM	98.197.208.193	Enable Account	user	CN=Julianna Black,OU=Corp,DC=bl dragon,DC=com	EC2AMAZ-4U NGPQH.bldrag on.com	Enabled Account CN = Julianna Black,OU=Corp,DC=bldragon,DC = com
11/3/2020	8:00:29PM	98.197.208.193	Enable Account	user	CN=Julianna Black,OU=Corp,DC=bl dragon,DC=com	EC2AMAZ-4U NGPQH.bldrag on.com	Enabled Account CN=Julianna Black,OU=Corp,DC=bldragon,DC=com
Copyright (c) Blue Lance.	Inc. 2020. All rights	reserved, www.BlueLa	ance.com			Page 1

BLUE LΔΠCE

Summary Grouped by Operation

This report output type is shown in graph form. Each audited operation being reported will represent one bar in the graph. The number of times that operation was performed will be shown by the height of each bar. The specific counts for each operation will be listed in text format below the graph. This report also permits the user to drill down into the details.

1

		LT Auditor+ Oversight Report		
Generated On: Thursday, Dece Generated By: BLDRAGON/ptt				
		Operation	Add Attribute Value	Add Member to Group
450 400 350 300			E Delete Attribute Value	
300 250 250 150 150			Enable Account	≡ Modify Object
			Modify Security DACL	Set Password
and spin at a second	of the state of the state state state state	and contract second second second	E User Account Locked Out	User Account Unlocked
Add Attribute Value	58			
Add Member to Group	<u>49</u>			
Delete Attribute Value	2			
Disable Account	4			
Enable Account	428			
Modify Object	11			
Modify Security DACL	5			
Set Password	216			
User Account Locked Out	1			

Summary Grouped by User

This report output type is shown in graph form. Each audited operation being reported will represent one bar in the graph. The number of times that operation was performed will be shown by the height of each bar. The specific counts for each operation will be listed in text format below the graph.

			LT Auditor	+ Oversight	Report			
ienerated On: Thursday, Dec ienerated By: BLDRAGON(c	cember 10, 2020 othomas							
			Ope	rations				
10			For BLDRA	GON\AH en derson			_	
Total Operations					_	1	Add Attribute Value Delete Attribute Value Diable Account Modfy Chject Modfy Chject Modfy Security DACL Set Pasavord User Account Unlocked	
and the state		Digities.	Profit COPE	Proditi DAC	the Property	UNE REPORT		
ser: BLDRAGON\AHer	nderson							
dd Attribute Value	<u>9</u>							
elete Attribute Value	5							
isable Account	4							
odify Object	2							
odify Security DACL	1							
et Password	2							
ser Account Unlocked	1							
		d. www.BlueLanc						Page

Failed Logon Summary Report

This is a report containing failed login data categorized by user and specified by a threshold of a minimum number of failed login attempts.

When selecting this type of report, return to the Report Settings tab and under Additional Arguments, enter **%T=n**, where "n" is the minimum number of failed login attempts by any one user to be generated in the report.

		Failed Logon Report	
		LT Auditor+ Oversight Report	
enerated On : enerated By:	Thursday, December 10, 2020 BLDRAGONipthomas		
perations	Total	Number of Failed Logons	
ser: bldrago	n\BWhite		
etwork Logon		5	
ser: Bldrago	on\CAustin		
etwork Logon		22	
ser: dragon			
etwork Clear Te	xt Logon	1	
nd of Report			

Description

Under the tab you can create a description of your query. You may choose to include any information regarding the purpose of the query, how it is configured, when it is scheduled to run and in what form it will be viewed.

BLUE LΔΠCE

Report Query Advanced Se	ettings	×
🌟 Report Settings 🖋	Output B Description	
	OK Cancel <u>H</u> elp	

Creating additional report query statements:

- 3. Select the report query statement.
- 4. Click New in the right pane displaying all the report query statements for the specific report query.

Modify a report query statement:

- 1. Select the report query statement.
- 2. Click Edit in the right pane, which displays all the report query statements for that report query.
- 3. Modify the report query statement data.
- 4. Click OK.

Delete a report query statement:

- 1. Select the report query statement.
- 2. Click Delete in the right pane, which displays all the report query statements for that report query.
- 3. Click Yes when prompted for confirmation.

Modify a Report Query:

- 1. Select the report query and select one of the following:
- 2. Click Report \rightarrow Edit in the menu OR Click Edit on the toolbar.
 - -----
- 3. Modify the report query data.
- 4. Click OK.

Delete a report query:

- 1. Select the report query.
- 2. Select one of the following:

Click Report \rightarrow Delete in the menu

OR

Click Delete on the toolbar.

3. Click Yes when prompted for confirmation.

Generate a report:

- 1. Select the report query.
- 2. Select Generate Report from the Report Console toolbar. A sample report is shown below.

ienerated On: Thursday, December 10, ; ienerated By: BLDRAGONpthomas iperations ser: bidragon\BWhite	Failed Logon Report LT Auditor+ Oversight Report 2020 Total Number of Failed Logons	
Benerated By: BLDRAGON\pthomas		
	Total Number of Failed Logons	
ser: bldragon\BWhite		
letwork Logon	5	
ser: Bldragon\CAustin		
letwork Logon	22	
	-	
ser: dragon\pthomas		
letwork Clear Text Logon	1	
nd of Report		
opyright (c) Blue Lance, Inc. 2020. All rights r	account www.Plust.anco.com	Page 1
opyright (c) blue cance, Inc. 2020. All rights h	asalvad, www.blueLairce.com	Page 1

Scheduling a Report

Scheduling a report in the Report Console is made simple by the Report Scheduler. Highlight the query

you would like to schedule and click Report \rightarrow Report Scheduler, or click on the schedule icon in the toolbar.

The Report Console will prompt you for database connection information.

Report Scheduler	×
Please select Database Settings	
Database Connections	OK <u>C</u> ancel <u>H</u> elp

Select your database from the drop-down box, or choose to create a new connection. Once you are connected, the Job Details window will appear.

nedule Report				
ease enter Job Det	ails			
Job <u>N</u> ame:	Test Job			
inte.	Trescool			
Job <u>F</u> requency:	Daily			
Day of Week:		V	Date: 6/ 3/2011	V
Job <u>S</u> tart Time:	3:33:52 PM	<u>.</u>	Day of the Month(s):	1 🚊
	,			
🔽 Use System Acc	ount			
,				
User <u>N</u> ame:				
Password:				
<u>R</u> e-type Passwo	rd:			
				Hele
			<u>O</u> k <u>C</u> ancel	<u>H</u> elp

Enter the job name, job frequency, date and start time as necessary. When properly configured, click OK. You will receive reports with the frequency you requested in the output format previously configured in the Advanced Settings window.

A list of all scheduled reports can be viewed by clicking on the menu Report \rightarrow View Scheduled Reports.

Task N	Report Query Name		Fr	Next Run Time	Last Run Time	Status	Modify
fest Job	Files Created Report	6/3/2011 3:33:00 PM	Daily	6/4/2011 3:33:00 PM	Never Run	-	
File Activity	All Activity Report	12/7/2010 5:53:00 AM	Daily	6/4/2011 5:53:00 AM	6/3/2011 5:53:00 AM	Ready	<u>D</u> elete

Chapter 5 – Securing LT Auditor +

Authenticating to the Workspace

There are several areas in LT Auditor+ that require authentication to access.

- Security Management Console
- Manager Console
- Report Console
- Remote Install for Agents

There are two levels of security for LT Auditor+. Level 1 security defines the users authorized to access the workspace. Level 2 securities define users authorized to access the managers.

LT Auditor+ Security Level 1

Authorized users will access the workspace by authentication. For example, LT Auditor+ for Windows will access the workspace through a Microsoft SQL server or through an Oracle server. The first level 1 user is added during the initial installation.

To launch the Security Management Console:

- 1. Click Start \rightarrow All Programs \rightarrow Blue Lance, Inc \rightarrow Management Console.
- 2. The screen displayed below prompts for the database connection information.
- 3. Connect to the workspace to add authorized users.

For SQL:

abase Connection I	Details			
Database Type				
Microsoft	SQL Server			
Microsoft SQL Ser	ver Settings			
<u>S</u> erver:				
<u>D</u> atabase:	in and a second s			
C Use NT	Integrated Sec	urity		
U <u>s</u> er N	ame and passwo	ord		
<u>U</u> ser Name				1
Password:				
				R:
	est Connection	ок	Cancel	<u>H</u> elp
		I		

- 1. Select Microsoft SQL Server for Database Type information.
- 2. Provide Server ID.
- 3. Provide Database Name.
- 4. If NT Integrated Security was enabled during installation, you should be signed in with your Windows password. If User Name and Password was selected, provide the username and the password.
- 5. Click OK.

For Oracle:

Database Type			
0racle			
Oracle Settings			
Host String	: [
<u>U</u> ser Name	: [
<u>P</u> assword:	[

- 1. Select Oracle for database type.
- 2. Provide host string.
- 3. Enter username.
- 4. Enter password.
- 5. Click OK.

The Management Console gets launched as soon as the user is authenticated to the workspace. The Management Console screen is shown in the following figure:

tem Options Help				
Agent 🔓 Authorized User	Job 🔓 Ellter Statement	* 🗶 🗗 🗭 😵		
<u></u>				
LTA9				
and the second	And the second se			
LTA9 - 🔞 LTA Manager Group	🛛 🗹 Configured filters	for Agent Group		
Data Rollup	Configured filters	for Agent Group		
- 🗸 Authorized Users	Name	Date of Creation	Filter Type	Filter Status
🗄 💕 Audit SubSystems	New Active Directory Filter Statement	4/10/2007 1:22:46 PM	Include	Enabled
🗄 🔘 LTA Manager Group 2	New Group Policy Filter Statement	4/10/2007 1:22:50 PM	Include	Enabled
🚽 🌗 Data Rollup	New Logon Server Filter Statement	4/10/2007 1:22:54 PM	Include	Enabled
🧟 Authorized Users	New File System Filter Statement	4/10/2007 1:23:06 PM	Include	Enabled
🕀 🧖 Audit SubSystems	New Native Event Log Filter Statement	4/10/2007 1:23:14 PM	Include	Enabled
Agent Group	New Removable Device Filter Statement	4/10/2007 1:23:21 PM	Include	Enabled
Data Transfer				
Audit SubSystems				
— 💆 Active Directory Auditing				

The Management Console is divided into two views. The left pane shows all of the currently configured workspace with the workspace name as the root node of the tree. Below the root nodes are the manager groups and agent groups of the workspace. The right pane displays the details of each node highlighted on the left side.

Select the workspace root node in the tree to display all the manager groups and agent groups in the pane on the right side.

LT Auditor+ Security Level 2

Adding Authorized Users and Groups to the LT Auditor+ Management Console

1. Open LT Auditor+ Management Console and navigate to Management Group directly under your Domain in the left panel.

S LT Auditor+ Management Console		-	۵	×
System Options Help				
🔬 👹 Add Agent 💁 Authorized I	Use 🗑 Job 🗸 Fiter Statement 🥒 🏶 📴 🥵			
🔒 blue	blue blue blue blue blue blue blue blue			
e	🔅 bluemanager			
- Authorized Users				
	Managers			
Member Server Group Morkstation Group				
Currently Authenticated Windows User: BLUELANCEPR	ACTTrugBespice Tell Expires in 15 Day(b)			

2. Click on Manager Group to expand and view Authorized Users.

LT Auditor+ Management Console stem Options Help				
	ed User 🗊 Job	Filter Statement	* * • • •	
blue blue Jobs Authorized Users Authorized Users		sgillespie sgillespie	roup:bluemanager	
RedHat Linux Group SUSE Linux Group Syslog Devices Group SUSE OES Linux Group				

3. Right-click on Authorized Users and select the Add Authorized User option.

LT Auditor + Management Console		^
System Options Help		
🎻 👹 Add Agent 🞥 Authorized	d User 🗊 Job 📮 Filter Statement 🖉 🏶 📭 🗭 🎇	
🔒 blue		
blue blue Jobs Authorized Users Audit SubSystems Windows Agent Group Domain Controller Group Member Server Group Workstation Group	Authorized Users for Group:bluemanager Authorized Users BLUELANCEPRACTI\sgillespie BLUELANCEPRACTI\sgillespie BLUELANCEPRACTI\sgillespie BLUELANCEPRACTI\IndigoGroup	
A SharePoint Group A RedHat Linux Group SUSE Linux Group	Select Users or Groups X Select this object type:	
Syslog Devices Group	Users or Groups Object Types	
🗉 🇑 SUSE OES Linux Group	From this location:	
	bluelancepractice.com	
	Enter the object names to select (examples): Check Names	
	Advanced OK Cancel	~

ΒΓΠΕ ΓΥυςε

LT Auditor + Management Console	
Select Users or Groups	X
Locations	×- 2 * 10 5 %
Select the location you want to search. Location: Entre Directory Big Biolectory Control of the Selectory Control of the Selectory Control of	
(B)- 윷을 Bluelancepractice com	for Group:bluemanager
ei- eu snarevoirt uroup	OK Cancel
ter egu snarrerom uroup (∃-∞) Aedhat Linux Group (∃-∞) SUSE Linux Group (∃-∞) Syslog Devices Group (∃-∞) SUSE OES Linux Group	

4. If needed, click on the Locations button to navigate to the domain that contains users or groups you want to add.

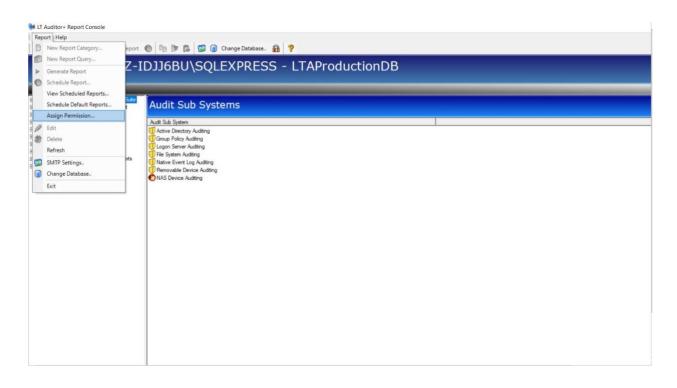
LT Auditor+ Management Console		^
System Options Help		
🧞 鬄 Add Agent 🔬 Authorize	ed User 🗊 Job 📮 Filter Statement 🖉 🏶 р 🗭 <table-cell></table-cell>	
🔒 blue		
blue blue	Authorized Users Authorized Users BLUELANCEPRACTI\sgillespie BLUELANCEPRACTI\sgillespie BLUELANCEPRACTI\IndigoGroup Select Users or Groups Select this object type: Users or Groups From this location: bluelancepractice.com Locations Enter the object names to select (examples): I Advanced OK	

- 5. With the desired domain location selected, enter name(s) of user(s) and/or group(s) to authorize.
- 6. After adding the desired users and/or groups, click the Check Names button to confirm.

7. Click the OK button, and the user/group path(s) will show up under Authorized Users.

Adding Authorized Users or Groups to the LT Auditor+ Reporting Console

- 1. Open the LT Auditor+ Reports Console and click on the Report tab.
- 2. Select the Assign Permissions option.



3. To add permissions for individual users or groups, click the Restrict Access option.

UT Auditor - Report Console Report Help D D A A A A A A A A A A A A A A A A A A	_	r 爲 😭 @ Change Database. 🛔 BU\SQLEXPRESS	ctionDB	
Cl T Audtor- for Windows Enterprise Sute Cl T Audtor- for Windows Assessment Cl T Audtor- for SU, Saver Cl T Audtor- for SU, Saver Cl T Audtor- for System Cl T Audtor- for NetWare Cl T Audtor- for NetWare Cl T Audtor- Compliance Reports Cl T Audtor- Utilities	Audt Audt Suk Active Group Logon File Sy Native Remov	ssigning LT Auditor+ Reporting Console f LT Auditor+ Reporting Console Acc C Full access Restrict access Assigned Permissions User/Group Diuelancepracti\domain admins	Restrict Access bluelancepract/domain admins Reporting Console Administrator Report Category Be LT Auditor+ for Windows Enterprise Suite DIT Auditor+ for Sysleg Devices DIT Auditor+ for Sysleg Devices DIT Auditor+ Cross Platform Reports DIT Auditor+ Cross Platform Reports DIT Auditor+ Utilities	
		AddDelete	Servers + -	

Note: if the Full Access option is selected, then anyone with access to the LT Auditor+ Reporting Console will be able to use the application.

4. Click the Add button to add users or groups.

M LT Auditor + Report Console	Addrey for Soverance & Overaide Reports Charles Constance Reports Charles			
Report Help				
📄 👩 🥒 🏶 🕨 Generate Report 🕥 📭 [🖻 🕵 👩 Change Database 👔 🧖			
		1917 (D.W.		
		oductior		
Constant of Subset and the second of th		^ <u></u>		
	Converse Report Converse Report Converse Report Converse Report Converse Reporting Console Access Control Converse Report Calegory Report Calegory Converse Reports Co			
Auditor+ for SQL Server	Compared Report Console Report Console Access Control Console Addressing Console Co			
	Restrict access		Reporting Console Administrator	
A LE L L L L L L L L L L L L L L L L L L			Report Category	
Goup				
Construction Platform Reports				
Cyber Governance & Oversight Reports Native				
Hemor		×		
-	Select this object type:		Cyber Governance & Oversight Reports	
	Users or Groups	Object Types	E- LT Auditor+ Utilities	
	From this location:	_		
	ECCAMMAZ-IDJJGBU\SQLEXPRESS - LTAProductionDB			
	Enter the object names to select (examples):		Samar	
	Dire die dijet, names to seet, (<u>eta totes</u>).	Charle Manua		
	1	Check Names	+ -	
B: C LT Audror- Korn Nurve Group Administrator Image: Construction of the construction of				
	Advanced	Connel		
	Advances	Cancel	4	
	Add Delete		Save	
	hereste Report			
Report Help Image: Construction of the second se				

5. If needed, click on the Location(s) button to navigate to the domain where you want to assign users or groups.

A Links				
rt Help		F 🎒 🍘 Change Database. 👔 💡		
EC2AMAZ-I	IDJJ6F	3U\SQLEXPRESS - LTAProduct	ionDB	
	A	ssigning LT Auditor+ Reporting Console Permissions	×	_
LT Auditor+ for Windows Enterprise Suite	Audi	LT Auditor+ Reporting Console Access Control	Restrict Access	
LT Auditor+ for Windows Assessment LT Auditor+ for SQL Server	Auui	C Full access	bluelancepracti\domain admins	
LT Auditor+ SUSE Linux LT Auditor+ for Syslog Devices	Audit Sub	Restrict access	Reporting Console Administrator	
LT Auditor+ for NetWare	Group	Assigned Permissions	Report Category	
LT Auditor+ Compliance Reports LT Auditor+ Cross Platform Reports	U Logon	User/Group Administrator	D LT Auditor+ for Windows Enterprise Suite	
Cyber Governance & Oversight Reports LT Auditor+ Utilities	Vative	bluelancepracti\domain admins True	D T Auditor+ SUSE Linux D LT Auditor+ for Syslog Devices	
	Removi	Select Users or Groups	X B- LT Auditor + for NetWare	
		Locations	X yber Governance & Oversight Reports	
		Select the location you want to search.	Auditor+ Utilities	
		Location:		
		EC2AMAZ-IDJJ6BU		
			- 1 - 1	
		In the construction	+ -	
	-			
		OK	Cancel Save	
Auditor+ Report Console				
ort Help	0 9 0	F 🕼 🚰 🕝 Change Database. 🏦 💡		
ort Help			onDB	
ort Help		BU\SQLEXPRESS - LTAProducti	onDB	
ort Help	IDJJ6E		ionDB ×	
ort Help		BU\SQLEXPRESS - LTAProducti	Restrict Access	
the p Contract Report Contract Report Contract Report CONTRACT Contract Report	DJJ6E	BU\SQLEXPRESS - LTAProductions signing LT Auditor + Reporting Console Permissions LT Auditor + Reporting Console Access Control C Full access	Restrict Access	
ort Help Control Help Contro	Audi Audi	BU\SQLEXPRESS - LTAProducti ssigning LT Auditor + Reporting Console Permissions	Restrict Access bluelancepracti\domain admins IV Reporting Console Administrator	
ort Help Control Help Contro	Audi Audi Audi Suk	BU\SQLEXPRESS - LTAProductions signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions	Restrict Access Duelancepract\domain admins Reporting Console Administrator Report Category	
ort Help Control Help Contro	Audi Audi	BU\SQLEXPRESS - LTAProducti ssigning LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User/Group Administrator	Restrict Access bluelancepract\domain admins F Reporting Console Administrator Report Category D	
ort Help Control Help Contro	Audi Audi Audi Audi Active Group Logen File Sy Native	BU\SQLEXPRESS - LTAProducti ssigning LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User/Group bluelancepracti\domain admins True	Restrict Access bluelancepract\domain admins V Reporting Console Administrator Report Category ⊕ LT Auditor+ for Windows Enterprise Suite ⊕ LT Auditor+ SUSE Linux ⊕ LT Auditor+ SUSE Linux	
ort Help Control Help Contro	Audi Audi Audi Audi Active Group Logen File Sy Native	BU\SQLEXPRESS - LTAProducti ssigning LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User/Group Administrator	Restrict Access Veleancepract/domain admins V Reporting Console Administrator Report Category I LT Auditor+ for Windows Enterprise Suite I LT Auditor+ SUSE Linux I LT Auditor+ for Sysleg Devices X B::::::::::::::::::::::::::::::::::::	
ort Help Control Help Contro	Audi Sub Audi Sub Active Group Logon Frie Sy Native Remov NAS I	BU\SQLEXPRESS - LTAProducti ssigning LT Auditor + Reporting Console Permissions LT Auditor + Reporting Console Access Control C Full access Restrict access Assigned Permissions User/Group Duelancepracti/domain admins True Select Users or Groups Select this object type:	Restrict Access bluelancepract\domain admins F Reporting Console Administrator Report Category ⊕ LT Auditor+ for Windows Enterprise Suite ⊕ LT Auditor+ SUSE Linux ⊕ LT Auditor+ for NetWare ⊕ LT Auditor+ for Subtorm Reports	
ort Help Control Help Contro	Audi Audi Audi Audi Caup U Grup U Grup U Grup Natre Remo NAS C	BU\SQLEXPRESS - LTAProductions Select Users or Groups Select type: Users or Groups Cobject Type Cobject C	Restrict Access bluelancepract\domain admins F Reporting Console Administrator Report Category ⊕ LT Auditor+ for Windows Enterprise Suite ⊕ LT Auditor+ SUSE Linux ⊕ LT Auditor+ for NetWare ⊕ LT Auditor+ for Subtorm Reports	
Ant Help Control Help Contro	Audi Audi Audi Adrive Group The Sy Herse Remot Remot Remot	BU\SQLEXPRESS - LTAProductions signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User/Group Diuelancepracti\domain admins True Select Users or Groups Select Users or Groups Select the object type: User or Groups From the location:	Restrict Access Velocal copyract/domain admins Reporting Console Administrator Report Category UT Auditor+ for Windows Enterprise Suite UT Auditor+ for Syslog Devices UT Auditor+ for NetWate UT Auditor+ Cross Platform Reports U_LT Auditor+ Utilities	
Ant Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProducti signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User/Group Administrator bluelancepractividomain admins True Select Users or Groups Select this object type: User or Groups From this location: Bluelancepractice com Locations	Restrict Access Viuelancepract/domain admins Report Category El T Auditor+ for Windows Enterprise Suite LT Auditor+ for SuSE Linux LT Auditor+ for Sulog Devices LT Auditor+ for NetWate LT Auditor+ Cross Platform Reports LT Auditor+ Cross Platform Reports LT Auditor+ Utilities	
ort Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProducti signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User(Group Administrator bluelancepractive domain admins True Select Users or Groups Select type: User or Groups Select type: User or Groups Select type: User or Groups Dem this locaton: bluelancepractice com Enter the object names to select (examples):	Restrict Access bluelancepract/domain admins P. Reporting Console Administrator Report Category Image: Category	
Ant Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProducti signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User/Group Administrator bluelancepractividomain admins True Select Users or Groups Select this object type: User or Groups From this location: Bluelancepractice com Locations	Restrict Access bluelancepract/domain admins P. Reporting Console Administrator Report Category Image: Category	
ort Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProducti signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User(Group Administrator bluelancepractive domain admins True Select Users or Groups Select type: User or Groups Select type: User or Groups Select type: User or Groups Dem this locaton: bluelancepractice com Enter the object names to select (examples):	Restrict Access bluelancepract/domain admins P. Reporting Console Administrator Report Category Image: Category	
oort Help	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProducti signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control C Full access Restrict access Assigned Permissions User(Group Administrator bluelancepractive domain admins True Select Users or Groups Select type: User or Groups Select type: User or Groups Select type: User or Groups Dem this locaton: bluelancepractice com Enter the object names to select (examples):	Restrict Access bluelancepract/domain admins P Reporting Console Administrator Report Category P LT Auditor+ for Windows Enterprise Suite D LT Auditor+ for Suite Devices P LT Auditor+ Utilities P LT Auditor+ Utilities P LT Auditor+ Utilities	
Ant Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProductions signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control Full access Assigned Permissions User(Group Administrator Ubuelancepractivity Lear or Groups Select the object type: User or Groups From the locaton: Buselancepractice com Locatons Erter the object names to select (examples): Check Name	Restrict Access bluelancepract/domain admins P Reporting Console Administrator Report Category P LT Auditor+ for Windows Enterprise Suite D LT Auditor+ for Suite Devices P LT Auditor+ Utilities P LT Auditor+ Utilities P LT Auditor+ Utilities	
Ant Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProductions signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control Full access Assigned Permissions User(Group Administrator Ubuelancepractivity Lear or Groups Select the object type: User or Groups From the locaton: Buselancepractice com Locatons Erter the object names to select (examples): Check Name	Restrict Access bluelancepract/domain admins P Reporting Console Administrator Report Category P LT Auditor+ for Windows Enterprise Suite D LT Auditor+ for Suite Devices P LT Auditor+ Utilities P LT Auditor+ Utilities P LT Auditor+ Utilities	
ort Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProductions signing LT Auditor+ Reporting Console Permissions LT Auditor+ Reporting Console Access Control Full access Assigned Permissions User(Group Administrator Ubuelancepractivity Lear or Groups Select the object type: User or Groups From the locaton: Buselancepractice com Locatons Erter the object names to select (examples): Check Name	Restrict Access bluelancepract/domain admins P Reporting Console Administrator Report Category P LT Auditor+ for Windows Enterprise Suite D LT Auditor+ for Suite Devices P LT Auditor+ Utilities P LT Auditor+ Utilities P LT Auditor+ Utilities	
ort Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProductions Select Area and a select for the select type: User of Groups Coech type: Co	Restrict Access bluelancepractb\domain admins Reporting Console Administrator Report Category P LT Auditor+ for Windows Enterprise Suite D LT Auditor+ for Syste Devices C LT Auditor+ for NetWare D LT Auditor+ for NetWare D LT Auditor+ Unities E L LT Auditor+ Unit	
ort Help Control Help Contro	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProductions Select Area and a select for the select type: User of Groups Coech type: Co	Restrict Access bluelancepractb\domain admins Reporting Console Administrator Report Category P LT Auditor+ for Windows Enterprise Suite D LT Auditor+ for Syste Devices C LT Auditor+ for NetWare D LT Auditor+ for NetWare D LT Auditor+ Unities E L LT Auditor+ Unit	
tt Help	Audt Sub Audt Sub Audt Sub Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp Grupp	BU\SQLEXPRESS - LTAProductions Select Area and a select for the select type: User of Groups Coech type: Co	Restrict Access bluelancepractb\domain admins Reporting Console Administrator Report Category P LT Auditor+ for Windows Enterprise Suite D LT Auditor+ for Syste Devices C LT Auditor+ for NetWare D LT Auditor+ for NetWare D LT Auditor+ Unities E L LT Auditor+ Unit	

- 6. Enter name(s) of user(s) and/or group(s) you want to authorize.
- 7. After adding the desired users and/or groups, click the Check Names button to confirm.
- 8. Click the OK button and the user/group path(s) will show up under Authorized Users.

BLUE LΔΠCE

If Auditor+ Report Console Report Help		BU\SQLEXPRESS		ctionDB	
LT Audtor+ for Windows Enterprise Suite LT Audtor+ for Windows Assessment LT Audtor+ for SQL Server LT Audtor+ SUSE Linux LT Audtor+ for Ssido Devices	Audi Audit Sub	ssigning LT Auditor+ Reporting Console P LT Auditor+ Reporting Console Acce C Full access @ Restrict access		Restrict Access bluelancepracti\domain admins Reporting Console Administrator	
B → LT Audtor + for SQL Server D → LT Audtor + for Sylds Devices LT Audtor + for Sylds Devices LT Audtor + for Sylds Devices LT Audtor + for NetWare Cycler Cores Platform Reports D → LT Audtor + Cores Platform Reports D → Cycler Cores Platform Report	Group Logon File Sy Native	Assigned Permissions User/Group bluelancepracti\domain admins	Administrator True	Report Category Image: Category	
		Add Delete		Save	

- 9. To add Restrictions to specific report categories, select the user or group under the Assigned Permissions table, and check the boxes for the needed accessibility rules under Report Category. If the user or group needs access to all report categories, check the Reporting Console Administrator check box.
- 10. Select the Save option when finished and exit the Assign Permissions console.

APPENDIX A

Update Agents

Overview

The purpose of the Update Agents Utility is to automatically upgrade patches remotely on LT Auditor+ Agents from a manager machine hosting LT Auditor+.

Blue Lance will periodically release patches for LT Auditor+. These patches can be downloaded from the Blue Lance support website at <u>www.bluelance.com/support</u>.

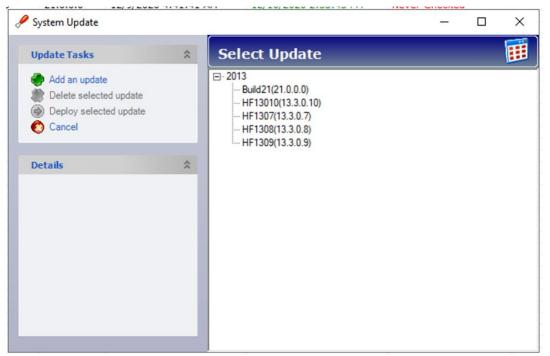
Following the patch download, the Update Agents Utility can be used to ensure that you have installed and deployed a patch across your environment for optimal performance.

NOTE

System should be accessed/launched by authorized users from existing Management Console application. No other application or process should be allowed to access or launch this application.

Follow the steps to update all Windows agents.

1. Launch the LT Auditor+ Management Console and bring the System Update window by clicking Options →Update Agents.



2. Select the latest update and click Deploy Selected update to bring up the following screen.

🔗 Select Agents for Update		- • ×
	Select Agents	🥫
	Agent Name	Search
	ws Domain Controller Group Member Server Group RedHat Linux Group StarePoint Group SUSE Linux Group SUSE DES Linux Group SUSE OES Linux Group Syslog Devices Gr	
	< Back Next > Cance	el Help

3. Select the Windows agents to be upgraded and click Next. The system will check each of the selected agents and will confirm if each agent is ready to be updated.

ΒΓΠΕ ΓΌΠCΕ

		1	,
Agent	IP	Version	Description
SVR2012	10.10.10.37	13.3.0.4	Ready to be updated
agent Ma	chines Not <i>i</i>	Available for	· Deployment
Agent Ma	chines Not <i>i</i>	Available for Version	Deployment
_			

4. Click Next to start the upgrade process. Each agent will be upgraded. This window can be closed during the upgrade process. However, if it is kept active, it will display the status of the update as shown below.

🖋 Update Status					
Update Sta	itus				
Agent	IP	Old Version	New Version	Status	
BLSVR2012	10.10.10.37	13.3.0.4	13.3.0.5	Updated Successfully	
Query Prog	press			Ag	ent 1 of 1
			View Error	Query Close	Help

5. Click Close to complete the upgrade process.

APPENDIX B

Auditing EMC Isilon

Overview

The purpose of this section is to review steps required for EMC Isilon NAS devices with LT Auditor+.



NAS Auditing requires installation and configuration of the LT Auditor+ Syslog Server. Please review documentation on LT Auditor+ Syslog Server prior to undertaking the following steps.

1. Launch the LT Auditor+ Syslog Server and set up the following configurations as shown:

- Horns	Date mo	anica	0125
💀 LT Auditor+ Syslog Server Config Application			– 🗆 ×
Settings Rules			
Connection © UDP Port O TCP 514 Messages Message offset 4	0	3 1002	s per thread
Target event log NAS Auditing	O Log all messages with		og messages with custom Event Ids based on content
Target event log source NAS Auditing	Contains		EventID
	audit_protocol		4344
Exclude logging for messages containing specific text	audit_config		4345
	sshd		4346
Use as delimiter to exclude multiple texts	•		
			Delete
Use rules to log messages to new event log		Log debug messages	
Rules event log Rules event log source SyslogAuditing SyslogAuditing Log mess	ages to target event log	Interval to log data received/record	led stats (minutes)
			Save

- Target event log must be set to "NAS Auditing."
- Log Messages must be set to the following event IDs with content message as shown:
 - \circ audit_protocol 4344
 - \circ audit_config. 4345
 - o sshd 4346
- Set Message offset to 4. (See explanation below)

mind if the port is different from UDP 514, please update LT Auditor+ Syslog Server with the different settings.

NOTE

Isilon is an enterprise class data storage system that can handle petabytes of data. Auditing this device can generate a tremendous volume of data. LT Auditor+ can control what data received from Isilon is recorded or alerted on. However, the LT Auditor+ Syslog Server receives all data; therefore, it is vital that a dedicated instance of LT Auditor+ Syslog Server be used for auditing Isilon devices. In this environment, if auditing is required for other Syslog devices, please use another instance of the LT Auditor+ Syslog Server.

3. Confirm LT Auditor+ Syslog Server is receiving messages from the Isilon device by reviewing the event log NAS Auditing. Messages should become as shown below:

🛃 Event Viewer							
File Action View Help							
🗢 🏟 🖄 📰 🖬 🖬							
	NAS Auditing N	lumber of events: 28 (!) Nev	/ events avail	able			
 Custom Views Windows Logs 	Level	Date and Time	Source	Event ID	Task C		~
Application	() Information	12/11/2020 1:29:03 AM	NAS A	4344	None		
Security	(i) Information	12/11/2020 1:29:03 AM	NAS A		None		
Setup	(1) Information	12/11/2020 1:29:03 AM	NAS A	4344	None		
System	Information	12/11/2020 1:29:03 AM	NAS A	4344	None		
Forwarded Events	Information	12/11/2020 1:29:03 AM	NAS A	4344	None		
Applications and Services Lo	Information	12/11/2020 1:29:03 AM	NAS A	4344	None		
Hardware Events	 Information 	12/11/2020 1:29:03 AM	NAS A		None		
Internet Explorer Key Management Service	 Information 	12/11/2020 1:29:03 AM	NAS A		None		
LTALog	mormation	12/11/2020 1:29:03 AM	NAS A		None		
> Microsoft	(i) Information	12/11/2020 1:29:03 AM	NAS A	4344	None		~
NAS Auditing	Event 4344, NAS A	Auditing					×
On-premises data gatew.	General Date						_
> 🧾 OpenSSH	General Detail	s					
SyslogAuditing	< 30 × 2020-03	18T20-16-24-06-00 BLCLUST	FR-1 audit n	rotocol(220	31: DChrid1	1000004[System]1]192.168.114.1]SMBJSET_SECURITY]SUCCESSJFILE]4297263255J/ifs/Financials/AR/CurrentAccounts.docx	
Windows PowerShell	1000 2020-03	10120.10.24-00.00 0202031	en-radon_p	1010001220	oj. o cinispi	www.layseniiiise.roome.roome.lacoomeripo consiline (essessis) in a manualise (or contractor and or contractor	
🛗 Subscriptions							

NOTE

Ensure that Date stamp of event in the log appears after the number of characters specified in the Message Offset. Example: <30>2020-03-18T20:16:24-0600. There are four characters highlighted before the date stamp; therefore, message offset should be set to "4." If the offset value is not correct, LT Auditor+ will not be able to read the time stamp of the event.

4. Setup an LT Auditor+ filter to audit activity received from Isilon via the LT Auditor+ Syslog Server.

Il Files and Folders S and Folders Add Modify	Include Sub Folders All Files and Folders iles and Folders Add	Include Sub Folders All Files and Folders Files and Folders Add	☑ Include Sub Folders
Il Files and Folders s and Folders Add Modify	All Files and Folders Add Modify	All Files and Folders Files and Folders Add	
s and Folders Add Modify.,	Add Add	Files and Folders Add	
s and Folders Add	Add	Files and Folders Add	
Modify	Modify		All Files and Folders
			Files and Folders Add
	Delete	Modify.,	
	Delete		Modify
Delete		Delete	
		Delete	
		Delete	
			Modi
		Delete	
		Delete	
Delete		Delete	
Delete			Modify
		Modify	
			Files and Folders Add.,

Additional filters can be configured to include or exclude activity.

LT Auditor+ audits the following File/Folder Isilon operations as shown:

NAS Devices System Filter	
🖸 General 🖉 Operations 👔 User 🕐 Nodes 😂 Files and Folders 🛞 Actio 🖉 Notes	
All Operations Image: Second Secon	
OK Cancel	↓ Help

LT Auditor+ also audits the following config and login Isilon operations as shown:

NAS Devices System Filter B General Operations User Piles and Folders Piles and Folders	;
☐ All Operations	^
Directory Make Directory Remove Directory Rename Directory D- Access Directory D- Access Directory	
□ ♥ Login □ ♥ Login □ ♥ Success □ ♥ Logon Failure - Bad Password □ ♥ Logon Failure - Illegal User □ ♥ Logon Failure - Invalid User	
⊡ · ♥ Config □ · ♥ Config Update □ · ♥ Success	~
OK Cancel	Help

5. Use similar settings in the LT Auditor+ Report Console to report on Isilon activity.

NAS Devices Report Query Statement	×
Statement Name: Isilon Activity	
🖋 Operations 🔞 Files 🚯 Users 🥙 Nodes 🖫 Servers 🔞 Date & Time	
All Operations	
Include Operations	
C Exclude Operations	
File Directory File/Directory G- Gon Config	
OK Cancel Help	

Reports can be queried based on operations, files, users, and date and time criteria. A sample report is shown below:

Date & Time	User	Node	Operation	File	Server	Remarks
I/2/2020 5:51:50PM	NFS\root	137.15.98.37	Write File	\\ifs\dmnas\data\sapmnt-sap \pr1\global\sapcontrol\1_520 13_52014_28_2_20_scspr1 -vip	BLCLUSTER-2	Wrote to File \\ifs\dmnas\data\sapmnt-sap\pr1\glo bal\sapcontrol\ 1_52013_52014_28_ 2_20_scspr1-vip
/2/2020 5:51:50PM	NFS\root	137.15.98.37	Write File	\\ifs\dmnas\data\sapmnt-sap \pr1\global\sapcontrol\1_520 13_52014_28_2_20_scspr1 -vip	BLCLUSTER-2	Wrote to File \\ifs\dmnas\data\sapmnt-sap\pr1\glo bal\sapcontrol\ 1_52013_52014_28_ 2_20_scspr1-vip
1/3/2020 5:39:45PM	\hhh	192.15.2.246	Login	: Failed password for invalid user hhh from 192.15.2.246 port 51842 ssh2	BLCLUSTER-2	
1/3/2020 5:39:48PM	\hhh	192.15.2.246	Login	: Failed password for invalid user hhh from 192.15.2.246 port 51842 ssh2	BLCLUSTER-2	
1/3/2020 5:39:50PM	\hhh	192.15.2.246	Login	Failed password for invalid user hhh from 192.15.2.246 port 51842 ssh2	BLCLUSTER-2	
3/19/2020 2:07:34AM	SMB\JSmith	ip-192-168-11 4-1.ec2.intern al	Create File	\\ifs\Financials\AR\Delinque ntAccounts.xlxs	BLCLUSTER-1	Created File \\ifs\Financials\AR\DelinquentAccounts.xlxs
3/19/2020 2:07:34AM	SMB\JSmith	ip-192-168-11 4-1.ec2.intern al	Create File	\\ifs\Financials\AR\Delinque ntAccounts.xlxs	BLCLUSTER-1	Created File \\ifs\Financials\AR\DelinquentAccounts.xlxs
3/19/2020 2:10:10AM	SMB\DSam	ip-192-168-11 4-1.ec2.intern al	Delete File	\\ifs\Financials\AR\Delinque ntAccounts.xlxs	BLCLUSTER-1	Deleted File \\ifs\Financials\AR\DelinquentAccounts.xlxs
3/19/2020 2:10:10AM	SMB\DSam	ip-192-168-11 4-1.ec2.intern al	Delete File	\\ifs\Financials\AR\Delinque ntAccounts.xlxs	BLCLUSTER-1	Deleted File \\ifs\Financials\AR\DelinquentAccounts.xlxs
3/19/2020 2:11:58AM	SMB\HFox	ip-192-168-11 4-1.ec2.intern al	Access File	\\ifs\Financials\AR\CurrentA ccounts.docx	BLCLUSTER-1	Accessed File \\ifs\Financials\AR\CurrentAccounts docx
3/19/2020 2:11:58AM	SMB\HFox	ip-192-168-11 4-1.ec2.intern al	Access File	\\ifs\Financials\AR\CurrentA ccounts.docx	BLCLUSTER-1	Accessed File \\ifs\Financials\AR\CurrentAccounts docx
3/19/2020 2:16:24AM	SMB\DChris	ip-192-168-11 4-1.ec2.intern al	Write Security DACL	\\ifs\Financials\AR\CurrentA ccounts.docx	BLCLUSTER-1	Modified Security DACL of \\ifs\Financials\AR\CurrentAccounts docx

Copyright (c) Blue Lance, Inc. 2020. All rights reserved. www.BlueLance.com

Page 2