BLUE LANCE

Installation Guide

Table of Contents

Overview

This document covers the installation steps required for installing LT Auditor+ agents on SLES (SUSE LINUX ENTERPRISE SERVER) servers hosting OES to audit eDirectory and NSS file auditing. LT Auditor+ supports OES, OES2015 and OES2018.

Prerequisites

- LT Auditor+ 2013 framework with Manager, Management Console and Reporting Console must have been setup on a Windows server to receive information from the LT Auditor+ SLES agents.
- Root access to the SLES servers to install the LT Auditor+ agents.

Download distributions

The following downloads are available based on the OES version

Download Filename	OES version
LT_Auditor_SLES_Buildxxx.zip	OES SP3 on SLES 10/SLES 11
LT_Auditor_OES2015.zip	OES 2015 on SLES 11 SP3
LT_Auditor_OES2018.zip	OES 2018 on SLES 12

Each of these distributions contain multiple RPM file distributions that can be used on a SLES server based on your auditing requirement.

Installation

Installation of the LT Auditor+ SUSE Linux requires the following steps to be performed on the LT Auditor+ Manager.

1. Setup a Windows Share folder on the machine hosting the LT Auditor+ Manager;

2. Installation of the LT Auditor+ SUSE Linux RPM package on the SLES OES server;

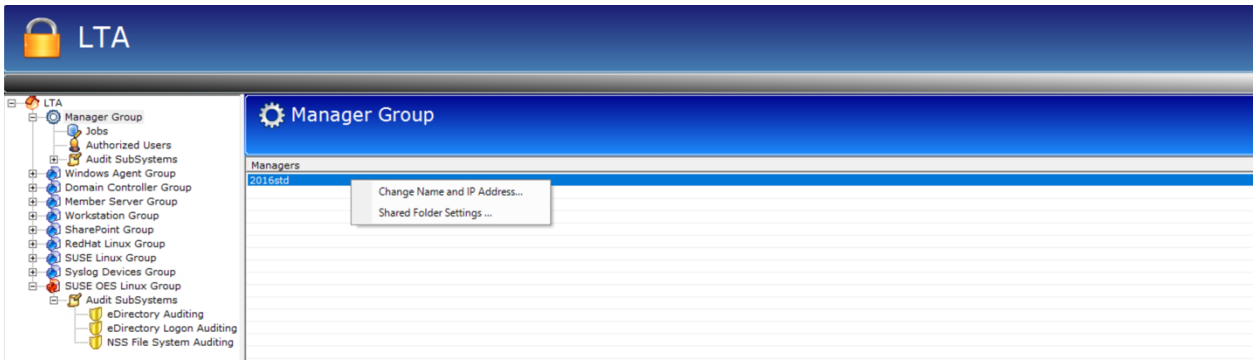
3. Establish a connection with the LT Auditor+ SUSE agent and the LT Auditor+ Manager;

4. Add the LT Auditor+ SUSE Linux agent into a SUSE Linux Agent Group on the Manager to deploy the filter policies and settings;

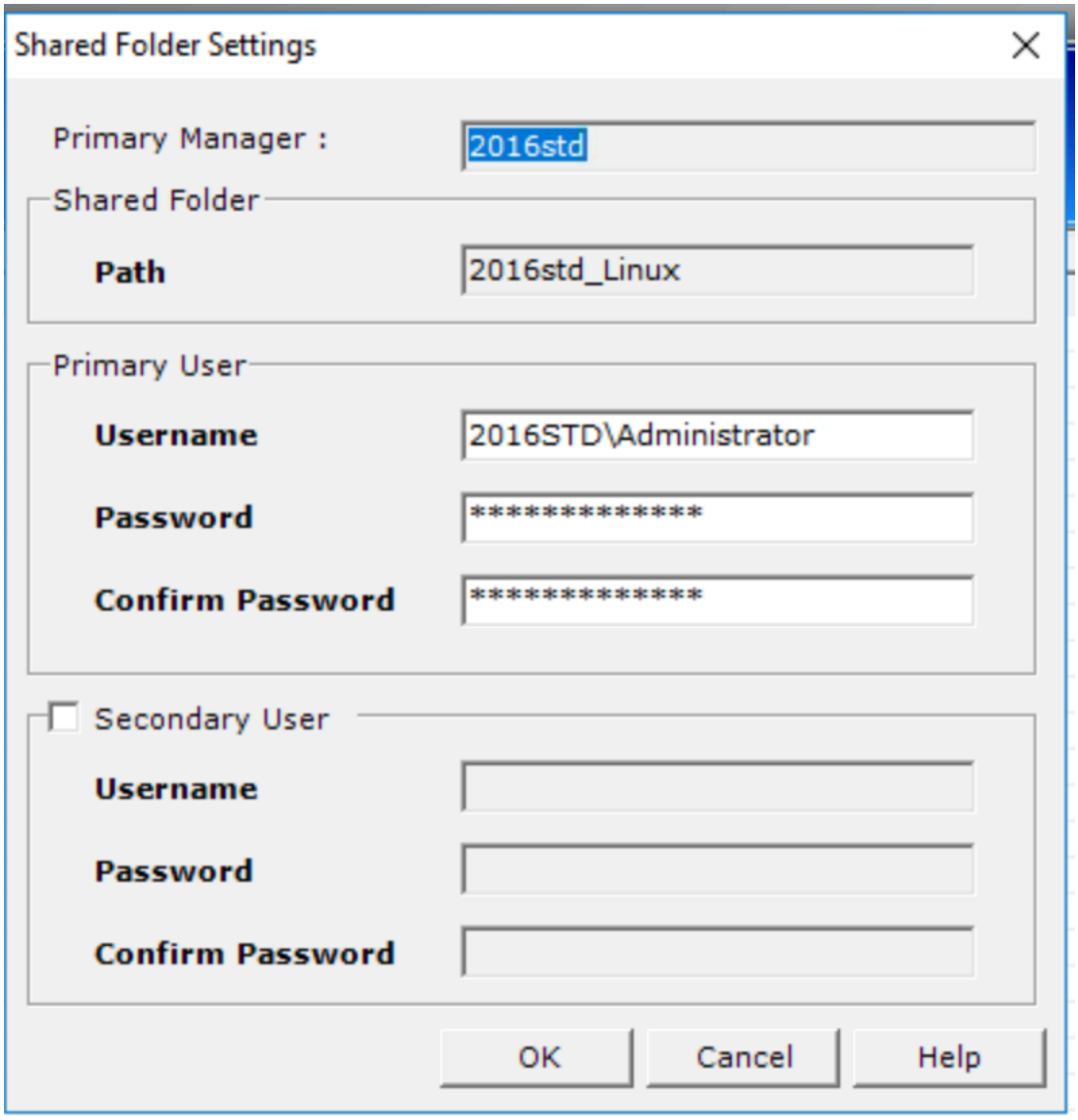
Set up the Windows Share Folder on the LT Auditor+ Manager.

A Windows Shared folder will be used to deploy all policies and configurations for all SUSE Linux agents. The SUSE Linux agents will also use this shared folder to transfer audit data to the LT Auditor+ Manager. The steps outlined below detail how the Share Folder setting can be setup.

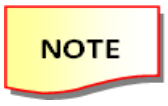
1. Launch the LT Auditor+ Management Console.
2. Click on any Manager group
3. Right click on the pane
4. The options to change Name and IP Address and Shared Folder appear as shown below.



5. Click on the *Share Folder Settings* option to display the Shared Folder Settings windows shown below:



6. Enter the username prefixed with the domain name or machine name
7. Enter password
8. Click OK to save.



The “Share Folder” displayed in the Path will be created. This folder will always have the name of the Manager machine concatenated with ‘_Linux’ as the name.

If the Manager is in a domain, on clicking OK, LT Auditor+ will assign the necessary permissions for the user specified. If the Manager is not in a domain, and if the user entered does not exist, the user will be created on the local machine and appropriate rights will assigned to the shared folder.

Installation of LT Auditor+ Agent on SLES OES Server

Copy the desired RPM to the server and use the command shown below to install the LT Auditor+ agent.

rpm –ivh LTAuditor+x-x.x.x-0.x86_64.rpm

After the installation of the rpm package, the /opt/bluelance folder is created along with following sub folders:

- /opt/bluelance/config
- /opt/bluelance/bin
- /opt/bluelance/lib
- /opt/bluelance/log

- /opt/bluelance/inbox
- /opt/bluelance/mnt
- /opt/bluelance/temp
- /opt/bluelance/outbox

Starting the Agent and establishing a connection with the LT Auditor+ SUSE agent and the LT Auditor+ Manager

Note: When using LT Auditor+ to audit NSS File System, please ensure that that the Novell auditing engine (Vigil) has been started.

To start LT Auditor+ agent/daemons, use the following command

/etc/init.d/ltaudit.rc start

When starting for the first time, The LT Auditor+ agents on SUSE Linux will need to establish a connection to the LT Auditor+ Manager. To do so, the program will show up the following prompts:

1. **Enter LT Auditor+ Windows Manager IP Address:<Please enter the IP address of the LT Auditor+ Manager>**

2. **Enter LT Auditor+ Windows Manager Share Name: <Enter the name of the share as discussed above e.g. ManageMachinename_Linux>**

3. **Enter LT Auditor+ Windows Manager Domain Name: <Enter the Domain name of the manager. If the manager is not in a domain enter the machine name>**

4. **Enter Username to Access Windows Share: <Enter Username>**

5. **Enter Password for User:**

If a connection was established successfully a mount point is created to the LT Auditor+ Manager's shared folder. The command *ls /opt/bluelance/mnt* will display folders on the shared drive. If a connection was not made error

are recorded in the file /opt/bluelance/log/ltstatus.log. The same folder contains nssstatus.log and edirstatus.log that display status of NSS and eDirectory auditing.

To view status of the LT Auditor+ daemons use the command

/etc/init.d/ltaudit.rc status

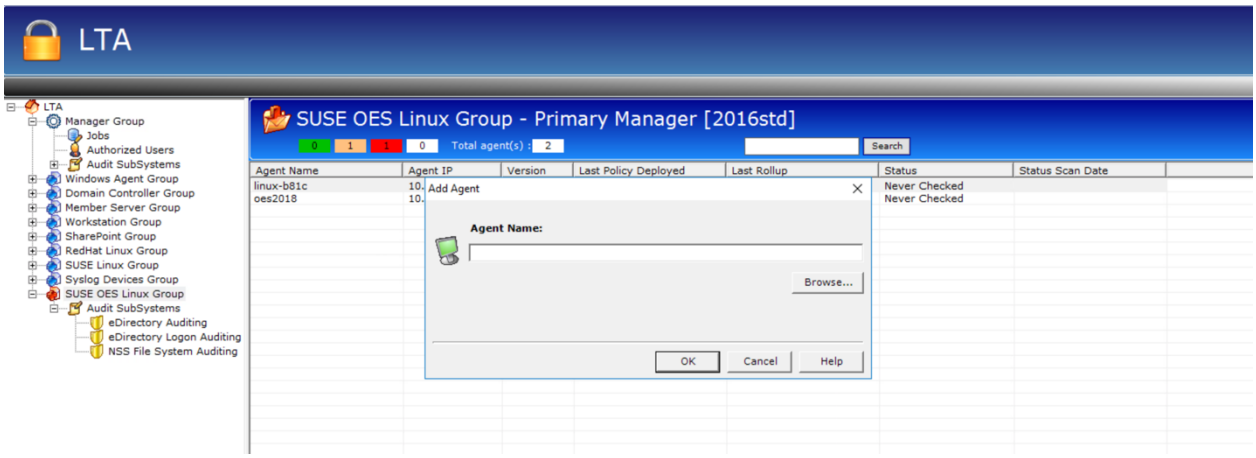
To stop the daemons use the command

/etc/init.d/ltaudit.rc stop

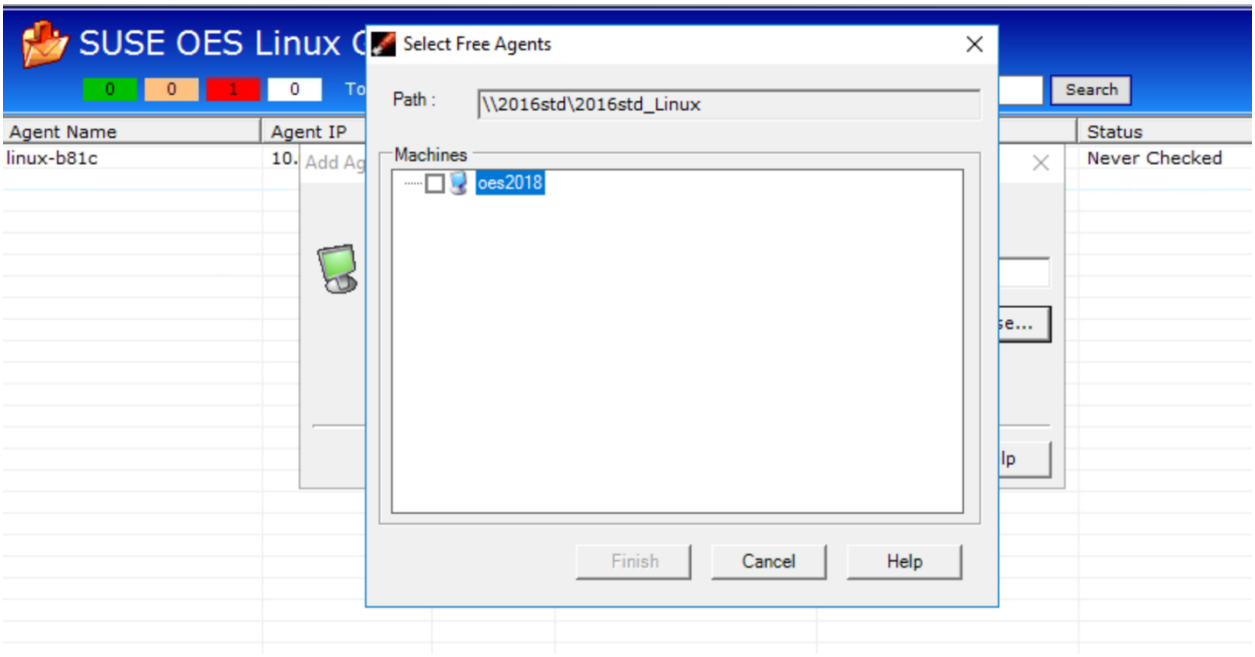
Add the LT Auditor+ SUSE Linux agent into a SUSE OES Linux Group on the Manager to deploy the appropriate filter policies and settings

To Add Agents to SUSE OES Linux Group:

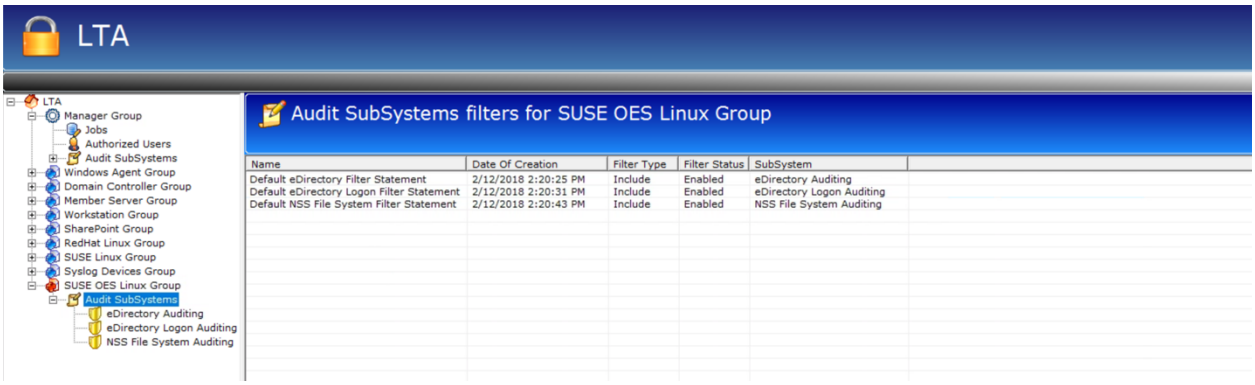
1. Right click on the SUSE OES Linux Group and click Add Agent to display screen shown below:



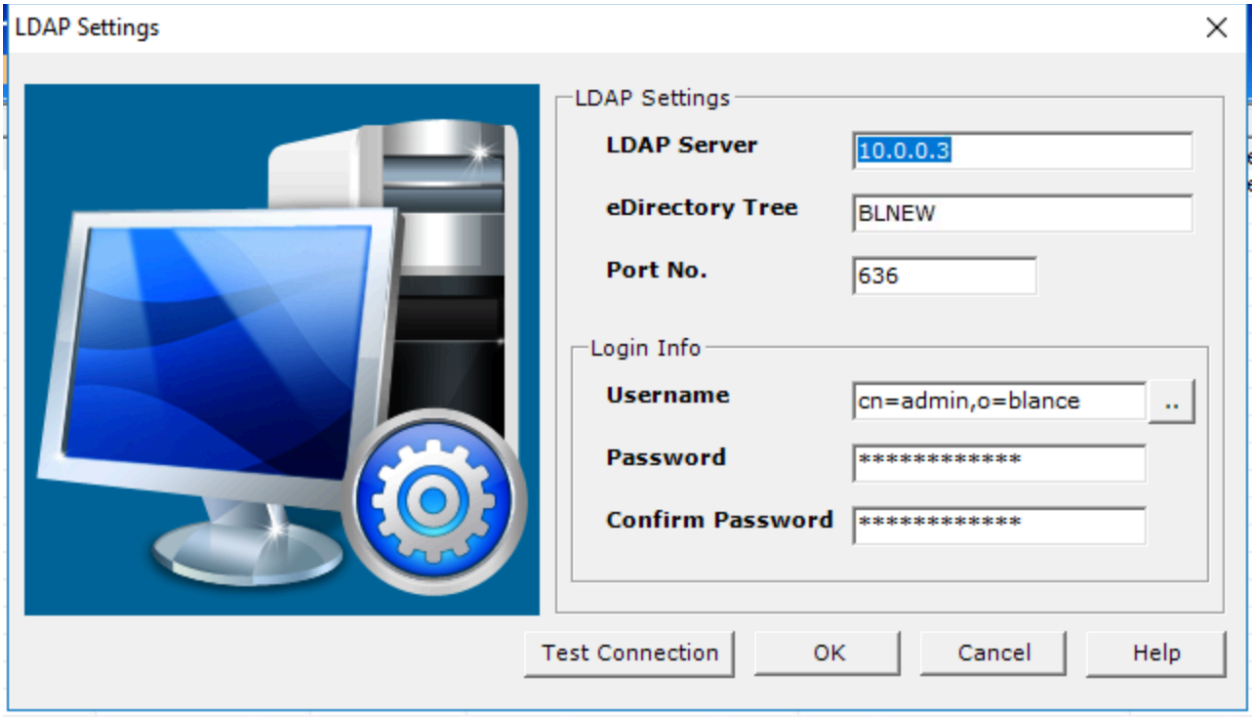
2. Click on the browse button to access the SLES agents that have not been assigned as shown below:



3. Select the agent(s) and click Finish.
4. Follow guidelines in the LT Auditor+ 2013: Configuration guide to setup policies for eDirectory and NSS auditing that define the audit data collected on SLES servers. After the policies have been setup, they will be listed as shown:



5. To successfully audit eDirectory the SLES agents would need to login to eDirectory with admin credentials. To configure, right click on the SUSE OES Linux Group and click LDAP Setting to bring up the LDAP Setting window:



6. Enter all information requested and test the connection. Port 636 is used for a TLS connection and 389 is used for a non-TLS connection.
7. Click OK to save.
8. Information on how to generate reports on data collected for eDirectory and NSS is available in the Configuration guide.